Acronis

acronis.com

Cyber Protection

24.03

Benutzeranleitung

REVISION: 11.04.2024

Inhaltsverzeichnis

Erste Schritte mit Cyber Protection

Das Konto aktivieren

Wenn ein Administrator ein Konto für Sie erstellt, wird eine E-Mail-Nachricht an Ihre E-Mail-Adresse gesendet. Die Nachricht enthält folgende Informationen:

- **Ihr Anmeldename.** Dies ist der Benutzername, mit dem Sie sich anmelden. Ihr Anmeldename wird auch auf der Kontoaktivierungsseite angezeigt.
- **Konto aktivieren**-Schaltfläche. Klicken Sie auf die Schaltfläche und legen Sie das Kennwort für Ihr Konto fest. Stellen Sie sicher, dass Ihr Kennwort mindestens neun Zeichen lang ist. Weitere Informationen über Kennwörter finden Sie im Abschnitt '"Anforderungen an das Kennwort" (S. 20)'.

Wenn Ihr Administrator die Zwei-Faktor-Authentifizierung aktiviert hat, werden Sie aufgefordert, diese für Ihr Konto einzurichten. Weitere Informationen dazu finden Sie im Abschnitt '"Zwei-Faktor-Authentifizierung" (S. 20)'.

Anforderungen an das Kennwort

Das Kennwort für ein Benutzerkonto muss mindestens 9 Zeichen lang sein. Kennwörter werden zudem auf ihre Komplexität geprüft und dabei in eine der folgenden Kategorien eingeteilt:

- Schwach
- Mittel
- Stark

Ein schwaches Kennwort kann nicht gespeichert werden, auch wenn es 9 oder mehr Zeichen enthält. Kennwörter, die den Benutzernamen, den Anmeldenamen, die Benutzer-E-Mail-Adresse oder den Namen des Mandanten, zu dem ein Benutzerkonto gehört, enthalten, gelten immer als schwach. Auch Kennwörter, die besonders gängig sind, werden als schwach eingestuft.

Wenn Sie ein Kennwort stärker machen wollen, fügen Sie ihm mehr Zeichen hinzu. Es ist nicht zwingend notwendig, unterschiedliche Zeichentypen (wie Zahlen, Groß- und Kleinbuchstaben oder Sonderzeichen) zu verwenden. Aber damit können stärkere oder kürzere Kennwörter erzeugt werden.

Zwei-Faktor-Authentifizierung

Die Zwei-Faktor-Authentifizierung (2FA) bietet einen zusätzlichen Schutz gegen unbefugte Zugriffe auf Ihr Konto. Wenn die 2FA eingerichtet ist, müssen Sie Ihr Kennwort (der erste Faktor) und einen Einmalcode (der zweite Faktor) eingeben, um sich an der Cyber Protect-Konsole anmelden zu können. Der Einmalcode, der auch Einmalkennwort genannt wird, wird von einer speziellen Applikation generiert, die auf Ihrem Smartphone oder einem anderen Gerät, das Ihnen gehört,

installiert werden muss. Selbst wenn jemand Ihre normalen Anmeldedaten herausfinden sollte, kann diese Person sich nicht anmelden, wenn sie nicht auch Zugriff auf Ihr Zweit-Faktor-Geräte hat.

So können Sie die Zwei-Faktor-Authentifizierung für Ihr Konto einrichten

Sie müssen 2FA für Ihr Konto einrichten, wenn der Administrator es für Ihre Organisation aktiviert hat. Wenn der Administrator die 2FA aktiviert, während Sie noch an der Cyber Protect-Konsole angemeldet sind, müssen Sie sie konfigurieren, wenn Ihre aktuelle Sitzung abläuft.

Voraussetzungen

- Die Zwei-Faktor-Authentifizierung wurde von einem Administrator für Ihre Organisation aktiviert.

So können Sie die Zwei-Faktor-Authentifizierung für Ihr Konto einrichten

1. Installieren Sie eine Authenticator-App auf Ihrem Mobilgerät.
   Beispiele für Authenticator-Apps:
   - Twilio Authy
   - Microsoft Authenticator
   - Google Authenticator
2. Scannen Sie den QR-Code mit Ihrer Authenticator-App und geben Sie dann den 6-stelligen Code ein, der in der Authenticator-App im Fenster **Zwei-Faktor-Authentifizierung einrichten** angezeigt wird.
3. Klicken Sie auf **Weiter**.
   Es werden Anweisungen angezeigt, wie Sie den Zugriff auf Ihr Konto wiederherstellen können, wenn Sie Ihr 2FA-Gerät verloren oder die Authenticator-App deinstalliert haben sollten.
4. Speichern oder drucken Sie die PDF-Datei aus.

   Hinweis
   Stellen Sie sicher, dass Sie die PDF-Datei an einem sicheren Ort speichern oder drucken Sie diese zur späteren Verwendung aus. Dies ist der beste Weg, um Ihren Zugriff wiederherzustellen.

5. Wechseln Sie wieder zur Anmeldeseite der Cyber Protect-Konsole und geben Sie den generierten Code ein.
   Jeder Einmalcode ist nur für 30 Sekunden gültig. Wenn Sie länger als 30 Sekunden gewartet haben, können Sie den nächsten generierten Code verwenden.

Wenn Sie sich das nächste Mal anmelden, können Sie das Kontrollkästchen **Diesem Browser vertrauen...** aktivieren. Dann wird der Code für spätere Anmeldungen, die über diesen Browser auf dieser Maschine erfolgen, nicht mehr benötigt.

Hinweis
Wir empfehlen Ihnen, dass Sie dieses Kontrollkästchen deaktiviert lassen. Ansonsten werden Sie nicht mehr auf die 2FA für Ihr Konto zugreifen können.

So können Sie die Zwei-Faktor-Authentifizierung (2FA) auf einem neuen Gerät wiederherstellen

Wenn Sie Zugriff auf die zuvor eingerichtete Authentifizierungs-App für Mobilgeräte haben

1. Installieren Sie eine Authenticator-App auf Ihrem neuen Gerät.
2. Verwenden Sie die PDF-Datei, die Sie beim Konfigurieren der 2FA auf Ihrem Gerät gesichert haben. Diese Datei enthält den 32-stelligen Code, den Sie in der Authenticator-App eingeben müssen, um die Authenticator-App erneut mit Ihrem Acronis Konto verknüpfen zu können.

   Wichtig
   Wenn der Code nicht funktioniert, stellen Sie sicher, dass die Uhrzeit in der Authenticator-App mit Ihrem Gerät synchronisiert ist.

   Wenn Sie die PDF-Datei nicht während der Einrichtung gespeichert haben:

a. Klicken Sie auf **2FA zurücksetzen** und geben Sie das Einmalkennwort ein, das in der Authenticator-App für Mobilgeräte angezeigt wird.
b. Folgen Sie den Bildschirmanweisungen.

Wenn Sie keinen Zugriff auf die zuvor eingerichtete Authenticator-App für Mobilgeräte haben:

1. Nehmen Sie ein neues Mobilgerät.
2. Verwenden Sie die gespeicherte PDF-Datei, um ein neues Gerät zu verknüpfen (der Standardname der Datei ist `cyberprotect-2fa-backupcode.pdf`).
3. Stellen Sie den Zugriff auf Ihr Konto aus dem Backup wieder her. Stellen Sie sicher, dass Backups von Ihrer Mobilgeräte-App unterstützt werden.
4. Öffnen Sie die App unter dem gleichen Konto von einem anderen Mobilgerät aus, wenn dies von der App unterstützt wird.

Datenschutzeinstellungen

Über die Datenschutzeinstellungen können Sie angeben, ob Sie mit der Erfassung, Verwendung und Offenlegung Ihrer persönlichen Daten einverstanden sind oder nicht.

In Abhängigkeit von dem Land, in dem Sie Cyber Protect Cloud verwenden, und dem Cyber Protect Cloud Datacenter, das Ihnen bestimmte Services bereitstellt, werden Sie bei der ersten Nutzung von Cyber Protect Cloud möglicherweise aufgefordert zu bestätigen, ob Sie mit der Verwendung von Google Analytics in Cyber Protect Cloud einverstanden sind.

Mithilfe von Google Analytics können wir das Nutzerverhalten besser verstehen und die Nutzererfahrung in Cyber Protect Cloud verbessern, indem wir pseudonymisierte Daten sammeln.

Auch wenn Sie Google Analytics beim ersten Start von Cyber Protect Cloud aktiviert oder abgelehnt haben, können Sie Ihre Entscheidung später jederzeit wieder ändern.

So können Sie Google Analytics aktivieren oder deaktivieren

1. Klicken Sie in der Cyber Protect-Konsole auf **Konto verwalten**.
2. Klicken Sie in der rechten oberen Ecke auf das Symbol für 'Konto'.

3. Wählen Sie **Meine Datenschutzeinstellungen** aus. Das Fenster **Meine Datenschutzeinstellungen** wird angezeigt.
4. Klicken Sie im Bereich **Google Analytics-Datenerhebung** auf eine der folgenden Schaltflächen:
   - **An** – um Google Analytics zu aktivieren
   - **Aus** – um Google Analytics zu deaktivieren

Im Bereich **So können Sie Cookies löschen** können Sie Cookies direkt in Ihrem Browser kontrollieren und verwalten.

Hinweis
Wenn Sie den Google Analytics-Bereich nicht sehen, bedeutet dies, dass Google Analytics in Ihrem Land nicht verwendet wird.

Im Bereich **Produktinternes Onboarding und interaktive Hilfe**, der anfänglich während des Testzeitraums angezeigt wird, können Sie einstellen, ob Sie zukünftig Informationen über Verbesserungen und neue Programmfunktionen erhalten wollen oder nicht.features in the program in the future. Diese Funktion ist standardmäßig eingeschaltet. Sie können diese jedoch deaktivieren, indem Sie den Umschalter auf **Aus** setzen.

Zugriff auf den Cyber Protection Service

Nachdem Sie Ihr Konto aktiviert haben, können Sie auf den Cyber Protection Service zugreifen, indem Sie sich an der Cyber Protect-Konsole oder über das Management-Portal anmelden.

So können Sie sich an der Cyber Protect-Konsole anmelden

1. Gehen Sie zur Cyber Protection Service-Anmeldeseite.
2. Geben Sie Ihren Anmeldenamen ein und klicken Sie dann auf **Weiter**.
3. Geben Sie Ihr Kennwort ein und klicken Sie dann auf **Weiter**.
4. [Wenn Sie mehr als einen Cyber Protect Cloud Service verwenden] Klicken Sie auf **Cyber Protection**.
   Benutzer, die nur Zugriff auf den Cyber Protection Service haben, melden sich direkt an der Cyber Protect-Konsole an.
   Wenn **Cyber Protection** nicht der einzige Service ist, den Sie Zugriff haben, können Sie über das Symbol  in der rechten oberen Ecke zwischen den Services umschalten. Administratoren können über das Symbol auch zum Management-Portal wechseln.

Das Zeitlimit für die Cyber Protect-Konsole beträgt 24 Stunden für aktive Sitzungen und 1 Stunde für inaktive Sitzungen.

Sie können die Sprache der Weboberfläche ändern, wenn Sie auf das Symbol für 'Konto' in der oberen rechten Ecke klicken.

So können Sie über das Management-Portal auf die Cyber Protect-Konsole zugreifen

1. Gehen Sie im Management-Portal zu **Monitoring** –> **Nutzung**.
2. Wählen Sie unter **Cyber Protect** das Element **Schutz** und klicken Sie dann auf **Service verwalten**.
   Alternativ können Sie unter **Clients** einen Kunden auswählen und dann auf **Service verwalten** klicken.

Als Ergebnis werden Sie auf die Cyber Protect-Konsole umgeleitet.

Wichtig
Wenn sich der Kunde im Verwaltungsmodus **Self-Service** befindet, können Sie keine Services für ihn verwalten. Nur die Kunden-Administratoren können den Modus des Kunden auf **Durch den Service-Provider verwaltet** ändern und dann die Services verwalten.

So können Sie Ihr Kennwort zurücksetzen

1. Gehen Sie zur Cyber Protection Service-Anmeldeseite.
2. Geben Sie Ihren Anmeldenamen ein und klicken Sie dann auf **Weiter**.
3. Klicken Sie auf **Kennwort vergessen?**
4. Bestätigen Sie, dass Sie weitere Anweisungen erhalten wollen, indem Sie auf **Senden** klicken.
5. Befolgen Sie die Anweisungen in der E-Mail, die Sie empfangen haben.
6. Legen Sie Ihr neues Kennwort fest.

Software-Anforderungen

Unterstützte Webbrowser

Die Cyber Protect-Konsole verwendet das TLS 1.2-Protokoll und unterstützt folgende Webbrowser:

- Google Chrome 29 (oder höher)
- Mozilla Firefox 23 (oder höher)
- Opera 16 (oder höher)
- Microsoft Edge 25 (oder höher)
- Safari 8 (oder höher), unter den Betriebssystemen macOS oder iOS ausgeführt

In anderen Webbrowsern (inkl. Safari-Browser, die unter anderen Betriebssystem laufen) wird möglicherweise die Benutzeroberfläche nicht korrekt angezeigt oder stehen einige Funktionen nicht zur Verfügung.

Unterstützte Betriebssysteme und Umgebungen

Agent für Windows

Dieser Agent enthält eine Komponente für die Antivirus & Antimalware Protection und URL-Filterung. Siehe Abschnitt '"Unterstützte Schutzfunktionen, nach Betriebssystem" (S. 46)' für weitere Informationen über Funktionalität, die je nach Betriebssystem unterstützt wird.

- Windows XP Professional SP1 (x64), SP2 (x64), SP3 (x86)
- Windows Server 2003 SP1/2003 R2 und höher – die Editionen Standard und Enterprise (x86, x64)
- Windows Small Business Server 2003/2003 R2
- Windows Server 2008, Windows Server 2008 SP2* – die Editionen Standard, Enterprise, Datacenter, Foundation und Web (x86, x64)
- Windows Small Business Server 2008, Windows Small Business Server 2008 SP2*
- Windows 7 – alle Editionen

Hinweis
Wenn Sie Cyber Protection noch mit Windows 7 verwenden wollen, müssen Sie sicherstellen, dass Sie folgende Updates von Microsoft installiert haben, bevor Sie den Protection Agenten installieren:

- Windows 7 Extended Security Updates (ESU)
- KB4474419
- KB4490628

Weitere Informationen zu den erforderlichen Updates finden Sie in diesem Knowledge Base-Artikel.

- Windows Server 2008 R2* – die Editionen Standard, Enterprise, Datacenter, Foundation und Web
- Windows Home Server 2011*
- Windows MultiPoint Server 2010*/2011*/2012
- Windows Small Business Server 2011* – alle Editionen
- Windows 8/8.1 – alle Editionen (x86, x64), ausgenommen Windows RT
- Windows Server 2012/2012 R2 – alle Editionen
- Windows Storage Server 2003/2008/2008 R2/2012/2012 R2/2016
- Windows 10 – Home, Pro, Education, Enterprise, IoT Enterprise und LTSC Editionen (früher LTSB)
- Windows Server 2016 – alle Installationsoptionen, mit Ausnahme des Nano Servers
- Windows Server 2019 – alle Installationsoptionen, mit Ausnahme des Nano Servers
- Windows 11 – alle Editionen
- Windows Server 2022 – alle Installationsoptionen, mit Ausnahme des Nano Servers

Hinweis

* Wenn Sie Cyber Protection mit dieser Version von Windows verwenden wollen, müssen Sie das Update zur Unterstützung der SHA-2-Codesignierung von Microsoft (KB4474419) installieren, bevor Sie den Protection Agenten installieren können.

Informationen zu Problemen im Zusammenhang mit dem SHA-2-Codesignierungs-Patch finden Sie in diesem Knowledge Base-Artikel.

Agent für SQL, Agent für Active Directory, Agent für Exchange (für Datenbank-Backups und applikationskonformen Backups)

Jeder dieser Agenten kann auf einer Maschine installiert werden, die unter einem der oben aufgeführten Betriebssysteme läuft und eine unterstützte Version der entsprechenden Applikation ausführt.

Agent für Data Loss Prevention

Gerätekontrolle

- Microsoft Windows 7 Service Pack 1 und höher
- Microsoft Windows Server 2008 R2 und höher
- macOS 10.15 (Catalina)
- macOS 11.2.3 (Big Sur)
- macOS 12 (Monterey)
- macOS 13 (Ventura)

Hinweis

Der Agent für Data Loss Prevention für macOS unterstützt nur x64-Prozessoren. ARM-basierte Apple Silicon-Prozessoren werden nicht unterstützt.

Data Loss Prevention

- Microsoft Windows 7 Service Pack 1 und höher
- Microsoft Windows Server 2008 R2 und höher

Hinweis

Der Agent für Data Loss Prevention kann auf nicht-unterstützten macOS-Systemen installiert werden, da er ein integraler Bestandteil von Agent für Mac ist. In diesem Fall wird die Cyber Protect-Konsole anzeigen, dass der Agent für Data Loss Prevention auf dem Computer installiert ist, aber die Gerätekontrolle-Funktionalität wird nicht funktionieren. Die Gerätekontrolle-Funktionalität funktioniert nur auf macOS-Systemen, die vom Agenten für Data Loss Prevention unterstützt werden.

Agent für Advanced Data Loss Prevention

- Microsoft Windows 7 Service Pack 1 und höher
- Microsoft Windows Server 2008 R2 und höher

Agent für File Sync & Share

Die Liste der unterstützten Betriebssysteme finden Sie in der Benutzeranleitung für Cyber Files Cloud.

Agent für Exchange (für Postfach-Backups)

- Windows Server 2008 – die Editionen Standard, Enterprise, Datacenter, Foundation und Web (x86, x64)
- Windows Small Business Server 2008
- Windows 7 – alle Editionen
- Windows Server 2008 R2 – die Editionen Standard, Enterprise, Datacenter, Foundation und Web
- Windows MultiPoint Server 2010/2011/2012
- Windows Small Business Server 2011 – alle Editionen
- Windows 8/8.1 – alle Editionen (x86, x64), ausgenommen Windows RT
- Windows Server 2012/2012 R2 – alle Editionen
- Windows Storage Server 2008/2008 R2/2012/2012 R2
- Windows 10 – die Editionen Home, Pro, Education und Enterprise
- Windows Server 2016 – alle Installationsoptionen, mit Ausnahme des Nano Servers
- Windows Server 2019 – alle Installationsoptionen, mit Ausnahme des Nano Servers
- Windows 11 – alle Editionen
- Windows Server 2022 – alle Installationsoptionen, mit Ausnahme des Nano Servers

Agent für Microsoft 365

- Windows Server 2008 – die Editionen Standard, Enterprise, Datacenter, Foundation und Web (nur x64)
- Windows Small Business Server 2008
- Windows Server 2008 R2 – die Editionen Standard, Enterprise, Datacenter, Foundation und Web
- Windows Home Server 2011
- Windows Small Business Server 2011 – alle Editionen
- Windows 8/8.1 – alle Editionen (nur x64), ausgenommen Windows RT
- Windows Server 2012/2012 R2 – alle Editionen

- Windows Storage Server 2008/2008 R2/2012/2012 R2/2016 (nur x64)
- Windows 10 – die Editionen Home, Pro, Education und Enterprise (nur x64)
- Windows Server 2016 – alle Installationsoptionen (nur x64), mit Ausname des Nano Servers
- Windows Server 2019 – alle Installationsoptionen (nur x64), mit Ausname des Nano Servers
- Windows 11 – alle Editionen
- Windows Server 2022 – alle Installationsoptionen, mit Ausnahme des Nano Servers

Agent für Oracle

- Windows Server 2008 R2 – Standard, Enterprise, Datacenter und Web Editionen (x86, x64)
- Windows Server 2012 R2 – Standard, Enterprise, Datacenter und Web Editionen (x86, x64)
- Linux – alle Kernel und Distributionen, die vom Agenten für Linux unterstützt werden (wie unten aufgelistet)

Agent für MySQL/MariaDB

- Linux – alle Kernel und Distributionen, die vom Agenten für Linux unterstützt werden (wie unten aufgelistet)

Agent für Linux

Dieser Agent enthält eine Komponente für die Antivirus & Antimalware Protection und URL-Filterung. Siehe Abschnitt '"Unterstützte Schutzfunktionen, nach Betriebssystem" (S. 46)' für weitere Informationen über Funktionalität, die je nach Betriebssystem unterstützt wird.

Die nachfolgenden Linux-Distributionen und Kernel-Versionen wurden speziell getestet. Aber auch wenn Ihre Linux-Distribution oder Kernel-Version nicht in der nachfolgenden Liste aufgeführt ist, kann sie aufgrund der Besonderheiten der Linux-Betriebssysteme dennoch in allen erforderlichen Szenarien korrekt funktionieren.

Wenn bei Ihrer Kombination aus Linux-Distribution und Kernel-Version bei der Verwendung von Cyber Protection Probleme auftreten, können Sie sich für weitere Untersuchungen an den Support wenden.

Linux mit Kernel 2.6.9 bis 5.19 und glibc 2.3.4 oder höher, inklusive der folgenden x86- und x86_64-Distributionen:

- Red Hat Enterprise Linux 4.x, 5.x, 6.x, 7.x, 8.x*, 9.0*, 9.1*, 9.2*, 9.3*
- Ubuntu 9.10, 10.04, 10.10, 11.04, 11.10, 12.04, 12.10, 13.04, 13.10, 14.04, 14.10, 15.04, 15.10, 16.04, 16.10, 17.04, 17.10, 18.04, 18.10, 19.04, 19.10, 20.04, 20.10, 21.04, 21.10, 22.04, 22.10, 23.04
- Fedora 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 37, 38
- SUSE Linux Enterprise Server 10, 11, 12, 15

Wichtig
Konfigurationen mit Btrfs werden nicht für SUSE Linux Enterprise Server 12 und SUSE Linux Enterprise Server 15 unterstützt.

- Debian 4.x, 5.x, 6.x, 7.0, 7.2, 7.4, 7.5, 7.6, 7.7, 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.11, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 9.7, 9.8, 10, 11
- CentOS 5.x, 6.x, 7.x, 8.x*
- CentOS Stream 8*, 9*
- Oracle Linux 5.x, 6.x, 7.x, 8.x*, 9.0*, 9.1*, 9.2* – sowohl Unbreakable Enterprise Kernel als auch Red Hat Compatible Kernel

Hinweis
Für die Installation des Protection Agenten auf einem System mit Oracle Linux 8.6 und höher, auf dem Secure Boot aktiviert ist, müssen die Kernel-Module manuell signiert werden. Weitere Informationen darüber, wie Sie ein Kernel-Modul signieren können, finden Sie in diesem Knowledge Base-Artikel.

- CloudLinux 5.x, 6.x, 7.x, 8.x*
- ClearOS 5.x, 6.x, 7.x
- AlmaLinux 8.x*,9.0*, 9.1*, 9.2*
- Rocky Linux 8.x*, 9.0*, 9.1*, 9.2*, 9.3*
- ALT Linux 7.0

* Ab Version 8.4, wird nur mit Kerneln von 4.18 bis 5.19 unterstützt

Agent für Mac

Dieser Agent enthält eine Komponente für die Antivirus & Antimalware Protection und URL-Filterung. Siehe Abschnitt '"Unterstützte Schutzfunktionen, nach Betriebssystem" (S. 46)' für weitere Informationen über Funktionalität, die je nach Betriebssystem unterstützt wird.

Es werden sowohl die x64- als auch die ARM-Architektur (die in Apple Silicon-Prozessoren wie dem Apple M1 und M2 verwendet wird) unterstützt.

Hinweis
Sie können keine Laufwerk-Backups von Intel-basierten Macs auf Macs wiederherstellen, die einen Apple Silicon-Prozessor verwenden (oder umgekehrt). Sie können jedoch einzelne Dateien und Ordner wiederherstellen.

- macOS High Sierra 10.13
- macOS Mojave 10.14
- macOS Catalina 10.15

- macOS Big Sur 11
- macOS Monterey 12
- macOS Ventura 13
- macOS Sonoma 14

Wichtig
Folgende Betriebssysteme werden von Cyber Protect Cloud ab Version C23.07 nicht mehr unterstützt: OS X Yosemite 10.10, OS X El Capitan 10.11 und macOS Sierra 10.12.

Wir empfehlen dringend, dass Sie Ihr Betriebssystem auf eine der unterstützten Versionen aktualisieren, um die weitere Kompatibilität zu gewährleisten und von der vollen Funktionalität von Cyber Protect Cloud profitieren zu können.

Agent für VMware (Virtuelle Appliance)

Dieser Agent wird als eine virtuelle Appliance ausgeliefert, die auf einem ESXi-Host ausgeführt werden kann.

VMware ESXi 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7.0, 8.0

Agent für VMware (Windows)

Dieser Agent wird in Form einer Windows-Applikation ausgeliefert und kann unter jedem Betriebssystem ausgeführt werden, welches weiter oben für den Agenten für Windows aufgelistet wurde – mit folgenden Ausnahmen:

- 32-Bit-Betriebssysteme werden nicht unterstützt.
- Windows XP, Windows Server 2003/2003 R2 und Windows Small Business Server 2003/2003 R2 werden nicht unterstützt.

Agent für Hyper-V

- Windows Server 2008 (nur x64) mit Hyper-V-Rolle, inklusive Server Core-Installationsmodus
- Windows Server 2008 R2 mit Hyper-V-Rolle, inklusive Server Core-Installationsmodus
- Microsoft Hyper-V Server 2008/2008 R2
- Windows Server 2012/2012 R2 mit Hyper-V-Rolle, inklusive Server Core-Installationsmodus
- Microsoft Hyper-V Server 2012/2012 R2
- Windows 8, 8.1 (nur x64) mit Hyper-V
- Windows 10 – die Editionen Pro, Education und Enterprise mit Hyper-V
- Windows Server 2016 mit Hyper-V-Rolle – alle Installationsoptionen, mit Ausnahme des Nano Servers
- Microsoft Hyper-V Server 2016

- Windows Server 2019 mit Hyper-V-Rolle – alle Installationsoptionen, mit Ausnahme des Nano Servers
- Microsoft Hyper-V Server 2019
- Windows Server 2022 – alle Installationsoptionen, mit Ausnahme des Nano Servers

Agent für Virtuozzo

- Virtuozzo 6.0.10, 6.0.11, 6.0.12, 7.0.13, 7.0.14
- Virtuozzo Hybrid Server 7.5

Agent für Virtuozzo Hybrid Infrastructure

Virtuozzo Hybrid Infrastructure 3.5, 4.0, 4.5, 4.6, 4.7, 5.0, 5.1, 5.2, 5.3, 5.4, 6.0

Agent für Scale Computing HC3

Scale Computing Hypercore 8.8, 8.9, 9.0, 9.1, 9.2, 9.3

Agent für oVirt

Red Hat Virtualization 4.2, 4.3, 4.4, 4.5

Agent für Synology

DiskStation Manager 6.2.x, 7.x

Der Agent für Synology unterstützt nur NAS-Geräte mit x86_64-Prozessoren. ARM-Prozessoren werden nicht unterstützt.

Cyber Protect Monitor

- Windows 7 und höher
- Windows Server 2008 R2 und höher
- Alle macOS-Versionen, die vom Agenten für Mac unterstützt werden

Unterstützte Microsoft SQL Server-Versionen

- Microsoft SQL Server 2022
- Microsoft SQL Server 2019
- Microsoft SQL Server 2017
- Microsoft SQL Server 2016
- Microsoft SQL Server 2014
- Microsoft SQL Server 2012
- Microsoft SQL Server 2008 R2

- Microsoft SQL Server 2008
- Microsoft SQL Server 2005

Die SQL Server Express-Editionen der oben genannten SQL Server-Versionen werden ebenfalls unterstützt.

Hinweis
Ein Microsoft SQL-Backup wird nur für Datenbanken unterstützt, die unter den Dateisystemen NFTS, REFS oder FAT32 laufen. ExFat wird nicht unterstützt.

Unterstützte Microsoft Exchange Server-Versionen

- Microsoft Exchange Server 2019 – alle Editionen.
- Microsoft Exchange Server 2016 – alle Editionen.
- Microsoft Exchange Server 2013 – alle Editionen, Kumulatives Update 1 und höher.
- Microsoft Exchange Server 2010 – alle Editionen, alle Service Packs. Postfach-Backup und granulares Recovery von Datenbank-Backups wird ab Service Pack 1 (SP1) unterstützt.
- Microsoft Exchange Server 2007 – alle Editionen, alle Service Packs. Postfach-Backup und granulares Recovery von Datenbank-Backups wird nicht unterstützt.

Unterstützte Microsoft SharePoint-Versionen

Cyber Protection unterstützt folgende Microsoft SharePoint-Versionen:

- Microsoft SharePoint 2013
- Microsoft SharePoint Server 2010 SP1
- Microsoft SharePoint Foundation 2010 SP1
- Microsoft Office SharePoint Server 2007 SP2*
- Microsoft Windows SharePoint Services 3.0 SP2*

*Um den SharePoint Explorer mit diesen Versionen verwenden zu können, benötigen Sie eine SharePoint-Wiederherstellungsfarm, an welche Sie die Datenbanken anfügen können.

Die Datenbanken, aus denen Sie Daten extrahieren, müssen von derselben SharePoint-Version stammen wie diejenige, wo der SharePoint Explorer installiert ist.

Unterstützte Oracle Database-Versionen

- Oracle Database-Version 11g, alle Editionen
- Oracle Database-Version 12c, alle Editionen
- Oracle Database-Version 19c, alle Editionen
- Oracle Database-Version 21c, alle Editionen

Es werden nur Einzelinstanz-Konfigurationen unterstützt.

Unterstützte SAP HANA-Versionen

HANA 2.0 SPS 03 installiert in RHEL 7.6 auf einer physischen Maschine oder virtuellen VMware ESXi-Maschine.

Weil SAP HANA die Wiederherstellung von mandantenfähigen Datenbank-Containern mithilfe von Storage-Snapshots nicht unterstützt, werden von dieser Lösung nur SAP HANA-Container mit einer Mandanten-Datenbank unterstützt.

Unterstützte MySQL-Versionen

- 5.5.x − Community Server, Enterprise, Standard und Classic Editionen
- 5.6.x − Community Server, Enterprise, Standard und Classic Editionen
- 5.7.x − Community Server, Enterprise, Standard und Classic Editionen
- 8.0.x − Community Server, Enterprise, Standard und Classic Editionen

Unterstützte MariaDB-Versionen

- 10.0.x
- 10.1.x
- 10.2.x
- 10.3.x
- 10.4.x
- 10.5.x
- 10.6.x
- 10.7.x

Unterstützte Virtualisierungsplattformen

Die nachfolgende Tabelle fasst zusammen, wie die verschiedenen Virtualisierungsplattformen unterstützt werden.

Weitere Informationen über die Unterschiede zwischen einem agentenbasiertem und agentenlosem Backup finden Sie im Abschnitt "Agentenbasiertes und agentenloses Backup" (S. 69).

Hinweis
Wenn Sie eine Virtualisierungsplattform oder Version verwenden, die nicht unten aufgeführt ist, kann die Methode **Agentenbasiertes Backup (Backup innerhalb eines Gast-Betriebssystems)** dennoch korrekt bei allen erforderlichen Szenarien funktionieren. Wenn Sie Probleme mit dem agentenbasierten Backup haben, wenden Sie sich zur weiteren Untersuchung an das Support-Team.

VMware

Plattform	Agentenloses Backup (Backup auf Hypervisor-Ebene)	Agentenbasiertes Backup (Backup innerhalb eines Gastbetriebssystems)
VMware vSphere-Versionen: 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7.0, 8.0 **VMware vSphere-Editionen:** VMware vSphere Essentials* VMware vSphere Essentials Plus* VMware vSphere Standard* VMware vSphere Advanced VMware vSphere Enterprise VMware vSphere Enterprise Plus	Unterstützt **Geräte** –> **Hinzufügen** –> **Virtualisierungshosts** –> **VMware ESXi** –> **Agent zur Installation unter Windows** oder **Geräte** –> **Hinzufügen** –> **Virtualisierungshosts** –> **VMware ESXi** –> **Virtuelle Appliance (OVF)**	Unterstützt **Geräte** –> **Hinzufügen** –> **Workstations** oder **Server** –> **Windows** oder **Linux**
VMware vSphere Hypervisor (Free ESXi)**	Nicht unterstützt	Unterstützt **Geräte** –> **Hinzufügen** –> **Workstations** oder **Server** –> **Windows** oder **Linux**
VMware Server (VMware Virtual Server) VMware Workstation VMware ACE VMware Player	Nicht unterstützt	Unterstützt **Geräte** –> **Hinzufügen** –> **Workstations** oder **Server** –> **Windows** oder **Linux**

* Bei diesen Editionen wird der HotAdd-Transport für virtuelle Laufwerke auf vSphere 5.0 (und später) unterstützt. Auf Version 4.1 können Backups langsamer laufen.

** Backups auf Hypervisor-Ebene werden nicht für vSphere Hypervisor unterstützt, da dieses Produkt den Zugriff auf die Remote-Befehlszeilenschnittstelle (Remote Command Line Interface, RCLI) auf den Nur-Lesen-Modus beschränkt. Der Agent arbeitet während des vSphere Hypervisor-Evaluierungszeitraums ohne Eingabe einer Seriennummer. Sobald Sie eine Seriennummer eingeben, hört der Agent auf zu funktionieren.

Hinweis
Cyber Protect Cloud unterstützt offiziell jedes Update innerhalb der unterstützten Hauptversion von vSphere.

Beispielsweise umfasst die Unterstützung für vSphere 8.0 auch die Unterstützung für alle Updates innerhalb dieser Version, sofern nicht anders angegeben. So wird beispielsweise vSphere 8.0 Update 1 ebenso unterstützt wie das zuerst veröffentlichte vSphere 8.0.

Die Unterstützung für eine bestimmte VMware vSphere-Version bedeutet, dass auch vSAN mit der entsprechenden Version unterstützt wird. Die Unterstützung von vSphere 8.0 bedeutet beispielsweise, dass auch vSAN 8.0 unterstützt wird.

Beschränkungen

- **Fehlertolerante Maschinen**
  Der Agent für VMware sichert eine fehlertolerante Maschine nur dann, wenn die Fehlertoleranz in VMware vSphere 6.0 (und später) aktiviert wurde. Falls Sie ein Upgrade von einer früheren vSphere-Version durchgeführt haben, reicht es aus, wenn Sie die Fehlertoleranz für jede Maschine deaktivieren und aktivieren. Wenn Sie eine frühere vSphere-Version verwenden, installieren Sie einen Agenten im Gastbetriebssystem.
- **Unabhängige Laufwerke und RDM-Laufwerke**
  Der Agent für VMware kann keine RDM-Laufwerke (Raw Device Mapping) im physischen Kompatibilitätsmodus und keine unabhängigen Laufwerke sichern. Der Agent überspringt diese Laufwerke und fügt dem Log entsprechende Warnmeldungen hinzu. Sie können diese Warnmeldungen vermeiden, indem Sie unabhängige Laufwerke und RDM-Laufwerke im physischen Kompatibilitätsmodus von einem Schutzplan ausschließen. Falls Sie diese Laufwerke sichern wollen, müssen Sie einen Agenten im Gastbetriebssystem installieren.
- **iSCSI-Verbindung im Gast**
  Der Agent für VMware sichert keine LUN-Volumes, die über einen iSCSI-Initiator verbunden sind, der von innerhalb des Gastbetriebssystems aus arbeitet. Weil dem ESXi-Hypervisor solche Volumes nicht bekannt sind, werden die Volumes nicht in die Hypervisor-basierten Snapshots aufgenommen und daher ohne Vorwarnung vom Backup ausgeschlossen. Wenn Sie diese Volumes oder bestimmte Daten auf diesen Volumes sichern wollen, müssen Sie einen Agenten im Gastbetriebssystem installieren.
- **Verschlüsselte virtuelle Maschinen** (mit VMware vSphere 6.5 eingeführt)
  - Verschlüsselte virtuelle Laufwerke werden im Backup in einem unverschlüsselten Zustand gespeichert. Falls die Verschlüsselung der entsprechenden Daten für Sie wichtig ist, können Sie bei der Erstellung eines Schutzplans festlegen, dass die Backups selbst verschlüsselt werden.
  - Wiederhergestellte virtuelle Maschinen sind immer unverschlüsselt. Sie können die Verschlüsselung nach Abschluss der Wiederherstellung aber wieder manuell aktivieren.
  - Wenn Sie verschlüsselte virtuelle Maschinen per Backup sichern, empfehlen wir Ihnen, außerdem auch die virtuelle Maschine zu verschlüsseln, auf welcher der Agent für VMware ausgeführt wird. Ansonsten sind die ausgeführten Aktionen mit den verschlüsselten

Maschinen möglicherweise langsamer als erwartet. Verwenden Sie den vSphere Webclient, um der Maschine des Agenten die **VM-Verschlüsselungsrichtlinie** zuzuweisen.

  - Verschlüsselte virtuelle Maschinen werden via LAN gesichert – und zwar auch dann, wenn Sie den SAN-Transportmodus für den Agenten konfiguriert haben. Der Agent wird stattdessen auf den NBD-Transportmodus zurückgreifen, weil VMware den SAN-Transportmodus beim Backup verschlüsselter virtueller Laufwerke nicht unterstützt.

- **Secure Boot**
  - Virtuelle VMware-Maschinen: (in VMware vSphere 6.5 eingeführt) **Secure Boot** ist deaktiviert, wenn eine virtuelle Maschine als neue virtuelle Maschine wiederhergestellt wurde. Sie können die Option nach Abschluss der Wiederherstellung aber wieder manuell aktivieren. Diese Einschränkung gilt für VMware
  - Virtuelle Hyper-V-Maschinen: Secure Boot ist bei allen GEN2-VMs deaktiviert, wenn die virtuelle Maschine als neue oder zu einer bereits vorhandenen virtuelle Maschine wiederhergestellt wurde.
- **ESXi-Konfigurations-Backups** werden nicht für VMware vSphere 7.0 unterstützt.
- **Unterstützte Aktionen für Maschinen mit logischen Volumes**

  Backups und Wiederherstellungen von Workloads mit logischen Volumes, wie LDM in Windows (dynamische Datenträger) und LVM in Linux, werden mit bestimmten Einschränkungen unterstützt. Weitere Informationen zu diesen Einschränkungen finden Sie unter "Unterstützte Aktionen mit logischen Volumes" (S. 59).

Microsoft

Plattform	Agentenloses Backup (Backup auf Hypervisor-Ebene)	Agentenbasiertes Backup (Backup innerhalb eines Gastbetriebssystems)
Windows Server 2008 (x64) mit Hyper-V Windows Server 2008 R2 mit Hyper-V Microsoft Hyper-V Server 2008/2008 R2 Windows Server 2012/2012 R2 mit Hyper-V Microsoft Hyper-V Server 2012/2012 R2 Windows 8, 8.1 (x64) mit Hyper-V Windows 10 mit Hyper-V Windows Server 2016 mit Hyper-V – alle Installationsoptionen, mit	Unterstützt **Geräte** –> **Hinzufügen** –> **Virtualisierungshosts** –> **Hyper-V**	Unterstützt **Geräte** –> **Hinzufügen** –> **Workstations** oder **Server** –> **Windows** oder **Linux**

Plattform	Agentenloses Backup (Backup auf Hypervisor-Ebene)	Agentenbasiertes Backup (Backup innerhalb eines Gastbetriebssystems)
Ausnahme des Nano Servers Microsoft Hyper-V Server 2016 Windows Server 2019 mit Hyper-V – alle Installationsoptionen, mit Ausnahme des Nano Servers Microsoft Hyper-V Server 2019 Windows Server 2022 mit Hyper-V – alle Installationsoptionen, mit Ausnahme des Nano Servers		
Microsoft Virtual PC 2004, 2007 Windows Virtual PC	Nicht unterstützt	Unterstützt **Geräte** –> **Hinzufügen** –> **Workstations** oder **Server** –> **Windows** oder **Linux**
Microsoft Virtual Server 2005	Nicht unterstützt	Unterstützt **Geräte** –> **Hinzufügen** –> **Workstations** oder **Server** –> **Windows** oder **Linux**

Hinweis
Virtuelle Hyper-V-Maschinen, die auf einem hyperkonvergenten Cluster mit 'Direkten Speicherplätzen' (Storage Spaces Direct, S2D) ausgeführt werden, werden unterstützt. Storage Spaces Direct wird auch als Backup Storage unterstützt.

Einschränkungen

- **Pass-Through-Laufwerke (Durchleitungslaufwerke)**
  Der Agent für Hyper-V kann keine Pass-Through-Laufwerke sichern. Der Agent überspringt diese Laufwerke während des Backups und fügt dem Log entsprechende Warnmeldungen hinzu. Sie können diese Warnmeldungen vermeiden, indem Sie Pass-through-Laufwerke von einem Schutzplan ausschließen. Falls Sie diese Laufwerke sichern wollen, müssen Sie einen Agenten im Gastbetriebssystem installieren.
- **Hyper-V-Gast-Clustering**
  Mit dem Agenten für Hyper-V können keine virtuellen Hyper-V-Maschinen gesichert werden, die Knoten eines Windows Server-Failover-Clusters sind. Ein VSS-Snapshot auf Host-Ebene kann sogar das externe Quorum-Laufwerk temporär vom Cluster trennen. Wenn Sie diese Maschinen per Backup sichern wollen, müssen Sie die Agenten in den entsprechenden Gastbetriebssystemen installieren.

- **iSCSI-Verbindung im Gast**
  Der Agent für Hyper-V sichert keine LUN-Volumes, die über einen iSCSI-Initiator verbunden sind, der von innerhalb des Gastbetriebssystems aus arbeitet. Weil dem Hyper-V-Hypervisor solche Volumes nicht bekannt sind, werden die Volumes nicht in die Hypervisor-basierten Snapshots aufgenommen und daher ohne Vorwarnung vom Backup ausgeschlossen. Wenn Sie diese Volumes oder bestimmte Daten auf diesen Volumes sichern wollen, müssen Sie einen Agenten im Gastbetriebssystem installieren.
- **Secure Boot**
  Secure Boot ist bei allen GEN2-VMs deaktiviert, wenn die virtuelle Maschine als neue oder zu einer bereits vorhandenen virtuelle Maschine wiederhergestellt wurde.
- **Unterstützte Aktionen für Maschinen mit logischen Volumes**
  Backups und Wiederherstellungen von Workloads mit logischen Volumes, wie LDM in Windows (dynamische Datenträger) und LVM in Linux, werden mit bestimmten Einschränkungen unterstützt. Weitere Informationen zu diesen Einschränkungen finden Sie unter "Unterstützte Aktionen mit logischen Volumes" (S. 59).
- **VHD-/VHDX-Dateinamen mit kaufmännischem Und-Zeichen**
  Auf Hyper-V-Hosts mit Windows Server 2016 oder höher können Sie keine virtuellen Maschinen (Version 5.0) sichern, die ursprünglich mit Hyper-V 2012 R2 oder älter erstellt wurden, wenn die Namen von deren VHD-/VHDX-Dateien ein kaufmännisches Und-Zeichen (&) enthalten.
  Wenn Sie solche Maschinen per Backup sichern wollen, müssen Sie im Hyper-V Manager das entsprechende virtuelle Laufwerk von der virtuellen Maschine trennen, den VHD-/VHDX-Dateinamen so bearbeiten, dass das &-Symbol entfernt wird, und dann das umbenannte Laufwerk wieder an die virtuelle Maschine anschließen.
- **Abhängigkeit vom Microsoft WMI-Subsystem**
  Agentenlose Backups von virtuellen Hyper-V-Maschinen hängen vom Microsoft WMI-Subsystem ab, insbesondere von der `Msvm_VirtualSystemManagementService`-Klasse. Wenn die WMI-Abfragen fehlschlagen, werden auch die Backups fehlschlagen. Weitere Informationen zur `Msvm_VirtualSystemManagementService`-Klasse finden Sie in der entsprechenden Microsoft-Dokumentation.

Scale Computing

Plattform	Agentenloses Backup (Backup auf Hypervisor-Ebene)	Agentenbasiertes Backup (Backup innerhalb eines Gastbetriebssystems)
Scale Computing Hypercore 8.8, 8.9, 9.0, 9.1, 9.2, 9.3	Unterstützt **Geräte** –> **Hinzufügen** –> **Virtualisierungshosts** –> **Scale Computing HC3**	Unterstützt **Geräte** –> **Hinzufügen** –> **Workstations** oder **Server** –> **Windows** oder **Linux**

Einschränkungen

Unterstützte Aktionen für Maschinen mit logischen Volumes

Backups und Wiederherstellungen von Workloads mit logischen Volumes, wie LDM in Windows (dynamische Datenträger) und LVM in Linux, werden mit bestimmten Einschränkungen unterstützt. Weitere Informationen zu diesen Einschränkungen finden Sie unter "Unterstützte Aktionen mit logischen Volumes" (S. 59).

Citrix

Plattform	Agentenloses Backup (Backup auf Hypervisor-Ebene)	Agentenbasiertes Backup (Backup innerhalb eines Gastbetriebssystems)
Citrix XenServer/Citrix Hypervisor 4.1.5, 5.5, 5.6, 6.0, 6.1, 6.2, 6.5, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 8.0, 8.1, 8.2	Nicht unterstützt	Wird nur für vollständig virtualisierte Gäste (HVM) unterstützt. Paravirtualisierte Gäste (PV-Gäste) werden nicht unterstützt. **Geräte** –> **Hinzufügen** –> **Virtualisierungshosts** –> **Citrix XenServer** –> **Windows** oder **Linux**

Red Hat und Linux

Plattform	Agentenloses Backup (Backup auf Hypervisor-Ebene)	Agentenbasiertes Backup (Backup innerhalb eines Gastbetriebssystems)
Red Hat Enterprise Virtualization (RHEV) 2.2, 3.0, 3.1, 3.2, 3.3, 3.4, 3.5, 3.6 Red Hat Virtualization (RHV) 4.0, 4.1	Nicht unterstützt	Unterstützt **Geräte** –> **Hinzufügen** –> **Workstations** oder **Server** –> **Windows** oder **Linux**
Red Hat Virtualization (verwaltet von oVirt) 4.2, 4.3, 4.4, 4.5	Unterstützt **Geräte** –> **Hinzufügen** –> **Virtualisierungshosts** –> **Red Hat Virtualization (oVirt)**	Unterstützt **Geräte** –> **Hinzufügen** –> **Workstations** oder **Server** –> **Windows** oder **Linux**
Kernel-based Virtual Machines (KVM)	Nicht unterstützt	Unterstützt **Geräte** –> **Hinzufügen** –> **KVM** –> **Windows** oder **Linux**
Kernel-based Virtual Machines (KVM), verwaltet von oVirt 4.3 unter Red Hat Enterprise Linux 7.6, 7.7 oder CentOS 7.6, 7.7	Unterstützt **Geräte** –> **Hinzufügen** –> **Virtualisierungshosts** –> **Red**	Unterstützt **Geräte** –> **Hinzufügen** –> **Workstations** oder **Server** –>

Plattform	Agentenloses Backup (Backup auf Hypervisor-Ebene)	Agentenbasiertes Backup (Backup innerhalb eines Gastbetriebssystems)
	Hat Virtualization (oVirt)	**Windows** oder **Linux**
Kernel-based Virtual Machines (KVM), verwaltet von oVirt 4.4 unter Red Hat Enterprise Linux 8.x oder CentOS Stream 8.x	Unterstützt **Geräte** –> **Hinzufügen** –> **Virtualisierungshosts** –> **Red Hat Virtualization (oVirt)**	Unterstützt **Geräte** –> **Hinzufügen** –> **Workstations** oder **Server** –> **Windows** oder **Linux**
Kernel-based Virtual Machines (KVM), verwaltet von oVirt 4.5 unter Red Hat Enterprise Linux 8.x oder CentOS Stream 8.x	Unterstützt **Geräte** –> **Hinzufügen** –> **Virtualisierungshosts** –> **Red Hat Virtualization (oVirt)**	Unterstützt **Geräte** –> **Hinzufügen** –> **Workstations** oder **Server** –> **Windows** oder **Linux**

Einschränkungen

Unterstützte Aktionen für Maschinen mit logischen Volumes

Backups und Wiederherstellungen von Workloads mit logischen Volumes, wie LDM in Windows (dynamische Datenträger) und LVM in Linux, werden mit bestimmten Einschränkungen unterstützt. Weitere Informationen zu diesen Einschränkungen finden Sie unter "Unterstützte Aktionen mit logischen Volumes" (S. 59).

Parallels

Plattform	Agentenloses Backup (Backup auf Hypervisor-Ebene)	Agentenbasiertes Backup (Backup innerhalb eines Gastbetriebssystems)
Parallels Workstation	Nicht unterstützt	Unterstützt **Geräte** –> **Hinzufügen** –> **Workstations** oder **Server** –> **Windows** oder **Linux**
Parallels Server 4 Bare Metal	Nicht unterstützt	Unterstützt **Geräte** –> **Hinzufügen** –> **Workstations** oder **Server** –> **Windows** oder **Linux**

Oracle

Plattform	Agentenloses Backup (Backup auf Hypervisor-Ebene)	Agentenbasiertes Backup (Backup innerhalb eines Gastbetriebssystems)
Oracle Virtualization Manager (basierend auf oVirt)* 4.3	Unterstützt **Geräte** –> **Hinzufügen** –> **Virtualisierungshosts** –> **Red Hat Virtualization (oVirt)**	Unterstützt **Geräte** –> **Hinzufügen** –> **Workstations** oder **Server** –> **Windows** oder **Linux**
Oracle VM Server 3.0, 3.3, 3.4	Nicht unterstützt	Wird nur für vollständig virtualisierte Gäste (HVM) unterstützt. Paravirtualisierte Gäste (PV-Gäste) werden nicht unterstützt. **Geräte** –> **Hinzufügen** –> **Virtualisierungshosts** –> **Oracle** –> **Windows** oder **Linux**
Oracle VM VirtualBox 4.x	Nicht unterstützt	Unterstützt **Geräte** –> **Hinzufügen** –> **Virtualisierungshosts** –> **Oracle** –> **Windows** oder **Linux**

*Der Oracle Virtualization Manager wird vom Agenten für oVirt unterstützt.

Einschränkungen

Unterstützte Aktionen für Maschinen mit logischen Volumes

Backups und Wiederherstellungen von Workloads mit logischen Volumes, wie LDM in Windows (dynamische Datenträger) und LVM in Linux, werden mit bestimmten Einschränkungen unterstützt. Weitere Informationen zu diesen Einschränkungen finden Sie unter "Unterstützte Aktionen mit logischen Volumes" (S. 59).

Nutanix

Plattform	Agentenloses Backup (Backup auf Hypervisor-Ebene)	Agentenbasiertes Backup (Backup innerhalb eines Gastbetriebssystems)
Nutanix Acropolis Hypervisor (AHV) 20160925.x bis 20180425.x	Nicht unterstützt	Unterstützt

Plattform	Agentenloses Backup (Backup auf Hypervisor-Ebene)	Agentenbasiertes Backup (Backup innerhalb eines Gastbetriebssystems)
		Geräte –> **Hinzufügen** –> **Virtualisierungshosts** –> **Nutanix AHV** –> **Windows** oder **Linux**

Virtuozzo

Plattform	Agentenloses Backup (Backup auf Hypervisor-Ebene)	Agentenbasiertes Backup (Backup innerhalb eines Gastbetriebssystems)
Virtuozzo 6.0.10, 6.0.11, 6.0.12	Unterstützt **Geräte** –> **Hinzufügen** –> **Virtualisierungshosts** –> **Virtuozzo**	Wird nur für virtuelle Maschinen unterstützt. Container werden nicht unterstützt. **Geräte** –> **Hinzufügen** –> **Workstations** oder **Server** –> **Windows** oder **Linux**
Virtuozzo 7.0.13, 7.0.14	Wird nur für Ploop-Container unterstützt. Virtuelle Maschinen werden nicht unterstützt. **Geräte** –> **Hinzufügen** –> **Virtualisierungshosts** –> **Virtuozzo**	Wird nur für virtuelle Maschinen unterstützt. Container werden nicht unterstützt. **Geräte** –> **Hinzufügen** –> **Workstations** oder **Server** –> **Windows** oder **Linux**
Virtuozzo Hybrid Server 7.5	Unterstützt **Geräte** –> **Hinzufügen** –> **Virtualisierungshosts** –> **Virtuozzo**	Wird nur für virtuelle Maschinen unterstützt. Container werden nicht unterstützt. **Geräte** –> **Hinzufügen** –> **Workstations** oder **Server** –> **Windows** oder **Linux**

Einschränkungen

Unterstützte Aktionen für Maschinen mit logischen Volumes

Backups und Wiederherstellungen von Workloads mit logischen Volumes, wie LDM in Windows (dynamische Datenträger) und LVM in Linux, werden mit bestimmten Einschränkungen unterstützt.

Weitere Informationen zu diesen Einschränkungen finden Sie unter "Unterstützte Aktionen mit logischen Volumes" (S. 59).

Virtuozzo Hybrid Infrastructure

Plattform	Agentenloses Backup (Backup auf Hypervisor-Ebene)	Agentenbasiertes Backup (Backup innerhalb eines Gastbetriebssystems)
Virtuozzo Hybrid Infrastructure 3.5, 4.5, 4.6, 4.7, 5.0, 5.1, 5.2, 5.3, 5.4, 6.0	Unterstützt **Geräte** –> **Hinzufügen** –> **Virtualisierungshosts** –> **Virtuozzo Hybrid infrastructure**	Unterstützt **Geräte** –> **Hinzufügen** –> **Workstations** oder **Server** –> **Windows** oder **Linux**

Einschränkungen

- **Agentenloses Backup von VMs mit Laufwerken auf einem externen iSCSI-Storage**
  Sie können keine VMs aus Virtuozzo Hybrid Infrastructure (VHI) sichern, wenn sich die VM-Laufwerke auf externen iSCSI-Volumes befinden (die an den VHI-Cluster angeschlossen sind).
- **Unterstützte Aktionen für Maschinen mit logischen Volumes**
  Backups und Wiederherstellungen von Workloads mit logischen Volumes, wie LDM in Windows (dynamische Datenträger) und LVM in Linux, werden mit bestimmten Einschränkungen unterstützt. Weitere Informationen zu diesen Einschränkungen finden Sie unter "Unterstützte Aktionen mit logischen Volumes" (S. 59).

Amazon

Plattform	Agentenloses Backup (Backup auf Hypervisor-Ebene)	Agentenbasiertes Backup (Backup innerhalb eines Gastbetriebssystems)
Amazon EC2-Instanzen	Nicht unterstützt	Unterstützt **Geräte** –> **Hinzufügen** –> **Workstations** oder **Server** –> **Windows** oder **Linux**

Microsoft Azure

Plattform	Agentenloses Backup (Backup auf Hypervisor-Ebene)	Agentenbasiertes Backup (Backup innerhalb eines Gastbetriebssystems)
Virtuelle Azure-Maschinen	Nicht unterstützt	Unterstützt

Plattform	Agentenloses Backup (Backup auf Hypervisor-Ebene)	Agentenbasiertes Backup (Backup innerhalb eines Gastbetriebssystems)
		Geräte –> **Hinzufügen** –> **Workstations** oder **Server** –> **Windows** oder **Linux**

Kompatibilität mit Verschlüsselungssoftware

Daten, die auf *Dateiebene* von einer Verschlüsselungssoftware verschlüsselt werden, können ohne Beschränkung gesichert und wiederhergestellt werden.

Verschlüsselungssoftware, die Daten auf Laufwerksebene *Laufwerksebene* verschlüsseln, tun dies 'on the fly'. Daher sind die entsprechenden, in ein Backup aufgenommenen Daten nicht verschlüsselt. Programme zur Laufwerksverschlüsselung modifizieren häufig wichtige Systembereiche: Boot-Record oder Partitionstabellen oder Dateisystemtabellen. Diese Faktoren können daher Backup- und Recovery-Aktionen mit solchen Laufwerken sowie die Fähigkeit eines wiederhergestellten Systems beeinflussen, booten oder auf eine Secure Zone zugreifen zu können.

Daten, die mit folgenden Software-Produkten zur Laufwerksverschlüsselung verschlüsselt wurden, können per Backup gesichert werden:

- Microsoft BitLocker-Laufwerksverschlüsselung
- McAfee Endpoint Encryption
- PGP Whole Disk Encryption

Um zuverlässige Wiederherstellungen auf Laufwerksebene zu garantieren, sollten Sie allgemeinen Regeln sowie Software-spezifischen Empfehlungen folgen.

Allgemeine Installationsregel

Wir empfehlen dringend, dass Sie die Verschlüsselungssoftware vor der Installation der Protection Agenten installieren.

Verwendung der Secure Zone

Die Secure Zone darf keiner Laufwerksverschlüsselung unterzogen werden. Die Secure Zone kann nur folgendermaßen verwendet werden:

1. Installieren Sie zuerst die Verschlüsselungssoftware und dann den Agenten.
2. Secure Zone erstellen.
3. Wenn Sie das Laufwerk oder dessen Volumes verschlüsseln, müssen Sie die Secure Zone von der Verschlüsselung ausschließen.

Allgemeine Backup-Regel

Sie können ein Laufwerk-Backup im Betriebssystem durchführen.

Software-spezifische Recovery-Prozeduren

Microsoft BitLocker-Laufwerksverschlüsselung

So können Sie ein System wiederherstellen, das per BitLocker verschlüsselt wurde:

1. Booten Sie mit einem Boot-Medium.
2. Stellen Sie das System wieder her. Die wiederhergestellten Daten sind unverschlüsselt.
3. Booten Sie das wiederhergestellte System neu.
4. Schalten Sie die BitLocker-Funktion ein.

Falls Sie nur ein Volume eines mehrfach partitionierten Laufwerks wiederherstellen müssen, so tun Sie dies unter dem Betriebssystem. Eine Wiederherstellung mit einem Boot-Medium kann dazu führen, dass Windows das wiederhergestellte Volume (die Partition) nicht mehr erkennen kann.

McAfee Endpoint Encryption und PGP Whole Disk Encryption

Sie können ein verschlüsseltes System-Volume nur durch Verwendung eines Boot-Mediums wiederherstellen.

Falls das wiederhergestellte System nicht mehr bootet, erstellen Sie einen neuen Master Boot Record, wie in folgendem Artikel der Microsoft Knowledge Base beschrieben: https://support.microsoft.com/kb/2622803

Kompatibilität mit Dell EMC Data Domain Storages

Sie können Dell EMC Data Domain-Geräte als Backup Storage verwenden.

Bei diesem Storage empfehlen wir Ihnen, ein Backup-Schema zu verwenden, das regelmäßig Voll-Backups erstellt. Beispielsweise das Schema **Immer vollständig**. Weitere Informationen über die verfügbaren Backup-Schemata finden Sie im Abschnitt '"Backup-Schemata" (S. 458)'.

Die Aufbewahrungssperre (der Governance-Modus) wird unterstützt. Wenn die Aufbewahrungssperre (Englisch: Retention Lock) aktiviert ist, müssen Sie auf der Maschine mit dem Protection Agenten, die diesen Storage als Backup-Ziel verwenden soll, die Umgebungsvariable `AR_RETENTION_LOCK_SUPPORT` hinzufügen.

Hinweis
Dell EMC Data Domain Storages mit aktivierter Aufbewahrungssperre werden nicht vom Agenten für Mac unterstützt.

So können Sie die Umgebungsvariable `AR_RETENTION_LOCK_SUPPORT` hinzufügen

Unter Windows

1. Melden Sie sich an der Maschine, auf der sich der Protection Agent befindet, als Administrator an.
2. Gehen Sie in der **Systemsteuerung** zu **System und Sicherheit** –> **System** –> **Erweiterte Systemeinstellungen**.
3. Klicken Sie auf der **Registerkarte Erweitert** auf den Befehl **Umgebungsvariablen**.
4. Klicken Sie im Fensterbereich **Systemvariablen** auf den Befehl **Neu**.
5. Geben Sie im Fenster **Neue Systemvariable** die neue Variable folgendermaßen ein:
   - Variablenname: `AR_RETENTION_LOCK_SUPPORT`
   - Variablenwert: `1`
6. Klicken Sie auf **OK**.
7. Klicken Sie im Fenster **Umgebungsvariablen** auf **OK**.
8. Starten Sie die Maschine neu.

Unter Linux

1. Melden Sie sich an der Maschine, auf der sich der Protection Agent befindet, als Administrator an.
2. Gehen Sie zum Verzeichnis `/sbin` und öffnen Sie die Datei `acronis_mms` zur Bearbeitung.
3. Fügen Sie über der Zeile `export LD_LIBRARY_PATH` folgende neue Zeile ein:

   ```
   export AR_RETENTION_LOCK_SUPPORT=1
   ```

4. Speichern Sie die Datei `acronis_mms`.
5. Starten Sie die Maschine neu.

In einer virtuellen Appliance

1. Melden Sie sich als Administrator an der virtuellen Appliance an.
2. Gehen Sie zum Verzeichnis `/bin` und öffnen Sie die Datei `autostart` zur Bearbeitung.
3. Fügen Sie unter der Zeile `export LD_LIBRARY_PATH` folgende neue Zeile ein:

   ```
   export AR_RETENTION_LOCK_SUPPORT=1
   ```

4. Speichern Sie die Datei `autostart`.
5. Starten Sie die virtuelle Appliance-Maschine neu.

Unterstützte Schutzfunktionen, nach Betriebssystem

Dieses Thema enthält Informationen über die Schutzfunktionen von Cyber Protect Cloud. Es werden jedoch keine Backup- und Recovery-Funktionen aufgeführt.

Die Schutzunktionen werden nur auf Maschinen unterstützt, auf denen ein Protection Agent installiert ist. Diese stehen nicht für virtuelle Maschinen zur Verfügung, die im agentenlosen Modus

gesichert werden, z.B. durch den Agenten für Hyper-V, den Agenten für VMware, den Agenten für Virtuozzo Hybrid Infrastructure, den Agenten für Scale Computing oder den Agenten für oVirt.

In Abhängigkeit davon, welches Lizenzierungsmodell angewendet wird, kann für einige Funktionen eine zusätzliche Lizenzierung erforderlich sein.

Unterstützte Betriebssysteme und Versionen

Windows

Sofern für einen bestimmten Funktionssatz nicht anders angegeben, werden folgende Windows-Versionen unterstützt:

- Windows 7 Service Pack 1 und höher
- Windows Server 2008 R2 Service Pack 1 und höher

Hinweis
Bei Windows 7 müssen Sie vor der Installation des Protection Agenten die nachfolgenden Updates von Microsoft installieren.

- Windows 7 Extended Security Updates (ESU)
- KB4474419
- KB4490628

Weitere Informationen zu den erforderlichen Updates finden Sie in diesem Knowledge Base-Artikel.

Linux

Die unterstützten Linux-Distributionen und deren Versionen hängen von den Funktionssätzen ab und sind am Ende jeder Tabelle aufgeführt.

macOS

Die unterstützten macOS-Versionen hängen von den Funktionssätzen ab und sind am Ende jeder Tabelle aufgeführt.

Funktionssatz	Windows	Linux	macOS
Standard-Schutzpläne			
Remote-Arbeiter	Ja	Nein	Nein
Büro-Arbeiter (Drittanbieter-Antivirus)	Ja	Nein	Nein
Büro-Arbeiter (Cyber Protect-Antivirus)	Ja	Nein	Nein
Cyber Protect Essentials (nur für die Cyber Protect Essentials-Edition)	Ja	Nein	Nein
Die unterstützten Windows-Versionen finden Sie unter ""Unterstützte Betriebssysteme und Versionen" (S.			

Funktionssatz	Windows	Linux	macOS
Standard-Schutzpläne			
47)'.			

Funktionssatz	Windows	Linux	macOS
Forensik-Backup			
Speicherabbilder sammeln	Ja	Nein	Nein
Snapshot der laufenden Prozesse	Ja	Nein	Nein
Beglaubigung von Forensik-Backups (lokale Images)	Ja	Nein	Nein
Beglaubigung von Forensik-Backups (Cloud-Images)	Ja	Nein	Nein
Die unterstützten Windows-Versionen finden Sie unter '"Unterstützte Betriebssysteme und Versionen" (S. 47)'.			

Funktionen	Windows	Linux	macOS
Kontinuierliche Datensicherung (CDP)			
CDP für Dateien und Ordner	Ja	Nein	Nein
CDP für geänderte Dateien über Anwendungsverfolgung	Ja	Nein	Nein
Die unterstützten Windows-Versionen finden Sie unter '"Unterstützte Betriebssysteme und Versionen" (S. 47)'.			

Funktionssatz	Windows	Linux	macOS
Automatische Erkennung und Remote-Installation			
Netzwerk-basierte Erkennung	Ja	Nein	Nein
Active Directory-basierte Erkennung	Ja	Nein	Nein
Vorlagen-basierte Erkennung (Machinen aus einer Datei importieren)	Ja	Nein	Nein
Geräte manuell hinzufügen	Ja	Nein	Nein
Die unterstützten Windows-Versionen finden Sie unter '"Unterstützte Betriebssysteme und Versionen" (S. 47)'.			

Funktionssatz	Windows	Linux	macOS
Active Protection			
Erkennung von Prozesseinschleusung	Ja	Nein	Nein
Automatisches Recovery von betroffenen Dateien aus lokalem Cache	Ja	Ja	Ja
Selbstschutzfunktion für Acronis Backup-Dateien	Ja	Nein	Nein
Selbstschutzfunktion für die Acronis Software	Ja	Nein	Ja (Nur Active Protection- und Antimalware-Komponenten)
Verwaltung vertrauenswürdiger/geblockter Prozesse	Ja	Nein	Ja
Ausschluss von Prozessen/Ordnern	Ja	Ja	Ja
Erkennung von Ransomware aufgrund von Prozessverhalten (KI-basiert)	Ja	Ja	Ja
Erkennung von Cryptomining-Prozessen anhand von Prozessverhalten	Ja	Nein	Nein
Schutz von externen Laufwerken (HDD, USB-Sticks, SD-Karten)	Ja	Nein	Ja
Netzwerkordnerschutz	Ja	Ja	Ja
Serverseitiger Schutz	Ja	Nein	Nein
Schutz für Cisco Webex, Citrix Workspace und Microsoft Teams	Ja	Nein	Nein
Für weitere Informationen über die unterstützten Betriebssysteme und deren Versionen finden Sie im Abschnitt '"Unterstützte Plattformen" (S. 896)'.			

Funktionssatz	Windows	Linux	macOS
Antivirus & Antimalware Protection			
Voll integrierte Active Protection-Funktionalität	Ja	Nein	Nein
Antimalware Protection in Echtzeit	Ja	Ja, mit dem Advanced Antimalware-Paket	Ja, mit dem Advanced Antimalware-Paket

Funktionssatz	Windows	Linux	macOS
Antivirus & Antimalware Protection			
Advanced Realtime Antimalware Protection mit lokaler signaturbasierter Erkennung	Ja	Ja	Ja
Statische Analyse für übertragbare ausführbare Dateien	Ja	Nein	Ja*
On-Demand-Antimalware-Scanning	Ja	Ja**	Ja
Netzwerkordnerschutz	Ja	Ja	Nein
Serverseitiger Schutz	Ja	Nein	Nein
Scannen von Archivdateien	Ja	Nein	Ja
Scannen von Wechsellaufwerken	Ja	Nein	Ja
Scannen von nur neuen und geänderten Dateien	Ja	Nein	Ja
Ausschluss von Dateien/Ordnern	Ja	Ja	Ja***
Ausschluss von Prozessen	Ja	Nein	Ja
Behavioral Analysis Engine (Verhaltensanalyse-Modul)	Ja	Nein	Ja
Exploit-Prävention	Ja	Nein	Nein
Quarantäne	Ja	Ja	Ja
Quarantäne-Speicherort automatisch bereinigen	Ja	Ja	Ja
URL-Filterung (http/https)	Ja	Nein	Nein
Unternehmensweite Positivliste	Ja	Nein	Ja
Firewall-Verwaltung****	Ja	Nein	Nein
Microsoft Defender Antivirus-Verwaltung*****	Ja	Nein	Nein
Microsoft Security Essentials-Management	Ja	Nein	Nein
Antivirus & Antimalware Protection im Windows-Sicherheitscenter registrieren und verwalten	Ja	Nein	Nein
Für weitere Informationen über die unterstützten Betriebssysteme und deren Versionen finden Sie im Abschnitt '"Unterstützte Plattformen" (S. 896)'.			

* Statische Analyse für übertragbare ausführbare Dateien wird nur für geplante Scans auf macOS unterstützt.

** Unter Linux werden keine Startbedingungen für On-Demand-Scans unterstützt.

*** Der Ausschluss von Dateien/Ordnern wird nur dann unterstützt, wenn Sie Dateien/Ordner spezifizieren, die weder vom Echtzeitschutz (Realtime Protection, RTP) noch von geplanten Scans auf macOS überprüft werden.

**** Die Firewall-Verwaltung wird unter Windows 8 und höher unterstützt. Windows Server werden nicht unterstützt.

***** Die Windows Defender Antivirus-Verwaltung wird unter Windows 8.1 und höher unterstützt.

Funktionssatz	Windows	Linux	macOS
Schwachstellenbewertung			
Schwachstellenbewertung des Betriebssystems und seiner nativen Applikationen	Ja	Ja******	Ja
Schwachstellenbewertung für Drittanbieter-Applikationen	Ja	Nein	Ja
Für weitere Informationen über die unterstützten Betriebssysteme und deren Versionen finden Sie in den Abschnitten '"Unterstützte Microsoft- und Drittanbieter-Produkte" (S. 1046)', '"Unterstützte Linux-Produkte" (S. 1048)' und '"Unterstützte Apple- und Drittanbieter-Produkte" (S. 1048)'.			

****** Die Schwachstellenbewertung hängt von der Verfügbarkeit offizieller Sicherheitswarnungen für eine bestimmte Distribution ab – beispielsweise https://lists.centos.org/pipermail/centos-announce/, https://lists.centos.org/pipermail/centos-cr-announce/ und andere.

Funktionssatz	Windows	Linux	macOS
Patch-Verwaltung			
Automatische Patch-Genehmigung	Ja	Nein	Nein
Automatische Patch-Installation	Ja	Nein	Nein
Testen von Patchs	Ja	Nein	Nein
Manuelle Patch-Installation	Ja	Nein	Nein
Patch-Planung	Ja	Nein	Nein
Ausfallsicheres Patching: Backup einer Maschine vor der Patch-Installation als Bestandteil eines Schutzplans	Ja	Nein	Nein
Maschinen-Neustarts während Backup-Ausführungen verhindern	Ja	Nein	Nein

Funktionssatz	Windows	Linux	macOS
Patch-Verwaltung			
Die unterstützten Windows-Versionen finden Sie unter '"Unterstützte Betriebssysteme und Versionen" (S. 47)'.			

Funktionen	Windows	Linux	macOS
Data Protection-Karte			
Anpassbare Definition von wichtigen Dateien	Ja	Nein	Nein
Maschinen scannen, um ungeschützte Dateien zu finden	Ja	Nein	Nein
Überblick über ungeschützte Speicherorte	Ja	Nein	Nein
Schutzaktion kann aus dem Widget 'Data Protection-Karte' gestartet werden (Aktion '**Alle Dateien schützen**')	Ja	Nein	Nein
Die unterstützten Windows-Versionen finden Sie unter '"Unterstützte Betriebssysteme und Versionen" (S. 47)'.			

Funktionssatz	Windows	Linux	macOS
Laufwerksintegrität			
KI-basierte Kontrolle der HDD-/SSD-Laufwerksintegrität	Ja	Nein	Nein
Die unterstützten Windows-Versionen finden Sie unter '"Unterstützte Betriebssysteme und Versionen" (S. 47)'.			

Funktionen	Windows	Linux	macOS
Smart Protection-Pläne basierend auf Alarmmeldungen des Acronis Cyber Protection Operations Centers (CPOC)			
Bedrohungsfeed	Ja	Nein	Nein
Assistent zur Schwachstellenbehebung	Ja	Nein	Nein
Die unterstützten Windows-Versionen finden Sie unter '"Unterstützte Betriebssysteme und Versionen" (S. 47)'.			

Funktionssatz	Windows	Linux	macOS
Backup-Scanning			
Antimalware-Scans von Image-Backups als Bestandteil eines Backup-Plans	Ja	Nein	Nein

Funktionssatz	Windows	Linux	macOS
Backup-Scanning			
Scannen von Image-Backups (in der Cloud) nach Malware	Ja	Nein	Nein
Scannen nach Malware in verschlüsselten Backups	Ja	Nein	Nein
Die unterstützten Windows-Versionen finden Sie unter '"Unterstützte Betriebssysteme und Versionen" (S. 47)'.			

Funktionssatz	Windows	Linux	macOS
Safe Recovery			
Antimalware-Scanning mit Antivirus & Antimalware Protection bei Wiederherstellungsprozessen	Ja	Nein	Nein
Safe Recovery von verschlüsselten Backups	Ja	Nein	Nein
Die unterstützten Windows-Versionen finden Sie unter '"Unterstützte Betriebssysteme und Versionen" (S. 47)'.			

Funktionssatz	Windows	Linux	macOS
Remote-Desktop-Verbindung			
Verbindung über NEAR	Ja	Ja	Ja
Verbindung über RDP	Ja	Nein	Nein
Verbindung über die Apple Bildschirmfreigabe	Nein	Nein	Ja
Verbindung über Webclient	Ja	Nein	Nein
Verbindung über Quick Assist	Ja	Ja	Ja
Remote-Unterstützung	Ja	Ja	Ja
Dateiübertragung	Ja	Ja	Ja
Screenshot-Übertragung	Ja	Ja	Ja
Für weitere Informationen über die unterstützten Betriebssysteme und deren Versionen finden Sie im Abschnitt '"Unterstützte Plattformen" (S. 1088)'.			

Funktionssatz	Windows	Linux	macOS
#CyberFit-Score			
#CyberFit-Score-Status	Ja	Nein	Nein

Funktionssatz	Windows	Linux	macOS
#CyberFit-Score			
#CyberFit-Score-Standalone-Tool	Ja	Nein	Nein
#CyberFit-Score-Empfehlungen	Ja	Nein	Nein
Die unterstützten Windows-Versionen finden Sie unter '"Unterstützte Betriebssysteme und Versionen" (S. 47)'.			

Funktionssatz	Windows	Linux	macOS
Data Loss Prevention			
Gerätekontrolle	Ja	Nein	Unterstützt auf Macs mit Intel-Prozessoren unter macOS 10.15 und höher oder macOS 11.2.3 und höher. Wird nicht für ARM-basierte Apple Silicon-Prozessoren (wie dem Apple M1 / M2) unterstützt
Advanced Data Loss Prevention	Ja	Nein	Nein
Die unterstützten Windows-Versionen finden Sie unter '"Unterstützte Betriebssysteme und Versionen" (S. 47)'.			

Funktionssatz	Windows	Linux	macOS
Management-Optionen			
Upselling-Szenarien, um den Verkauf der Cyber Protect-Editionen zu fördern	Ja	Ja	Ja
Webbasierte zentrale Management-Konsole mit Remote-Verwaltungsfähigkeiten	Ja	Ja	Ja
Unterstützte Betriebssysteme und Versionen: Plattformunabhängig.			

Funktionssatz	Windows	Linux	macOS
Schutzoptionen			
Remote-Löschung	Ja	Nein	Nein
Für Windows 10 und höher unterstützt.			

Funktionssatz	Windows	Linux	macOS
Cyber Protect Monitor			
Cyber Protect App	Ja	Nein	Ja
Schutzstatus für Zoom	Ja	Nein	Nein
Schutzstatus für Cisco Webex	Ja	Nein	Nein
Schutzstatus für Citrix Workspace	Ja	Nein	Nein
Schutzstatus für Microsoft Teams	Ja	Nein	Nein
Die unterstützten Windows-Versionen finden Sie unter '"Unterstützte Betriebssysteme und Versionen" (S. 47)'. Unter macOS wird der Cyber Protect Monitor für alle Versionen unterstützt, auf denen Sie den Agenten für Mac installieren können. Weitere Informationen finden Sie im Abschnitt '" Agent für Mac" (S. 29)'.			

Funktionssatz	Windows	Linux	macOS
Software-Inventarisierung			
Software-Inventarisierungsscan	Ja	Nein	Ja
Monitoring der Software-Inventarisierung	Ja	Nein	Ja
Die unterstützten Windows-Versionen finden Sie unter '"Unterstützte Betriebssysteme und Versionen" (S. 47)'. Unter macOS wird die Software-Inventarisierung für die Versionen 10.13.x–13.x unterstützt.			

Funktionssatz	Windows	Linux	macOS
Hardware-Inventarisierung			
Hardware-Inventarisierungsscan	Ja	Nein	Ja
Monitoring der Software-Inventarisierung	Ja	Nein	Ja
Die unterstützten Windows-Versionen finden Sie unter '"Unterstützte Betriebssysteme und Versionen" (S. 47)'. Unter macOS wird die Hardware-Inventarisierung für die Versionen 10.13.x–13.x unterstützt.			

Unterstützte Dateisysteme

Ein Protection Agent kann jedes Dateisystem per Backup sichern, auf welches das Betriebssystem, auf dem der Agent installiert ist, zugreifen kann. Der Agent für Windows kann beispielsweise ein ext4-Dateisystem sichern und wiederherstellen, sofern ein entsprechender ext4-Treiber unter Windows installiert wurde.

Die nachfolgende Tabelle fasst die Dateisysteme zusammen, die gesichert und wiederhergestellt werden können (Boot-Medien unterstützen nur Wiederherstellungen). Angegebene Beschränkungen gelten sowohl für die Agenten als auch Boot-Medien.

Dateisystem	Unterstützt durch			Einschränkungen
	Agenten	Boot-Medien für Windows und Linux	Boot-Medien für Mac	
FAT16/32	Alle Agenten	+	+	Keine Beschränkungen
NTFS	Alle Agenten	+	+	
ext2/ext3/ext4	Alle Agenten	+	-	
HFS+	Agent für Mac	-	+	
APFS	Agent für Mac	-	+	• Wird ab macOS High Sierra 10.13 unterstützt • Bei Wiederherstellungen zu einer anderen als der ursprünglichen (wie einer fabrikneuen) Maschine muss die ursprüngliche Laufwerkskonfigurationen manuell neu erstellt werden.
JFS	Agent für Linux	+	-	• Dateifilter (Einschlüsse/Ausschlüsse) werden nicht unterstützt • Schnelle inkrementelle/differentielle Backups werden nicht unterstützt.
ReiserFS3	Agent für Linux	+	-	

Dateisystem	Unterstützt durch			Einschränkungen
	Agenten	Boot-Medien für Windows und Linux	Boot-Medien für Mac	
ReiserFS4	Agent für Linux	+	-	• Dateifilter (Einschlüsse/Ausschlüsse) werden nicht unterstützt • Schnelle inkrementelle/differentielle Backups werden nicht unterstützt. • Keine Größenänderung von Volumes während einer Wiederherstellung
ReFS	Alle Agenten	+	+	• Dateifilter (Einschlüsse/Ausschlüsse) werden nicht unterstützt • Schnelle inkrementelle/differentielle Backups werden nicht unterstützt. • Keine Größenänderung von Volumes während einer Wiederherstellung • Während einer Dateiwiederherstellung aus einem ReFS-Backup wird nur dessen Inhalt wiederhergestellt. Zugriffssteuerungsliste (ACL) und Alternate Data Streams werden nicht wiederhergestellt. Dateien mit geringer Dichte (Sparse-Dateien) werden als reguläre Dateien wiederhergestellt.
XFS	Alle Agenten	+	+	• Dateifilter (Einschlüsse/Ausschlüsse) werden nicht unterstützt • Schnelle inkrementelle/differentielle Backups werden nicht unterstützt.

Dateisystem	Unterstützt durch			Einschränkungen
	Agenten	**Boot-Medien für Windows und Linux**	**Boot-Medien für Mac**	
				• Keine Größenänderung von Volumes während einer Wiederherstellung • Der Modus 'schnelles inkrementelles Backup' wird für das XFS-Dateisystem nicht unterstützt. Inkrementelle und differenzielle Backups von XFS-Volumes in die Cloud können deutlich langsamer erfolgen als vergleichbare ext4-Backups, die den Modus 'schnelles inkrementelles Backup' verwenden.
Linux Swap	Agent für Linux	+	-	Keine Beschränkungen
exFAT	Alle Agenten	+ Sie können kein Boot-Medium für eine Wiederherstellung verwenden, wenn das Backup auf einem Laufwerk mit dem Dateisystem exFAT *gespeichert ist*	+	• Es werden nur Laufwerk-/Volume-Backups unterstützt • Dateifilter (Einschlüsse/Ausschlüsse) werden nicht unterstützt • Es können keine einzelnen Dateien aus einem Backup wiederhergestellt werden

Die Software schaltet automatisch auf den Sektor-für-Sektor-Modus um, wenn ein Laufwerk ein Dateisystem verwendet, welches nicht erkannt oder nicht unterstützt wird (z.B. Btrfs). Ein Sektor-für-Sektor-Backup ist für jedes Dateisystem möglich, welches:

- Block-basiert ist
- sich nur über ein Laufwerk erstreckt
- ein Standard-MBR-/GPT-Partitionierungsschema verwendet

Falls ein Dateisystem diese Anforderungen nicht erfüllt, wird ein Backup fehlschlagen.

Datendeduplizierung

Unter Windows Server 2012 (und höher) können Sie die Datendeduplizierungsfunktion für NTFS-Volumes aktivieren. Datendeduplizierung reduziert den auf dem Volume belegten Speicherplatz, indem doppelt vorhandene Fragemente der Dateien des Volumes nur je einmal gespeichert werden.

Sie können ein Volume, für das die Datendeduplizierung aktiviert ist, ohne Einschränkungen auf Laufwerksebene per Backup sichern und wiederherstellen. Backups auf Dateiebene werden unterstützt, ausgenommen bei Verwendung des Acronis VSS Providers. Wenn Sie Dateien aus einem Laufwerk-Backup wiederherstellen wollen, können Sie entweder das entsprechende Backup als virtuelle Maschine ausführen oder das Backup auf einer Maschine mounten, die Windows Server 2012 (oder höher) ausführt – und dann die Dateien aus dem gemounteten Volume heraus kopieren.

Die Datendeduplierungsfunktion von Windows Server und die Deduplizierungsfunktion von Acronis Backup sind eigenständig und ohne Bezug zueinander.

Unterstützte Aktionen mit logischen Volumes

Backups und Wiederherstellungen von Workloads mit logischen Volumes, wie LDM in Windows (dynamische Datenträger) und LVM in Linux, werden mit folgenden Einschränkungen unterstützt.

Backup

Ein agentenbasiertes Backup ist ein Backup, das von einem Protection Agent erstellt wird, der auf dem Workload oder auf einem Boot-Medium installiert ist.

Ein agentenloses Backup ist nur für virtuelle Maschinen verfügbar. Das agentenlose Backup wird auf Hypervisor-Ebene von einem Agenten durchgeführt, der alle virtuellen Maschinen in der Umgebung sichern und wiederherstellen kann. Auf den geschützten virtuellen Maschinen werden keine individuellen Agenten installiert.

Weitere Informationen über die Unterschiede zwischen einem agentenbasierten und einem agentenlosen Backup finden Sie im Abschnitt "Agentenbasiertes und agentenloses Backup" (S. 69).

Agentenbasiertes Backup	Agentenloses Backup
• Logische Volumes werden auf Basis der einzelnen Volumes gesichert. • Dateifilter (Einschlüsse/Ausschlüsse) werden unterstützt.	• Wenn ein logisches Volume auf einem Laufwerk erkannt wird, wird das Laufwerk im Sektor-für-Sektor-Modus (also im RAW-Format) gesichert. Die Partitionsstruktur des Laufwerks wird nicht analysiert und es werden keine Volume-Images separat gespeichert. • Einzelne LDM- oder LVM-Volumes können nicht als Backup-Quelle ausgewählt werden - weder durch direkte Auswahl noch durch die Verwendung von Richtlinienregeln. Im Bereich

Agentenbasiertes Backup	Agentenloses Backup
	Backup-Quelle eines Schutzplans ist nur die Option **Komplette Maschine** verfügbar. • Es werden keine Dateifilter (Einschlüsse/Ausschlüsse) unterstützt. Alle dennoch konfigurierten Ein- bzw. Ausschlüsse werden ignoriert.

Recovery

Eine agentenbasierte Wiederherstellung ist eine Wiederherstellung durch einen Agenten, der auf dem Workload oder auf einem Boot-Medium installiert ist.

Bei agentenlosen Wiederherstellungen werden nur virtuelle Maschinen als Ziele unterstützt. Die agentenlose Wiederherstellung wird auf Hypervisor-Ebene von einem Agenten durchgeführt, der alle virtuellen Maschinen in der Umgebung sichern und wiederherstellen kann. Der Anwender muss keine Zielmaschine manuell erstellen, auf der das Backup dann wiederhergestellt werden sollte.

	Aus einem agentenbasierten Backup	Aus einem agentenlosen Backup
Agentenbasierte Wiederherstellung	• Wiederherstellungen einzelner Volumes sind möglich. • Wiederherstellungen von Dateien und Ordnern sind möglich.	• Wiederherstellungen einzelner Volumes sind nicht möglich. • Wiederherstellungen von Dateien und Ordnern sind möglich.
Agentenlose Wiederherstellung	• Maschinen-Migrationen (P2V, V2P und V2V) werden nicht unterstützt. Um Daten aus einem agentenbasierten Backup wiederherzustellen, müssen Sie ein Boot-Medium verwenden. • Die Aktion **Als VM ausführen** wird nicht unterstützt. • Wiederherstellungen von Dateien und Ordnern sind möglich.	• Wiederherstellungen einzelner Volumes sind nicht möglich. • Wiederherstellungen einer kompletten Maschine sind möglich. • Wiederherstellungen von Dateien und Ordnern sind möglich. • Die Aktion **Als VM ausführen** wird unterstützt. Um die virtuelle Maschine bootfähig zu machen, müssen Sie evtl. die Boot-Reihenfolge ändern. Weitere Informationen dazu finden Sie in diesem Knowledge Base-Artikel. • Es werden Konvertierungen zu folgenden Arten von virtuellen Maschinen unterstützt: ◦ VMware ESXi

	Aus einem agentenbasierten Backup	Aus einem agentenlosen Backup
		◦ Microsoft Hyper-V ◦ Scale Computing HC3

Cyber Protection Agenten installieren und bereitstellen

Vorbereitung

Schritt 1:

Wählen Sie einen Agenten danach aus, welche Art von Daten Sie per Backup sichern wollen. Weitere Informationen über die Auswahlmöglichkeiten finden Sie im Abschnitt 'Welcher Agent wird wofür benötigt?'

Schritt 2:

Stellen Sie sicher, dass auf Ihrem Festplattenlaufwerk genügend freier Speicherplatz für die Installation eines Agenten vorhanden ist. Ausführlichere Informationen über den erforderlichen Speicherplatz finden Sie im Abschnitt '"Systemanforderungen für Agenten" (S. 70)'.

Schritt 3:

Laden Sie das Setup-Programm herunter. Sie können die Download-Links ermitteln, indem Sie auf **Alle Geräte** –> **Hinzufügen** klicken.

Auf der '**Geräte hinzufügen**'-Seite werden die Webinstaller für jeden Agenten bereitgestellt, der unter Windows installiert wird. Ein Webinstaller ist eine kleine, ausführbare Datei, die das Setup-Hauptprogramm aus dem Internet herunterlädt und dieses als temporäre Datei speichert. Die temporäre Datei wird direkt nach der Installation wieder gelöscht.

Falls Sie die Setup-Programme lokal speichern möchten, müssen Sie ein Paket herunterladen, welches alle Agenten zur Installation unter Windows enthält. Nutzen Sie dafür den Link im unteren Bereich der Seite '**Geräte hinzufügen**'. Es gibt sowohl 32-Bit- wie auch 64-Bit-Pakete. Mit diesem Paket können Sie festlegen, welche Komponenten installiert werden sollen. Diese Pakete ermöglichen Ihnen außerdem, eine unbeaufsichtigte Installation (beispielsweise per Gruppenrichtlinie) durchzuführen. Dieses erweiterte Szenario ist im Abschnitt '"Agenten per Gruppenrichtlinie bereitstellen" (S. 182)' beschrieben.

Um das Setup-Programm des Agenten für Microsoft 365 herunterzuladen, klicken Sie in der oberen rechten Ecke zuerst auf das Symbol für 'Konto' und dann auf **Downloads** –> **Agent für Microsoft 365**.

Die Installation unter Linux und macOS wird mithilfe herkömmlicher Setup-Programme durchgeführt.

Alle Setup-Programme benötigen eine Internetverbindung, um die Maschine im Cyber Protection Service registrieren zu können. Wenn es keine Internetverbindung gibt, schlägt die Installation fehl.

Schritt 4:

Die Cyber Protect-Funktionen erfordern ein installiertes Microsoft Visual C++ 2017 Redistributable-Paket. Sie sollten überprüfen, dass dieses bereits auf Ihrer Maschine installiert ist – oder es anderenfalls vor der Installation des Agenten installieren. Nach der Installation des Microsoft Visual C++ Redistributable-Pakets ist möglicherweise ein Neustart der Maschine erforderlich. Sie können das Microsoft Visual C++ Redistributable-Paket unter dieser Adresse finden: https://support.microsoft.com/help/2999226/update-for-universal-c-runtime-in-windows.

Schritt 5:

Überprüfen Sie, dass die Firewalls und anderen Komponenten Ihres Netzwerksicherheitssystems (z.B. ein Proxy-Server) ausgehende Verbindungen über folgende TCP-Ports erlauben:

- Die Ports **443** und **8443**

  Diese Ports werden verwendet, um auf die Cyber Protect-Konsole zuzugreifen, die Agenten zu registrieren, Zertifikate herunterzuladen, Benutzer zu autorisieren und Dateien aus dem Cloud Storage herunterzuladen.
- Die Ports im Bereich von **7770** bis **7800**

  Die Agenten verwenden diese Ports, um mit dem Management Server zu kommunizieren.
- Die Ports **44445** und **55556**

  Die Agenten verwenden diese Ports, um Daten bei Backup- und Recovery-Aktionen zu übertragen.

Falls in Ihrem Netzwerk ein Proxy-Server aktiv ist, sollten Sie sich unter '"Proxy-Server-Einstellungen konfigurieren" (S. 76)' darüber informieren, ob und wann Sie diese Einstellungen für jede Maschine konfigurieren müssen, die einen Protection Agenten ausführt.

Die minimale Internetverbindungsgeschwindigkeit, um den Agenten noch aus der Cloud verwalten zu können, beträgt 1 Mbit/s. Diese Geschwindigkeit sollte nicht mit der minimalen Übertragungsrate verwechselt werden, die benötigt wird, um Backups in die Cloud erstellen zu können. Berücksichtigen Sie dies, wenn Sie eine Internetanschlusstechnologie mit niedriger Bandbreite (wie ADSL) verwenden.

TCP-Ports, die für Backup und Replikation von virtuellen VMware-Maschinen erforderlich sind

- Der Port **443**

  Der Agent für VMware (Windows und Virtuelle Appliance) verbindet sich über diesen Port mit dem vCenter Server/ESXi-Host, um bei Backup-, Wiederherstellungs- und VM-Replikationsaktionen bestimmte VM-Verwaltungsaktionen (z.B. VMs auf vSphere erstellen, aktualisieren oder löschen) durchführen zu können.
- Der Port **902**

Der Agent für VMware (Windows und Virtuelle Appliance) verbindet sich über diesen Port mit dem ESXi-Host, um NFC-Verbindungen aufzubauen, um bei Backup-, Wiederherstellungs- und VM-Replikationsaktionen Daten auf VM-Laufwerken lesen bzw. schreiben zu können.

- Der Port **3333**

  Wenn der Agent für VMware (Virtuelle Appliance) auf dem ESXi-Host/Cluster läuft, der als Ziel der VM-Replikation dient, geht der VM-Replikations-Datenverkehr nicht direkt zum ESXi-Host auf dem Port **902**. Stattdessen geht der Datenverkehr vom als Quelle dienenden Agenten für VMware zum TCP-Port **3333** des Agenten für VMware (Virtuelle Appliance), der sich auf dem als Ziel dienenden ESXi-Host/Cluster befindet.

  Der als Quelle dienende Agent für VMware, der Daten von den ursprünglichen VM-Laufwerken liest, kann sich einem beliebigen Ort befinden und von jedem Typ sein: Virtuelle Appliance oder Windows.

  Der Dienst, der für den Empfang der VM-Replikationsdaten auf dem als Ziel dienenden Agenten für VMware (Virtuelle Appliance) verantwortlich ist, heißt 'Replica Disk Server'. Dieser Dienst ist für die WAN-Optimierungstechniken (wie die Komprimierung und Deduplizierung der Daten während der VM-Replikation) und das Replikat-Seeding verantwortlich (siehe den Abschnitt 'Seeding eines anfänglichen Replikats'). Wenn auf dem als Ziel dienenden ESXi-Host kein Agent für VMware (Virtuelle Appliance) ausgeführt wird, ist dieser Dienst nicht verfügbar, und wird folglich auch kein Replikat-Seeding-Szenario unterstützt.

Ports, die für die Downloader-Komponente erforderlich sind

Die Komponente 'Downloader' ist dafür zuständig, Updates auf einen Computer bereitzustellen und diese an andere Downloader-Instanzen zu verteilen. Er kann im Agenten-Modus laufen, wodurch der Computer zu einem Downloader-Agenten wird. Der Downloader-Agent lädt Updates aus dem Internet und von Servern als Quelle für die Verteilung der Updates an weitere Computer herunter. Der Downloader benötigt folgende Ports, um zu funktionieren.

- TCP- und UDP-Port (eingehend) **6888**

  Wird vom BitTorrent-Protokoll für Torrent-basierte Peer-to-Peer-Updates verwendet.
- UDP-Port **6771**

  Wird als lokaler Peer-Discovery-Port verwendet. Nimmt auch an den Peer-zu-Peer-Updates teil.
- TCP-Port **18018**

  Wird für die Kommunikation zwischen Updatern verwendet, die in verschiedenen Modi arbeiten: Updater und UpdaterAgent.
- TCP-Port **18019**

  Lokaler Port, der für die Kommunikation zwischen dem Updater und dem Protection Agenten verwendet wird.

Schritt 6:

Überprüfen Sie auf derjenigen Maschine, auf der Sie den Protection Agenten installieren wollen, ob die folgenden lokalen Ports nicht von anderen Prozessen verwendet werden:

- 127.0.0.1:**9999**
- 127.0.0.1:**43234**
- 127.0.0.1:**9850**

Hinweis
Sie müssen diese nicht in der Firewall öffnen.

Die vom Protection Agenten verwendeten Ports ändern

Es kann sein, dass einige der für den Protection Agenten erforderlichen Ports von anderen Applikationen in Ihrer Umgebung verwendet werden. Um Konflikte zu vermeiden, können Sie die standardmäßig vom Protection Agenten verwendeten Ports ändern, indem Sie folgende Dateien bearbeiten:

- Unter Linux: `/opt/Acronis/etc/aakore.yaml`
- Unter Windows: `\ProgramData\Acronis\Agent\etc\aakore.yaml`

Welcher Agent wird wofür benötigt?

Die Auswahl eines Agenten hängt davon ab, was Sie per Backup sichern wollen. Die untere Tabelle soll Ihnen durch eine Zusammenfassung aller relevanten Informationen bei dieser Entscheidung helfen.

Unter Windows erfordern der Agent für Exchange, der Agent für SQL, der Agent für Active Directory sowie der Agent für Oracle, dass auch der Agent für Windows installiert wird. Wenn Sie also beispielsweise den Agenten für SQL installieren, können Sie zudem auch immer ein Backup der kompletten Maschine (auf welcher der Agent installiert ist) erstellen.

Wir empfehlen Ihnen, dass Sie auch den Agenten für Windows installieren, wenn Sie den Agenten für VMware (Windows) und den Agenten für Hyper-V installieren.

Unter Linux erfordern der Agent für Oracle, der Agent für MySQL/MariaDB und der Agent für Virtuozzo, dass zusätzlich der Agent für Linux (64 Bit) installiert wird. Diese Agenten sind in der Setup-Datei des Agenten für Linux (64 Bit) als Bundle enthalten.

Was möchten Sie sichern?	Welchen Agenten soll ich installieren?	Wo soll die Installation erfolgen?
Physische Maschinen		
Unter Windows laufende physische Maschinen	Agent für Windows	Auf der Maschine, die gesichert werden soll.
Physische Maschinen, auf denen Linux läuft	Agent für Linux	
Unter macOS laufende physische Maschinen	Agent für Mac	

Datenbanken		
SQL-Datenbanken	Agent für SQL	Auf der Maschine, die den Microsoft SQL Server ausführt.
MySQL-Datenbanken	Agent für MySQL/MariaDB (In der Setup-Datei des Agenten für Linux (64 Bit) als Bundle enthalten)	Auf der Maschine, auf der der MySQL Server läuft.
MariaDB-Datenbanken	Agent für MySQL/MariaDB (In der Setup-Datei des Agenten für Linux (64 Bit) als Bundle enthalten)	Auf der Maschine, auf der der MariaDB Server läuft.
Exchange-Datenbanken	Agent für Exchange	Auf der Maschine, auf der die Postfachrolle des Microsoft Exchange Servers ausgeführt wird.*
Oracle-Datenbanken	Agent für Oracle (Unter Linux in der Setup-Datei des Agenten für Linux (64 Bit) als Bundle enthalten)	Auf der Maschine, die Oracle Database ausführt.
Cloud-zu-Cloud-Workloads		
Microsoft 365-Postfächer (Cloud Agent und lokaler Agent)	Cloud Agent (Keine Installation erforderlich)	Diese Funktionalität ist mit einem Cloud Agenten verfügbar, der im Datacenter bereitgestellt wird. Weitere Informationen finden Sie im Abschnitt '"Den Cloud Agenten für Microsoft 365 verwenden" (S. 664)'.

	Agent für Office 365	Auf einer Windows-Maschine, die über eine Internetverbindung verfügt. Weitere Informationen finden Sie im Abschnitt '"Den lokal installierten Agenten für Office 365 verwenden" (S. 659)'.
Microsoft 365 OneDrive-Dateien und SharePoint Online-Websites	Cloud Agent (Keine Installation erforderlich)	Diese Funktionalität ist mit einem Cloud Agenten verfügbar, der im Datacenter bereitgestellt wird. Weitere Informationen finden Sie im Abschnitt '"Den Cloud Agenten für Microsoft 365 verwenden" (S. 664)'.
Google Workspace Gmail-Postfächer, Google Drive-Dateien und Shared Drive-Dateien	Cloud Agent (Keine Installation erforderlich)	Diese Funktionalität ist mit einem Cloud Agenten verfügbar, der im Datacenter bereitgestellt wird. Weitere Informationen finden Sie im Abschnitt '"Google Workspace-Daten sichern" (S. 703)'.
Active Directory		
Maschinen, auf denen die Active Directory Domain Services (Active Directory-Domänendienste) laufen	Agent für Active Directory	Auf dem Domain Controller.
Virtuelle Maschinen		
Virtuelle VMware ESXi-Maschinen	Agent für VMware (Windows)	Auf einer Windows-Maschine, die Netzwerkzugriff auf den vCenter Server und den Storage für virtuelle Maschinen hat.**

	Agent für VMware (Virtuelle Appliance)	Auf dem ESXi-Host.
Virtuelle Hyper-V-Maschinen	Agent für Hyper-V	Auf dem Hyper-V-Host.
Virtuelle Scale Computing HC3-Maschinen	Agent für Scale Computing HC3 (Virtuelle Appliance)	Auf dem Scale Computing HC3-Host.
Virtuelle Red Hat Virtualization-Maschinen (verwaltet von oVirt)	Agent für oVirt (Virtuelle Appliance)	Auf dem Red Hat Virtualization-Host.
Virtuelle Virtuozzo-Maschinen und -Container***	Agent für Virtuozzo (In der Setup-Datei des Agenten für Linux (64 Bit) als Bundle enthalten)	Auf dem Virtuozzo-Host.
Virtuelle Virtuozzo Hybrid Infrastructure-Maschinen	Agent für Virtuozzo Hybrid Infrastructure (Virtuelle Appliance)	Auf dem Virtuozzo Hybrid Infrastructure-Host.
Virtuelle Maschinen, die auf Amazon EC2 gehostet werden	Wie bei den physischen Maschinen****	Auf der Maschine, die gesichert werden soll.
Virtuelle Maschinen, auf Windows Azure gehostet		
Virtuelle Citrix XenServer-Maschinen		
Red Hat Virtualization (RHV/RHEV), not managed by oVirt		
Kernel-basierte virtuelle Maschinen (KVM), nicht von oVirt verwaltet		
Virtuelle Oracle-Maschinen, nicht von oVirt verwaltet		
Virtuelle Nutanix AHV-Maschinen		
Red Hat Virtualization (RHV/RHEV), von oVirt verwaltet	Agent für oVirt (Virtuelle Appliance)	Auf dem Virtualisierungshost.
Kernel-basierte virtuelle Maschinen (KVM), von oVirt verwaltet		
Virtuelle Oracle-Maschinen, von oVirt verwaltet		
Mobilgeräte		

Mobilgeräte mit Android	Mobile App für Android	Auf dem Mobilgerät, das gesichert werden soll.
Mobilgeräte mit iOS	Mobile App für iOS	

*Der Agent für Exchange überprüft während der Installation, ob die Maschine, auf welcher er ausgeführt wird, genügend freier Speicherplatz hat. Während einer granularen Wiederherstellung wird temporär so viel freier Speicherplatz benötigt, wie es 15% der größten Exchange-Datenbank entspricht.

**Sollte Ihr ESXi einen per SAN angeschlossenen Storage verwenden, dann installieren Sie den Agenten auf einer Maschine, die an dasselbe SAN angeschlossen ist. Der Agent führt das Backup der virtuellen Maschinen dann direkt vom Storage aus, statt über den ESXi-Host und das LAN. Weitere Informationen dazu finden Sie im Abschnitt '"Agent für VMware – LAN-freies Backup" (S. 756)'.

***Für Virtuozzo 7 werden nur Ploop-Container unterstützt. Virtuelle Maschinen werden nicht unterstützt.

****Eine virtuelle Maschine wird dann als virtuell betrachtet, wenn Sie von einem externen Agenten gesichert wird. Sollte ein Agent dagegen in einem Gastsystem installiert sein, werden Backup- und Recovery-Aktionen genauso wie bei physischen Maschinen durchgeführt. Wenn Cyber Protection jedoch eine virtuelle Maschine mithilfe der CPUID-Anweisung identifizieren kann, wird ihr eine Service-Quota für virtuelle Maschinen zugewiesen. Wenn Sie direktes Passthrough oder eine andere Option verwenden, die die CPU-Hersteller-ID maskiert, können nur Service-Quotas für physische Maschinen zugewiesen werden.

Agentenbasiertes und agentenloses Backup

Ein agentenbasiertes Backup erfordert es, dass auf jeder geschützten Maschine ein Protection Agent installiert ist. Das agentenbasierte Backup wird auf allen physischen und virtuellen Maschinen unterstützt. Weitere Informationen darüber, welchen Agenten Sie benötigen und wo Sie diesen installieren können, finden Sie im Abschnitt "Welcher Agent wird wofür benötigt?" (S. 65)

Ein agentenloses Backup wird von einigen Virtualisierungsplattformen unterstützt und ist nicht für physische Maschinen verfügbar. Für das agentenlose Backup ist lediglich ein Protection Agent erforderlich, der auf einer speziellen Maschine in der virtuellen Umgebung installiert wird. Dieser Agent sichert alle anderen virtuellen Maschinen in dieser Umgebung. Weitere Informationen zu den unterstützten Backup-Typen pro Virtualisierungsplattform finden Sie im Abschnitt "Unterstützte Virtualisierungsplattformen" (S. 33).

Für einige Virtualisierungsplattformen sind virtuelle Appliances verfügbar. Eine virtuelle Appliance (VA) ist eine vorgefertigte virtuelle Maschine, die bereits einen Protection Agenten enthält. Die virtuellen Appliances liegen in Hypervisor-spezifischen Formaten vor (z.B. als .ovf-, .ova- oder .qcow-Dateien).

Welcher Backup-Typ wird benötigt?

Wir empfehlen ein agentenbasiertes Backup, wenn Sie Folgendes benötigen:

- Zusätzliche Schutzfunktionen, wie Antivirus- und Antimalware, Patch-Verwaltung oder Remote-Desktop-Verbindungen. Weitere Informationen zu diesen Funktionen finden Sie unter "Unterstützte Schutzfunktionen, nach Betriebssystem" (S. 46).
- Sie müssen die virtuellen Maschinen auf der Mandanten-Ebene voneinander separieren, weil Sie beispielsweise den Benutzern in diesem Mandanten nur den Zugriff auf ihre jeweils eigenen Backups gewähren wollen.
- Backups auf Dateiebene, die Sie zu den Gast-Betriebssystemen wiederherstellen können.

Wir empfehlen ein agentenbasiertes Backup, wenn Sie Folgendes benötigen:

- Nur die Backup-Funktionalität, ohne weitere Schutzfunktionen.
- Vereinfachte Verwaltung - Sie können mehrere virtuelle Maschinen per Backup sichern, indem Sie nur einen Agenten installieren und konfigurieren.
- Minimale Ressourcennutzung - ein dedizierter Agent verbraucht weniger CPU und RAM als mehrere Agenten, die auf jeder virtuellen Maschine in Ihrer Umgebung installiert sind.
- Spezifische Backup-Einrichtungen, wie zum Beispiel LAN-freies Backup. Weitere Informationen zu dieser Funktion finden Sie unter "Agent für VMware – LAN-freies Backup" (S. 756).
- Weniger Konfigurationsaufwand. Der dedizierte Agent sichert die virtuellen Maschinen auf Hypervisor-Ebene, unabhängig von den Gast-Betriebssystemen.

Systemanforderungen für Agenten

Agent	Für die Installation erforderlicher Speicherplatz
Agent für Windows	1,2 GB
Agent für Linux	2 GB
Agent für Mac	1 GB
Agent für SQL und Agent für Windows	1,2 GB
Agent für Exchange und Agent für Windows	1,3 GB
Agent für Data Loss Prevention	500 MB
Agent für Microsoft 365	500 MB
Agent für Active Directory und Agent für Windows	2 GB
Agent für VMware und Agent für Windows	1,5 GB
Agent für Hyper-V und Agent für Windows	1,5 GB

Agent für Virtuozzo und Agent für Linux	1 GB
Agent für Virtuozzo Hybrid Infrastructure	700 MB
Agent für Oracle und Agent für Windows	2,2 GB
Agent für Oracle und Agent für Linux	2 GB
Agent für MySQL/MariaDB und Agent für Linux	2 GB

Für Backup-Aktionen (einschließlich dem Löschen von Backups) werden etwa 1 GB RAM pro 1 TB Backup-Größe benötigt. Der Speicherverbrauch kann – abhängig von der Art und Menge der Daten, die die Agenten verarbeiten – variieren.

Hinweis
Der RAM-Bedarf kann ansteigen, wenn besonders große Backup-Sets (4 TB und mehr) gesichert werden.

Auf x64-Systemen müssen für Aktionen mit Boot-Medien und Laufwerkswiederherstellungen, bei denen ein Neustart erforderlich ist, mindestens 2 GB Arbeitsspeicher vorhanden sein.

Auf Workloads mit modernen Prozessoren (z.B. Intel Core-CPUs der 11. Generation oder AMD Ryzen 7), die die CET-Technologie unterstützen, werden einige Funktionen des Agenten für Data Loss Prevention deaktiviert, um Konflikte zu vermeiden. In der nachfolgenden Tabelle wird aufgeführt, welche der Gerätekontrolle- und Advanced DLP-Funktionen auf Systemen mit solchen CPUs verfügbar sind.

Funktionen	Gerätekontrolle	Advanced DLP
Lokale Kanäle		
Wechselmedien	n/a	Ja
Verschlüsselte Wechsellaufwerke	Ja	n/a
Drucker	n/a	Nein
Umgeleitetes Netzlaufwerke	n/a	Ja
Umgeleitete Zwischenablage	n/a	Nein
Netzwerkkommunikationen		
SMTP-E-Mails	n/a	Ja
Microsoft Outlook (MAPI)	n/a	Ja
IBM Notes	n/a	Nein
Webmails	n/a	Ja

Instant Messaging (ICQ)	n/a	Nein
Instant Messaging (Viber)	n/a	Nein
Instant Messaging (IRC, Jabber, Skype, Viber)	n/a	Ja
File Sharing Services	n/a	Ja
Soziale Netzwerke	n/a	Ja
Dateifreigaben im lokalen Netzwerk (SMB)	n/a	Ja
Webzugriff (HTTP/HTTPS)	n/a	Ja
Dateiübertragungen (FTP/FTPS)	n/a	Ja
Positivliste für Datenübertragungen		
Positivliste für Gerätetypen	n/a	Ja
Positivliste für Netzwerkkommunikation	n/a	Ja
Positivliste für Remote-Hosts	n/a	Ja
Positivliste für Applikationen	n/a	Ja
Peripheriegeräte		
Wechselmedien	Ja	Ja
Verschlüsselte Wechsellaufwerke	Ja	Ja
Drucker	Nein	Nein
Über MTP angeschlossene Mobilgeräte	Nein	Nein
Bluetooth-Adapter	Ja	Ja
Optische Laufwerke	Ja	Ja
Diskettenlaufwerke	Ja	Ja
Windows-Zwischenablage	Nein	Nein
Screenshot-Aufnahme	Nein	Nein
Umgeleitetes Netzlaufwerke	Ja	Ja
Umgeleitete Zwischenablage	Nein	Nein
Selbstschutzfunktion für den Cyber Protect Agenten		
Schutz vor regulären Endbenutzern	Ja	Ja
Schutz vor lokalen Systemadministratoren	Ja	Ja

Linux-Pakete

Um die benötigten Module dem Linux-Kernel hinzufügen zu können, benötigt das Setup-Programm folgende Linux-Pakete:

- Das Paket mit den Kernel-Headers oder Kernel-Quellen. Die Paketversion muss zur Kernel-Version passen.
- Das GNU Compiler Collection (GCC) Compiler System. Die GCC-Version muss dieselbe sein, mit der der Kernel kompiliert wurde.
- Das Tool 'Make'.
- Der Perl-Interpreter.
- Die Bibliotheken `libelf-dev`, `libelf-devel` oder `elfutils-libelf-devel`, um Kernels ab v4.15 zu erstellen, die mit dem Parameter CONFIG_UNWINDER_ORC=y konfiguriert wurden. Für einige Distributionen, wie z.B. Fedora 28, müssen diese separat von Kernel-Headern installiert werden.

Die Namen dieser Pakete variieren je nach Ihrer Linux-Distribution.

Unter Red Hat Enterprise Linux, CentOS und Fedora werden die Pakete normalerweise vom Setup-Programm installiert. Bei anderen Distributionen müssen Sie die Pakete installieren, sofern Sie noch nicht installiert sind oder nicht die benötigten Versionen haben.

Sind die erforderlichen Pakete bereits installiert?

Führen Sie folgende Schritte aus, um zu überprüfen, ob die Pakete bereits installiert sind:

1. Führen Sie folgenden Befehl aus, um die Kernel-Version und die erforderliche GCC-Version zu ermitteln:

   ```
   cat /proc/version
   ```

   Die Ausgabezeilen dieses Befehls sehen ungefähr so aus: `Linux-Version 2.6.35.6` und `GCC-Version 4.5.1`
2. Führen Sie folgenden Befehl aus, um zu ermitteln, ob das Tool 'Make' und der GCC-Compiler installiert sind:

   ```
   make -v
   gcc -v
   ```

   Stellen Sie für **gcc** sicher, dass die vom Befehl zurückgemeldete Version die gleiche `GCC-Version` ist wie die in Schritt 1. Bei **make** müssen Sie nur sicherstellen, dass der Befehl ausgeführt wird.
3. Überprüfen Sie, ob für die Pakete zur Erstellung der Kernel-Module die passende Version installiert ist:
   - Führen Sie unter Red Hat Enterprise Linux, CentOS und Fedora folgenden Befehl aus:

     ```
     yum list installed | grep kernel-devel
     ```

- Führen Sie unter Ubuntu folgende Befehle aus:

```
dpkg --get-selections | grep linux-headers
dpkg --get-selections | grep linux-image
```

Stellen Sie in jedem Fall sicher, dass die Paketversionen die gleichen sind wie in der `Linux-Version` von Schritt 1.

4. Mit folgendem Befehl können Sie überprüfen, ob der Perl-Interpreter installiert ist:

```
perl --version
```

Der Interpreter ist installiert, wenn Ihnen Informationen über die Perl-Version angezeigt werden.

5. Führen Sie unter Red Hat Enterprise Linux, CentOS und Fedora folgenden Befehl aus, um zu überprüfen, ob `elfutils-libelf-devel` installiert ist:

```
yum list installed | grep elfutils-libelf-devel
```

Die Bibliothek ist installiert, wenn Ihnen Informationen über die Bibliotheksversion angezeigt werden.

Installation der Pakete aus dem Repository

Die folgende Tabelle führt auf, wie Sie die erforderlichen Pakete in verschiedenen Linux-Distributionen installieren können.

Linux-Distribution	Paketnamen	Art der Installation
Red Hat Enterprise Linux	**kernel-devel** **gcc** **make** **elfutils-libelf-devel**	Das Setup-Programm wird die Pakete unter Verwendung Ihres Red Hat-Abonnements automatisch herunterladen und installieren.
	perl	Führen Sie folgenden Befehl aus: `yum install perl`
CentOS Fedora	**kernel-devel** **gcc** **make** **elfutils-libelf-devel**	Das Setup-Programm wird die Pakete automatisch herunterladen und installieren.
	perl	Führen Sie folgenden Befehl aus: `yum install perl`

Ubuntu
Debian
	linux-headers
	linux-image
	gcc
	make
	perl
		Führen Sie folgende Befehle aus:
		`sudo apt-get update`
		`sudo apt-get install linux-headers-$(uname -r)`
		`sudo apt-get install linux-image-$(uname -r)`
		`sudo apt-get install gcc-<package version>`
		`sudo apt-get install make`
		`sudo apt-get install perl`

SUSE Linux
OpenSUSE
	kernel-source
	gcc
	make
	perl
		`sudo zypper install kernel-source`
		`sudo zypper install gcc`
		`sudo zypper install make`
		`sudo zypper install perl`

Die Pakete werden aus dem Repository der Distribution heruntergeladen und installiert.

Informieren Sie sich für andere Linux-Distribution in den Dokumentationen der Distribution, wie die exakten Namen der erforderlichen Pakete dort lauten und wie diese installiert werden.

Manuelle Installation der Pakete

Sie müssen die Pakete **manuell** installieren, falls:

- Die Maschine kein aktives Red Hat-Abonnement oder keine Internetverbindung hat.
- Das Setup-Programm kann die zu Ihrer Kernel-Version passenden Versionen von **kernel-devel** oder **gcc** nicht finden. Sollte das verfügbare **kernel-devel** neuer als Ihr Kernel sein, dann müssen Sie den Kernel aktualisieren oder die passende **kernel-devel**-Version manuell installieren.
- Sie haben die erforderlichen Pakete im lokalen Netzwerk und möchten keine Zeit für automatische Suche und Download aufbringen.

Beziehen Sie die Pakete aus Ihrem lokalen Netzwerk oder von der Webseite eines vertrauenswürdigen Drittherstellers – und installieren Sie diese dann wie folgt:

- Führen Sie unter Red Hat Enterprise Linux, CentOS oder Fedora folgenden Befehl als Benutzer 'root' aus:

  ```
  rpm -ivh PACKAGE_FILE1 PACKAGE_FILE2 PACKAGE_FILE3
  ```

- Führen Sie unter Ubuntu folgenden Befehl aus:

  ```
  sudo dpkg -i PACKAGE_FILE1 PACKAGE_FILE2 PACKAGE_FILE3
  ```

Beispiel: Manuell Installation der Pakete unter Fedora 14

Folgen Sie diesen Schritten, um die erforderlichen Pakete unter Fedora 14 auf einer 32-Bit-Maschine zu installieren:

1. Führen Sie folgenden Befehl aus, um die Kernel-Version und die erforderliche GCC-Version zu ermitteln:

```
cat /proc/version
```

Die Ausgabe dieses Befehls beinhaltet Folgendes:

```
Linux version 2.6.35.6-45.fc14.i686
gcc version 4.5.1
```

2. Besorgen Sie sich die Pakete für **kernel-devel** und **gcc**, die zu dieser Kernel-Version passen:

```
kernel-devel-2.6.35.6-45.fc14.i686.rpm
gcc-4.5.1-4.fc14.i686.rpm
```

3. Besorgen Sie sich das **make**-Paket für Fedora 14:

```
make-3.82-3.fc14.i686
```

4. Führen Sie folgende Befehle als Benutzer 'root' aus, um die Pakete zu installieren:

```
rpm -ivh kernel-devel-2.6.35.6-45.fc14.i686.rpm
rpm -ivh gcc-4.5.1.fc14.i686.rpm
rpm -ivh make-3.82-3.fc14.i686
```

Sie können all diese Pakete mit einem einzigen `rpm`-Befehl spezifizieren. Die Installation jeder dieser Pakete kann die Installation weiterer Pakete erfordern, um Abhängigkeiten aufzulösen.

Proxy-Server-Einstellungen konfigurieren

Die Protection Agenten können ihre Daten auch über einen HTTP/HTTPS-Proxy-Server übertragen. Der Server muss durch einen HTTP-Tunnel arbeiten, ohne den HTTP-Verkehr zu scannen oder zu beeinflussen. Man-in-the-Middle-Proxies werden nicht unterstützt.

Da sich der Agent bei der Installation selbst in der Cloud registriert, müssen die Proxy-Server-Einstellungen während der Installation des Agenten oder schon vorher konfigurieren.

Für Windows

Wenn ein Proxy-Server unter **Systemsteuerung** –> **Internetoptionen** –> **Verbindungen** konfiguriert ist, liest das Setup-Programm die entsprechenden Proxy-Server-Einstellungen aus der Registry aus und übernimmt diese automatisch.

Verwenden Sie diese Prozedur, wenn Sie die nachfolgenden Tasks ausführen wollen.

- Die Proxy-Einstellungen vor der Installation des Agenten konfigurieren.
- Die Proxy-Einstellungen nach der Installation des Agenten aktualisieren.

Informationen zur Konfiguration der Proxy-Einstellungen während der Installation des Agenten finden Sie im Abschnitt '"Protection Agenten in Windows installieren" (S. 82)'.

Hinweis
Diese Prozedur ist nur gültig, wenn auf der Maschine die Datei `http-proxy.yaml` nicht vorhanden ist. Wenn die Datei `http-proxy.yaml` auf der Maschine vorhanden ist, müssen Sie die Proxy-Einstellungen in dieser Datei aktualisieren, da sie die Einstellungen in der Datei `aakore.yaml` aufhebt.

Die Datei `%programdata%\Acronis\Agent\var\aakore\http-proxy.yaml` wird erstellt, wenn Sie die Proxy-Server-Einstellungen über den Cyber Protection Monitor konfigurieren. Weitere Informationen finden Sie im Abschnitt '"Proxy-Server-Einstellungen im Cyber Protect Monitor konfigurieren" (S. 342)'.

Um die Datei `http-proxy.yaml` öffnen zu können, müssen Sie in Windows zur Benutzergruppe der Administratoren gehören.

So können Sie die Proxy-Einstellungen konfigurieren

1. Erstellen Sie ein neues Text-Dokument und öffnen Sie dieses in einem Text-Editor (wie Notepad).
2. Kopieren Sie die nachfolgenden Zeilen und fügen Sie diese dann in die Datei ein.

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\Global\HttpProxy]
"Enabled"=dword:00000001
"Host"="proxy.company.com"
"Port"=dword:000001bb
"Login"="proxy_login"
"Password"="proxy_password"
```

3. Ersetzen Sie `proxy.company.com` mit dem Host-Namen/der IP-Adresse Ihres Proxy-Servers – und verwenden Sie `000001bb` als Hexadezimalwert für die Port-Nummer. Beispielsweise entspricht `000001bb` dem Port 443.
4. Wenn Ihr Proxy-Server eine Authentifizierung benötigt, ersetzen Sie `proxy_login` und `proxy_password` mit den entsprechenden Anmeldedaten des Proxy-Servers. Anderenfalls können Sie diese Zeilen aus der Datei löschen.
5. Speichern Sie das Dokument als '`proxy.reg`'.
6. Führen Sie die Datei 'als Administrator' aus.
7. Bestätigen Sie, dass Sie die Änderung der Windows Registry wirklich ausführen wollen.
8. Wenn der Agent auf diesem Workload noch nicht installiert ist, müssen Sie ihn jetzt installieren. Wenn der Agent bereits auf dem Workload installiert ist, können Sie mit dem nächsten Schritt fortfahren.
9. Öffnen Sie die Datei `%programdata%\Acronis\Agent\etc\aakore.yaml` in einem Text-Editor.
   Um diese Datei öffnen zu können, müssen Sie in Windows zur Benutzergruppe der Administratoren gehören.
10. Suchen Sie den Abschnitt **env** (oder erstellen Sie diesen) und fügen Sie dann folgende Zeilen hinzu:

```
env:
    http-proxy: proxy_login:proxy_password@proxy_address:port
    https-proxy: proxy_login:proxy_password@proxy_address:port
```

11. Ersetzen Sie `proxy_login` und `proxy_password` mit den Anmeldedaten des Proxy-Servers – und `proxy_address:port` mit der Adresse und der Port-Nummer des Proxy-Servers.
12. Klicken Sie im **Start**-Menü auf **Ausführen** und geben Sie Folgendes ein: **cmd**. Klicken Sie anschließend auf **OK**.
13. Starten Sie den aakore-Dienst mit folgenden Befehlen neu:

```
net stop aakore
net start aakore
```

14. Starten Sie den Agenten mit folgenden Befehlen neu:

```
net stop mms
net start mms
```

Für macOS

Verwenden Sie diese Prozedur, wenn Sie die nachfolgenden Tasks ausführen wollen.

- Die Proxy-Einstellungen vor der Installation des Agenten konfigurieren.
- Die Proxy-Einstellungen nach der Installation des Agenten aktualisieren.

Informationen zur Konfiguration der Proxy-Einstellungen während der Installation des Agenten finden Sie im Abschnitt '"Protection Agenten in macOS installieren" (S. 87)'.

So können Sie die Proxy-Einstellungen konfigurieren

1. Erstellen Sie die Datei '`/Library/Application Support/Acronis/Registry/Global.config`' und öffnen Sie diese in einem Text-Editor (wie z.B. Text Edit).
2. Kopieren Sie die nachfolgenden Zeilen und fügen Sie diese dann in die Datei ein.

```
<?xml version="1.0" ?>
<registry name="Global">
    <key name="HttpProxy">
        <value name="Enabled" type="Tdword">"1"</value>
        <value name="Host" type="TString">"proxy.company.com"</value>
        <value name="Port" type="Tdword">"443"</value>
        <value name="Login" type="TString">"proxy_login"</value>
        <value name="Password" type="TString">"proxy_password"</value>
    </key>
</registry>
```

3. Ersetzen Sie `proxy.company.com` mit dem Host-Namen/der IP-Adresse Ihres Proxy-Servers – und verwenden Sie `443` als Dezimalwert für die Port-Nummer.

4. Wenn Ihr Proxy-Server eine Authentifizierung benötigt, ersetzen Sie `proxy_login` und `proxy_password` mit den entsprechenden Anmeldedaten des Proxy-Servers. Anderenfalls können Sie diese Zeilen aus der Datei löschen.
5. Speichern Sie die Datei.
6. Wenn der Agent auf diesem Workload noch nicht installiert ist, müssen Sie ihn jetzt installieren. Wenn der Agent bereits auf dem Workload installiert ist, können Sie mit dem nächsten Schritt fortfahren.
7. Öffnen Sie die Datei `/Library/Application Support/Acronis/Agent/etc/aakore.yaml` in einem Text-Editor.
8. Suchen Sie den Abschnitt **env** (oder erstellen Sie diesen) und fügen Sie dann folgende Zeilen hinzu:

```
env:
    http-proxy: proxy_login:proxy_password@proxy_address:port
    https-proxy: proxy_login:proxy_password@proxy_address:port
```

9. Ersetzen Sie `proxy_login` und `proxy_password` mit den Anmeldedaten des Proxy-Servers – und `proxy_address:port` mit der Adresse und der Port-Nummer des Proxy-Servers.
10. Gehen Sie zu **Applikationen** –> **Dienstprogramme** –> **Terminal**.
11. Starten Sie den aakore-Dienst mit folgenden Befehlen neu:

```
sudo launchctl stop aakore
sudo launchctl start aakore
```

12. Starten Sie den Agenten mit folgenden Befehlen neu:

```
sudo launchctl stop acronis_mms
sudo launchctl start acronis_mms
```

Für Linux

Starten Sie die Installationsdatei mit den Parametern `--http-proxy-host=ADDRESS --http-proxy-port=PORT --http-proxy-login=LOGIN --http-proxy-password=PASSWORD`. Verwenden Sie die nachfolgende Prozedur, um die Proxy-Einstellungen nach der Installation des Protection Agenten zu aktualisieren.

So können Sie die Proxy-Einstellungen konfigurieren

1. Öffnen Sie die Datei `/etc/Acronis/Global.config` in einem Text-Editor.
2. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Wenn die Proxy-Einstellungen während der Installation des Agenten spezifiziert wurden, suchen Sie nach dem folgenden Abschnitt.

```
<key name="HttpProxy">
    <value name="Enabled" type="Tdword">"1"</value>
    <value name="Host" type="TString">"ADDRESS"</value>
    <value name="Port" type="Tdword">"PORT"</value>
    <value name="Login" type="TString">"LOGIN"</value>
```

```
    <value name="Password" type="TString">"PASSWORD"</value>
</key>
```

- Wenn die Proxy-Einstellungen nicht während der Installation des Agenten spezifiziert wurden, müssen Sie die nachfolgenden Zeilen kopieren und zwischen den Tags `<registry name="Global">...</registry>` in die Datei einfügen.

```
<key name="HttpProxy">
    <value name="Enabled" type="Tdword">"1"</value>
    <value name="Host" type="TString">"ADDRESS"</value>
    <value name="Port" type="Tdword">"PORT"</value>
    <value name="Login" type="TString">"LOGIN"</value>
    <value name="Password" type="TString">"PASSWORD"</value>
</key>
```

3. Ersetzen Sie `ADDRESS` mit dem Host-Namen/der IP-Adresse des neuen Proxy-Servers – und `PORT` mit dem Dezimalwert der dazugehörigen Port-Nummer.
4. Wenn Ihr Proxy-Server eine Authentifizierung benötigt, ersetzen Sie `LOGIN` und `PASSWORD` mit den entsprechenden Anmeldedaten des Proxy-Servers. Anderenfalls können Sie diese Zeilen aus der Datei löschen.
5. Speichern Sie die Datei.
6. Öffnen Sie die Datei `/opt/acronis/etc/aakore.yaml` in einem Text-Editor.
7. Suchen Sie den Abschnitt **env** (oder erstellen Sie diesen) und fügen Sie dann folgende Zeilen hinzu:

```
env:
    http-proxy: proxy_login:proxy_password@proxy_address:port
    https-proxy: proxy_login:proxy_password@proxy_address:port
```

8. Ersetzen Sie `proxy_login` und `proxy_password` mit den Anmeldedaten des Proxy-Servers – und `proxy_address:port` mit der Adresse und der Port-Nummer des Proxy-Servers.
9. Starten Sie den aakore-Dienst mit dem folgenden Befehl neu:

```
sudo service aakore restart
```

10. Starten Sie den Agenten neu, indem Sie den folgenden Befehl in einem beliebigen Verzeichnis ausführen.

```
sudo service acronis_mms restart
```

Für Boot-Medien

Wenn Sie unter einem Boot-Medium arbeiten, müssen Sie möglicherweise über einen Proxy-Server auf den Cloud Storage zugreifen. Wenn Sie die Proxy-Server-Einstellungen konfigurieren wollen, müssen Sie auf **Tools** –> **Proxy-Server** klicken und dann den Host-Namen/die IP-Adresse, den Port und die Anmeldedaten des Proxy-Servers konfigurieren.

Protection Agenten installieren

Sie können Agenten auf Maschinen installieren, die eines der im Abschnitt 'Unterstützte Betriebssysteme und Umgebungen' aufgeführten Betriebssysteme ausführen. Die Betriebssysteme, die die Cyber Protect-Funktionen unterstützen, sind im Abschnitt 'Unterstützte Cyber Protect-Funktionen, nach Betriebssystem' aufgeführt.

Protection Agenten herunterladen

Bevor Sie einen Agenten installieren können, müssen Sie dessen Installationsdatei von der Cyber Protect-Konsole herunterladen.

So können Sie einen Agent herunterladen, wenn Sie einen zu schützenden Workload hinzufügen

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte** –> **Alle Geräte**.
2. Klicken Sie im oberen rechten Fensterbereich auf **Gerät hinzufügen**.
3. Wählen Sie im Panel **Geräte hinzufügen** aus dem Listenfeld **Release-Kanal** eine Agenten-Version aus.
   - **Vorherige Version** – laden Sie den Agenten des letzten Version herunter.
   - **Aktuell** – laden Sie die neueste verfügbare Agenten-Version herunter.
4. Wählen Sie den Agenten aus, der dem Betriebssystem des Workloads entspricht, den Sie hinzufügen wollen.
   Der Dialog **Speichern unter** wird angezeigt.
5. [Nur für Macs mit Apple Silicon-Prozessoren (z.B. Apple M1)] Klicken Sie auf **Abbrechen**. Klicken Sie im dann angezeigten Dialog **Mac hinzufügen** auf den Link **ARM-Installer herunterladen**.
6. Wählen Sie einen Speicherort für die Installationsdatei des Agenten und klicken Sie anschließend auf **Speichern**.

So können Sie einen Agenten zur späteren Verwendung herunterladen

1. Klicken Sie in der oberen rechten Ecke der Cyber Protect-Konsole auf das **Benutzer**-Symbol.
2. Klicken Sie auf **Downloads**.
3. Wählen Sie im Dialog **Downloads** aus dem Listenfeld **Release-Kanal** eine Agenten-Version aus.
   - **Vorherige Version** – laden Sie den Agenten des letzten Version herunter.
   - **Aktuell** – laden Sie die neueste verfügbare Agenten-Version herunter.
4. Scrollen Sie durch die Liste der verfügbaren Installer, um den gewünschten Agenten-Installer zu finden, und klicken Sie dann am Ende der entsprechenden Zeile auf das Download-Symbol.
   Der Dialog **Speichern unter** wird angezeigt.
5. Wählen Sie einen Speicherort für die Installationsdatei des Agenten und klicken Sie anschließend auf **Speichern**.

Protection Agenten in Windows installieren

Voraussetzungen

Laden Sie den Agenten herunter, den Sie auf dem Workload benötigen, den Sie schützen wollen. Siehe Abschnitt '"Protection Agenten herunterladen" (S. 81)'.

So können Sie den Agenten für Windows installieren

1. Überprüfen Sie, dass die Maschine mit dem Internet verbunden ist.
2. Melden Sie sich als Administrator an und starten Sie den Installer.
3. [Optional] Klicken Sie auf **Installationseinstellungen anpassen**, um (sofern gewünscht) eine oder mehrere der folgenden Änderungen durchzuführen:
   - Um die zu installierenden Komponenten zu ändern (beispielsweise, um die Installation des Cyber Protection Monitors oder des Befehlszeilenwerkzeugs zu deaktivieren oder, um den Agenten für Antimalware Protection und den Agenten URL-Filterung zu installieren).

     Hinweis
     Auf Windows-Maschinen ist es für die Antimalware Protection-Funktion die Installation des Agenten für Antimalware Protection sowie für die URL-Filterungsfunktion die Installation des Agenten für URL-Filterung erforderlich. Diese Agenten werden automatisch auf den geschützten Workloads installiert, wenn die Module **Antivirus & Antimalware Protection** und/oder **URL-Filterung** in deren Schutzplänen aktiviert werden.

   - Die Methode ändern, mit der der Workload im Cyber Protection Service registriert wird. Sie können von **Service-Konsole verwenden** (Standard) zu **Anmeldedaten verwenden** oder **Registrierungstoken verwenden** umstellen.
   - Um den Installationspfad zu ändern.
   - Um das Benutzerkonto zu ändern, unter dem der Dienst des Agenten ausgeführt werden soll. Weitere Informationen finden Sie hier: "Das Anmeldekonto auf Windows-Maschinen ändern" (S. 90).
   - Um den Host-Namen/die IP-Adresse, den Port und die Anmeldedaten des Proxy-Servers zu überprüfen oder zu ändern. Unter Windows wird ein verfügbarer Proxy-Server automatisch erkannt und verwendet.
4. Klicken Sie auf **Installieren**.
5. [Nur, wenn Sie den Agenten für VMware installieren] Spezifizieren Sie die Adresse und Anmeldedaten für den vCenter Server oder den eigenständigen ESXi-Host, auf dem Sie virtuelle Maschinen sichern und wiederherstellen wollen – und klicken Sie dann auf **Fertig**.
   Wir empfehlen, dass Sie für den Zugriff auf den vCenter Server oder den ESXi Host ein dediziertes Konto verwenden, anstatt ein bereits vorhandenes Konto mit der Administrator-Rolle zu verwenden. Weitere Informationen zu den erforderlichen Berechtigungen für das dedizierte Konto finden Sie im Abschnitt '"Agent für VMware – notwendige Berechtigungen" (S. 766)'.

6. [Nur, wenn Sie eine Installation auf einem Domain Controller durchführen] Spezifizieren Sie das Benutzerkonto, unter dem der Agenten-Dienst ausgeführt werden soll – und klicken Sie dann auf **Fertig**. Das Setup-Programm erstellt aus Sicherheitsgründen nicht automatisch neue Konten auf einem Domain Controller.

   Hinweis
   Das von Ihnen spezifizierte Benutzerkonto muss die Berechtigung `Anmelden als Dienst` erhalten. Dieses Konto muss bereits auf dem Domain Controller verwendet worden sein, damit sein Profilordner auf dieser Maschine erstellt werden kann.

   Weitere Informationen zur Installation des Agenten auf einem schreibgeschützten Domain Controller (RODC, Read-only Domain Controller) finden Sie in diesem Knowledge Base-Artikel.
7. Wenn Sie die Standardregistrierungsmethode **Service-Konsole verwenden** in Schritt 3 übernommen haben, warten Sie, bis die Registrierungsanzeige erscheint, und fahren Sie dann mit dem nächsten Schritt fort. Ansonsten sind keine weiteren Aktionen erforderlich.
8. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Wenn Sie sich mit dem Konto eines Firmenadministrators anmelden, müssen Sie Workloads für Ihr Unternehmen registrieren:
     a. Klicken Sie auf **Workload registrieren**.
     b. Melden Sie sich im geöffneten Browser-Fenster an der Cyber Protect-Konsole an und überprüfen Sie die Registrierungsdetails.
     c. Wählen Sie in der Liste **Für Konto registrieren** das Benutzerkonto, unter dem Sie den Workload registrieren wollen.
     d. Klicken Sie zuerst auf **Code überprüfen** und anschließend auf **Registrierung bestätigen**.
   - Wenn Sie sich mit dem Konto eines Partner-Administrator anmelden, müssen Sie die Workloads für Ihre Kunden registrieren:
     a. Klicken Sie auf **Workload registrieren**.
     b. Melden Sie sich im geöffneten Browser-Fenster an der Cyber Protect-Konsole an und überprüfen Sie die Registrierungsdetails.
     c. Wählen Sie in der Liste **Für Konto registrieren** das Benutzerkonto Ihres Kunden, unter dem Sie den Workload registrieren wollen.
     d. Klicken Sie zuerst auf **Code überprüfen** und anschließend auf **Registrierung bestätigen**.
   - Klicken Sie auf **Registrierungsinfo anzeigen**. Im Setup-Programm werden der Registrierungslink und Registrierungscode angezeigt. Wenn Sie die Workload-Registrierung auf der aktuellen Maschine nicht abschließen können, müssen Sie den Registrierungslink und den Registrierungscode kopieren und dann die Registrierungsschritte auf einer anderen Maschine durchführen. In diesem Fall müssen Sie den Registrierungscode in das Registrierungsformular eingeben. Der Registrierungscode ist für eine (1) Stunde gültig.
     Alternativ können Sie das Registrierungsformular auch aufrufen, wenn Sie zuerst auf **Alle Geräte** –> **Hinzufügen** klicken, dann nach unten bis zu **Registrierung per Code** scrollen und anschließend auf **Registrieren** klicken.

Hinweis
Beenden Sie das Setup-Programm nicht, bevor Sie die Registrierung bestätigt haben! Um die Registrierung erneut zu initiieren, müssen Sie das Setup-Programm neu starten. Wiederholen Sie anschließend die Installationsprozedur.

Dadurch wird der Workload dem Konto zugewiesen, welches zur Anmeldung an die Cyber Protect-Konsole verwendet wurde.

- Registrieren Sie den Workload manuell unter Verwendung der Befehlszeile. Weitere Informationen über die entsprechende Durchführung finden Sie im Abschnitt '"Workloads manuell registrieren und deregistrieren" (S. 130)'.

9. [Wenn der Agent für ein Konto registriert ist, dessen Mandant sich im Compliance-Modus befindet] Legen Sie das Verschlüsselungskennwort fest.

Protection Agenten in Linux installieren

Vorbereitung

- Laden Sie den Agenten herunter, den Sie auf der Maschine benötigen, die Sie schützen wollen. Siehe Abschnitt '"Protection Agenten herunterladen" (S. 81)'.
- Überprüfen Sie, dass die erforderlichen Linux-Pakete auf der Maschine installiert sind.
- Wenn Sie den Agenten unter SUSE Linux installieren, sollten Sie sicherstellen, dass Sie `su -` statt `sudo` verwenden. Anderenfalls kommt es zu folgendem Fehler, wenn Sie versuchen, den Agenten über die Cyber Protect-Konsole zu registrieren: `Der Webbrowser konnte nicht gestartet werden. Es ist keine Anzeige verfügbar.`

  Einige Linux-Distributionen (z.B. SUSE) übergeben die Variable DISPLAY nicht, wenn Sie sudo verwenden. Der Installer kann dann den Browser nicht in der grafischen Benutzeroberfläche (GUI) öffnen.graphical user interface (GUI).

Installation

Sie benötigen mindestens 2 GB freien Speicherplatz auf dem Laufwerk, um den Agenten für Linux installieren zu können.

So können Sie den Agenten für Linux installieren

1. Überprüfen Sie, dass die Maschine mit dem Internet verbunden ist.
2. Wechseln Sie als Root-Benutzer in das Verzeichnis mit der Installationsdatei, machen Sie die Datei ausführbar und starten Sie diese.

```
chmod +x <installation file name>
```

```
./<installation file name>
```

Falls in Ihrem Netzwerk ein Proxy-Server aktiviert ist, spezifizieren Sie beim Ausführen der Installationsdatei den Host-Namen/die IP-Adresse und den Port des Servers im folgenden Format: `--http-proxy-host=ADDRESS --http-proxy-port=PORT --http-proxy-login=LOGIN --http-proxy-password=PASSWORD`.

Wenn Sie die Standardmethode zur Registrierung der Maschine im Cyber Protection Service ändern wollen, starten Sie die Installationsdatei mit einem der folgenden Parameter:

- `--register-with-credentials` – um während der Installation nach einem Benutzernamen und Kennwort zu fragen
- `--token=STRING` – um ein Registrierungstoken zu verwenden
- `--skip-registration` – um die Registrierung zu überspringen

3. Aktivieren Sie die Kontrollkästchen derjenigen Agenten, die Sie installieren wollen. Folgende Agenten sind verfügbar:
   - Agent für Linux
   - Agent für Virtuozzo
   - Agent für Oracle
   - Agent für MySQL/MariaDB

   Der Agent für Virtuozzo, der Agent für Oracle und der Agent für MySQL/MariaDB erfordern, dass zusätzlich der Agent für Linux (64 Bit) installiert wird.
4. Wenn Sie die Standardregistrierungsmethode in Schritt 2 übernommen haben, können Sie mit dem nächsten Schritt fortfahren. Anderenfalls müssen Sie die Anmeldedaten (Benutzername, Kennwort) für den Cyber Protection Service eingeben oder darauf warten, bis die Maschine mithilfe des Tokens registriert wird.
5. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Wenn Sie sich mit dem Konto eines Firmenadministrators anmelden, müssen Sie Workloads für Ihr Unternehmen registrieren:
     a. Klicken Sie auf **Workload registrieren**.
     b. Melden Sie sich im geöffneten Browser-Fenster an der Cyber Protect-Konsole an und überprüfen Sie die Registrierungsdetails.
     c. Wählen Sie in der Liste **Für Konto registrieren** das Benutzerkonto, unter dem Sie den Workload registrieren wollen.
     d. Klicken Sie zuerst auf **Code überprüfen** und anschließend auf **Registrierung bestätigen**.
   - Wenn Sie sich mit dem Konto eines Partner-Administrator anmelden, müssen Sie die Workloads für Ihre Kunden registrieren:
     a. Klicken Sie auf **Workload registrieren**.
     b. Melden Sie sich im geöffneten Browser-Fenster an der Cyber Protect-Konsole an und überprüfen Sie die Registrierungsdetails.
     c. Wählen Sie in der Liste **Für Konto registrieren** das Benutzerkonto Ihres Kunden, unter dem Sie den Workload registrieren wollen.
     d. Klicken Sie zuerst auf **Code überprüfen** und anschließend auf **Registrierung bestätigen**.

- Klicken Sie auf **Registrierungsinfo anzeigen**. Im Setup-Programm werden der Registrierungslink und Registrierungscode angezeigt. Wenn Sie die Workload-Registrierung auf der aktuellen Maschine nicht abschließen können, müssen Sie den Registrierungslink und den Registrierungscode kopieren und dann die Registrierungsschritte auf einer anderen Maschine durchführen. In diesem Fall müssen Sie den Registrierungscode in das Registrierungsformular eingeben. Der Registrierungscode ist für eine (1) Stunde gültig.
  Alternativ können Sie das Registrierungsformular auch aufrufen, wenn Sie zuerst auf **Alle Geräte** –> **Hinzufügen** klicken, dann nach unten bis zu **Registrierung per Code** scrollen und anschließend auf **Registrieren** klicken.

  Hinweis
  Beenden Sie das Setup-Programm nicht, bevor Sie die Registrierung bestätigt haben! Um die Registrierung erneut zu initiieren, müssen Sie das Setup-Programm neu starten. Wiederholen Sie anschließend die Installationsprozedur.

  Dadurch wird der Workload dem Konto zugewiesen, welches zur Anmeldung an die Cyber Protect-Konsole verwendet wurde.
- Registrieren Sie den Workload manuell unter Verwendung der Befehlszeile. Weitere Informationen über die entsprechende Durchführung finden Sie im Abschnitt '"Workloads manuell registrieren und deregistrieren" (S. 130)'.

6. [Wenn der Agent für ein Konto registriert ist, dessen Mandant sich im Compliance-Modus befindet] Legen Sie das Verschlüsselungskennwort fest.
7. Wenn im UEFI-BIOS der Maschine die Secure Boot-Funktion (kurz 'UEFI Secure Boot') aktiviert ist, werden Sie darüber informiert, dass Sie das System nach der Installation neu starten müssen. Denken Sie daran, welches Kennwort (das des root-Benutzers oder 'acronis') verwendet werden soll.

   Hinweis
   Bei der Installation wird ein neuer Schlüssel generiert, der zum Signieren der Kernel-Module verwendet wird. Sie müssen diesen neuen Schlüssel in der sogenannten MOK-Liste (Machine Owner Key) registrieren, indem Sie die Maschine neu starten. Ohne die Registrierung des neuen Schlüssels wird Ihr Agent nicht funktionsfähig sein. Wenn Sie die UEFI Secure Boot-Funktion nach der Installation des Agenten aktivieren, müssen Sie den Agenten neu installieren.

8. Führen Sie einen der folgenden Schritte aus, nachdem die Installation abgeschlossen wurde:
   - Klicken Sie auf **Neustart**, wenn Sie im vorherigen Schritt aufgefordert wurden, das System neu zu booten.
     Wählen Sie während des Systemstarts die Option zur Verwaltung des MOK (Machine Owner Key), wählen Sie den (üblichweise englischen) Befehl **Enroll MOK** und registrieren Sie dann den Schlüssel mit dem im vorherigen Schritt empfohlenen Kennwort.
   - Anderenfalls können Sie auf **Beenden** klicken.

Troubleshooting-Informationen können Sie in folgender Datei finden:
`/usr/lib/Acronis/BackupAndRecovery/HOWTO.INSTALL`

Protection Agenten in macOS installieren

Voraussetzungen

Laden Sie den Agenten herunter, den Sie auf dem Workload benötigen, den Sie schützen wollen. Siehe Abschnitt '"Protection Agenten herunterladen" (S. 81)'.

So können Sie den Agenten für Mac (x64 oder ARM64) installieren

1. Überprüfen Sie, dass die Maschine mit dem Internet verbunden ist.
2. Klicken Sie doppelt auf die Installationsdatei (.dmg).
3. Warten Sie, bis das Betriebssystem das Disk-Image für die Installation geladen hat.
4. Klicken Sie doppelt auf **Installieren**.
5. Falls in Ihrem Netzwerk ein Proxy-Server verwendet wird, klicken Sie in der Menüleiste auf **Protection Agent**, dann auf **Proxy-Server-Einstellungen** und spezifizieren Sie anschließend den Host-Namen/die IP-Adresse, den Port und die Anmeldedaten des Proxy-Servers.
6. Geben Sie auf Nachfrage die Administrator-Anmeldedaten an.
7. Klicken Sie auf **Weiter**.
8. Warten Sie, bis die Registrierungsanzeige erscheint.
9. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Wenn Sie sich mit dem Konto eines Firmenadministrators anmelden, müssen Sie Workloads für Ihr Unternehmen registrieren:
     a. Klicken Sie auf **Workload registrieren**.
     b. Melden Sie sich im geöffneten Browser-Fenster an der Cyber Protect-Konsole an und überprüfen Sie die Registrierungsdetails.
     c. Wählen Sie in der Liste **Für Konto registrieren** das Benutzerkonto, unter dem Sie den Workload registrieren wollen.
     d. Klicken Sie zuerst auf **Code überprüfen** und anschließend auf **Registrierung bestätigen**.
   - Wenn Sie sich mit dem Konto eines Partner-Administrator anmelden, müssen Sie die Workloads für Ihre Kunden registrieren:
     a. Klicken Sie auf **Workload registrieren**.
     b. Melden Sie sich im geöffneten Browser-Fenster an der Cyber Protect-Konsole an und überprüfen Sie die Registrierungsdetails.
     c. Wählen Sie in der Liste **Für Konto registrieren** das Benutzerkonto Ihres Kunden, unter dem Sie den Workload registrieren wollen.
     d. Klicken Sie zuerst auf **Code überprüfen** und anschließend auf **Registrierung bestätigen**.
   - Klicken Sie auf **Registrierungsinfo anzeigen**. Im Setup-Programm werden der Registrierungslink und Registrierungscode angezeigt. Wenn Sie die Workload-Registrierung auf der aktuellen Maschine nicht abschließen können, müssen Sie den Registrierungslink und

den Registrierungscode kopieren und dann die Registrierungsschritte auf einer anderen Maschine durchführen. In diesem Fall müssen Sie den Registrierungscode in das Registrierungsformular eingeben. Der Registrierungscode ist für eine (1) Stunde gültig.

Alternativ können Sie das Registrierungsformular auch aufrufen, wenn Sie zuerst auf **Alle Geräte** –> **Hinzufügen** klicken, dann nach unten bis zu **Registrierung per Code** scrollen und anschließend auf **Registrieren** klicken.

Hinweis
Beenden Sie das Setup-Programm nicht, bevor Sie die Registrierung bestätigt haben! Um die Registrierung erneut zu initiieren, müssen Sie das Setup-Programm neu starten. Wiederholen Sie anschließend die Installationsprozedur.

Dadurch wird der Workload dem Konto zugewiesen, welches zur Anmeldung an die Cyber Protect-Konsole verwendet wurde.

- Registrieren Sie den Workload manuell unter Verwendung der Befehlszeile. Weitere Informationen über die entsprechende Durchführung finden Sie im Abschnitt '"Workloads manuell registrieren und deregistrieren" (S. 130)'.

10. [Wenn der Agent für ein Konto registriert ist, dessen Mandant sich im Compliance-Modus befindet] Legen Sie das Verschlüsselungskennwort fest.
11. Wenn Sie als macOS-Version Mojave 10.14.x oder höher einsetzen, müssen Sie dem Protection Agenten die Berechtigung 'Vollzugriff auf Festplatte' gewähren, damit Backup-Aktionen durchgeführt werden können.

    Anweisungen dazu finden Sie in folgendem Artikel: Die Berechtigung 'Vollzugriff auf Festplatte' für den Cyber Protection Agenten gewähren (64657).
12. Wenn Sie die Remote-Desktop-Funktionalität verwenden wollen, müssen Sie dem Connect Agenten die erforderlichen Systemberechtigungen erteilen. Weitere Informationen finden Sie im Abschnitt '"Dem Connect Agenten die erforderlichen Systemberechtigungen gewähren" (S. 88)'.

Dem Connect Agenten die erforderlichen Systemberechtigungen gewähren

Um alle Funktionen der Remote-Desktop-Funktionalität auf macOS Workloads aktivieren zu können, müssen Sie dem Connect Agenten zusätzlich zur Berechtigung 'Vollzugriff auf Festplatte' noch die folgenden Berechtigungen gewähren:

- Bildschirmaufnahme – ermöglicht Bildschirmaufnahmen vom macOS-Workload über NEAR. Ohne diese Berechtigung werden alle Remote-Steuerungsverbindungen verweigert.
- Bedienungshilfen – ermöglicht Remote-Verbindungen im Steuermodus über NEAR
- Mikrofon – ermöglicht die Sound-Ausgabe des macOS-Remote-Workloads an den lokalen Workload über NEAR umzuleiten. Um die Funktion zur Sound-Umleitung aktivieren zu können, muss auf dem Workload ein sogenannter Sound Capture-Treiber (Tonaufnahme-Treiber) installiert sein. Weitere Informationen finden Sie im Abschnitt '"Remote-Sound-Umleitung" (S.

1090)'.

- Automatisierung – ermöglicht es, die Aktion "Papierkorb leeren" durchführen zu können

Wenn Sie den Agenten auf dem macOS-Workload starten, wird überprüft, ob der Agent über diese Berechtigungen verfügt. Falls erforderlich, werden Sie aufgefordert, die benötigten Berechtigungen zu erteilen.

So können Sie die Berechtigung zur Bildschirmaufnahme gewähren

1. Klicken Sie im Dialog **Erforderliche Systemberechtigungen gewähren** für den Cyber Protect Agenten auf **Systemberechtigungen einrichten**.
2. Klicken Sie im Dialog **Systemberechtigungen** auf **Berechtigung 'Bildschirmaufnahme' anfordern**.
3. Klicken Sie auf **Systemeinstellungen öffnen**.
4. Wählen Sie **Connect Agent**.

Wenn Sie versuchen, remote auf einen Workload zuzugreifen, und der Agent die Berechtigung nicht hat, wird das entsprechende Dialogfenster (Berechtigung 'Bildschirmaufnahme' anfordern) angezeigt. Nur der lokale Benutzer kann auf den Dialog reagieren.

So können Sie die Berechtigung 'Bedienungshilfen' gewähren

1. Klicken Sie im Dialog **Erforderliche Systemberechtigungen gewähren** für den Cyber Protect Agenten auf **Systemberechtigungen einrichten**.
2. Klicken Sie im Dialog **Systemberechtigungen** auf **Berechtigung 'Bedienungshilfen' anfordern**.
3. Klicken Sie auf **Systemeinstellungen öffnen**.
4. Klicken Sie in der linken unteren Fensterecke auf das Schlosssymbol, damit dieses entsperrt wird. Das System wird Sie nach dem Administrator-Kennwort fragen, um die Änderungen vornehmen zu können.
5. Wählen Sie **Connect Agent**.

So können Sie die Berechtigung 'Mikrofon' gewähren

1. Klicken Sie im Dialog 'Dem Connect Agenten **die erforderliche Systemberechtigungen erteilen**' auf den Befehl **Systemberechtigungen einrichten**.
2. Klicken Sie im Dialog **Systemberechtigungen** auf **Berechtigung 'Mikrofon' anfordern**.
3. Klicken Sie auf **OK**.

Hinweis
Sie müssen auch einen entsprechenden Sound Capture-Treiber auf dem macOS-Workload installieren, damit der Agent die erteilte Berechtigung nutzen und die Tonausgabe des Workloads umleiten kann. Weitere Informationen finden Sie im Abschnitt '"Remote-Sound-Umleitung" (S. 1090)'.

So können Sie die Berechtigung 'Automatisierung' gewähren

1. Klicken Sie im Dialog 'Dem Connect Agenten **die erforderliche Systemberechtigungen erteilen**' auf den Befehl **Systemberechtigungen einrichten**.
2. Klicken Sie im Dialog **Systemberechtigungen** auf **Berechtigung 'Automatisierung' anfordern**.

Das Anmeldekonto auf Windows-Maschinen ändern

Definieren Sie über die Anzeige **Komponenten auswählen** das Konto, unter dem die Dienste ausgeführt werden sollen, indem Sie die Option **Anmeldekonto für den Agenten-Dienst** konfigurieren. Sie können eine der folgenden Optionen wählen:

- **Service User-Konten verwenden** (Standard für den Agenten-Dienst)

  Service User-Konten sind Windows-System-Konten, die verwendet werden, um Dienste auszuführen. Der Vorteil dieser Einstellung ist, dass die Domänen-Sicherheitsrichtlinien keinen Einfluss auf die Benutzerrechte dieser Konten haben. Standardmäßig wird der Agent unter dem Konto **Lokales System** ausgeführt.
- **Neues Konto erstellen**

  Der Kontoname für den Agenten lautet 'Agent User'.
- **Folgendes Konto verwenden**

  Wenn Sie den Agenten auf einem Domain Controller installieren, wird Sie das System auffordern, für den Agenten vorhandene Konten (oder dasselbe Konto) zu spezifizieren. Das System erstellt aus Sicherheitsgründen nicht automatisch neue Konten auf einem Domain Controller.

  Das Benutzerkonto, das Sie spezifizieren, wenn das Setup-Programm auf einem Domain Controller ausgeführt wird, muss die Berechtigung `Anmelden als Dienst` erhalten. Dieses Konto muss bereits auf dem Domain Controller verwendet worden sein, damit sein Profilordner auf dieser Maschine erstellt werden kann.

  Weitere Informationen zur Installation des Agenten auf einem schreibgeschützten Domain Controller (RODC, Read-only Domain Controller) finden Sie in diesem Knowledge Base-Artikel.

Wenn Sie die Option **Neues Konto erstellen** oder **Folgendes Konto verwenden** wählen, sollten Sie sicherstellen, dass die Domänen-Sicherheitsrichtlinien die Rechte der entsprechenden Konten nicht beeinträchtigen. Wenn einem Konto Benutzerrechte wieder entzogen werden, die diesem bei der Installation zugewiesen wurden, wird die Komponente möglicherweise fehlerhaft oder gar nicht funktioniert.

Für das Anmeldekonto erforderliche Berechtigungen

Ein Protection Agent wird auf einer Windows-Maschine als Managed Machine Service (MMS) ausgeführt. Das Konto, unter dem der Agent ausgeführt wird, muss spezifische Rechte haben, damit der Agent korrekt funktioniert. Daher sollten dem MMS-Benutzer folgende Berechtigungen zugewiesen werden:

1. Mitglied in der Benutzergruppe der **Sicherungs-Operatoren** und **Administratoren**. Auf einem Domain Controller muss der Benutzer Mitglied in der Gruppe der **Domänen-Admins** sein.

2. Dem Konto wird die Berechtigung **Vollzugriff** auf den Ordner `%PROGRAMDATA%\Acronis` (bei Windows XP und Server 2003 `%ALLUSERSPROFILE%\Application Data\Acronis`) und seine Unterordner gewährt.
3. Die Berechtigung **Vollzugriff** muss für bestimmte Registry-Schlüssel in folgendem Schlüssel gewährt sein: `HKEY_LOCAL_MACHINE\SOFTWARE\Acronis`.
4. Die folgenden Benutzerrechte müssen gewährt sein:
   - Als Dienst anmelden
   - Anpassen von Speicherkontingenten für einen Prozess
   - Ersetzen eines Tokens auf Prozessebene
   - Verändern der Firmwareumgebungsvariablen

So können Sie die Benutzerrechte zuweisen

Befolgen Sie die unteren Anweisungen, um die Benutzerrechte zuzuweisen (in diesem Beispiel wird das Benutzerrecht **Als Dienst anmelden** verwendet, die Schritte für die anderen Benutzerrechte sind aber gleich):

1. Melden Sie sich am Computer unter Verwendung eines Kontos mit administrative Berechtigungen an.
2. Öffnen Sie in der **Systemsteuerung** den Unterpunkt **Verwaltung** (oder verwenden Sie die Tastenkombination Win+R, geben Sie im erscheinenden Eingabefenster **control admintools** ein und bestätigen Sie mit der Eingabetaste) und öffnen Sie den Unterpunkt **Lokale Sicherheitsrichtlinie**.
3. Erweitern Sie den Unterpunkt **Lokale Richtlinien** und klicken Sie auf **Zuweisen von Benutzerrechten**.
4. Klicken Sie im rechten Fensterbereich mit der rechten Maustaste auf **Anmelden als Dienst** und wählen Sie den Befehl **Eigenschaften**.
5. Klicken Sie auf die Schaltfläche **Benutzer oder Gruppe hinzufügen...**, um einen neuen Benutzer hinzufügen zu können.
6. Suchen Sie im Fenster **Benutzer, Computer, Dienstkonten oder Gruppen auswählen** den Benutzer, den Sie eingeben wollen, und klicken Sie anschließend auf **OK**.
7. Klicken Sie im Fenster **Eigenschaften von Anmelden als Dienst** auf **OK**, damit die Änderungen gespeichert werden.

Wichtig
Stellen Sie sicher, dass der Benutzer, den Sie zur Benutzerrichtlinie **Anmelden als Dienst** hinzugefügt haben, nicht in der Richtlinie **Anmelden als Dienst verweigern** (ebenfalls im Bereich **Lokale Sicherheitsrichtlinien**) aufgelistet ist.

Beachten Sie, dass wir davon abraten, Anmeldekonten nach Abschluss der Installation noch mal manuell zu ändern.

Dynamische Installation und Deinstallation von Komponenten

Für Windows-Workloads, die durch die Agent-Version 15.0.26986 (im Mai 2021 veröffentlicht) oder höher geschützt werden, werden folgende Komponenten dynamisch installiert (jedoch nur, sofern ein Schutzplan dies erfordert):

- Agent für URL-Filterung – erforderlich zur Ausführung der URL-Filterungsfunktion.
- Der Agent für Antimalware Protection – ist für die Verwendung der Antimalware Protection-Funktionen erforderlich.
- Der Agent für Data Loss Prevention – ist für die Ausführung der Gerätekontrolle-Funktionen erforderlich.

Diese Komponenten werden nicht standardmäßig installiert. Die jeweilige Komponente wird dann automatisch installiert, wenn ein Workload durch einen Plan geschützt wird, in dem eines der folgenden Module aktiviert wurde:

- Antivirus & Antimalware Protection
- URL-Filterung
- Gerätekontrolle

Auf entsprechende Weise wird die jeweilige Komponente automatisch wieder deinstalliert, wenn kein Schutzplan mehr Funktionen der Antimalware Protection, URL-Filterung oder Gerätekontrolle benötigt.

Die dynamische Installation oder Deinstallation von Komponenten dauert bis zu 10 Minuten, wenn Sie den entsprechenden Schutzplan ändern. Wenn jedoch eine der nachfolgenden Aktionen ausgeführt wird, beginnt die dynamische Installation bzw. Deinstallation erst, nachdem die entsprechende Aktion abgeschlossen wurde:

- Backup
- Recovery
- Backup-Replikation
- Replikation von virtuellen Maschinen
- Ein Replikat testen
- Eine virtuelle Maschine aus einem Backup heraus ausführen (einschließlich Finalisierung)
- Disaster Recovery-Failover
- Disaster Recovery-Failback
- Ein Skript ausführen (für Cyber Scripting-Funktionalität)
- Patch-Installation
- ESXi-Konfigurations-Backup

Unbeaufsichtigte Installation oder Deinstallation

Unbeaufsichtigte Installation oder Deinstallation unter Windows

Unter Windows können Sie eine unbeaufsichtigte Installation bzw. Deinstallation auf folgende Arten durchführen:

- Indem Sie die EXE-Datei des Setup-Programms verwenden und die Installationsparameter über die Befehlszeile spezifizieren.
- Indem Sie eine MSI-Datei verwenden, die Sie aus dem Setup-Programm extrahieren, und die Installationsparameter auf eine der folgenden Arten spezifizieren:
  - In einer MST-Datei
  - Direkt über die Befehlszeile

Unbeaufsichtigte Installation und Deinstallation mit einer EXE-Datei

Für diese Art der unbeaufsichtigten Installation müssen Sie das Setup-Programm herunterladen und es dann über die Befehlszeile mit den erforderlichen Installationsparametern starten. Die Parameter, die Sie verwenden können, sind im Abschnitt '"Parameter für eine unbeaufsichtigte Installation (EXE)" (S. 95)' aufgeführt.

Sie müssen keine Installationspakete, MSI- oder MST-Dateien im Voraus extrahieren.

Agenten und Komponenten (EXE) installieren und deinstallieren

Wenn Sie eine unbeaufsichtigte Installation mit einer EXE-Datei durchführen wollen, führen Sie das Setup-Programm aus und spezifizieren Sie die Installationsparameter über die Befehlszeile.

Wenn Sie das Setup-Programm herunterladen wollen, müssen Sie in der rechten oberen Ecke der Cyber Protect-Konsole zuerst auf das Symbol 'Konto' klicken und anschließend auf **Downloads**. Der Download-Link ist auch im Fensterbereich **Geräte hinzufügen** verfügbar.

So können Sie Agenten und Komponenten installieren

1. Starten Sie die Befehlszeilenschnittstelle als Administrator und gehen Sie dann zur EXE-Datei des Setup-Programms.
2. Führen Sie folgenden Befehl aus, um das Setup-Programm starten und die Installationsparameter spezifizieren zu können:

   ```
   <file path>/<EXE file><PARAMETER 1>=<value 1> ... <PARAMETER N>=<value n>
   ```

   Verwenden Sie Leerzeichen, um die Parameter zu trennen, und Kommata ohne Leerzeichen, um die Werte für einen Parameter zu trennen. Beispiel:

   ```
   C:\Users\Administrator\Downloads\AgentForWindows_web.exe --add-
   components=agentForWindows,agentForSql,commandLine --install-dir="C:\Program
   ```

```
Files\BackupClient" --reg-address=https://eu2-cloud.company.com --reg-token=34F6-
8C39-4A5C --quiet
```

Weitere Informationen zu den verfügbaren Parametern und deren Werten finden Sie im Abschnitt '"Parameter für eine unbeaufsichtigte Installation (EXE)" (S. 95)'.

Beispiele

- Den Agenten für Windows, den Agenten für Antimalware, den Agenten für URL-Filterung, das Befehlszeilenwerkzeug und den Cyber Protect Monitor installieren. Den Workload im Cyber Protection Service unter Verwendung eines Benutzernamens und Kennworts registrieren.

```
C:\Users\Administrator\Downloads\AgentForWindows_web.exe --add-
components=agentForWindows,agentForAmp,commandLine,trayMonitor --install-
dir="C:\Program Files\BackupClient" --agent-account=system --reg-
address=https://cloud.company.com --reg-login=johndoe --reg-password=johnspassword
```

- Den Agenten für Windows, das Befehlszeilenwerkzeug und den Cyber Protect Monitor installieren. Ein neues Anmeldekonto für den Agenten-Dienst in Windows erstellen. Den Workload im Cyber Protection Service unter Verwendung eines Tokens registrieren.

```
C:\Users\Administrator\Downloads\AgentForWindows_web.exe --add-
components=agentForWindows,commandLine,trayMonitor --install-dir="C:\Program
Files\BackupClient" --agent-account=new --reg-address=https://eu2-cloud.company.com -
-reg-token=34F6-8C39-4A5C
```

- Den Agenten für Windows, das Befehlszeilenwerkzeug, den Agenten für Oracle und den Cyber Protect Monitor installieren. Die Maschine im Cyber Protection Service unter Verwendung eines Benutzernamens und Kennworts registrieren.

```
C:\Users\Administrator\Downloads\AgentForWindows_web.exe --add-
components=agentForWindows,commandLine,agentForOracle,trayMonitor --install-
dir="C:\Program Files\BackupClient" --language=en --agent-account=system --reg-
address=https://cloud.company.com --reg-login=johndoe --reg-password=johnspassword
```

- Den Agenten für Windows, das Befehlszeilenwerkzeug und den Cyber Protect Monitor installieren. Die Sprache der Benutzeroberfläche auf Deutsch festlegen. Die Maschine im Cyber Protection Service unter Verwendung eines Tokens registrieren. Einen HTTP-Proxy einrichten.

```
C:\Users\Administrator\Downloads\AgentForWindows_web.exe --add-
components=agentForWindows,commandLine,agentForOracle,trayMonitor --install-
dir="C:\Program Files\BackupClient"--language=de --agent-account=system --reg-
address=https://eu2-cloud.company.com --reg-token=34F6-8C39-4A5C --http-proxy-
address=https://my-proxy.company.com:80 --http-proxy-login=tomsmith --http-proxy-
password=tomspassword
```

So können Sie eine installierte Komponente entfernen

1. Führen Sie die Befehlszeilenschnittstelle als Administrator aus und gehen Sie dann zum Verzeichnis `%ProgramFiles%\BackupClient\RemoteInstall`.
2. Führen Sie folgenden Befehl aus:

   ```
   web_installer.exe --remove-components=<value 1>,<value 2> --quiet
   ```

   Weitere Informationen zu den verfügbaren Parametern und deren Werten finden Sie im Abschnitt '"Parameter für eine unbeaufsichtigte Installation (EXE)" (S. 95)'.

Beispiel

- Den Cyber Protect Monitor deinstallieren

  ```
  C:\Program Files\BackupClient\RemoteInstall\web_installer.exe --remove-components=trayMonitor --quiet
  ```

So können Sie einen Agenten deinstallieren

1. Führen Sie die Befehlszeilenschnittstelle als Administrator aus und gehen Sie dann zum Verzeichnis `%Program Files%\Common Files\Acronis\BackupAndRecovery`.
2. Führen Sie folgenden Befehl aus:

   ```
   Uninstaller.exe --quiet --delete-all-settings
   ```

   Weitere Informationen zu den verfügbaren Parametern und deren Werten finden Sie im Abschnitt '"Parameter für eine unbeaufsichtigte Installation (EXE)" (S. 95)'.

Beispiele

- Den Agenten für Windows und all seine Komponenten deinstallieren. Alle Protokolle, Tasks und Konfigurationseinstellungen löschen.

  ```
  C:\Program Files\Common Files\Acronis\BackupAndRecovery\Uninstaller.exe --quiet --delete-all-settings
  ```

- Einen kennwortgeschützten Agenten für Windows und all seine Komponenten deinstallieren. Alle Protokolle, Tasks und Konfigurationseinstellungen löschen.

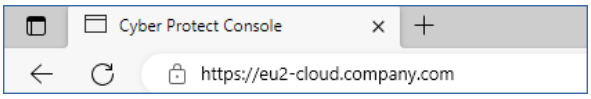
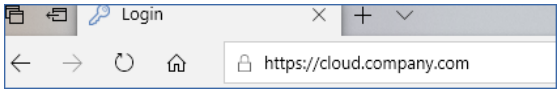
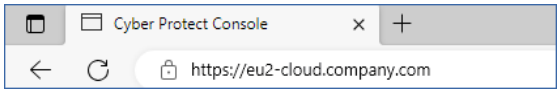
  ```
  C:\Program Files\Common Files\Acronis\BackupAndRecovery\Uninstaller.exe --anti-tamper-password=<password> --quiet --delete-all-settings
  ```

Parameter für eine unbeaufsichtigte Installation (EXE)

In der nachfolgenden Tabelle werden die Parameter für eine unbeaufsichtigte Installation mit einer EXE-Datei zusammengefasst.

Parameter	Beschreibung
Allgemeine Parameter	
`--add-components=`<Komponente1,Komponente2,...,KomponenteN>	Die Komponenten, die installiert werden sollen. Die vollständige Liste der verfügbaren Komponenten finden Sie im Abschnitt '"Komponenten für eine unbeaufsichtigte Installation (EXE)" (S. 101)'. Wenn Sie mehrere Komponenten spezifizieren, müssen Sie diese per Kommata trennen. Fügen Sie keine Leerzeichen vor oder nach einem Komma ein. Wenn Sie bereits installierte Komponenten spezifizieren, werden diese Komponenten je nach Version des Setup-Programms und der Version der installierten Komponenten repariert oder aktualisiert. Wenn Sie diesen Parameter nicht spezifizieren, wird je nach Maschine, auf der Sie die Installation durchführen, ein Standardsatz von Komponenten installiert. Der Agent für SQL wird beispielsweise nur auf Maschinen installiert, auf denen der MS SQL Server läuft.
`--install-dir=`<Pfad>	Der Ordner, in dem die ausgewählten Komponenten installiert werden sollen. Falls der spezifizierte Ordner nicht existiert, wird er automatisch erstellt. Wenn Sie diesen Parameter nicht spezifizieren, wird ein vorgegebener Ordner verwendet: `C:\Programme\BackupClient`.
`--log-dir=`<Pfad>	Der Ordner, in dem die Installationsprotokolle (Log-Dateien) gespeichert werden sollen. Wenn Sie diesen Parameter nicht spezifizieren, wird ein vorgegebener Ordner verwendet: `%ProgramData%\Acronis\InstallationLogs`.
`--language=`<Code>	Die Sprache für das Produkt. Folgende Werte sind verfügbar: en, bn, bg, cs, da, de, es, fr, ko, id, it, hi, hu, ms, nl, ja, nb, pl, pt, pt_BR, ru, fi, sr, sv, th, tr, vi, zh, zh_TW. Wenn Sie diesen Parameter nicht spezifizieren und die Systemsprache der Maschine, auf der Sie die Installation durchführen wollen, eine der oben aufgeführten ist, wird die jeweilige Systemsprache verwendet. In allen anderen Fällen wird der Wert

Parameter	Beschreibung
	auf en festgelegt.
`--quiet`	Verwenden Sie diesen Parameter, um das Setup-Programm auszuführen, ohne dass die grafische Benutzeroberfläche angezeigt wird. Verwenden Sie ihn nicht zusammen mit dem Parameter `--register-only`.
`--help`	Verwenden Sie diesen Parameter, damit Ihnen eine Liste aller verfügbaren Parameter, die Sie in der Befehlszeile verwenden können, sowie eine Beschreibung zu diesen angezeigt wird.
`--fss-onboarding-auto-start`	Verwenden Sie diesen Parameter zusammen mit dem Parameter `--quiet`, damit nach einer unbeaufsichtigten Installation der File Sync & Share Onboarding-Assistent angezeigt wird.
Registrierungsparameter	
`--registration=`{skip | by-credentials | by-token | device-flow}	Verwenden Sie diesen Parameter, um festzulegen, wie der Agent nach der Installation registriert werden soll. Wenn Sie die Registrierung überspringen wollen, spezifizieren Sie `skip`. Sie können den Agenten später registrieren, indem Sie den Parameter `--register-only` verwenden. Wenn Sie den Agenten mit Anmeldedaten registrieren wollen, müssen Sie den Parameter `by-credentials` spezifizieren und dann die Parameter `--reg-login` und `--reg-password` verwenden. Außerdem können Sie nur die Parameter `--reg-login` und `--reg-password` verwenden, was die Angabe von `--registration=by-credentials` optional macht. Wenn Sie den Agenten mit einem Registrierungstoken registrieren wollen, müssen Sie den Parameter `by-token` spezifizieren und dann den Parameter `--reg-token` verwenden. Außerdem können Sie nur den Parameter `--reg-token` verwenden, was die Angabe von `--registration=by-token` optional macht. Wenn Sie den Agenten über das OAuth 2.0-Protokoll registrieren wollen, müssen Sie `device-flow`

Parameter	Beschreibung
	spezifizieren. Wenn die Installation abgeschlossen ist, wird automatisch die Registrierungsseite geöffnet. Wenn Sie `--registration=device-flow` verwenden, müssen Sie die genaue Datacenter-Adresse als Wert für den Parameter `--reg-address` spezifizieren. Dies ist die URL, die Sie sehen, sobald Sie sich am Cyber Protection Service **angemeldet haben**. Beispielsweise `https://eu2-cloud.company.com`.  Sie dürfen `--registration=device-flow` nicht zusammen mit dem Parameter `--quiet` verwenden.
`--reg-address=`<URL>	Die URL des Cyber Protection Service. Sie können diesen Parameter entweder mit den Parametern `--reg-login` und `--reg-password` oder mit dem Parameter `--reg-token` verwenden. • Wenn Sie ihn mit den Parametern `--reg-login` und `--reg-password` verwenden, müssen Sie die Adresse spezifizieren, die Sie verwenden, um sich am Cyber Protection Service **anzumelden**. Beispielsweise `https://cloud.company.com`:  • Wenn Sie ihn mit dem Parameter `--reg-token` verwenden, müssen Sie die genaue Datacenter-Adresse spezifizieren. Dies ist die URL, die Sie sehen, sobald Sie sich am Cyber Protection Service **angemeldet haben**. Beispielsweise `https://eu2-cloud.company.com`.  Sie dürfen `https://cloud.company.com` nicht mit dem Parameter `--reg-token` verwenden.
`--reg-login=`<Anmeldename> `--reg-password=`<Kennwort>	Die Anmeldedaten für das Konto, unter dem der Agent im Cyber Protection Service registriert wird. Dies darf kein Partner-Administrator-Konto sein. Wenn Sie diese Parameter verwenden, ist die Spezifikation des Parameters `--registration` optional.

Parameter	Beschreibung
	Verwenden Sie diese Parameter nicht zusammen mit dem Parameter `--reg-token`.
`--reg-token=`<Token>	Das Registrierungstoken. Das Registrierungstoken ist eine Folge von 12 Zeichen, die durch Bindestriche in 3 Segmente separiert sind. Weitere Informationen darüber, wie man ein Token generiert, finden Sie im Abschnitt '"Ein Registrierungstoken generieren" (S. 182)'. Wenn Sie diesen Parameter verwenden, ist die Spezifikation des Parameters `--registration` optional. Verwenden Sie diesen Parameter nicht mit den Parametern `--reg-login` und `--reg-password`.
`--register-only`	Verwenden Sie diesen Parameter, um die Installation zu überspringen und den Agenten über das OAuth 2.0-Protokoll (device-flow) zu registrieren. Wenn die Installation abgeschlossen ist, wird automatisch die Registrierungsseite geöffnet. Sie dürfen `--register-only` nicht zusammen mit dem Parameter `--quiet` verwenden.
Anmeldekonto für den Agenten-Dienst	
`--agent-account=`{system | new | custom} oder `--agent-account-login=`<Anmeldename> `--agent-account-password=`<Kennwort>	Verwenden Sie diesen Parameter, um das Anmeldekonto zu spezifizieren, unter dem der Dienst des Agenten ausgeführt wird. Weitere Informationen über Anmeldekonten Sie im Abschnitt '"Das Anmeldekonto auf Windows-Maschinen ändern" (S. 90)'. Wenn Sie das **Lokales System**-Konto verwenden wollen, müssen Sie `--agent-account=system` spezifizieren – oder den Parameter `--agent-account` in Ihrem Befehl weglassen. Wenn Sie den Dienst des Agenten unter einem neuen Anmeldekonto, nämlich **Acronis Agent User**, das automatisch erstellt wird, ausführen wollen, müssen Sie `new` spezifizieren. Wenn Sie den Dienst des Agenten unter einem vorhandenen Konto ausführen wollen, müssen Sie die Konto-Anmeldedaten über die Parameter `--`

Parameter	Beschreibung
	`agent-account-login` und `--agent-account-password` spezifizieren. In diesem Fall ist die Spezifikation des Parameters `--agent-account=custom` optional.
vCenter/ESXi-Parameter	
`--esxi-address=`<Host>	Der Host-Name oder die IP-Adresse des vCenter Servers oder ESXi-Hosts. Verwenden Sie diesen Parameter, wenn Sie den Agent für VMware installieren.
`--esxi-login=`<Anmeldename> `--esxi-password=`<Kennwort>	Die Anmeldedaten, um auf den vCenter Server oder ESXi-Host zugreifen zu können. Verwenden Sie diese Parameter, wenn Sie den Agent für VMware installieren.
Proxy-Parameter	
`--http-proxy=`{none | system | custom}	Verwenden Sie diesen Parameter, um den HTTP-Proxy-Server zu spezifizieren, den Sie für Backups zum und für Wiederherstellungen aus dem Cloud Storage verwenden wollen. Wenn Sie die Proxy-Server-Verbindungen deaktivieren wollen, spezifizieren Sie `--http-proxy=none`. Wenn Sie einen systemweiten Proxy-Server verwenden wollen, müssen Sie `--http-proxy=system` spezifizieren oder den Parameter `--http-proxy` in Ihrem Befehl weglassen. Wenn Sie einen anderen Proxy-Server verwenden wollen, müssen Sie die Adresse des Proxy-Servers und dessen Anmeldedaten über die Parameter `--http-proxy-address`, `--http-proxy-login` und `--http-proxy-password` spezifizieren. In diesem Fall ist die Spezifikation des Parameters `--http-proxy=custom` optional.
`--http-proxy-address=`<Host>:<Port>	Der Host-Name oder die IP-Adresse sowie der Port des benutzerdefinierten HTTP-Proxy-Servers.
`--http-proxy-login=`<Anmeldename>	Anmeldename für den benutzerdefinierten HTTP-Proxy-Server.
`--http-proxy-password=`<Kennwort>	Das Kennwort für den benutzerdefinierten HTTP-Proxy-Server.

Parameter	Beschreibung
Deinstallationsparameter	
`--remove-components=` <Komponente1,Komponente2,...,KomponenteN>	Die Komponenten, die deinstalliert werden sollen. Die vollständige Liste der verfügbaren Komponenten finden Sie im Abschnitt '"Komponenten für eine unbeaufsichtigte Installation (EXE)" (S. 101)'. Wenn Sie mehrere Komponenten spezifizieren, müssen Sie diese per Kommata trennen. Fügen Sie keine Leerzeichen vor oder nach einem Komma ein. **Wichtig** Mit diesem Parameter können Sie nur Komponenten deinstallieren. Wenn Sie das Produkt vollständig deinstallieren wollen, gehen Sie in Windows zu 'Systemsteuerung' –> 'Programme und Features', wählen Sie das Produkt aus und klicken Sie dann auf den Befehl **Deinstallieren**.
`--delete-all-settings`	Verwenden Sie diesen optionalen Parameter, wenn Sie den Parameter `--remove-components` verwenden, um alle Produktprotokolle, Tasks und Konfigurationseinstellungen zu löschen.
`--anti-tamper-password=`<Kennwort>	Das Kennwort, das zur Deinstallation eines kennwortgeschützten Agenten für Windows oder zur Änderung seiner Komponenten erforderlich ist.

Komponenten für eine unbeaufsichtigte Installation (EXE)

In der nachfolgenden Tabelle werden die Komponenten zusammengefasst, die Sie für eine unbeaufsichtigte Installation über eine EXE-Datei verwenden können. Verwenden Sie die Wertnamen, um die Werte für den Parameter `--add-components` zu spezifizieren.

Weitere Informationen finden Sie im Abschnitt '"Parameter für eine unbeaufsichtigte Installation (EXE)" (S. 95)"Parameter für eine unbeaufsichtigte Installation (MSI)" (S. 106)'

Wertname	Komponenten-Beschreibung
`agentForWindows`	Agent für Windows
`agentForSas`	Agent für Files Sync & Share
`agentForAd`	Agent für Active Directory
`agentForAmp`	Agent für Antimalware Protection und Agent für URL-Filterung

Wertname	Komponenten-Beschreibung
agentForDlp	Agent für Data Loss Prevention
agentForEsx	Agent für VMware (Windows)
agentForExchange	Agent für Exchange
agentForHyperV	Agent für Hyper-V
agentForOffice365	Agent für Office 365
agentForOracle	Agent für Oracle
agentForSql	Agent für SQL
commandLine	Befehlszeilenwerkzeug
mediaBuilder	Bootable Media Builder
trayMonitor	Cyber Protect Monitor
all	Diese Gruppe kombiniert alle Komponenten.
allAgents	Diese Gruppe kombiniert alle Agenten.

Unbeaufsichtigte Installation und Deinstallation mit einer MSI-Datei

Verwenden Sie für diese Art der unbeaufsichtigten Installation den Windows-Installer (das `Msiexec`-Programm). Extrahieren Sie die Installationspakete und die MSI-Datei im Voraus über die grafische Benutzeroberfläche des Setup-Programms.

Wenn Sie Komponenten mit einer MSI-Datei installieren, können Sie eine MST-Transformationsdatei verwenden, um die Installationsparameter anzupassen. Weitere Informationen darüber, wie Sie die Kombination von MSI- und MST-Dateien verwenden können, finden Sie im Abschnitt '"Agenten und Komponenten installieren (MSI- und MST-Kombination)" (S. 103)'. Sie können diese Installationsmethode in einer Active Directory-Domain verwenden, um Protection Agenten mithilfe einer Windows-Gruppenrichtlinie zu installieren. Weitere Informationen finden Sie im Abschnitt '"Agenten per Gruppenrichtlinie bereitstellen" (S. 182)'.

Alternativ können Sie die Installationsparameter auch manuell über die Befehlszeile spezifizieren. In diesem Fall brauchen Sie keine MST-Datei. Weitere Informationen finden Sie im Abschnitt '"Beispiele" (S. 104)'.

Die MSI-, MST- und CAB-Dateien extrahieren

Extrahieren Sie die MSI-, MST- und CAB-Dateien mit den Installationspaketen, indem Sie das Setup-Programm über dessen grafische Benutzeroberfläche ausführen.

So können Sie die MSI-, MST- und CAB-Dateien extrahieren

1. Starten Sie die grafische Benutzeroberfläche des Setup-Programms und klicken Sie dann auf den Befehl **.mst- und .msi-Dateien für eine unbeaufsichtigte Installation erstellen**.
2. Wählen Sie bei **Zu installierende Komponenten** diejenigen Komponenten, die Sie aufspielen wollen, und klicken Sie dann auf **Fertig**.

   Die Installationspakete für diese Komponenten werden vom Setup-Programm als CAB-Dateien extrahiert.
3. Wählen Sie bei den **Registrierungseinstellungen** den Befehl **Anmeldedaten verwenden** oder **Registrierungstoken verwenden**. Spezifizieren Sie je nach Ihrer Wahl die Anmeldedaten oder das Registrierungstoken und klicken Sie dann auf **Fertig**.

   Weitere Informationen über die Generierung eines Registrierungstokens finden Sie im Abschnitt '"Ein Registrierungstoken generieren" (S. 182)'.
4. [Nur, wenn Sie eine Installation auf einem Domain Controller durchführen] Wählen Sie bei **Anmeldekonto für den Agenten-Dienst** die Option **Folgendes Konto verwenden**. Spezifizieren Sie das Benutzerkonto, unter dem der Agenten-Dienst ausgeführt werden soll, und klicken Sie dann auf **Fertig**. Das Setup-Programm erstellt aus Sicherheitsgründen nicht automatisch neue Konten auf einem Domain Controller.

   Hinweis
   Das von Ihnen spezifizierte Benutzerkonto muss die Berechtigung `Anmelden als Dienst` erhalten. Dieses Konto muss bereits auf dem Domain Controller verwendet worden sein, damit sein Profilordner auf dieser Maschine erstellt werden kann.

   Weitere Informationen zur Installation des Agenten auf einem schreibgeschützten Domain Controller (RODC, Read-only Domain Controller) finden Sie in diesem Knowledge Base-Artikel.
5. Überprüfen oder ändern Sie andere Installationseinstellungen, die der MST-Datei hinzugefügt werden, und klicken Sie dann auf **Fortsetzen**.
6. Bestimmen Sie den Ordner, in dem die MSI-, MST- und CAB-Dateien extrahiert werden sollen, und klicken Sie dann auf den Befehl **Generieren**.

Agenten und Komponenten installieren (MSI- und MST-Kombination)

Verwenden Sie die MST-Datei, um die Installationseinstellungen für die MSI-Datei anzupassen. Verwenden Sie die MSI- und MST-Kombination, wenn Sie Agenten auf mehreren Maschinen per Windows-Gruppenrichtlinie installieren. Weitere Informationen finden Sie im Abschnitt '"Agenten per Gruppenrichtlinie bereitstellen" (S. 182)'.

So können Sie Komponenten mit MSI- und MST-Dateien installieren

1. Extrahieren Sie die MSI- und MST-Dateien (wie im Abschnitt '"Die MSI-, MST- und CAB-Dateien extrahieren" (S. 102)' beschrieben).
2. Führen Sie über die Befehlszeilenschnittstelle der Maschine, auf der Sie Komponenten installieren wollen, folgenden Befehl aus:

```
msiexec /i <MSI file> TRANSFORMS=<MST file>
```

Beispiel:

```
msiexec /i BackupClient64.msi TRANSFORMS=BackupClient64.msi.mst
```

Agenten und Komponenten installieren und deinstallieren (MSI und Direktauswahl)

Starten Sie die MSI-Datei, wählen Sie die zu installierenden Komponenten manuell aus und spezifizieren Sie deren Installationsparameter über die Befehlszeile. In diesem Fall brauchen Sie keine MST-Datei.

So können Sie Agenten und Komponenten installieren

1. Extrahieren Sie die MSI-Datei und die Installationspakete (CAB-Dateien) wie im Abschnitt '"Die MSI-, MST- und CAB-Dateien extrahieren" (S. 102)' beschrieben.
   Für diese Installationsmethode benötigen Sie nur die MSI- und CAB-Dateien. Sie benötigen keine MST-Datei.
2. Führen Sie folgenden Befehl über die Befehlszeilenschnittstelle der Maschine aus:

   ```
   msiexec /i <MSI file><PARAMETER 1>=<value 1> ... <PARAMETER N>=<value n>
   ```

   Verwenden Sie Leerzeichen, um die Parameter zu trennen, und Kommata ohne Leerzeichen, um die Werte für einen Parameter zu trennen. Beispiel:

   ```
   msiexec.exe /i BackupClient64.msi
   ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,CommandLineTool,TrayMonitor
   TARGETDIR="C:\Program Files\BackupClient" REGISTRATION_ADDRESS=https://eu2-
   cloud.company.com REGISTRATION_TOKEN=34F6-8C39-4A5C
   ```

   Weitere Informationen zu den verfügbaren Parametern und deren Werten finden Sie im Abschnitt '"Parameter für eine unbeaufsichtigte Installation (MSI)" (S. 106)'.

Beispiele

- Den Agenten für Windows, den Agenten für Antimalware, den Agenten für URL-Filterung, das Befehlszeilenwerkzeug und den Cyber Protect Monitor installieren. Den Workload im Cyber Protection Service unter Verwendung eines Benutzernamens und Kennworts registrieren.

  ```
  msiexec.exe /i BackupClient64.msi /l*v my_log.txt /qn
  ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,AmpAgentFeature,CommandLineTool,Tray
  Monitor TARGETDIR="C:\Program Files\BackupClient" REBOOT=ReallySuppress MMS_USE_
  SYSTEM_ACCOUNT=1 REGISTRATION_ADDRESS=https://cloud.company.com REGISTRATION_
  LOGIN=johndoe REGISTRATION_PASSWORD=johnspassword
  ```

- Den Agenten für Windows, das Befehlszeilenwerkzeug und den Cyber Protect Monitor installieren. Ein neues Anmeldekonto für den Agenten-Dienst in Windows erstellen. Den Workload im Cyber Protection Service unter Verwendung eines Tokens registrieren.

```
msiexec.exe /i BackupClient64.msi /l*v my_log.txt /qn
ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,CommandLineTool,TrayMonitor
TARGETDIR="C:\Program Files\BackupClient" REBOOT=ReallySuppress MMS_CREATE_NEW_
ACCOUNT=1 REGISTRATION_ADDRESS=https://eu2-cloud.company.com REGISTRATION_TOKEN=34F6-
8C39-4A5C
```

- Den Agenten für Windows, das Befehlszeilenwerkzeug, den Agenten für Oracle und den Cyber Protect Monitor installieren. Die Maschine im Cyber Protection Service unter Verwendung eines Benutzernamens und eines Base64-codierten Kennworts registrieren. Möglicherweise müssen Sie Ihr Kennwort codieren, wenn es Sonderzeichen oder Leerzeichen enthält. Weitere Informationen über das Codieren eines Kennworts finden Sie im Abschnitt '"Kennwörter mit Sonderzeichen oder Leerzeichen" (S. 134)'.

  ```
  msiexec.exe /i BackupClient64.msi /l*v my_log.txt /qn
  ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,CommandLineTool,OracleAgentFeature,T
  rayMonitor TARGETDIR="C:\Program Files\BackupClient" REBOOT=ReallySuppress CURRENT_
  LANGUAGE=en MMS_USE_SYSTEM_ACCOUNT=1 REGISTRATION_ADDRESS=https://cloud.company.com
  REGISTRATION_LOGIN=johndoe REGISTRATION_PASSWORD_ENCODED=am9obnNwYXNzd29yZA==
  ```

- Den Agenten für Windows, das Befehlszeilenwerkzeug und den Cyber Protect Monitor installieren. Die Maschine im Cyber Protection Service unter Verwendung eines Tokens registrieren. Einen HTTP-Proxy einrichten.

  ```
  msiexec.exe /i BackupClient64.msi /l*v my_log.txt /qn
  ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,CommandLineTool,TrayMonitor
  TARGETDIR="C:\Program Files\BackupClient" REBOOT=ReallySuppress CURRENT_LANGUAGE=en
  MMS_USE_SYSTEM_ACCOUNT=1 REGISTRATION_ADDRESS=https://eu2-cloud.company.com
  REGISTRATION_TOKEN=34F6-8C39-4A5C HTTP_PROXY_ADDRESS=https://my-proxy.company.com
  HTTP_PROXY_PORT=80 HTTP_PROXY_LOGIN=tomsmith HTTP_PROXY_PASSWORD=tomspassword
  ```

So können Sie eine installierte Komponente entfernen

1. Extrahieren Sie die MSI-Datei und die Installationspakete (CAB-Dateien) wie im Abschnitt '"Die MSI-, MST- und CAB-Dateien extrahieren" (S. 102)' beschrieben.

   Für diese Installationsmethode benötigen Sie nur die MSI- und CAB-Dateien. Sie benötigen keine MST-Datei.
2. Führen Sie folgenden Befehl über die Befehlszeilenschnittstelle der Maschine aus:

   ```
   msiexec /i <MSI file><REMOVE>=<value 1>,<value 2> REBOOT=ReallySuppress /qn
   ```

   Weitere Informationen zu den verfügbaren Parametern und deren Werten finden Sie im Abschnitt '"Parameter für eine unbeaufsichtigte Installation (MSI)" (S. 106)'.

Beispiel

- Den Cyber Protect entfernen.

```
msiexec.exe /i BackupClient64.msi /l*v uninstall_log.txt REMOVE=TrayMonitor
REBOOT=ReallySuppress /qn
```

So können Sie einen Agenten deinstallieren

1. Extrahieren Sie die MSI-Datei und die Installationspakete (CAB-Dateien) wie im Abschnitt '"Die MSI-, MST- und CAB-Dateien extrahieren" (S. 102)' beschrieben.

   Für diese Installationsmethode benötigen Sie nur die MSI- und CAB-Dateien. Sie benötigen keine MST-Datei.
2. Führen Sie folgenden Befehl über die Befehlszeilenschnittstelle der Maschine aus:

   ```
   msiexec /x <MSI file> /l*v uninstall_log.txt DELETE_ALL_SETTINGS=1
   REBOOT=ReallySuppress /qn
   ```

   Weitere Informationen zu den verfügbaren Parametern und deren Werten finden Sie im Abschnitt '"Parameter für eine unbeaufsichtigte Installation (MSI)" (S. 106)'.

Beispiele

- Den Agenten für Windows und all seine Komponenten deinstallieren. Alle Protokolle, Tasks und Konfigurationseinstellungen löschen.

```
msiexec.exe /x BackupClient64.msi /l*v uninstall_log.txt DELETE_ALL_SETTINGS=1
REBOOT=ReallySuppress /qn
```

- Einen kennwortgeschützten Agenten für Windows und all seine Komponenten deinstallieren. Alle Protokolle, Tasks und Konfigurationseinstellungen löschen.

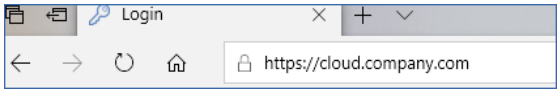
```
msiexec.exe /x BackupClient64.msi /l*v uninstall_log.txt ANTI_TAMPER_
PASSWORD=<password> DELETE_ALL_SETTINGS=1 REBOOT=ReallySuppress /qn
```

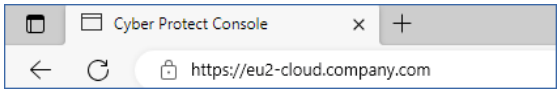
Parameter für eine unbeaufsichtigte Installation (MSI)

In der nachfolgenden Tabelle werden die Parameter für eine unbeaufsichtigte Installation zusammengefasst, wenn Sie eine MSI-Datei verwenden.

Sie können außerdem zusätzliche `msiexec`-Parameter verwenden. Sie können beispielsweise den Parameter `/qn` verwenden, um zu verhindern, dass irgendwelche GUI-Elemente angezeigt werden. Weitere Informationen zu den `msiexec`-Parametern finden Sie in der entsprechenden Microsoft-Dokumentation.

Parameter	Beschreibung
Allgemeine Parameter	
ADDLOCAL= <Komponente1,Komponente2,...,KomponenteN>	Die Komponenten, die installiert werden sollen. Die vollständige Liste der verfügbaren Komponenten finden Sie im Abschnitt '"Komponenten für eine unbeaufsichtigte Installation (MSI)" (S. 111)'. Wenn Sie mehrere Komponenten spezifizieren, müssen Sie diese per Kommata trennen. Fügen Sie keine Leerzeichen vor oder nach einem Komma ein. **Hinweis** Sie müssen die Installationsdateien für alle Komponenten, die Sie installieren wollen, extrahieren. Weitere Informationen darüber, wie Sie diese extrahieren können, finden Sie im Abschnitt '"Die MSI-, MST- und CAB-Dateien extrahieren" (S. 102)'.
TARGETDIR=<Pfad>	Der Ordner, in dem die ausgewählten Komponenten installiert werden sollen. Falls der spezifizierte Ordner nicht existiert, wird er automatisch erstellt. Wenn Sie diesen Parameter nicht spezifizieren, wird ein vorgegebener Ordner verwendet: C:\Programme\BackupClient.
REBOOT=ReallySuppress	Spezifizieren Sie diesen Parameter, wenn Sie Komponenten installieren wollen, ohne dass die Maschine neu gestartet werden muss.
/l*v <Protokolldatei>	Spezifizieren Sie diesen Parameter, um ein ausführliches Protokoll zu speichern. Dieses Protokoll ist erforderlich, wenn Sie Installationsprobleme untersuchen müssen.
CURRENT_LANGUAGE=<Sprach-ID>	Die Sprache für das Produkt. Folgende Werte sind verfügbar: en, bn, bg, cs, da, de, es, fr, ko, id, it, hi, hu, ms, nl, ja, nb, pl, pt, pt_BR, ru, fi, sr, sv, th, tr, vi, zh, zh_TW. Wenn Sie diesen Parameter nicht spezifizieren und die Systemsprache der Maschine, auf der Sie die Installation durchführen wollen, eine der oben aufgeführten ist, wird die jeweilige Systemsprache verwendet. In allen anderen Fällen wird der Wert auf en festgelegt.

Parameter	Beschreibung
SKIP_SHA2_KB_CHECK={0,1}	Verwenden Sie diesen Parameter, um festzulegen, ob geprüft werden soll, ob das Update zur Unterstützung der SHA2-Codesignierung von Microsoft (KB4474419) auf der Maschine installiert ist. Die Überprüfung läuft nur auf Betriebssystemen, die dieses Update benötigen. Informationen darüber, ob es für Ihr Betriebssystem erforderlich ist, finden Sie unter '"Unterstützte Betriebssysteme und Umgebungen" (S. 25)'. Verwenden Sie diesen Parameter mit einem auf 1 festgelegten Wert, wenn Sie die Überprüfung überspringen wollen. Wenn Sie den Parameter nicht spezifizieren oder seinen Wert mit 0 festlegen und das Update zur Unterstützung der SHA2-Codesignierung auf der Maschine nicht gefunden wird, wird die Installation fehlschlagen.
FSS_ONBOARDING_AUTO_START={0,1}	Verwenden Sie diesen Parameter zusammen mit einem auf 1 festgelegten Wert, damit nach einer unbeaufsichtigten Installation der File Sync & Share Onboarding-Assistent angezeigt wird. Wenn Sie diesen Parameter nicht spezifizieren oder dessen Wert auf 0 festgelegt ist, wird der Onboarding-Assistent nicht angezeigt.
Registrierungsparameter	
REGISTRATION_ADDRESS	Die URL des Cyber Protection Service. Sie können diesen Parameter entweder mit den Parametern REGISTRATION_LOGIN und REGISTRATION_PASSWORD verwenden oder mit dem Parameter REGISTRATION_TOKEN. • Wenn Sie ihn mit den Parametern REGISTRATION_LOGIN und REGISTRATION_PASSWORD verwenden, müssen Sie die Adresse spezifizieren, die Sie verwenden, um sich am Cyber Protection Service **anzumelden**. Beispielsweise https://cloud.company.com:  • Wenn Sie ihn mit dem Parameter REGISTRATION_TOKEN verwenden, müssen Sie die genaue

Parameter	Beschreibung
	Datacenter-Adresse spezifizieren. Dies ist die URL, die Sie sehen, sobald Sie sich am Cyber Protection Service **angemeldet haben**. Beispielsweise `https://eu2-cloud.company.com`.  Sie dürfen `https://cloud.company.com` nicht mit dem Parameter `REGISTRATION_TOKEN` verwenden.

`REGISTRATION_LOGIN`
 	
`REGISTRATION_PASSWORD`
	Die Anmeldedaten für das Konto, unter dem der Agent im Cyber Protection Service registriert wird. Dies darf kein Partner-Administrator-Konto sein.
	
	Sie dürfen diese Parameter nicht zusammen mit dem Parameter `REGISTRATION_TOKEN` verwenden.

`REGISTRATION_PASSWORD_ENCODED`	Das Kennwort für das Konto, unter dem der Agent im Cyber Protection Service registriert wird, codiert in Base64. Weitere Informationen darüber, wie Sie Ihr Kennwort codieren können, finden Sie im Abschnitt '"Kennwörter mit Sonderzeichen oder Leerzeichen" (S. 134)'.
`REGISTRATION_TOKEN`	Das Registrierungstoken. Das Registrierungstoken ist eine Folge von 12 Zeichen, die durch Bindestriche in 3 Segmente separiert sind. Weitere Informationen darüber, wie man ein Token generiert, finden Sie im Abschnitt '"Ein Registrierungstoken generieren" (S. 182)'. Sie dürfen diesen Parameter nicht zusammen mit den Parametern `REGISTRATION_LOGIN` und `REGISTRATION_PASSWORD` verwenden.
`REGISTRATION_REQUIRED={0,1}`	Verwenden Sie diesen Parameter, um festzulegen, was geschehen soll, wenn die Registrierung fehlschlagen sollte. Wenn der Wert mit `1` festgelegt ist, wird auch die Installation fehlschlagen. Wenn Sie den Wert mit `0` festlegen oder den Parameter nicht spezifizieren, wird die Installation auch dann erfolgreich abgeschlossen, wenn die Registrierung fehlschlagen sollte.
Anmeldekonto für den Agenten-Dienst	
`MMS_USE_SYSTEM_ACCOUNT={0,1}`	Verwenden Sie diesen Parameter mit dem Wert `1`,

Parameter	Beschreibung
	damit der Service unter dem Anmeldekonto **Lokales System** ausgeführt wird. Weitere Informationen über Anmeldekonten Sie im Abschnitt '"Das Anmeldekonto auf Windows-Maschinen ändern" (S. 90)'.
MMS_CREATE_NEW_ACCOUNT={0,1}	Verwenden Sie diesen Parameter mit dem Wert 1, damit der Dienst des Agenten unter einem neuen Anmeldekonto, nämlich **Acronis Agent User**, ausgeführt wird, das automatisch erstellt wird.
MMS_SERVICE_USERNAME=<Benutzername> MMS_SERVICE_PASSWORD=<Kennwort>	Verwenden Sie diese Parameter, um ein vorhandenes Anmeldekonto zu spezifizieren, unter dem der Dienst des Agenten ausgeführt werden soll.
vCenter/ESXi-Parameter	
SET_ESX_SERVER={0,1}	Verwenden Sie diesen Parameter, wenn Sie den Agent für VMware installieren. Wenn Sie den Wert mit 0 festlegen, wird der Agent für VMware nicht mit dem vCenter Server oder einem ESXi-Host verbunden. Wenn Sie den Wert mit 1 festlegen, spezifizieren Sie auch folgende Parameter: ESX_HOST, EXI_USER, ESX_PASSWORD.
ESX_HOST=<Host-Name>	Der Host-Name oder die IP-Adresse des vCenter Servers oder ESXi-Hosts.
ESX_USER=<Benutzername> ESX_PASSWORD=<Kennwort>	Die Anmeldedaten, um auf den vCenter Server oder ESXi-Host zugreifen zu können.
Proxy-Parameter	
HTTP_PROXY_ADDRESS=<IP-Adresse> HTTP_PROXY_PORT=<Port>	Verwenden Sie diese Parameter, um den HTTP-Proxy-Server zu spezifizieren, den der Agent verwenden soll. Wenn Sie keinen Proxy-Server verwenden, dürfen Sie diese Parameter nicht spezifizieren.
HTTP_PROXY_LOGIN=<Anmeldename> HTTP_PROXY_PASSWORD=<Kennwort>	Die Anmeldedaten für den HTTP-Proxy-Server. Verwenden Sie diese Parameter, wenn der Proxy-Server eine Authentifizierung benötigt.

Parameter	Beschreibung
Deinstallationsparameter	
`REMOVE={<list of components>|ALL}`	Die Komponenten, die deinstalliert werden sollen. Wenn Sie mehrere Komponenten spezifizieren, müssen Sie diese per Kommata trennen. Fügen Sie keine Leerzeichen vor oder nach einem Komma ein. Wenn Sie alle Produktkomponenten entfernen wollen, müssen Sie den Wert auf `ALL` festlegen.
`DELETE_ALL_SETTINGS={0, 1}`	Wenn Sie alle Produktprotokolle, Tasks und Konfigurationseinstellungen löschen wollen, müssen Sie den Wert auf `1` festlegen. Verwenden Sie diesen optionalen Parameter, wenn Sie den Parameter `REMOVE` verwenden.
`ANTI_TAMPER_PASSWORD=<Kennwort>`	Das Kennwort, das zur Deinstallation eines kennwortgeschützten Agenten für Windows oder zur Änderung seiner Komponenten erforderlich ist.

Komponenten für eine unbeaufsichtigte Installation (MSI)

In der nachfolgenden Tabelle werden die Komponenten zusammengefasst, die Sie für eine unbeaufsichtigte Installation über eine MSI-Datei verwenden können. Verwenden Sie die Wertnamen, um die Werte für den Parameter `ADDLOCAL` zu spezifizieren. Weitere Informationen finden Sie im Abschnitt '"Parameter für eine unbeaufsichtigte Installation (MSI)" (S. 106)'.

Wertname	Komponenten-Beschreibung	Musst gemeinsam installiert werden mit	Bit-Anzahl
AgentFeature	Kernkomponenten für Agenten		32 Bit/64 Bit
MmsMspComponents	Kernkomponenten für die Backup-Funktionalität	AgentFeature	32 Bit/64 Bit
BackupAndRecoveryAgent	Agent für Windows	MmsMspComponents	32 Bit/64 Bit
AmpAgentFeature	Agent for Antimalware protection	BackupAndRecoveryAgent	32 Bit/64 Bit
UrlFilteringAgentFeature	Agent for URL Filtering		32

		BackupAndRecoveryAgent	Bit/64 Bit
DlpAgentFeature	Agent für Data Loss Prevention	BackupAndRecoveryAgent	32 Bit/64 Bit
SasAgentFeature	Agent für File Sync & Share	TrayMonitor	32 Bit/64 Bit
ArxAgentFeature	Agent für Exchange	MmsMspComponents	32 Bit/64 Bit
ArsAgentFeature	Agent für SQL	BackupAndRecoveryAgent	32 Bit/64 Bit
ARADAgentFeature	Agent für Active Directory	BackupAndRecoveryAgent	32 Bit/64 Bit
ArxOnlineAgentFeature	Agent für Microsoft 365	MmsMspComponents	32 Bit/64 Bit
OracleAgentFeature	Agent für Oracle	BackupAndRecoveryAgent	32 Bit/64 Bit
AcronisESXSupport	Agent für VMware ESX (i) (Windows)	BackupAndRecoveryAgent	64 Bit
HyperVAgent	Agent für Hyper-V	BackupAndRecoveryAgent	32 Bit/64 Bit
CommandLineTool	Befehlszeilenwerkzeug		32 Bit/64 Bit
TrayMonitor	Cyber Protect Monitor	AgentFeature	32 Bit/64 Bit
BackupAndRecoveryBootableComponents	Bootable Media Builder		32 Bit/64 Bit

Unbeaufsichtigte Installation oder Deinstallation unter Linux

Dieser Abschnitt beschreibt, wie Sie die Protection Agenten auf einer unter Linux laufenden Maschine und mithilfe der Befehlszeile im unbeaufsichtigten Modus installieren oder deinstallieren können.

So können Sie einen Agenten installieren

1. Öffnen Sie die Applikation 'Terminal'.

2. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:

- Führen Sie folgenden Befehl aus, um die Installation mit Parametern zu starten, die Sie über die Befehlszeile spezifizieren:

  ```
  <package name> -a <Parameter 1> ... <Parameter N>
  ```

  Wobei <package name> die Bezeichnung der Installationspakete ist (eine .i686- oder .x86_64-Datei). Alle verfügbaren Parameter und ihre Werte sind unter '"Parameter für eine unbeaufsichtigte Installation oder Deinstallation" (S. 114)' beschrieben.
- Führen Sie folgenden Befehl aus, um die Installation mit Parametern zu starten, die in einer separaten Textdatei spezifiziert wurden:

  ```
  <package name> -a --options-file=<path to the file>
  ```

  Dieser Ansatz kann nützlich sein, wenn Sie keine sensiblen Informationen über die Befehlszeile eingeben wollen. In diesem Fall können Sie die Konfigurationseinstellungen in einer separaten Textdatei spezifizieren und sicherstellen, dass nur Sie auf diese zugreifen können. Verwenden Sie für jeden Parameter eine neue Zeile, gefolgt von dem Wert für diesen Parameter. Beispiel:

  ```
  --rain=https://cloud.company.com
  --login=johndoe
  --password=johnspassword
  --auto
  ```

  oder

  ```
  -C
  https://cloud.company.com
  -g
  johndoe
  -w
  johnspassword
  -a
  --language
  en
  ```

  Wenn derselbe Parameter sowohl über die Befehlszeile als auch in der Textdatei spezifiziert wird, hat der Befehlszeilenwert Vorrang.

3. Wenn im UEFI-BIOS der Maschine die Secure Boot-Funktion (kurz 'UEFI Secure Boot') aktiviert ist, werden Sie darüber informiert, dass Sie das System nach der Installation neu starten müssen. Denken Sie daran, welches Kennwort (das des root-Benutzers oder 'acronis') verwendet werden soll. Wählen Sie während des Systemstarts die Option zur Verwaltung des MOK (Machine Owner Key), wählen Sie den (üblichweise englischen) Befehl **Enroll MOK** und registrieren Sie dann den Schlüssel mit dem empfohlenen Kennwort.

Wenn Sie UEFI Secure Boot nach der Installation des Agenten aktivieren, müssen Sie die Installation (einschließlich Schritt 3) wiederholen. Anderenfalls werden die Backups fehlschlagen.

So können Sie einen Agenten deinstallieren

1. Öffnen Sie die Applikation 'Terminal'.
2. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Führen Sie folgenden Befehl aus, um den Agenten zu deinstallieren und dabei auch alle Protokolle, Tasks und Konfigurationseinstellungen zu entfernen:

     ```
     /usr/lib/Acronis/BackupAndRecovery/uninstall/uninstall -a
     ```

   - Wenn Sie den Agenten deinstallieren wollen, dabei aber seine ID behalten wollen (weil Sie beispielsweise vorhaben, den Agenten später zu installieren), müssen Sie folgenden Befehl ausführen:

     ```
     /usr/lib/Acronis/BackupAndRecovery/uninstall/uninstall -a --no-purge
     ```

   - Wenn Sie den Agenten mithilfe der Installationsdatei deinstallieren wollen, müssen Sie folgenden Befehl ausführen:

     ```
     <package name> -a -u
     ```

     Wobei `<package name>` die Bezeichnung der Installationspakete ist (eine .i686- oder .x86_64-Datei). Alle verfügbaren Parameter und ihre Werte sind unter '"Parameter für eine unbeaufsichtigte Installation oder Deinstallation" (S. 114)' beschrieben.

     Hinweis
     Verwenden Sie diesen Befehl nur, wenn das Installationspaket die gleiche Version wie der installierte Agent hat und wenn das Verzeichnis `/usr/lib/Acronis/BackupAndRecovery/uninstall/uninstall` beschädigt oder unzugänglich sein sollte.

Parameter für eine unbeaufsichtigte Installation oder Deinstallation

Dieser Abschnitt beschreibt die Parameter, die bei einer unbeaufsichtigten Installation oder Deinstallation unter Linux verwendet werden können.

Die minimale Konfiguration für eine unbeaufsichtigte Installation beinhaltet den Parameter `-a` sowie die Registrierungsparameter (beispielsweise die Parameter `--login` und `--password` oder die

Parameter `--rain` und `--token`). Sie können weitere Parameter verwenden, um Ihre Installation anzupassen.

Installationsparameter

Grundlegende Parameter

`{-i |--id=}<list of components>`

Die zu installierenden Komponenten, durch Kommata getrennt und ohne Leerzeichen. Folgende Komponenten sind im .x86_64-Installationspaket verfügbar:

Komponente	Komponenten-Beschreibung
BackupAndRecoveryAgent	Agent für Linux
AgentForPCS	Agent für Virtuozzo
OracleAgentFeature	Agent für Oracle
MySQLAgentFeature	Agent für MySQL/MariaDB

Ohne diesen Parameter werden alle oberen Komponenten installiert.

Der Agent für Virtuozzo, der Agent für Oracle und der Agent für MySQL/MariaDB erfordern, dass zusätzlich der Agent für Linux installiert wird.

Das .i686-Installationspaket enthält nur den 'BackupAndRecoveryAgent'.

`{-a|--auto}`

Der Installations- und Registrierungsprozess wird ohne weitere Benutzereingriffe abgeschlossen. Wenn Sie diesen Parameter verwenden, müssen Sie das Konto spezifizieren, unter dem der Agent im Cyber Protection Service registriert wird – entweder über den Parameter `--token` oder mithilfe der Parameter `--login` und `--password`.

`{-t|--strict}`

Wird der Parameter spezifiziert, bewirkt jede Warnung, die während der Installation auftritt, dass die Installation fehlschlägt. Ohne diesen Parameter wird die Installation auch bei Warnungen erfolgreich abgeschlossen.

`{-n|--nodeps}`

Wenn erforderliche Linux-Pakete während der Installation fehlen, so wird dies ignoriert.

`{-d|--debug}`

Schreibt das Installationsprotokoll (Log) im ausführlichen Modus (Verbose-Modus).

`--options-file=<Speicherort>`

Die Installationsparameter werden aus einer Textdatei ausgelesen (statt über die Befehlszeile spezifiziert).

`--language=<Sprach-ID>`

Die Sprache für das Produkt. Die verfügbaren Werte sind: `en`, `bg`, `cs`, `da`, `de`, `es`, `fr`, `hu`, `id`, `it`, `ja`, `ko`, `ms`, `nb`, `nl`, `pl`, `pt`, `pt_BR`, `ru`, `fi`, `sr`, `sv`, `tr`, `zh`, `zh_TW`.
Wenn der Parameter nicht spezifiziert wird, wird die Produktsprache durch die Sprache Ihres Systems definiert (vorausgesetzt, dass diese Sprache in der oberen Liste enthalten ist). Ansonsten wird Englisch als Produktsprache festgelegt (`en`).

Registrierungsparameter

Spezifizieren Sie einen der folgenden Parameter:

- `{-g|--login=}<Benutzername>` und `{-w|--password=}<Kennwort>`

  Anmeldedaten für das Konto, unter dem der Agent im Cyber Protection Service registriert wird. Dies darf kein Partner-Administrator-Konto sein.

- `--token=<Token>`

  Das Registrierungstoken ist eine Folge von 12 Zeichen, die durch Bindestriche in 3 Segmente separiert sind. Sie können ein Token in der Cyber Protect-Konsole generieren, wie im Abschnitt 'Agenten per Gruppenrichtlinie bereitstellen' erläutert.

  Sie können den Parameter `--token` nicht zusammen mit den Parametern `--login`, `--password` und `--register-with-credentials` verwenden.

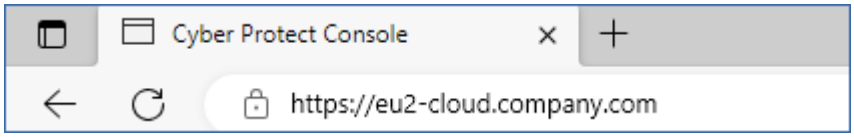
  - `{-C|--rain=}<Service-Adresse>`

    Die URL des Cyber Protection Service.

    Sie müssen diesen Parameter nicht explizit einschließen, wenn Sie die Parameter `--login` und `--password` zur Registrierung verwenden, weil der Installer standardmäßig die korrekte Adresse verwendet – nämlich die Adresse, die Sie zur **Anmeldung** am Cyber Protection Service verwenden. Beispiel:

    Wenn Sie jedoch `{-C|--rain=}` mit dem Parameter `--token` verwenden, müssen Sie die genaue Datacenter-Adresse spezifizieren. Dies ist die URL, die Sie sehen, sobald Sie sich am Cyber Protection Service **angemeldet haben**. Beispiel:

- `--register-with-credentials`

  Wenn dieser Parameter spezifiziert wird, dann wird die Benutzeroberfläche des Installers gestartet. Um die Registrierung abschließen zu können, müssen Sie die Anmeldedaten (Benutzername, Kennwort) für das Konto spezifizieren, unter dem der Agent im Cyber Protection Service registriert wird. Dies darf kein Partner-Administrator-Konto sein.

- `--skip-registration`

  Verwenden Sie diesen Parameter, wenn Sie den Agenten installieren müssen, diesen jedoch erst später im Cyber Protection Service registrieren wollen. Weitere Informationen über die entsprechende Durchführung finden Sie im Abschnitt 'Maschinen manuell registrieren'.

Zusätzliche Parameter

`--http-proxy-host=<IP-Adresse>` und `--http-proxy-port=<Port>`

Der HTTP-Proxy-Server, den der Agent für Backups in die Clouds, für Wiederherstellungen aus der Cloud und für Verbindungen mit dem Management Server verwenden wird. Ohne diesen Parameter wird kein Proxy-Server verwendet.

`--http-proxy-login=<Anmeldename>` und `--http-proxy-password=<Kennwort>`

Die Anmeldedaten für den HTTP-Proxy-Server. Verwenden Sie diese Parameter, wenn der Server eine Authentifizierung benötigt.

`--tmp-dir=<Speicherort>`

Spezifiziert den Ordner, wo die temporären Dateien während der Installation gespeichert werden. Der Standardordner lautet: **/var/tmp**.

`{-s|--disable-native-shared}`

Die 'Redistributable Libraries' (weiterverbreitbare Bibliotheken) werden während der Installation verwendet – selbst dann, wenn Sie bereits auf Ihrem System vorhanden sind.

`--skip-prereq-check`

Es wird nicht überprüft, ob die zur Kompilierung des snapapi-Moduls erforderlichen Pakete bereits installiert sind.

`--force-weak-snapapi`

Der Installer wird kein snapapi-Modul kompilieren. Stattdessen wird er ein vorgefertigtes Modul verwenden, welches möglicherweise nicht genau zum Linux-Kernel passt. Wir raten davon ab, diese Option zu verwenden.

`--skip-svc-start`

Die Services werden nach der Installation nicht automatisch gestartet. Dieser Parameter wird am häufigsten mit dem Parameter `--skip-registration` verwendet.

Informationsparameter

`{-?|--help}`

Zeigt eine Beschreibung der Parameter an.

`--usage`

Zeigt eine kurze Beschreibung an, wie der Befehl verwendet wird.

`{-v|--version}`

Zeigt die Version des Installationspaketes an.

`--product-info`

Zeigt den Produktnamen und die Version des Installationspaketes an.

`--snapapi-list`

Zeigt die verfügbaren vorgefertigten snapapi-Module an.

`--components-list`

Zeigt die Installer-Komponenten an.

Parameter für ältere Funktionen

Diese Parameter gehören zu einer Komponente aus einer Vorgängerversion: agent.exe.

`{-e|--ssl=}<Pfad>`

Spezifiziert den Pfad zu einer benutzerdefinierten Zertifikatsdatei für SSL-Verbindungen.

`{-p|--port=}<Port>`

Spezifiziert den Port, den 'agent.exe' auf Verbindungen abhören soll. Der Standard-Port ist 9876.

Deinstallationsparameter

`{-u|--uninstall}`

Das Produkt wird deinstalliert.

`--purge`

Deinstalliert das Produkt und entfernt dessen Protokolle (Logs), Tasks und Konfigurationseinstellungen. Sie müssen den Parameter `--uninstall` nicht explizit spezifizieren, wenn Sie den Parameter `--purge` verwenden.

Beispiele

- Den Agenten für Linux installieren, ohne ihn zu registrieren.

  ```
  ./Cyber_Protection_Agent_for_Linux_x86_64.bin -i BackupAndRecoveryAgent -a --skip-registration
  ```

- Den Agenten für Linux, den Agenten für Virtuozzo und den Agenten für Oracle installieren und diese mithilfe von Anmeldedaten registrieren.

  ```
  ./Cyber_Protection_Agent_for_Linux_x86_64.bin -a --login=johndoe --password=johnspassword
  ```

- Den Agenten für Oracle und den Agenten für Linux installieren und diese mithilfe eines Registrierungstokens registrieren.

```
./Cyber_Protection_Agent_for_Linux_x86_64.bin -i
BackupAndRecoveryAgent,OracleAgentFeature -a --rain=https://eu2-cloud.company.com --
token=34F6-8C39-4A5C
```

- Den Agenten für Linux, den Agenten für Virtuozzo und den Agenten für Oracle mit Konfigurationseinstellungen in einer separaten Textdatei installieren.

```
./Cyber_Protection_Agent_for_Linux_x86_64.bin -a --options-
file=/home/mydirectory/configuration_file
```

- Den Agenten für Linux, den Agenten für Virtuozzo und den Agenten für Oracle deinstallieren und dabei deren Protokolle, Tasks und Konfigurationseinstellungen löschen.

```
./Cyber_Protection_Agent_for_Linux_x86_64.bin -a --purge
```

Unbeaufsichtigte Installation oder Deinstallation unter macOS

Dieser Abschnitt beschreibt, wie Sie den Protection Agenten auf einer unter macOS laufenden Maschine und mithilfe der Befehlszeile im unbeaufsichtigten Modus installieren, registrieren und deinstallieren können.

Erforderliche Berechtigungen

Bevor Sie eine unbeaufsichtigte Installation auf einem Mac-Workload einleiten, müssen Sie die „Richtliniensteuerung in der Systemeinstellung 'Sicherheit'“ anpassen, um den App-Zugriff sowie die Kernel- und Systemerweiterungen im macOS des Workloads zuzulassen, damit der Cyber Protection Agent installiert werden kann. Siehe Abschnitt '"Erforderliche Berechtigungen für die unbeaufsichtigte Installation in macOS" (S. 121)'.

Nachdem Sie die PPPC-Payload bereitgestellt haben, können Sie mit den nachfolgenden Prozeduren fortfahren.

So können Sie die Installationsdatei (.dmg) herunterladen

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte** –> **Alle Geräte**.
2. Klicken Sie auf **Hinzufügen** und anschließend auf **Mac**.

So können Sie einen Agenten installieren

1. Öffnen Sie die Applikation 'Terminal'.
2. Erstellen Sie ein temporäres Verzeichnis, wo Sie die Installationsdatei (.dmg) mounten werden.

   ```
   mkdir <dmg_root>
   ```

   Wobei der Platzhalter `<dmg_root>` für einen Name Ihrer Wahl steht.
3. Mounten Sie die .dmg-Datei.

```
hdiutil attach <dmg_file> -mountpoint <dmg_root>
```

Wobei der Platzhalter `<dmg_file>` für den Name der Installationsdatei steht. Beispiel: **Cyber_Protection_Agent_for_MAC_x64.dmg**.

4. Starten Sie den Installer.
   - Wenn Sie einen vollständigen Installer für den Mac (wie `CyberProtect_AgentForMac_x64.dmg` oder `CyberProtect_AgentForMac_arm64.dmg`) verwenden, führen Sie folgenden Befehl aus.

     ```
     sudo installer -pkg <dmg_root>/Install.pkg -target LocalSystem
     ```

     Hinweis
     Wenn Sie das automatische Onboarding für File Sync & Share aktivieren müssen, führen Sie stattdessen den nachfolgenden Befehl aus. Bei dieser Option wird das Kennwort des Administrators abgefragt.

     ```
     open <dmg_root>/Install.app --args --unattended --fss-onboarding-auto-start
     ```

   - Wenn Sie einen universellen Installer für den Mac verwenden (wie `CyberProtect_AgentForMac_web.dmg`), führen Sie folgenden Befehl aus.

     ```
     sudo <dmg_root>/Install.app/Contents/MacOS/cyber_installer -a
     ```

5. Trennen Sie die Installationsdatei (.dmg).

   ```
   hdiutil detach <dmg_root>
   ```

Beispiel

```
mkdir mydirectory
```

```
hdiutil attach /Users/JohnDoe/Cyber_Protection_Agent_for_MAC_x64.dmg -mountpoint
mydirectory
```

```
sudo installer -pkg mydirectory/Install.pkg -target LocalSystem
```

```
hdiutil detach mydirectory
```

So können Sie einen Agenten deinstallieren

1. Öffnen Sie die Applikation 'Terminal'.
2. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Führen Sie folgenden Befehl aus, um den Agenten zu deinstallieren:

     ```
     sudo /Library/Application\ Support/BackupClient/Acronis/Cyber\ Protect\ Agent\
     Uninstall.app/Contents/MacOS/AgentUninstall /confirm
     ```

- Führen Sie folgenden Befehl aus, um den Agenten zu deinstallieren und dabei auch alle Protokolle, Tasks und Konfigurationseinstellungen zu entfernen:

```
sudo /Library/Application\ Support/BackupClient/Acronis/Cyber\ Protect\ Agent\
Uninstall.app/Contents/MacOS/AgentUninstall /confirm /purge
```

Erforderliche Berechtigungen für die unbeaufsichtigte Installation in macOS

Bevor Sie eine unbeaufsichtigte Installation auf einem Mac-Workload einleiten, müssen Sie die „Richtliniensteuerung in der Systemeinstellung 'Sicherheit'“ anpassen, um den App-Zugriff sowie die Kernel- und Systemerweiterungen im macOS des Workloads zuzulassen, damit der Cyber Protection Agent installiert werden kann. Sie können dies tun, indem Sie eine benutzerdefinierte PPPC-Payload (Privacy Preferences Policy Control, Richtliniensteuerung in der Systemeinstellung 'Sicherheit') bereitstellen oder indem Sie die Einstellungen in der grafischen Benutzeroberfläche des Workloads konfigurieren. Die nachfolgenden Berechtigungen sind erforderlich.

Anforderungen für macOS 11 (Big Sur) oder höher

Registerkarte	Abschnitt	Feld	Wert

Richtliniensteuerung in der Systemeinstellung 'Sicherheit'	App-Zugriff	Kennung (ID)	com.acronis.backup

		Kennungstyp	Bundle-ID

		Code-Anforderung	identifier "com.acronis.backup" and anchor apple generic and certificate 1 [field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf [field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf [subject.OU] = ZU2TV78AA6
		APP ODER DIENST	SystemPolicyAllFiles
		ZUGRIFF	Erlauben
	App-Zugriff	Kennung (ID)	com.acronis.backup.aakore
		Kennungstyp	Bundle-ID
		Code-Anforderung	identifier "com.acronis.backup.aakore" and anchor apple generic and certificate 1 [field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf [field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf [subject.OU] = ZU2TV78AA6
		APP ODER DIENST	SystemPolicyAllFiles
		ZUGRIFF	Erlauben
	App-Zugriff	Identifiziert	com.acronis.backup.activeprotection
		Kennungstyp	Bundle-ID
		Code-Anforderung	identifier "com.acronis.backup.activeprotection" and anchor apple generic and certificate 1 [field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf [field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf [subject.OU] = ZU2TV78AA6
		APP ODER DIENST	SystemPolicyAllFiles
		ZUGRIFF	Erlauben

	App-Zugriff	Kennung (ID)	cyber-protect-service
		Kennungstyp	Bundle-ID
		Code-Anforderung	`identifier "cyber-protect-service" and anchor apple generic and certificate 1 [field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf [field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = ZU2TV78AA6`
		APP ODER DIENST	SystemPolicyAllFiles
		ZUGRIFF	Erlauben
Systemerweiterungen		Benutzern erlauben, Systemerweiterungen zu genehmigen	Aktiviert
	Zulässige Team-IDs und Systemerweiterungen	Anzeigename	Acronis Cyber Protection Agent-Systemerweiterungen
		Systemerweiterungstypen	Zulässige Team-IDs
		Team-ID	ZU2TV78AA6

Anforderungen für macOS-Versionen vor Version 11

Registerkarte	Abschnitt	Feld	Wert

Richtliniensteuerung in der Systemeinstellung 'Sicherheit'	App-Zugriff	Kennung (ID)	com.acronis.backup

		Kennungstyp	Bundle-ID

		Code-Anforderung	identifier "com.acronis.backup" and anchor apple generic and certificate 1 [field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf [field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf [subject.OU] = ZU2TV78AA6
		APP ODER DIENST	SystemPolicyAllFiles
		ZUGRIFF	Erlauben
	App-Zugriff	Kennung (ID)	com.acronis.backup.aakore
		Kennungstyp	Bundle-ID
		Code-Anforderung	identifier "com.acronis.backup.aakore" and anchor apple generic and certificate 1 [field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf [field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf [subject.OU] = ZU2TV78AA6
		APP ODER DIENST	SystemPolicyAllFiles
		ZUGRIFF	Erlauben
	App-Zugriff	Identifiziert	com.acronis.backup.activeprotection
		Kennungstyp	Bundle-ID
		Code-Anforderung	identifier "com.acronis.backup.activeprotection" and anchor apple generic and certificate 1 [field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf [field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf [subject.OU] = ZU2TV78AA6
		APP ODER DIENST	SystemPolicyAllFiles
		ZUGRIFF	Erlauben

	App-Zugriff	Kennung (ID)	cyber-protect-service
		Kennungstyp	Bundle-ID
		Code-Anforderung	identifier "cyber-protect-service" and anchor apple generic and certificate 1 [field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf [field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf [subject.OU] = ZU2TV78AA6
		APP ODER DIENST	SystemPolicyAllFiles
		ZUGRIFF	Erlauben
Zulässige Kernel-Erweiterungen		Benutzern erlauben, Kernel-Erweiterungen zu genehmigen	Aktiviert
		Standardbenutzern erlauben, veraltete Kernel-Erweiterungen zu genehmigen (macOS 11 oder höher)	Aktiviert
	Zulässige Team-IDs und Kernel-Erweiterungen	Zulässige Team-ID – Anzeigename	Acronis Cyber Protection Agent-Kernel-Erweiterungen
		Team-ID	ZU2TV78AA6
		Kernel-Erweiterung Bundle-IDs	• com.acronis.systeminterceptors • com.acronis.ngscan • com.acronis.notifyframework
Systemerweiterungen		Benutzern erlauben, Systemerweiterungen zu genehmigen	Aktiviert
	Zulässige Team-IDs und Systemerweiterungen	Anzeigename	Acronis Cyber Protection Agent-Systemerweiterungen
		Systemerweiterungstypen	Zulässige Team-IDs
		Team-ID	ZU2TV78AA6

Workloads manuell registrieren und deregistrieren

Workloads werden automatisch im Cyber Protection Service registriert, wenn Sie den Protection Agenten auf den entsprechenden Workloads installieren. Wenn Sie den Protection Agenten deinstallieren, wird die Registrierung der Workloads automatisch aufgehoben und sie werden nicht mehr in der Cyber Protect-Konsole angezeigt.

Sie können einen Workload auch manuell über die Befehlszeilenschnittstelle registrieren. Sie müssen die manuelle Registrierung möglicherweise verwenden, wenn beispielsweise die automatische Registrierung fehlschlägt oder wenn Sie einen Workload zu einem neuen Mandanten oder unter ein neues Benutzerkonto verschieben wollen.

So können Sie einen Workload mithilfe eines Benutzernamens und Kennworts registrieren

Unter Windows

Führen Sie in der Befehlszeile folgenden Befehl aus:

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud
-a <service address> -u <user name> -p <password>
```

Beispiel:

```
"C:\ProgramFiles\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud
-a https://cloud.company.com -u johndoe -p johnspassword
```

Unter Linux

Führen Sie in der Befehlszeile folgenden Befehl aus:

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a <service
address> -u <user name> -p <password>
```

Beispiel:

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a
https://cloud.company.com -u johndoe -p johnspassword
```

Unter macOS

Führen Sie in der Befehlszeile folgenden Befehl aus:

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent"
-o register -t cloud -a <service address> -u <user name> -p <password>
```

Beispiel:

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent"
-o register -t cloud -a https://cloud.company.com -u johndoe -p johnspassword
```

Hinweis
Verwenden Sie den Benutzernamen und das Kennwort für dasjenige Konto, unter dem Sie den Workload registrieren wollen. Dies darf kein Partner-Administrator-Konto sein.

Die Service-Adresse ist die URL, die Sie verwenden, um sich am Cyber Protection Service **anzumelden**. Beispiel: `https://cloud.company.com`.

Wichtig
Wenn Sie in Ihrem Kennwort Sonder- oder Leerzeichen verwenden, sollten Sie sich im Abschnitt '"Kennwörter mit Sonderzeichen oder Leerzeichen" (S. 134)' informieren.

Wichtig
Wenn Sie macOS 10.14 oder höher einsetzen, müssen Sie dem Protection Agenten die Berechtigung 'Vollzugriff auf Festplatte' gewähren. Gehen Sie dafür zu **Programme** –> **Dienstprogramme** und führen Sie den **Cyber Protect Agent-Assistenten** aus. Folgen Sie dann den Anweisungen im Applikationsfenster.

So können Sie einen Workload mithilfe eines Registrierungstokens registrieren

Unter Windows

Führen Sie in der Befehlszeile folgenden Befehl aus:

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud
-a <service address> --token <registration token>
```

Beispiel:

```
"C:\ProgramFiles\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud
-a https://au1-cloud.company.com --token 3B4C-E967-4FBD
```

Unter Linux

Führen Sie in der Befehlszeile folgenden Befehl aus:

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a <service
address> --token <registration token>
```

Beispiel:

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a
https://eu2-cloud.company.com --token 34F6-8C39-4A5C
```

Unter macOS

Führen Sie in der Befehlszeile folgenden Befehl aus:

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent"
-o register -t cloud -a <service address> --token <registration token>
```

Beispiel:

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent"
-o register -t cloud -a https://us5-cloud.company.com --token 9DBF-3DA9-4DAB
```

Wichtig
Wenn Sie macOS 10.14 oder höher einsetzen, müssen Sie dem Protection Agenten die Berechtigung 'Vollzugriff auf Festplatte' gewähren. Gehen Sie dafür zu **Programme** –> **Dienstprogramme** und führen Sie den **Cyber Protect Agent-Assistenten** aus. Folgen Sie dann den Anweisungen im Applikationsfenster.

Virtuelle Appliance

1. Drücken Sie in der Konsole der virtuellen Appliance die Tastenkombination STRG+UMSCHALT+F2, um die Befehlszeilenschnittstelle zu öffnen.
2. Führen Sie in der Eingabeaufforderung folgenden Befehl aus:

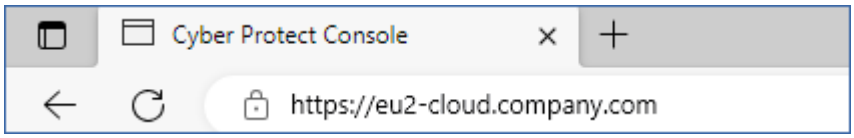
   ```
   register_agent -o register -t cloud -a <service address> --token <registration token>
   ```

   Beispiel:

   ```
   register_agent -o register -t cloud -a https://eu2-cloud.company.com --token 34F6-
   8C39-4A5C
   ```

3. Drücken Sie die Tastenkombination ALT+F1, um zur grafischen Oberfläche der Appliance zurückzukehren.

Hinweis
Wenn Sie ein Registrierungstoken verwenden, müssen Sie die genaue Datacenter-Adresse spezifizieren. Dies ist die URL, die Sie sehen, sobald Sie sich am Cyber Protection Service **angemeldet haben**. Beispielsweise `https://eu2-cloud.company.com`.



Sie dürfen hier nicht die Adresse `https://cloud.company.com` verwenden.

Das Registrierungstoken ist eine Folge von 12 Zeichen, die durch Bindestriche in 3 Segmente separiert sind. Weitere Informationen über dessen Generierung finden Sie im Abschnitt '"Ein Registrierungstoken generieren" (S. 182)'.

So können Sie die Registrierung eines Workloads aufheben

Unter Windows

Führen Sie in der Befehlszeile folgenden Befehl aus:

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o unregister
```

Beispiel:

```
"C:\ProgramFiles\BackupClient\RegisterAgentTool\register_agent.exe" -o unregister
```

Unter Linux

Führen Sie in der Befehlszeile folgenden Befehl aus:

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o unregister
```

Unter macOS

Führen Sie in der Befehlszeile folgenden Befehl aus:

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent"
-o unregister
```

Virtuelle Appliance

1. Drücken Sie in der Konsole der virtuellen Appliance die Tastenkombination STRG+UMSCHALT+F2, um die Befehlszeilenschnittstelle zu öffnen.
2. Führen Sie in der Eingabeaufforderung folgenden Befehl aus:

   ```
   register_agent -o unregister
   ```

3. Drücken Sie die Tastenkombination ALT+F1, um zur grafischen Oberfläche der Appliance zurückzukehren.

Einen Workload zu einem anderen Mandanten verschieben

Das Verschieben eines Workloads zu einem anderen Mandanten wird nicht standardmäßig unterstützt. Als Workaround können Sie jedoch die Registrierung des Workloads aufheben und diesen dann wieder in einem anderen Mandanten registrieren. Alle bisher angewendeten Schutzpläne für diesen Workload werden widerrufen. Außerdem verliert er den Zugriff auf seine Backups im Cloud Storage für den ursprünglichen Mandanten.

Weitere Informationen darüber, wie Sie einen Workload in einem neuen Tenant oder unter einem neuen Benutzerkonto registrieren können, finden Sie im Abschnitt '"Die Registrierung eines Workloads ändern" (S. 135)'.

Kennwörter mit Sonderzeichen oder Leerzeichen

Wenn Ihr Kennwort Sonderzeichen oder Leerzeichen enthält, müssen Sie es in Anführungszeichen einschließen, wenn Sie es über die Befehlszeile eingeben.

Führen Sie beispielsweise folgenden Befehl unter Windows aus:

Befehlsvorlage:

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud
-a <service address> -u <user name> -p <"password">
```

Befehlsbeispiel:

```
"C:\ProgramFiles\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud
-a https://cloud.company.com -u johndoe -p "johns password"
```

Sollte dieser Befehl fehlschlagen, codieren Sie Ihr Kennwort im Base64-Format über die Website https://www.base64encode.org/. Spezifizieren Sie dann das codierte Kennwort in der Befehlszeile unter Verwendung der Parameter -b oder --base64.

Führen Sie beispielsweise folgenden Befehl unter Windows aus:

Befehlsvorlage:

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud
-a <service address> -u <user name> -b -p <encoded password>
```

Befehlsbeispiel:

```
"C:\ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t
cloud -a https://cloud.company.com -u johndoe -b -p am9obnNwYXNzd29yZA==
```

Die Registrierung eines Workloads ändern

Sie können die aktuelle Registrierung eines Workloads ändern, indem Sie diesen in einem neuen Mandanten oder unter einem neuen Benutzerkonto registrieren.

Wichtig
Wenn Sie die Registrierung eines Workloads ändern, werden alle Schutzpläne, die auf diesen Workload angewendet wurden, widerrufen. Wenn Sie den Workload weiterhin schützen wollen, müssen Sie einen neuen Schutzplan auf ihn anwenden.

Wenn Sie den Workload in einem neuen Mandanten registrieren, wird der Workload nicht mehr auf die Backups im Cloud Storage des ursprünglichen Mandanten zugreifen können. Auf Backups, die sich auf „Nicht-Cloud“-Storages befinden, besteht ein unveränderter Zugriff.

Sie können die Registrierung eines Workloads entweder über die Befehlszeile oder über den Installer mit der grafischen Benutzeroberfläche (GUI-Installer) ändern. Wenn Sie die Befehlszeile verwenden, müssen Sie den Agenten nicht deinstallieren.

So können Sie die Registrierung eines Workloads ändern

Über die Befehlszeile

1. Heben Sie die Registrierung des Protection Agenten auf, wie im Abschnitt '"So können Sie die Registrierung eines Workloads aufheben" (S. 133)' beschrieben.
2. Registrieren Sie den Protection Agenten im neuen Mandanten oder unter dem neuen Benutzerkonto, wie in den Abschnitten '"So können Sie einen Workload mithilfe eines Benutzernamens und Kennworts registrieren" (S. 130)' oder '"So können Sie einen Workload mithilfe eines Registrierungstokens registrieren" (S. 131)' beschrieben.

Über den GUI-Installer

1. Deinstallieren Sie den Protection Agenten.
2. Installieren Sie den Protection Agenten und registrieren Sie diesen dann im neuen Mandanten oder unter dem neuen Benutzerkonto.

Weitere Informationen darüber, wie Sie einen Agenten installieren und registrieren können, finden Sie im Abschnitt '"Protection Agenten installieren" (S. 81)'.

Automatische Erkennung von Maschinen

Mit der automatischen Erkennung können Sie:

- Die Installation von Protection Agenten sowie die Registrierung von Maschinen automatisieren, indem Sie die Maschinen in Ihrer Active Directory-Domain oder Ihrem lokalen Netzwerk erkennen lassen.
- Protection Agenten auf mehreren Maschinen installieren und aktualisieren.

- Synchronisierungen mit dem Active Directory verwenden, um die Bereitstellung von Ressourcen und Verwaltung von Maschinen in einer großen Active Directory-Domain zu erleichtern.

Voraussetzungen

Um eine automatische Erkennung durchführen zu können, benötigen Sie mindestens eine Maschine in Ihrem lokalen Netzwerk oder Ihrer Active Directory-Domain, auf der ein Protection Agent installiert ist. Dieser Agent wird dann als sogenannter Discovery Agent verwendet.

Wichtig
Nur Agenten, die auf Windows-Maschinen installiert sind, können Discovery Agenten sein. Wenn es in Ihrer Umgebung keine Discovery Agenten gibt, können Sie nicht die Option **Mehrere Geräte** im Fensterbereich **Geräte hinzufügen** verwenden.

Die Remote-Installation von Agenten wird nur für Maschinen unter Windows unterstützt (wobei Windows XP nicht mehr unterstützt wird). Um eine Remote-Installation auf einer Maschine mit Windows Server 2012 R2 durchführen zu können, muss auf dieser Maschine das Windows-Update KB2999226 installiert sein.

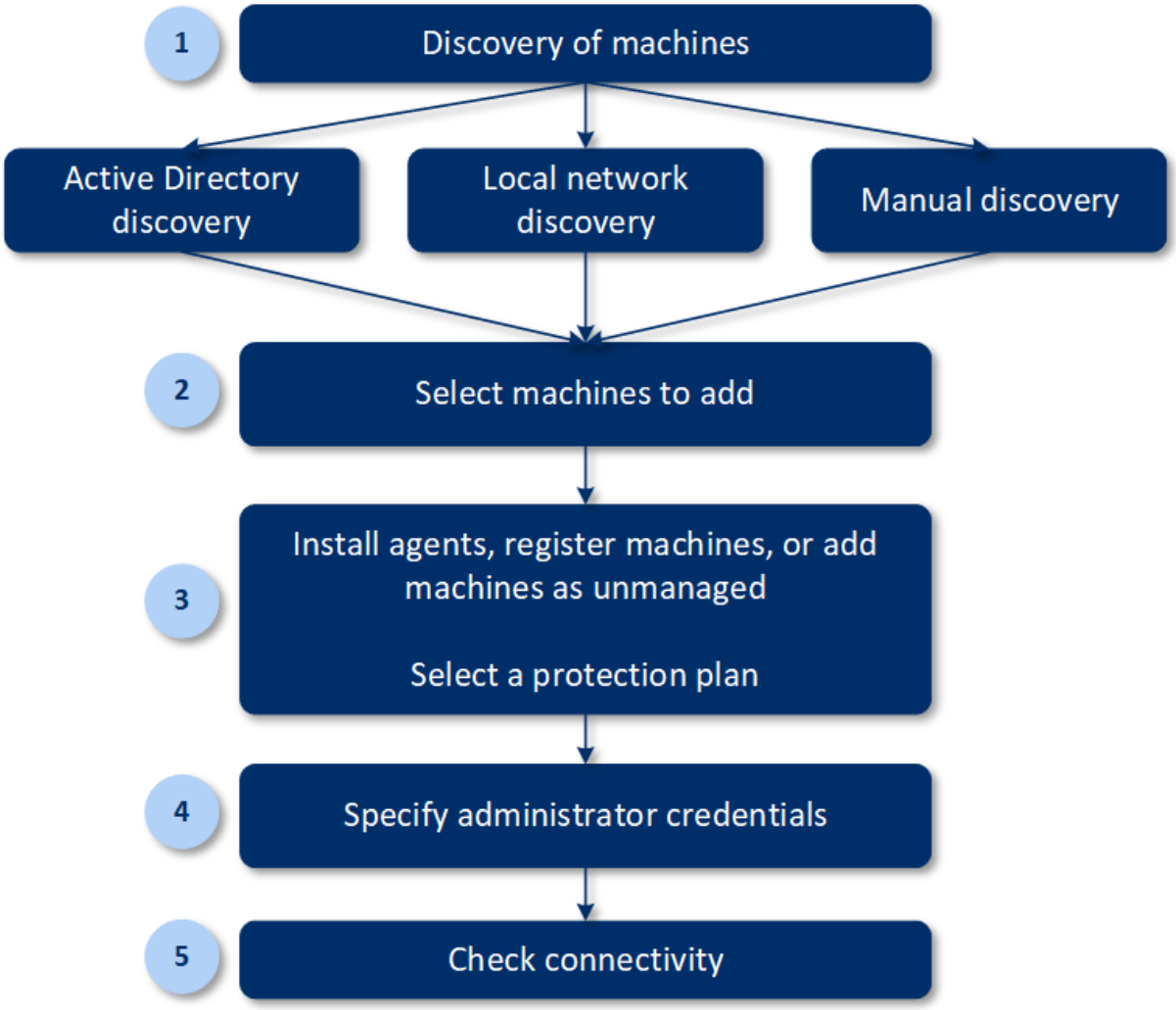
So funktioniert die automatische Erkennung

Bei einer Erkennung im lokalen Netzwerk werden vom Discovery Agenten mithilfe der NetBIOS-Erkennung, der WSD-Funktion (Web Service Discovery, Webdiensterkennung) und der ARP-Tabelle (Address Resolution Protocol) folgende Informationen für jede Maschine im Netzwerk gesammelt:

- Name (Kurzname/NetBIOS-Host-Name)
- Vollqualifizierter Domain-Name (FQDN)
- Domain/Arbeitsgruppe
- IPv4-/IPv6-Adressen
- MAC-Adressen
- Betriebssystem (Name/Version/Familie)
- Maschinen-Kategorie (Workstation/Server/Domain Controller)

Bei einer Erkennung im Active Directory werden vom Discovery Agenten (zusätzlich zur oberen Liste) noch Informationen über die Organisationseinheit (OE) der Maschinen sowie detailliertere Informationen über deren Namen und Betriebssysteme gesammelt. Die IP- und MAC-Adressen werden jedoch nicht erfasst.

Das nachfolgende Diagramm fasst den automatischen Erkennungsprozess zusammen.



1. Bestimmen Sie die Erkennungsmethode:
   - Erkennung im Active Directory
   - Erkennung im lokalen Netzwerk
   - Manuelle Erkennung – Mithilfe der IP-Adresse oder dem Host-Namen einer Maschine oder indem eine Liste von Maschinen aus einer Datei importiert wird

   Aus den Ergebnissen einer Erkennung im Active Directory oder einer Erkennung im lokalen Netzwerk werden Maschinen, auf denen ein Protection Agent installiert ist, ausgeschlossen.

   Bei einer manuellen Erkennung werden bereits vorhandene Protection Agenten aktualisiert und neu registriert. Wenn Sie die automatische Erkennung unter demselben Konto durchführen, unter dem ein Agent registriert ist, wird der Agent lediglich auf die neueste Version aktualisiert. Wenn Sie die automatische Erkennung unter einem anderen Konto durchführen, wird der Agent auf die neueste Version aktualisiert und zudem unter dem Mandanten, zu dem das Konto gehört, neu registriert.
2. Wählen Sie die Maschinen aus, die Sie Ihrem Mandanten hinzufügen wollen.
3. Bestimmen Sie, wie diese Maschinen hinzugefügt werden sollen:

- Einen Protection Agent und weitere Komponenten auf den Maschinen installieren und diese dann in der Cyber Protect-Konsole registrieren.
- Die Maschinen in der Cyber Protect-Konsole registrieren (wenn ein Protection Agent bereits installiert wurde).
- Die Maschinen zur Cyber Protect-Konsole als **Nicht verwaltete Maschinen** hinzufügen, ohne einen Protection Agenten zu installieren.

Sie können auf die Maschinen, auf denen Sie einen Protection Agenten installieren oder die Sie in der Cyber Protect-Konsole registrieren wollen, auch einen vorhandenen Schutzplan anwenden.

4. Geben Sie die Administrator-Anmeldedaten für die ausgewählten Maschinen an.
5. Überprüfen Sie, ob Sie mit den angegebenen Anmeldedaten eine Verbindung zu den Maschinen herstellen können.

Die Maschinen, die in der Cyber Protect-Konsole angezeigt werden, fallen in folgende Kategorien:

- **Erkannt** – Maschinen, die erkannt wurden, auf denen jedoch noch kein Protection Agent installiert ist.
- **Verwaltet** – Maschinen, auf denen ein Protection Agent installiert ist.
- **Ungeschützt** – Maschinen, auf die noch kein Schutzplan angewendet wurde. Zu den ungeschützten Maschinen gehören sowohl erkannte als auch verwaltete Maschinen, auf die noch kein Schutzplan angewendet wurde.
- **Geschützt** – Maschinen, auf die ein Schutzplan angewendet wurde.

Wie die Remote-Installation von Agenten funktioniert

1. Der Discovery Agent verbindet sich mit den Zielmaschinen, indem er den Host-Namen, die IP-Adresse sowie die Administrator-Anmeldedaten verwendet, die im Erkennungsassistent (Discovery Wizard) spezifiziert wurden, und wird dann die Datei `web_installer.exe` zu diesen Maschinen hochladen.
2. Die Datei `web_installer.exe` wird auf den Zielmaschinen im unbeaufsichtigten Modus ausgeführt.
3. Der Webinstaller ruft zusätzliche Installationspakete aus der Cloud ab und installiert diese dann mithilfe des Befehls `msiexec` auf den Zielmaschinen.
4. Nach Abschluss der Installation werden die Komponenten in der Cloud registriert.

Hinweis
Bei Domain Controllern wird keine Remote-Installation des Agenten unterstützt, da zur Ausführung des Agenten-Dienstes zusätzliche Berechtigungen erforderlich sind.

Automatische und manuelle Erkennung durchführen

Stellen Sie vor dem Start der Erkennung sicher, dass die Voraussetzungen erfüllt sind.

Hinweis
Beim Hinzufügen von Domain Controllern wird keine automatische Erkennung (Autodiscovery-Funktionalität) unterstützt, da zur Ausführung des Agenten-Dienstes zusätzliche Berechtigungen erforderlich sind.

So können Sie Maschinen erkennen

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte** –> **Alle Geräte**.
2. Klicken Sie auf **Hinzufügen**.
3. Klicken Sie bei **Mehrere Geräte** auf **Nur Windows**. Der Erkennungsassistent wird geöffnet.
4. [Wenn es Einheiten/Abteilungen in Ihrer Organisation gibt] Wählen Sie eine Organisationseinheit. Anschließend können Sie im **Discovery Agenten** diejenigen Agenten auswählen, die mit der ausgewählten Einheit und deren Untereinheiten assoziiert sind.
5. Wählen Sie den Discovery Agenten aus, der den Scan zum Erkennen der Maschinen durchführen soll.
6. Bestimmen Sie die Erkennungsmethode:
   - **Active Directory durchsuchen**. Stellen Sie sicher, dass die Maschine mit dem Discovery Agenten ein Mitglied der Active Directory-Domain ist.
   - **Lokales Netzwerk scannen**. Wenn der ausgewählte Discovery Agent keine Maschinen finden konnte, wählen Sie einen anderen Discovery Agenten aus.
   - **Manuell spezifizieren oder aus Datei importieren**. Definieren Sie die hinzuzufügenden Maschinen manuell oder importieren Sie diese aus einer Textdatei.
7. [Wenn die Erkennungsmethode 'Active Directory' ausgewählt wurde] Bestimmen Sie, wie nach den Maschinen gesucht werden soll:
   - **In der Liste der Organisationseinheiten**. Wählen Sie die Gruppe der Maschinen aus, die hinzugefügt werden sollen.
   - **Per LDAP-Dialekt-Abfrage**. Verwenden Sie die LDAP-Dialekt-Abfrage, um die Maschinen auszuwählen. Die **Such-Basis** definiert, wo gesucht werden soll, während Sie über **Filter** die Kriterien zur Auswahl der Maschinen spezifizieren können.
8. Je nach der von Ihnen gewählten Erkennungsmethode können Sie eine der folgenden Aktionen durchführen:

Erkennungsmethode	Aktion
Active Directory durchsuchen	Wählen Sie aus der Liste der erkannten Maschinen diejenigen aus, die Sie hinzufügen wollen.
Lokales Netzwerk scannen	Wählen Sie aus der Liste der erkannten Maschinen diejenigen aus, die Sie hinzufügen wollen.
Manuell spezifizieren oder aus Datei importieren	Spezifizieren Sie die IP-Adressen oder Host-Namen der Maschinen – oder importieren Sie eine Liste der Maschinen aus einer Textdatei. Die Datei muss je eine IP-Adresse bzw. einen Host-Namen pro Zeile enthalten. Hier

Erkennungsmethode	Aktion

	ist ein Beispiel für eine entsprechende Datei:
	`156.85.34.10`
	`156.85.53.32`
	`156.85.53.12`
	`EN-L00000100`
	`EN-L00000101`
	Nachdem die Adressen der Maschinen manuell hinzugefügt oder über eine Datei importiert wurden, versucht der Agent, die hinzugefügten Maschinen anzupingen und deren Verfügbarkeit zu ermitteln.

9. Bestimmen Sie, welche Aktionen nach der Erkennung durchgeführt werden sollen:

Option	Beschreibung
Agenten installieren und Maschinen registrieren	Sie können auswählen, welche Komponenten auf den Maschinen installiert werden sollen, indem Sie auf **Komponenten auswählen** klicken. Weitere Details finden Sie unter "Zu installierende Komponenten auswählen" (S. 144).
Anmeldekonto für den Agenten-Dienst	Diese Einstellung ist auf der Anzeige **Komponenten auswählen** verfügbar. Die Einstellung definiert das Konto, unter dem die Dienste ausgeführt werden. Sie können eine der folgenden Optionen auswählen: • **Service User-Konten verwenden** (Standard für den Agenten-Dienst) Service User-Konten sind Windows-System-Konten, die verwendet werden, um Dienste auszuführen. Der Vorteil dieser Einstellung ist, dass die Domänen-Sicherheitsrichtlinien keinen Einfluss auf die Benutzerrechte dieser Konten haben. Standardmäßig wird der Agent unter dem Konto **Lokales System** ausgeführt. • **Neues Konto erstellen** Der Kontoname für den Agenten lautet 'Agent User'. • **Folgendes Konto verwenden** Wenn Sie den Agenten auf einem Domain Controller installieren, wird Sie das System auffordern, für den Agenten vorhandene Konten (oder dasselbe Konto) zu spezifizieren. Das System erstellt aus Sicherheitsgründen nicht automatisch neue Konten auf einem Domain Controller. Wenn Sie die Option **Neues Konto erstellen** oder **Folgendes Konto verwenden** wählen, sollten Sie sicherstellen, dass die Domänen-Sicherheitsrichtlinien die Rechte der entsprechenden Konten nicht beeinträchtigen. Wenn einem Konto Benutzerrechte wieder entzogen werden, die diesem bei der Installation zugewiesen wurden, wird die Komponente möglicherweise fehlerhaft oder gar nicht funktioniert.
Maschinen mit installierten Agenten	Verwenden Sie diese Option, wenn der Agent bereits auf den Maschinen installiert ist und Sie diese nur in Cyber Protection registrieren müssen. Wenn auf den Maschinen kein Agent gefunden wird, werden diese als **Nicht verwaltete**

Option	Beschreibung
registrieren	Maschinen hinzugefügt.
Als nicht verwaltete Maschinen hinzufügen	Wenn Sie diese Option wählen, wird der Agent nicht auf den Maschinen installiert. Sie können sich die Maschinen in der Konsole anzeigen lassen und den Agenten später installieren oder registrieren.
Maschine bei Bedarf neu starten	Diese Option erscheint, wenn **Agenten installieren und Maschinen registrieren** ausgewählt wurde. Wenn Sie diese Option auswählen, wird die Maschine so oft neu gestartet, wie es zur Fertigstellung der Installation erforderlich ist. Ein Neustart der Maschine kann in einem der folgenden Fälle erforderlich sein: • Die Installation der Vorgaben ist abgeschlossen. Es ist ein Neustart erforderlich, um mit der Installation fortfahren zu können. • Die Installation ist abgeschlossen. Es ist jedoch ein Neustart erforderlich, weil einige Dateien während der Installation gesperrt wurden. • Die Installation ist abgeschlossen. Für andere, zuvor installierte Software ist jedoch ein Neustart erforderlich.
Nicht neu starten, wenn der Benutzer angemeldet ist	Diese Option erscheint, wenn **Maschine bei Bedarf neu starten** ausgewählt wurde. Wenn Sie diese Option auswählen, wird die Maschine nicht automatisch neu gestartet, solange der Benutzer im System angemeldet ist. Wenn ein Benutzer also beispielsweise arbeitet, während die Installation einen Neustart erfordert, wird das System nicht neu gestartet. Wenn die Voraussetzungen installiert wurden, aber die Maschine nicht neu gestartet wurde, weil ein Benutzer angemeldet war, müssen Sie zur Fertigstellung der Installation die Maschine neu starten und dann die Installation erneut starten. Wenn der Agent installiert wurde, aber der Computer dann nicht neu gestartet wurde, müssen Sie den Computer selbst neu starten.
Benutzer, bei dem die Maschinen registriert werden sollen	[Wenn es Abteilungen in Ihrer Organisation gibt] Wählen Sie das Benutzerkonto der Abteilung oder Unterabteilungen aus, unter dem Sie die Maschinen registrieren möchten. [Wenn Sie eine automatische Erkennung auf der Partner-Mandanten-Ebene durchführen] Erweitern Sie in der Liste der von Ihnen verwalteten Kunden-Mandanten die Verzeichnisstruktur und wählen Sie dann das Benutzerkonto aus, unter dem Sie die Maschinen registrieren wollen. [Wenn Sie eine automatische Erkennung als Kunden-Administrator durchführen] Wenn Sie **Agenten installieren und Maschinen registrieren** oder **Maschinen mit installierten Agenten registrieren** ausgewählt haben, gibt es auch die Option, den Schutzplan auf die Maschinen anwenden zu lassen. Wenn Sie mehrere Schutzpläne haben, können Sie auswählen, welchen Sie verwenden möchten.

10. Spezifizieren Sie die Anmeldedaten eines Benutzers mit administrativen Berechtigungen für all diese Maschinen.

    Wichtig
    Beachten Sie, dass die Remote-Installation eines Agenten nur dann ohne Vorbereitungen funktioniert, wenn Sie die Anmeldedaten des integrierten Administratorkontos (das erste Konto, das bei der Installation des Betriebssystems erstellt wird) spezifizieren. Wenn Sie einige benutzerdefinierte Administrator-Anmeldedaten definieren wollen, dann müssen Sie zusätzliche manuelle Vorbereitungen treffen, wie im Abschnitt '"Eine Maschine für die Remote-Installation vorbereiten" (S. 142)' erläutert.

11. Das System überprüft, ob eine Verbindung mit all diesen Maschinen möglich ist. Wenn mit einigen Maschinen keine Verbindung aufgebaut werden kann, können Sie die Anmeldedaten für diese Maschinen ändern.

Wenn die Erkennung für diese Maschinen initiiert ist, können Sie den entsprechenden Task in der Aktivität **Monitoring** –> **Aktivitäten** –> **Maschinen erkennen** finden.

Eine Maschine für die Remote-Installation vorbereiten

- Damit die Installation auf einer Remote-Maschine mit Windows 7 (oder höher) erfolgreich ist, muss die Option **Systemsteuerung** –> **Ordneroptionen** –> **Ansicht** –> **Freigabe-Assistent verwenden** auf dieser Maschine *deaktiviert* sein.
- Zur erfolgreichen Installation auf einer Remote-Maschine, die *kein* Mitglied einer Active Directory-Domain ist, muss auf dieser Maschine die Benutzerkontensteuerung (UAC) *deaktiviert sein*. Weitere Informationen darüber, wie Sie diese Funktion deaktivieren können, finden im Abschnitt 'Anforderungen an die Benutzerkontensteuerung (UAC)' –> 'So können Sie die UAC deaktivieren'.
- Um die Remote-Installation auf einer Windows-Maschine durchführen zu können, werden standardmäßig die Anmeldedaten des integrierten Administratorkontos benötigt. Um eine Remote-Installation mit den Anmeldedaten eines anderen Administratorkontos durchführen zu können, müssen die Remote-Beschränkungen der Benutzerkontensteuerung (UAC) *deaktiviert* sein. Weitere Informationen darüber, wie Sie diese deaktivieren können, finden im Abschnitt 'Anforderungen an die Benutzerkontensteuerung (UAC)' –> 'So können Sie die UAC-Remote-Beschränkungen deaktivieren'.
- Auf der Remote-Maschine muss die Datei- und Druckerfreigabe *aktiviert* sein. So erhalten Sie Zugriff auf diese Option:
  - Auf einer Maschine, die unter Windows 2003 Server läuft: gehen Sie zu **Systemsteuerung** > **Windows-Firewall** > **Ausnahmen** > **Datei- und Druckerfreigabe**.
  - Auf einer Maschine, die unter Windows Server 2008, Windows 7 oder höher läuft: gehen Sie zu **Systemsteuerung** > **Windows-Firewall** > **Netzwerk- und Freigabecenter** > **Erweiterte Freigabeeinstellungen ändern**.
- Cyber Protection verwendet zur Remote-Installation die TCP-Ports 445, 25001 und 43234.

  Port 445 wird automatisch geöffnet, wenn Sie die Datei- und Drucker-Freigabe aktivieren. Ports 43234 und 25001 werden automatisch durch die Windows-Firewall geöffnet. Stellen Sie bei

Verwendung einer anderen Firewall sicher, dass diese drei Ports für ein- und ausgehende Anfragen geöffnet sind (indem Sie den 'Ausnahmen' hinzugefügt werden).

Nach Abschluss der Remote-Installation wird der Port 25001 automatisch von der Windows-Firewall geschlossen. Die Ports 445 und 43234 müssen offen bleiben, wenn Sie zukünftig irgendwann ein Remote-Update des Agenten durchführen wollen. Der Port 25001 wird von der Windows Firewall bei jedem Update automatisch geöffnet und wieder geschlossen. Wenn Sie eine andere Firewall verwenden, sollten Sie alle drei Ports geöffnet lassen.

Anforderungen an die Benutzerkontensteuerung (UAC)

Die zentralen Verwaltungsaktionen (einschließlich der Remote-Installationen) erfordern bei Maschinen, die unter Windows 7 und höher laufen und kein Mitglied einer Active Directory-Domain sind, dass die Benutzerkontensteuerung (UAC) und deren Remote-Beschränkungen deaktiviert ist.

So deaktivieren Sie UAC

Führen Sie in Abhängigkeit vom vorliegenden Betriebssystem einen der nachfolgenden Schritte aus:

- **Bei einem Windows-Betriebssystem vor Windows 8:**
  Gehen Sie zur **Systemsteuerung –> Anzeige: Kleine Symbole –> Benutzerkonten –> Einstellungen der Benutzerkontensteuerung ändern** und ziehen Sie den Schieber auf **Nie benachrichtigen**. Starten Sie die Maschine dann neu.
- **Bei jedem anderen Windows-Betriebssystem**:
  1. Öffnen Sie den Registrierungseditor.
  2. Suchen Sie folgenden Registry-Schlüssel: **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System**
  3. Ändern Sie für den Wert **EnableLUA** die Einstellung auf **0**.
  4. Starten Sie die Maschine neu.

So können Sie die UAC-Remote-Beschränkungen deaktivieren

1. Öffnen Sie den Registrierungseditor.
2. Suchen Sie folgenden Registry-Schlüssel: **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System**
3. Ändern Sie für den Wert **LocalAccountTokenFilterPolicy** die Einstellung auf **1**.
   Wenn der Wert '**LocalAccountTokenFilterPolicy**' nicht vorhanden ist, erstellen Sie diesen als DWORD (32 Bit). Weitere Informationen zu diesem Wert finden Sie in der Microsoft-Dokumentation: https://support.microsoft.com/de-de/help/951016/description-of-user-account-control-and-remote-restrictions-in-windows.

Hinweis
Aus Sicherheitsgründen empfehlen wir, dass Sie nach Abschluss der Verwaltungsaktion (z.B. einer Remote-Installation) beide Einstellungen auf ihren ursprünglichen Zustand zurücksetzen: **EnableLUA**=**1** und **LocalAccountTokenFilterPolicy** = **0**

Zu installierende Komponenten auswählen

In der folgenden Tabelle finden Sie eine Beschreibung der zwingend erforderlichen und zusätzlichen Komponenten:

Komponente	Beschreibung
Obligatorische Komponente	
Agent für Windows	Dieser Agent sichert Laufwerke, Volumes und Dateien und wird auf Windows-Maschinen installiert. Er wird immer installiert und ist nicht auswählbar.
Zusätzliche Komponenten	
Agent für Data Loss Prevention	Dieser Agent ermöglicht es Ihnen, Benutzerzugriffe auf lokale oder umgeleitete Peripheriegeräte, auf Ports sowie die Zwischenablage von Maschinen mithilfe von Schutzplänen zu beschränken. Er wird installiert, sofern er ausgewählt wurde.
Antimalware Protection und URL-Filterung	Diese Komponente aktiviert das Antivirus & Antimalware Protection-Modul und das URL-Filterung-Modul in Schutzplänen. Auch wenn Sie erst einmal festlegen, dass diese Module nicht installiert werden sollen, werden diese später doch automatisch installiert, wenn eines der Module in einem Schutzplan für die entsprechende Maschine aktiviert wird.
Agent für Hyper-V	Dieser Agent sichert virtuellen Hyper-V-Maschinen und wird auf Hyper-V-Hosts installiert. Er wird installiert, sofern er ausgewählt wurde und auf einer Maschine eine Hyper-V-Rolle gefunden hat.
Agent für SQL	Dieser Agent sichert SQL Server-Datenbanken und wird auf Maschinen installiert, auf denen der Microsoft SQL Server ausgeführt wird. Er wird installiert, sofern er ausgewählt wurden und die entsprechende Applikation auf einer Maschine gefunden wurde.
Agent für Exchange	Dieser Agent sichert Exchange-Datenbanken sowie -Postfächer und wird auf Maschinen installiert, auf denen die Postfachrolle des Microsoft Exchange Servers ausgeführt wird. Er wird installiert, sofern er ausgewählt wurden und die entsprechende Applikation auf einer Maschine gefunden wurde.
Agent für Active Directory	Dieser Agent sichert die Daten von Active Directory-Domänendiensten und wird auf Domain Controllern installiert. Er wird installiert, sofern er ausgewählt wurden und die entsprechende Applikation auf einer Maschine gefunden wurde.
Agent für VMware (Windows)	Dieser Agent sichert virtuelle VMware-Maschinen und wird auf Windows-Maschinen installiert, die Netzwerkzugriff auf vCenter Server haben. Er wird installiert, sofern er ausgewählt wurde.
Agent für Microsoft 365	Dieser Agent sichert Microsoft 365-Postfächer zu einem lokalen Backup-Ziel und wird auf Windows-Maschinen installiert. Er wird installiert, sofern er ausgewählt wurde.
Agent für Oracle	Dieser Agent sichert Oracle-Datenbanken und wird auf Maschinen mit Oracle Database installiert. Er wird installiert, sofern er ausgewählt wurde.

Cyber Protection Monitor	Diese Komponente ermöglicht es einem Benutzer, die Ausführung laufender Tasks im Infobereich der Taskleiste zu überwachen, und wird auf Windows-Maschinen installiert. Er wird installiert, sofern er ausgewählt wurde. Unterstützt unter Windows 7 Service Pack 1 und höher sowie Windows Server 2008 R2 Service Pack 1 und höher.

Erkannte Maschinen verwalten

Nachdem ein Erkennungsprozess durchgeführt wurde, können Sie alle erkannten Maschinen im Bereich **Geräte** –> **Nicht verwaltete Maschinen** finden.

Dieser Bereich ist nach der verwendeten Erkennungsmethode in Unterbereiche aufgeteilt. Eine vollständige Liste der Maschinenparameter ist unten dargestellt (sie können je nach Entdeckungsmethode variieren).

Name	Beschreibung
Name	Der Name der Maschine. Wenn der Name der Maschine nicht ermittelt werden konnte, wird ihre IP-Adresse angezeigt.
IP-Adresse	Die IP-Adresse der Maschine.
Erkennungstyp	Die Erkennungsmethode, die zum Auffinden der Maschine verwendet wurde.
Organisationseinheit	Die Organisationseinheit im Active Directory, zu der die Maschine gehört. Diese Spalte wird angezeigt, wenn Sie die Liste der Maschinen in **Nicht verwaltete Maschinen** –> **Active Directory** einsehen.
Betriebssystem	Das auf der Maschine installierte Betriebssystem.

Es gibt einen Bereich **Ausnahmen**, wo Sie Maschinen hinzufügen können, die während des Erkennungsprozesses übersprungen werden sollen. Wenn Sie es z.B. für bestimmte Maschinen nicht benötigen, dass diese gefunden werden, können Sie diese in die Liste aufnehmen.

Wenn Sie eine Maschine in die **Ausnahmen** aufnehmen wollen, müssen Sie diese in der Liste auswählen und dann auf **Zu den Ausnahmen hinzufügen** klicken. Wenn Sie eine Maschine aus den **Ausnahmen** entfernen wollen, müssen Sie zu **Nicht verwaltete Maschinen** –> **Ausnahmen** gehen, die entsprechende Maschine auswählen und dann auf den Befehl **Aus den Ausnahmen entfernen** klicken.

Sie können den Protection Agenten installieren und die erkannten Maschinen in einem Batch in Cyber Protection installieren, indem Sie diese in der Liste auswählen und dann auf den Befehl **Installieren und registrieren** klicken. Im daraufhin geöffneten Assistenten können Sie außerdem den Maschinen auch stapelweise einen Schutzplan zuzuweisen.

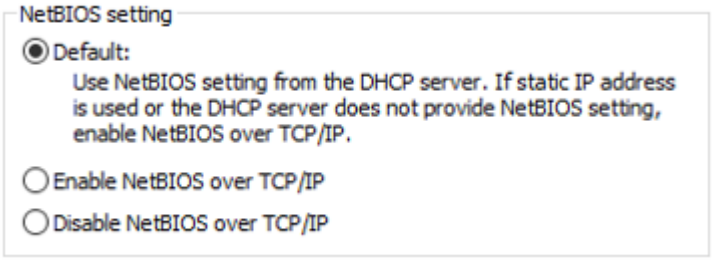
Diese Maschinen werden nach der Installation des Protection Agenten im Bereich **Geräte** –> **Maschinen mit Agenten** angezeigt.

Um Ihren Status zu überprüfen, gehen Sie zu **Monitoring** –> **Überblick** und fügen Sie dann das Widget **Sicherungsstatus** oder das Widget **Erkannte Maschinen** hinzu.

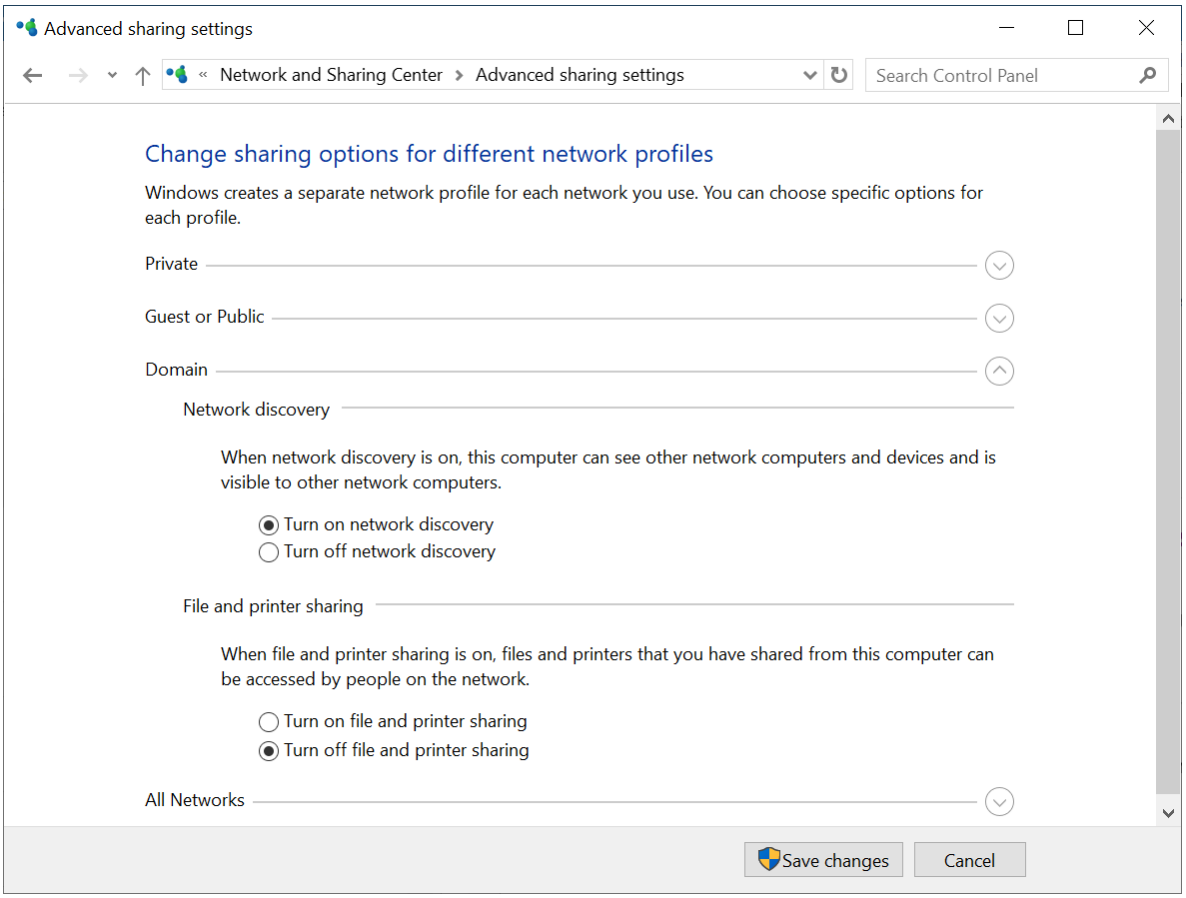
Problembehebung (Troubleshooting)

Wenn Sie ein Problem mit der automatischen Erkennungsfunktion haben, sollten Sie versuchen, Folgendes zu überprüfen:

- Überprüfen Sie, dass 'NetBIOS über TCP/IP' aktiviert oder als Standard aktiviert ist.



- Schalten Sie unter 'Systemsteuerung\Netzwerk- und Freigabecenter\Erweiterte Freigabeeinstellungen ändern' (von Windows) die Netzwerkerkennung ein.



- Überprüfen Sie, dass der 'Hostdienst für den Funktionssuchanbieter' (von Windows) auf der Maschine läuft, die die Erkennung durchführt, und zudem auf den Maschinen, die erkannt werden sollen.

- Überprüfen Sie, dass der 'Dienst zur Funktionssuche-Ressourcenveröffentlichung' (von Windows) auf den Maschinen läuft, die erkannt werden sollen.

Den Agenten für VMware (Virtuelle Appliance) bereitstellen

Bevor Sie beginnen

Systemanforderungen für den Agenten

Standardmäßig werden der virtuellen Appliance 4 GB RAM und 2 vCPUs zugeordnet, was für die meisten Aktionen optimal und ausreichend ist.

Um die Backup-Performance zu verbessern und Fehler durch zu wenig Arbeitsspeicher zu vermeiden, empfehlen wir für anspruchsvollere Fälle, diese Ressourcen auf 4 vCPUs und 16 GB RAM zu erhöhen. Wenn Sie beispielsweise erwarten, dass der Backup-Datenverkehr 100 MB pro Sekunde überschreitet (z.B. in 10-Gigabit-Netzwerken) oder wenn Sie mehrere virtuelle Maschinen mit großen Festplatten (500 GB oder mehr) gleichzeitig sichern wollen, sollten Sie die zugewiesenen Ressourcen erhöhen.

Die eigenen virtuellen Laufwerke der Appliance belegen nicht mehr als 6 GB. Das Laufwerksformat (ob „Thick“ oder „Thin“) spielt keine Rolle und hat daher keinen Einfluss auf die Performance der Appliance.

Wie viele Agenten benötige ich?

Obwohl bereits eine virtuelle Appliance in der Lage ist, eine komplette vSphere-Umgebung zu sichern, hat es sich bewährt, je eine virtuelle Appliance pro vSphere-Cluster (oder pro Host, wenn es keine Cluster gibt) bereitzustellen. Dies ermöglicht schnellere Backups, weil die Appliance die gesicherten Laufwerke per HotAdd-Transport anschließen kann und der Backup-Verkehr daher von einem lokalen Laufwerk zu einem anderen weitergeleitet wird.

Es ist normal, sowohl die virtuelle Appliance als auch den Agenten für VMware (Windows) gleichzeitig zu verwenden, sofern diese mit demselben vCenter Server *oder* mit verschiedenen ESXi-Hosts verbunden sind. Vermeiden Sie Situationen, bei denen ein Agent direkt mit einem ESXi-Host und ein anderer Agent mit dem vCenter Server verbunden ist, der diesen ESXi-Host verwaltet.

Sie sollten keinen lokal angeschlossenen Storage verwenden (also Backups auf virtuellen Laufwerken speichern, die an die virtuelle Appliance angeschlossen sind), wenn Sie mehr als einen Agenten haben. Weitere Informationen und Überlegungen dazu finden Sie im Abschnitt '"Einen lokal angeschlossenen Storage verwenden" (S. 759)'.

Automatischen DRS (Distributed Resource Scheduler) für den Agenten deaktivieren

Wenn die virtuelle Appliance in einem vSphere-Cluster bereitgestellt wird, sollten Sie überprüfen, dass für diesen die Funktion 'automatisches vMotion' deaktiviert ist. Aktivieren Sie in den DRS-Einstellungen des Clusters einzelne Automatisierungslevel für jede virtuelle Maschine und schalten Sie den **Automatisierungslevel** für die virtuelle Appliance auf **Deaktiviert**.

Deployment der OVF-Vorlage

1. Klicken Sie auf **Alle Geräte** –> **Hinzufügen** –> **VMware ESXi** –> **Virtuelle Appliance (OVF)**.
   Das .zip-Archiv wird zu Ihrer Maschine heruntergeladen.
2. Entpacken Sie das .zip-Archiv. Der Ordner enthält eine .ovf-Datei und zwei .vmdk-Dateien.
3. Stellen Sie sicher, dass die Maschine, die den vSphere Client ausführt, auf diese Dateien zugreifen kann.
4. Starten Sie den vSphere Client und melden Sie sich am vCenter Server an.
5. Führen ein Deployment der OVF-Vorlage durch.
   - Wählen Sie beim Konfigurieren des Storage den gemeinsam genutzten Datenspeicher (sofern vorhanden). Das Laufwerksformat (ob „Thick“ oder „Thin“) spielt keine Rolle und hat daher keinen Einfluss auf die Performance der Appliance.
   - Achten Sie beim Konfigurieren der Netzwerkverbindungen darauf, ein Netzwerk auszuwählen, das eine Internetverbindung zulässt, damit sich der Agent korrekt in der Cloud registrieren kann.

Die virtuelle Appliance konfigurieren

Nach der Bereitstellung der virtuellen Appliance müssen Sie diese so konfigurieren, dass sie auf den vCenter Server oder den ESXi-Host sowie auf den Cyber Protection Service zugreifen kann.

So konfigurieren Sie die virtuelle Appliance

1. Öffnen Sie im vSphere Client die Konsole der virtuellen Appliance.
2. Überprüfen Sie, dass die Netzwerkverbindung richtig konfiguriert ist.
   Die Verbindung wird automatisch per DHCP (Dynamic Host Configuration Protocol) konfiguriert.
   Wenn Sie die Standardkonfiguration ändern wollen, klicken Sie unter **Agentenoptionen** im Feld **eth0** auf den Befehl **Ändern** und spezifizieren dann die gewünschten Netzwerkeinstellungen.
3. Verbinden Sie die virtuelle Appliance mit dem vCenter Server oder dem ESXi-Host.
   a. Klicken Sie unter **Agentenoptionen**, im Feld **vCenter/ESX(i)**, den Befehl **Ändern** und spezifizieren Sie dann die nachfolgenden Einstellungen.
      - [Wenn Sie einen vCenter Server verwenden] Den Namen oder die IP-Adresse des vCenter Servers.

- [Wenn Sie keinen vCenter Server verwenden] Den Namen oder die IP-Adresse desjenigen ESXi-Hosts, auf dem Sie virtuelle Maschinen sichern und wiederherstellen wollen. Für schnellere Backups sollten Sie die virtuelle Appliance auf demselben Host bereitstellen.
- Die für die Appliance erforderlichen Anmeldedaten, um eine Verbindung zum vCenter Server oder zum ESXi-Host herstellen zu können.

  Wir empfehlen, dass Sie für den Zugriff auf den vCenter Server oder den ESXi Host ein dediziertes Konto verwenden, anstatt ein bereits vorhandenes Konto mit der Administrator-Rolle zu verwenden. Weitere Informationen zu den erforderlichen Berechtigungen für das dedizierte Konto finden Sie im Abschnitt '"Agent für VMware – notwendige Berechtigungen" (S. 766)'.

b. Klicken Sie auf **Verbindung prüfen**, um zu kontrollieren, ob die Einstellungen richtig sind.

c. Klicken Sie auf **OK**.

4. Registrieren Sie die Appliance im Cyber Protection Service, indem Sie eine der folgenden Methoden anwenden.
   - [Nur für Mandanten ohne Zwei-Faktor-Authentifizierung] Registrieren Sie die Appliance in ihrer grafischen Oberfläche.
     a. Klicken Sie bei **Agent-Optionen** im Feld **Management Server** auf den Befehl **Ändern**.
     b. Wählen Sie im Feld **Server-Name/IP** die Option **Cloud**.

        Die Adresse des Cyber Protection Service wird angezeigt. Ändern Sie diese Adresse nicht, solange es keine anderslautenden Anweisungen gibt.
     c. Spezifizieren Sie in die Felder **Benutzername** und **Kennwort** die Anmeldedaten für Ihr Konto im Cyber Protection Service ein. Die virtuelle Appliance und die virtuellen Maschinen, die von der Appliance verwaltet werden, sind unter diesem Konto registriert.
     d. Klicken Sie auf **OK**.
   - Registrieren Sie die Appliance in der Befehlszeilenschnittstelle.

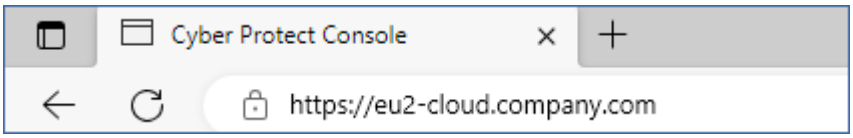
     Hinweis
     Für diese Methode benötigen Sie einen Registrierungstoken. Weitere Informationen darüber, wie Sie ein solches generieren können, finden Sie im Abschnitt '"Ein Registrierungstoken generieren" (S. 182)'.

     a. Drücken Sie STRG+UMSCHALT+F2, um die Befehlszeilenschnittstelle zu öffnen.
     b. Führen Sie folgenden Befehl aus:

        ```
        register_agent -o register -t cloud -a <service address> --token <registration token>
        ```

Hinweis

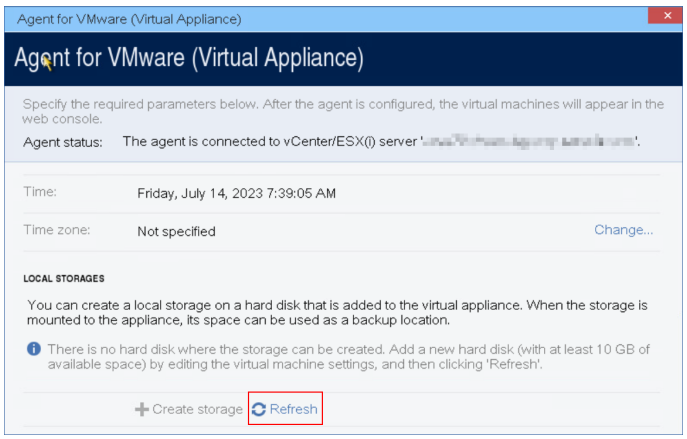
Wenn Sie ein Registrierungstoken verwenden, müssen Sie die genaue Datacenter-Adresse spezifizieren. Dies ist die URL, die Sie sehen, sobald Sie sich an der Cyber Protect-Konsole **angemeldet haben**. Beispielsweise `https://eu2-cloud.company.com`.



Sie dürfen hier nicht die Adresse `https://cloud.company.com` verwenden.

c. Drücken Sie die Tastenkombination ALT+F1, um zur grafischen Oberfläche der Appliance zurückzukehren.

5. [Optional] Fügen Sie einen lokalen Storage hinzu.
   a. Schließen Sie im vSphere Client ein virtuelles Laufwerk an die virtuelle Appliance an. Das virtuelle Laufwerk muss über mindestens 10 GB freien Speicherplatz verfügen.
   b. Klicken Sie in der grafischen Benutzeroberfläche der Appliance auf den Befehl **Aktualisieren**.



   Die Schaltfläche **Storage erstellen** wird aktiviert.
   c. Klicken Sie auf **Storage erstellen**.
   d. Spezifizieren Sie eine Bezeichnung für den Storage und klicken Sie dann auf **OK**.
   e. Bestätigen Sie Ihre Wahl durch Klicken auf **Ja**.
6. [Falls in Ihrem Netzwerk ein Proxy-Server verwendet wird] Konfigurieren Sie den Proxy-Server.
   a. Drücken Sie STRG+UMSCHALT+F2, um die Befehlszeilenschnittstelle zu öffnen.
   b. Öffnen Sie die Datei **/etc/Acronis/Global.config** in einem Text-Editor.
   c. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
      - Wenn die Proxy-Einstellungen während der Installation des Agenten spezifiziert wurden, suchen Sie nach dem folgenden Abschnitt:

```
<key name="HttpProxy">
    <value name="Enabled" type="Tdword">"1"</value>
    <value name="Host" type="TString">"ADDRESS"</value>
    <value name="Port" type="Tdword">"PORT"</value>
    <value name="Login" type="TString">"LOGIN"</value>
```

```
    <value name="Password" type="TString">"PASSWORD"</value>
</key>
```

- Sie können die obigen Zeilen auch kopieren und in die Datei zwischen den Tags '`<registry name="Global">...</registry>`' einfügen.

d. Ersetzen Sie `ADDRESS` mit dem Host-Namen/der IP-Adresse des neuen Proxy-Servers – und `PORT` mit dem Dezimalwert der dazugehörigen Port-Nummer.

e. Wenn Ihr Proxy-Server eine Authentifizierung benötigt, ersetzen Sie `LOGIN` und `PASSWORD` mit den entsprechenden Anmeldedaten des Proxy-Servers. Anderenfalls können Sie diese Zeilen aus der Datei löschen.

f. Speichern Sie die Datei.

g. Öffnen Sie die Datei **/opt/acronis/etc/aakore.yaml** in einem Text-Editor.

h. Suchen Sie den Abschnitt **env** (oder erstellen Sie diesen) und fügen Sie dann folgende Zeilen hinzu:

```
env:
    http-proxy: proxy_login:proxy_password@proxy_address:port
    https-proxy: proxy_login:proxy_password@proxy_address:port
```

i. Ersetzen Sie `proxy_login` und `proxy_password` mit den Anmeldedaten des Proxy-Servers – und `proxy_address:port` mit der Adresse und der Port-Nummer des Proxy-Servers.

j. Führen Sie den Befehl `reboot` aus:

Hinweis

Wenn Sie eine virtuelle Appliance aktualisieren wollen, die hinter einem Proxy bereitgestellt wurde, müssen Sie auf der Appliance die Datei `config.yaml` (unter `/opt/acronis/etc/va-updater/config.yaml`) bearbeiten, indem Sie folgende Zeile am Ende der Datei hinzufügen und dann die Werte eingeben, die für Ihre Umgebung gelten:

```
httpProxy: http://<proxy_login>:<proxy_password>@<proxy_address>:<port>
```

Beispiel:

```
httpProxy: http://mylogin:mypassword@192.168.2.300:8080
```

Den Agenten für Scale Computing HC3 (Virtuelle Appliance) bereitstellen

Bevor Sie beginnen

Diese Appliance ist eine vorkonfigurierte virtuelle Maschine, die Sie in einem Scale Computing HC3-Cluster bereitstellen können. Sie enthält einen Protection Agenten, der es Ihnen ermöglicht, die Cyber Protection-Funktionalität für alle virtuellen Maschinen in dem Cluster zu verwalten.

Systemanforderungen für den Agenten

Standardmäßig verwendet die virtuelle Maschine mit dem Agenten zwei (2) vCPUs und vier (4) GiB RAM. Diese Einstellungen sind für die meisten Operationen ausreichend. Sie können die Einstellungen jedoch ändern, indem Sie die virtuelle Maschine in der Scale Computing HC3-Weboberfläche bearbeiten.

Um die Backup-Performance zu verbessern und Fehler durch zu wenig Arbeitsspeicher zu vermeiden, empfehlen wir für anspruchsvollere Fälle, diese Ressourcen auf 4 vCPUs und 8 GiB RAM zu erhöhen. Wenn Sie beispielsweise erwarten, dass der Backup-Datenverkehr 100 MB pro Sekunde überschreitet (z.B. in 10-Gigabit-Netzwerken) oder wenn Sie mehrere virtuelle Maschinen mit großen Festplatten (500 GB oder mehr) gleichzeitig sichern wollen, sollten Sie die zugewiesenen Ressourcen erhöhen.

Die Größe des virtuellen Laufwerks der Appliance beträgt ca. 9 GB.

Wie viele Agenten benötige ich?

Ein Agent kann den kompletten Cluster schützen. Sie können jedoch mehr als einen Agenten im Cluster verwenden, wenn Sie die Bandbreitenbelastung des Backup-Datenverkehrs verteilen wollen.

Wenn Sie mehr als einen Agenten in einem Cluster haben, werden die virtuellen Maschinen automatisch gleichmäßig zwischen den Agenten verteilt, sodass jeder Agent eine ähnliche Anzahl von Maschinen verwaltet.

Wenn es bei der Auslastung zwischen den Agenten zu einem Ungleichgewicht von über 20% kommt, erfolgt eine automatische Neuverteilung. Dazu kann es kommen, nachdem Sie eine Maschine oder einen Agent hinzugefügt oder entfernt haben. Beispielsweise, wenn Sie erkennen, dass Sie mehr Agenten zur Unterstützung des Durchsatzes benötigen, und eine virtuelle Appliance auf einen Cluster bereitstellen. Der Management Server wird die geeignetsten Maschinen dem neuen Agenten zuweisen. Die Last der alten Agenten wird reduziert. Wenn Sie einen Agenten vom Management Server entfernen, dann werden die diesem Agenten zugewiesenen Maschinen unter den verbliebenen Agenten neu verteilt. Diese passiert jedoch nicht, wenn ein Agent beschädigt wird oder manuell aus dem Scale Computing HC3-Cluster gelöscht wird. Eine Neuverteilung wird in diesem Fall nur dann gestartet, wenn Sie einen solchen Agenten über die Cyber Protect-Konsole entfernen.

So können Sie überprüfen, welcher Agent eine bestimmte Maschine verwaltet

1. Klicken Sie zuerst in der Cyber Protect-Konsole auf **Geräte** und wählen Sie dann den Eintrag **Scale Computing**.
2. Klicken Sie in der rechten oberen Ecke der Tabelle auf das Zahnradsymbol und aktivieren Sie unter **System** das Kontrollkästchen **Agent**.
3. Kontrollieren Sie den Namen des Agenten in der angezeigten Spalte.

Die QCOW2-Vorlage bereitstellen

1. Melden Sie sich an Ihrem Cyber Protection Konto an.
2. Klicken Sie auf **Geräte** –> **Alle Geräte** –> **Hinzufügen** –> **Scale Computing HC3**.
   Das .zip-Archiv wird zu Ihrer Maschine heruntergeladen.
3. Entpacken Sie das .zip-Archiv und speichern Sie dann die .qcow2- und .xml-Datei in einem Ordner namens **ScaleAppliance**.
4. Laden Sie den **ScaleAppliance**-Ordner zu einer Netzwerkfreigabe hoch und stellen Sie sicher, dass der Scale Computing HC3-Cluster darauf zugreifen kann.
5. Melden Sie sich am Scale Computing HC3-Cluster als Administrator an, dem die Rolle **VM erstellen/bearbeiten** zugewiesen wurde. Weitere Informationen zu den Rollen, die für Aktionen mit virtuellen Scale Computing HC3-Maschinen erforderlich sind, finden Sie in Abschnitt '"Agent für Scale Computing HC3 – erforderliche Rollen" (S. 156)'.
6. Importieren Sie in der Scale Computing HC3-Weboberfläche die Virtuelle-Maschinen-Vorlage aus dem **ScaleAppliance**-Ordner.
   a. Klicken Sie auf das Symbol **HC3-VM importieren**.
   b. Spezifizieren Sie im Fenster **HC3-VM importieren** Folgendes:
      - Einen Namen für die neue virtuelle Maschine.
      - Die Netzwerkfreigabe, auf der sich der **ScaleAppliance**-Ordner befindet.
      - Die Anmeldedaten (Benutzername, Kennwort), die für den Zugriff auf diese Netzwerkfreigabe erforderlich sind.
      - [Optional] Ein Domain-Tag für die neue virtuelle Maschine.
      - Den Pfad zum **ScaleAppliance**-Ordner auf der Netzwerkfreigabe.
   c. Klicken Sie auf **Importieren**.

Nachdem die Bereitstellung abgeschlossen wurde, müssen Sie die virtuelle Appliance konfigurieren. Weitere Informationen zu deren Konfiguration finden Sie im Abschnitt '"Die virtuelle Appliance konfigurieren" (S. 153)'.

Hinweis
Wenn Sie mehr als eine virtuelle Appliance in Ihrem Cluster benötigen, müssen Sie die oberen Schritte wiederholen und dabei weitere virtuelle Appliances bereitstellen. Sie sollten eine vorhandene virtuelle Appliance nicht klonen, indem Sie die Option **VM klonen** in der Scale Computing HC3-Weboberfläche verwenden.

Die virtuelle Appliance konfigurieren

Nachdem Sie die virtuelle Appliance bereitgestellt haben, müssen Sie diese so konfigurieren, dass sie sowohl den Scale Computing HC3-Cluster, der von ihr geschützt werden soll, als auch den Cyber Protection Service erreichen kann.

So konfigurieren Sie die virtuelle Appliance

1. Melden Sie sich an Ihrem Scale Computing HC3-Konto an.
2. Wählen Sie die virtuelle Appliance aus, die Sie konfigurieren wollen, und klicken Sie dann auf das Symbol **Konsole**.
3. Konfigurieren Sie im Feld **eth0** die Netzwerkschnittstellen der Appliance.

   Stellen Sie sicher, dass die automatisch zugewiesenen DHCP-Adressen (sofern vorhanden) in den von Ihrer virtuellen Maschine verwendeten Netzwerken gültig sind – oder weisen Sie alternativ die Adressen manuell zu. Abhängig von der Anzahl der Netzwerke, die die Appliance verwendet, müssen möglicherweise eine oder mehrere Schnittstellen konfiguriert werden.
4. Klicken Sie im Feld **Scale Computing** auf **Ändern**, um die Adresse des Scale Computing HC3-Clusters sowie die Anmeldedaten zu spezifizieren, um auf den Cluster zugreifen zu können.
   a. Geben Sie im Feld **Server-Name/IP** den DNS-Namen oder die IP-Adresse des Clusters ein.
   b. Geben Sie in die Felder **Benutzername** und **Kennwort** die Anmeldedaten für das Scale Computing HC3-Administratorkonto ein.

      Stellen Sie sicher, dass dieses Konto über die Rollen verfügt, die für Aktionen mit virtuellen Scale Computing HC3-Maschinen erforderlich sind. Weitere Informationen über diese Rollen finden Sie im Abschnitt '"Agent für Scale Computing HC3 – erforderliche Rollen" (S. 156)'.
   c. Klicken Sie auf **Verbindung prüfen**, um zu kontrollieren, ob die Einstellungen richtig sind.
   d. Klicken Sie auf **OK**.
5. Registrieren Sie die Appliance im Cyber Protection Service, indem Sie eine der folgenden Methoden anwenden.
   - [Nur für Mandanten ohne Zwei-Faktor-Authentifizierung] Registrieren Sie die Appliance in ihrer grafischen Oberfläche.
     a. Klicken Sie bei **Agent-Optionen** im Feld **Management Server** auf den Befehl **Ändern**.
     b. Wählen Sie im Feld **Server-Name/IP** die Option **Cloud**.

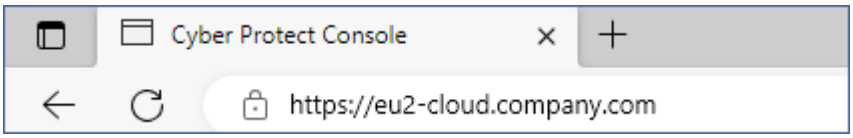
        Die Adresse des Cyber Protection Service wird angezeigt. Ändern Sie diese Adresse nicht, solange es keine anderslautenden Anweisungen gibt.
     c. Spezifizieren Sie in die Felder **Benutzername** und **Kennwort** die Anmeldedaten für Ihr Konto im Cyber Protection Service ein. Die virtuelle Appliance und die virtuellen Maschinen, die von der Appliance verwaltet werden, sind unter diesem Konto registriert.
     d. Klicken Sie auf **OK**.
   - Registrieren Sie die Appliance in der Befehlszeilenschnittstelle.

     Hinweis
     Für diese Methode benötigen Sie einen Registrierungstoken. Weitere Informationen darüber, wie Sie ein solches generieren können, finden Sie im Abschnitt '"Ein Registrierungstoken generieren" (S. 182)'.

     a. Drücken Sie STRG+UMSCHALT+F2, um die Befehlszeilenschnittstelle zu öffnen.
     b. Führen Sie folgenden Befehl aus:

```
register_agent -o register -t cloud -a <service address> --token <registration
token>
```

Hinweis
Wenn Sie ein Registrierungstoken verwenden, müssen Sie die genaue Datacenter-Adresse spezifizieren. Dies ist die URL, die Sie sehen, sobald Sie sich an der Cyber Protect-Konsole **angemeldet haben**. Beispielsweise `https://eu2-cloud.company.com`.



Sie dürfen hier nicht die Adresse `https://cloud.company.com` verwenden.

c. Drücken Sie die Tastenkombination ALT+F1, um zur grafischen Oberfläche der Appliance zurückzukehren.

6. [Optional] Klicken Sie im Feld **Name** auf **Ändern**, um den Standardnamen für die virtuelle Appliance zu bearbeiten, der **localhost** lautet. Der Name wird in der Cyber Protect-Konsole angezeigt.
7. [Optional] Klicken Sie im Feld **Zeit** auf **Ändern** und wählen Sie dann die Zeitzone Ihres Standortes aus, um sicherzustellen, dass die geplanten Aktionen zur korrekten Zeit ausgeführt werden.
8. [Falls in Ihrem Netzwerk ein Proxy-Server verwendet wird] Konfigurieren Sie den Proxy-Server.
   a. Drücken Sie STRG+UMSCHALT+F2, um die Befehlszeilenschnittstelle zu öffnen.
   b. Öffnen Sie die Datei **/etc/Acronis/Global.config** in einem Text-Editor.
   c. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
      - Wenn die Proxy-Einstellungen während der Installation des Agenten spezifiziert wurden, suchen Sie nach dem folgenden Abschnitt:

```
<key name="HttpProxy">
    <value name="Enabled" type="Tdword">"1"</value>
    <value name="Host" type="TString">"ADDRESS"</value>
    <value name="Port" type="Tdword">"PORT"</value>
    <value name="Login" type="TString">"LOGIN"</value>
    <value name="Password" type="TString">"PASSWORD"</value>
</key>
```

      - Sie können die obigen Zeilen auch kopieren und in die Datei zwischen den Tags '`<registry name="Global">...</registry>`' einfügen.

   d. Ersetzen Sie `ADDRESS` mit dem Host-Namen/der IP-Adresse des neuen Proxy-Servers – und `PORT` mit dem Dezimalwert der dazugehörigen Port-Nummer.
   e. Wenn Ihr Proxy-Server eine Authentifizierung benötigt, ersetzen Sie `LOGIN` und `PASSWORD` mit den entsprechenden Anmeldedaten des Proxy-Servers. Anderenfalls können Sie diese Zeilen aus der Datei löschen.
   f. Speichern Sie die Datei.

g. Öffnen Sie die Datei **/opt/acronis/etc/aakore.yaml** in einem Text-Editor.

h. Suchen Sie den Abschnitt **env** (oder erstellen Sie diesen) und fügen Sie dann folgende Zeilen hinzu:

```
env:
    http-proxy: proxy_login:proxy_password@proxy_address:port
    https-proxy: proxy_login:proxy_password@proxy_address:port
```

i. Ersetzen Sie `proxy_login` und `proxy_password` mit den Anmeldedaten des Proxy-Servers – und `proxy_address:port` mit der Adresse und der Port-Nummer des Proxy-Servers.

j. Führen Sie den Befehl `reboot` aus:

Hinweis

Wenn Sie eine virtuelle Appliance aktualisieren wollen, die hinter einem Proxy bereitgestellt wurde, müssen Sie auf der Appliance die Datei `config.yaml` (unter `/opt/acronis/etc/va-updater/config.yaml`) bearbeiten, indem Sie folgende Zeile am Ende der Datei hinzufügen und dann die Werte eingeben, die für Ihre Umgebung gelten:

```
httpProxy: http://<proxy_login>:<proxy_password>@<proxy_address>:<port>
```

Beispiel:

```
httpProxy: http://mylogin:mypassword@192.168.2.300:8080
```

So können Sie virtuelle Maschinen im Scale Computing HC3-Cluster schützen

1. Melden Sie sich an Ihrem Cyber Protection Konto an.
2. Gehen Sie zu **Geräte** –> **Scale Computing HC3** –> <Ihr Cluster> – oder suchen Sie Ihre Maschinen unter **Geräte** –> **Alle Geräte**.
3. Wählen Sie die Maschinen aus und wenden Sie einen Schutzplan auf diese an.

Agent für Scale Computing HC3 – erforderliche Rollen

Dieser Abschnitt beschreibt die Rollen, die für Aktionen mit virtuellen Scale Computing HC3-Maschinen erforderlich sind.

Aktion	Rolle
Backup einer virtuellen Maschine	Backup VM erstellen/bearbeiten VM löschen
Recovery zu einer existierenden virtuellen Maschine	Backup VM erstellen/bearbeiten

	VM-Energiesteuerung VM löschen Cluster-Einstellungen
Recovery zu einer neuen virtuellen Maschine	Backup VM erstellen/bearbeiten VM-Energiesteuerung VM löschen Cluster-Einstellungen

Den Agenten für Virtuozzo Hybrid Infrastructure (Virtuelle Appliance) bereitstellen

Bevor Sie beginnen

Diese Appliance ist eine vorkonfigurierte virtuelle Maschine, die Sie in Virtuozzo Hybrid Infrastructure bereitstellen können. Sie enthält einen Protection Agenten, der es Ihnen ermöglicht, die Cyber Protection-Funktionalität für alle virtuellen Maschinen in einem Virtuozzo Hybrid Infrastructure-Cluster zu verwalten.

Hinweis
Wenn Sie gewährleisten wollen, dass Backups mit aktivierter Backup-Option **VSS (Volume Shadow Copy Service) für virtuelle Maschinen** ordnungsgemäß ausgeführt werden und die Daten in einem applikationskonsistenten Zustand erfasst werden, müssen Sie sicherstellen, dass die Virtuozzo Guest Tools auf den geschützten virtuellen Maschinen installiert und aktuell sind.

Systemanforderungen für den Agenten

Wenn Sie die virtuelle Appliance bereitstellen, können Sie zwischen verschiedenen vordefinierten Kombinationen von vCPUs und RAM wählen. Diese vordefinierten Kombinationen werden 'Varianten' (Englisch: Flavor) genannt. Sie können auch Ihre eigenen Varianten erstellen.

2 vCPUs und 4 GB RAM (mittlere Variante) sind für die meisten Operationen optimal und ausreichend. Um die Backup-Performance zu verbessern und Fehler durch zu wenig Arbeitsspeicher zu vermeiden, empfehlen wir für anspruchsvollere Fälle, diese Ressourcen auf 4 vCPUs und 8 GB RAM zu erhöhen. Wenn Sie beispielsweise erwarten, dass der Backup-Datenverkehr 100 MB pro Sekunde überschreitet (z.B. in 10-Gigabit-Netzwerken) oder wenn Sie mehrere virtuelle Maschinen mit großen Festplatten (500 GB oder mehr) gleichzeitig sichern wollen, sollten Sie die zugewiesenen Ressourcen erhöhen.

Wie viele Agenten benötige ich?

Ein Agent kann den kompletten Cluster schützen. Sie können jedoch mehr als einen Agenten im Cluster verwenden, wenn Sie die Bandbreitenbelastung des Backup-Datenverkehrs verteilen wollen.

Wenn Sie mehr als einen Agenten in einem Cluster haben, werden die virtuellen Maschinen automatisch gleichmäßig zwischen den Agenten verteilt, sodass jeder Agent eine ähnliche Anzahl von Maschinen verwaltet.

Wenn es bei der Auslastung zwischen den Agenten zu einem Ungleichgewicht von über 20% kommt, erfolgt eine automatische Neuverteilung. Dazu kann es kommen, nachdem Sie eine Maschine oder einen Agent hinzugefügt oder entfernt haben. Beispielsweise, wenn Sie erkennen, dass Sie mehr Agenten zur Unterstützung des Durchsatzes benötigen, und eine virtuelle Appliance auf einen Cluster bereitstellen. Der Management Server wird die geeignetsten Maschinen dem neuen Agenten zuweisen. Die Last der alten Agenten wird reduziert. Wenn Sie einen Agenten vom Management Server entfernen, dann werden die diesem Agenten zugewiesenen Maschinen unter den verbliebenen Agenten neu verteilt. Dies geschieht jedoch nicht, wenn ein Agent beschädigt wird oder manuell aus dem Virtuozzo Hybrid Infrastructure-Knoten gelöscht wird. Eine Neuverteilung wird in diesem Fall nur dann gestartet, wenn Sie einen solchen Agenten über die Cyber Protection-Weboberfläche entfernen.

So können Sie überprüfen, welcher Agent eine bestimmte Maschine verwaltet

1. Klicken Sie in der Cyber Protect-Konsole zuerst auf **Geräte** und wählen Sie dann **Virtuozzo Hybrid Infrastructure**.
2. Klicken Sie in der rechten oberen Ecke der Tabelle auf das Zahnradsymbol und aktivieren Sie unter **System** das Kontrollkästchen **Agent**.
3. Kontrollieren Sie den Namen des Agenten in der angezeigten Spalte.

Einschränkungen

- Die Virtuozzo Hybrid Infrastructure-Appliance kann nicht remote bereitgestellt werden.
- Applikationskonforme Backups von virtuellen Maschinen werden nicht unterstützt.

Netzwerke in Virtuozzo Hybrid Infrastructure konfigurieren

Bevor Sie die virtuelle Appliance bereitstellen und konfigurieren können, müssen Sie Ihre Netzwerke in Virtuozzo Hybrid Infrastructure konfiguriert haben.

Netzwerkanforderungen für den Agenten für Virtuozzo Hybrid Infrastructure (Virtuelle Appliance)

- Die virtuelle Appliance benötigt 2 Netzwerkadapter.
- Die virtuelle Appliance muss mit Virtuozzo-Netzwerken mit folgenden Netzwerk-Traffic-Typen verbunden sein:

- Compute-API
- VM-Backup
- ABGW öffentlich
- VM öffentlich

Weitere Informationen über die Konfiguration der Netzwerke finden Sie im Abschnitt 'Compute cluster requirements' (Compute-Cluster-Anforderungen) der englischsprachigen Virtuozzo-Dokumentation.

Benutzerkonten in Virtuozzo Hybrid Infrastructure konfigurieren

Um die virtuelle Appliance konfigurieren zu können, benötigen Sie ein Virtuozzo Hybrid Infrastructure-Benutzerkonto. Dieses Konto muss über die Rolle **Administrator** in der Domain **Default** (Standard) verfügen. Weitere Informationen über Benutzer finden Sie im Abschnitt 'Managing admin panel users' (Admin-Panel-Benutzer verwalten) in der englischsprachigen Virtuozzo Hybrid Infrastructure-Dokumentation. Stellen Sie sicher, dass Sie diesem Konto Zugriff auf alle Projekte in der Domain **Default** (Standard) gewährt haben.

So können Sie Zugriff auf alle Projekte in der Domain 'Default' (Standard) gewähren

1. Erstellen Sie eine Umgebungsdatei für den Systemadministrator. Führen Sie dafür das nachfolgende Skript im Virtuozzo Hybrid Infrastructure-Cluster über die OpenStack-Befehlszeilenschnittstelle aus. Weitere Informationen darüber, wie Sie eine Verbindung zu dieser Schnittstelle herstellen können, finden Sie in Abschnitt 'Connecting to OpenStack command-line interface' (Mit der OpenStack-Befehlszeilenschnittstelle verbinden) der englischsprachigen Virtuozzo Hybrid Infrastructure-Dokumentation.

   ```
   su - vstoradmin
   kolla-ansible post-deploy
   exit
   ```

2. Verwenden Sie die Umgebungsdatei, um weitere OpenStack-Befehle zu autorisieren:

   ```
   . /etc/kolla/admin-openrc.sh
   ```

3. Führen Sie folgende Befehle aus:

   ```
   openstack --insecure user set --project admin --project-domain Default --domain
   Default <username>
   openstack --insecure role add --domain Default --user <username> --user-domain
   Default compute --inherited
   ```

   Wobei <Benutzername> das Virtuozzo Hybrid Infrastructure-Konto mit der Rolle **Administrator** und der Domain **Default** (Standard) ist. Die virtuelle Appliance wird dieses Konto verwenden, um die virtuellen Maschinen in allen untergeordneten Projekten unter der Domain **Default** (Standard) sichern und wiederherstellen zu können.

Beispiel

```
su - vstoradmin
kolla-ansible post-deploy
exit
. /etc/kolla/admin-openrc.sh
openstack --insecure user set --project admin --project-domain Default --domain Default
johndoe
openstack --insecure role add --domain Default --user johndoe --user-domain Default
compute --inherited
```

Um Backups für virtuelle Maschinen in einer Domain verwalten zu können, die sich von der Domain **Default** (Standard) unterscheidet, müssen Sie auch den nachfolgenden Befehl ausführen.

So können Sie Zugriff auf alle Projekte in einer anderen Domain gewähren

```
openstack --insecure role add --domain <domain name> --inherited --user <username> --
user-domain Default admin
```

Wobei <Domain-Name> die Domain für die Projekte ist, in denen das Konto <Benutzername> Zugriff haben wird.

Beispiel

```
openstack --insecure role add --domain MyNewDomain --inherited --user johndoe --user-
domain Default admin
```

Nachdem Sie Zugriffe auf die Projekte gewährt haben, müssen Sie überprüfen, welche Rollen dem Konto zugewiesen wurden.

So können Sie zugewiesene Rollen überprüfen

```
openstack --insecure role assignment list --user <username> --names
```

Wobei <Benutzername> das Virtuozzo Hybrid Infrastructure-Konto ist.

Beispiel

```
openstack --insecure role assignment list --user johndoe --names -c Role -c User -c
Project -c Domain
+--------------+-----------------+---------+-------------+
| Role         | User            | Project | Domain      |
+--------------+-----------------+---------+-------------+
| admin        | johndoe@Default |         | MyNewDomain |
| compute      | johndoe@Default |         | Default     |
| domain_admin | johndoe@Default |         | Default     |
```

```
| domain_admin | johndoe@Default |         | Default     |
+--------------+-----------------+---------+-------------+
```

In diesem Beispiel werden die Optionen `-c Role`, `-c User`, `-c Project` und `-c Domain` verwendet, um die Befehlsausgabe so zu kürzen, dass diese auf die Seite passt.

Wenn Sie überprüfen wollen, welche effektiven Rollen dem Konto in allen Projekten zugewiesen wurden, führen Sie außerdem den nachfolgenden Befehl aus.

So können Sie die effektiven Rollen in allen Projekten überprüfen

```
openstack --insecure role assignment list --user <username> --names --effective
```

Wobei <Benutzername> das Virtuozzo Hybrid Infrastructure-Konto ist.

Beispiel

```
openstack --insecure role assignment list --user johndoe --names --effective  -c Role -c
User -c Project -c Domain
+--------------+-----------------+-----------------+---------+
| Role         | User            | Project         | Domain  |
+--------------+-----------------+-----------------+---------+
| domain_admin | johndoe@Default |                 | Default |
| compute      | johndoe@Default | admin@Default   |         |
| compute      | johndoe@Default | service@Default |         |
| domain_admin | johndoe@Default | admin@Default   |         |
| domain_admin | johndoe@Default | service@Default |         |
| project_user | johndoe@Default | service@Default |         |
| member       | johndoe@Default | service@Default |         |
| reader       | johndoe@Default | service@Default |         |
| project_user | johndoe@Default | admin@Default   |         |
| member       | johndoe@Default | admin@Default   |         |
| reader       | johndoe@Default | admin@Default   |         |
| project_user | johndoe@Default |                 | Default |
| member       | johndoe@Default |                 | Default |
| reader       | johndoe@Default |                 | Default |
+--------------+-----------------+-----------------+---------+
```

In diesem Beispiel werden die Optionen `-c Role`, `-c User`, `-c Project` und `-c Domain` verwendet, um die Befehlsausgabe so zu kürzen, dass diese auf die Seite passt.

Die QCOW2-Vorlage bereitstellen

1. Melden Sie sich an Ihrem Cyber Protection Konto an.
2. Klicken Sie auf **Geräte** –> **Alle Geräte** –> **Hinzufügen** –> **Virtuozzo Hybrid Infrastructure**.
   Das .zip-Archiv wird zu Ihrer Maschine heruntergeladen.
3. Entpacken Sie das .zip-Archiv. Es enthält eine .qcow2-Image-Datei.
4. Melden Sie sich an Ihrem Virtuozzo Hybrid Infrastructure-Konto an.

5. Fügen Sie die .qcow2-Image-Datei folgendermaßen dem Virtuozzo Hybrid Infrastructure-Compute-Cluster hinzu:
   - Klicken Sie in der Registerkarte **Compute** –> **Virtuelle Maschinen** –> **Images** auf **Image hinzufügen**.
   - Klicken Sie im Fenster **Image hinzufügen** auf den Befehl **Durchsuchen** und wählen Sie dann die .qcow2-Datei aus.
   - Spezifizieren Sie den Image-Namen, wählen Sie **Generic Linux-Betriebssystem** als Typ aus und klicken Sie dann auf **Hinzufügen**.
6. Klicken Sie in der Registerkarte **Compute** –> **Virtuelle Maschinen** –> **Virtuelle Maschinen** auf den Befehl**Virtuelle Maschine erstellen**. Daraufhin wird ein Fenster geöffnet, wo Sie folgende Parameter spezifizieren müssen:
   - Einen Namen für die neue virtuelle Maschine.
   - Wählen Sie bei **Bereitstellungsquelle** die Option **Image**.
   - Wählen Sie im Fenster **Images** die .qcow2-Image-Datei der Appliance aus und klicken Sie dann auf **Fertig**.
   - Sie müssen im Fenster **Volumes** keine Volumes hinzufügen. Das automatisch als Systemlaufwerk hinzugefügte Volume ist ausreichend.
   - Wählen Sie im Fenster **Variante** (Englisch: Flavor) die von Ihnen gewünschte Kombination aus vCPUs und RAM aus – und klicken Sie dann auf **Fertig**. 2 vCPUs und 4 GiB RAM sind normalerweise ausreichend.
   - Klicken Sie im Fenster **Netzwerkschnittstellen** auf den Befehl **Hinzufügen**, wählen Sie das virtuelle Netzwerk vom Typ *öffentlich* aus und klicken Sie anschließend auf **Hinzufügen**. Er wird dann in der Liste **Netzwerkschnittstellen** angezeigt.
     Wenn Sie eine Konfiguration mit mehr als einem physischen Netzwerk verwenden (und daher auch mit mehr als einem virtuellen Netzwerk vom Typ 'öffentlich'), wiederholen Sie diesen Schritt und wählen Sie die von Ihnen benötigten virtuellen Netzwerke aus.
7. Klicken Sie auf **Fertig**.
8. Klicken Sie, wenn Sie zurück im Fenster **Virtuelle Maschine erstellen** sind auf den Befehl **Bereitstellen**, um die virtuelle Maschine zu erstellen und zu booten.

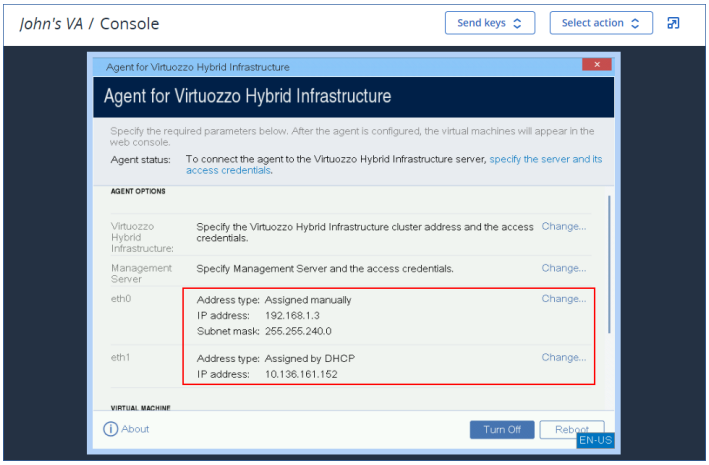
Die virtuelle Appliance konfigurieren

Nachdem Sie den Agenten für Virtuozzo Hybrid Infrastructure (virtuelle Appliance) bereitgestellt haben, müssen Sie die virtuelle Appliance so konfigurieren, dass diese sowohl den Virtuozzo Hybrid Infrastructure-Cluster, der vom Agenten geschützt werden soll, als auch den Cyber Protection Cloud Service erreichen kann.

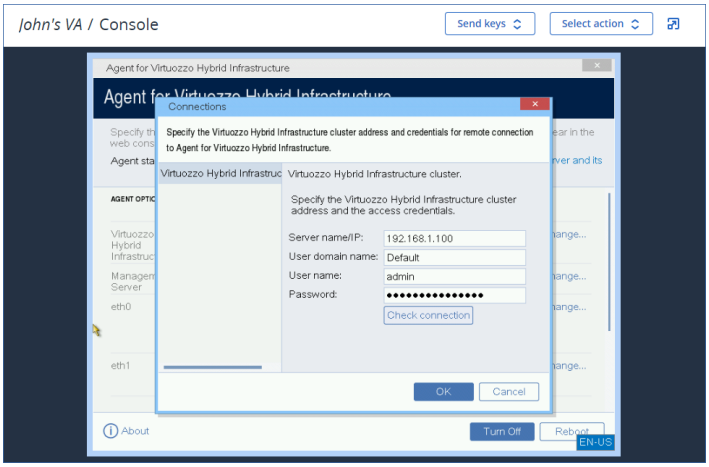
So konfigurieren Sie die virtuelle Appliance

1. Melden Sie sich an Ihrem Virtuozzo Hybrid Infrastructure-Konto an.
2. Wählen Sie in der Registerkarte **Compute** –> **Virtuelle Maschinen** –> **Virtuelle Maschinen** die von Ihnen erstellte virtuelle Maschine aus. Klicken Sie dann auf **Konsole**.

3. Konfigurieren Sie die Netzwerkschnittstellen der Appliance. Abhängig von der Anzahl der virtuellen Netzwerke, die die Appliance verwendet, kann es eine oder mehrere zu konfigurierende Schnittstellen geben. Stellen Sie sicher, dass die automatisch zugewiesenen DHCP-Adressen (sofern vorhanden) in den von Ihrer virtuellen Maschine verwendeten Netzwerken gültig sind – oder weisen Sie alternativ die Adressen manuell zu.



4. Spezifizieren Sie die Adresse und Anmeldedaten des Virtuozzo-Clusters:
   - DNS-Name oder IP-Adresse des Virtuozzo Hybrid Infrastructure-Clusters – dies ist die Adresse des Management-Knotens des Clusters. Der Standard-Port 5000 wird automatisch festgelegt. Wenn Sie einen anderen Port verwenden wollen, müssen Sie diesen manuell spezifizieren.
   - Spezifizieren Sie im Feld **Benutzer-Domain-Name** Ihre Domain in Virtuozzo Hybrid Infrastructure. Beispiel: **Default** (Standard).
     Beim Domain-Namen wird nach Groß-/Kleinschreibung unterschieden.
   - Geben Sie in den Feldern **Benutzername** und **Kennwort** die Anmeldedaten eines Virtuozzo Hybrid Infrastructure-Kontos ein, das in der spezifizierten Domain die Rolle **Administrator** hat. Weitere Informationen über Benutzer, Rollen und Domains finden Sie im Abschnitt 'Benutzerkonten in Virtuozzo Hybrid Infrastructure konfigurieren'.



5. Registrieren Sie die Appliance im Cyber Protection Service, indem Sie eine der folgenden Methoden anwenden.
   - [Nur für Mandanten ohne Zwei-Faktor-Authentifizierung] Registrieren Sie die Appliance in ihrer grafischen Oberfläche.

a. Klicken Sie bei **Agent-Optionen** im Feld **Management Server** auf den Befehl **Ändern**.

b. Wählen Sie im Feld **Server-Name/IP** die Option **Cloud**.

   Die Adresse des Cyber Protection Service wird angezeigt. Ändern Sie diese Adresse nicht, solange es keine anderslautenden Anweisungen gibt.

c. Spezifizieren Sie in die Felder **Benutzername** und **Kennwort** die Anmeldedaten für Ihr Konto im Cyber Protection Service ein. Die virtuelle Appliance und die virtuellen Maschinen, die von der Appliance verwaltet werden, sind unter diesem Konto registriert.

d. Klicken Sie auf **OK**.

- Registrieren Sie die Appliance in der Befehlszeilenschnittstelle.

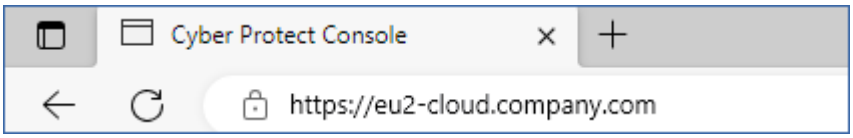
  Hinweis
  Für diese Methode benötigen Sie einen Registrierungstoken. Weitere Informationen darüber, wie Sie ein solches generieren können, finden Sie im Abschnitt '"Ein Registrierungstoken generieren" (S. 182)'.

  a. Drücken Sie STRG+UMSCHALT+F2, um die Befehlszeilenschnittstelle zu öffnen.

  b. Führen Sie folgenden Befehl aus:

  ```
  register_agent -o register -t cloud -a <service address> --token <registration token>
  ```

  Hinweis
  Wenn Sie ein Registrierungstoken verwenden, müssen Sie die genaue Datacenter-Adresse spezifizieren. Dies ist die URL, die Sie sehen, sobald Sie sich an der Cyber Protect-Konsole **angemeldet haben**. Beispielsweise `https://eu2-cloud.company.com`.

  Sie dürfen hier nicht die Adresse `https://cloud.company.com` verwenden.

  c. Drücken Sie die Tastenkombination ALT+F1, um zur grafischen Oberfläche der Appliance zurückzukehren.

6. [Falls in Ihrem Netzwerk ein Proxy-Server verwendet wird] Konfigurieren Sie den Proxy-Server.

   a. Drücken Sie STRG+UMSCHALT+F2, um die Befehlszeilenschnittstelle zu öffnen.

   b. Öffnen Sie die Datei **/etc/Acronis/Global.config** in einem Text-Editor.

   c. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:

   - Wenn die Proxy-Einstellungen während der Installation des Agenten spezifiziert wurden, suchen Sie nach dem folgenden Abschnitt:

     ```
     <key name="HttpProxy">
         <value name="Enabled" type="Tdword">"1"</value>
         <value name="Host" type="TString">"ADDRESS"</value>
         <value name="Port" type="Tdword">"PORT"</value>
         <value name="Login" type="TString">"LOGIN"</value>
     ```

```
    <value name="Password" type="TString">"PASSWORD"</value>
</key>
```

- Sie können die obigen Zeilen auch kopieren und in die Datei zwischen den Tags '<registry name="Global">...</registry>' einfügen.

d. Ersetzen Sie ADDRESS mit dem Host-Namen/der IP-Adresse des neuen Proxy-Servers – und PORT mit dem Dezimalwert der dazugehörigen Port-Nummer.

e. Wenn Ihr Proxy-Server eine Authentifizierung benötigt, ersetzen Sie LOGIN und PASSWORD mit den entsprechenden Anmeldedaten des Proxy-Servers. Anderenfalls können Sie diese Zeilen aus der Datei löschen.

f. Speichern Sie die Datei.

g. Öffnen Sie die Datei **/opt/acronis/etc/aakore.yaml** in einem Text-Editor.

h. Suchen Sie den Abschnitt **env** (oder erstellen Sie diesen) und fügen Sie dann folgende Zeilen hinzu:

```
env:
    http-proxy: proxy_login:proxy_password@proxy_address:port
    https-proxy: proxy_login:proxy_password@proxy_address:port
```

i. Ersetzen Sie proxy_login und proxy_password mit den Anmeldedaten des Proxy-Servers – und proxy_address:port mit der Adresse und der Port-Nummer des Proxy-Servers.

j. Führen Sie den Befehl reboot aus:

Hinweis

Wenn Sie eine virtuelle Appliance aktualisieren wollen, die hinter einem Proxy bereitgestellt wurde, müssen Sie auf der Appliance die Datei config.yaml (unter /opt/acronis/etc/va-updater/config.yaml) bearbeiten, indem Sie folgende Zeile am Ende der Datei hinzufügen und dann die Werte eingeben, die für Ihre Umgebung gelten:

```
httpProxy: http://<proxy_login>:<proxy_password>@<proxy_address>:<port>
```

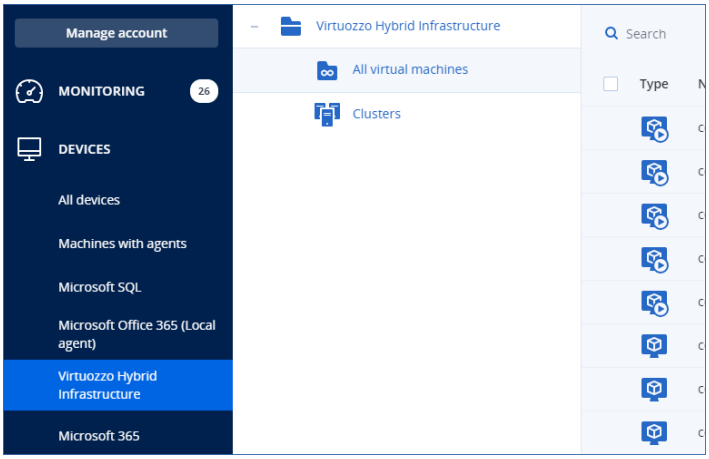
Beispiel:

```
httpProxy: http://mylogin:mypassword@192.168.2.300:8080
```

So können Sie die virtuellen Maschinen im Virtuozzo Hybrid Infrastructure-Cluster schützen

1. Melden Sie sich an Ihrem Cyber Protection Konto an.
2. Gehen Sie zu **Geräte** –> **Virtuozo Hybrid Infrastructure** –> <Ihr Cluster> –> **Standardprojekt** –> **admin** – oder suchen Sie Ihre Maschinen in **Geräte** –> **Alle Geräte**.

3. Wählen Sie die Maschinen aus und wenden Sie einen Schutzplan auf diese an.



Den Agenten für oVirt (Virtuelle Appliance) bereitstellen

Bevor Sie beginnen

Diese Appliance ist eine vorkonfigurierte virtuelle Maschine, die Sie in einem Red Hat Virtualization/oVirt-Datacenter bereitstellen können. Die Appliance enthält einen Protection Agenten, der es Ihnen ermöglicht, die Cyber Protection-Funktionalität für alle virtuellen Maschinen in diesem Datacenter zu verwalten.

Systemanforderungen für den Agenten

Standardmäßig verwendet die virtuelle Maschine mit dem Agenten zwei (2) vCPUs und vier (4) GiB RAM. Diese Einstellungen sind für die meisten Operationen ausreichend. Aber Sie diese auch im Red Hat Virtualization/oVirt-Administrationsportal bearbeiten.

Um die Backup-Performance zu verbessern und Fehler durch zu wenig Arbeitsspeicher zu vermeiden, empfehlen wir für anspruchsvollere Fälle, diese Ressourcen auf 4 vCPUs und 8 GiB RAM zu erhöhen. Wenn Sie beispielsweise erwarten, dass der Backup-Datenverkehr 100 MB pro Sekunde überschreitet (z.B. in 10-Gigabit-Netzwerken) oder wenn Sie mehrere virtuelle Maschinen mit großen Festplatten (500 GB oder mehr) gleichzeitig sichern wollen, sollten Sie die zugewiesenen Ressourcen erhöhen.

Die Größe des virtuellen Laufwerks der Appliance beträgt 8 GiB.

Wie viele Agenten benötige ich?

Ein (1) Agent kann das komplette Datacenter schützen. Sie können jedoch mehr als einen Agenten im Datacenter verwenden, wenn Sie die Bandbreitenbelastung des Backup-Datenverkehrs verteilen wollen.

Wenn Sie mehr als einen Agenten in einem Datacenter haben, werden die virtuellen Maschinen automatisch zwischen den Agenten verteilt, sodass jeder Agent eine ähnliche Anzahl von Maschinen verwaltet.

Wenn es bei der Auslastung zwischen den Agenten zu einem Ungleichgewicht von über 20% kommt, erfolgt eine automatische Neuverteilung. Dazu kann es kommen, nachdem Sie eine Maschine oder einen Agent hinzugefügt oder entfernt haben. Sie bemerken beispielsweise, dass Sie mehr Agenten benötigen, um den Durchsatz zu erhöhen, und stellen eine zusätzliche virtuelle Appliance im Datacenter bereit. Der Management Server wird die geeignetsten Maschinen dem neuen Agenten zuweisen. Die Last der alten Agenten wird reduziert. Wenn Sie einen Agenten entfernen, dann werden die diesem Agenten zugewiesenen Maschinen unter den verbliebenen Agenten neu verteilt. Dies geschieht jedoch nicht, wenn ein Agent beschädigt wird oder manuell aus dem Red Hat Virtualization/oVirt-Administrationsportal entfernt wird. Eine Neuverteilung wird in diesem Fall nur dann gestartet, wenn Sie einen solchen Agenten über die Cyber Protect-Konsole entfernen.

So können Sie überprüfen, welcher Agent eine bestimmte Maschine verwaltet

1. Klicken Sie zuerst in der Cyber Protect-Konsole auf **Geräte** und wählen Sie dann den Eintrag **oVirt**.
2. Klicken Sie in der rechten oberen Ecke der Tabelle auf das Zahnradsymbol und aktivieren Sie unter **System** das Kontrollkästchen **Agent**.
3. Kontrollieren Sie den Namen des Agenten in der angezeigten Spalte.

Einschränkungen

Folgende Aktionen werden bei virtuellen Red Hat Virtualization/oVirt-Maschinen nicht unterstützt:

- Applikationskonformes Backup
- Eine virtuelle Maschine aus einem Backup heraus ausführen
- Replikation von virtuellen Maschinen
- Changed Block Tracking (CBT)

Die OVF-Vorlage bereitstellen

1. Melden Sie sich an Ihrem Cyber Protection Konto an.
2. Klicken Sie auf **Geräte** –> **Alle Geräte** –> **Hinzufügen** –> **Red Hat Virtualization (oVirt)**.
   Das .zip-Archiv wird zu Ihrer Maschine heruntergeladen.
3. Entpacken Sie das .zip-Archiv. Es enthält eine .ova-Datei.
4. Laden Sie die .ova-Datei zu einem Host im Red Hat Virtualization/oVirt-Datacenter hoch, das Sie schützen wollen.
5. Melden Sie sich am Red Hat Virtualization/oVirt-Administrationsportal als Administrator an. Weitere Informationen zu den Rollen, die für Aktionen mit virtuellen Maschinen erforderlich sind, finden Sie in Abschnitt '"Agent für oVirt – erforderliche Rollen und Ports" (S. 172)'.
6. Wählen Sie im Navigationsmenü die Elemente **Compute** –> **Virtuelle Maschinen** aus.
7. Klicken Sie zuerst auf das vertikale Drei-Punkte-Symbol  oberhalb der Haupttabelle und dann auf den Befehl **Importieren**.

8. Führen Sie im Fenster **Virtuelle Maschine(n) importieren** folgende Schritte aus:
   a. Wählen Sie bei **Datacenter** das Datacenter aus, welches Sie schützen wollen.
   b. Wählen Sie bei **Quelle** den Eintrag **Virtuelle Appliance (OVA)** aus.
   c. Wählen Sie bei **Host** den Host aus, zu dem Sie die .ova-Datei hochgeladen haben.
   d. Spezifizieren Sie bei **Dateipfad** den Pfad zu demjenigen Verzeichnis, welches die .ova-Datei enthält.
   e. Klicken Sie auf **Laden**.
      Die Vorlage für die virtuelle oVirt-Appliance aus der .ova-Datei erscheint im Bereich **Virtuelle Maschinen auf Quelle**.
      Wenn die Vorlage nicht in diesem Fensterbereich erscheint, sollten Sie sicherstellen, dass Sie den richtigen Pfad zur Datei spezifiziert haben, die Datei nicht beschädigt ist und der Host erreichbar ist.
   f. Wählen Sie bei **Virtuelle Maschinen auf Quelle** die Vorlage der virtuellen oVirt-Appliance und klicken Sie dann auf den rechten Pfeil.
      Die Vorlage erscheint im Fensterbereich **Zu importierende Virtuelle Maschinen**.
   g. Klicken Sie auf **Weiter**.
9. Klicken Sie im neuen Fenster auf den Namen der Appliance und konfigurieren Sie dann folgende Einstellungen:
   - Konfigurieren Sie auf der Registerkarte **Netzwerkschnittstellen** die Netzwerkschnittstellen.
   - [Optional] Ändern Sie auf der Registerkarte **Allgemein** den Standardnamen der virtuellen Maschine mit dem Agenten.

Die Bereitstellung ist nun abgeschlossen. Als nächstes müssen Sie die virtuelle Appliance konfigurieren. Weitere Informationen zu deren Konfiguration finden Sie im Abschnitt '"Die virtuelle Appliance konfigurieren" (S. 168)'.

Hinweis
Wenn Sie mehr als eine virtuelle Appliance in Ihrem Datacenter benötigen, müssen Sie die oberen Schritte wiederholen und dabei weitere virtuelle Appliances bereitstellen. Sie sollten eine vorhandene virtuelle Appliance nicht klonen, indem Sie die Option **VM klonen** im Red Hat Virtualization/oVirt-Administrationsportal verwenden.

Wenn Sie die virtuelle Appliance von dynamischen Gruppen-Backups ausschließen wollen, müssen Sie diese auch aus der Liste der virtuellen Maschinen in der Cyber Protect-Konsole ausschließen. Um diese auszuschließen, müssen Sie im Red Hat Virtualization/oVirt-Administrationsportal zuerst die virtuelle Maschine mit dem Agenten auswählen und dieser dann das Tag `acronis_virtual_appliance` zuweisen.

Die virtuelle Appliance konfigurieren

Nachdem Sie die virtuelle Appliance bereitgestellt haben, müssen Sie diese so konfigurieren, dass sie sowohl die oVirt-Engine als auch den Cyber Protection Service erreichen kann.

So konfigurieren Sie die virtuelle Appliance

1. Melden Sie sich am Red Hat Virtualization/oVirt-Administrationsportal an.
2. Wählen Sie die virtuelle Appliance aus, die Sie konfigurieren wollen, und klicken Sie dann auf das Symbol **Konsole**.
3. Konfigurieren Sie im Feld **eth0** die Netzwerkschnittstellen der Appliance.
   Stellen Sie sicher, dass die automatisch zugewiesenen DHCP-Adressen (sofern vorhanden) in den von Ihrer virtuellen Maschine verwendeten Netzwerken gültig sind – oder weisen Sie alternativ die Adressen manuell zu. Abhängig von der Anzahl der Netzwerke, die die Appliance verwendet, müssen möglicherweise eine oder mehrere Schnittstellen konfiguriert werden.
4. Klicken Sie im Feld **oVirt** auf **Ändern**, um die Adresse der oVirt-Engine sowie die Anmeldedaten zu spezifizieren, um auf die Engine zugreifen zu können:
   a. Geben Sie im Feld **Server-Name/IP** den DNS-Namen oder die IP-Adresse der Engine ein.
   b. Geben Sie in die Felder **Benutzername** und **Kennwort** die Administrator-Anmeldedaten für diese Engine ein.
      Stellen Sie sicher, dass dieses Administratorkonto über die Rollen verfügt, die für Aktionen mit virtuellen Red Hat Virtualization/oVirt-Maschinen erforderlich sind. Weitere Informationen über diese Rollen finden Sie im Abschnitt '"Agent für oVirt – erforderliche Rollen und Ports" (S. 172)'.
      Wenn Keycloak der Anbieter für einmaliges Anmelden (Single-Sign-On, SSO) für die oVirt-Engine ist (Standard in oVirt 4.5.1), verwenden Sie das Keycloak-Format bei der Angabe des Benutzernamens. Spezifizieren Sie beispielsweise das Standard-Administratorkonto als `admin@ovirt@internalsso` anstelle von `admin@internal`.
   c. [Optional] Klicken Sie auf den Befehl **Verbindung prüfen**, um sicherzustellen, dass die bereitgestellten Anmeldedaten korrekt sind.
   d. Klicken Sie auf **OK**.
5. Registrieren Sie die Appliance im Cyber Protection Service, indem Sie eine der folgenden Methoden anwenden.
   - [Nur für Mandanten ohne Zwei-Faktor-Authentifizierung] Registrieren Sie die Appliance in ihrer grafischen Oberfläche.
     a. Klicken Sie bei **Agent-Optionen** im Feld **Management Server** auf den Befehl **Ändern**.
     b. Wählen Sie im Feld **Server-Name/IP** die Option **Cloud**.
        Die Adresse des Cyber Protection Service wird angezeigt. Ändern Sie diese Adresse nicht, solange es keine anderslautenden Anweisungen gibt.
     c. Spezifizieren Sie in die Felder **Benutzername** und **Kennwort** die Anmeldedaten für Ihr Konto im Cyber Protection Service ein. Die virtuelle Appliance und die virtuellen Maschinen, die von der Appliance verwaltet werden, sind unter diesem Konto registriert.
     d. Klicken Sie auf **OK**.
   - Registrieren Sie die Appliance in der Befehlszeilenschnittstelle.

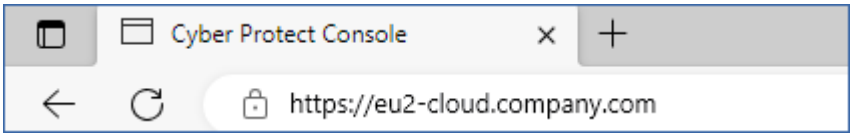
Hinweis
Für diese Methode benötigen Sie einen Registrierungstoken. Weitere Informationen darüber, wie Sie ein solches generieren können, finden Sie im Abschnitt '"Ein Registrierungstoken generieren" (S. 182)'.

a. Drücken Sie STRG+UMSCHALT+F2, um die Befehlszeilenschnittstelle zu öffnen.

b. Führen Sie folgenden Befehl aus:

```
register_agent -o register -t cloud -a <service address> --token <registration
token>
```

Hinweis
Wenn Sie ein Registrierungstoken verwenden, müssen Sie die genaue Datacenter-Adresse spezifizieren. Dies ist die URL, die Sie sehen, sobald Sie sich an der Cyber Protect-Konsole **angemeldet haben**. Beispielsweise `https://eu2-cloud.company.com`.



Sie dürfen hier nicht die Adresse `https://cloud.company.com` verwenden.

c. Drücken Sie die Tastenkombination ALT+F1, um zur grafischen Oberfläche der Appliance zurückzukehren.

6. [Optional] Klicken Sie im Feld **Name** auf **Ändern**, um den Standardnamen für die virtuelle Appliance zu bearbeiten, der **localhost** lautet. Der Name wird in der Cyber Protect-Konsole angezeigt.
7. [Optional] Klicken Sie im Feld **Zeit** auf **Ändern** und wählen Sie dann die Zeitzone Ihres Standortes aus, um sicherzustellen, dass die geplanten Aktionen zur korrekten Zeit ausgeführt werden.
8. [Optional] [Falls in Ihrem Netzwerk ein Proxy-Server verwendet wird] Konfigurieren Sie den Proxy-Server.
   a. Drücken Sie STRG+UMSCHALT+F2, um die Befehlszeilenschnittstelle zu öffnen.
   b. Öffnen Sie die Datei **/etc/Acronis/Global.config** in einem Text-Editor.
   c. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
      - Wenn die Proxy-Einstellungen während der Installation des Agenten spezifiziert wurden, suchen Sie nach dem folgenden Abschnitt:

```
<key name="HttpProxy">
    <value name="Enabled" type="Tdword">"1"</value>
    <value name="Host" type="TString">"ADDRESS"</value>
    <value name="Port" type="Tdword">"PORT"</value>
    <value name="Login" type="TString">"LOGIN"</value>
    <value name="Password" type="TString">"PASSWORD"</value>
</key>
```

- Sie können die obigen Zeilen auch kopieren und in die Datei zwischen den Tags '<registry name="Global">...</registry>' einfügen.

d. Ersetzen Sie ADDRESS mit dem Host-Namen/der IP-Adresse des neuen Proxy-Servers – und PORT mit dem Dezimalwert der dazugehörigen Port-Nummer.

e. Wenn Ihr Proxy-Server eine Authentifizierung benötigt, ersetzen Sie LOGIN und PASSWORD mit den entsprechenden Anmeldedaten des Proxy-Servers. Anderenfalls können Sie diese Zeilen aus der Datei löschen.

f. Speichern Sie die Datei.

g. Öffnen Sie die Datei **/opt/acronis/etc/aakore.yaml** in einem Text-Editor.

h. Suchen Sie den Abschnitt **env** (oder erstellen Sie diesen) und fügen Sie dann folgende Zeilen hinzu:

```
env:
    http-proxy: proxy_login:proxy_password@proxy_address:port
    https-proxy: proxy_login:proxy_password@proxy_address:port
```

i. Ersetzen Sie `proxy_login` und `proxy_password` mit den Anmeldedaten des Proxy-Servers – und `proxy_address:port` mit der Adresse und der Port-Nummer des Proxy-Servers.

j. Führen Sie den Befehl `reboot` aus:

Hinweis

Wenn Sie eine virtuelle Appliance aktualisieren wollen, die hinter einem Proxy bereitgestellt wurde, müssen Sie auf der Appliance die Datei `config.yaml` (unter `/opt/acronis/etc/va-updater/config.yaml`) bearbeiten, indem Sie folgende Zeile am Ende der Datei hinzufügen und dann die Werte eingeben, die für Ihre Umgebung gelten:

```
httpProxy: http://<proxy_login>:<proxy_password>@<proxy_address>:<port>
```

Beispiel:

```
httpProxy: http://mylogin:mypassword@192.168.2.300:8080
```

So können Sie virtuelle Maschinen im Red Hat Virtualization/oVirt-Datacenter schützen

1. Melden Sie sich an Ihrem Cyber Protection Konto an.
2. Gehen Sie zu **Geräte** –> **oVirt** –> <Ihr Cluster> – oder suchen Sie Ihre Maschinen unter **Geräte** –> **Alle Geräte**.
3. Wählen Sie die Maschinen aus und wenden Sie einen Schutzplan auf diese an.

Agent für oVirt – erforderliche Rollen und Ports

Erforderliche Rollen

Der Agent für oVirt benötigt für seine Bereitstellung und seinen Betrieb ein Administratorkonto, dem die nachfolgenden Rollen zugewiesen wurden.

oVirt/Red Hat Virtualization 4.2 und 4.3/Oracle Virtualization Manager 4.3

- DiskCreator
- UserVmManager
- TagManager
- UserVmRunTimeManager
- VmCreator

oVirt/Red Hat Virtualization 4.4, 4.5

- SuperUser

Erforderliche Ports

Der Agent für oVirt verbindet sich mit der oVirt-Engine über diejenige URL, die Sie bei der Konfiguration der virtuellen Appliance spezifizieren. Normalerweise hat die Engine-URL folgendes Format: `https://ovirt.company.com`. In diesem Fall werden das HTTPS-Protokoll sowie Port 443 verwendet.

Nicht standardmäßige oVirt-Einstellungen erfordern möglicherweise einen anderen Port. Sie können den genauen Port ermitteln, indem Sie das URL-Format analysieren. Zum Beispiel:

oVirt-Engine-URL	Port	Protokoll
`https://ovirt.company.com/`	443	HTTPS
`http://ovirt.company.com/`	80	HTTP
`https://ovirt.company.com:1234/`	1234	HTTPS

Für Lese-/Schreib-Operationen mit Laufwerken werden keine zusätzlichen Ports benötigt, weil das Backup im HotAdd-Modus durchgeführt wird.

Den Agenten für Synology bereitstellen

Bevor Sie beginnen

Mit dem Agenten für Synology können Sie Dateien und Ordner von und zu Synology NAS-Geräten sichern. Die NAS-spezifischen Eigenschaften und Zugriffsberechtigungen für Freigaben, Ordner und Dateien bleiben dabei erhalten.

Der Agent für Synology wird auf dem NAS-Gerät ausgeführt. Daher können Sie die Ressourcen des Geräts für Off-Host Data Processing-Aktionen (wie Backup-Replikationen, Validierungen und Bereinigungen) nutzen. Weitere Informationen über diese Aktionen finden Sie im Abschnitt '"Off-Host Data Processing" (S. 214)'.

Hinweis
Der Agent für Synology unterstützt nur NAS-Geräte mit x86_64-Prozessoren. ARM-Prozessoren werden nicht unterstützt.

Sie können ein Backup am ursprünglichen oder einem neuen Speicherort auf dem NAS-Gerät wiederherstellen – oder in einem Netzwerkordner, auf den über das NAS-Gerät zugegriffen werden kann. Backups, die sich im Cloud Storage befinden, können auch auf einem NAS-Gerät wiederhergestellt werden, das nicht das Originalgerät ist und auf dem der Agent für Synology installiert ist.

In der nachfolgenden Tabelle werden die verfügbaren Backup-Quellen und -Ziele zusammengefasst.

Backup-Quelle	Elemente für das Backup (Backup-Quelle)	Backup-Ort (Backup-Ziel)
Dateien/Ordner	Lokaler Ordner*	Cloud Storage
		Lokaler Ordner*
	Netzwerkordner (SMB)**	Netzwerkordner (SMB)**
		NFS-Ordner

* Einschließlich USB-Laufwerke, die an das NAS-Gerät angeschlossen sind.

Hinweis
Verschlüsselte Ordner werden nicht unterstützt. Diese Ordner werden in der grafischen Benutzeroberfläche von Cyber Protection nicht angezeigt.

** Die Verwendung von externen Netzwerkfreigaben als Backup-Quelle oder Backup-Ziel über das SMB-Protokoll ist nur für Agenten verfügbar, die unter dem Synology DiskStation Manager 6.2.3 und

höher laufen. Die Daten, die auf dem Synology NAS-Gerät selbst gehostet werden (einschließlich gehosteter Netzwerkfreigaben), können ohne Einschränkungen per Backup gesichert werden.

Einschränkungen

- Der Agent für Synology unterstützt nur NAS-Geräte mit x86_64-Prozessoren. ARM-Prozessoren werden nicht unterstützt.
- Verschlüsselte Freigaben, die per Backup gesichert wurden, werden unverschlüsselt wiederhergestellt.
- Per Backup gesicherte Freigaben, für die die Option **Dateikomprimierung** aktiviert ist, werden mit deaktivierter Option wiederhergestellt.
- Sie können nur Backups auf einem Synology NAS-Gerät wiederherstellen, die vom Agenten für Synology erstellt wurden.

Laden Sie das Setup-Programm herunter.

Das Setup-Programm des Agenten für Synology ist als SPK-Datei verfügbar.

Agent für Synology 7.x

So können Sie das Setup-Programm herunterladen

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte** –> **Alle Geräte**.
2. Klicken Sie in der oberen rechten Fensterecke auf **Hinzufügen**.
3. Klicken Sie unter **NAS-Geräte (Network Attached Storage)** auf **Synology**.
   Das Setup-Programm wird auf Ihre Maschine heruntergeladen.

Agent für Synology 6.x

So können Sie das Setup-Programm herunterladen

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte** –> **Alle Geräte**.
2. Klicken Sie in der oberen rechten Fensterecke auf **Hinzufügen**.
3. Klicken Sie unter **NAS-Geräte (Network Attached Storage)** auf **Synology**.
   Das Setup-Programm für den Agenten für Synology 7.x wird auf Ihre Maschine heruntergeladen. Sie können den Prozess gefahrlos abbrechen oder die heruntergeladene Datei ignorieren.
4. Klicken Sie auf **Agent für Synology 6.x herunterladen**.
   Das Setup-Programm für den Agenten für Synology 6.x wird auf Ihre Maschine heruntergeladen.

Den Agenten für Synology installieren

Wenn Sie den Agenten für Synology installieren wollen, müssen Sie die SPK-Datei im Synology DiskStation Manager ausführen.

Hinweis
Der Agent für Synology unterstützt nur NAS-Geräte mit x86_64-Prozessoren. ARM-Prozessoren werden nicht unterstützt.

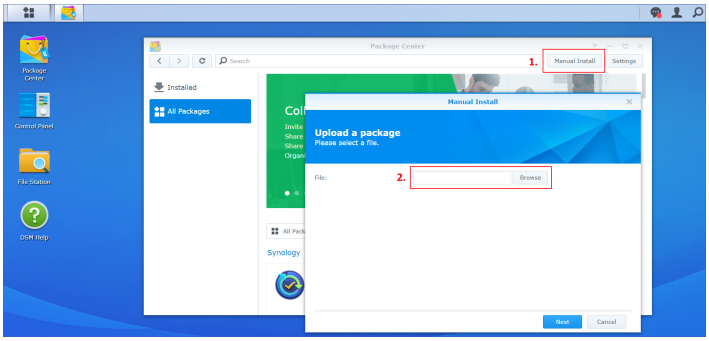
Agent für Synology 7.x

Voraussetzungen

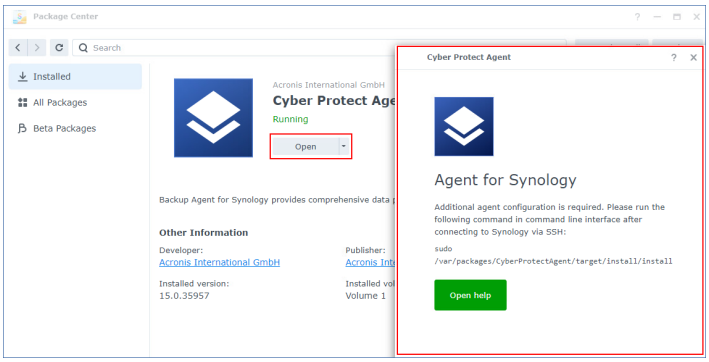
- Auf dem NAS-Gerät läuft der DiskStation Manager 7.x.
- Sie auf dem NAS-Gerät ein Mitglied der Gruppe der **Administratoren** sind.
- Auf dem NAS-Volume, auf dem Sie den Agenten installieren wollen, mindestens 200 MB an freiem Speicherplatz vorhanden sind.
- Auf Ihrer Maschine ist ein SSH-Client verfügbar. In diesem Dokument wird Putty als Beispiel verwendet.

So können Sie den Agenten für Synology installieren

1. Melden Sie sich am Synology DiskStation Manager an.
2. Öffnen Sie das **Paket-Zentrum**.
3. Klicken Sie dort zuerst auf **Manuelle Installation** und dann auf **Durchsuchen**.



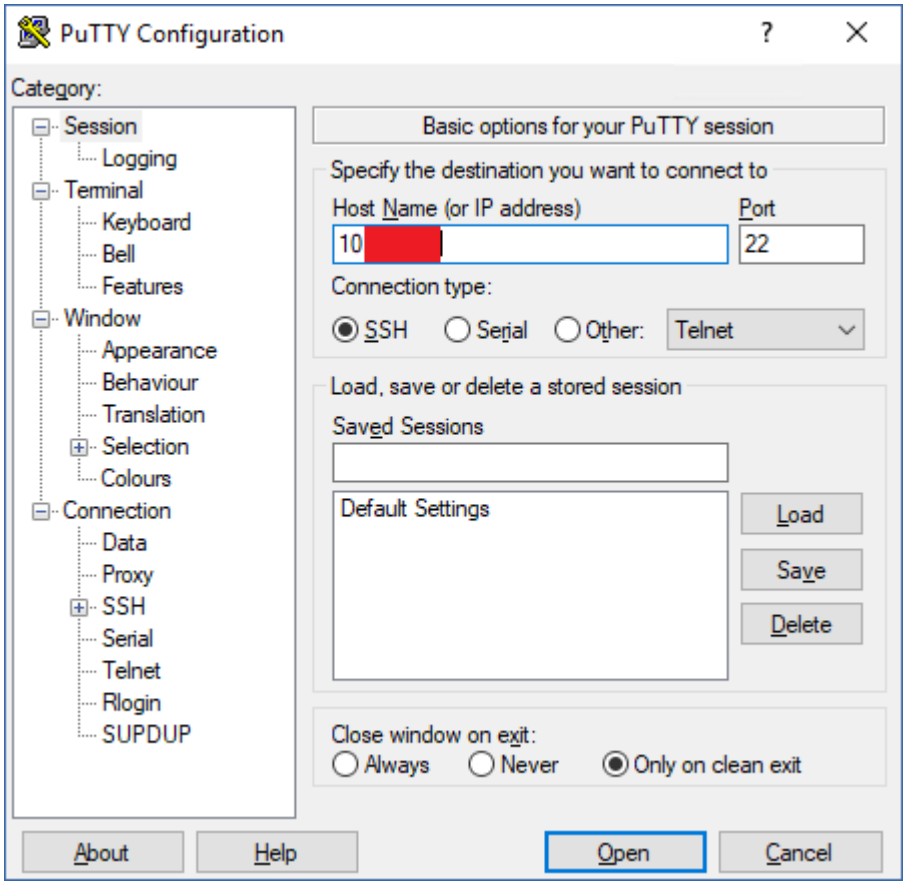
4. Wählen Sie die SPK-Datei aus, die Sie von der Cyber Protect-Konsole heruntergeladen haben, und klicken Sie dann auf **Weiter**.
   Es wird eine Warnung angezeigt, dass Sie dabei sind, das Software-Paket eines Drittanbieters zu installieren. Diese Meldung ist Teil der Standardinstallationsprozedur.
5. Klicken Sie auf **Zustimmen**, um zu bestätigen, dass Sie das Paket installieren wollen.
6. Bestimmen Sie das Volume, auf dem Sie den Agenten installieren wollen, und klicken Sie anschließend auf **Weiter**.
7. Überprüfen Sie die Einstellungen und klicken Sie dann auf **Fertig**.
8. Öffnen Sie im Synology DiskStation Manager **Paket-Zentrum** den Cyber Protect Agenten für Synology und überprüfen Sie dann, ob Sie den nachfolgenden Bildschirm sehen.



9. Gehen Sie in der **Systemsteuerung** des Synology DiskStation Managers zu **Terminal & SNMP** und aktivieren Sie dort den SSH-Zugriff auf das NAS-Gerät.
10. Führen Sie das Skript `install` auf dem NAS-Gerät mithilfe eines SSH-Clients (in diesem Beispiel: Putty) aus.

    Das Skript ermöglicht einen Root-Zugriff auf DSM 7.0 oder höher, der für die Konfiguration des Agenten erforderlich ist.

    a. Starten Sie Putty und spezifizieren Sie die IP-Adresse oder den Host-Namen Ihres NAS-Geräts von Synology.



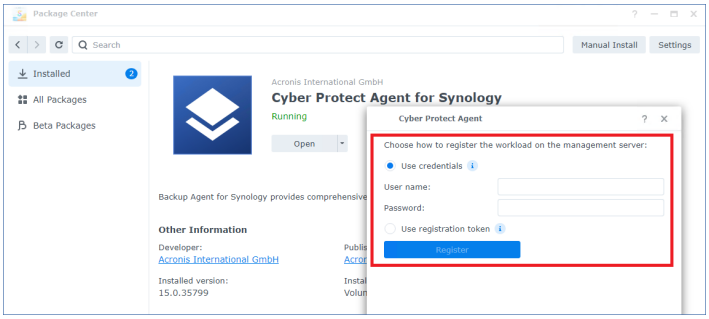
    b. Klicken Sie auf **Öffnen** und melden Sie sich dann als Synology DSM-Administrator an.

    c. Führen Sie den nachfolgenden Befehl aus.

```
sudo /var/packages/CyberProtectAgent/target/install/install
```

Warten Sie nach dem Start des Skripts rund 15 Sekunden, in denen die Cyber Protection Services initialisiert werden.

11. Gehen Sie in der **Systemsteuerung** des Synology DiskStation Managers zu **Terminal & SNMP** und deaktivieren Sie dort den SSH-Zugriff auf das NAS-Gerät. Der SSH-Zugriff wird nicht mehr benötigt.
12. Öffnen Sie im **Paket-Zentrum** des Synology DiskStation Managers den Cyber Protect Agenten für Synology.
13. Wählen Sie die Registrierungsmethode aus.



- [So können Sie den Agenten mit Anmeldedaten registrieren]
  - Geben Sie in den Feldern **Benutzername** und **Kennwort** die Anmeldedaten für das Konto an, unter dem der Agent registriert wird. Dieses Konto darf kein Partner-Administrator-Konto sein.
- [So können Sie den Agenten mit einem Registrierungstoken registrieren]
  - Spezifizieren Sie bei **Registrierungsadresse** die genaue Datacenter-Adresse. Bei dieser handelt es sich um die URL, die Sie sehen, wenn Sie sich an der Cyber Protect-Konsole angemeldet haben. Ein Beispiel wäre: `https://us5-cloud.acronis.com`.

    Hinweis
    Verwenden Sie kein URL-Format ohne die Datencenter-Adresse. Sie sollten zum Beispiel nicht `https://cloud.acronis.com` verwenden.

  - Spezifizieren Sie im Feld **Token** das Registrierungstoken.
    Weitere Informationen über die Generierung eines Registrierungstokens finden Sie im Abschnitt '"Ein Registrierungstoken generieren" (S. 182)'.

14. Klicken Sie auf **Registrieren**.

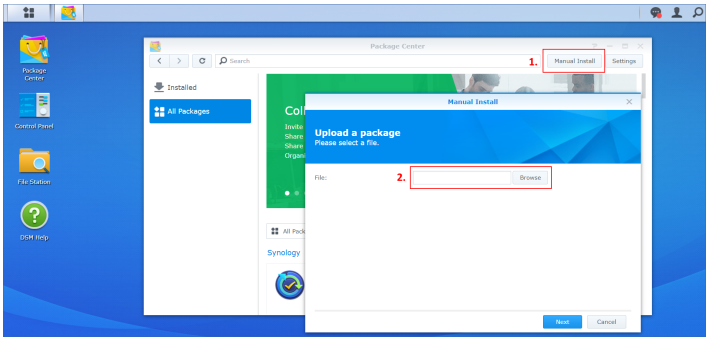
Agent für Synology 6.x

Voraussetzungen

- Auf dem NAS-Gerät läuft der DiskStation Manager 6.2.x.
- Sie auf dem NAS-Gerät ein Mitglied der Gruppe der **Administratoren** sind.
- Auf dem NAS-Volume, auf dem Sie den Agenten installieren wollen, mindestens 200 MB an freiem Speicherplatz vorhanden sind.

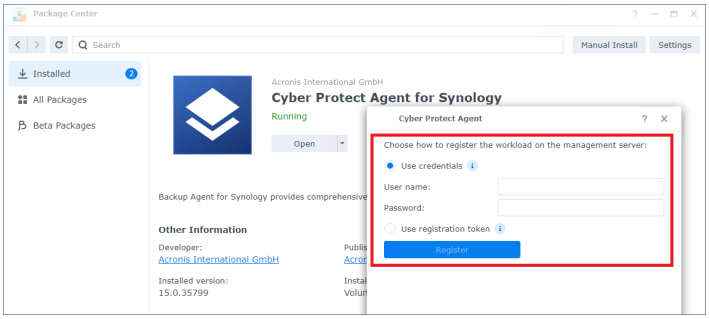
So können Sie den Agenten für Synology installieren

1. Melden Sie sich am Synology DiskStation Manager an.
2. Öffnen Sie das **Paket-Zentrum**.
3. Klicken Sie dort zuerst auf **Manuelle Installation** und dann auf **Durchsuchen**.



4. Wählen Sie die SPK-Datei aus, die Sie von der Cyber Protect-Konsole heruntergeladen haben, und klicken Sie dann auf **Weiter**.

   Es wird eine Warnung angezeigt, dass Sie dabei sind, ein Paket ohne digitale Signatur zu installieren. Diese Meldung ist Teil der Standardinstallationsprozedur.
5. Klicken Sie auf **Ja**, um zu bestätigen, dass Sie das Paket installieren wollen.
6. Bestimmen Sie das Volume, auf dem Sie den Agenten installieren wollen, und klicken Sie anschließend auf **Weiter**.
7. Überprüfen Sie die Einstellungen und klicken Sie dann auf **Anwenden**.
8. Öffnen Sie im **Paket-Zentrum** des Synology DiskStation Managers den Cyber Protect Agenten für Synology.
9. Wählen Sie die Registrierungsmethode aus.



   - [So können Sie den Agenten mit Anmeldedaten registrieren]
     - Geben Sie in den Feldern **Benutzername** und **Kennwort** die Anmeldedaten für das Konto an, unter dem der Agent registriert wird. Dieses Konto darf kein Partner-Administrator-Konto sein.
   - [So können Sie den Agenten mit einem Registrierungstoken registrieren]
     - Spezifizieren Sie bei **Registrierungsadresse** die genaue Datacenter-Adresse. Bei dieser handelt es sich um die URL, die Sie sehen, wenn Sie sich an der Cyber Protect-Konsole angemeldet haben. Ein Beispiel wäre: `https://us5-cloud.acronis.com`.

Hinweis
Verwenden Sie kein URL-Format ohne die Datencenter-Adresse. Sie sollten zum Beispiel nicht `https://cloud.acronis.com` verwenden.

- Spezifizieren Sie im Feld **Token** das Registrierungstoken.
  Weitere Informationen über die Generierung eines Registrierungstokens finden Sie im Abschnitt '"Ein Registrierungstoken generieren" (S. 182)'.

10. Klicken Sie auf **Registrieren**.

Wenn die Registrierung abgeschlossen ist, wird das Synology NAS-Gerät in der Cyber Protect-Konsole unter der Registerkarte **Geräte** –> **NAS-Gerät (Network Attached Storage)** angezeigt.

Wenn Sie die Daten auf diesem NAS-Gerät sichern wollen, müssen Sie einen entsprechenden Schutzplan anwenden.

Den Agenten für Synology aktualisieren

Sie können den Agenten für Synology 6.x auf eine neuere Version des Agenten für Synology 6.x aktualisieren. Auf ähnliche Weise können Sie auch den Agenten für Synology 7.x auf eine neuere Version des Agenten für Synology 7.x aktualisieren.

Wenn Sie den Agenten aktualisieren wollen, müssen Sie die entsprechende neuere Version des Setup-Programms im Synology DiskStation Manager ausführen. Die ursprüngliche Registrierung des Agenten, dessen Einstellungen und die Pläne, die auf die geschützten Workloads angewendet werden, bleiben erhalten.

Hinweis
Sie können den Agenten nicht über die Konsole von Cyber Protect aktualisieren.

Ein Upgrade des Agenten für Synology 6.x auf den Agenten für Synology 7.x ist nur möglich, indem Sie den älteren Agenten deinstallieren und dann den neueren Agenten installieren. In diesem Fall werden auch alle Schutzpläne widerrufen, sodass Sie diese anschließend erneut manuell anwenden müssen.

Agent für Synology 7.x

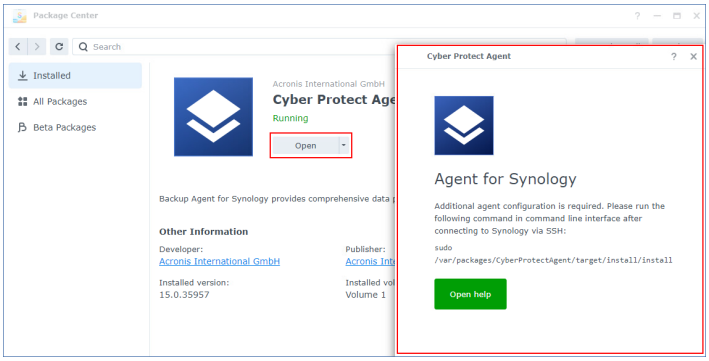
Voraussetzungen

- Sie auf dem NAS-Gerät ein Mitglied der Gruppe der **Administratoren** sind.
- Auf dem NAS-Volume, auf dem Sie den Agenten installieren wollen, mindestens 200 MB an freiem Speicherplatz vorhanden sind.
- Auf Ihrer Maschine ist ein SSH-Client verfügbar. In diesem Dokument wird Putty als Beispiel verwendet.

So können Sie den Agenten für Synology aktualisieren

1. Öffnen Sie das **Paket-Zentrum** im DiskStation Manager.
2. Klicken Sie dort zuerst auf **Manuelle Installation** und dann auf **Durchsuchen**.
3. Wählen Sie die neuere SPK-Datei des Agenten für Synology 7.x aus, die Sie von der Cyber Protect-Konsole heruntergeladen haben, und klicken Sie dann auf **Weiter**.

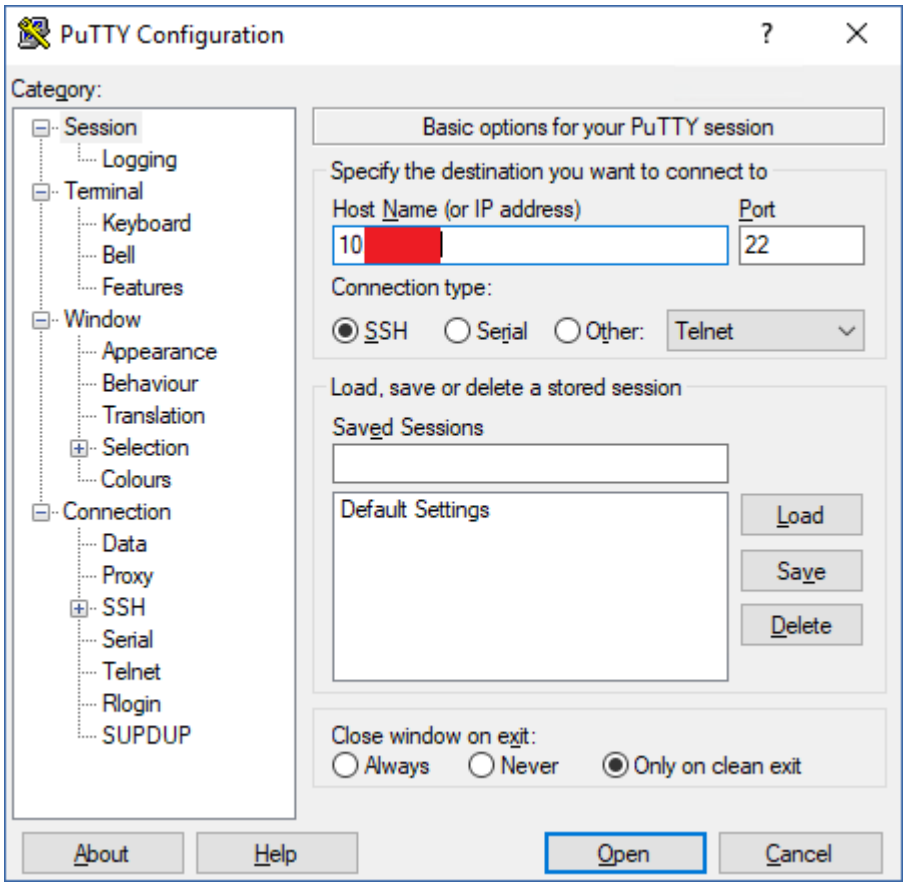
   Es wird eine Warnung angezeigt, dass Sie dabei sind, das Software-Paket eines Drittanbieters zu installieren. Diese Meldung ist Teil der Standardinstallationsprozedur.
4. Klicken Sie auf **Zustimmen**, um zu bestätigen, dass Sie das Paket installieren wollen.
5. Überprüfen Sie die Einstellungen und klicken Sie dann auf **Fertig**.
6. Öffnen Sie im Synology DiskStation Manager **Paket-Zentrum** den Cyber Protect Agenten für Synology und überprüfen Sie dann, ob Sie den nachfolgenden Bildschirm sehen.



7. Gehen Sie in der **Systemsteuerung** des Synology DiskStation Managers zu **Terminal & SNMP** und aktivieren Sie dort den SSH-Zugriff auf das NAS-Gerät.
8. Führen Sie das Skript `install` auf dem NAS-Gerät mithilfe eines SSH-Clients (in diesem Beispiel: Putty) aus.

   Das Skript ermöglicht einen Root-Zugriff auf DSM 7.0 oder höher, der für die Konfiguration des Agenten erforderlich ist.

   a. Starten Sie Putty und spezifizieren Sie die IP-Adresse oder den Host-Namen Ihres NAS-Geräts von Synology.



b. Klicken Sie auf **Öffnen** und melden Sie sich dann als Synology DSM-Administrator an.

c. Führen Sie den nachfolgenden Befehl aus.

```
sudo /var/packages/CyberProtectAgent/target/install/install
```

9. Gehen Sie in der **Systemsteuerung** des Synology DiskStation Managers zu **Terminal & SNMP** und deaktivieren Sie dort den SSH-Zugriff auf das NAS-Gerät. Der SSH-Zugriff wird nicht mehr benötigt.

Agent für Synology 6.x

Voraussetzungen

- Sie auf dem NAS-Gerät ein Mitglied der Gruppe der **Administratoren** sind.
- Auf dem NAS-Volume, auf dem Sie den Agenten installieren wollen, mindestens 200 MB an freiem Speicherplatz vorhanden sind.

So können Sie den Agenten für Synology aktualisieren

1. Öffnen Sie das **Paket-Zentrum** im DiskStation Manager.
2. Klicken Sie dort zuerst auf **Manuelle Installation** und dann auf **Durchsuchen**.
3. Wählen Sie die neuere SPK-Datei des Agenten für Synology 6.x aus, die Sie von der Cyber Protect-Konsole heruntergeladen haben, und klicken Sie dann auf **Weiter**.

Es wird eine Warnung angezeigt, dass Sie dabei sind, ein Paket ohne digitale Signatur zu installieren. Diese Meldung ist Teil der Standardinstallationsprozedur.

4. Klicken Sie auf **Ja**, um zu bestätigen, dass Sie das Paket installieren wollen.
5. Überprüfen Sie die Einstellungen und klicken Sie dann auf **Anwenden**.

Agenten per Gruppenrichtlinie bereitstellen

Sie können den Agenten für Windows durch Verwendung einer Windows-Gruppenrichtlinie zentral auf Maschinen installieren (oder bereitstellen), die Mitglieder einer Active Directory-Domain sind.

Dieser Abschnitt erläutert, wie Sie ein Gruppenrichtlinienobjekt einrichten, um Agenten auf Maschinen in einer kompletten Domain oder deren Organisationseinheit bereitzustellen.

Jedes Mal, wenn sich eine Maschine an der Domain anmeldet, stellt das entsprechende Gruppenrichtlinienobjekt sicher, dass der Agent installiert und registriert ist.

Voraussetzungen

- Eine Active Directory-Domain mit einem Domain Controller, die unter Microsoft Windows Server 2003 oder höher läuft.
- Sie müssen in dieser Domain ein Mitglied der Gruppe **Domänen-Admins** sein.
- Sie das Setup-Programm **Alle Agenten für Windows** heruntergeladen haben.
  Wenn Sie das Setup-Programm herunterladen wollen, müssen Sie in der rechten oberen Ecke der Cyber Protect-Konsole zuerst auf das Symbol 'Konto' klicken und anschließend auf **Downloads**. Der Download-Link ist auch im Fensterbereich **Geräte hinzufügen** verfügbar.

So können Sie Agenten über Gruppenrichtlinien bereitstellen

1. Generieren Sie ein Registrierungstoken (wie im Abschnitt '"Ein Registrierungstoken generieren" (S. 182)' beschrieben).
2. Erstellen Sie die .mst-, .msi- und .cab-Dateien (wie in Abschnitt '"Die Transformdatei erstellen und die Installationspakete erstellen" (S. 185)' beschrieben).
3. Richten Sie das Gruppenrichtlinienobjekt ein (wie im Abschnitt '"Das Gruppenrichtlinienobjekt aufsetzen" (S. 186)' beschrieben).

Ein Registrierungstoken generieren

Ein Registrierungstoken übermittelt die Identität eines Benutzers an das Setup-Programm des Agenten, ohne dass dabei die Anmeldedaten des Benutzers für die Cyber Protect-Konsole gespeichert werden. Dadurch können Benutzer eine beliebige Anzahl von Maschinen unter ihrem Konto registrierenoder Schutzpläne auf ihre Workloads anzuwenden, ohne sich anmelden zu müssen.

Hinweis
Schutzpläne werden während der Registrierung einer Maschine nicht automatisch angewendet. Das Anwenden eines Schutzplans ist ein separater Task.

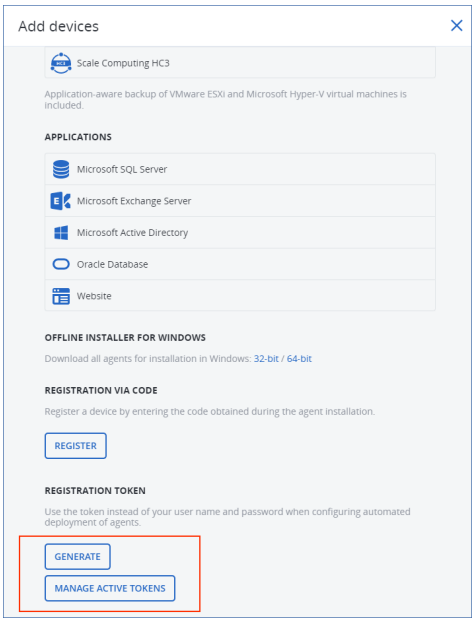
Aus Sicherheitsgründen haben die Token eine begrenzte Lebensdauer, die Sie festlegen können. Die Standard-Lebensdauer beträgt 3 Tage.

Benutzer können Registrierungstoken nur für ihre eigenen Konten generieren. Administratoren können Registrierungstoken für alle Benutzerkonten in demjenigen Mandanten generieren, der von ihnen verwaltet wird.

So können Sie ein Registrierungstoken generieren

Als Benutzer

1. Melden Sie sich an der Cyber Protect-Konsole an.
2. Klicken Sie auf **Geräte** –> **Alle Geräte** –> **Hinzufügen**.
   Der Fensterbereich **Geräte hinzufügen** wird auf der rechten Seite geöffnet.
3. Scrollen Sie bis zu **Registrierungstoken** runter und klicken Sie dann auf **Generieren**.



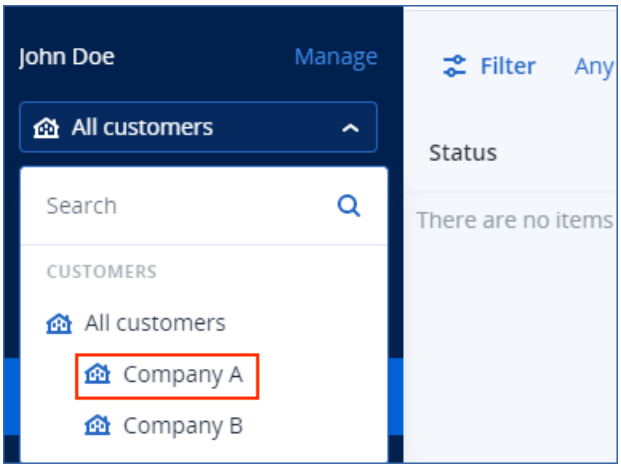
4. Spezifizieren Sie die Token-Lebensdauer.
5. Klicken Sie auf **Token generieren**.
6. Klicken Sie auf **Kopieren**, um das Token in die Zwischenablage Ihres Geräts zu kopieren. Alternativ können Sie das Token auch manuell aufschreiben.

Als Administrator

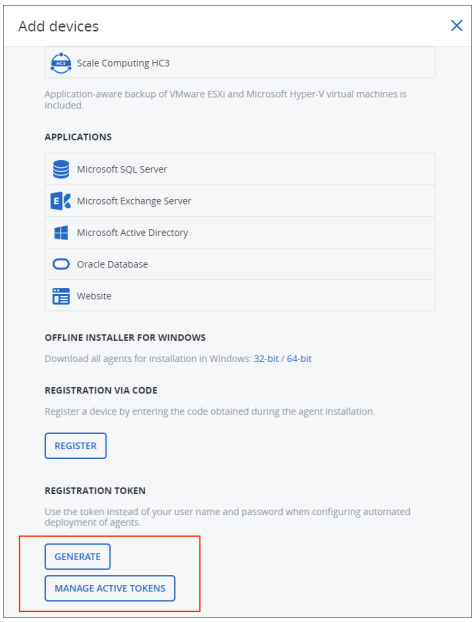
1. Melden Sie sich als Administrator an der Cyber Protect-Konsole an.

Wenn Sie bereits am Management-Portal angemeldet sind, können Sie zur Cyber Protect-Konsole gehen, indem Sie zu **Monitoring** –> **Nutzung** navigieren und dann in der Registerkarte **Schutz** auf **Service verwalten**.

[Für Partner-Administratoren, die Kunden-Mandanten verwalten] Wählen Sie in der Cyber Protect-Konsole den Mandanten mit demjenigen Benutzer aus, für den Sie ein Token generieren wollen. Sie können kein Token auf der Ebene **Alle Kunden** generieren.



2. Klicken Sie unter **Geräte** auf **Alle Geräte** –> **Hinzufügen**.
   Der Fensterbereich **Geräte hinzufügen** wird auf der rechten Seite geöffnet.
3. Scrollen Sie bis zu **Registrierungstoken** runter und klicken Sie dann auf **Generieren**.



4. Spezifizieren Sie die Token-Lebensdauer.
5. Wählen Sie den Benutzer, für den Sie ein Token generieren wollen.

   Hinweis
   Wenn Sie das Token verwenden, werden die Workloads unter dem Benutzerkonto registriert, welches Sie hier auswählen.

6. [Optional] Wenn Sie es dem Benutzer des Tokens ermöglichen wollen, auf den hinzugefügten Workloads einen Schutzplan anzuwenden oder zu widerrufen, wählen Sie den entsprechenden Plan in dem Listenfeld aus.
   Beachten Sie, dass Sie ein Skript ausführen müssen, das einen Schutzplan auf den hinzugefügten Workloads anwendet oder die Anwendung wieder aufhebt. Weitere Informationen finden Sie in diesem Knowledge Base-Artikel.
7. Klicken Sie auf **Token generieren**.
8. Klicken Sie auf **Kopieren**, um das Token in die Zwischenablage Ihres Geräts zu kopieren. Alternativ können Sie das Token auch manuell aufschreiben.

So können Sie Registrierungstoken anzeigen oder löschen

1. Melden Sie sich an der Cyber Protect-Konsole an.
2. Klicken Sie auf **Geräte** –> **Alle Geräte** –> **Hinzufügen**.
3. Scrollen Sie bis zu **Registrierungstoken** runter und klicken Sie dann auf **Aktive Tokens verwalten**.
   Auf der rechten Seite wird eine Liste mit den aktiven Token angezeigt, die für Ihren Mandanten generiert wurden.

   Hinweis
   Aus Sicherheitsgründen werden in der Spalte **Token** nur die ersten beiden Zeichen des jeweiligen Token-Wertes angezeigt.

4. [Wenn Sie ein Token löschen wollen] Wählen Sie das Token zuerst aus und klicken Sie dann auf **Löschen**.

Die Transformdatei erstellen und die Installationspakete erstellen

Wenn Sie die Protection Agenten per Windows-Gruppenrichtlinie bereitstellen wollen, benötigen Sie eine Transformdatei (.mst) und die Installationspakete (.msi- und .cab-Dateien).

Hinweis
Die nachfolgende Prozedur verwendet die Standardregistrierungsoption, nämlich eine Registrierung per Token. Weitere Informationen über die Generierung eines Registrierungstokens finden Sie im Abschnitt '"Ein Registrierungstoken generieren" (S. 182)'.

So können Sie die .mst-Datei erstellen und die Installationspakete (.msi- und .cab-Dateien) extrahieren

1. Melden Sie sich als Administrator an einer beliebigen Maschine in der Active Directory-Domain an.
2. Erstellen Sie einen freigegebenen Ordner, in dem die Installationspakete gespeichert werden sollen. Stellen Sie sicher, dass alle Domain-Benutzer auf diesen freigegebenen Ordner zugreifen können – beispielsweise indem Sie die vorgegebenen Freigabeeinstellungen für **Jeder** übernehmen.
3. Führen Sie das Setup-Programm des Agenten aus.
4. Klicken Sie auf **.mst- und .msi-Dateien für eine unbeaufsichtigte Installation erstellen**.
5. Wählen Sie bei **Zu installierende Komponenten** diejenigen Komponenten aus, die Sie in die Installation aufnehmen wollen, und klicken Sie anschließend auf **Fertig**.
6. Klicken Sie in den **Registrierungseinstellungen** auf **Spezifizieren**, geben Sie ein Registrierungstoken ein und klicken Sie anschließend auf **Fertig**.
   Sie können die Registrierungsmethode von **Registrierungstoken verwenden** (Standard) auf **Anmeldedaten verwenden** oder **Registrierung überspringen** ändern. Die Option **Registrierung überspringen** setzt voraus, dass Sie die Workloads später manuell registrieren werden.
7. Überprüfen oder ändern Sie die Installationseinstellungen, die der .mst-Datei hinzugefügt werden, und klicken Sie dann auf **Fortsetzen**.
8. Spezifizieren Sie bei **Speicherziel für die Dateien** den Pfad zu dem freigegebenen Ordner, den Sie erstellt haben.
9. Klicken Sie auf **Generieren**.

Als Ergebnis werden die .mst-, .msi- und .cab-Dateien erstellt und in den von Ihnen spezifizierten freigegebenen Ordner kopiert.

Als Nächstes müssen Sie das Windows-Gruppenrichtlinienobjekt einrichten. Informationen zur entsprechenden Durchführung finden Sie im Abschnitt '"Das Gruppenrichtlinienobjekt aufsetzen" (S. 186)'.

Das Gruppenrichtlinienobjekt aufsetzen

Sie verwenden in dieser Prozedur die Installationspakete, die Sie in '"Die Transformdatei erstellen und die Installationspakete erstellen" (S. 185)' erstellt haben, um ein Gruppenrichtlinienobjekt einzurichten. The Group Policy object will deploy the agents onto the machines in your domain.

So können Sie das Gruppenrichtlinienobjekt einrichten

1. Melden Sie sich als Domain-Administrator am Domain Controller an.
   Wenn es in der Domain mehr als einen Domain Controller gibt, können Sie sich bei jedem von diesen als Domain-Administrator anmelden.

2. [Wenn Sie Agenten in einer Organisationseinheit bereitstellen] Stellen Sie sicher, dass die Organisationseinheit, in der Sie die Agenten bereitstellen wollen, in der Domain auch vorhanden ist.
3. Gehen Sie im Windows-**Startmenü** zu **Verwaltung** und klicken Sie dann auf **Gruppenrichtlinienverwaltung** (oder beim Windows Server 2003 auf **Active Directory-Benutzer und -Computer**).
4. [Für Windows Server 2008 oder höher] Klicken Sie mit der rechten Maustaste auf den Namen der Domain oder Organisationseinheit, klicken Sie danach auf **Gruppenrichtlinienobjekt hier erstellen und verknüpfen**.
5. [Für Windows Server 2003] Klicken Sie mit der rechten Maustaste auf den Namen der Domain oder Organisationseinheit und wählen Sie dann **Eigenschaften**. Klicken Sie im Dialogfenster auf die Registerlasche **Gruppenrichtlinien** und wählen Sie dann **Neu**.
6. Bezeichnen Sie das neue Gruppenrichtlinienobjekt als **Agent für Windows**.
7. Öffnen Sie das Gruppenrichtlinienobjekt **Agent für Windows** zur Bearbeitung:
   - [Im Windows Server 2008 oder höher] Klicken Sie unter **Gruppenrichtlinienobjekte** mit der rechten Maustaste auf das Gruppenrichtlinienobjekt und dann auf den Befehl **Bearbeiten**.
   - [Im Windows Server 2003] Klicken Sie auf das Gruppenrichtlinienobjekt und dann auf den Befehl **Bearbeiten**.
8. Erweitern Sie im Snap-In 'Gruppenrichtlinienobjekt-Editor' den Eintrag **Computerkonfiguration**.
9. [Für Windows Server 2012 oder höher] Erweitern Sie **Richtlinien** –> **Softwareeinstellungen**.
10. [Für Windows Server 2003 und Windows Server 2008] Erweitern Sie **Softwareeinstellungen**.
11. Klicken Sie mit der rechten Maustaste auf **Softwareinstallation**, wählen Sie dort **Neu** und klicken Sie anschließend auf **Paket**.
12. Wählen Sie das .mis-Installationspaket des Agenten in dem von Ihnen erstellten, freigegebenen Ordner und klicken Sie dann auf **Öffnen**.
13. Klicken Sie im Dialogfenster **Software bereitstellen** auf **Erweitert** und bestätigen Sie dann mit **OK**.
14. Klicken Sie in der Registerkarte **Modifikationen** auf **Hinzufügen** und wählen Sie dann die .mst-Datei in dem freigegebenen Ordner, den Sie erstellt haben.
15. Klicken Sie auf **OK** und schließen Sie das Dialogfenster **Software bereitstellen**.

SSH-Verbindungen zu einer virtuellen Appliance

Verwenden Sie eine SSH-Verbindung (Secure Socket Shell), wenn Sie eine virtuelle Appliance per Remote-Zugriff fernwarten wollen.

Den Secure Shell-Daemon starten

Wenn Sie SSH-Verbindungen zu einer virtuellen Appliance zulassen wollen, müssen Sie zunächst den Secure Shall-Daemon (sshd) auf der Appliance starten.

So können Sie den Secure Shell-Daemon starten

1. Öffnen Sie in der Hypervisor-Software die Konsole der virtuellen Appliance.
2. Drücken Sie in der grafischen Benutzeroberfläche der Appliance die Tastenkombination STRG+Umschalt+F2, um die Befehlszeilenschnittstelle zu öffnen.
3. Führen Sie folgenden Befehl aus:

   ```
   /bin/sshd
   ```

4. [Nur bei der ersten Verbindung zur Appliance] Legen Sie das Kennwort für den Benutzer `root` fest.

   Weitere Informationen darüber, wie Sie das Kennwort festlegen können, finden Sie im Abschnitt '"Das root-Kennwort für eine virtuelle Appliance festlegen" (S. 188)'.

Hinweis
Wir empfehlen Ihnen, den Secure Shell-Daemon zu stoppen, wenn Sie die SSH-Verbindung nicht verwenden.

Das root-Kennwort für eine virtuelle Appliance festlegen

Bevor Sie erstmalig eine SSH-Verbindung zu einer virtuellen Appliance herstellen, müssen Sie das root-Kennwort auf der Appliance festlegen.

So können Sie das root-Kennwort festlegen

1. Öffnen Sie in der Hypervisor-Software die Konsole der virtuellen Appliance.
2. Drücken Sie in der grafischen Benutzeroberfläche der Appliance die Tastenkombination STRG+Umschalt+F2, um die Befehlszeilenschnittstelle zu öffnen.
3. Führen Sie folgenden Befehl aus:

   ```
   passwd
   ```

4. Spezifizieren Sie ein Kennwort und drücken Sie dann die Eingabetaste.

   Das Kennwort muss mindestens neun Zeichen enthalten und einen Komplexitäts-Score von drei oder mehr haben. Der Komplexitäts-Score wird automatisch berechnet. Wenn Sie einen höheren Score erreichen wollen, müssen Sie eine Kombination aus Sonderzeichen, Groß- und Kleinbuchstaben sowie Zahlen verwenden.
5. Bestätigen Sie das Kennwort und drücken Sie dann die Eingabetaste.

Auf eine virtuelle Appliance über einen SSH-Client zugreifen

Voraussetzungen

- Auf der Remote-Maschine muss ein SSH-Client verfügbar sein. Die nachfolgende Prozedur verwendet den WinSCP-Client als Beispiel. Sie können jeden SSH-Client verwenden, wenn Sie die Schritte entsprechend anpassen.

- Der Secure Shell-Daemon (sshd) muss auf der virtuellen Appliance gestartet werden. Weitere Informationen finden Sie im Abschnitt '"Den Secure Shell-Daemon starten" (S. 187)'.

So können Sie per WinSCP auf eine virtuelle Appliance zugreifen

1. Öffnen Sie WinSCP auf der Remote-Maschine.
2. Klicken Sie auf **Sitzung** –> **Neue Sitzung**.
3. Wählen Sie bei **Übertragungsprotokoll** den Eintrag **SCP**.
4. Spezifizieren bei **Host-Name** die IP-Adresse Ihrer virtuellen Appliance.
5. Spezifizieren Sie unter **Benutzername** und **Kennwort** `root` und das Kennwort für den Benutzer `root`.
6. Klicken Sie auf **Anmelden**.

Es wird eine Liste mit allen Verzeichnissen auf der virtuellen Appliance angezeigt.

Update der Agenten

Sie können alle Agenten manuell aktualisieren – und zwar entweder über die Cyber Protect-Konsole oder indem Sie die Installationsdatei herunterladen und ausführen.

Sie können automatische Updates für folgende Agenten konfigurieren:

- Agent für Windows
- Agent für Linux
- Agent für Mac
- Cyber Files Cloud Agent für File Sync & Share

Für die Aktualisierung eines Agenten, egal ob automatisch oder manuell über die Cyber Protect-Konsole, sind 4,2 GB freier Platz an folgenden Speicherorten erforderlich:

- Für Linux – das Stammverzeichnis
- Bei Windows – das Volume, auf dem der Agent installiert ist

Für die Aktualisierung eines Agenten unter macOS werden 5 GB freier Speicherplatz benötigt – im Stammverzeichnis.

Hinweis
[Für alle Agenten, die über eine virtuelle Appliance bereitgestellt werden, einschließlich dem Agenten für VMware, dem Agenten für Scale Computing, dem Agenten für Virtuozzo Hybrid Infrastructure und dem Agenten für RHV (oVirt)]

Um ein automatisches oder manuelles Update einer virtuellen Appliance, die sich hinter einem Proxy befindet, durchführen zu können, muss der Proxy-Server auf jeder Appliance wie nachfolgend beschrieben konfiguriert werden.

Fügen Sie in der Datei '`/opt/acronis/etc/va-updater/config.yaml`' an deren Ende die nachfolgende Zeile ein und tragen Sie dabei die für Ihre Umgebung spezifischen Werte ein:

```
httpProxy: http://proxy_login:proxy_password@proxy_address:port
```

Agenten manuell aktualisieren

Sie können Agenten entweder über die Cyber Protect-Konsole aktualisieren oder indem Sie die entsprechende Installationsdatei herunterladen und ausführen.

Virtuelle Appliances mit folgenden Versionen dürfen nur über die Cyber Protect-Konsole aktualisiert werden:

- Agent für VMware (Virtuelle Appliance): Version 12.5.23094 und höher.
- Agent für Virtuozzo Hybrid Infrastructure (Virtuelle Appliance): Version 12.5.23094 und höher.

Agenten mit/ab folgenden Versionen können auch über die Cyber Protect-Konsole aktualisiert werden:

- Agent für Windows, Agent für VMware (Windows), Agent für Hyper-V: Version 12.5.21670 und höher.
- Agent für Linux: Version 12.5.23094 und höher.
- Andere Agenten: Version 12.5.23094 und höher.

Sie können die Agenten-Version in der Cyber Protect-Konsole ermitteln, indem Sie die betreffende Maschine auswählen und dann auf den Befehl **Details** klicken.

Wenn Sie ältere Versionen dieser Agenten aktualisieren wollen, müssen Sie die neueste Agenten-Version erst manuell herunterladen und installieren. Sie können die Download-Links ermitteln, indem Sie auf **Alle Geräte** –> **Hinzufügen** klicken.

Voraussetzungen

Auf Windows-Maschinen ist es für die Cyber Protect-Funktionen erforderlich, dass das Microsoft Visual C++ 2017 Redistributable-Paket installiert ist. Überprüfen Sie, dass dieses bereits auf Ihrer Maschine installiert ist. Wenn nicht, müssen Sie es vor dem Update des Agenten installieren. Nach der Installation ist möglicherweise ein Neustart der Maschine erforderlich. Sie können das Microsoft

Visual C++ Redistributable-Paket auf der Microsoft-Website finden: https://support.microsoft.com/help/2999226/update-for-universal-c-runtime-in-windows.

So können Sie das Update eines Agenten über die Cyber Protect-Konsole durchführen:

1. Klicken Sie auf **Einstellungen** –> **Agenten**.
   Die Software zeigt eine Liste der Maschinen an. Maschinen mit einer veralteten Agenten-Version sind mit einem orangefarbenen Ausrufezeichen gekennzeichnet.
2. Wählen Sie die Maschinen aus, auf denen Sie die Agenten aktualisieren wollen. Diese Maschinen müssen online sein.
3. Klicken Sie auf **Agent aktualisieren**.

Hinweis
Alle Backups, die während des Updates ausgeführt werden, werden fehlschlagen.

So können Sie einen Agenten für VMware (Virtuelle Appliance), dessen Version kleiner als 12.5.23094 ist, aktualisieren

1. Klicken Sie auf **Einstellungen** –> **Agenten** –> den zu aktualisierenden Agenten –> **Details** und untersuchen Sie den Bereich **Zugewiesene virtuelle Maschinen**. Sie müssen diese Einstellungen nach dem Update erneut eingeben.
   a. Notieren Sie sich die Position des Schalters **Automatische Zuweisung**.
   b. Um herauszufinden, welche virtuellen Maschinen dem Agenten manuell zugewiesen wurden, müssen Sie auf den Link **Zugewiesen:** klicken. Die Software zeigt eine Liste der zugewiesenen virtuellen Maschinen an. Notieren Sie sich die Maschinen, die ein `(M)` nach dem Agenten-Namen in der Spalte **Agent** haben.
2. Entfernen Sie den Agenten für VMware (Virtuelle Appliance) gemäß der Beschreibung im Abschnitt 'Agenten deinstallieren'. Löschen Sie in Schritt 5 den Agenten über **Einstellungen** –> **Agenten**, obwohl Sie planen, den Agenten erneut zu installieren.
3. Stellen Sie den Agenten für VMware (Virtuelle Appliance) gemäß der Beschreibung im Abschnitt 'Deployment der OVF-Vorlage' bereit.
4. Konfigurieren Sie den Agenten für VMware (Virtuelle Appliance) gemäß der Beschreibung im Abschnitt 'Agenten deinstallieren'.
   Wenn Sie den lokal angeschlossenen Storage wieder aufbauen wollen, gehen Sie in Schritt 7 folgendermaßen vor:
   a. Fügen Sie das Laufwerk, welches den lokalen Storage enthält, der virtuellen Appliance hinzu.
   b. Klicken Sie auf **Aktualisieren** –> **Storage erstellen** > **Mounten**.
   c. Die Software zeigt den ursprünglichen **Buchstaben** und die **Bezeichung** des Laufwerks an. Übernehmen Sie die Einstellungen, ohne diese zu ändern.
   d. Klicken Sie auf **OK**.
5. Klicken Sie auf folgende Befehlsreihe: **Einstellungen** –> **Agenten** –> den Agenten, den Sie aktualisieren wollen, –> **Details** und rekonstruieren Sie dann die Einstellungen, die Sie sich in Schritt 1 notiert haben. Wenn einige virtuelle Maschinen dem Agenten manuell zugewiesen

wurden, weisen Sie diese erneut zu (wie im Abschnitt 'Virtuelle Maschinen anbinden' beschrieben).

Sobald die Agenten-Konfiguration abgeschlossen ist, werden die Schutzpläne, die auf den alten Agenten angewendet wurden, automatisch wieder auf den neuen Agenten angewendet.

6. Pläne mit aktiviertem applikationskonformen Backup erfordern eine erneute Eingabe der Anmeldedaten für das Gastbetriebssystem. Bearbeiten Sie diese Pläne und geben Sie die Anmeldedaten neu ein.
7. Pläne, mit denen die ESXi-Konfiguration gesichert wird, erfordern eine erneute Eingabe des Kennworts für das 'root'-Konto. Bearbeiten Sie diese Pläne und geben Sie das Kennwort neu ein.

So können Sie die Cyber Protection-Definitionen auf einer Maschine aktualisieren

1. Klicken Sie auf **Einstellungen** –> **Agenten**.
2. Wählen Sie die Maschine aus, auf welcher Sie die Cyber Protection-Definitionen aktualisieren wollen, und klicken Sie dann auf **Definitionen aktualisieren**. Diese Maschine muss online sein.

So können Sie einem Agenten die Rolle 'Updater' zuweisen

1. Klicken Sie auf **Einstellungen** –> **Agenten**.
2. Wählen Sie die Maschine aus, der Sie die Updater-Rolle zuweisen wollen, klicken Sie auf **Details** und aktivieren Sie dann im Bereich **Cyber Protection-Definitionen** die Option **Diesen Agenten verwenden, um Patches und Updates herunterzuladen und zu verteilen**.

Hinweis
Ein Agent mit der Rolle 'Updater' kann nur Patches für Windows-Produkte von Drittanbietern herunterladen und verteilen. Die Verteilung von Patches für Microsoft-Produkte wird vom Updater-Agenten nicht unterstützt.

So können Sie zwischengespeicherte Daten auf einem Agenten löschen

1. Klicken Sie auf **Einstellungen** –> **Agenten**.
2. Wählen Sie die Maschine aus, auf der Sie die zwischengespeicherten Daten (veraltete Update-Dateien und Patch-Verwaltungsdateien) bereinigen wollen, und klicken Sie auf **Cache löschen**.

Agenten automatisch aktualisieren

Wenn Sie die Verwaltung mehrerer Workloads erleichtern wollen, können Sie konfigurieren, dass der Agent für Windows, der Agent für Linux und der Agent für Mac automatisch aktualisiert werden sollen. Automatische Updates sind für Agenten mit der Version 15.0.26986 (im Mai 2021 veröffentlicht) und höher verfügbar. Ältere Agenten müssen zuerst noch manuell auf die neueste Version aktualisiert werden.

Automatische Updates werden auf Maschinen unterstützt, die unter einem der folgenden Betriebssysteme laufen:

- Windows XP SP 3 und höher
- Red Hat Enterprise Linux 6 und höher, CentOS 6 und höher
- OS X 10.9 Mavericks und höher

Die Einstellungen für automatische Updates werden auf Datacenter-Ebene vorkonfiguriert. Ein Firmenadministrator kann diese Einstellungen anpassen – entweder für alle Maschinen in einer Firma, einer Abteilung oder für einzelne Maschinen. Wenn keine benutzerdefinierten Einstellungen vorgenommen werden, werden die Einstellungen aus der übergeordneten Ebene verwendet – und zwar in dieser Reihenfolge:

1. Cyber Protection Datacenter
2. Firma (Kunden-Mandanten)
3. Abteilung
4. Maschine

Ein Abteilungsadministrator kann beispielsweise benutzerdefinierte Auto-Update-Einstellungen für alle Maschinen in der Abteilung konfigurieren, die sich von der Einstellung für die Maschinen auf Firmenebene unterscheiden können. Der Administrator kann auch unterschiedliche Einstellungen für eine oder mehrere bestimmte Maschinen in der Abteilung konfigurieren, für die weder die Einstellungen der Abteilung noch die der Firma übernommen werden.

Nachdem Sie die automatischen Updates aktiviert haben, können Sie folgende Optionen konfigurieren:

- **Update-Channel**
  Der Update-Channel definiert, welche Version der Agenten verwendet wird – die aktuellste oder die letzte Version aus dem vorherigen Release.
- **Wartungsfenster**
  Das Wartungsfenster definiert, wann Updates installiert werden können. Wenn das Wartungsfenster deaktiviert ist, können Updates immer ausgeführt werden.
  Auch innerhalb eines aktivierten Wartungsfensters werden keine Updates installiert, wenn der Agent gerade eine der folgenden Aktionen ausführt:
  - Backup
  - Recovery
  - Backup-Replikation
  - Replikation von virtuellen Maschinen
  - Ein Replikat testen
  - Eine virtuelle Maschine aus einem Backup heraus ausführen (einschließlich Finalisierung)
  - Disaster Recovery-Failover
  - Disaster Recovery-Failback
  - Ein Skript ausführen (für Cyber Scripting-Funktionalität)

- Patch-Installation
- ESXi-Konfigurations-Backup

So können Sie die Auto-Update-Einstellungen anpassen

1. Gehen Sie in der Cyber Protect-Konsole zu **Einstellungen** –> **Agenten**.
2. Wählen Sie den Umfang für die Einstellungen:
   - Wenn Sie die Einstellungen für alle Maschinen ändern wollen, klicken Sie auf **Standardeinstellungen für das Agenten-Update bearbeiten**.
   - Wenn Sie die Einstellungen nur für bestimmte Maschinen ändern wollen, wählen Sie die gewünschten Maschinen aus und klicken Sie dann auf **Einstellungen für das Agenten-Update**.
3. Konfigurieren Sie die Einstellungen nach Ihren Anforderungen und klicken Sie anschließend auf **Anwenden**.

So können Sie die benutzerdefinierten Auto-Update-Einstellungen entfernen

1. Gehen Sie in der Cyber Protect-Konsole zu **Einstellungen** –> **Agenten**.
2. Wählen Sie den Umfang für die Einstellungen:
   - Wenn Sie die benutzerdefinierten Einstellungen für alle Maschinen entfernen wollen, klicken Sie auf **Standardeinstellungen für das Agenten-Update bearbeiten**.
   - Wenn Sie die benutzerdefinierten Einstellungen für bestimmte Maschinen entfernen wollen, wählen Sie die gewünschten Maschinen aus und klicken Sie dann auf **Einstellungen für das Agenten-Update**.
3. Klicken Sie zuerst auf **Auf Standard zurücksetzen** und dann auf **Anwenden**.

So können Sie den Auto-Update-Status überprüfen

1. Gehen Sie in der Cyber Protect-Konsole zu **Einstellungen** –> **Agenten**.
2. Klicken Sie in der rechten oberen Ecke der Tabelle auf das Zahnradsymbol und stellen Sie sicher, dass das Kontrollkästchen **Auto-Update** aktiviert ist.
3. Überprüfen Sie den Status, der in der Spalte **Auto-Update** angezeigt wird.

Agenten auf BitLocker-geschützten Workloads aktualisieren

Agenten-Updates, die Änderungen am Startup Recovery Manager vornehmen, beeinträchtigen BitLocker auf solchen Workloads, auf denen sowohl BitLocker als auch der Startup Recovery Manager aktiviert sind. In diesem Fall wird nach einem Neustart der BitLocker-Wiederherstellungsschlüssel benötigt. Wenn Sie dieses Problem vermeiden wollen, sollten Sie BitLocker vor dem Agenten-Update aussetzen oder deaktivieren.

Betroffene Agenten-Versionen:

- 23.12.36943, im Dezember 2023 veröffentlicht

Hinweise darüber, ob ein Update Änderungen am Startup Recovery Manager mit sich bringt, können Sie den jeweiligen Release Notes für den Protection Agenten entnehmen.

So können Sie den Agenten auf einem Workload aktualisieren, auf dem BitLocker und der Startup Recovery Manager aktiviert sind

1. Setzen Sie auf dem Workload, auf dem Sie den Agenten aktualisieren wollen, BitLocker aus oder deaktivieren Sie dieses.
2. Aktualisieren Sie den Agenten.
3. Starten Sie den Workload neu.
4. Aktivieren Sie Bitlocker.

Unbefugte Deinstallationen oder Änderungen der Agenten verhindern

Sie können den Agenten für Windows vor einer unbefugten Deinstallation oder Änderung schützen, wenn Sie in einem Schutzplan die Einstellung **Kennwortschutz** aktivieren. Diese Einstellung ist jedoch nur verfügbar, wenn die Einstellung **Selbstschutz** aktiviert ist.

So können Sie den Kennwortschutz aktivieren

1. Erweitern Sie in einem Schutzplan das Modul **Antivirus & Antimalware Protection** (bei den Cyber Backup-Editionen ist es das Modul **Active Protection**).
2. Klicken Sie auf **Selbstschutz** und überprüfen Sie, dass der Schalter **Selbstschutz** eingeschaltet ist.
3. Aktivieren Sie den Schalter **Kennwortschutz**.
4. Kopieren Sie in dem sich öffnenden Fenster das Kennwort, das Sie zur Deinstallation oder Änderung der Komponenten eines geschützten Agenten für Windows benötigen.
   Dieses Kennwort ist individuell und Sie können es nicht wiederherstellen, nachdem Sie dieses Fenster geschlossen haben. Wenn Sie dieses Kennwort verlieren oder vergessen, können Sie jedoch den Schutzplan bearbeiten und ein neues Kennwort erstellen.
5. Klicken Sie auf **Schließen**.
6. Klicken Sie im Fensterbereich **Selbstschutz** auf den Befehl **Fertig**.
7. Speichern Sie den Schutzplan.

Der Kennwortschutz wird für all die Maschinen aktiviert, auf die dieser Schutzplan angewendet wird. Der Kennwortschutz ist nur für Agenten für Windows mit der Version *15.0.25851* und höher verfügbar. Diese Maschinen müssen online sein.

Sie können einen Schutzplan mit aktiviertem Kennwortschutz zwar auf eine Maschine anwenden, die unter macOS läuft, aber der entsprechende Schutz wird hier nicht bereitgestellt. Sie können einen solchen Plan auf keine Maschine anwenden, die unter Linux läuft.

Sie können auch nicht mehrere Schutzpläne mit aktiviertem Kennwortschutz auf ein und dieselbe Maschine anwenden, die unter Windows läuft. Weitere Informationen zur Lösung eines möglichen Konflikts finden Sie im Abschnitt 'Plan-Konflikte lösen'.

So können Sie das Kennwort in einem bereits vorhandenen Schutzplan ändern

1. Erweitern Sie in einem entsprechenden Schutzplan das Modul **Antivirus & Antimalware Protection** (bei der Cyber Backup-Edition ist es das Modul **Active Protection**).
2. Klicken Sie auf **Selbstschutz**.
3. Klicken Sie auf **Neues Kennwort erstellen**.
4. Kopieren Sie in dem sich öffnenden Fenster das Kennwort, das Sie zur Deinstallation oder Änderung der Komponenten eines geschützten Agenten für Windows benötigen.
   Dieses Kennwort ist individuell und Sie können es nicht wiederherstellen, nachdem Sie dieses Fenster geschlossen haben. Wenn Sie dieses Kennwort verlieren oder vergessen, können Sie jedoch den Schutzplan bearbeiten und ein neues Kennwort erstellen.
5. Klicken Sie auf **Schließen**.
6. Klicken Sie im Fensterbereich **Selbstschutz** auf den Befehl **Fertig**.
7. Speichern Sie den Schutzplan.

Agenten deinstallieren

Wenn Sie einen Agenten von einem Workload deinstallieren, wird dieser Workload automatisch aus der Cyber Protect-Konsole entfernt. Sollte der Workload (z.B. aufgrund eines Netzwerkproblems) auch nach der Deinstallation des Agenten noch angezeigt werden, müssen Sie diesen Workload manuell aus der Konsole entfernen. Weitere Informationen über die entsprechende Durchführung finden Sie im Abschnitt '"Workloads aus der Cyber Protect-Konsole entfernen" (S. 366)'.

Hinweis
Bei der Deinstallation eines Agenten werden keine Pläne oder Backups gelöscht.

So können Sie einen Agenten deinstallieren

Windows

1. Melden Sie sich an der Maschine, auf der sich der Agent befindet, als Administrator an.
2. Gehen Sie in der **Systemsteuerung** zu **Programme und Funktionen** (**Software** bei Windows XP).
3. Klicken Sie mit der rechten Maustaste auf **Acronis Cyber Protect** und wählen Sie dann den Befehl **Deinstallieren**.
4. [Für kennwortgeschützte Agenten] Spezifizieren Sie das Kennwort, welches Sie zur Deinstallation des Agenten benötigen, und klicken Sie dann auf **Weiter**.
5. [Optional] Aktivieren Sie das Kontrollkästchen **Protokolle (Logs) und Konfigurationseinstellungen entfernen**.

Falls Sie vorhaben, den Agenten später erneut zu installieren, lassen Sie dieses Kontrollkästchen deaktiviert. Wenn Sie das Kontrollkästchen aktivieren und dann den Agent erneut installieren, wird dieser Workload möglicherweise in der Cyber Protect-Konsole doppelt angezeigt und werden dessen alte Backups möglicherweise nicht mit ihm verknüpft sein.

6. Klicken Sie auf **Deinstallieren**.

Linux

1. Führen Sie auf der Maschine mit dem Agenten den Befehl `/usr/lib/Acronis/BackupAndRecovery/uninstall/uninstall` als Root-Benutzer aus.
2. [Optional] Aktivieren Sie das Kontrollkästchen **Alle Spuren des Produkts (Logs, Tasks, Depots und Konfigurationseinstellungen) entfernen**.
   Falls Sie vorhaben, den Agenten später erneut zu installieren, lassen Sie dieses Kontrollkästchen deaktiviert. Wenn Sie das Kontrollkästchen aktivieren und dann den Agent erneut installieren, wird dieser Workload möglicherweise in der Cyber Protect-Konsole doppelt angezeigt und werden dessen alte Backups möglicherweise nicht mit ihm verknüpft sein.
3. Bestätigen Sie Ihre Entscheidung.

macOS

1. Klicken Sie auf der Maschine, auf der sich der Agent befindet, doppelt auf die .dmg-Installationsdatei.
2. Warten Sie, bis das Betriebssystem das Disk-Image für die Installation geladen hat.
3. Klicken Sie im Image doppelt auf **Deinstallieren**.
4. Geben Sie auf Nachfrage die Administrator-Anmeldedaten an.
5. Bestätigen Sie Ihre Entscheidung.

So können Sie Komponenten deinstallieren, die im Bundle mit dem Agenten für Windows installiert wurden

Sie können einzelne Komponenten, die normalerweise im Bundle mit dem Agenten für Windows kommen (wie etwa den Cyber Protect Monitor, den Agenten für Data Loss Prevention oder den Bootable Media Builder) deinstallieren, ohne dass der Agent für Windows selbst dabei deinstalliert wird.

1. Melden Sie sich an der Maschine, auf der sich der Agent befindet, als Administrator an.
2. Führen Sie das Setup-Programm aus und klicken Sie dann auf **Installierte Komponenten ändern**.
3. Deaktivieren Sie die Kontrollkästchen neben den Komponenten, die Sie deinstallieren wollen – und klicken Sie dann auf **Fertig**.

So können Sie den Agenten für VMware (Virtuelle Appliance) entfernen

1. Melden Sie sich mit dem vSphere Client am vCenter Server an.
2. [Sollte die virtuelle Appliance eingeschaltet sein] Klicken Sie zuerst mit der rechten Maustaste auf die virtuelle Appliance und anschließend auf die Befehle **Betrieb** –> **Ausschalten**. Bestätigen Sie Ihre Entscheidung.
3. [Wenn die virtuelle Appliance einen lokal angeschlossenen Storage auf einem virtuellen Festplattenlaufwerk verwendet] Entfernen Sie den virtuellen Storage aus der virtuellen Appliance.
   a. Klicken Sie mit der rechten Maustaste auf die virtuelle Appliance und wählen Sie **Einstellungen bearbeiten**.
   b. Wählen Sie die virtuelle Festplatte mit dem Storage und klicken Sie auf **Entfernen**.
   c. Klicken Sie unter **Optionen beim Entfernen** auf **Von der virtuellen Maschine entfernen**.
   d. Klicken Sie auf **OK**.

   Die Festplatte verbleibt als Ergebnis im Datenspeicher. Sie können die virtuelle Festplatte an eine andere virtuelle Appliance anschließen.
4. Klicken Sie mit der rechten Maustaste auf die virtuelle Appliance und wählen Sie **Von Festplatte löschen**. Bestätigen Sie Ihre Entscheidung.
5. [Optional] [Wenn Sie diese Appliance nicht mehr verwenden wollen] Gehen Sie in der Cyber Protect-Konsole zu **Backup Storage** –> **Speicherorte** und löschen Sie dann den Speicherort, der dem lokal angeschlossenen Storage entspricht.

Schutzeinstellungen

Wenn Sie die allgemeinen Schutzeinstellungen für Cyber Protection konfigurieren wollen, müssen Sie in der Cyber Protect-Konsole zu **Einstellungen** –> **Schutz** gehen.

Automatische Updates für Komponenten

Standardmäßig können sich alle Agenten mit dem Internet verbinden und Updates herunterladen.

Ein Administrator kann die Bandbreite des Netzwerkverkehrs minimieren, indem er einen oder mehrere Agenten in der Umgebung auswählt und diesen die Updater-Rolle zuweist. Dadurch werden sich die dedizierten Agenten mit dem Internet verbinden und die Updates herunterladen. Alle anderen Agenten werden sich mithilfe der Peer-zu-Peer-Technologie mit den dedizierten Updater-Agenten verbinden und dann die Updates von diesen herunterladen.

Die Agenten ohne die Updater-Rolle werden sich mit dem Internet verbinden, wenn kein dedizierter Updater-Agent in der Umgebung vorhanden ist – oder wenn die Verbindung zu einem dedizierten Updater-Agenten für ca. fünf Minuten nicht hergestellt werden konnte.

Der Updater Agent verteilt Updates und Patches für die Antivirus & Antimalware Protection-, Schwachstellenbewertungs- und Patch-Verwaltungsfunktionalität. Es werden aber keine Updates auf eine neue Agenten-Version verteilt.

Hinweis
Ein Agent mit der Rolle 'Updater' kann nur Patches für Windows-Produkte von Drittanbietern herunterladen und verteilen. Die Verteilung von Patches für Microsoft-Produkte wird vom Updater-Agenten nicht unterstützt.

Bevor Sie einem Agenten die Updater-Rolle zuweisen, sollten Sie sicherstellen, dass die Maschine mit diesem Agenten ausreichend leistungsfähig ist, einen stabilen und schnellen Internetzugang hat und über genügend freien Speicherplatz verfügt.

So können Sie eine Maschine für die Updater-Rolle vorbereiten

1. Wenden Sie auf der Maschine des Agenten, auf der Sie die Updater-Rolle aktivieren wollen, folgende Firewall-Regeln an:
   - Eingehend (ankommend) "updater_incoming_tcp_ports": erlaube die Verbindung zu den TCP-Ports 18018 und 6888 für alle Firewall-Profile (öffentlich, privat und Domain).
   - Eingehend (ankommend) "updater_incoming_udp_ports": erlaube die Verbindung zu den UDP-Ports 6888 für alle Firewall-Profile (öffentlich, privat und Domain).
2. Starten Sie den Dienst 'Acronis Agent Core Service' neu.
3. Starten Sie den Firewall-Dienst neu.

Wenn Sie diese Regeln nicht anwenden und die Firewall aktiviert ist, werden die Peer-Agenten die Updates aus der Cloud heruntergeladen.

So können Sie einem Protection Agenten die Rolle 'Updater' zuweisen

1. Gehen Sie in der Cyber Protect-Konsole zu **Einstellungen** –> **Agenten**.
2. Wählen Sie die Maschine mit demjenigen Agenten aus, dem Sie die Updater-Rolle zuweisen wollen.
3. Klicken Sie auf **Details** und aktivieren Sie dann den Schalter **Diesen Agenten verwenden, um Patches und Updates herunterzuladen und zu verteilen**.

Das Peer-zu-Peer-Update funktioniert folgendermaßen.

1. Der Agent mit der Updater-Rolle prüft per Zeitplan eine vom Service-Provider bereitgestellte Indexdatei, um die Kernkomponenten zu aktualisieren.
2. Der Agent mit der Updater-Rolle startet den Download und verteilt die heruntergeladenen Updates anschließend an alle anderen Agenten.

Sie können die Updater-Rolle mehreren Agenten in der Umgebung zuweisen. Wenn dann ein Agent mit der Updater-Rolle offline ist, können andere Agenten mit dieser Rolle als Quelle für die Definitions-Updates dienen.

Die Cyber Protection-Definitionen per Planung aktualisieren

Sie können in der Registerkarte **Planung** für jede der folgenden Komponenten festlegen, ob die Cyber Protection-Definitionen automatisch per Zeitplanung aktualisiert werden sollen.

- Antimalware
- Schwachstellenbewertung
- Patch-Verwaltung

Wenn Sie die Einstellungen der Definitionsupdates ändern wollen, müssen Sie zu **Einstellungen** –> **Schutz** –> **Update der Schutzdefinitionen** –> **Planung** gehen.

Planungstyp:

- **Täglich** – definieren Sie, an welchen Wochentagen die Definitionen aktualisiert werden sollen.
  Starten um – wählen Sie, zu welchem Zeitpunkt die Definitionen aktualisiert werden sollen.
- **Stündlich** – definieren Sie eine genauere stündliche Planung für die Aktualisierungen.
  Ausführen alle/jede(n) – definieren Sie eine Periodizität für die Aktualisierungen.
  Von ... **Bis** – definieren Sie einen bestimmten Zeitraum für die Aktualisierungen.

Die Cyber Protection-Definitionen bei Bedarf aktualisieren

So können Sie das Update der Cyber Protection-Definitionen auf einer bestimmten Maschine manuell anstoßen

1. Gehen Sie in der Cyber Protect-Konsole zu **Einstellungen** –> **Agenten**.
2. Wählen Sie die Maschinen aus, auf denen Sie die Schutzdefinitionen aktualisieren wollen, und klicken Sie dann auf **Definitionen aktualisieren**.

Cache Storage

Der Speicherort der gecachten Daten ist:

- Auf Windows-Maschinen: `C:\ProgramData\Acronis\Agent\var\atp-downloader\Cache`
- Auf Linux-Maschinen: `/opt/acronis/var/atp-downloader/Cache`
- Auf macOS-Maschinen: `/Library/Application Support/Acronis/Agent/var/atp-downloader/Cache`

Wenn Sie die Einstellungen der Cache Storage ändern wollen, müssen Sie zu **Einstellungen** –> **Schutz** –> **Update der Schutzdefinitionen** –> **Cache Storage** gehen.

Spezifizieren Sie über die Option **Veraltete Update-Dateien und Patch-Verwaltungsdaten**, nach welchem Zeitraum die zwischengespeicherten Daten wieder entfernt werden sollen.

Maximale Größe des Cache Storage (GB) für Agenten:

- **Updater-Rolle** – definieren Sie den Speicherplatz, der dem Cache auf den Maschinen mit der Rolle 'Updater' zugewiesen wird.
- **Andere Rollen** – definieren Sie den Speicherplatz, der dem Cache auf anderen Maschinen zugewiesen wird.

Hinweis
Cyber Protection sammelt Samples von erkannter Malware für zusätzliche Analysen, damit wir unsere Software verbessern können. Sie können diese Einstellung jederzeit über die Registerkarte **Schutz** ändern, indem Sie den Schalter **Malware-Samples sammeln und zum CPOC hochladen** deaktivieren.

Die Service-Quota von Maschinen ändern

Eine Service-Quota wird automatisch zugewiesen, wenn ein Schutzplan erstmalig auf eine Maschine angewendet wird.

Die am besten geeignete Quota wird in Abhängigkeit von der Art der geschützten Maschine, ihrem Betriebssystem, der erforderlichen Schutzstufe sowie der Quota-Verfügbarkeit zugewiesen. Wenn die am besten geeignete Quota nicht in Ihrem Unternehmen verfügbar ist, wird die zweitbeste Quota zugewiesen. Wenn beispielsweise die Quota **Webhosting-Server** am besten geeignet wäre, diese jedoch nicht verfügbar ist, wird die Quota **Server** zugewiesen.

Beispiele für Quota-Zuweisungen:

- Einer physischen Maschine, auf der ein Windows Server- oder ein Linux Server-Betriebssystem (wie Ubuntu Server) ausgeführt wird, wird die Quota **Server** zugewiesen.
- Einer physischen Maschine, auf der ein Windows- oder ein Linux-Desktop-Betriebssystem (wie Ubuntu Desktop) ausgeführt wird, wird die Quota **Workstation** zugewiesen.
- Einer physischen Maschine, auf der Windows 10 mit aktivierter Hyper-V-Rolle ausgeführt wird, wird die Quota **Workstation** zugewiesen.
- Einer Desktop-Maschine, die auf einer virtuellen Desktop-Infrastruktur läuft und deren Protection Agent innerhalb des Gastbetriebssystems installiert wurde (wie etwa der Agent für Windows), wird die Quota **Virtuelle Maschine** zugewiesen. Diese Art von Maschine kann auch die Quota **Workstation** verwenden, wenn die Quota **Virtuelle Maschine** nicht verfügbar ist.
- Einer Desktop-Maschine, die auf einer virtuellen Desktop-Infrastruktur läuft und deren Backup im agentenlosen Modus erstellt wird (z.B. durch den Agenten für VMware oder den Agenten für Hyper-V), wird die Quota **Virtuelle Maschine** zugewiesen.
- Einem Hyper-V- oder vSphere-Server wird die Quota **Server** zugewiesen.
- Einem Server mit cPanel oder Plesk wird die Quota **Webhosting-Server** zugewiesen. Abhängig von Art der Maschine, auf welcher der Webserver läuft, könnte er auch die Quota **Virtuelle Maschine** oder **Server** verwenden (falls die die Quota **Webhosting-Server** nicht verfügbar ist).
- Für applikationskonforme Backups ist die Quota **Server** erforderlich, auch wenn es sich bei der Maschine um eine Workstation handelt.

Sie können die ursprüngliche Zuweisung später noch manuell ändern. Wenn Sie etwa einen weitergehenden Schutzplan auf dieselbe Maschine anwenden möchten, müssen Sie möglicherweise die Service-Quota der Maschine upgraden. Wenn die von diesem Schutzplan benötigten Funktionen durch die aktuell zugewiesene Service-Quota nicht unterstützt werden, wird der Schutzplan fehlschlagen.

Sie können die Service-Quota auch noch ändern, wenn Sie eine passendere Quota erwerben, nachdem die ursprüngliche Quota zugewiesen wurde. Beispielsweise, wenn die Quota **Workstations** einer virtuellen Maschine zugewiesen wurde. Nachdem Sie ein Quota **Virtuelle Maschine** erworben haben, können Sie der Maschine dann diese Quota (statt der ursprünglichen Quota **Workstation**) manuell zuweisen.

Sie können die aktuell zugewiesene Service-Quota auch freigeben und diese Quota dann einer ganz anderen Maschine zuweisen.

Sie können die Service-Quota einer einzelnen Maschine oder für eine Gruppe von Maschinen ändern.

So können Sie die Service-Quota einer einzelnen Maschine ändern

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte**.
2. Wählen Sie die gewünschte Maschine und klicken Sie dann auf **Details**.
3. Klicken Sie im Bereich **Service-Quota** auf **Ändern**.
4. Wählen Sie im Fenster **Quota ändern** die gewünschte Service-Quota oder **Keine Quota** aus – und klicken Sie dann auf **Ändern**.

So können Sie die Service-Quota für eine Gruppe von Maschinen ändern

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte**.
2. Wählen Sie mehr als eine Maschine aus und klicken Sie dann auf **Quota zuweisen**.
3. Wählen Sie im Fenster **Quota ändern** die gewünschte Service-Quota oder **Keine Quota** aus – und klicken Sie dann auf **Ändern**.

Die Cyber Protection Services, die in Ihrer Umgebung installiert werden

In Abhängigkeit davon, welche Cyber Protection-Optionen Sie verwenden, installiert Cyber Protection einige oder alle der folgenden Services.

In Windows installierte Services

Service-Name	Zweck
Acronis Managed Machine Service	Stellt die Funktionalität für Backup, Recovery, Replikation, Aufbewahrung und Validierung bereit
Acronis Scheduler2 Service	Führt geplante Tasks bei bestimmten Ereignissen
Acronis Active Protection Service	Stellt Schutzfunktionen gegen Ransomware bereit (Ransomware Protection)
Acronis Cyber Protection Service	Stellt Schutzfunktionen gegen Malware bereit (Antimalware Protection)

In macOS installierte Services

Service-Name und -Speicherort	Zweck
`/Library/LaunchDaemons/com.acronis.aakore.plist`	Ermöglicht die Kommunikation zwischen dem Agenten und den Verwaltungskomponenten
`/Library/LaunchDaemons/com.acronis.cyber-protect-service.plist`	Ermöglicht die Erkennung von Malware
`/Library/LaunchDaemons/com.acronis.mms.plist`	Stellt die Backup- und Recovery-Funktionalität bereit
`/Library/LaunchDaemons/com.acronis.schedule.plist`	Führt geplante Tasks aus

Eine Agent-Protokolldatei speichern

Sie können ein Agentenprotokoll in einer .zip-Datei speichern. Wenn ein Backup aus irgendeinem Grund fehlschlägt, hilft diese Datei dem technischen Support, das Problem zu identifizieren.

Standardmäßig ist die Information im Protokoll auf die letzten drei Tage ausgelegt, aber Sie können diesen Zeitraum ändern.

So können Sie Agenten-Protokolle sammeln lassen

1. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Wählen Sie bei **Geräte** die Maschine aus, deren Protokolle gesammelt werden sollen, und klicken Sie dann auf **Aktivitäten**.
   - Wählen Sie bei **Einstellungen** > **Agenten** die Maschine aus, deren Protokolle gesammelt werden sollen, und klicken Sie dann auf **Details**.
2. [Optional] Um den Standardzeitraum zu ändern, für den die Systeminformationen aufgenommen werden sollen, klicken Sie auf den Pfeil neben der Schaltfläche **Systeminformationen sammeln** und bestimmen Sie dann den Zeitraum.
3. Klicken Sie auf **Systeminformationen sammeln**.
4. Spezifizieren Sie bei Aufforderung durch Ihren Webbrowser, wo die Datei gespeichert werden soll.

Site-to-Site-OpenVPN – Zusätzliche Informationen

Wenn Sie einen Recovery-Server erstellen, konfigurieren Sie dessen **IP-Adresse im Produktionsnetzwerk** und dessen **Test-IP-Adresse**.

Nachdem Sie einen Failover durchgeführt (die virtuelle Maschine in der Cloud ausgeführt) und sich an der virtuellen Maschine angemeldet haben, um die IP-Adresse des Servers zu überprüfen, sehen Sie die **IP-Adresse im Produktionsnetzwerk**.

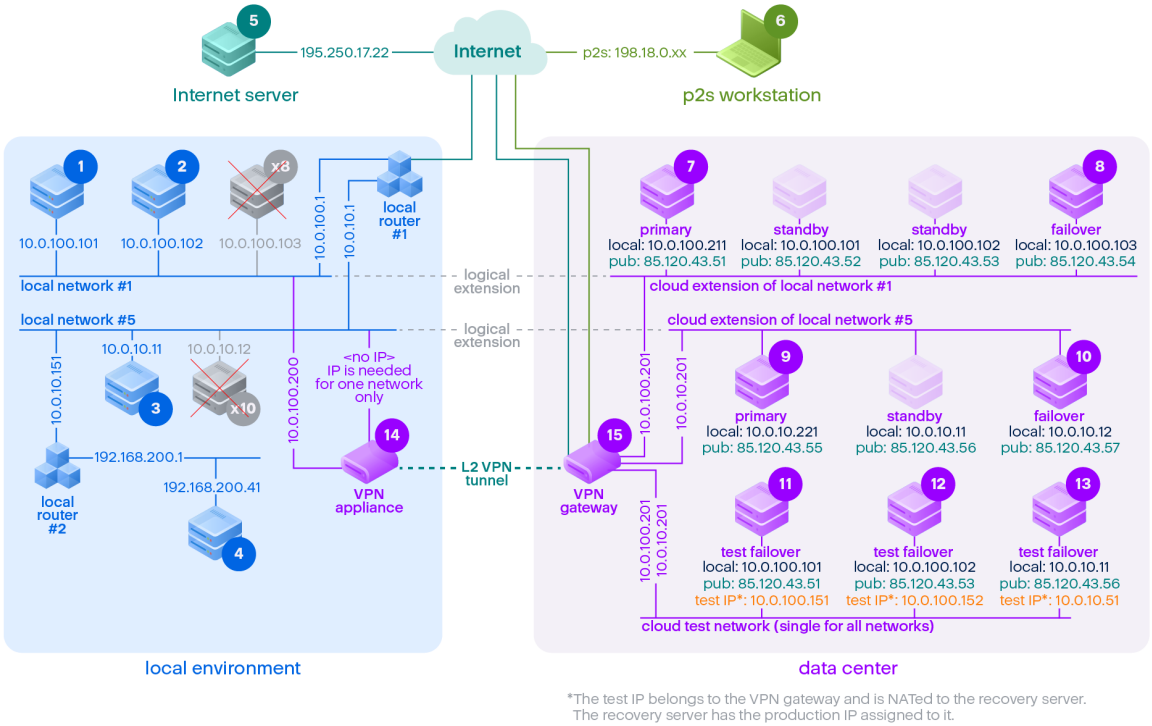
Wenn Sie einen Test-Failover durchführen, können Sie den Test-Server nur über die **Test-IP-Adresse** erreichen, die wiederum nur in der Konfiguration des Recovery-Servers sichtbar ist.

Wenn Sie einen Test-Server von Ihrem lokalen Standort aus erreichen wollen, müssen Sie die **Test-IP-Adresse** verwenden.

Hinweis
Die Netzwerkkonfiguration des Servers zeigt immer die **IP-Adresse im Produktionsnetzwerk** an (weil der Test-Server spiegelt, wie der Produktionsserver aussehen würde). Dies geschieht, weil die Test-IP-Adresse nicht zum Test-Server, sondern zum VPN-Gateway gehört und per NAT in die Produktions-IP-Adresse übersetzt wird.

Das untere Diagramm zeigt ein Beispiel für eine Site-to-Site-OpenVPN-Konfiguration. Einige der Server in der lokalen Umgebung werden per Failover zur Cloud wiederhergestellt (während die Netzwerkinfrastruktur in Ordnung ist).

1. Der Kunde hat das Disaster Recovery durch folgende Maßnahmen aktiviert:
   a. er hat die VPN-Appliance (14) konfiguriert und sie mit dem dedizierten Cloud VPN-Server (15) verbunden
   b. er hat einige der lokalen Server per Disaster Recovery geschützt (1, 2, 3, x8 und x10)
   Einige Server am lokalen Standort (wie 4) sind mit Netzwerken verbunden, die nicht mit der VPN-Appliance verbunden sind. Solche Server sind nicht per Disaster Recovery geschützt.
2. Ein Teil der Server (die mit verschiedenen Netzwerken verbunden sind) arbeitet am lokalen Standort: (1, 2, 3 und 4)
3. Die geschützten Server (1, 2 und 3) werden per Test-Failover (11, 12 und 13) getestet
4. Einige Server am lokalen Standort sind nicht verfügbar (x8, x10). Nach der Durchführung des Failovers werden sie in der Cloud verfügbar (8 und 10)
5. Einige primäre Server (7 und 9), die mit verschiedenen Netzwerken verbunden sind, sind in der Cloud-Umgebung verfügbar
6. (5) ist ein Server im Internet mit einer öffentlichen IP-Adresse
7. (6) ist eine Workstation, die über eine Point-to-Site-Verbindung (P2S) mit der Cloud verbunden ist



In diesem Beispiel sind folgende Verbindungen von einem Server in der Zeile **Von:** zu einem Server in der Spalte **Zu:** möglich.

	Zu:	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
Von:		lokal	lokal	lokal	lokal	Internet	P2S	primär	Failover	primär	Failover	Test-Failover	Test-Failover	Test-Failover	VPN-Appliance	VPN-Server
1	lokal		direkt	über lokalen Router 1	über lokalen Router 2	über lokalen Router 1 und Internet	nein	über Tunnel: lokal über lokalen Router 1 und Internet:	über Tunnel: lokal über lokalen Router 1 und Internet:	über Tunnel: lokal über lokalen Router 1 und Internet:	über Tunnel: lokal über lokalen Router 1 und Internet:	über Tunnel: NAT (VPN-Server) über lokalen Router 1	über Tunnel: NAT (VPN-Server) über lokalen Router 1	über lokalen Router 1 und Tunnel: NAT (VPN-Server) über	direkt	nein

	Zu:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
								pub	pub	pub	pub	und Internet: pub	und Internet: pub	r lokalen Router 1 und Internet: pub		
2	lokal	direkt		über lokalen Router 1	über lokalen Router 2	über lokalen Router 1 und Internet	nein	über Tunnel: lokal über lokalen Router 1 und Internet: pub	über Tunnel: lokal über lokalen Router 1 und Internet: pub	über Tunnel: lokal über lokalen Router 1 und Internet: pub	über Tunnel: lokal über lokalen Router 1 und Internet: pub	über Tunnel: NAT (VPN-Server) über lokalen Router 1 und Internet: pub	über Tunnel: NAT (VPN-Server) über lokalen Router 1 und Internet: pub	über lokalen Router 1 und Tunnel: NAT (VPN-Server) über lokalen Router 1 und Internet: pub	direkt	nein
3	lokal	über lokalen	über lokalen		über lokalen	über lokalen	nein	über Tunnel: loka	über Tunnel: loka	über Tunnel: loka	über Tunnel: loka	über Tunnel: NAT	über Tunnel: NAT	über lokalen Rou	über lokalen Router	nein

	Zu:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
		Router 1	Router 1		Router 2	Router 1 und Internet		l über lokalen Router 1 und Internet: pub	l über lokalen Router 1 und Internet: pub	l über lokalen Router 1 und Internet: pub	l über lokalen Router 1 und Internet: pub	(VPN-Server) über lokalen Router 1 und Internet: pub	(VPN-Server) über lokalen Router 1 und Internet: pub	ter 1 und Tunnel: NAT (VPN-Server) über lokalen Router 1 und Internet: pub		
4	lokal	über lokalen Router 2 und Router 1	über lokalen Router 2 und Router 1	über lokalen Router 2		über lokalen Router 2 und Router 1 und Internet	nein	über lokalen Router 2 und Tunnel: lokal über lokalen Router 2 und loka	über lokalen Router 2 und Tunnel: lokal über lokalen Router 2 und loka	über lokalen Router 2 und Tunnel: lokal über lokalen Router 2 und loka	über lokalen Router 2 und Tunnel: lokal über lokalen Router 2 und loka	über Tunnel: NAT (VPN-Server) über lokalen Router 2 und Router 1 und	über Tunnel: NAT (VPN-Server) über lokalen Router 2 und Router 1 und	über Tunnel: NAT (VPN-Server) über lokalen Router 2 und Router 1 und	über lokalen Router 2	nein

	Zu:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
								len Router 1 und Internet: pub	len Router 1 und Internet: pub	len Router 1 und Internet: pub	len Router 1 und Internet: pub	Internet: pub	Internet: pub	Internet: pub		
5	Internet	nein	nein	nein	nein		n/a	über Internet: pub	über Internet: pub	über Internet: pub	über Internet: pub	über Internet: pub	über Internet: pub	über Internet: pub	nein	nein
6	P2S	nein	nein	nein	nein	über Internet		über P2S-VPN (VPN-Server): lokal über Internet: pub	über P2S-VPN (VPN-Server): lokal über Internet: pub	über P2S-VPN (VPN-Server): lokal über Internet: pub	über P2S-VPN (VPN-Server): lokal über Internet: pub	über P2S-VPN – NAT (VPN-Server) über Internet: pub	über P2S-VPN – NAT (VPN-Server) über Internet: pub	über P2S-VPN – NAT (VPN-Server) über Internet: pub	nein	nein
7	primär	über Tunnel	über Tunnel	über Tunnel und lokalen Route	über Tunnel und lokalen Route	über Internet (über VPN-Server)	nein		direkt in der Cloud: lokal	über Tunnel und lokalen Router 1: lokal	über Tunnel und lokalen Router 1: lokal	über VPN-Server: NAT	über VPN-Server: NAT	über Tunnel und lokalen Router 1: NAT	nein	Nur DHCP- und DNS-Protokolle

	Zu:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
				r 1	r 1 und 2											
8	Failover	über Tunnel	über Tunnel	über Tunnel und lokalen Router 1	über Tunnel und lokalen Router 1 und 2	über Internet (über VPN-Server)	nein	direkt in der Cloud: lokal		über Tunnel und lokalen Router 1: lokal	über Tunnel und lokalen Router 1: lokal	über VPN-Server: NAT	über VPN-Server: NAT	über Tunnel und lokalen Router 1: NAT	nein	Nur DHCP- und DNS-Protokolle
9	primär	über Tunnel und lokalen Router 1	über Tunnel und lokalen Router 1	über Tunnel	über Tunnel	über Internet (über VPN-Server)	nein	über Tunnel und lokalen Router 1: lokal	über Tunnel und lokalen Router 1: lokal		direkt in der Cloud: lokal	über Tunnel und lokalen Router 1: NAT	über Tunnel und lokalen Router 1: NAT	über VPN-Server: NAT	nein	Nur DHCP- und DNS-Protokolle
10	Failover	über Tunnel und lokalen Route	über Tunnel und lokalen Route	über Tunnel	über Tunnel	über Internet (über VPN-Server)	nein	über Tunnel und lokalen Router 1: lokal	über Tunnel und lokalen Router 1: lokal	direkt in der Cloud: lokal		über Tunnel und lokalen Router 1: NAT	über Tunnel und lokalen Router 1: NAT	über VPN-Server: NAT	nein	Nur DHCP- und DNS-Protokolle

	Zu:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
		r 1	r 1													
11	Test-Failover	nein	nein	nein	nein	über Internet (über VPN-Server)	nein	nein	nein	nein	nein		direkt in der Cloud: lokal	über VPN-Server: lokal (Routing)	nein	Nur DHCP- und DNS-Protokolle
12	Test-Failover	nein	nein	nein	nein	über Internet (über VPN-Server)	nein	nein	nein	nein	nein	direkt in der Cloud: lokal		über VPN-Server: lokal (Routing)	nein	Nur DHCP- und DNS-Protokolle
13	Test-Failover	nein	nein	nein	nein	über Internet (über VPN-Server)	nein	nein	nein	nein	nein	über VPN-Server: lokal (Routing)	über VPN-Server: lokal (Routing)		nein	Nur DHCP- und DNS-Protokolle
14	VPN-Appliance	direkt	direkt	über lokalen Router 1	über lokalen Router 2	über Internet (lokaler Route	nein	nein	nein	nein	nein	nein	nein	nein		nein

	Zu:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
						r 1)										
15	VPN-Server	nein	nein	nein	nein	nein	nein	nein	nein	nein	nein	nein	nein	nein	nein	

Lizenzverwaltung für lokale Management Server

Ausführliche Informationen zur Aktivierung eines lokalen Management Servers (On-Premise-Bereitstellung) oder wie Sie diesem Lizenzen zuordnen können, finden Sie im Abschnitt 'Lizenzierung' in der Benutzeranleitung von Cyber Protect.

Definieren, was wie zu schützen ist

Die Registerkarte 'Verwaltung'

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Alle von Ihnen erstellten Pläne sind über die Registerkarte **Verwaltung** in der Cyber Protect-Konsole verfügbar.

Folgende Bereiche sind verfügbar:

- **Schutzpläne**
- **Remote-Verwaltungspläne**
- **Skripting-Pläne**
- **Monitoring-Pläne**
- **Skript-Repository**
- **Cloud-Applikationen-Backup**
- **Backup-Scanning**
- **Backup-Replikation**
- **Validierung**
- **Bereinigung**
- **Konvertierung zu VM**
- **VM-Replikation**

Plan-Statuszustände

Für Schutzpläne und VM-Replikationspläne zeigt eine Statusleiste die folgenden farbcodierten Statuszustände an:

- OK (Grün)
- Warnung (Orange)
- Fehler (Dunkelorange)
- Kritisch (Rot)
- Der Plan wird gerade ausgeführt (Blau)
- Der Plan ist deaktiviert (Grau)

Klicken Sie auf die Statusleiste, um Details zu den Plan-Statuszuständen aller Workloads anzuzeigen, auf die der Plan angewendet wurde.

Klicken Sie auf einen bestimmten Status, um eine Liste aller Workloads mit diesem Status zu sehen.

Schutzpläne

Auf der Registerkarte **Verwaltung** –> **Schutzpläne** können Sie Informationen über Ihre vorhandenen Schutzpläne einsehen, Aktionen mit diesen durchführen und neue Pläne erstellen.

Weitere Informationen über Schutzpläne finden Sie im Abschnitt '"Schutzpläne und Module" (S. 231)'.

Backup-Pläne für Cloud-Applikationen

Auf der Registerkarte **Verwaltung** –> **Cloud-Applikationen-Backup** werden Cloud-zu-Cloud-Backup-Pläne angezeigt. Mit diesen Pläne werden in der Cloud laufende Applikationen von Agenten gesichert, die ebenfalls in der Cloud laufen und den Cloud Storage als Backup-Speicherort verwenden.

Sie können in diesem Bereich folgende Aktionen durchführen:

- Einen Backup-Plan erstellen, anzeigen, ausführen, stoppen, bearbeiten und löschen
- Aktivitäten anzeigen, die mit einem betreffenden Backup-Plan verbunden sind
- Alarmmeldungen einsehen, die mit einem betreffenden Backup-Plan verbunden sind

Weitere Informationen über Cloud-Applikationen-Backups finden Sie unter:

- Microsoft 365-Daten sichern
- Google Workspace-Daten sichern

Cloud-zu-Cloud-Backups manuell ausführen

Um Störungen des Cyber Protection Service zu vermeiden, ist die Anzahl der manuellen Cloud-zu-Cloud-Backup-Ausführungen auf 10 Starts pro Microsoft 365- oder Google Workspace-Organisation und Stunde begrenzt. Wenn dieser Wert erreicht ist, wird die Anzahl der zulässigen Ausführungen auf eine (1) pro Stunde zurückgesetzt und danach jede Stunde eine zusätzliche Ausführung verfügbar (z.B. Stunde 1, 10 Ausführungen; Stunde 2, 1 Ausführung; Stunde 3, 2 Ausführungen), bis insgesamt 10 Ausführungen pro Stunde erreicht sind.

Backup-Pläne, die auf Gerätegruppen (Postfächer, Laufwerke, Standorte) angewendet werden oder mehr als 10 Geräte umfassen, können nicht manuell ausgeführt werden.

Backup-Scanning-Pläne

Um Backups nach Malware (Ransomware eingeschlossen) durchsuchen zu lassen, erstellen Sie einen Backup-Scanning-Plan.

Wichtig
Backup-Scanning-Pläne werden nicht für alle Workloads und Backup Storages unterstützt. Weitere Informationen finden Sie hier: "Beschränkungen" (S. 947).

So können Sie einen Backup-Scanning-Plan erstellen

1. Gehen Sie in der Cyber Protect-Konsole zum Bereich **Verwaltung** –> **Backup-Scanning**.
2. Klicken Sie auf **Plan erstellen**.
3. Spezifizieren Sie den Namen des Plans und folgende Parameter:
   - **Scan-Typ**:
     - **Cloud** – diese Option kann nicht geändert werden. Ein automatisch ausgewählter Cloud Agent wird den Backup-Scan durchführen.
   - **Zu scannende Backups**:
     - **Speicherorte** – wählen Sie Speicherorte mit den Backup-Sets aus, die gescannt werden sollen.
     - **Backups** – wählen Sie Backup-Sets aus, die gescannt werden sollen.
   - **Scannen nach**:
     - **Malware** – diese Option kann nicht geändert werden. Der Scan überprüft die ausgewählten Backup-Sets auf Malware (einschließlich Ransomware).
   - **Verschlüsselung** – um verschlüsselte Backup-Sets scannen zu können, müssen Sie das Verschlüsselungskennwort spezifizieren. Wenn Sie einen Speicherort oder mehrere Backup-Sets auswählen und das spezifizierte Kennwort bei einem Backup-Set nicht passt, wird eine Alarmmeldung erzeugt.
   - **Planung** – diese Option kann nicht geändert werden. Im Cloud Storage wird der Scan automatisch gestartet.
4. Klicken Sie auf **Erstellen**.

Als Ergebnis wird ein Backup-Scanplan erstellt und ein Cloud Agent wird die von Ihnen spezifizierten Speicherorte oder Backup-Sets auf Malware untersuchen.

Off-Host Data Processing

Hinweis
Diese Funktion ist für Kunden-Mandanten verfügbar, für die die Quota **Advanced Backup - Server** oder **Advanced Backup - NAS** als Teil des Advanced Backup-Pakets aktiviert wurde.

Replikation, Validierung und Bereinigung werden normalerweise vom Protection Agenten durchgeführt, der das Backup ausführt. Dies belastet die Maschine, auf der der Agent läuft, zusätzlich, auch nach Abschluss des Backup-Prozesses. Um die Maschine zu entlasten, können Sie Off-Host-Datenschutzpläne erstellen - das heißt, separate Pläne für Replikation, Validierung, Bereinigung und Konvertierung in eine virtuelle Maschine.

Mit den Off-Host-Data-Protection-Pläne können Sie Folgendes tun:

- Verschiedene Agenten für Backup- und Off-Host-Data-Protection-Aktionen wählen
- Off-Host-Datenverarbeitungsaktionen der üblichen Stoßzeiten planen, um den Netzwerkbandbreitenverbrauch zu minimieren
- Off-Host-Datenverarbeitungsaktionen außerhalb der üblichen Geschäftszeiten planen, wenn Sie keinen dedizierten Agenten für die entsprechende Off-Host-Daten-Verarbeitung installieren wollen

Hinweis
Die Off-Host-Datenverarbeitungspläne laufen gemäß den Zeiteinstellungen (einschließlich der Zeitzone) der Maschine, auf der der Protection Agent installiert ist. Bei einer virtuellen Appliance (z.B. dem Agenten für VMware oder dem Agenten für Scale Computing HC3) können Sie die Zeitzone in der grafischen Benutzeroberfläche des Agenten konfigurieren.

Backup-Replikation

Hinweis
Diese Funktion ist für Kunden-Mandanten verfügbar, für die die Quota **Advanced Backup - Server** oder **Advanced Backup - NAS** als Teil des Advanced Backup-Pakets aktiviert wurde.

Mit einer Backup-Replikation kann ein Backup zu einem anderen Speicherort kopiert werden. Sie wird als Off-Host Data Processing-Aktionen in einem Backup-Replikationsplan konfiguriert.

Die Backup-Replikation kann auch Bestandteil eines Schutzplans sein. Weitere Informationen über diese Option finden Sie im Abschnitt '"Replikation" (S. 482)'.

Einen Backup-Replikationsplan erstellen

Wenn Sie Backups über eine Off-Host Data Processing-Operation replizieren wollen, müssen Sie einen Backup-Replikationsplan erstellen.

So können Sie einen Backup-Replikationsplan erstellen

1. Klicken Sie in der Cyber Protect-Konsole auf **Verwaltung** –> **Backup-Replikation**.
2. Klicken Sie auf **Plan erstellen**.
3. Wählen Sie bei **Agent** denjenigen Agenten aus, der die Replikation durchführen soll.
   Sie können jeden Agenten auswählen, der sowohl auf den Quell- als auch auf den Replikations-Speicherort zugreifen kann.
4. Wählen Sie bei **Zu replizierende Elemente** die Archive oder Backup-Speicherorte aus, die repliziert werden sollen.
   Wenn Sie zwischen Archiven und Speicherorten wechseln wollen, müssen Sie den Umschalter **Speicherorte** / **Backups** in der rechten oberen Ecke verwenden.
   Wenn Sie mehrere verschlüsselte Archive auswählen, müssen diese alle dasselbe Verschlüsselungskennwort haben. Für Archive, die unterschiedliche Verschlüsselungskennwörter verwenden, müssen Sie separate Backup-Pläne erstellen.

5. Spezifizieren Sie bei **Ziel** den Speicherort für die Replikationsdaten.
6. Bestimmen Sie bei **Art der Replikation**, welche Backups (die auch als Recovery-Punkte bezeichnet werden) repliziert werden sollen.

   Folgende Optionen sind verfügbar:

   - **Alle Backups**
   - **Nur Voll-Backups**
   - **Nur jeweils das letzte Backup**

   Weitere Informationen über diese Optionen finden Sie im Abschnitt '"Replikations-Quelle" (S. 216)'.
7. Konfigurieren Sie bei **Planung** den entsprechenden Replikationsplan.

   Wenn Sie die Planung des Backup-Replikationsplans konfigurieren, müssen Sie sicherstellen, dass das zuletzt replizierte Backup noch an seinem ursprünglichen Speicherort verfügbar ist, wenn die Backup-Replikation gestartet wird. Wenn dieses Backup nicht mehr am ursprünglichen Speicherort verfügbar ist (weil es beispielsweise durch eine Aufbewahrungsregel gelöscht wurde), wird das komplette Archiv in Form eines vollständigen Backups repliziert. Dies kann sehr zeitaufwendig sein und wird zusätzlichen Speicherplatz beanspruchen.
8. Spezifizieren Sie bei **Bereinigungsregeln** die Bereinigungsregeln für den Zielspeicherort.

   Folgende Optionen sind verfügbar:

   - **Nach Backup-Anzahl**
   - **Nach Backup-Alter** (separate Einstellungen für monatliche, wöchentliche, tägliche und stündliche Backups)
   - **Nach der Gesamtgröße der Backups**
   - **Backups unbegrenzt aufbewahren**

     Hinweis
     Wenn Sie diese Option auswählen, führt dies zu einer erhöhten Storage-Nutzung. Sie müssen die nicht mehr benötigten Backups manuell löschen.
9. [Wenn Sie unter **Zu replizierende Elemente** verschlüsselte Archive ausgewählt haben] Aktivieren Sie den Schalter **Backup-Kennwort** und geben Sie das entsprechende Verschlüsselungskenntwort ein.
10. [Optional] Klicken Sie zum Ändern der Plan-Optionen auf das Zahnrad-Symbol und konfigurieren Sie dann die gewünschten Optionen je nach Bedarf.
11. Klicken Sie auf **Erstellen**.

Replikations-Quelle

Hinweis
Einige Replikationsaktionen (wie die Replikation eines kompletten Speicherortes oder die Replikation aller Backups in einem Backup-Satz) können sehr zeitaufwendig sein.

Sie können einzelne Backup-Sätze oder komplette Backup-Speicherorte replizieren. Wenn Sie einen Backup-Speicherort replizieren, werden alle dort befindlichen Backup-Sätze repliziert.

Backup-Sätze bestehen aus Backups (die auch als Recovery-Punkte bezeichnet werden). Sie müssen auswählen, welche Backups repliziert werden sollen.

Folgende Optionen sind verfügbar:

- **Alle Backups**
  Alle Backups im Backup-Satz werden jedes Mal repliziert, wenn der Replikationsplan ausgeführt wird.
- **Nur Voll-Backups**
  Es werden nur die vollständigen Backups (Voll-Backups) des Backup-Satzes repliziert.
- **Nur jeweils das letzte Backup**
  Es wird nur das neueste Backup im Backup-Satz repliziert, unabhängig von dessen Typ (vollständig, differentiell oder inkrementell).

Wählen Sie eine Option, die Ihren Anforderungen und dem von Ihnen verwendeten Backup-Schema entspricht. Wenn Sie beispielsweise das Backup-Schema **Nur inkrementell (Einzeldatei)** verwenden und nur das neueste inkrementelle Backup replizieren wollen, müssen Sie im Backup-Replikationsplan die Option **Nur das letzte Backup** auswählen.

Die folgende Tabelle fasst zusammen, welche Backups mit verschiedenen Backup-Schemata repliziert werden.

	Nur inkrementell (Einzeldatei)	**Nur vollständig**	**Wöchentlich vollständig, täglich inkrementell**	**Monatlich vollständig, wöchentlich differentiell, täglich inkrementell (GFS)**
Alle Backups	Alle Backups im Backup-Satz	Alle Backups im Backup-Satz	Alle Backups im Backup-Satz	Alle Backups im Backup-Satz
Nur Voll-Backups	Nur das erste Backup, das vollständig ist	Alle Backups	Ein Backup pro Woche*	Ein Backup pro Monat*
Nur das letzte Backup	Nur das neueste Backup im Backup-Satz*	Nur das neueste Backup im Backup-Satz*	Nur das neueste Backup, unabhängig von dessen Typ*	Nur das neueste Backup, unabhängig von dessen Typ*

*Wenn Sie die Planung des Backup-Replikationsplans konfigurieren, müssen Sie sicherstellen, dass das zuletzt replizierte Backup noch an seinem ursprünglichen Speicherort verfügbar ist, wenn die Backup-Replikation gestartet wird. Wenn dieses Backup nicht mehr am ursprünglichen Speicherort verfügbar ist (weil es beispielsweise durch eine Aufbewahrungsregel gelöscht wurde), wird das

komplette Archiv in Form eines vollständigen Backups repliziert. Dies kann sehr zeitaufwendig sein und wird zusätzlichen Speicherplatz beanspruchen.

Unterstützte Speicherorte

Die folgende Tabelle fasst Backup-Speicherorte zusammen, die von Backup-Replikationsplänen unterstützt werden.

Backup-Speicherort	Als Quelle unterstützt	Als Ziel unterstützt
Cloud Storage	+	+
Lokaler Ordner	+	+
Netzwerkordner	+	+
Public Cloud	+	+
NFS-Ordner	–	–
Secure Zone	–	–

Validierung

Hinweis
Diese Funktion ist für Kunden-Mandanten verfügbar, für die die Quota **Advanced Backup - Server** oder **Advanced Backup - NAS** als Teil des Advanced Backup-Pakets aktiviert wurde.

Indem Sie ein Backup validieren, können Sie sicherstellen, dass Sie die Daten aus diesem Backup wiederherstellen können.

Wenn Sie eine Backup-Validierung über eine Off-Host Data Processing-Operation auf ein anderes System auslagern wollen, müssen Sie einen Validierungsplan erstellen. Wie Sie einen solchen erstellen können, finden Sie im Abschnitt '"Einen Validierungsplan erstellen" (S. 220)' erläutert.

Die folgenden Validierungsmethoden sind verfügbar:

- Prüfsummen-Verifizierung
- Als virtuelle Maschine ausführen
  - VM-Takt (Heartbeat)
  - Screenshot-Validierung

Sie können eine oder mehrere dieser Methoden auswählen. Wenn mehrere Methoden ausgewählt sind, werden die Aktionen für jede Validierungsmethode nacheinander ausgeführt. Weitere Informationen über die Methoden finden Sie im Abschnitt '"VM-Takt (Heartbeat)" (S. 223)'.

Sie können Backup-Sets oder Backup-Speicherorte validieren. Wenn Sie einen Backup-Speicherort validieren, werden alle Backup-Sets in diesem Speicherort validiert.

Unterstützte Speicherorte

Die nachfolgende Tabelle listet die unterstützten Backup-Speicherorte und Validierungsmethoden auf.

Hinweis
Die Validierungsoption ist nicht für Public Cloud-Backups verfügbar, da die Kosten für das Lesen eines kompletten Archivs aus einer Public Cloud zu hoch wären.

Backup-Speicherort	Prüfsummen-Verifizierung	Als virtuelle Maschine ausführen	
		VM-Takt (Heartbeat)	Screenshot-Validierung
Cloud Storage	+	+	+
Lokaler Ordner	+	+	+
Netzwerkordner	+	+	+
NFS-Ordner	–	–	–
Secure Zone	–	–	–

Validierungsstatus

Nach erfolgreicher Validierung wird das Backup mit einem grünen Punkt und der Bezeichnung **Validiert** markiert.

Sollte die Validierung fehlschlagen, wird das Backup mit einem roten Punkt markiert. Eine Überprüfung wird dann als fehlgeschlagen eingestuft, wenn auch nur eine der verwendeten Validierungsmethoden nicht funktioniert. In einigen Fällen kann dies auf eine falsche Konfiguration des Validierungsplans zurückzuführen sein – wie etwa, wenn Sie die Methode **VM-Takt (Heartbeat)** für virtuelle Maschinen auf einem falschen Host verwenden.

Der Validierungsstatus eines Backups wird nach jedem neuen Validierungsvorgang aktualisiert. Der Status für jede Validierungsmethode wird separat aktualisiert. Aus diesem Grund wird die Validierung eines Backups, bei dem eine Methode fehlschlug, so lange als fehlgeschlagen angezeigt, bis dieselbe Validierungsmethode erfolgreich abgeschlossen wurde, auch wenn die letzten Validierungsaktionen die fehlgeschlagene Methode nicht verwenden und erfolgreich abgeschlossen wurden.

Weitere Informationen zur Überprüfung des Validierungsstatus finden Sie im Abschnitt '"Den Validierungsstatus eines Backups überprüfen" (S. 225)'.

Einen Validierungsplan erstellen

Wenn Sie die Validierung eines Backup-Satzes über eine Off-Host Data Processing-Operation auf ein anderes System auslagern wollen, müssen Sie einen Validierungsplan erstellen.

So können Sie einen Validierungsplan erstellen

1. Klicken Sie in der Cyber Protect-Konsole auf **Verwaltung** –> **Validierung**.
2. Klicken Sie auf **Plan erstellen**.
   Die Vorlage für einen neuen Validierungsplan wird geöffnet.
3. [Optional] Wenn Sie den Namen des Plans ändern wollen, klicken Sie auf den vorgegebenen Standardnamen.
4. Wählen Sie im Bereich **Agent** denjenigen Agenten aus, der die Validierung durchführen soll, und klicken Sie abschließend auf **OK**.
   Wenn Sie eine Validierung durchführen wollen, indem Sie eine virtuelle Maschine aus einem Backup ausführen, müssen Sie eine Maschine mit dem Agenten für VMware oder dem Agenten für Hyper-V auswählen. Ansonsten können Sie jede Maschine auswählen, die auf den Backup-Speicherort zugreifen kann.
5. Wählen Sie bei **Zu validierende Elemente** die Backup-Sets aus, die validiert werden sollen.
   a. Bestimmen Sie den Umfang des Plans (ob einzelne Backup-Sets oder ganze Standorte validiert werden sollen), indem Sie in der rechten oberen Ecke auf **Speicherorte** oder **Backups** klicken.
      Wenn die ausgewählten Backups verschlüsselt sind, müssen diese alle dasselbe Verschlüsselungskennwort verwenden. Erstellen Sie für Backups, die unterschiedliche Verschlüsselungskennwörter verwenden, separate Backup-Pläne.
   b. Klicken Sie auf **Hinzufügen**.
   c. Wählen Sie je nach Umfang des Validierungsplans die Standorte oder einen Standort und Backup-Sets aus und klicken Sie dann auf **Fertig**.
   d. Klicken Sie auf **Fertig**.
6. Wählen Sie bei **Validierungsquelle**, welche Backups (auch Recovery-Punkte genannt) innerhalb der ausgewählten Backup-Sets validiert werden sollen. Folgende Optionen sind verfügbar:
   - **Alle Backups**
   - **Nur jeweils das letzte Backup**
7. Wählen Sie bei **Art der Validierung** die gewünschte Validierungsmethode aus.
   Sie können eine oder beide der folgenden Optionen wählen:
   - **Prüfsummen-Verifizierung**
   - **Als virtuelle Maschine ausführen**

   Weitere Informationen über die Methoden finden Sie im Abschnitt '"VM-Takt (Heartbeat)" (S. 223)'.
8. [Wenn Sie **Prüfsummen-Verifizierung** ausgewählt haben] Klicken Sie auf **Fertig**.

9. [Wenn Sie **Als virtuelle Maschine ausführen** ausgewählt haben]. Konfigurieren Sie die Einstellungen für diese Methode.
   a. Wählen Sie bei **Zielmaschine** den Typ der virtuellen Maschine (ESXi oder Hyper-V), den Host sowie die Vorlage für den Maschinennamen aus und klicken Sie anschließend auf **OK**.
      Der Standardname ist **[Maschinenname]_validieren**.
   b. Wählen Sie bei **Datenspeicher** (für ESXi) oder **Pfad** (für Hyper-V) den Datenspeicher für die virtuelle Maschine aus.
   c. Wählen Sie eine oder beide der Überprüfungsmethoden, die die Möglichkeit **Als virtuelle Maschine ausführen** bereitstellt:
      - **VM-Takt (Heartbeat)**
      - **Screenshot-Validierung**
   d. [Optional] Klicken Sie auf **VM-Einstellungen**, um die Größe des Arbeitsspeichers und die Netzwerkverbindungen der virtuellen Maschine zu ändern.
      Die virtuelle Maschine ist standardmäßig nicht mit einem Netzwerk verbunden und die Größe ihres Arbeitsspeichers entspricht der der ursprünglichen Maschine.
   e. Klicken Sie auf **Fertig**.
10. [Optional] Klicken Sie in der Vorlage für den Validierungsplan auf **Planung** und konfigurieren Sie diese.
11. [Wenn die Backup-Sets, die bei **Zu validierende Elemente** ausgewählt wurden, verschlüsselt sind] Aktivieren Sie den Schalter **Backup-Kennwort** und geben Sie dann das entsprechende Verschlüsselungskennwort an.
12. [Optional] Wenn Sie die Plan-Optionen ändern wollen, klicken Sie auf das Zahnradsymbol.
13. Klicken Sie auf **Erstellen**.

Als Ergebnis ist Ihr Validierungsplan bereit und wird gemäß der von Ihnen konfigurierten Planung ausgeführt. Wenn Sie den Plan sofort ausführen wollen, müssen Sie ihn unter **Verwaltung** –> **Validierung** auswählen und anschließend auf **Jetzt ausführen** klicken.

Nachdem der Plan gestartet wurde, können Sie in der Cyber Protect-Konsole unter **Monitoring** –> **Aktivitäten** die laufenden Aktivitäten überprüfen und deren Details nachschlagen.

Ein Validierungsplan kann mehrere Backups umfassen und umgekehrt kann ein einzelnes Backup von mehreren Validierungsplänen validiert werden.

Hinweis
Alle Backups werden sequentiell, eins nach dem anderen, von einem einzigen Validierungstask verarbeitet.

Auf einem bestimmten Agenten kann jeweils nur ein Validierungstask ausgeführt werden. Mehrere Validierungstasks können parallel laufen, wenn sie von verschiedenen Agenten ausgeführt werden: zwei gleichzeitige Tasks erfordern zwei Agenten, drei Tasks drei Agenten usw.

Die nachfolgende Tabelle gibt einen Überblick über die möglichen Statuszustände der Validierungsaktivität.

Aktivitätsergebnis	Plan mit einem Backup	Plan mit mehreren Backups
Erfolgreich	Alle Validierungsmethoden waren erfolgreich	Alle Validierungsmethoden waren bei allen Backups erfolgreich
Mit Warnungen abgeschlossen	Nicht verfügbar	Bei mindestens einem Backup ist mindestens eine Validierungsmethode fehlgeschlagen
Fehlgeschlagen	Mindestens eine Validierungsmethode ist fehlgeschlagen	Mindestens eine Validierungsmethode ist bei allen Backups fehlgeschlagen

Validierungsmethoden

In einem Validierungsplan sind folgende Validierungsmethoden verfügbar:

- Prüfsummen-Verifizierung
- Als virtuelle Maschine ausführen
  - VM-Takt (Heartbeat)
  - Screenshot-Validierung

Prüfsummen-Verifizierung

Bei einer Validierung mittels Prüfsummen-Verifizierung wird für jeden Datenblock, der aus dem Backup wiederhergestellt werden kann, eine Prüfsumme berechnet und diese anschließend mit der ursprünglichen Prüfsumme für diesen Datenblock verglichen, der während des Backup-Prozesses geschrieben wurde. Es gibt nur eine Ausnahmen, nämlich die Validierung von Datei-Backups, die im Cloud Storage gespeichert sind. Diese Backups werden validiert, indem die Konsistenz der im Backup gespeicherten Metadaten überprüft wird.

Eine Validierung mittels Prüfsummen-Verifizierung ist ein zeitaufwendiger Prozess (auch bei inkrementellen oder differentiellen Backups, die normalerweise kleiner sind). Der Grund dafür ist, dass bei dem Validierungsvorgang nicht nur die Daten geprüft werden, die physisch im jeweiligen Backup enthalten sind, sondern alle Daten, die wiederhergestellt werden müssen. Es kann also sein, dass auch noch weitere, frühere Backups validiert werden müssen.

Eine erfolgreiche Validierung mittels Prüfsummen-Verifizierung bedeutet, dass eine spätere Datenwiederherstellung mit hoher Wahrscheinlichkeit möglich ist. Bei der Validierung mit dieser Methode werden jedoch nicht alle Faktoren geprüft, die den Prozess der Wiederherstellung beeinflussen können.

Wenn Sie ein Betriebssystem sichern, empfehlen wir Ihnen daher, einige der nachfolgenden zusätzlichen Operationen zu verwenden:

- Eine Testwiederherstellung mit einem Boot-Medium auf einem freien, ungenutzen Festplattenlaufwerk.
- Eine virtuelle Maschine aus einem Backup heraus ausführen (in einer ESXi- oder Hyper-V-Umgebung).

- Einen Validierungsplan ausführen, in dem die Validierungsmethode **Als virtuelle Maschine ausführen** aktiviert ist.

Als virtuelle Maschine ausführen

Diese Methode funktioniert nur für Laufwerk-Backups, die ein Betriebssystem enthalten. Wenn Sie diese Methode verwenden wollen, benötigen Sie einen ESXi- oder Hyper-V-Host und einen Protection Agenten (einen Agenten für VMware oder für Hyper-V), der diesen Host verwaltet.

Die Validierungsmethode **Als virtuelle Maschine ausführen** ist in folgenden Varianten verfügbar:

- VM-Takt (Heartbeat)
- Screenshot-Validierung

Sie müssen mindestens eine davon auswählen.

VM-Takt (Heartbeat)

Bei dieser Validierungsmethode führt der Agent eine virtuelle Maschine direkt aus dem jeweiligen Backup aus, stellt eine Verbindung zu den VMware Tools oder Hyper-V-Integrationsdiensten her und überprüft dann die Heartbeat-Antwort, um sicherzustellen, dass das Betriebssystem erfolgreich gestartet wurde. Wenn die Verbindung fehlschlägt, versucht der Agent, alle zwei Minuten (und maximal fünfmal) eine Verbindung herzustellen. Falls keine der Verbindungsversuche erfolgreich ist, schlägt die Validierung fehl.

Unabhängig von der Anzahl der Validierungspläne und der validierten Backups: der Agent, der die Validierung durchführt, führt immer nur jeweils eine virtuelle Maschine aus. Sobald das Ergebnis der Validierung feststeht, löscht der Agent die betreffende virtuelle Maschine wieder und führt anschließend die nächste aus.

Hinweis
Verwenden Sie diese Methode nur, wenn Sie Backups von virtuellen VMware-Maschinen validieren, indem Sie diese Backups als virtuelle Maschinen auf einem ESXi-Host ausführen – oder Backups von virtuellen Hyper-V-Maschinen, indem Sie diese als virtuelle Maschinen auf einem Hyper-V Host ausführen.

Screenshot-Validierung

Bei dieser Validierungsmethode führt der Agent eine virtuelle Maschine aus dem jeweiligen Backup aus. Und während die virtuelle Maschine hochgefahren wird, werden Screenshots des Boot-Ablaufs erstellt. Ein mit maschineller Intelligenz (MI) arbeitendes Modul überprüft dann die Screenshots. Wenn darauf ein Anmeldebildschirm zu erkennen ist, wird das Backup als validiert gekennzeichnet.

Der Screenshot wird an den Recovery-Punkt angehängt und Sie können ihn für ein Jahr lang (nach der Validierung) über die Cyber Protect-Konsole herunterladen. Weitere Informationen zur Überprüfung des Screenshots finden Sie im Abschnitt '"Den Validierungsstatus eines Backups überprüfen" (S. 225)'.

Wenn die Benachrichtigungen für Ihr Benutzerkonto aktiviert sind, werden Sie eine E-Mail über den Validierungsstatus des Backups erhalten, an das der Screenshot angehängt wurde. Weitere Informationen zu Benachrichtigungen finden Sie im Abschnitt Die Benachrichtigungseinstellungen für einen Benutzer ändern.

Die Screenshot-Validierung wird von der Agent-Version 15.0.30971 (im November 2022 veröffentlicht) und höher unterstützt.

Hinweis
Die Screenshot-Validierung funktioniert am besten bei Backups von Windows- und Linux-Systemen, die einen Anmeldebildschirm mit grafischer Benutzeroberfläche bieten. Diese Methode ist nicht für Linux-Systeme optimiert, die einen Konsolen-basierten Anmeldebildschirm haben.

Das Zeitlimit für den VM-Takt (Heartbeat) und die Screenshot-Validierung ändern

Wenn Sie ein Backup validieren, indem Sie es als virtuelle Maschine ausführen, können Sie das Zeitlimit zwischen dem Booten der virtuellen Maschine und dem Senden der Heartbeat-Anfrage oder der Aufnahme eines Screenshots konfigurieren.

Der Standardzeitraum ist folgendermaßen festgelegt:

- Eine Minute – für Backups, die in einem lokalen Ordner oder auf einer Netzwerkfreigabe gespeichert sind
- Fünf Minuten – für Backups, die in der Cloud gespeichert sind

Sie können diese Einstellung ändern, indem Sie die Konfigurationsdatei für den Agenten für VMware oder den Agenten für Hyper-V bearbeiten.

So können Sie das Zeitlimit ändern

1. Öffnen Sie die Konfigurationsdatei, um diese zu bearbeiten. Sie können die Datei an folgenden Speicherorten finden:
   - Für den Agenten für VMware oder den Agenten für Hyper-V, der unter Windows läuft: `C:\Program Files\BackupClient\BackupAndRecovery\settings.config`
   - Für den Agenten für VMware (Virtuelle Appliance): `/bin/mms_settings.config`
     Weitere Informationen darüber, wie Sie auf die Konfigurationsdatei auf einer virtuellen Appliance zugreifen können, finden Sie im Abschnitt '"SSH-Verbindungen zu einer virtuellen Appliance" (S. 187)'.
2. Gehen Sie zu `<validation>` und ändern Sie dann die Werte für lokale Backups und Cloud-Backups nach Ihren Anforderungen:

```
<validation>
<run_vm>
<initial_timeout_minutes>
<local_backups>1</local_backups>
<cloud_backups>5</cloud_backups>
</initial_timeout_minutes>
```

```
</run_vm>
</validation>
```

3. Speichern Sie die Konfigurationsdatei.
4. Starten Sie den Agenten neu.
   - [Für den Agenten für VMware oder den Agenten für Hyper-V, die unter Windows laufen] Führen Sie folgende Befehle über die Eingabeaufforderung aus:

     ```
     net stop mms
     ```

     ```
     net start mms
     ```

   - [Für den Agenten für VMware (Virtuelle Appliance)] Starten Sie die virtuelle Maschine mit dem Agenten neu.

Die Anzahl der Wiederholungsversuche im Falle eines Fehlers konfigurieren

Wenn Sie die Anzahl der erfolgreichen Validierungen maximieren wollen, können Sie für Validierungsaktionen, die mit einem Fehler enden, automatische Wiederholungsversuche konfigurieren.

So können Sie automatische Wiederholungsversuche konfigurieren

1. Klicken Sie beim Erstellen eines Validierungsplans auf das Zahnradsymbol.
2. Wählen Sie im Fensterbereich **Optionen** die Option **Fehlerbehandlung**.
3. Klicken Sie unter **Erneut versuchen, wenn ein Fehler auftritt** auf **Ja**.
4. Konfigurieren Sie bei **Anzahl der Versuche** die maximale Anzahl der Wiederholungen, wenn ein Fehler auftritt.

   Die Validierungsaktion wird so lange wiederholt, bis sie erfolgreich abgeschlossen wurde oder bis die maximale Anzahl von Wiederholungen erreicht wurde.
5. Konfigurieren Sie bei **Intervall zwischen den Versuchen** die Zeitspanne zwischen zwei aufeinanderfolgenden Wiederholungsversuchen.
6. Klicken Sie auf **Fertig**.

Den Validierungsstatus eines Backups überprüfen

Sie können den Validierungsstatus eines Backups auf der Registerkarte **Geräte** oder auf der Registerkarte **Backup Storage** überprüfen.

Sie können außerdem den Status für jede Validierungsmethode einsehen und den Screenshot herunterladen, der bei der Screenshot-Validierungsmethode aufgenommen wurde.

Weitere Informationen darüber, wie Statuszustände funktionieren, finden Sie im Abschnitt '"Validierungsstatus" (S. 219)'.

So können Sie den Validierungsstatus eines Backups überprüfen

Geräte

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte** –> **Alle Geräte**.
2. Wählen Sie den Workload, dessen Backup-Validierungsstatus Sie überprüfen wollen, und klicken Sie anschließend auf **Recovery**.
3. [Wenn mehr als ein Backup-Speicherort verfügbar ist] Wählen Sie den Backup-Speicherort aus.
4. Wählen Sie das Backup, dessen Status Sie überprüfen wollen.

Backup Storage

1. Gehen Sie in der Cyber Protect-Konsole zu **Backup Storage**.
2. Wählen Sie den Ort, an dem Ihr Backup-Set gespeichert ist.
3. Wählen Sie das gewünschte Backup-Set aus und klicken Sie auf **Backups anzeigen**.
4. Wählen Sie das Backup, dessen Validierungsstatus Sie überprüfen wollen.

Bereinigung

Eine Bereinigung ist eine Aktion, die veraltete Backups gemäß von spezifizierten Aufbewahrungsregeln löscht. Diese Aktion gilt nur für Agenten und Workloads, aber nicht für Cloud-zu-Cloud-Backups (die nur manuell gelöscht werden können).

Hinweis
Diese Funktion ist für Kunden-Mandanten verfügbar, für die die Quota **Advanced Backup - Server** oder **Advanced Backup - NAS** als Teil des Advanced Backup-Pakets aktiviert wurde.

Unterstützte Speicherorte

Bereinigungspläne unterstützten alle Backup-Speicherorte – ausgenommen NFS-Ordner und die Secure Zone.

So können Sie einen Bereinigungsplan erstellen

1. Klicken Sie in der Cyber Protect-Konsole auf **Verwaltung** –> **Bereinigung**.
2. Klicken Sie auf **Plan erstellen**.
3. Wählen Sie bei **Agent** denjenigen Agenten aus, der die Bereinigung durchführen soll.
   Sie können jeden Agenten auswählen, der auf den Backup-Speicherort zugreifen kann.
4. Wählen Sie bei **Zu bereinigende Elemente** die Archive oder Backup-Speicherorte aus, die bereinigt werden sollen.
   Wenn Sie zwischen Archiven und Speicherorten wechseln wollen, müssen Sie den Umschalter **Speicherorte** / **Backups** in der rechten oberen Ecke verwenden.
   Wenn Sie mehrere verschlüsselte Archive auswählen, müssen diese alle dasselbe Verschlüsselungskennwort haben. Für Archive, die unterschiedliche Verschlüsselungskennwörter verwenden, müssen Sie separate Backup-Pläne erstellen.
5. Konfigurieren Sie bei **Planung** den entsprechenden Bereinigungsplan.

6. Spezifizieren Sie bei **Bereinigungsregeln** die entsprechenden Bereinigungsregeln.
   Folgende Optionen sind verfügbar:
   - **Nach Backup-Anzahl**
   - **Nach Backup-Alter** (separate Einstellungen für monatliche, wöchentliche, tägliche und stündliche Backups)
   - **Nach der Gesamtgröße der Backups**
7. [Wenn Sie unter **Zu replizierende Elemente** verschlüsselte Archive ausgewählt haben] Aktivieren Sie den Schalter **Backup-Kennwort** und geben Sie das entsprechende Verschlüsselungskenntwort ein.
8. [Optional] Klicken Sie zum Ändern der Plan-Optionen auf das Zahnrad-Symbol und konfigurieren Sie dann die gewünschten Optionen je nach Bedarf.
9. Klicken Sie auf **Erstellen**.

Konvertierung zu einer virtuellen Maschine

Nur Laufwerk-Backups können zu einer virtuellen Maschine konvertiert werden. Wenn ein Backup das System-Volume und alle Informationen enthält, die für den Start des entsprechenden Betriebssystems erforderlich sind, kann auch die resultierende virtuelle Maschine selbstständig starten. Ansonsten können Sie die entsprechenden virtuellen Laufwerke zu einer anderen virtuellen Maschine hinzufügen.

Hinweis
VMs, die über die native VM-Replikationsfunktion von Scale Computing repliziert werden, können nicht per Backup gesichert werden.

Sie können einen separaten Plan für die Konvertierung zu einer virtuellen Maschine erstellen und diesen Plan manuell oder zeitgesteuert ausführen.

Informationen zu Voraussetzungen und Einschränkungen finden Sie im Abschnitt '"Was Sie über Konvertierungen wissen müssen" (S. 229)'.

Hinweis
Diese Funktion ist für Kunden-Mandanten verfügbar, für die die Quota **Advanced Backup - Server** oder **Advanced Backup - NAS** als Teil des Advanced Backup-Pakets aktiviert wurde.

So können Sie einen Plan für die Konvertierung zu einer virtuellen Maschine erstellen

1. Klicken Sie auf **Verwaltung** –> **Konvertierung zu VM**.
2. Klicken Sie auf **Plan erstellen**.
   Die Software zeigt eine Vorlage für den neuen Plan an.
3. [Optional] Wenn Sie den Namen des Plans ändern wollen, klicken Sie auf den vorgegebenen Standardnamen.
4. Bestimmen Sie bei **Konvertieren zu** den Typ der virtuellen Zielmaschine. **Sie können eine der folgenden Varianten wählen**:

- **VMware ESXi**
- **Microsoft Hyper-V**
- **Scale Computing HC3**
- **VMware Workstation**
- **VHDX-Dateien**

Hinweis
Um Speicherplatz zu sparen, werden bei jeder Konvertierung zu VHDX-Dateien oder VMware Workstation die entsprechenden VHDX/VMDK-Dateien am Zielort überschrieben, die bei der vorherigen Konvertierung erstellt wurden.

5. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - [Für VMware ESXi, Hyper-V und Scale Computing HC3] Klicken Sie auf **Host**, wählen Sie den Zielhost und spezifizieren Sie die Vorlage für den Namen der neuen Maschine.
   - [Für andere Arten von virtuellen Maschinen] Spezifizieren Sie bei **Pfad**, wo die Dateien der virtuellen Maschinen und die Dateinamensvorlage gespeichert werden sollen.

   Der Standardname ist **[Maschinenname]_konvertiert**.
6. Klicken Sie auf **Agent** und bestimmen Sie den Agenten, der die Konvertierung durchführen soll.
7. Klicken Sie auf **Zu konvertierende Elemente** und bestimmen Sie dann die Backups, die dieser Plan zu virtuellen Maschinen konvertieren soll.

   Mit dem Schalter **Speicherorte** / **Backups** (in der rechten oberen Ecke) können Sie zwischen der Auswahl von Backups und der Auswahl kompletter Speicherorte wechseln.

   Wenn die ausgewählten Backups verschlüsselt sind, müssen diese alle dasselbe Verschlüsselungskennwort verwenden. Erstellen Sie für Backups, die unterschiedliche Verschlüsselungskennwörter verwenden, separate Backup-Pläne.
8. [Nur für VMware ESXi und Hyper-V] Klicken Sie auf **Datenspeicher** für ESXi oder **Pfad** für Hyper-V – und bestimmten Sie dann den Datenspeicher (Storage) für die virtuelle Maschine.
9. [Nur für VMware ESXi und Hyper-V] Wählen Sie den Laufwerk-Provisioning-Modus. Die Standardeinstellung ist **Thin** für VMware ESXi und **Dynamisch erweiterbar** für Hyper-V.
10. [Optional] [Für VMware ESXi, Hyper-V und Scale Computing HC3] Klicken Sie auf **VM-Einstellungen**, um die Größe des Arbeitsspeichers, die Anzahl der Prozessoren und die Netzwerkverbindungen für die virtuelle Maschine zu ändern.
11. [Optional] Klicken Sie auf **Planung**, wenn Sie die Planung ändern wollen.
12. Wenn die Backups, die bei **Zu konvertierende Elemente** ausgewählt wurden, verschlüsselt sind, müssen Sie den Schalter **Backup-Kennwort** aktivieren und dann das entsprechende Verschlüsselungskennwort eingeben. Ansonsten können Sie diesen Schritt überspringen.
13. [Optional] Wenn Sie die Plan-Optionen ändern wollen, klicken Sie auf das Zahnradsymbol.
14. Klicken Sie auf **Erstellen**.

Was Sie über Konvertierungen wissen müssen

Diese Typen von virtuellen Maschinen werden unterstützt

Die Konvertierung eines Backups zu einer virtuellen Maschine kann von dem Agenten durchgeführt werden, der das Backup erstellt hat – oder auch von einem anderen Agenten durchgeführt werden.

Um eine Konvertierung zu VMware ESXi, Hyper-V oder Scale Computing HC3 durchzuführen, benötigen Sie einen ESXi-, Hyper-V- bzw. Scale Computing HC3-Host und einen Protection Agenten (Agenten für VMware, Agenten für Hyper-V oder Agenten für Scale Computing HC3), der diesen Host verwaltet.

Eine Konvertierung zu VHDX-Dateien setzt voraus, dass die Dateien als virtuelle Festplatten mit einer virtuellen Hyper-V-Maschine verbunden werden.

Die nachfolgende Tabelle fasst die verschiedenen Typen von virtuellen Maschinen zusammen, die Sie mit der Aktion **Zu VM konvertieren** erstellen können. In den Zeilen der Tabelle ist der Typ der konvertierten virtuellen Maschinen angegeben. In den Spalten sind die Agenten aufgeführt, die die Konvertierung durchführen.

VM-Typ	Agent für VMware	Agent für Hyper-V	Agent für Windows	Agent für Linux	Agent für Mac	Agent für Scale Computing HC3	Agent für oVirt (KVM)	Agent für Virtuozzo Hybrid Infrastructure	Agent für Virtuozzo
VMware ESXi	+	–	–	–	–	–	–	–	–
Microsoft Hyper-V	–	+	–	–	–	–	–	–	–
VMware Workstation	+	+	+	+	–	–	–	–	–
VHDX-Dateien	+	+	+	+	–	–	–	–	–
Scale Computing HC3	–	–	–	–	–	+	–	–	–

Einschränkungen

- Backups, die auf NFS gespeichert sind, können nicht konvertiert werden.
- Backups, die in einer Secure Zone gespeichert sind, können nur von dem Agenten konvertiert werden, der auf derselben Maschine läuft.
- Backups, die logische Linux-Volumes (LVMs) enthalten, können nur konvertiert werden, wenn sie mit dem Agenten für VMware, dem Agenten für Hyper-V oder dem Agenten für Scale Computing HC3 erstellt wurden und auf den gleichen Hypervisor ausgerichtet sind. Eine Hypervisor-übergreifende Konvertierung wird nicht unterstützt.
- Wenn die Backups einer Windows-Maschine zu VMware Workstation- oder VHDX-Dateien konvertiert werden, übernimmt die resultierende virtuelle Maschine den CPU-Typ von derjenigen Maschine, die die Konvertierung durchführt. Als Ergebnis werden auch die entsprechenden CPU-Treiber im Gastbetriebssystem installiert. Beim Start auf einem Host mit einem anderen CPU-Typ zeigt das Gastsystem einen Treiberfehler an. Aktualisieren Sie diesen Treiber manuell.

Regelmäßige Konvertierung zu einer virtuellen Maschine im Vergleich zur Ausführung einer virtuellen Maschine aus einem Backup

Beide Aktionen liefern Ihnen eine virtuelle Maschine, die in wenigen Sekunden, nachdem die ursprüngliche Maschine fehlgeschlagen ist, gestartet werden kann.

Eine regelmäßige Konvertierung zu einer virtuellen Maschine beansprucht CPU- und Arbeitsspeicher-Ressouren. Die Dateien der virtuellen Maschine belegen fortlaufend Speicherplatz im Datenspeicher (Storage). Dies ist möglicherweise nicht praktikabel, wenn ein Produktions-Host zur Konvertierung verwendet wird. Dafür wird die Performance der virtuellen Maschine nur durch die Ressourcen des Hosts beschränkt.

Die Ausführung einer virtuellen Maschine aus einem Backup heraus beansprucht nur dann Ressourcen, wenn die virtuelle Maschine tatsächlich ausgeführt wird. Platz im Datenspeicher (Storage) ist nur dann erforderlich, um Änderungen, die an den virtuellen Laufwerken durchgeführt werden, zu speichern. Die Ausführungsgeschwindigkeit der virtuellen Maschine ist jedoch möglicherweise niedriger, da der Host nicht direkt auf die virtuellen Laufwerke zugreift, sondern mit dem Agenten kommuniziert, der die entsprechenden Daten aus dem Backup liest. Zudem existiert die virtuelle Maschine nur temporär.

So funktioniert die regelmäßige Konvertierung zu einer virtuellen Maschine

Wie die regelmäßige Konvertierung abläuft, hängt davon ab, wo die virtuelle Maschine erstellt werden soll.

- **Bei Auswahl, dass die virtuelle Maschine als ein Satz von Dateien gespeichert werden soll:** Erstellt jede Konvertierung die virtuelle Maschine von Grund aus neu.
- **Bei Auswahl, dass die virtuelle Maschine auf einem Virtualisierungsserver erstellt werden soll:** Wird die Software die vorhandene virtuelle Maschine inkrementell aktualisieren, statt sie neu zu erstellen, wenn ein inkrementelles oder differentielles Backup konvertiert wird. Eine

solche Konvertierung ist normalerweise schneller. Sie geht sparsamer mit Netzwerkverkehr und CPU-Ressourcen des Hosts um, der die Konvertierung durchführt. Falls eine virtuelle Maschine nicht aktualisiert werden kann, erstellt die Software auch diese von Grund auf neu.

Nachfolgend finden Sie eine genauere Beschreibung beider Fälle.

Bei Auswahl, dass die virtuelle Maschine als ein Satz von Dateien gespeichert werden soll

Als Folge der ersten Konvertierung wird eine neue virtuelle Maschine erstellt. Jede nachfolgende Konvertierung wird diese Maschine jeweils ganz neu erstellen. Zuerst wird die alte Maschine temporär umbenannt. Dann wird eine neue virtuelle Maschine erstellt, die den vorherigen Namen der alten Maschine hat. Sobald diese Aktion erfolgreich abgeschlossen wurde, wird die alte Maschine gelöscht. Wenn die Aktion fehlschlägt, wird die neue Maschine gelöscht und die alte Maschine erhält ihren früheren Namen zurück. Auf diese Art schließt die Konvertierung immer mit einer einzelnen Maschine ab. Jedoch wird während der Konvertierung zusätzlicher Speicherplatz benötigt, um die alte Maschine aufzunehmen.

Bei Auswahl, dass die virtuelle Maschine auf einem Virtualisierungsserver erstellt werden soll

Die erste Konvertierung erstellt eine ganz neue virtuelle Maschine. Jede nachfolgende Konvertierung arbeitet folgendermaßen:

- Falls es seit der letzten Konvertierung *ein Voll-Backup* gegeben hat, wird die virtuelle Maschine ganz neu erstellt (wie zuvor in diesem Abschnitt beschrieben).
- Anderenfalls wird die existierende virtuelle Maschine so aktualisiert, dass sie die Änderungen seit der letzten Konvertierung widerspiegelt. Wenn eine Aktualisierung (Update) nicht möglich ist (beispielsweise, weil Sie die zwischenzeitlichen Snapshots gelöscht haben, siehe nachfolgend), wird die virtuelle Maschine ganz neu erstellt.

Zwischenzeitliche Snapshots

Damit die konvertierte virtuelle Maschine zuverlässig aktualisiert werden kann, speichert die Software einen temporären Hypervisor-Snapshot von dieser Maschine. Der Snapshot wird **Replikat...** genannt und muss aufbewahrt werden.

Der **Replikat...**-Snapshot korrespondiert mit dem Ergebnis der letzten Konvertierung. Sie können zu diesem Snapshot zurückgehen, falls Sie die Maschine auf dieses Stadium zurücksetzen wollen – beispielsweise, weil Sie mit der Maschine gearbeitet haben und nun durchgeführte Änderungen verwerfen wollen.

Für konvertierte virtuelle Scale Computing HC3-Maschinen wird ein zusätzlicher **Utility-Snapshot** erstellt. Dieser wird nur vom Cyber Protection Service verwendet.

Schutzpläne und Module

Um Ihre Daten zu schützen, müssen Sie Schutzpläne erstellen und diese dann auf Ihre Workloads anwenden.

Ein Schutzplan besteht aus verschiedenen Schutzmodulen. Aktivieren Sie die Module, die Sie benötigen, und konfigurieren Sie deren Einstellungen, um Schutzpläne zu erstellen, die Ihren spezifischen Anforderungen genügen.

Folgende Module sind verfügbar:

- Backup. Kann Ihre Datenquellen zu einem lokalen Speicherort oder einem Cloud Storage sichern.
- "Disaster Recovery implementieren" (S. 804). Kann bei Bedarf exakte Kopien Ihrer Maschinen auf einer Cloud-Site ausführen und entsprechende Workloads von beschädigten Maschinen zu Recovery-Servern in der Cloud umschalten.
- Antivirus & Antimalware Protection. Kann Ihre Workloads mithilfe einer integrierten Antimalware-Lösung überprüfen.
- Endpoint Detection & Response (EDR). Die Funktionalität kann verdächtige Aktivitäten (einschließlich unbemerkter Angriffe) auf einem Workload erkennen und entsprechende Vorfälle generieren, die Ihnen helfen zu verstehen, wie es zu einem Angriff gekommen ist und wie Sie verhindern können, dass dieser erneut stattfindet.
- URL-Filterung. Schützt Ihre Maschinen vor Bedrohungen aus dem Internet, indem der Zugriff auf schädliche URLs und herunterladbare Inhalte blockiert wird.
- Windows Defender Antivirus. Ermöglicht es, die Einstellungen von Windows Defender Antivirus zu verwalten, damit Sie Ihre Umgebung schützen können.
- Microsoft Security Essentials. Ermöglicht es, die Einstellungen von Microsoft Security Essentials zu verwalten, damit Sie Ihre Umgebung schützen können.
- Schwachstellenbewertung. Ermöglicht es, Microsoft-, Linux-, macOS- sowie Microsoft- und macOS-Drittanbieter-Produkte, die auf Ihren Maschinen installiert sind, auf Schwachstellen zu überprüfen und benachrichtigt Sie, sofern welche gefunden werden.
- Patch-Verwaltung. Ermöglicht es, für Microsoft-, Linux-, macOS- sowie Microsoft- und macOS-Drittanbieter-Produkte, die auf Ihren Maschinen erkannt werden, Patches und Updates zu installieren, um die gefundenen Schwachstellen zu beheben.
- Data Protection-Karte. Ermöglicht es, bestimmte Daten zu ermitteln, um den Sicherungsstatus wichtiger Dateien überwachen zu können.
- Gerätekontrolle. Ermöglicht es Ihnen, bestimmte Geräte zu spezifizieren, die Anwender auf Ihren Maschinen verwenden dürfen oder nicht.
- Advanced Data Loss Prevention. Die Funktionalität verhindert auf der Grundlage einer Datenfluss-Richtlinie, dass sensible Daten über Peripheriegeräte (z.B. Drucker oder Wechseldatenträger) oder über interne und externe Netzwerkübertragungen unautorisiert abfließen können.

Einen Schutzplan erstellen

Sie können einen Schutzplan auf folgende Arten erstellen:

- Auf der Registerkarte **Geräte**: Wählen Sie einen oder mehrere Workloads aus, die Sie schützen wollen, und erstellen Sie anschließend einen Schutzplan für diese Workloads.

- Auf der Registerkarte **Verwaltung** > **Schutzpläne**. Erstellen Sie einen Schutzplan und wählen Sie dann einen oder mehrere Workloads aus, auf die der Plan angewendet werden soll.

Wenn Sie einen Schutzplan erstellen, werden nur diejenigen Module angezeigt, die für Ihre Art von Workload geeignet sind.

Sie können einen Schutzplan auf mehrere Workloads anwenden. Sie können auch mehrere Schutzpläne auf denselben Workload anwenden. Informationen über mögliche Konflikte zu finden Sie unter "Plan-Konflikte lösen" (S. 239).

So können Sie einen Schutzplan erstellen

Geräte

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte** –> **Alle Geräte**.
2. Wählen Sie die Workloads, die Sie schützen wollen, und klicken Sie dann auf **Schützen**.
3. [Wenn es bereits angewendete Pläne gibt] Klicken Sie auf **Plan hinzufügen**.
4. Klicken Sie auf **Plan erstellen** –> **Schutz**.
   Der Fensterbereich 'Schutzplan' wird geöffnet.
5. [Optional] Um den Schutzplan umzubenennen, klicken Sie auf das Stiftsymbol und geben Sie dann den neuen Namen ein.
6. [Optional] Wenn Sie ein Modul in dem Plan (de)aktivieren wollen, müssen Sie den Schalter neben dem Modulnamen umschalten.
7. [Optional] Wenn Sie ein Modul konfigurieren wollen, müssen Sie es anklicken, um es zu erweitern, und dann die Einstellungen entsprechend Ihren Anforderungen anpassen.
8. Klicken Sie, wenn Sie fertig sind, auf **Erstellen**.

> **Hinweis**
> Um einen Schutzplan mit Verschlüsselung zu erstellen, geben Sie ein Verschlüsselungskennwort an. Für weitere Informationen siehe "Verschlüsselung" (S. 484).

Verwaltung –> Schutzpläne

1. Gehen Sie in der Cyber Protect-Konsole zum Bereich **Verwaltung** –> **Schutzpläne**.
2. Klicken Sie auf **Plan erstellen**.
   Die Vorlage für einen Schutzplan wird geöffnet.
3. [Optional] Um den Schutzplan umzubenennen, klicken Sie auf das Stiftsymbol und geben Sie dann den neuen Namen ein.
4. [Optional] Wenn Sie ein Modul in dem Plan (de)aktivieren wollen, müssen Sie den Schalter neben dem Modulnamen umschalten.
5. [Optional] Wenn Sie ein Modul konfigurieren wollen, müssen Sie es anklicken, um es zu erweitern, und dann die Einstellungen entsprechend Ihren Anforderungen anpassen.
6. [Optional] Klicken Sie auf **Geräte hinzufügen**, um diejenigen Workloads auszuwählen, auf die Sie den Plan anwenden wollen.

Hinweis
Sie können einen Plan erstellen, ohne ihn auf Workloads anzuwenden. Sie können die Workloads später hinzufügen, indem Sie den Plan bearbeiten. Weitere Informationen darüber, wie Sie Workloads zu einem Plan hinzufügen können, finden Sie unter "Einen Schutzplan auf einen Workload anwenden" (S. 235).

7. Klicken Sie, wenn Sie fertig sind, auf **Erstellen**.

Hinweis
Um einen Schutzplan mit Verschlüsselung zu erstellen, geben Sie ein Verschlüsselungskennwort an. Für weitere Informationen siehe "Verschlüsselung" (S. 484).

Wenn Sie ein Modul bei Bedarf manuell ausführen wollen (z.B. das **Backup**-, **Antivirus & Antimalware Protection**-, **Schwachstellenbewertungs**-, **Patch-Verwaltungs**- oder **Data Protection-Karten**-Modul), klicken Sie auf **Jetzt ausführen**.

Schauen Sie sich das Anleitungsvideo 'Den ersten Schutzplan erstellen an.

Für weitere Informationen zum Disaster Recovery-Modul siehe "Einen Disaster Recovery-Schutzplan erstellen" (S. 811).

Für weitere Informationen zum Gerätekontrolle-Modul siehe "Mit dem Gerätekontrolle-Modul arbeiten" (S. 398).

Aktionen mit Schutzplänen

Nachdem Sie einen Schutzplan erstellt haben, können Sie folgende Aktionen mit ihm durchführen:

- Einen Plan auf einen Workload oder eine Gerätegruppe anwenden.
- Einen Plan umbenennen.
- Einen Plan bearbeiten.
  Sie können die Module in einem Plan aktivieren und deaktivieren sowie deren Einstellungen ändern.
- Einen Plan aktivieren oder deaktivieren.
  Ein deaktivierter Plan wird auf den Workloads, auf die er angewendet wurde, nicht mehr ausgeführt.
  Diese Aktion ist nützlich für Administratoren, die beabsichtigen, den betreffenden Workload zu einem späteren Zeitpunkt wieder mit diesem Plan zu schützen. Der Plan wird also nicht vom Workload widerrufen und Sie können den Schutz jederzeit schnell wiederherstellen, indem Sie den Plan einfach wieder aktivieren.
- Einen Plan von einem Workload widerrufen.
  Ein Plan zu widerrufen bedeutet, dass dieser nicht mehr auf den Workload angewendet wird.
  Diese Aktion eignet sich für Administratoren, die nicht vorhaben, den Schutz für diesen Workload (mit dem gleichen Plan) kurzfristig wiederherzustellen. Wenn Sie den Schutz durch einen

widerrufenen Plan wiederherstellen wollen, müssen Sie den Namen dieses Plans kennen, ihn aus der Liste der verfügbaren Pläne auswählen und ihn dann erneut auf den gewünschten Workload anwenden.

- Einen Plan stoppen.
  Durch diese Aktion werden alle laufenden Backup-Aktionen auf allen Workloads, auf die der Plan angewendet wurde, gestoppt. Die erneute Ausführung der Backups erfolgt nach dem im Plan konfigurierten Zeitplan.
  Antimalware-Scans sind von dieser Aktion nicht betroffen und werden regulär weiter gemäß der für sie konfigurierten Planung durchgeführt.
- Einen Plan klonen.
  Sie können eine exakte Kopie eines bestehenden Plans erstellen. Der neue Plan ist dann noch keinem Workload zugewiesen.
- Einen Plan exportieren oder importieren.
  Sie können einen Plan als JSON-Datei exportieren. Diese können Sie dann zu einem späteren Zeitpunkt auch wieder importieren. Sie müssen so also keinen neuen Plan manuell erstellen und dann dessen Einstellungen konfigurieren.

  Hinweis
  Sie können Schutzpläne importieren, die in Cyber Protection 9.0 (im März 2020 veröffentlicht) und höher erstellt wurden. Pläne, die mit älteren Versionen erstellt wurden, sind nicht mit Cyber Protection 9.0 und höher kompatibel.

- Die Details eines Plans überprüfen.
- Die Aktivitäten und Alarmmeldungen überprüfen, die zu einem Plan gehören.
- Einen Plan löschen.

Einen Schutzplan auf einen Workload anwenden

Wenn Sie einen Workload schützen wollen, müssen Sie einen Schutzplan auf ihn anwenden.

Sie können einen Plan von der Registerkarte **Geräte** und der Registerkarte **Verwaltung** > **Schutzpläne** aus anwenden.

Geräte

1. Wählen Sie einen oder mehrere Workloads, die Sie schützen wollen.
2. Klicken Sie auf den Befehl **Schützen**.
3. [Wenn auf die ausgewählten Workloads bereits ein anderer Schutzplan angewendet wurde] Klicken Sie auf **Plan hinzufügen**.
4. Es wird eine Liste der verfügbaren Schutzpläne wird angezeigt.
5. Wählen Sie den Schutzplan, den Sie verwenden wollen, aus und klicken Sie dann auf **Anwenden**.

Verwaltung –> Schutzpläne

1. Gehen Sie in der Cyber Protect-Konsole zum Bereich **Verwaltung** –> **Schutzpläne**.
2. Wählen Sie den Schutzplan aus, den Sie anwenden wollen.
3. Klicken Sie auf **Bearbeiten**.
4. Klicken Sie auf **Geräte verwalten**.
5. Klicken Sie im Fenster **Geräte** auf **Hinzufügen**.
6. Wählen Sie die Workloads, auf die Sie den Plan anwenden lassen wollen, aus und klicken Sie anschließend auf **Hinzufügen**.
7. Klicken Sie im Fenster **Geräte** auf **Fertig**.
8. Klicken Sie im Fensterbereich für den Schutzplan auf **Speichern**.

Um zu lernen, wie man einen Schutzplan auf eine Gerätegruppe anwendet, siehe "Einen Plan auf eine Gruppe anwenden" (S. 396).

Einen Schutzplan bearbeiten

Wenn Sie einen Plan bearbeiten, können Sie die darin enthaltenen Module (de)aktivieren und deren Einstellungen ändern.

Sie können einen Schutzplan für alle Workloads, auf die der Plan angewendet wird, bearbeiten oder auch nur für bestimmte Workloads.

Sie können einen Plan über die Registerkarten **Geräte** oder **Verwaltung** > **Schutzpläne** bearbeiten.

Geräte

1. Wählen Sie einen oder mehrere Workloads aus, auf die der Plan angewendet werden soll.
2. Klicken Sie auf den Befehl **Schützen**.
3. Wählen Sie den Schutzplan aus, den Sie bearbeiten wollen.
4. Klicken Sie neben dem Namen des Plans auf das Drei-Punkte-Symbol (...) und anschließend auf den Befehl **Bearbeiten**.
5. Klicken Sie auf ein Modul, das Sie bearbeiten wollen, und konfigurieren Sie dann dessen Einstellungen nach Ihren Anforderungen.
6. Klicken Sie auf **Speichern**.
7. [Wenn Sie nicht alle Workloads ausgewählt haben, auf die der Plan angewendet wurde] Wählen Sie den Umfang der Bearbeitung aus:
   - Wenn Sie den Schutzplan für alle Workloads (auf die er angewendet wird) bearbeiten wollen, klicken Sie auf **Änderungen auf diesen Plan anwenden (wird auch andere Geräte beeinflussen)**.
   - Wenn Sie den Plan nur für bestimmte Workloads ändern wollen, klicken Sie auf **Einen neuen Schutzplan nur für die ausgewählten Geräte erstellen**.

     Als Ergebnis wird der bestehende Plan von den ausgewählten Workloads widerrufen. Es wird ein neuer Schutzplan mit den von Ihnen konfigurierten Einstellungen erstellt und auf diese Workloads angewendet.

Verwaltung –> Schutzpläne

1. Gehen Sie in der Cyber Protect-Konsole zum Bereich **Verwaltung** –> **Schutzpläne**.
2. Wählen Sie den Schutzplan aus, den Sie bearbeiten wollen.
3. Klicken Sie auf **Bearbeiten**.
4. Klicken Sie auf die Module, die Sie bearbeiten wollen, und konfigurieren Sie dann deren Einstellungen nach Ihren Anforderungen.
5. Klicken Sie auf **Speichern**.

Hinweis
Wenn Sie einen Plan über die Registerkarte **Verwaltung** > **Schutzpläne** bearbeiten, betrifft das alle Workloads, auf die dieser Plan angewendet wurden.

Einen Schutzplan widerrufen

Wenn Sie einen Plan widerrufen, wird er von einem oder mehreren Workloads entfernt. Der Plan wird weiterhin die anderen Workloads schützen, auf die er angewendet wird.

Sie können einen Plan über die Registerkarten **Geräte** oder **Verwaltung** > **Schutzpläne** widerrufen.

Geräte

1. Wählen Sie die Workloads aus, von denen Sie den Plan widerrufen wollen.
2. Klicken Sie auf den Befehl **Schützen**.
3. Wählen Sie den Schutzplan aus, den Sie widerrufen wollen.
4. Klicken Sie neben dem Namen des Plans auf das Drei-Punkte-Symbol (...) und anschließend auf den Befehl **Widerrufen**.

Verwaltung –> Schutzpläne

1. Gehen Sie in der Cyber Protect-Konsole zum Bereich **Verwaltung** –> **Schutzpläne**.
2. Wählen Sie den Schutzplan aus, den Sie widerrufen wollen.
3. Klicken Sie auf **Bearbeiten**.
4. Klicken Sie auf **Geräte verwalten**.
5. Wählen Sie im Fenster **Geräte** diejenigen Workloads aus, von denen Sie den Plan widerrufen wollen.
6. Klicken Sie auf **Entfernen**.
7. Klicken Sie im Fenster **Geräte** auf **Fertig**.
8. Klicken Sie in der Schutzplan-Vorlage auf **Speichern**.

Einen Schutzplan aktivieren oder deaktivieren

Ein aktivierter Plan ist eingeschaltet und wird auf den Workloads ausgeführt, auf die er angewendet wird. Ein deaktivierter Plan ist ausgeschaltet. Er bleibt jedoch weiterhin auf die Workloads

angewendet, wird aber nicht mehr auf diesen ausgeführt.

Wenn Sie einen Schutzplan über die Registerkarte **Geräte** aktivieren oder deaktivieren, beeinflusst diese Aktion nur die ausgewählten Workloads.

Wenn Sie einen Schutzplan über die Registerkarte **Verwaltung** –> **Schutzpläne** aktivieren oder deaktivieren, beeinflusst diese Aktion alle Workloads, auf die der Plan angewendet wurde. Außerdem können Sie mehrere Schutzpläne aktivieren oder deaktivieren.

Geräte

1. Wählen Sie den Workload aus, dessen Plan Sie deaktivieren wollen.
2. Klicken Sie auf den Befehl **Schützen**.
3. Wählen Sie den Schutzplan aus, den Sie deaktivieren wollen.
4. Klicken Sie neben dem Namen des Plans auf das Drei-Punkte-Symbol (...) und anschließend auf **Aktivieren** bzw. **Deaktivieren**.

Verwaltung –> Schutzpläne

1. Gehen Sie in der Cyber Protect-Konsole zum Bereich **Verwaltung** –> **Schutzpläne**.
2. Wählen Sie einen oder mehrere Schutzpläne aus, die Sie aktivieren oder deaktivieren wollen.
3. Klicken Sie auf **Bearbeiten**.
4. Klicken Sie auf **Aktivieren** oder **Deaktivieren**.

Hinweis
Diese Aktion wirkt sich nicht auf Schutzpläne aus, die sich bereits im Zielstadium befinden. Wenn Ihre Auswahl zum Beispiel sowohl aktivierte als auch deaktivierte Pläne enthält und Sie auf **Aktivieren** klicken, werden alle ausgewählten Pläne aktiviert.

Einen Schutzplan löschen

Wenn Sie einen Plan löschen, so wird dieser von allen Workloads widerrufen und aus der Konsole von Cyber Protect entfernt.

Sie können einen Plan über die Registerkarten **Geräte** oder **Verwaltung** > **Schutzpläne** löschen.

Geräte

1. Wählen Sie irgendeinen Workload aus, auf den der zu löschende Schutzplan angewendet wird.
2. Klicken Sie auf den Befehl **Schützen**.
3. Wählen Sie den Schutzplan aus, den Sie löschen wollen.
4. Klicken Sie neben dem Namen des Plans auf das Drei-Punkte-Symbol (...) und anschließend auf den Befehl **Löschen**.

Verwaltung –> Schutzpläne

1. Gehen Sie in der Cyber Protect-Konsole zum Bereich **Verwaltung** –> **Schutzpläne**.
2. Wählen Sie den Schutzplan aus, den Sie löschen wollen.
3. Klicken Sie auf **Löschen**.
4. Bestätigen Sie Ihre Wahl, indem Sie das Kontrollkästchen für **Ich bestätige die Löschung von folgendem Plan:** aktivieren, und klicken Sie anschließend auf **Löschen**.

Plan-Konflikte lösen

Sie können mehrere Schutzpläne auf denselben Workload anwenden. Sie können beispielsweise einen Schutzplan anwenden, in dem Sie nur das Modul **Antivirus & Antimalware** aktiviert und konfiguriert haben, und einen anderen Schutzplan, in dem Sie nur das Modul **Backup** aktiviert und konfiguriert haben.

Sie können Schutzpläne kombinieren, in denen verschiedene Module aktiviert sind. Sie können auch mehrere Schutzpläne kombinieren, in denen nur das **Backup**-Modul aktiviert ist. Wenn jedoch ein anderes Modul in mehr als einem Plan aktiviert ist, kommt es zu einem Konflikt. Damit Sie den Plan anwenden können, müssen Sie zuerst den Konflikt lösen.

Ein Konflikt zwischen einem neuen und einem vorhandenen Plan

Wenn ein neuer Plan mit einem bestehenden Plan in Konflikt steht, können Sie diesen auf eine der folgenden Arten lösen:

- Erstellen Sie einen neuen Plan, wenden Sie diesen an und deaktivieren Sie dann den vorhandenen Plan, der mit dem neuen in Konflikt steht.
- Erstellen Sie einen neuen Plan und deaktivieren Sie diesen anschließend.

Ein Konflikt zwischen einem individuellen Plan und einem Gruppenplan

Wenn ein individueller Schutzplan mit einem Gruppenplan in Konflikt steht, der auf eine Gerätegruppe angewendet wird, können Sie den Konflikt auf eine der folgenden Arten lösen:

- Entfernen Sie den Workload von der Gerätegruppe und wenden Sie dann den individuellen Schutzplan auf diesen an.
- Bearbeiten Sie den vorhandenen Gruppenplan oder wenden Sie einen neuen Gruppenplan auf die Gerätegruppe an.

Lizenzproblem

Ein Schutzplan-Modul kann verlangen, dass dem geschützten Workload eine bestimmte Service-Quota zugewiesen wird. Falls die zugewiesene Service-Quota nicht geeignet ist, können Sie den Schutzplan, in dem das entsprechende Modul aktiviert ist, nicht ausführen, aktualisieren oder anwenden.

Führen Sie einen der folgenden Schritte aus, um ein Lizenzproblem zu beheben:

- Deaktivieren Sie das Modul, das von der aktuell zugewiesenen Service-Quota nicht unterstützt wird, und verwenden Sie dann den Schutzplan weiter wie bisher.
- Ändern Sie die zugewiesene Service-Quota manuell. Wie dies geht, wird unter "Die Service-Quota von Maschinen ändern" (S. 201) erläutert.

Standard-Schutzpläne

Ein Standard-Schutzplan ist eine vorkonfigurierte Vorlage, die Sie auf Ihre Workloads anwenden können, um deren schnellen Schutz zu gewährleisten. Wenn Sie einen Standard-Schutzplan verwenden, müssen Sie nicht extra ganz neue Schutzpläne erstellen.

Wenn Sie einen Standard-Schutzplan erstmalig anwenden, wird die Vorlage zu Ihrem Mandanten kopiert. Sie können dann die Module in dem Plan und deren Einstellungen bearbeiten.

Folgende Standardpläne sind verfügbar:

- Cyber Protect Essentials

  Dieser Plan bietet grundlegende Schutzfunktionen und ermöglicht Backups auf Dateiebene.
- Remote-Arbeiter

  Dieser Plan ist für Benutzer optimiert, die außerhalb der Firma (remote) arbeiten wollen. Er bietet häufigere Tasks (wie Backup, Antimalware Protection und Schwachstellenbewertungen), strengere Schutzaktionen sowie optimierte Performance- und Energieoptionen.
- Büro-Arbeiter (Drittanbieter-Antivirus)

  Dieser Plan ist für Anwender optimiert, die im Büro arbeiten und eine Antivirus-Software von einem Drittanbieter bevorzugen. In diesem Plan ist das Modul **Antivirus & Antimalware Protection** deaktiviert.
- Büro-Arbeiter (Acronis Antivirus)

  Dieser Plan ist für Anwender optimiert, die im Büro arbeiten und die Antivirus-Software von Acronis bevorzugen.

Vergleich der Standard-Schutzpläne

Module und Optionen	Standard-Schutzpläne			
	Cyber Protect Essentials	**Remote-Arbeiter**	**Büro-Arbeiter (Drittanbieter-Antivirus)**	**Büro-Arbeiter (Acronis Antivirus)**
Backup	Verfügbar	Verfügbar	Verfügbar	Verfügbar
Backup-Quelle Elemente für das Backup	Dateien/Ordner [Ordner 'Alle Benutzerprofile']	Komplette Maschine	Komplette Maschine	Komplette Maschine

Module und Optionen	Standard-Schutzpläne			
	Cyber Protect Essentials	**Remote-Arbeiter**	**Büro-Arbeiter (Drittanbieter-Antivirus)**	**Büro-Arbeiter (Acronis Antivirus)**
Kontinuierliche Datensicherung (CDP)	Deaktiviert	Aktiviert	Deaktiviert	Deaktiviert
Backup-Ziel	Cloud Storage	Cloud Storage	Cloud Storage	Cloud Storage
Planung	Montag bis Freitag um 23:00:00 Uhr	Montag bis Freitag um 00:00 Uhr Zusätzlich aktivierte Optionen und Startbedingungen: • Task bei Neustart der Maschine ausführen, wenn die Maschine zur geplanten Zeit ausgeschaltet war • Aus Standby- oder Ruhezustandsmodus aufwecken, um ein geplantes Backup zu starten • Akkubelastung senken: Nicht starten, wenn im Akkubetrieb • Nicht starten, wenn eine getaktete Verbindung besteht	Montag bis Freitag um 23:00:00 Uhr	Montag bis Freitag um 23:00:00 Uhr
Backup-Schema	Nur inkrementell	Nur inkrementell	Nur inkrementell	Nur inkrementell
Aufbewahrungsdauer	Backups unbegrenzt behalten	Monatlich: 12 Monate Wöchentlich: 4 Wochen Täglich: 7 Tage	Monatlich: 12 Monate Wöchentlich: 4 Wochen Täglich: 7 Tage	Monatlich: 12 Monate Wöchentlich: 4 Wochen Täglich: 7 Tage
Backup-Optionen	Standardoptionen	Standardoptionen, plus: • Performance und	Standardoptionen	Standardoptionen

Module und Optionen	Standard-Schutzpläne			
	Cyber Protect Essentials	**Remote-Arbeiter**	**Büro-Arbeiter (Drittanbieter-Antivirus)**	**Büro-Arbeiter (Acronis Antivirus)**
		Backup-Fenster (der grüne Satz): CPU-Priorität: Niedrig Ausgabegeschwindigkeit: 50%		
Antivirus & Antimalware Protection	Verfügbar	Verfügbar	Nicht verfügbar	Verfügbar
Active Protection	Aus	Aus	–	Aus
Advanced Antimalware	An	An	–	An
Netzwerkordnerschutz	An	An	–	An
Serverseitiger Schutz	Aus	Aus	–	Aus
Selbstschutz	An	An	–	An
Erkennung von Cryptomining-Prozessen	An	An	–	An
Quarantäne	Dateien aus der Quarantäne entfernen nach: 30 Tagen	Dateien aus der Quarantäne entfernen nach: 30 Tagen	–	Dateien aus der Quarantäne entfernen nach: 30 Tagen
Behavior Engine	Quarantäne	Quarantäne	–	Quarantäne
Exploit-Prävention	Benachrichtigen und den Prozess stoppen	Benachrichtigen und den Prozess stoppen	–	Benachrichtigen und den Prozess stoppen
Echtzeitschutz	Quarantäne	Quarantäne	–	Quarantäne
Scan planen	Schnellscan: Quarantäne Um 14:20 Uhr, Sonntag bis Samstag Vollständiger Scan: Aus	Schnellscan: Aus Vollständiger Scan: Quarantäne Um 13:55 Uhr, Sonntag bis Samstag Zusätzlich aktivierte	–	Schnellscan: Quarantäne Um 14:20 Uhr, Sonntag bis Samstag Vollständiger Scan: Aus

Module und Optionen	Standard-Schutzpläne			
	Cyber Protect Essentials	**Remote-Arbeiter**	**Büro-Arbeiter (Drittanbieter-Antivirus)**	**Büro-Arbeiter (Acronis Antivirus)**
		Optionen und Startbedingungen: • Task bei Neustart der Maschine ausführen, wenn die Maschine zur geplanten Zeit ausgeschaltet war • Aus Standby- oder Ruhezustandsmodus aufwecken, um ein geplantes Backup zu starten • Akkubelastung senken: Nicht starten, wenn im Akkubetrieb		
Ausschlüsse	Ohne	Ohne	–	Ohne
URL-Filterung	Verfügbar	Verfügbar	Verfügbar	Verfügbar
Zugriff auf schädliche Website	Immer den Benutzer fragen	Blockieren	Immer den Benutzer fragen	Immer den Benutzer fragen
Zu filternde Kategorien	Standardoptionen	Standardoptionen	Standardoptionen	Standardoptionen
Ausschlüsse	Ohne	Ohne	Ohne	Ohne
Schwachstellenbewertung	Verfügbar	Verfügbar	Verfügbar	Verfügbar
Schwachstellenbewertungsumfang	Microsoft-Produkte, Windows-Produkte von Drittanbietern	Microsoft-Produkte, Windows-Produkte von Drittanbietern	Microsoft-Produkte, Windows-Produkte von Drittanbietern	Microsoft-Produkte, Windows-Produkte von Drittanbietern
Planung	Um 13:15 Uhr, nur am Montag	Um 14:20 Uhr, nur am Montag	Um 13:15 Uhr, nur am Montag	Um 13:15 Uhr, nur am Montag

Module und Optionen	Standard-Schutzpläne			
	Cyber Protect Essentials	**Remote-Arbeiter**	**Büro-Arbeiter (Drittanbieter-Antivirus)**	**Büro-Arbeiter (Acronis Antivirus)**
Patch-Verwaltung	Verfügbar	Verfügbar	Verfügbar	Verfügbar
Microsoft-Produkte	Alle Updates	Alle Updates	Alle Updates	Alle Updates
Windows-Produkte von Drittherstellern	Nur größere Updates	Nur größere Updates	Nur größere Updates	Nur größere Updates
Planung	Um 15:10 Uhr, nur am Montag	Um 14:20 Uhr, Montag bis Freitag	Um 15:10 Uhr, nur am Montag	Um 15:10 Uhr, nur am Montag
Vor-Update-Backup	Aus	An	Aus	Aus
Data Protection-Karte	Nicht verfügbar	Verfügbar	Verfügbar	Verfügbar
Erweiterungen und Ausnahmeregeln	–	Standardoptionen und folgende zusätzliche Erweiterungen: **Images** • .jpeg • .jpg • .png • .gif • .bmp • .ico • .wbmp • .xcf • .psd • .tiff • .dwg **Audio und Video** • .avi, • .mov, • .mpeg, • .mpg, • .mkv • .wav • .aif • .aifc	Standardoptionen (66 zu erkennende Erweiterungen)	Standardoptionen (66 zu erkennende Erweiterungen)

Module und Optionen	Standard-Schutzpläne			
	Cyber Protect Essentials	Remote-Arbeiter	Büro-Arbeiter (Drittanbieter-Antivirus)	Büro-Arbeiter (Acronis Antivirus)
		• .aiff • .au • .snd • .mid • .midi • .mpga • .mp3 • .oga • .flac • .opus • .spx • .ogg • .ogx • .mp4		
Planung	–	Um 15:35 Uhr, Montag bis Freitag	Um 15:40 Uhr, Montag bis Freitag	Um 15:40 Uhr, Montag bis Freitag

Hinweis
Die Anzahl der Module in einem Standard-Schutzplan kann in Abhängigkeit von Ihrer Cyber Protection-Lizenz variieren.

Einen Standard-Schutzplan anwenden

Die anfänglichen Standard-Schutzpläne sind Vorlagen, deren Einstellungen Sie nicht bearbeiten können. Wenn Sie einen Standardplan erstmalig anwenden, wird die Vorlage als vorkonfigurierter Schutzplan zu Ihrem Mandanten kopiert und auf den ausgewählten Workloads aktiviert.

Der Schutzplan wird auf der Registerkarte **Verwaltung** –> **Schutzpläne** angezeigt, wo Sie ihn dann verwalten können.

So können Sie einen Standard-Schutzplan zum ersten Mal anwenden

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte** –> **Alle Geräte**.
2. Wählen Sie die Workloads aus, die Sie schützen wollen.
3. Klicken Sie auf den Befehl **Schützen**.
4. Wählen Sie einen der Standardpläne aus und klicken Sie dann auf **Anwenden**.

Einen Standard-Schutzplan bearbeiten

Sie können einen Standard-Schutzplan bearbeiten, nachdem Sie ihn zum ersten Mal angewendet haben.

So können Sie einen angewendeten Standard-Schutzplan bearbeiten

1. Gehen Sie in der Cyber Protect-Konsole zum Bereich **Verwaltung** –> **Schutzpläne**.
2. Wählen Sie den zu bearbeitenden Plan aus und klicken Sie dann auf **Bearbeiten**.
3. Ändern Sie die Module, die in diesem Plan enthalten sind, oder deren Optionen – und klicken Sie dann auf **Speichern**.

Wichtig
Einige der Optionen können nicht geändert werden.

Individuelle Schutzpläne für die Integration von Webhosting Control Panels

Wenn Sie Webhosting Control Panel-Integrationen auf Ihren Webhosting-Servern aktivieren, die DirectAdmin, cPanel oder Plesk verwenden, wird der Cyber Protection Service automatisch für jeden Workload einen individuellen Schutzplan unter Ihrem Benutzerkonto erstellen. Dieser Schutzplan ist mit dem jeweiligen Workload assoziiert, der das Erstellen des Schutzplans initiiert hat. Er kann nicht widerrufen oder anderen Workloads zugewiesen werden.

Wenn Sie einen individuellen Schutzplan nicht mehr verwenden wollen, können Sie ihn aus der Cyber Protect-Konsole löschen. Sie können die jeweiligen Schutzpläne an dem Zeichen neben ihrem Namen erkennen.

Wenn Sie einen Schutzplan zur Absicherung mehrerer Webhosting-Server wollen, die Webhosting Control Panel-Integrationen verwenden, können Sie in der Cyber Protect-Konsole einen regulären Schutzplan erstellen und ihm diese Workloads zuweisen. Ein Schutzplan, der von mehreren Webhosting Control Panels gemeinsam genutzt wird, kann jedoch nur über die Cyber Protect-Konsole und nicht innerhalb der Integrationen geändert werden.

#CyberFit-Score für Maschinen

Der #CyberFit-Score bietet Ihnen einen Sicherheitsbewertungs- und Scoring-Mechanismus, der die Sicherheitslage Ihrer Maschine bewertet. Er identifiziert Sicherheitslücken in Ihrer IT-Umgebung sowie offene Angriffsvektoren für die Endpunkte – und stellt anschließend 'empfohlene Aktionen' für Verbesserungen bereit (in Form eines Berichts). Diese Funktionalität ist in allen Editionen von Cyber Protect verfügbar.

Die #CyberFit-Score-Funktionalität wird unterstützt für:

- Windows 7 (erste Version) und höhere Versionen
- Windows Server 2008 R2 und höhere Versionen

Und so funktioniert es

Der auf einer Maschine installierte Protection Agent führt eine Sicherheitsbewertung durch und berechnet den #CyberFit-Score für diese Maschine. Der #CyberFit-Score einer Maschine wird automatisch und in regelmäßigen Abständen neu berechnet.

Der #CyberFit-Scoring-Mechanismus

Der #CyberFit-Score für eine Maschine wird auf der Grundlage folgender Metriken berechnet:

- Antimalware Protection 0-275
- Backup-Schutz 0-175
- Firewall 0-175
- VPN (Virtual Private Network) 0-75
- Vollständige Laufwerksverschlüsselung 0-125
- Netzwerksicherheit 0-25

Der maximale #CyberFit-Score für eine Maschine ist 850.

Metrik	Was wird bewertet?	Empfehlungen an die Benutzer	Scoring
Antimalware	Der Agent überprüft, ob auf der Maschine eine Antimalware-Software installiert ist.	Ergebnisse: • Sie haben die Antimalware Protection aktiviert (+275 Punkte) • Sie haben keine Antimalware Protection; Ihr System ist möglicherweise gefährdet (0 Punkte) Vom #CyberFit-Score gegebene Empfehlungen: Sie sollten eine Antimalware-Lösung auf Ihrer Maschine installiert und aktiviert haben, um vor Sicherheitsrisiken geschützt zu sein. Sie können auf Websites wie	275 – auf einer Maschine ist eine Antimalware-Software installiert 0 – auf einer Maschine ist keine Antimalware-Software installiert

		AV-Test oder AV-Comparatives zurückgreifen, wenn Sie eine Liste von empfohlenen Antimalware-Lösungen einsehen wollen.	
Backup	Der Agent überprüft, ob auf einer Maschine eine Backup-Lösung installiert ist.	Ergebnisse: • Sie haben eine Backup-Lösung, die Ihre Daten sichert (+175 Punkte) • Es wurde keine Backup-Lösung gefunden; Ihre Daten sind möglicherweise gefährdet (0 Punkte) Vom #CyberFit-Score gegebene Empfehlungen: Wir empfehlen, dass Sie Ihre Daten regelmäßig sichern, um Datenverluste (z.B. durch Ransomware-Angriffe) zu verhindern. Nachfolgend sind einige Backup-Lösungen aufgeführt, deren Verwendung Sie erwägen sollten: • Acronis Cyber Protect / Cyber Backup / True Image • Windows Server Backup (Windows Server 2008 R2 und höher)	175 – auf einer Maschine ist eine Backup-Lösung installiert 0 – auf einer Maschine ist keine Backup-Lösung installiert
Firewall	Der Agent überprüft, ob eine Firewall verfügbar ist und in Ihrer Umgebung aktiviert wurde. Der Agent macht Folgendes: 1. Er überprüft im Windows Firewall- und Netzwerkschutz, ob eine öffentliche Firewall eingeschaltet ist.	Ergebnisse: • Sie haben eine Firewall für öffentliche und private Netzwerke aktiviert – oder es wurde eine Firewall-Lösung eines Drittherstellers gefunden (+175 Punkte) • Sie haben eine Firewall nur für öffentliche Netzwerke aktiviert (+100 Punkte)	100 – die öffentliche Windows-Firewall ist aktiviert 75 – die private Windows-Firewall ist aktiviert 175 – die öffentliche und

	2. Er überprüft im Windows Firewall- und Netzwerkschutz, ob eine private Firewall eingeschaltet ist. 3. Er überprüft, ob es eine Firewall-Lösung eines Drittherstellers gibt, wenn die öffentliche und private Windows-Firewall deaktiviert ist.	• Sie haben eine Firewall nur für private Netzwerke aktiviert (+75 Punkte) • Sie haben keine Firewall aktiviert, Ihre Netzwerkverbindung ist nicht sicher (0 Punkte) Vom #CyberFit-Score gegebene Empfehlungen: Wir empfehlen, eine Firewall für Ihre öffentlichen und/oder privaten Netzwerke zu aktivieren, um den Sicherheitsschutz Ihres Systems gegenüber bösartigen Angriffen zu verbessern. Nachfolgend finden Sie ausführliche Anleitungen zur Einrichtung Ihrer Windows-Firewall, in Abhängigkeit von Ihren Sicherheitsanforderungen und Ihrer Netzwerkarchitektur: Anleitungen für Endbenutzer/Mitarbeiter: So können Sie die Windows Defender-Firewall auf Ihrem PC einrichten So können Sie die Windows-Firewall auf Ihrem PC einrichten Anleitungen für Systemadministratoren und Techniker: So können Sie die Window Defender-Firewall mit erweiterter Sicherheit bereitstellen So können Sie erweiterte Regeln in der Windows-Firewall erstellen	private Windows-Firewall ist aktiviert ODER die Firewall-Lösung eines Drittherstellers ist aktiviert 0 – es ist weder eine Windows-Firewall noch eine Firewall-Lösung eines Drittanbieters aktiviert

VPN (Virtual Private Network)	Der Agent überprüft, ob auf einer Maschine eine VPN-Lösung installiert ist und, falls ja, ob das VPN aktiviert ist und läuft.	Ergebnisse: • Sie haben eine VPN-Lösung und können daher Daten sicher über öffentliche und freigegebene Netzwerke empfangen bzw. senden (+75 Punkte) • Es wurde keine VPN-Lösung gefunden; Ihre Verbindung zu öffentlichen und freigegebenen Netzwerken ist nicht sicher (0 Punkte) Vom #CyberFit-Score gegebene Empfehlungen: Wir empfehlen, ein VPN zu verwenden, um auf Ihr Unternehmensnetzwerk bzw. vertrauliche Daten zuzugreifen. Es ist wichtig, ein VPN zu verwenden, damit Ihre Kommunikation sicher und vertraulich bleibt. Das gilt insbesondere, wenn Sie einen kostenlosen bzw. öffentlichen Internetzugang (z.B. in einem Café, einer Bibliothek, einem Flughafen etc.) verwenden. Nachfolgend sind einige VPN-Lösungen aufgeführt, deren Verwendung Sie erwägen sollten: • Acronis Business VPN • OpenVPN • Cisco AnyConnect • NordVPN • TunnelBear • ExpressVPN • PureVPN • CyberGhost VPN • Perimeter 81	75 – ein VPN ist aktiviert und wird ausgeführt 0 – kein VPN ist aktiviert

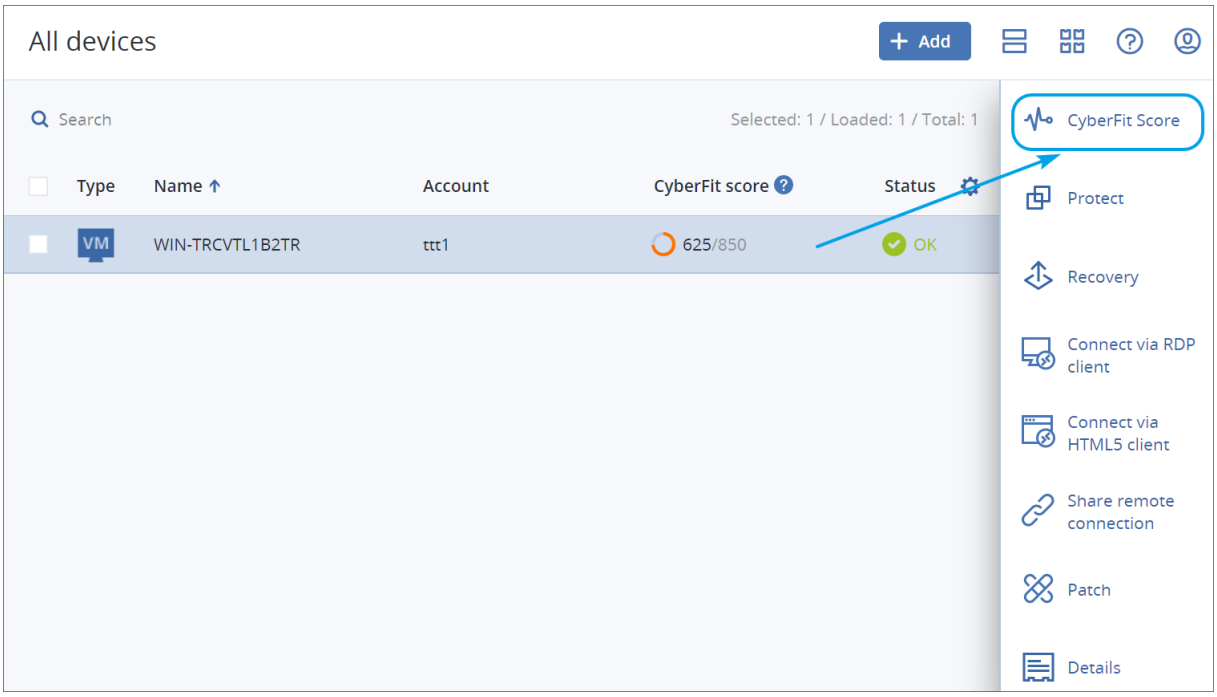
		• VyprVPN • IPVanish VPN • Hotspot Shield VPN • Fortigate VPN • ZYXEL VPN • SonicWall GVPN • LANCOM VPN	
Laufwerksverschlüsselung	Der Agent überprüft, ob für Ihre Maschine eine Laufwerksverschlüsselung aktiviert ist. Der Agent überprüft, ob Windows BitLocker eingeschaltet ist.	Ergebnisse: • Sie haben eine vollständige Laufwerksverschlüsselung aktiviert, Ihre Maschine ist vor physischen Manipulationen geschützt (+125 Punkte) • Es sind nur einige Laufwerke verschlüsselt; Ihre Maschine ist möglicherweise für physische Manipulation anfällig (+75 Punkte) • Es wurde keine Laufwerksverschlüsselung gefunden; Ihre Maschine ist für physische Manipulationen anfällig (0 Punkte) Vom #CyberFit-Score gegebene Empfehlungen: Wir empfehlen, dass Sie Windows BitLocker einschalten, um den Schutz Ihrer Daten und Dateien zu verbessern. Anleitung: So können Sie die Laufwerksverschlüssung unter Windows einschalten	125 – alle Laufwerke sind verschlüsselt 75 – mindestens eine Ihrer Laufwerke ist verschlüsselt, aber es gibt auch unverschlüsselte Laufwerke 0 – keine Laufwerke sind verschlüsselt
Netzwerksicherheit (ausgehender NTLM-Traffic zu Remote-Servern)	Der Agent überprüft, ob eine Maschine den ausgehenden NTLM-Traffic (Datenverkehr) zu Remote-Servern	Ergebnisse: • Ausgehender NTLM-Traffic zu Remote-Servern wird verweigert; Ihre	25 – der ausgehende NTML-Traffic ist auf 'Alle verweigern'

	eingeschränkt hat.	Anmeldedaten sind geschützt (+25 Punkte) • Ausgehender NTLM-Traffic zu Remote-Servern wird nicht verweigert; Ihre Anmeldedaten sind für eine Offenlegung anfällig (0 Punkte) Vom #CyberFit-Score gegebene Empfehlungen: Für einen besseren Sicherheitsschutz empfehlen wir, den gesamten ausgehenden NTLM-Traffic zu Remote-Servern zu verweigern. Informationen über die Änderung der NTLM-Einstellungen und das Hinzufügen von Ausnahmen finden Sie unter diesem Link: Anleitung: Ausgehenden NTLM-Traffic zu Remote-Servern einschränken	eingestellt 0 – der ausgehende NTML-Traffic ist auf einen anderen Wert eingestellt

Basierend auf der Summe der Punkte, die für jede Metrik vergeben werden, kann der #CyberFit-Gesamt-Score einer Maschine einer der folgenden Bewertungen entsprechen, die das Schutzniveau des betreffenden Endpunkts widerspiegeln:

- 0-579 – Schlecht
- 580-669 – Ausreichend
- 670-739 – Gut
- 740-799 – Sehr gut
- 800-850 – Hervorragend

Sie können den #CyberFit-Score für Ihre Maschinen in der Cyber Protect-Konsole einsehen: gehen Sie zu **Geräte** –> **Alle Geräte**. In der Liste der Geräte wird die Spalte **#CyberFit-Score** angezeigt. Sie können außerdem den #CyberFit-Score-Scan für eine Maschine ausführen, um deren Sicherheitslage zu überprüfen.

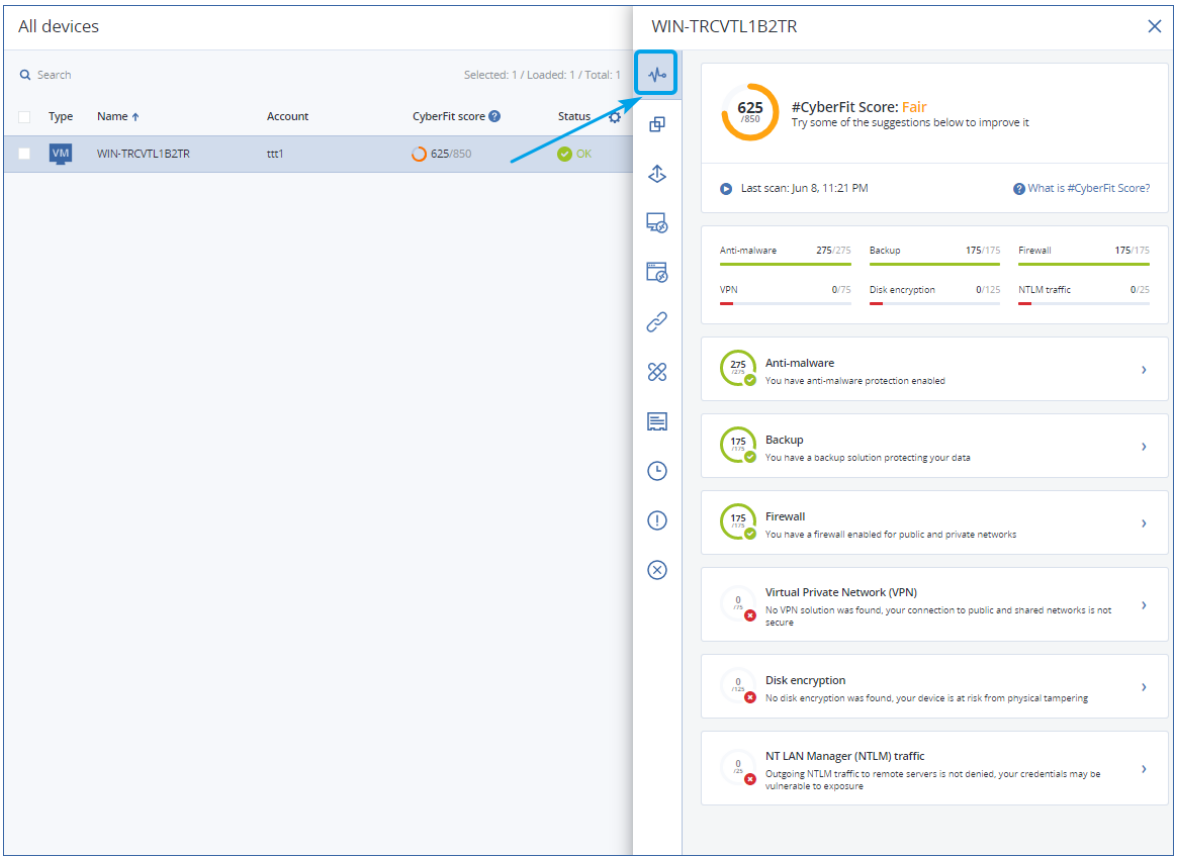


Außerdem können Sie Informationen über den #CyberFit-Score auf den entsprechenden Seiten 'Widget' und/oder 'Bericht' erhalten.

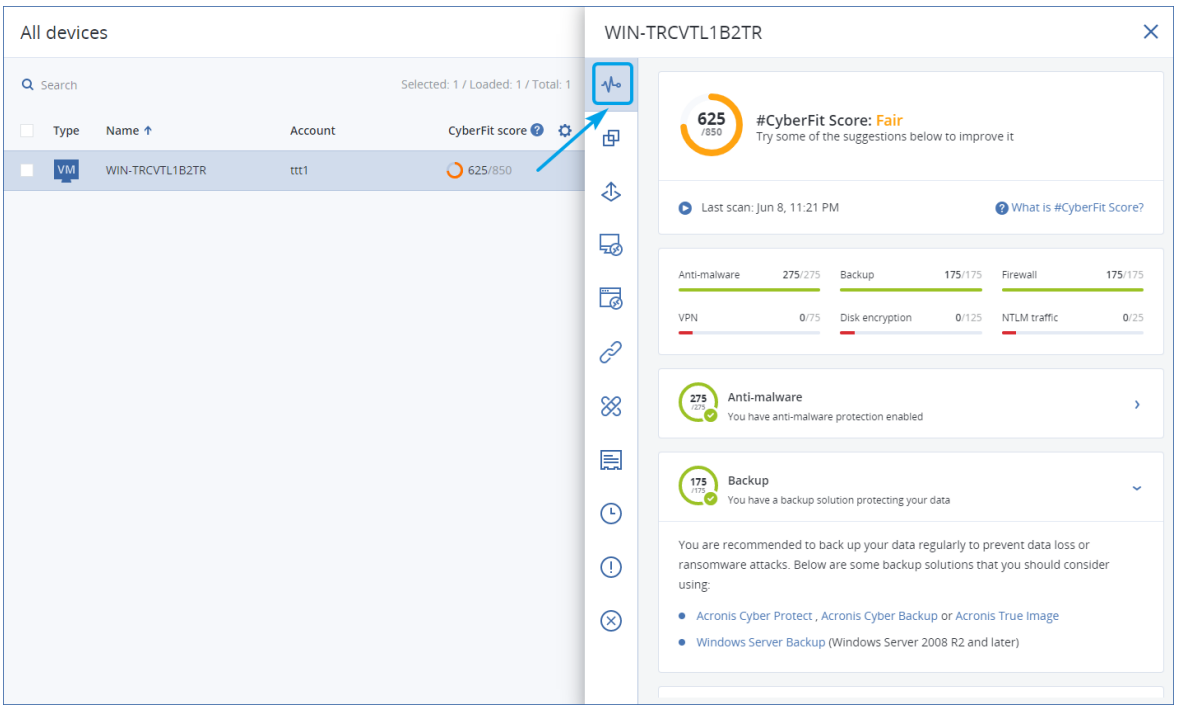
Einen #CyberFit-Score-Scan ausführen

So können Sie einen #CyberFit-Score-Scan ausführen

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte**.
2. Wählen Sie die gewünschte Maschine aus und klicken Sie auf **#CyberFit-Score**.
3. Wenn die Maschine bisher noch nie gescannt wurde, klicken Sie auf den Befehl **Einen ersten Scan durchführen**.
4. Nachdem der Scan abgeschlossen wurde, sehen Sie den #CyberFit-Gesamt-Score für die Maschine zusammen mit den Einzel-Scores für jede der sechs bewerteten Metriken: Antimalware Protection, Backup, Firewall, VPN (Virtual Private Network), Laufwerksverschlüsselung und NTLM-Traffic (NT-LAN-Manager).



5. Wenn Sie überprüfen wollen, wie Sie den Score für jede Metrik, für die die Sicherheitskonfigurationen verbessert werden könnten, erhöhen können, erweitern Sie den entsprechenden Abschnitt und lesen Sie die gegebenen Empfehlungen.



6. Wenn Sie die Empfehlungen umgesetzt haben sollten, können Sie den #CyberFit-Score der Maschine jederzeit neu berechnen lassen, indem Sie auf die Pfeilschaltfläche rechts unter dem #CyberFit-Gesamt-Score klicken.

Cyber Scripting

Mit Cyber-Scripting können Sie regelmäßige Aktionen auf Windows- und macOS-Maschinen in Ihrer Umgebung durch das Ausführen von entsprechenden Skripten automatisieren – wie etwa Software zu installieren, Konfigurationen zu ändern, Dienste zu starten oder zu stoppen und Konten zu erstellen. So können Sie den Zeitaufwand für solche Aktionen verringern und das Fehlerrisiko senken, das manuelle Ausführungen ansonsten mit sich bringen würden.

Cyber-Skripting ist für Administratoren und Benutzer auf Kundenebene sowie für Partner-Administratoren (Service-Provider) verfügbar. Weitere Informationen zu den verschiedenen Verwaltungsebenen finden Sie im Abschnitt "Unterstützung für mehrere Mandanten" (S. 358).

Um Skripte verwenden zu können, müssen diese vorher genehmigt werden. Nur Administratoren mit der Rolle **Cyber-Administrator** können neue Skripte testen und genehmigen. Weitere Informationen zur Änderung des Skript-Status finden Sie unter "Den Skript-Status ändern" (S. 266).

In Abhängigkeit von Ihrer Benutzerrolle können Sie verschiedene Aktionen mit Skripten und Skripting-Plänen durchführen. Weitere Informationen zu Benutzerrollen finden Sie unter "Benutzerrollen und Cyber-Skripting-Rechte" (S. 256).

Voraussetzungen

- Für die Cyber-Skripting-Funktionalität ist das Advanced Management-Paket erforderlich.
- Um alle Cyber-Skripting-Funktionen verwenden zu können (wie etwa Skripte zu bearbeiten, Skripte auszuführen, Skripting-Pläne zu erstellen usw.), müssen Sie die Zwei-Faktor-Authentifizierung für Ihr Konto aktivieren.

Einschränkungen

- Folgende Skripting-Sprachen werden unterstützt:
  - PowerShell
  - Bash
- Cyber-Skripting-Aktionen können nur auf solchen Zielmaschinen ausgeführt werden, auf denen ein Protection Agent installiert ist.

Unterstützte Plattformen

Cyber Scripting ist für Windows- und macOS-Workloads verfügbar.

Die nachfolgende Tabelle fasst die unterstützten Versionen zusammen.

Betriebssystem	Version
Windows	Windows 7 SP1 und höher – alle Editionen
	Windows 8/8.1 – alle Editionen (x86, x64), ausgenommen Windows RT
	Windows 10 – die Editionen Home, Pro, Education, Enterprise und IoT Enterprise
	Windows 11
	Windows Server 2008 R2 SP1 und höher – die Editionen Standard, Enterprise, Datacenter, Foundation und Web
	Windows Server 2012/2012 R2 – alle Editionen
	Windows Server 2016
	Windows Server 2019
	Windows Server 2022
	Windows Storage Server (2008 R2, 2012, 2012 R2, 2016)
macOS	macOS Mojave 10.14
	macOS Catalina 10.15
	macOS Big Sur 11
	macOS Monterey 12

Benutzerrollen und Cyber-Skripting-Rechte

Die Aktionen, die mit Skripten und Skripting-Plänen verfügbar sind, hängen vom Skript-Status und Ihrer Benutzerrolle ab.

Administratoren können Objekte in ihrem eigenen Mandanten und in dessen Untermandanten verwalten. Sie können keine Objekte auf einer höheren Verwaltungsebene sehen oder auf diese zugreifen (sofern solche vorhanden sind).

Administratoren einer niedrigeren Ebene können nur lesend auf die Skripting-Pläne zugreifen, die von einem Administrator einer höheren Ebene auf ihre Workloads angewendet wurden.

Folgende Rollen gewähren Rechte, die sich auf Cyber-Skripting beziehen:

- **Firmenadministrator**
  Diese Rolle gewährt dem Administrator vollständige Rechte in allen Services. In Bezug auf Cyber-Skripting gewährt diese Rolle die gleichen Rechte wie die Rolle 'Cyber-Administrator'.
- **Cyber-Administrator**

Diese Rolle gewährt volle Berechtigungen, einschließlich der Genehmigung von Skripten, die im Mandanten verwendet werden können – und die Fähigkeit, Skripte mit dem Status **Wird getestet** auszuführen.

- **Administrator**
  Diese Rolle gewährt Teilberechtigungen, mit der Möglichkeit, genehmigte Skripte auszuführen – sowie Skripting-Pläne zu erstellen und auszuführen, die genehmigte Skripte verwenden.
- **Nur-Lesen-Administrator**
  Diese Rolle gewährt eingeschränkte Berechtigungen, mit der Möglichkeit, Skripte und Schutzpläne einzusehen, die im Mandanten verwendet werden.
- **Benutzer**
  Diese Rolle gewährt Teilberechtigungen, mit der Möglichkeit, genehmigte Skripte auszuführen – sowie Skripting-Pläne zu erstellen und auszuführen, die genehmigte Skripte verwenden, jedoch nur auf der eigenen Maschine des Benutzers.

Die nachfolgende Tabelle fasst alle verfügbaren Aktionen zusammen, abhängig vom Skript-Status und der Benutzerrolle.

Rolle	**Objekt**	**Skript-Status**		
		Entwurf	**Wird getestet**	**Genehmigt**
Cyber-Administrator **Firmenadministrator**	Skripting-Plan	Bearbeiten (Einen Skript-Entwurf aus einem Plan entfernen) Löschen Widerrufen Deaktivieren Stopp	Erstellen Bearbeiten Anwenden Aktivieren Ausführen Löschen Widerrufen Deaktivieren Stopp	Erstellen Bearbeiten Anwenden Aktivieren Ausführen Löschen Widerrufen Deaktivieren Stopp
	Skript	Erstellen Bearbeiten Status ändern Klonen Löschen Ausführung abbrechen	Erstellen Bearbeiten Status ändern Ausführen Klonen Löschen Ausführung abbrechen	Erstellen Bearbeiten Status ändern Ausführen Klonen Löschen Ausführung abbrechen

Administrator **Benutzer** (für deren eigene Workloads)	Skripting-Plan	Anzeigen Widerrufen Deaktivieren Stopp	Anzeigen Ausführung abbrechen	Erstellen Bearbeiten Anwenden Aktivieren Ausführen Löschen Widerrufen Deaktivieren Stopp
	Skript	Erstellen Bearbeiten Klonen Löschen Ausführung abbrechen	Anzeigen Klonen Ausführung abbrechen	Ausführen Klonen Ausführung abbrechen
Nur-Lesen-Administrator	Skripting-Plan	Anzeigen	Anzeigen	Anzeigen
	Skript	Anzeigen	Anzeigen	Anzeigen

Skripte

Ein Skript ist ein Satz von Anweisungen, die nur zur Laufzeit interpretiert und auf einer Zielmaschine ausgeführt werden. Ein Skript ist eine komfortable Lösung, um wiederkehrende oder komplexe Tasks zu automatisieren.

Die Cyber-Scripting-Funktionalität ermöglicht Ihnen, vordefinierte Skripte auszuführen oder eigene Skripte zu erstellen. Sie können alle Skripte, die Ihnen zur Verfügung stehen, unter **Verwaltung** > **Skript-Repository** einsehen. Alle vordefinierten Skripte befinden sich im Bereich **Bibliothek**. Skripte, die Sie für Ihren Mandanten erstellt oder zu diesem geklont haben, befinden sich im Bereich **Meine Skripte**.

Sie können ein Skript verwenden, indem Sie es in einen Skripting-Plan aufnehmen oder das Skript über die Aktion **Schnelle Skript-Ausführung** starten.

Hinweis
Sie können nur Skripte verwenden, die in Ihrem Mandanten erstellt oder zu diesem geklont wurden. Wenn ein Skript aus dem Skript-Repository entfernt wurde oder wenn dessen Status auf **Entwurf** geändert wurde, wird es nicht ausgeführt. Wenn Sie die Details einer Skripting-Aktion überprüfen oder die Aktion abbrechen wollen, können Sie dies unter **Monitoring** > **Aktivitäten** tun.

Die folgende Tabelle bietet weitere Informationen über die möglichen Aktionen, die mit einem Skript und in Abhängigkeit von dessen Status durchgeführt werden können.

Status	Mögliche Aktionen
Entwurf	Die neuen Skripte, die Sie erstellen, sowie die Skripte, die Sie in Ihr Repository klonen, befinden sich im Status **Entwurf**. Ihnen fehlen jedoch die Berechtigungen, diese Skripte auszuführen oder sie in Skripting-Plänen einzuschließen.
Wird getestet	Nur Administratoren mit der **Cyber-Administrator**-Rolle können diese Skripte ausführen und sie in Skripting-Plänen einbinden.
Genehmigt	Sie können diese Skripte ausführen und in Skripting-Pläne einbinden.

Nur Administratoren mit der Rolle des **Cyber-Administrators** können den Status eines Skripts ändern oder ein genehmigtes Skript löschen. Weitere Informationen finden Sie unter "Den Skript-Status ändern" (S. 266).

Ein Skript erstellen

Sie können ein Skript auch manuell erstellen, indem Sie dessen Code selbst schreiben.

So können Sie ein Skript erstellen

1. Gehen Sie in der Cyber Protect-Konsole zum Bereich **Verwaltung** –> **Skript-Repository**.
2. Klicken Sie bei **Meine Skripte** auf **Skript mithilfe von KI erstellen**.
3. Geben Sie im Hauptfenster den Textkörper des Skripts ein.

   Wichtig
   Wenn Sie ein Skript erstellen, sollten Sie für jede Aktion (Operation) eine Exit-Code-Prüfung einschließen. Anderenfalls könnte eine fehlgeschlagene Aktion ignoriert werden und der Status der Skripting-Aktivität unter **Monitoring** –> **Aktivitäten** fälschlicherweise als **Erfolgreich** angezeigt werden.

4. Spezifizieren Sie die Skript-Einstellungen.

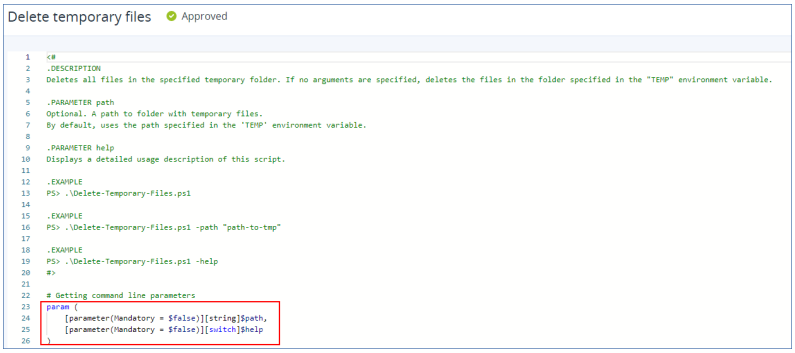
Einstellung	Beschreibung
Skript-Name	Skriptname. Das Feld wird automatisch ausgefüllt, aber Sie können den Wert

Einstellung	Beschreibung
	ändern.
Beschreibung	Skript-Beschreibung. Diese Einstellung ist optional. [Bei per KI generierten Skripten] Das Feld wird automatisch bei der Erstellung des Skripts ausgefüllt. Sie können die von der KI bereitgestellte Beschreibung bearbeiten.
Sprache	Skript-Sprache. Die verfügbaren Werte sind: • **PowerShell**. Dies ist der Standardwert. • **Bash** [Bei per KI generierten Skripten] Diese Einstellung wird konfiguriert, bevor das Skript generiert wird.
Betriebssystem	Das Betriebssystem, das auf dem Ziel-Workload installiert ist, auf dem das Skript ausgeführt wird. Die verfügbaren Werte sind: • **Windows** . Dies ist der Standardwert. • **macOS** [Bei per KI generierten Skripten] Diese Einstellung wird konfiguriert, bevor das Skript generiert wird.
Status	Skript-Status. • **Entwurf**. Dies ist der Standardwert. Die neuen Skripte, die Sie erstellen, sowie die Skripte, die Sie in Ihr Repository klonen, befinden sich im Status **Entwurf**. Ihnen fehlen die Berechtigungen, Skripte mit dem Status **Entwurf** auszuführen oder diese in Skripting-Pläne einzubeziehen. • **Wird getestet**. Nur Administratoren mit der Rolle **Cyber-Administrator** können den Status eines Skripts zu **Wird getestet** ändern, Skripte mit dem Status **Wird getestet** ausführen oder Skripting-Pläne mit solchen Skripten ausführen. • **Genehmigt**. Sie können Skripte mit dem Status **Genehmigt** ausführen und diese in Skripting-Pläne einbeziehen. Nur Administratoren mit der Rolle des **Cyber-Administrators** können den Status eines Skripts ändern oder ein genehmigtes Skript löschen. Weitere Informationen finden Sie unter "Den Skript-Status ändern" (S. 266).
Tags	Bei Tags wird nicht zwischen Groß- und Kleinschreibung unterschieden und sie können bis zu 32 Zeichen lang sein. Sie dürfen keine runden oder spitzen Klammern, keine Kommata und keine Leerzeichen verwenden. Diese Einstellung ist optional. [Bei per KI generierten Skripten] Das Tag **KI-generiert** wird als Kennzeichnung automatisch bei der Skript-Erstellung hinzugefügt. Sie können dieses Tag manuell löschen oder weitere Tags hinzufügen.

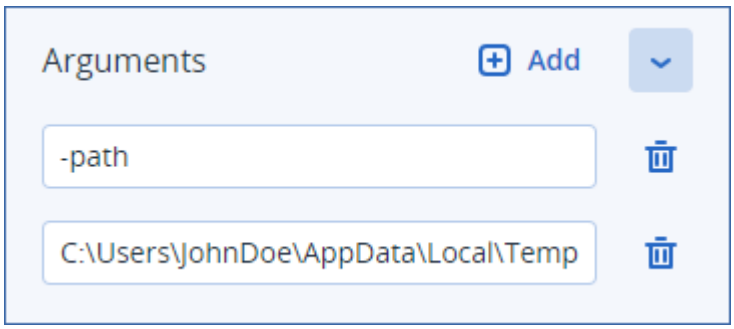
5. [Nur für Skripte, die Anmeldedaten erfordern] Spezifizieren Sie die Anmeldedaten.
   Sie können Einzel-Anmeldedaten (z.B. ein Token) oder paarweise Anmeldedaten (z.B. aus Benutzernamen und Kennwort) verwenden.

6. [Nur für Skripte, die Argumente erfordern] Spezifizieren Sie die Argumente und deren Werte auf folgende Weise:
   a. Klicken Sie auf **Hinzufügen**.
   b. Spezifizieren Sie das Argument im Feld **Argumente hinzufügen**.
   c. Klicken Sie auf **Hinzufügen**.
   d. Spezifizieren Sie den Argumentwert im zweiten Feld, das angezeigt wird.

   Hinweis
   Sie können nur Argumente spezifizieren, die Sie bereits im Skript-Textkörper definiert haben.

   Beispiel:

   e. Wiederholen Sie die oberen Schritte, wenn Sie mehr als ein Argument hinzufügen wollen.
7. Klicken Sie auf **Speichern**.

Das Skript wird in Ihrem Repository mit dem Status **Entwurf** gespeichert.

Sie können das Skript solange nicht verwenden, bis ein Administrator mit der **Cyber-Administrator**-Rolle dessen Status auf **Genehmigt** ändert. Weitere Informationen dazu finden Sie unter "Den Skript-Status ändern" (S. 266).

Um ein Skript in einem anderen von Ihnen verwalteten Mandanten zu verwenden, müssen Sie das Skript zu diesem Mandanten klonen. Weitere Informationen finden Sie unter "Ein Skript klonen" (S. 264).

Ein Skript mithilfe von KI (erstellen

Hinweis
Für diese Funktionalität ist das Advanced Management-Paket erforderlich.

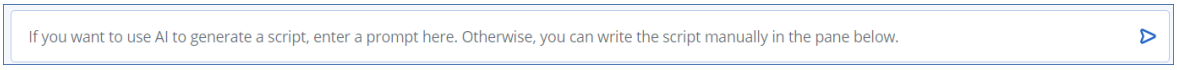
Können Sie Künstliche Intelligenz (KI) einzusetzen, um entsprechende Eingabeanforderungen (Prompts) in leistungsstarke Skripte zu verwandeln. Das kann Ihnen viel Zeit und Mühe ersparen. Sie können die Funktionalität folgendermaßen nutzen:

- Geben Sie einen Prompt ein, um die KI anzuweisen, ein komplett neues Skript zu erstellen.
- Geben Sie einem Prompt ein, um die KI anzuweisen, einen Code zu überprüfen und zu vervollständigen, den Sie im Skript-Body (Haupttext) eingegeben haben. Sie können diese KI-Fähigkeit einsetzen, wenn Sie sich mit komplexeren Skript-Codes herumschlagen.

Diese Funktionalität verwendet das GPT-4-Modell von OpenAI. Sie können diesen einsetzen, um kostenlos bis zu 100 Skripte pro Kalendermonat für Ihre Organisation erstellen zu lassen.

So können Sie ein Skript mithilfe von KI erstellen lassen

1. Gehen Sie in der Cyber Protect-Konsole zum Bereich **Verwaltung** –> **Skript-Repository**.
2. Klicken Sie bei **Meine Skripte** auf **Ein Skript mithilfe von KI erstellen**.
3. Geben Sie im Prompt eine Beschreibung ein, was das Skript tun sollte. Stellen Sie sicher, dass die von Ihnen eingegebene Beschreibung möglichst klar und ausführlich ist.

   Beispiel:

   ```
   I need a script that deletes Temporary files for all users (including user profiles +
   Windows Temps) and disable Windows Update Service to allow the script to run
   ```

4. Klicken Sie im Prompt auf die Pfeiltaste.
5. Wählen Sie im Bestätigungsfenster die Sprache sowie das Betriebssystem aus und klicken dann auf **Generieren**.
   Das per KI generierte Skript wird im Hauptfensterbereich angezeigt. Der Name und die Beschreibung des Skripts werden automatisch von der KI so generiert, dass sie zum Skript passen. Außerdem wird dem Skript die Kennzeichnung **KI-generiert** zugewiesen.
6. Überprüfen Sie das KI-generierte Skript und bearbeiten Sie es bei Bedarf manuell.
7. Bearbeiten Sie bei Bedarf die Skript-Einstellungen.

Einstellung	Beschreibung
Skript-Name	Skriptname. Das Feld wird automatisch ausgefüllt, aber Sie können den Wert ändern.
Beschreibung	Skript-Beschreibung. Diese Einstellung ist optional.

Einstellung	Beschreibung
	[Bei per KI generierten Skripten] Das Feld wird automatisch bei der Erstellung des Skripts ausgefüllt. Sie können die von der KI bereitgestellte Beschreibung bearbeiten.
Sprache	Skript-Sprache. Die verfügbaren Werte sind: • **PowerShell**. Dies ist der Standardwert. • **Bash** [Bei per KI generierten Skripten] Diese Einstellung wird konfiguriert, bevor das Skript generiert wird.
Betriebssystem	Das Betriebssystem, das auf dem Ziel-Workload installiert ist, auf dem das Skript ausgeführt wird. Die verfügbaren Werte sind: • **Windows** . Dies ist der Standardwert. • **macOS** [Bei per KI generierten Skripten] Diese Einstellung wird konfiguriert, bevor das Skript generiert wird.
Status	Skript-Status. • **Entwurf**. Dies ist der Standardwert. Die neuen Skripte, die Sie erstellen, sowie die Skripte, die Sie in Ihr Repository klonen, befinden sich im Status **Entwurf**. Ihnen fehlen die Berechtigungen, Skripte mit dem Status **Entwurf** auszuführen oder diese in Skripting-Pläne einzubeziehen. • **Wird getestet**. Nur Administratoren mit der Rolle **Cyber-Administrator** können den Status eines Skripts zu **Wird getestet** ändern, Skripte mit dem Status **Wird getestet** ausführen oder Skripting-Pläne mit solchen Skripten ausführen. • **Genehmigt**. Sie können Skripte mit dem Status **Genehmigt** ausführen und diese in Skripting-Pläne einbeziehen. Nur Administratoren mit der Rolle des **Cyber-Administrators** können den Status eines Skripts ändern oder ein genehmigtes Skript löschen. Weitere Informationen finden Sie unter "Den Skript-Status ändern" (S. 266).
Tags	Bei Tags wird nicht zwischen Groß- und Kleinschreibung unterschieden und sie können bis zu 32 Zeichen lang sein. Sie dürfen keine runden oder spitzen Klammern, keine Kommata und keine Leerzeichen verwenden. Diese Einstellung ist optional. [Bei per KI generierten Skripten] Das Tag **KI-generiert** wird als Kennzeichnung automatisch bei der Skript-Erstellung hinzugefügt. Sie können dieses Tag manuell löschen oder weitere Tags hinzufügen.

8. [Optional] [Nur für Skripte, die Anmeldedaten erfordern] Spezifizieren Sie die Anmeldedaten.
   Sie können Einzel-Anmeldedaten (z.B. ein Token) oder paarweise Anmeldedaten (z.B. aus Benutzernamen und Kennwort) verwenden.
9. [Nur für Skripte, die Argumente erfordern] Spezifizieren Sie die Argumente und deren Werte auf folgende Weise:

a. Klicken Sie auf **Hinzufügen**.

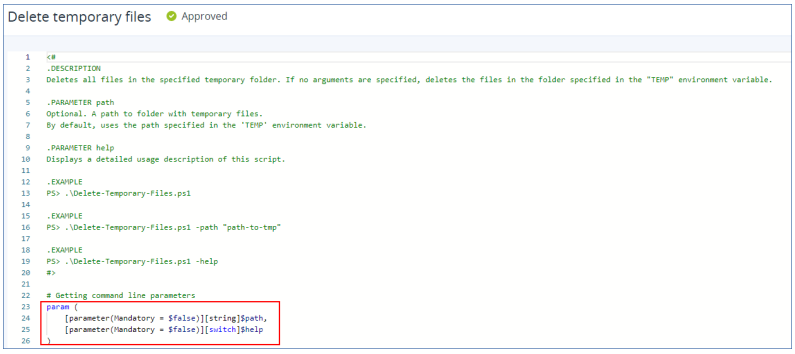
b. Spezifizieren Sie das Argument im Feld **Argumente hinzufügen**.

c. Klicken Sie auf **Hinzufügen**.

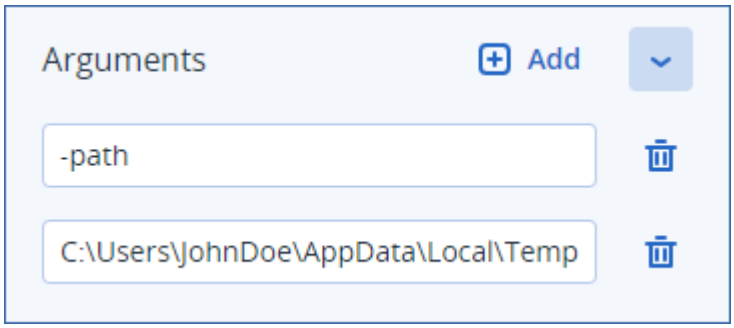
d. Spezifizieren Sie den Argumentwert im zweiten Feld, das angezeigt wird.

Hinweis

Sie können nur Argumente spezifizieren, die Sie bereits im Skript-Textkörper definiert haben.



Beispiel:



e. Wiederholen Sie die oberen Schritte, wenn Sie mehr als ein Argument hinzufügen wollen.

10. Klicken Sie auf **Speichern**.

    Das Skript wird in Ihrem Repository mit dem Status **Entwurf** gespeichert.

    Sie können das Skript solange nicht verwenden, bis ein Administrator mit der **Cyber-Administrator**-Rolle dessen Status auf **Genehmigt** ändert. Weitere Informationen dazu finden Sie unter "Den Skript-Status ändern" (S. 266).

    Um ein Skript in einem anderen von Ihnen verwalteten Mandanten zu verwenden, müssen Sie das Skript zu diesem Mandanten klonen. Weitere Informationen finden Sie unter "Ein Skript klonen" (S. 264).

Ein Skript klonen

Das Klonen eines Skripts ist in folgenden Fällen erforderlich:

- Bevor Sie ein Skript aus der **Bibliothek** verwenden. In diesem Fall müssen Sie zuerst das Skript in den Bereich **Meine Skripte** klonen.

- Wenn Sie Skripte, die Sie in einem übergeordneten Mandanten erstellt haben, zu dessen untergeordnete Mandanten oder Abteilungen klonen wollen.

So können Sie ein Skript klonen

1. Suchen Sie im **Skript-Repository** nach dem Skript, das Sie klonen wollen.
2. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - [Wenn Sie ein Skript aus dem Bereich **Meine Skripte** klonen] Klicken Sie neben dem Skript-Namen auf das Drei-Punkte-Symbol (...) und anschließend auf **Klonen**.
   - [Wenn Sie ein Skript aus **Bibliothek** klonen] Klicken Sie neben dem Namen des Skripts, das Sie ausgewählt haben, auf **Klonen**.
3. Wählen Sie im Pop-up-Fenster **Skript klonen** einen der folgenden Skript-Statuszustände aus dem Listenfeld **Status** aus:
   - **Entwurf** (standardmäßig) – dieser Status erlaubt es Ihnen nicht, das Skript sofort auszuführen.
   - **Wird getestet** – dieser Status erlaubt es Ihnen, das Skript auszuführen.
   - **Genehmigt** – dieser Status erlaubt es Ihnen, das Skript auszuführen.
4. [Wenn Sie mehr als einen Mandanten oder eine Abteilung verwalten] Wählen Sie den Speicherort aus, wohin Sie das Skript klonen wollen.
   Sie sehen im Dialogfenster **Skript klonen** nur diejenigen Mandanten, die Sie verwalten können und für die das Advanced Management-Paket aktiviert wurde.

Dadurch wird das Skript in den Bereich **Meine Skripte** des Mandanten oder der Abteilung geklont, den/die Sie ausgewählt haben. Wenn Sie nur einen Mandanten ohne Abteilungen verwalten, wird das Skript automatisch in Ihren Bereich **Meine Skripte** kopiert.

Wichtig
Wenn in einem Skript Anmeldedaten verwendet werden, werden diese nicht kopiert, wenn Sie ein Skript zu einem Mandanten klonen, der nicht identisch mit dem ursprünglichen Mandanten ist.

Ein Skript bearbeiten oder löschen

Hinweis
In Abhängigkeit von Ihrer Benutzerrolle können Sie verschiedene Aktionen mit Skripten und Skripting-Plänen durchführen. Weitere Informationen zu Benutzerrollen finden Sie unter "Benutzerrollen und Cyber-Skripting-Rechte" (S. 256).

So können Sie ein Skript bearbeiten

1. Gehen Sie im **Skript-Repository** zu **Meine Skripte** und suchen Sie dann das Skript, dessen Versionen Sie vergleichen wollen.
2. Klicken Sie neben dem Skript-Namen auf das Drei-Punkte-Symbol (...) und anschließend auf den Befehl **Bearbeiten**.
3. Bearbeiten Sie das Skript und klicken Sie dann auf **Speichern**.

4. [Wenn Sie ein Skript bearbeiten, das von einem Skripting-Plan verwendet wird] Bestätigen Sie Ihre Wahl, indem Sie auf **Skript speichern** klicken.

Hinweis
Bei der nächsten Ausführung des Skripting-Plans wird die neueste Version des Skripts verwendet.

Skript-Versionen

Eine neue Version des Skripts wird erstellt, wenn Sie eines der folgenden Skript-Attribute bearbeiten:

- Skript-Textkörper
- Skript-Name
- Beschreibung
- Skript-Sprache
- Anmeldedaten
- Argumente

Wenn Sie andere Attribute ändern, werden Ihre Bearbeitungen der aktuellen Skript-Version hinzugefügt. Weitere Informationen über Versionen und wie man diese miteinander vergleichen kann, finden Sie in Abschnitt '"Skript-Versionen vergleichen" (S. 267)'.

Hinweis
Der Skript-Status wird nur aktualisiert, wenn Sie den Wert im Feld **Status** ändern. Nur Administratoren mit der Rolle 'Cyber-Administrator' können den Status eines Skripts ändern.

So können Sie ein Skript löschen

1. Gehen Sie im **Skript-Repository** zu **Meine Skripte** und suchen Sie dann das Skript, das Sie löschen wollen.
2. Klicken Sie neben dem Skript-Namen auf das Drei-Punkte-Symbol (...) und anschließend auf den Befehl **Löschen**.
3. Klicken Sie auf **Löschen**.
4. [Wenn Sie ein Skript löschen wollen, das von einem Skripting-Plan verwendet wird] Bestätigen Sie Ihre Wahl, indem Sie auf **Skript speichern** klicken.

Hinweis
Skripting-Pläne, die das gelöschte Skript verwenden, werden nicht mehr ausgeführt.

Den Skript-Status ändern

Ein neu erstelltes Skript, das sich im Stadium **Entwurf** befindet, kann solange nicht verwendet werden, bis sein Status auf **Genehmigt** geändert wurde. Abhängig vom Anwendungsfall kann sich ein Skript für eine bestimmte Zeit im Status **Wird getestet** befinden, bevor es genehmigt wird.

Hinweis
In Abhängigkeit von Ihrer Benutzerrolle können Sie verschiedene Aktionen mit Skripten und Skripting-Plänen durchführen. Weitere Informationen zu Benutzerrollen finden Sie unter "Benutzerrollen und Cyber-Skripting-Rechte" (S. 256).

Voraussetzungen

- Ihr Benutzer ist ein Administrator, dem die **Cyber-Administrator**-Rolle zugewiesen wurde.
- Es ist ein Skript mit dem entsprechenden Stadium verfügbar.

So können Sie den Status eines Skripts ändern

1. Gehen Sie im **Skript-Repository** zu **Meine Skripte**.
2. Klicken Sie neben dem Skript-Namen auf das Drei-Punkte-Symbol (...) und anschließend auf den Befehl **Bearbeiten**.
3. Wählen Sie im Listenfeld **Status** den entsprechenden Status aus.
4. Klicken Sie auf **Speichern**.
5. [Wenn Sie den Status eines genehmigten Skripts ändern wollen] Klicken Sie auf **Skript speichern**, um die Änderung zu bestätigen.

   Hinweis
   Wenn der Skript-Status auf **Entwurf** herabgestuft wurde, werden die Skripting-Pläne, die das Skript verwenden, nicht mehr ausgeführt.
   Nur Administratoren mit der **Cyber-Administrator**-Rolle können Skripte im Status **Wird getestet** ausführen und Skripting-Pläne mit solchen Skripten durchführen.

Skript-Versionen vergleichen

Sie können zwei Versionen eines Skripts vergleichen und zu einer früheren Version zurückkehren. Sie können auch überprüfen, wer eine bestimmte Version erstellt hat und wann.

So können Sie Skripting-Versionen vergleichen

1. Gehen Sie im **Skript-Repository** zu **Meine Skripte** und suchen Sie dann das Skript, dessen Versionen Sie vergleichen wollen.
2. Klicken Sie neben dem Skript-Namen auf das Drei-Punkte-Symbol (...) und anschließend auf **Versionsverlauf**.
3. Wählen Sie zwei Versionen, die Sie miteinander vergleichen wollen, und klicken Sie anschließend auf **Versionen vergleichen**.
   Alle Änderungen im Textkörper des Skripts, dessen Argumente oder Anmeldedaten werden hervorgehoben.

So können Sie auf eine frühere Version zurücksetzen

1. Klicken Sie im Fenster **Skript-Versionen vergleichen** auf **Auf diese Version zurücksetzen**.
2. Wählen Sie im Pop-up-Fenster **Auf eine frühere Version zurücksetzen** im Listenfeld **Status** den entsprechenden Skript-Status aus.

Die ausgewählte Version wird wiederhergestellt und als neueste Version im Versionsverlauf gespeichert.

Wenn Sie ein bestimmtes Skript wiederherstellen wollen, können Sie auch eine Version aus dem Fenster **Versionsverlauf** auswählen und dann auf die Schaltfläche **Wiederherstellen** klicken.

Wichtig
Sie können nur Skripte mit den Statuszuständen **Wird getestet** oder **Genehmigt** ausführen. Für weitere Informationen finden Sie unter "Den Skript-Status ändern" (S. 266).

Die Ausgabe einer Skripting-Aktion herunterladen

Sie können die Ausgabe einer Skripting-Aktion als .zip-Datei herunterladen. Es enthält zwei Textdateien: `stdout` und `stderr` In `stdout` können Sie die Ergebnisse einer erfolgreich abgeschlossenen Skripting-Aktion einsehen. Die Datei `stderr` enthält Informationen über die Fehler, die während der Skripting-Aktion aufgetreten sind.

So können Sie die Ausgabedatei herunterladen

1. Gehen Sie in der Cyber Protect-Konsole zu **Monitoring** –> **Aktivitäten**.
2. Klicken Sie auf die Cyber-Skripting-Aktivität, deren Ausgabe Sie herunterladen wollen.
3. Klicken Sie in der Anzeige **Aktivitätsdetails** auf **Ausgabe herunterladen**.

Skript-Repository

Sie können das Skript-Repository auf der Registerkarte **Verwaltung** finden. Im Repository können Sie die Skripte über ihren Namen und ihre Beschreibung suchen. Sie können auch Filter verwenden oder die Skripte nach Namen oder Status sortieren.

Wenn Sie ein Skript verwalten wollen, klicken Sie neben dessen Namen auf das Drei-Punkte-Symbol (...) und wählen Sie dann die gewünschte Aktion aus. Alternativ können Sie auch auf das Skript klicken und die Schaltflächen auf der sich öffnenden Anzeige verwenden.

Das Skript-Repository enthält folgende Abschnitte:

- **Meine Skripte**
  Hier finden Sie die Skripte, die Sie direkt in Ihrer Umgebung verwenden können. Dies sind die Skripte, die Sie ganz neu erstellt haben, sowie die Skripte, die Sie hierher geklont haben.
  Sie können die Skripte in diesem Abschnitt nach folgenden Kriterien filtern:
  - Tags
  - Status
  - Sprache

- Betriebssystem
- Skript-Besitzer

- **Bibliothek**

  Die Bibliothek enthält vordefinierte Skripte, die Sie in Ihrer Umgebung verwenden können, nachdem Sie diese in den Abschnitt **Meine Skripte** geklont haben. Sie können diese Skripte nur inspizieren und klonen.

  Sie können die Skripte in diesem Abschnitt nach folgenden Kriterien filtern:

  - Tags
  - Sprache
  - Betriebssystem

  Weitere Informationen finden Sie im englischsprachigen Knowlege Base-Artikel Vendor-Approved Scripts (70595).

Skripting-Pläne

Ein Skripting-Plan ermöglicht es Ihnen, ein Skript auf mehreren Workloads auszuführen, die Ausführung eines Skripts zu planen und zusätzliche Einstellungen zu konfigurieren.

Sie können die von Ihnen erstellten Skripting-Pläne sowie die Pläne, die auf Ihre Workloads angewendet werden, unter **Verwaltung** –> **Skripting-Pläne** finden. Hier können Sie überprüfen, wo der Plan ausgeführt wird, wem er gehört und welchen Status er hat.

Eine anklickbare Leiste zeigt folgende farbcodierte Statuszuständen für die Skripting-Pläne an:

- Wird ausgeführt (Blau)
- Wird auf Kompatibilität geprüft (Dunkelgrau)
- Deaktiviert (Hellgrau)
- OK (Grün)
- Kritischer Alarm (Rot)
- Fehler (Orange)
- Warnung (Gelb)

Wenn Sie auf die Leiste klicken, können Sie sehen, welchen Status ein Plan hat und auf wie vielen Workloads dies der Fall ist. Auf jeden Status kann zudem geklickt werden.

In der Registerkarte **Skripting-Pläne** können Sie die Pläne verwalten, indem Sie folgende Aktionen durchführen:

- Ausführen
- Stopp
- Bearbeiten
- Umbenennen

- Deaktivieren
- Aktivieren
- Klonen
- Exportieren. Die Plan-Konfiguration wird im JSON-Format auf die lokale Maschine exportiert.
- Löschen

Die Sichtbarkeit eines Skripting-Plans und die Aktionen, die mit diesem Plan möglich sind, hängen vom Besitzer des Plans sowie von Ihrer Benutzerrolle ab. Firmenadministratoren können beispielsweise nur die Partner-eigenen Skripting-Pläne sehen, die auf ihre Workloads angewendet wurden, und können mit diesen Plänen keine Aktionen durchführen.

Weitere Informationen darüber, wer Skripting-Pläne erstellen und verwalten kann, finden Sie im Abschnitt '"Benutzerrollen und Cyber-Skripting-Rechte" (S. 256)'.

So können Sie einen Skripting-Plan verwalten

1. Gehen Sie in der Cyber Protect-Konsole zum Bereich **Verwaltung** –> **Skripting-Pläne**.
2. Suchen Sie den Plan, den Sie verwalten wollen, und klicken Sie dann neben diesem auf das Drei-Punkte-Symbol (...).
3. Wählen Sie die gewünschte Aktion aus und befolgen Sie dann die angezeigten Anweisungen.

Einen Skripting-Plan erstellen

Sie können einen Skripting-Plan auf folgende Arten erstellen:

- In der Registerkarte **Geräte**:
  Wählen Sie die Workloads aus und erstellen Sie dann für diese einen Skripting-Plan.
- In der Registerkarte **Verwaltung** –> **Skripting Pläne**
  Erstellen Sie einen Skripting-Plan und wählen Sie dann die Workloads aus, auf die der Plan angewendet werden soll.

So können Sie einen Skripting-Plan auf der Registerkarte 'Geräte' erstellen

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte** –> **Maschinen mit Agenten**.
2. Wählen Sie die Workloads oder die Gerätegruppen, auf die Sie einen Skripting-Plan anwenden wollen, und klicken Sie dann auf **Schützen** oder **Gruppe schützen**.
3. [Wenn es bereits angewendete Pläne gibt] Klicken Sie auf **Plan hinzufügen**.
4. Klicken Sie auf **Plan erstellen** –> **Skripting-Plan**.
   Es wird eine Vorlage für den Skripting-Plan geöffnet.
5. [Optional] Wenn Sie den Namen des Skripting-Plans ändern wollen, klicken Sie auf das Stiftsymbol.
6. Klicken Sie auf **Skript auswählen**, wählen Sie dann das gewünschte Skript und klicken Sie anschließend auf **Fertig**.

Hinweis
Sie können nur Ihre genehmigten Skripte aus dem **Skript-Repository** > **Meine Skripte** verwenden. Nur ein Administrator mit der Rolle **Cyber-Administrator** kann Skripte im Status **Wird getestet** verwenden. Weitere Informationen über diese Rollen finden Sie im Abschnitt "Benutzerrollen und Cyber-Skripting-Rechte" (S. 256).

7. Konfigurieren Sie die Planung und Startbedingungen für den Skripting-Plan.
8. Wählen Sie, unter welchem Konto das Skript auf dem Ziel-Workload ausgeführt werden soll. Folgende Optionen sind verfügbar:
   - Systemkonto (unter macOS ist dies das root-Konto)
   - Derzeit angemeldetes Konto
9. Spezifizieren Sie, wie lange das Skript auf dem Ziel-Workload ausgeführt werden kann.
   Wenn das Skript nicht innerhalb des festgelegten Zeitfensters ausgeführt werden kann, wird die Cyber Scripting-Aktion fehlschlagen.
   Der kleinste Wert, den Sie spezifizieren können, ist eine (1) Minute, der größte ist 1440 Minuten.
10. [Nur für PowerShell-Skripte] Konfigurieren Sie die PowerShell-Ausführungsrichtlinie.
    Weitere Informationen zu dieser Richtlinie finden Sie in der Microsoft-Dokumentation.
11. Klicken Sie auf **Erstellen**.

So können Sie einen Skripting-Plan auf der Registerkarte 'Skripting-Pläne' erstellen

1. Gehen Sie in der Cyber Protect-Konsole zum Bereich **Verwaltung** –> **Skripting-Pläne**.
2. Klicken Sie auf **Plan erstellen**.
   Es wird eine Vorlage für den Skripting-Plan geöffnet.
3. [Optional] Wenn Sie die Workloads oder Gerätegruppen auswählen wollen, auf die der neue Plan angewendet werden soll, klicken Sie auf **Workloads hinzufügen**.
   a. Klicken Sie auf **Maschinen mit Agenten**, um die Liste zu erweitern, und wählen Sie dann die gewünschten Workloads bzw. Gerätegruppen aus.
   b. Klicken Sie auf **Hinzufügen**.

   Weitere Informationen über das Erstellen von Gerätegruppen auf Partnerebene finden Sie im Abschnitt '"Die Registerkarte 'Geräte'" (S. 353)'.

Hinweis
Sie können die Workloads oder Gerätegruppen auch noch auswählen, nachdem Sie den Plan erstellt haben.

4. [Optional] Wenn Sie den Namen des Skripting-Plans ändern wollen, klicken Sie auf das Stiftsymbol.
5. Klicken Sie auf **Skript auswählen**, wählen Sie dann das gewünschte Skript und klicken Sie anschließend auf **Fertig**.

Hinweis
Sie können nur Ihre genehmigten Skripte aus dem **Skript-Repository** > **Meine Skripte** verwenden. Nur ein Administrator mit der Rolle **Cyber-Administrator** kann Skripte im Status **Wird getestet** verwenden. Weitere Informationen über diese Rollen finden Sie im Abschnitt "Benutzerrollen und Cyber-Skripting-Rechte" (S. 256).

6. Konfigurieren Sie die Planung und Startbedingungen für den Skripting-Plan.
7. Wählen Sie, unter welchem Konto das Skript auf dem Ziel-Workload ausgeführt werden soll. Folgende Optionen sind verfügbar:
   - Systemkonto (unter macOS ist dies das root-Konto)
   - Derzeit angemeldetes Konto
8. Spezifizieren Sie, wie lange das Skript auf dem Ziel-Workload ausgeführt werden kann.
   Wenn das Skript nicht innerhalb des festgelegten Zeitfensters ausgeführt werden kann, wird die Cyber Scripting-Aktion fehlschlagen.
   Der kleinste Wert, den Sie spezifizieren können, ist eine (1) Minute, der größte ist 1440 Minuten.
9. [Nur für PowerShell-Skripte] Konfigurieren Sie die PowerShell-Ausführungsrichtlinie.
   Weitere Informationen zu dieser Richtlinie finden Sie in der Microsoft-Dokumentation.
10. Klicken Sie auf **Erstellen**.

Planung und Startbedingungen

Planung

Sie können einen Skripting-Plan so konfigurieren, dass er nur einmalig oder mehrfach ausgeführt wird, nach einem Zeitplan gestartet wird oder durch ein bestimmtes Ereignis ausgelöst wird.

Folgende Optionen sind verfügbar:

- Einmalige Ausführung
  Für diese Option müssen Sie das Datum und den Zeitpunkt konfigurieren, zu dem der Plan ausgeführt werden soll.
- Planung nach Zeit
  Mit dieser Option können Sie Skripting-Pläne konfigurieren, die stündlich, täglich oder monatlich ausgeführt werden sollen.
  Wenn Sie wollen, dass die Planung nur zu bestimmten Zeiten wirksam ist, aktivieren Sie das Kontrollkästchen **Innerhalb eines Zeitraums ausführen** und konfigurieren Sie dann die Zeitspanne, innerhalb derer die Planung ausgeführt werden soll.
- Wenn sich ein Benutzer am System anmeldet
  Sie können bestimmen, ob nur ein bestimmter Benutzer oder jeder Benutzer, der sich anmeldet, den Skripting-Plan auslöst.
- Wenn sich ein Benutzer vom System abmeldet

Sie können bestimmen, ob nur ein bestimmter Benutzer oder jeder Benutzer, der sich abmeldet, den Skripting-Plan auslöst.

- Beim Systemstart
- Wenn das System heruntergefahren wird

Hinweis
Diese Planungsoption funktioniert nur mit Skripten, die unter dem Systemkonto ausgeführt werden.

- Wenn das System online geht

Startbedingungen

Die Startbedingungen bieten Ihnen mehr Flexibilität bei der Planung. Wenn Sie mehrere Bedingungen konfigurieren, müssen diese alle gleichzeitig erfüllt sein, damit der Plan gestartet wird.

Startbedingungen sind nicht wirksam, wenn Sie den Plan manuell ausführen, indem Sie die Option **Jetzt ausführen** verwenden.

Bedingung	Beschreibung
Nur ausführen, wenn der Workload online ist	Das Skript wird ausgeführt, wenn der Ziel-Workload eine Internetverbindung hat.
Benutzer ist inaktiv	Diese Bedingung ist erfüllt, wenn auf der Maschine ein Bildschirmschoner angezeigt wird oder die Maschine gesperrt ist.
Benutzer ist abgemeldet	Mit dieser Bedingung können Sie einen geplanten Skripting-Plan verschieben, bis sich der Benutzer des Ziel-Workloads abmeldet.
Entspricht Zeitintervall	Mit dieser Bedingung kann ein Skripting-Plan nur innerhalb des spezifizierten Zeitintervalls starten. Sie können diese Bedingung beispielsweise verwenden, um die Bedingung **Benutzer ist abgemeldet** einzuschränken.
Akkubelastung senken	Mit dieser Bedingung können Sie sicherstellen, dass der Skripting-Plan nicht unterbrochen wird, weil die Maschine einen niedrigen Akkustand hat. Folgende Optionen sind verfügbar: • Nicht starten, wenn im Akkubetrieb Der Plan wird nur gestartet, wenn die Maschine mit einer externen Stromquelle verbunden ist. • Im Akkubetrieb starten, wenn Akkustand höher ist als Der Plan wird gestartet, wenn die Maschine mit einer externen Stromquelle verbunden ist oder der Akkustand über dem spezifizierten Wert liegt.
Nicht starten, wenn eine getaktete Verbindung besteht	Diese Bedingung verhindert, dass der Plan gestartet wird, wenn der Ziel-Workload über eine gebührenpflichtige Verbindung auf das Internet zugreift.

Bedingung	Beschreibung
Nicht starten, wenn eine Verbindung mit folgenden WLANs besteht	Diese Bedingung verhindert, dass der Plan gestartet wird, wenn der Ziel-Workload mit einem der spezifizierten WLANs verbunden ist. Wenn Sie diese Bedingung verwenden wollen, müssen Sie die SSID des verbotenen WLANs spezifizieren. Die Sperre gilt für alle Netzwerke, die den angegebenen Namen als Teilzeichenfolge in ihrer SSID enthalten (unabhängig von Groß-/Kleinschreibung). Beispiel: wenn Sie `phone` als Netzwerkname spezifizieren, wird der Plan nicht gestartet, wenn das Gerät mit einem WLAN mit einer der folgenden SSIDs verbunden ist: `Johns iPhone`, `phone_wlan` oder `mein_PHONE_wlan`.
IP-Adresse des Gerätes überprüfen	Diese Bedingung verhindert, dass der Plan gestartet wird, wenn eine der IP-Adressen des Ziel-Workloads innerhalb oder außerhalb des spezifizierten IP-Adressbereichs liegt. Folgende Optionen sind verfügbar: • Starten, wenn außerhalb des IP-Bereichs • Starten, wenn innerhalb des IP-Bereichs Es werden nur IPv4-Adressen unterstützt.
Wenn die Startbedingungen nicht erfüllt sind, Task trotzdem ausführen	Mit dieser Option können Sie das Zeitintervall festlegen, nach dem der Plan ausgeführt wird, ungeachtet aller anderen Bedingungen. Der Plan beginnt, sobald die anderen Bedingungen erfüllt sind oder der spezifizierte Zeitraum endet – je nachdem, welche Bedingung zuerst eintritt. Diese Option ist nicht verfügbar, wenn Sie den Skripting-Plan so konfiguriert haben, dass er nur einmal ausgeführt wird.

Die Ziel-Workloads für einen Plan verwalten

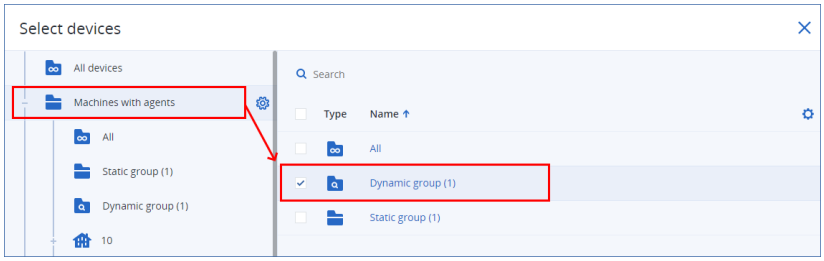
Sie können die Workloads oder Gerätegruppen, auf die ein Skripting-Plan angewendet werden soll, direkt während der Plan-Erstellung auswählen oder zu einem späteren Zeitpunkt.

Partner-Administratoren können denselben Plan auf die Workloads von verschiedenen Kunden anwenden und zudem Gerätegruppen erstellen, die Workloads von verschiedenen Kunden enthalten. Wie Sie eine statische oder dynamische Gerätegruppe auf Partnerebene erstellen können, erfahren Sie im Abschnitt '"Die Registerkarte 'Geräte'" (S. 353)'.

So können Sie erstmals Workloads zu einem Plan hinzufügen

1. Gehen Sie in der Cyber Protect-Konsole zum Bereich **Verwaltung** –> **Skripting-Pläne**.
2. Klicken Sie auf den Namen des Plans, für den Sie bestimmte Ziel-Workloads spezifizieren wollen.
3. Klicken Sie auf **Workloads hinzufügen**.
4. Wählen Sie die gewünschten Workloads oder Gerätegruppen aus und klicken Sie dann auf **Hinzufügen**.

Hinweis
Wenn Sie eine Gerätegruppe auswählen wollen, klicken Sie zuerst auf deren übergeordnete Ebene und aktivieren Sie dann im Hauptbereich das Kontrollkästchen neben dem Namen der Gruppe.

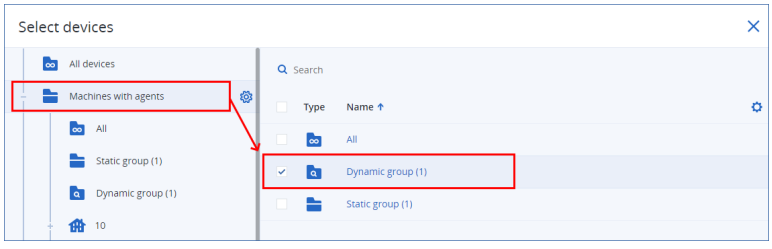


5. Klicken Sie auf **Speichern**, damit der bearbeitete Plan gesichert wird.

So können Sie vorhandene Workloads für einen Plan verwalten

1. Gehen Sie in der Cyber Protect-Konsole zum Bereich **Verwaltung** –> **Skripting-Pläne**.
2. Klicken Sie auf den Namen desjenigen Plans, dessen Ziel-Workloads Sie ändern wollen.
3. Klicken Sie auf **Workloads verwalten**.
   In der Anzeige **Geräte** werden die Workloads aufgelistet, auf die der Skripting-Plan derzeit angewendet wird. Wenn Sie mehr als einen Mandanten verwalten, werden die Workloads nach Mandanten sortiert.
   - Klicken Sie auf **Hinzufügen**, wenn Sie neue Workloads oder Gerätegruppen hinzufügen wollen.
     a. Wählen Sie die gewünschten Workloads oder Gerätegruppen aus. Sie können Workloads von allen Mandanten hinzufügen, die Sie verwalten.

     Hinweis
     Wenn Sie eine Gerätegruppe auswählen wollen, klicken Sie zuerst auf deren übergeordnete Ebene und aktivieren Sie dann im Hauptbereich das Kontrollkästchen neben dem Namen der Gruppe.

     b. Klicken Sie auf **Hinzufügen**.
   - Wenn Sie Workloads oder Gerätegruppen entfernen wollen, müssen Sie diese erst auswählen und dann auf **Entfernen** klicken.
4. Klicken Sie auf **Fertig**.
5. Klicken Sie auf **Speichern**, damit der bearbeitete Plan gesichert wird.

Pläne auf verschiedenen Verwaltungsebenen

Die nachfolgende Tabelle fasst zusammen, welche Pläne von Administratoren verschiedener Ebenen eingesehen und verwaltet werden können.

Administrator	Verwaltungsebene	Pläne	Rechte
Partner-Administrator	Partnerebene	Eigene Pläne	Vollzugriff
		Kundenpläne (einschließlich Pläne in Abteilungen)	Vollzugriff
		Abteilungspläne	Vollzugriff
	Kundenebene (für Kunden, die vom Service Provider verwaltet werden)	Partnerpläne, die auf Workloads dieses Kunden angewendet werden	Nur Lesen
		Kundenpläne (einschließlich Pläne in Abteilungen)	Vollzugriff
		Abteilungspläne	Vollzugriff
	Abteilungsebene (für Kunden, die vom Service Provider verwaltet werden)	Partnerpläne, die auf Workloads dieser Abteilung angewendet werden	Nur Lesen
		Kundenpläne, die auf Workloads dieser Abteilung angewendet werden	Nur Lesen
		Abteilungspläne	Vollzugriff
Firmenadministrator	Kundenebene	Partnerpläne, die auf Workloads dieses Kunden oder dieser Abteilung angewendet werden	Nur Lesen
		Kundenpläne (einschließlich Pläne in Abteilungen)	Vollzugriff
		Abteilungspläne	Vollzugriff
	Abteilungsebene	Partnerpläne, die auf Workloads dieser Abteilung angewendet werden	Nur Lesen
		Kundenpläne, die auf Workloads dieser Abteilung angewendet werden	Nur Lesen
		Abteilungspläne	Vollzugriff
Abteilungsadministrator	Abteilungsebene	Partnerpläne, die auf Workloads	Nur Lesen

Administrator	Verwaltungsebene	Pläne	Rechte
		dieser Abteilung angewendet werden	
		Kundenpläne, die auf Workloads dieser Abteilung angewendet werden	Nur Lesen
		Abteilungspläne	Vollzugriff

Wichtig
Der Besitzer eines Plans ist der Mandant, in dem der Plan erstellt wurde. Wenn daher ein Partner-Administrator einen Plan auf der Kunden-Mandanten-Ebene erstellt hat, ist der Kunden-Mandant der Besitzer dieses Plans.

Kompatibilitätsprobleme mit Skripting-Plänen

In einigen Fällen kann es zu Kompatibilitätsproblemen kommen, wenn Sie einen Skripting-Plan auf einen Workload anwenden. Sie werden möglicherweise folgende Kompatibilitätsprobleme feststellen:

- Inkompatibles Betriebssystem – zu diesem Problem kommt es, wenn das Betriebssystem des Workloads nicht unterstützt wird.
- Nicht unterstützter Agent – zu diesem Problem kommt es, wenn die Version des Protection Agenten auf dem Workload veraltet ist und die Cyber Scripting-Funktionalität nicht unterstützt.
- Unzureichende Quota – zu diesem Problem kommt es, wenn im Mandanten die Service-Quota nicht ausreicht, um sie den ausgewählten Workloads zuweisen zu können.

Wenn der Skripting-Plan auf bis zu 150 persönlich ausgewählte Workloads angewendet wird, werden Sie aufgefordert, die bestehenden Konflikte zu lösen, bevor Sie den Plan speichern. Sie können einen Konflikt auflösen, indem Sie entweder dessen Ursache beseitigen oder indem Sie die betroffenen Workloads aus dem Plan entfernen. Weitere Informationen finden Sie im Abschnitt '"Kompatibilitätsprobleme mit Skripting-Plänen beheben" (S. 277)'. Wenn Sie den Plan speichern, ohne die Konflikte zu lösen, wird er automatisch für die inkompatiblen Workloads deaktiviert und werden entsprechende Alarmmeldungen angezeigt.

Wenn der Skripting-Plan auf mehr als 150 Workloads oder Gerätegruppen angewendet wird, wird der Plan gespeichert und dann auf Kompatibilität überprüft. Der Plan wird automatisch für die nicht unterstützten Workloads deaktiviert und es werden entsprechende Alarmmeldungen angezeigt.

Kompatibilitätsprobleme mit Skripting-Plänen beheben

Je nach Art der Kompatibilitätsprobleme können Sie beim Erstellen eines neuen Skripting-Plans verschiedene Aktionen durchführen, um diese Kompatibilitätsprobleme zu beheben.

Hinweis
Wenn Sie ein Kompatibilitätsproblem beheben wollen, indem Sie Workloads aus einem Plan entfernen, können Sie keine Workloads entfernen, die zu einer Gerätegruppe gehören.

So können Sie die Kompatibilitätsprobleme beheben

1. Klicken Sie auf **Probleme überprüfen**.
2. [So können Sie Kompatibilitätsprobleme mit inkompatiblen Betriebssystemen lösen]
   a. Wählen Sie auf der Registerkarte **Inkompatibles Betriebssystem** diejenigen Workloads aus, die Sie entfernen wollen.
   b. Klicken Sie auf **Workloads aus dem Plan entfernen**.
   c. Klicken Sie zuerst auf **Entfernen** und dann auf **Schließen**.
3. [So können Sie Kompatibilitätsprobleme mit nicht unterstützten Agenten beheben, indem Sie Workloads aus dem Plan entfernen]
   a. Wählen Sie auf der Registerkarte **Nicht unterstützte Agenten** diejenige Workloads aus, die Sie entfernen wollen.
   b. Klicken Sie auf **Workloads aus dem Plan entfernen**.
   c. Klicken Sie zuerst auf **Entfernen** und dann auf **Schließen**.
4. [Wenn Sie Kompatibilitätsprobleme mit nicht unterstützten Agenten durch Aktualisierung der Agenten-Version beheben wollen] Klicken Sie auf **Zur Agenten-Liste gehen**.

   Hinweis
   Diese Option ist nur für Kunden-Administratoren verfügbar.

5. [So können Sie Kompatibilitätsprobleme durch eine unzureichende Quota beheben, indem Sie Workloads aus dem Plan entfernen]
   a. Wählen Sie auf der Registerkarte **Unzureichende Quota** diejenige Workloads aus, die Sie entfernen wollen.
   b. Klicken Sie auf **Workloads aus dem Plan entfernen**.
   c. Klicken Sie zuerst auf **Entfernen** und dann auf **Schließen**.
6. [So können Sie Kompatibilitätsprobleme mit einer unzureichenden Quota lösen, indem Sie die Quota des Mandanten vergrößern]

   Hinweis
   Diese Option ist nur für Partner-Administratoren verfügbar.

   a. Klicken Sie auf der Registerkarte **Unzureichende Quota** auf den Befehl **Zum Management-Portal gehen**.
   b. Vergrößern Sie die Service-Quota für den Kunden.

Schnelle Skript-Ausführung

Sie können ein Skript sofort ausführen, ohne es in einen Skripting-Plan aufzunehmen. Sie können diese Aktion nicht auf mehr als 150 Workloads, auf Offline-Workloads oder auf Gerätegruppen anwenden.

Dem Ziel-Workload muss ein Service-Quota zugewiesen sein, welche die Funktionalität 'Schnelle Skript-Ausführung' unterstützt – und außerdem muss für den entsprechenden Mandanten das Advanced Management-Paket aktiviert sein. Wenn in dem Mandanten eine entsprechende Service-Quota verfügbar ist, wird diese automatisch zugewiesen.

Hinweis
Sie können nur Ihre genehmigten Skripte aus dem **Skript-Repository** > **Meine Skripte** verwenden. Nur ein Administrator mit der Rolle **Cyber-Administrator** kann Skripte im Status **Wird getestet** verwenden. Weitere Informationen über diese Rollen finden Sie im Abschnitt "Benutzerrollen und Cyber-Skripting-Rechte" (S. 256).

Sie können eine schnelle Ausführung auf folgende Arten starten:

- Über die Registerkarte **Geräte**
  Wählen Sie zuerst einen oder mehrere Workloads aus und dann das Skript, welches auf dem/den Workload(s) ausgeführt werden soll.
- Über die Registerkarte **Verwaltung** –> **Skript-Repository**
  Wählen Sie zuerst ein Skript und dann einen oder mehrere Ziel-Workloads aus.

So können Sie ein Skript über die Registerkarte 'Geräte' ausführen

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte** –> **Alle Geräte**.
2. Bestimmen Sie den Workload, auf dem das Skript ausgeführt werden soll, und klicken Sie anschließend auf **Schützen**.
3. Klicken Sie auf **Schnelle Skript-Ausführung**.
4. Klicken Sie auf **Skript auswählen**, wählen Sie dann das gewünschte Skript und klicken Sie anschließend auf **Fertig**.
5. Wählen Sie, unter welchem Konto das Skript auf dem Ziel-Workload ausgeführt werden soll. Folgende Optionen sind verfügbar:
   - Systemkonto (unter macOS ist dies das root-Konto)
   - Derzeit angemeldetes Konto
6. Spezifizieren Sie, wie lange das Skript auf dem Ziel-Workload ausgeführt werden kann.
   Wenn das Skript nicht innerhalb des festgelegten Zeitfensters ausgeführt werden kann, wird die Cyber Scripting-Aktion fehlschlagen.
   Sie können Werte zwischen 1 und 1440 Minuten verwenden.
7. [Nur für PowerShell-Skripte] Konfigurieren Sie die PowerShell-Ausführungsrichtlinie.

Weitere Informationen zu dieser Richtlinie finden Sie in der Microsoft-Dokumentation.

8. Klicken Sie auf **Jetzt ausführen**.

So können Sie ein Skript über die Registerkarte 'Skript-Repository' ausführen

1. Gehen Sie in der Cyber Protect-Konsole zum Bereich **Verwaltung** –> **Skript-Repository**.
2. Wählen Sie das auszuführende Skript aus und klicken Sie dann auf **Schnelle Skript-Ausführung**.
3. Klicken Sie zuerst auf **Workloads hinzufügen**, damit Sie die Ziel-Workloads auswählen können, und anschließend auf **Hinzufügen**.
4. Klicken Sie auf **Skript auswählen**, wählen Sie dann das gewünschte Skript und klicken Sie anschließend auf **Fertig**.
5. Wählen Sie, unter welchem Konto das Skript auf dem Ziel-Workload ausgeführt werden soll. Folgende Optionen sind verfügbar:
   - Systemkonto (unter macOS ist dies das root-Konto)
   - Derzeit angemeldetes Konto
6. Spezifizieren Sie, wie lange das Skript auf dem Ziel-Workload ausgeführt werden kann.
   Wenn das Skript nicht innerhalb des festgelegten Zeitfensters ausgeführt werden kann, wird die Cyber Scripting-Aktion fehlschlagen.
   Sie können Werte zwischen 1 und 1440 Minuten verwenden.
7. [Nur für PowerShell-Skripte] Konfigurieren Sie die PowerShell-Ausführungsrichtlinie.
   Weitere Informationen zu dieser Richtlinie finden Sie in der Microsoft-Dokumentation.
8. Klicken Sie auf **Jetzt ausführen**.

Schutz von Applikationen für Zusammenarbeit und Kommunikation

Zoom, Cisco Webex Meetings, Citrix Workspace und Microsoft Teams werden mittlerweile häufig für Video-/Web-Konferenzen bzw. zur Kommunikation verwendet. Der Cyber Protection Service ermöglicht Ihnen, Ihre Kollaborationstools zu schützen.

Die Schutzkonfigurationen für Zoom, Cisco Webex Meetings, Citrix Workspace und Microsoft Teams sind ähnlich. In dem unteren Beispiel betrachten wir die Konfiguration für Zoom.

So richten Sie die Cyber Protection für Zoom ein

1. Installieren Sie den Protection Agenten auf der Maschine, auf welcher die Kollaborationsapplikation installiert ist.
2. Melden Sie sich an der Cyber Protect-Konsole an und wenden Sie einen Schutzplan an, für den eines der folgenden Module aktiviert ist:
   - **Antivirus & Antimalware Protection** (wo die Einstellungen **Selbstschutz** und and **Active Protection** aktiviert sind) – wenn Sie eine der Cyber Protect-Editionen haben.

- **Active Protection** (wo die Einstellung **Selbstschutz** aktiviert ist) – wenn Sie eine der Cyber Backup-Editionen haben.

3. [Optional] Konfigurieren Sie das Modul **Patch-Verwaltung** im Schutzplan, wenn Sie die automatische Installation von Updates nutzen wollen.

Als Ergebnis wird Ihre Zoom-Applikation geschützt, was folgende Aktivitäten umfasst:

- Zoom-Client-Updates automatisch installieren
- Zoom-Prozesse vor Schadcode-Einschleusung schützen
- Verdächtige Aktionen durch Zoom-Prozesse verhindern
- Die Datei 'hosts' davor schützen, dass Domains hinzugefügt werden, die sich auf Zoom beziehen

Ihre aktuelle Schutzstufe verstehen

Monitoring

Die Registerkarte **Monitoring** stellt wichtige Informationen über Ihre aktuelle Schutzstufe bereit und umfasst folgende Dashboards:

- **Überblick**
- **Aktivitäten**
- **Alarmmeldungen**
- **Bedrohungsfeed** (weitere Informationen finden Sie unter '"Bedrohungsfeed" (S. 331)')

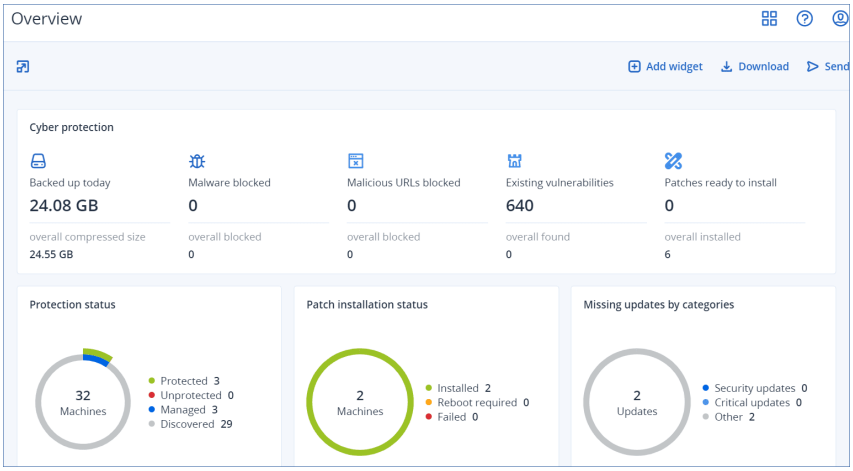
Das Dashboard 'Überblick'

Das Dashboard **Überblick** enthält eine Reihe benutzerdefinierbarer Widgets, die Ihnen einen Überblick über diejenigen Aktionen geben, die im Zusammenhang mit dem Cyber Protection Service stehen. Widgets für andere Services werden in zukünftigen Versionen verfügbar sein.

Die Widgets werden alle fünf Minuten aktualisiert. Die Widgets haben anklickbare Elemente, über die Sie Probleme untersuchen und beheben können. Sie können den aktuellen Zustand des Dashboards in Form einer .pdf- und/oder .xlsx-Datei herunterladen oder als E-Mail versenden.

Sie können aus einer Vielzahl von Widgets wählen, die als Tabellen, Torten- und Balkendiagramme, Listen und Treemaps (Kacheldiagramm mit Baumstruktur) angezeigt werden. Sie können mehrere Widgets desselben Typs hinzufügen, die aber unterschiedliche Filter verwenden.

Die Schaltflächen **Download** und **Senden** in **Monitoring** –> **Überblick** sind in den Standard-Editionen von Cyber Protection Service nicht verfügbar.



So können Sie die Widgets auf dem Dashboard neu anordnen

Verschieben Sie die Widgets per Drag & Drop-Aktion, indem Sie zuvor auf deren Namen klicken.

So können Sie ein Widget bearbeiten

Klicken Sie neben dem Widget-Namen auf das Stiftsymbol. Mit der Funktion 'Bearbeiten' können Sie ein Widget umbenennen, den Zeitraum ändern, Filter festlegen und Zeilen gruppieren.

So können Sie ein Widget hinzufügen

Klicken Sie auf **Widget hinzufügen** und gehen Sie dann nach einer der folgenden Möglichkeiten vor:

- Klicken Sie auf das hinzuzufügende Widget. Das Widget wird daraufhin mit den Standardeinstellungen hinzugefügt.
- Wenn Sie das Widget vor dem Hinzufügen bearbeiten wollen, dann klicken Sie nach der Auswahl des Widgets auf den Befehl Anpassen. Klicken Sie, nachdem Sie das Widget bearbeitet haben, auf **Fertig**.

So können Sie ein Widget entfernen

Klicken Sie neben dem Widget-Namen auf das X-Symbol.

Das Dashboard 'Aktivitäten'

Das Dashboard **Aktivitäten** bietet einen Überblick über aktuelle und zurückliegende Aktivitäten. Die vorgegebene Aufbewahrungsdauer beträgt 90 Tage.

Wenn Sie die Darstellung des Dashboards **Aktivitäten** anpassen wollen, können Sie auf das Zahnradsymbol klicken und dann die Spalten auswählen, die angezeigt werden sollen.

Wenn Sie den Aktivitätsfortschritt in Echtzeit sehen wollen, aktivieren Sie das Kontrollkästchen **Automatisch aktualisieren**. Eine häufige Aktualisierung mehrerer Aktivitäten kann jedoch die Performance des Management Servers herabsetzen.

Sie können die aufgelisteten Aktivitäten nach den folgenden Kriterien durchsuchen:

- **Gerätename**
  Dies ist die Maschine, auf welcher die Aktivität ausgeführt wird.
- **Gestartet von**
  Dies ist das Konto, welches die Aktivität gestartet hat.

Sie können die Aktivitäten auch nach folgenden Eigenschaften filtern:

- **Status**
  Zum Beispiel: erfolgreich, fehlgeschlagen, wird ausgeführt, abgebrochen.
- **Typ**
  Zum Beispiel: Plan anwenden, Backups löschen, Software-Updates installieren.
- **Zeit**
  Zum Beispiel: die jüngsten Aktivitäten, die Aktivitäten der letzten 24 Stunden oder die Aktivitäten während eines bestimmten Zeitraums innerhalb der vorgegebenen Aufbewahrungsdauer.

Wenn Sie weitere Details zu einer Aktivität einsehen wollen, wählen Sie zuerst diese Aktivität in der Liste aus und klicken Sie dann im Bereich **Aktivitätsdetails** auf **Alle Eigenschaften**. Weitere

Informationen zu den verfügbaren Eigenschaften finden Sie in den API-Referenzen Aktivität und Task im Developer Network Portal.

Das Dashboard 'Alarmmeldungen'

Auf dem Dashboard **Alarmmeldungen** werden alle Alarmmeldungen angezeigt, die Sie aktuell haben. Es werden entweder kritische Alarmmeldungen oder Fehlermeldungen aufgelistet. Diese beziehen sich in der Regel auf Tasks (wie etwa Backups), die aus irgendeinem Grund fehlgeschlagen sind.

So können Sie Alarmmeldungen auf dem Dashboard filtern

1. Wählen Sie im Listenfeld **Ansicht** eines der folgenden Kriterien aus:
   - **Alarmschweregrad**
   - **Alarmkategorie**
   - **Alarmtyp**
   - **Monitoring-Typ**
   - **Datumsbereich: von... bis ...**
   - **Workload**
   - **Plan**
   - **Kunde**
2. Wenn Sie die **Alarmkategorie** bestimmt haben, dann wählen Sie im Listenfeld **Kategorie** diejenige Kategorie der Alarmmeldungen aus, die Sie sehen wollen.
3. Wenn Sie ungefiltert alle Alarmmeldungen sehen wollen, klicken Sie auf **Alle Alarmtypen**.

Innerhalb eines Alarms können Sie Folgendes tun:

- Auf das entsprechende Gerät zugreifen, auf das sich der Alarm bezieht, indem Sie auf den Link **Geräte** klicken.
- Lesen Sie die Hinweise im Bereich **Problembehebung (Troubleshooting)** des Alarms und versuchen Sie, diese zu befolgen.
- Lesen Sie die entsprechende Dokumentation und den Knowledge Base-Artikel durch, indem Sie auf den Link **Nach Lösung suchen** klicken. Die Funktionalität **Nach Lösung suchen** wird Ihre Anfrage mit den aktuellen Details aus dem Alarm vorausfüllen, um Sie bestmöglich zu unterstützen.

So können Sie Alarmmeldungen auf dem Dashboard sortieren

Klicken Sie in der Tabelle der Alarmmeldungen neben einem der folgenden Spaltennamen auf die Pfeilschaltfläche:

- **Alarmschweregrad**
- **Alarmtyp**
- **Erstellt**

- **Alarmkategorie**
- **Workload**
- **Plan**

Wenn der Advanced Automation Service für Ihr Konto aktiviert wurde, können Sie zudem direkt aus den Alarmmeldungen heraus ein neues Service Desk-Ticket erstellen.

So können Sie ein Service Desk-Ticket erstellen

1. Klicken Sie in der entsprechenden Alarmmeldung auf **Ein neues Ticket erstellen**.
   Alternativ, wenn Sie in der Tabellenansicht arbeiten, können Sie eine Alarmmeldung auswählen und dann im rechten Fensterbereich den Befehl **Ein neues Ticket erstellen** auswählen.
2. Definieren Sie Folgendes:
   - Aktivieren Sie im Kopfbereich das Kontrollkästchen **Abrechenbar**, wenn Sie wollen, dass die auf dem Ticket erfasste Zeit dem Kunden in Rechnung gestellt wird. Außerdem können Sie das Kontrollkästchen **E-Mail an den Kunden senden** aktivieren, wenn Sie Ticket-Aktualisierungen an den Kunden schicken wollen.
   - Definieren Sie im Bereich **Allgemeine Informationen** einen Titel für das Ticket. Dieses Feld wird standardmäßig mit einer Zusammenfassung für die Alarmmeldung ausgefüllt, die Sie aber bearbeiten können.
   - Die Felder im Bereich **Kundeninformationen** werden mit den relevanten Informationen aus der Alarmmeldung vorausgefüllt.
   - Die Felder im Bereich **Konfigurationselement oder Service** werden mit Informationen zu dem Gerät vorausgefüllt, das mit dem Alarm verknüpft ist. Sie können ein Gerät bei Bedarf neu zuweisen.
   - Im Abschnitt **Support-Agent** werden die Felder mit dem standardmäßigen Support-Agenten, der Kategorie und der Support-Gruppe vorausgefüllt. Sie können bei Bedarf auch einen anderen Agenten zuweisen.
   - Die Felder im Bereich **Ticket-Aktualisierung** werden mit den Beschreibungen und Details der entsprechenden Alarmmeldung vorausgefüllt. Das Feld **Status** wird standardmäßig auf **Neu** festgelegt – was aber geändert werden kann.
   - Fügen Sie in den Bereichen **Anhänge**, **Abrechenbare Elemente** und **Interne Notizen** je nach Bedarf passende Elemente hinzu.
3. Klicken Sie auf **Fertig**. Wenn das Ticket erstellt wurde, wird in der Alarmmeldung ein Link auf das Ticket hinzufügt.
   Wenn eine Alarmmeldung geschlossen wird, wird auch das dazugehörige Ticket automatisch geschlossen.

Hinweis
Sie können nur ein Ticket pro Alarmmeldung erstellen.

Alarmtypen

Für folgende Alarmtypen werden Alarmmeldungen generiert:

- Backup-Alarmmeldungen
- Disaster Recovery-Alarmmeldungen
- Antimalware Protection-Alarmmeldungen
- Lizenzierungsalarmmeldungen
- URL-Filter-Alarmmeldungen
- EDR-Alarmmeldungen
- Gerätekontrolle-Alarmmeldungen
- System-Alarmmeldungen

Backup-Alarmmeldungen

Alarm	Beschreibung	So können Sie den Alarm auflösen
Backup ist fehlgeschlagen	Es wird ein Alarm generiert, wenn das Backup während der Ausführung mit einem behebbaren Problem fehlgeschlagen ist oder es abgebrochen wurde, weil das System heruntergefahren wurde.	Überprüfen Sie das Protokoll der fehlerhaften Backup-Aktion: Klicken Sie zuerst auf den Workload, um diesen auszuwählen, und anschließend auf **Aktivitäten**, um die Warnung im Protokoll zu finden. Die Meldung sollte Sie zur Ursache des Problems führen, über das Sie von der Software alarmiert wurden.
Backup mit Warnungen abgeschlossen	Es wird ein Alarm generiert, wenn das Backup zwar erfolgreich, aber mit Warnungen abgeschlossen wurde.	Überprüfen Sie die Protokolle für die Konvertierung zu VM-, Replikations- oder Validierungspläne. Probleme, die bei diesen Aktionen auftreten, generieren Alarmmeldungen vom Typ 'Aktivität fehlgeschlagen' oder 'Die Aktivität wurde mit einer Warnung beendet'.
Backup wurde abgebrochen	Es wird jedes Mal ein Alarm generiert, wenn der Benutzer eine Backup-Aktivität manuell abbricht.	Sie können das Backup entweder manuell starten, indem Sie auf 'Jetzt ausführen' klicken – oder darauf warten, bis es am nächsten geplanten Zeitpunkt ausgeführt wird.
Das Backup wurde abgebrochen, weil das Backup-Fenster geschlossen wurde	Es wird ein Alarm generiert, wenn die Backup-Aktivität verpasst wurde, weil sie nicht	Konfigurieren Sie die Planung neu oder bearbeiten Sie die Optionen des Backup-Plans im Fenster

Alarm	Beschreibung	So können Sie den Alarm auflösen
	in das Zeitfenster passte, das in den Backup-Optionen spezifiziert wurde.	**Performance und Backup**. Erweitern Sie den Bereich mit Ihrem Produkt, um Anweisungen zu erhalten.
Backup befindet sich in Wartestellung	Dieser Alarm wird jedes Mal generiert, wenn es einen Planungskonflikt gibt, weil zwei Backup-Tasks zur gleichen Zeit gestartet wurden. In diesem Fall wird der zweite Backup-Task in die Warteschlange gestellt, bis der erste fertiggestellt oder gestoppt wurde.	Stellen Sie sicher, dass Ihre Backups in den erwarteten Zeitfenstern und gemäß ihrer Planung ausgeführt werden, und vermeiden Sie möglichst jeden Planungskonflikt.
Backup antwortet nicht mehr	Es wird ein Alarm generiert, wenn das gerade laufende Backup seit einiger Zeit keinen Fortschritt mehr gemeldet hat und möglicherweise eingefroren ist.	Das Problem kann durch einen Programmhänger verursacht werden. Befolgen Sie die Anweisungen in diesem Artikel, um die notwendigen Troubleshooting-Informationen zu sammeln.
Backup wurde nicht gestartet	Es wird ein Alarm generiert, wenn das geplante Backup aus unbekannten Gründen fehlgeschlagen ist.	Stellen Sie sicher, dass Sie die aktuellste Version Ihres Acronis Backup-Produkts verwenden. • Wenn die Maschine des Agenten zum Zeitpunkt des Backup-Starts verfügbar war: 1. Bearbeiten Sie die Startzeit des Backup Tasks. 2. Sollte der Alarm erneut auftreten, sollten Sie den Backup-Task ganz neu erstellen. 3. Wenn auch der neu erstellte Backup-Task wieder den Alarm auslöst, kontaktieren Sie den Acronis Support, um weitere Unterstützung zu erhalten. • Wenn der Agent offline war: 1. Schalten Sie die Maschine nicht während der Backup-Zeit aus.

Alarm	Beschreibung	So können Sie den Alarm auflösen
		2. Wenn die Maschine nicht ausgeschaltet war, stellen Sie sicher, dass der Dienst 'Acronis Managed Machine Service' ausgeführt wird: Suchen Sie den Acronis Managed Machine Service mithilfe der Befehlskette Start –> Suchen –> services.msc. Kontaktieren Sie den Acronis Support, wenn Sie weitere Hilfe benötigen.
Backup-Status ist unbekannt	es wird ein Alarm generiert, wenn der Backup Agent an einem geplanten Backup-Zeitpunkt offline war. Der Status der Ressourcen-Backups ist solange unbekannt, bis der Backup-Agent wieder online ist.	1. Überprüfen Sie, ob es nicht unerwartet ist, dass der Agent offline ist (z.B. weil es sich um ein Notebook handelt, das sich außerhalb des Management Server-Netzwerks befindet). 2. Wenn der Agent nicht offline sein sollte, stellen Sie sicher, dass der Dienst 'Acronis Managed Machine Service' ausgeführt wird: Suchen Sie den Acronis Managed Machine Service mithilfe der Befehlskette Start –> Suchen –> services.msc und überprüfen Sie dessen Status. Sollte der Dienst gestoppt sein, dann starten Sie ihn wieder.
Backup fehlt	Es wird ein Alarm generiert, wenn seit mehr als [Tage seit dem letzten Backup] Tagen kein erfolgreiches Backup mehr durchgeführt wurde.	
Backup ist beschädigt	Es wird ein Alarm generiert, wenn die Validierungsaktivität abgeschlossen wurde und zeigt, dass das Backup beschädigt ist.	Befolgen Sie die Anweisungen im Artikel Probleme mit beschädigten Backups beheben. Wenn Sie Hilfe benötigen, um die grundlegende Ursache für die Archivbeschädigung zu ermitteln, wenden Sie sich an den Acronis Support.

Alarm	Beschreibung	So können Sie den Alarm auflösen
Die kontinuierliche Datensicherung (CDP) ist fehlgeschlagen	Es wird ein Alarm generiert, wenn die kontinuierliche Datensicherung (CDP) fehlgeschlagen ist.	Überprüfen Sie folgende Einschränkungen: 1. Die kontinuierliche Datensicherung wird nur für das Dateisystem NTFS und folgende Betriebssysteme unterstützt: • Desktop: Windows 7 und höher • Server: Windows Server 2008 R2 und höher 2. Die **Acronis Secure Zone** kann nicht als Ziel für die kontinuierlichen Datensicherung (CDP) verwendet werden. 3. NFS-Ordner, die unter Windows gemountet sind, werden nicht unterstützt. 4. Es wird keine kontinuierliche Replikation unterstützt: Wenn es im Schutzplan zwei Standorte gibt, werden nur im ersten Backup-Ziel CDP-Slices erstellt. Die Änderungen werden dann mit dem nächsten Backup zum zweiten Ziel repliziert. 5. Wenn Änderungen in einem geschützten lokalen Ordner von einer Netzwerkquelle übernommen werden (z. B. wenn Benutzer über das Netzwerk auf den Ordner zugreifen), werden sie von der kontinuierlichen Datensicherung (CDP) nicht erkannt. 6. Wenn eine Datei gerade verwendet wird (weil beispielsweise Änderungen an einer Excel-Datei vorgenommen werden), wird die

Alarm	Beschreibung	So können Sie den Alarm auflösen
		kontinuierliche Datensicherung (CDP) diese Änderungen nicht erkennen. Damit die Änderungen von der kontinuierlichen Datensicherung (CDP) erkannt werden, muss die Datei gespeichert und geschlossen werden.
Die Konfiguration der Hyper-V-Hosts ist ungültig	Es wird ein Alarm generiert, wenn zwei oder mehr Agenten für Hyper-V auf Hyper-V-Hosts installiert sind, die denselben Host-Namen haben, was auf derselben Kontoebene nicht unterstützt wird.	Sie sollten diese Agenten für Hyper-V unter verschiedenen Unterabteilungen dieses Kontos registrieren, um Konflikte zu vermeiden.
Die Validierung ist fehlgeschlagen	Es wird ein Alarm generiert, wenn der Validierungsprozess Ihres Backups nicht abgeschlossen werden konnte.	Überprüfen Sie das Protokoll der fehlerhaften Aktion: Klicken Sie zuerst auf die Maschine, um diese auszuwählen, und anschließend auf **Aktivitäten**, um die Warnung im Protokoll zu finden. Die Meldung sollte Sie zur Ursache des Problems führen, über das Sie von der Software alarmiert wurden.
Die Backups im Cloud Storage konnten nicht in das neue Format umgewandelt werden	Es wird ein Alarm generiert, wenn die Backups nicht im neuen Format in den Cloud Storage migriert werden konnten.	Die Migration von Acronis Cyber Backup Advanced-Archiven wird hier beschrieben. Die Migration von Acronis Cyber Backup-Archiven wird hier beschrieben. Bevor Sie den Acronis Support kontaktieren, sammeln Sie bitte mithilfe des Tools 'migrate_ archives' folgende Berichte: **migrate_archives.exe --account=<Acronis Konto> --password=<Kennwort> --subaccounts=All > report1.txt**

Alarm	Beschreibung	So können Sie den Alarm auflösen
		migrate_archives.exe --cmd=finishUpgrade --account=<Acronis Konto> --password=<Kennwort> > report2.txt
Das Verschlüsselungskennwort fehlt	Es wird ein Alarm generiert, wenn der Datenbank-Chiffrierschlüssel falsch, beschädigt oder nicht vorhanden ist.	Falls Sie Ihr Kennwort verlieren, gibt es keine Möglichkeit, Ihre verschlüsselten Backups wiederherzustellen! Sie müssen das Verschlüsselungskennwort lokal festlegen, also auf dem geschützten Gerät. Sie können das Verschlüsselungskennwort nicht in einem Schutzplan festlegen. Weitere Informationen finden Sie im Abschnitt Das Verschlüsselungskennwort festlegen.
Der Upload ist ausstehend	Es wird ein Alarm generiert, wenn die geplante Prüfung ergibt, dass der physische Datenversand in die Cloud für diesen Backup-Plan nicht in den Storage hochgeladen wurde.	
Backup-Wiederherstellung ist fehlgeschlagen	Es wird ein Alarm generiert, wenn die Recovery-Aktion fehlschlägt, während Sie versuchen, Dateien oder System-Backups wiederherzustellen.	Ermitteln Sie das genaue Datum des Backup-Fehlers und versuchen Sie, mit dem letzten erfolgreichen Backup die Wiederherstellung zu wiederholen.

Disaster Recovery-Alarmmeldungen

Alarm	Beschreibung	So können Sie den Alarm auflösen
Die Storage-Quota wurde überschritten	Es wird ein Alarm generiert, wenn die weiche Quota für den Disaster Recovery Storage überschritten wurde.	Vergrößern Sie die Quota oder entfernen Sie einige Archive aus dem Cloud Storage.
Die Quota ist erreicht	Es wird ein Alarm generiert,	

Alarm	Beschreibung	So können Sie den Alarm auflösen
	wenn: • Die weiche Quota für Cloud Server überschritten wird. • Die weiche Quota für Berechnungspunkte überschritten wird. • Die weiche Quota für öffentliche IP-Adressen überschritten wird.	
Die Storage-Quota wurde überschritten	Es wird ein Alarm generiert, wenn die harte Quota für den Disaster Recovery Storage überschritten wurde. Dieser Storage wird von primären Servern und Recovery-Servern verwendet. Wenn die Überschreitungsgrenze für diese Quota erreicht ist, können keine primären Server oder Recovery-Server erstellt oder Laufwerke zu vorhandenen primären Servern hinzufügt/erweitert werden. Wenn die Überschreitungsgrenze für diese Quota erreicht ist, kann kein Failover initiiert oder ein gestoppter Server gestartet werden. Die Ausführung laufender Server wird aber fortgesetzt.	
Quota wurde überschritten	Es wird ein Alarm generiert, wenn: • Die harte Quota für Cloud Server überschritten wird. • Die harte Quota für Berechnungspunkte überschritten wird. • Die harte Quota für öffentliche IP-Adressen	Erwägen Sie, zusätzliche Geräte-Quotas zu erwerben oder Backup-Tasks für die Geräte, die Sie nicht mehr schützen müssen, zu deaktivieren.

Alarm	Beschreibung	So können Sie den Alarm auflösen
	überschritten wird.	
Failover-Fehler	Es wird ein Alarm generiert, wenn ein Systemproblem aufgetreten ist, nachdem die Failover-Aktion übermittelt wurde.	1. Klicken Sie auf dem Recovery-Server auf **Bearbeiten**. Weitere Informationen finden Sie im Abschnitt 'Einen Recovery-Server erstellen'. 2. Verringern Sie CPU-/RAM-Zuordnung für den Recovery-Server. 3. Versuchen Sie, den Failover-Prozess erneut durchzuführen.
Fehler beim Test-Failover	Es wird ein Alarm generiert, wenn ein Systemproblem aufgetreten ist, nachdem die Test-Aktion übermittelt wurde.	1. Klicken Sie auf dem Recovery-Server auf **Bearbeiten**. Weitere Informationen finden Sie im Abschnitt 'Einen Recovery-Server erstellen'. 2. Verringern Sie CPU-/RAM-Zuordnung für den Recovery-Server. 3. Versuchen Sie, den Failover-Prozess erneut durchzuführen. **Hinweis** Stellen Sie sicher, dass die IP-Adresse im Produktionsnetzwerk mit der IP-Adresse übereinstimmt, die im DHCP-Server konfiguriert ist.
Failback-Fehler	Es wird ein Alarm generiert, wenn ein Systemproblem aufgetreten ist, nachdem die Failback-Aktion initiiert wurde.	Sie können den fehlerhaften Speicherort in der Liste der Backup Storages sehen: Er hat eine Nummer statt eines Namens (normalerweise entspricht ein Speicherortname einem der vorhandenen Endbenutzernamen) und Sie haben diesen Speicherort nicht erstellt. Entfernen Sie den fehlerhaften Speicherort: 1. Gehen Sie in der Cyber Protect-Konsole zu 'Backup Storage'. 2. Suchen Sie den Speicherort und klicken Sie auf das Kreuzsymbol

Alarm	Beschreibung	So können Sie den Alarm auflösen
		(x), um diesen zu löschen. 3. Bestätigen Sie Ihre Auswahl, indem Sie auf 'Löschen' klicken. 4. Wiederholen Sie die Failover-Aktion.
Der Failback-Prozess wurde abgebrochen	Es wird ein Alarm generiert, wenn der Failback-Prozess durch den Benutzer abgebrochen wurde.	Schließen Sie den Alarm manuell über die Konsole.
Fehler bei der VPN-Verbindung	Es wird ein Alarm generiert, wenn die VPN-Verbindung aus Gründen fehlschlägt, die nichts mit den Aktionen des Benutzers zu tun haben. Der Statusbericht der VPN-Appliance ist veraltet.	Sollten Sie beim Bereitstellen oder Verbinden der Acronis VPN-Appliance ein Problem feststellen, können Sie sich an den Acronis Support wenden. Bitte senden Sie dann folgende Informationen mit Ihrer E-Mail: • Screenshots der Fehlermeldungen (sofern es welche gibt) • Einen Screenshot der Acronis VPN-Appliance-Befehlszeilenschnittstelle • Ihr Acronis Backup Cloud-Datacenter und den Gruppennamen.
(VPN nicht erreichbar) Das Verbindungsgateway ist nicht erreichbar	Es wird ein Alarm generiert, wenn der DR Service das Verbindungsgateway nicht erreichen kann. Der Statusbericht des Verbindungsgateways ist veraltet.	Sollten Sie beim Bereitstellen oder Verbinden der Acronis VPN-Appliance ein Problem feststellen, können Sie sich an den Acronis Support wenden. Bitte senden Sie dann folgende Informationen mit Ihrer E-Mail: • Screenshots der Fehlermeldungen (sofern es welche gibt) • Einen Screenshot der Acronis VPN-Appliance-Befehlszeilenschnittstelle • Ihr Acronis Backup Cloud-Datacenter und den

Alarm	Beschreibung	So können Sie den Alarm auflösen
		Gruppennamen
Es ist eine Neuzuweisung der DR-IP-Adresse erforderlich	Es wird ein Alarm generiert, wenn die VPN-Appliance Änderungen im Netzwerk erkennt.	Weisen Sie die IP-Adresse neu zu. Weitere Informationen dazu finden Sie im Abschnitt 'IP-Adressen neu zuweisen'.
Fehler beim Verbindungsgateway	Es wird ein Alarm generiert, wenn der VPN-Server nicht in der Cloud bereitgestellt werden konnte.	Verwenden Sie das Connection Verification Tool und überprüfen Sie dessen Ausgabe auf Fehler. Erlauben Sie die Acronis Software über die Anwendungssteuerung Ihrer Firewalls und Antimalware-Software.
Fehler bei der Erstellung des primären Servers	Es wird ein Alarm generiert, wenn der primäre Server aufgrund eines Fehlers nicht erstellt werden konnte.	
Fehler bei der Erstellung des Recovery-Servers	Es wird ein Alarm generiert, wenn der Recovery-Server aufgrund eines Fehlers nicht erstellt werden konnte.	Stellen Sie sicher, dass der Recovery-Server den Software-Anforderungen entspricht.
Primären Server löschen	Es wird ein Alarm generiert, wenn ein primärer Server gelöscht wird.	
Fehler bei der Wiederherstellung des Servers	Es wird ein Alarm generiert, wenn die Wiederherstellung des primären oder Recovery-Servers fehlgeschlagen ist.	Finden Sie die Details. Wenn es sich um eine allgemeine oder unklare Fehlermeldung handelt (wie z.B. „Interner Fehler“), gehen Sie zu **Disaster Recovery → Servers**, wählen Sie die betroffene Maschine aus und klicken Sie dann auf **Aktivitäten**. Klicken Sie auf eine Aktivität, halten Sie die Strg-Taste gedrückt und klicken Sie dann mit der linken Maustaste auf die entsprechende Aktivität. Jetzt können Sie das Drei-Punkte-Symbol (...) neben jeder Aktivität sehen. Klicken Sie darauf und wählen Sie **Info zur Task-Aktivität**

Alarm	Beschreibung	So können Sie den Alarm auflösen
Backup ist fehlgeschlagen	Es wird ein Alarm generiert, wenn das Backup des Cloud Servers (ein primärer Server oder ein Server im Produktions-Failover-Stadium) fehlgeschlagen ist.	1. Überprüfen Sie die Verbindung zum Backup-Speicherort. 2. Überprüfen Sie das Backup Storage-Gerät (lokale Backups).
Das Netzwerk-Limit wurde überschritten	Es wird ein Alarm generiert, wenn die maximale Anzahl von Cloud-Netzwerken erreicht ist (nämlich 5 Netzwerke).	
Runbook-Fehler	Ein wird ein Alarm generiert, wenn die Runbook-Ausführung fehlgeschlagen ist.	Dadurch wird die Produktfunktionalität nicht beeinträchtigt, sodass sie ohne Bedenken ignoriert werden kann. Weitere Informationen finden Sie im Abschnitt 'Ein Runbook erstellen'.
Runbook-Warnung	Es wird ein Alarm generiert, wenn die Runbook-Ausführung zwar erfolgreich, aber mit Warnungen abgeschlossen wurde.	Dadurch wird die Produktfunktionalität nicht beeinträchtigt, sodass sie ohne Bedenken ignoriert werden kann. Weitere Informationen finden Sie im Abschnitt 'Ein Runbook erstellen'.
Es ist ein Runbook-Benutzereingriff erforderlich	Es wird ein Alarm generiert, wenn das Runbook auf einen Benutzereingriff wartet.	Dadurch wird die Produktfunktionalität nicht beeinträchtigt, sodass sie ohne Bedenken ignoriert werden kann. Weitere Informationen finden Sie im Abschnitt 'Ein Runbook erstellen'.
Der Internet-Datenverkehr wurde blockiert	Es wird ein Alarm generiert, wenn der Internet-Datenverkehr vom Administrator blockiert wurde.	
Die Blockierung des Internet-Datenverkehr wurde aufgehoben	Es wird ein Alarm generiert, wenn die Blockierung des Internet-Datenverkehrs durch den Administrator wieder aufgehoben wurde.	

Alarm	Beschreibung	So können Sie den Alarm auflösen
Die lokalen Netzwerke überlappen sich	Es wird ein Alarm generiert, wenn identische oder überlappende lokale Netzwerke erkannt wurden.	
Unzureichende Server-Quota beim Lizenzwechsel	Es wird ein Alarm generiert, wenn die Cloud Server-Quota nicht ausreicht.	• Stellen Sie sicher, dass der Mandant und der Benutzer über eine Webhosting-Server-Quota oder eine Server-Quota für einen physischen Server verfügen. • Stellen Sie sicher, dass der Mandant und der Benutzer über eine Webhosting-Server-Quota oder eine Virtuelle-Maschinen-Quota für einen virtuellen Server verfügen. Ein virtueller Server kann keine Server-Quota verwenden.
Unzureichendes Angebotselement beim Lizenzwechsel	Es wird ein Alarm generiert, wenn das Disaster Recovery Storage-Angebotselement deaktiviert ist.	Weitere Informationen finden Sie im Abschnitt Disaster Recovery-Quotas.
Fehler beim Lizenzwechsel	Es wird ein Alarm generiert, wenn beim Disaster Recovery-Upgrade ein Fehler aufgetreten ist.	
Unzureichende Berechnungspunkte beim Lizenzwechsel	Es wird ein Alarm generiert, wenn keine Berechnungspunkte verfügbar sind.	Überprüfen und vergrößern Sie im Management-Portal die harte Quota für Berechnungspunkte.
Unzureichendes Server-Angebotselement beim Lizenzwechsel	Es wird ein Alarm generiert, wenn das Cloud Server-Angebotselement deaktiviert ist.	
Die Richtlinie konnte den Recovery-Server nicht erstellen	Es wird ein Alarm generiert, wenn beim Einrichten der Disaster Recovery-Infrastruktur ein Fehler aufgetreten ist.	Erstellen Sie einen Recovery-Server manuell ohne die Eigenschaft 'Internetzugriff'. Weitere Informationen finden Sie im Abschnitt 'Einen Recovery-Server erstellen'.
Backup-Prozessor automatischer	Es wird ein Alarm generiert,	

Alarm	Beschreibung	So können Sie den Alarm auflösen
Test-Failover neu geplant	wenn die automatisierte Test-Failover-Ausführung neu geplant wurde.	
Backup-Prozessor automatischer Test-Failover – Zeitlimit wurde erreicht	Es wird ein Alarm generiert, wenn die automatisierte Test-Failover-Aktion abgelaufen ist. **Hinweis** Jede automatisierte Test-Failover-Ausführung verbraucht kostenpflichtige Berechnungspunkte.	
Backup-Prozessor automatischer Test-Failover – allgemeiner Fehler	Es wird ein Alarm generiert, wenn die letzte geplante automatisierte Test-Failover-Ausführung des Recovery-Servers fehlgeschlagen ist.	1. Starten Sie einen Test-Failover des Recovery-Servers manuell. Weitere Informationen finden Sie im Abschnitt 'Einen Test-Failover durchführen'. 2. Warten Sie auf den nächsten geplanten Zeitpunkt, an dem ein automatischer Test-Failover durchgeführt werden soll
Failback-Datenübertragungsfehler	Es wird ein Alarm generiert, wenn die Failback-Datenübertragung fehlschlägt.	
Failback ist fehlgeschlagen	Es wird ein Alarm generiert, wenn beim Failback-Prozess ein Fehler aufgetreten ist.	Sie können den fehlerhaften Speicherort in der Liste der Backup Storages sehen: Er hat eine Nummer statt eines Namens (normalerweise entspricht ein Speicherortname einem der vorhandenen Endbenutzernamen) und Sie haben diesen Speicherort nicht erstellt. Entfernen Sie den fehlerhaften Speicherort: 1. Gehen Sie in Cyber Protection zu 'Backup Storage'. 2. Suchen Sie den Speicherort und klicken Sie auf das Kreuzsymbol (x), um diesen zu löschen. 3. Bestätigen Sie Ihre Auswahl, indem Sie auf **Löschen** klicken.

Alarm	Beschreibung	So können Sie den Alarm auflösen
		Wiederholen Sie die Failover-Aktion.
Die Failback-Bestätigung ist fehlgeschlagen	Ein wird ein Alarm generiert, wenn die Failback-Bestätigung fehlgeschlagen ist.	
Die Failback-Maschine ist bereit für den Switchover-Prozess	Es wird ein Alarm generiert, wenn die Maschine für den Switchover-Prozess bereit ist.	
Der Failback-Switchover-Prozess wurde fertiggestellt	Ein wird ein Alarm generiert, wenn der Switchover-Prozess erfolgreich war.	Schließen Sie den Alarm manuell über die Konsole.
Der Failback-Ziel-Agent ist offline	Ein wird ein Alarm generiert, wenn der Agent offline ist.	

Antimalware Protection-Alarmmeldungen

Alarm	Beschreibung	So können Sie den Alarm auflösen
Es wurde eine verdächtige Remote-Verbindungsaktivität erkannt	Es wird ein Alarm generiert, wenn eine Ransomware erkannt wird, die von einer Remote-Verbindung stammt.	Schließen Sie den Alarm manuell über die Konsole.
Es wurde eine verdächtige Aktivität erkannt	Es wird ein Alarm generiert, wenn im Workload eine Ransomware erkannt wird.	Schließen Sie den Alarm manuell über die Konsole., um den Alarm zu deaktivieren. Je nach der Option, die Sie im Active Protection-Plan spezifiziert haben, wird der schädliche Prozess gestoppt, die vom Prozess vorgenommenen Änderungen werden rückgängig gemacht – oder es wurden noch keine Maßnahmen ergriffen und Sie müssen das Problem manuell lösen. Lesen Sie die Details zum Alarm, um zu ermitteln, welcher Prozess die Dateien verschlüsselt und welche Dateien betroffen sind. Wenn Sie feststellen, dass der Prozess, der die Dateien verschlüsselt, eigentlich zulässig ist (also ein Falsch-Positiv-Alarm

Alarm	Beschreibung	So können Sie den Alarm auflösen
		vorliegt), können Sie diesen Prozess in die Liste der vertrauenswürdigen Prozesse aufnehmen: 1. Öffnen Sie den Active Protection-Plan. 2. Klicken Sie auf **Bearbeiten**, um die Einstellungen zu ändern. 3. Spezifizieren Sie bei **Vertrauenswürdige Prozesse** diejenigen Prozesse, die niemals als Ransomware eingestuft werden sollen. Spezifizieren Sie den vollständigen Pfad zur ausführbaren Datei des Prozesses (mit dem Laufwerksbuchstaben beginnend). Beispiel: C:\Windows\Temp\er76s7sdkh.exe.
Es wurde eine verdächtige Cryptomining-Aktivität erkannt	Es wird ein Alarm generiert, wenn im Workload illegales Krypto-Mining erkannt wird.	Schließen Sie den Alarm manuell über die Konsole.
MBR-Schutz: Es wurde eine verdächtige Aktivität erkannt und angehalten	Es wird ein Alarm generiert, wenn im Workload eine Ransomware entdeckt wird (insbesondere, wenn die MBR-/GPT-Partition durch Ransomware verändert wurde).	Schließen Sie den Alarm manuell über die Konsole.
Es wurde ein nicht unterstützer Netzwerkpfad spezifiziert	Es wird ein Alarm generiert, wenn es sich bei dem vom Administrator bereitgestellten Wiederherstellungspfad nicht um einen Pfad zu einem lokalen Ordner handelt.	Spezifizieren Sie den lokalen Pfad für den Netzwerkordnerschutz (den Wiederherstellungspfad). Schließen Sie den Alarm manuell über die Konsole
Der kritische Prozess wurde dem Active Protection-Plan als schädlich hinzugefügt	Es wird ein Alarm generiert, wenn ein wichtiger Prozess in die Liste der Schutzausschlüsse als zu blockierender Prozess	Schließen Sie den Alarm manuell über die Konsole.

Alarm	Beschreibung	So können Sie den Alarm auflösen
	aufgenommen wurde.	
Die Active Protection-Richtlinie konnte nicht angewendet werden	Es wird ein Alarm generiert, wenn die Active Protection-Richtlinie nicht angewendet werden konnte.	Überprüfen Sie die Fehlermeldung, um zu ermitteln, warum die Active Protection-Richtlinie nicht angewendet werden konnte.
Secure Zone: Nicht autorisierte Aktionen werden erkannt und blockiert	Es wird ein Alarm generiert, wenn im Workload eine Ransomware entdeckt wird (wenn die ASZ-Partition durch Ransomware verändert wurde).	Schließen Sie den Alarm manuell über die Konsole.
Active Protection Service wird nicht ausgeführt	Es wird ein Alarm generiert, wenn der Dienst 'Active Protection Service' abgestürzt ist / nicht ausgeführt wird.	Überprüfen Sie die Fehlermeldung, um zu ermitteln, warum der Active Protection Service nicht ausgeführt wird.
Der Active Protection Service ist nicht verfügbar	Es wird ein Alarm generiert, wenn der Active Protection Service nicht verfügbar ist, weil ein Treiber fehlt oder eine Inkompatibilität vorliegt.	Überprüfen Sie die Windows-Ereignisprotokolle auf Abstürze des Acronis Active Protection Service (acronis_protection_service.exe).
Es liegt ein Konflikt mit einer anderen Sicherheitslösung vor	Es wird ein Alarm generiert, wenn die Active Protection-Funktionalität für die Maschine '{{resourceName}}' nicht verfügbar ist, weil ein Konflikt mit einer anderen Sicherheitslösung erkannt wurde. Wenn Sie Active Protection aktivieren wollen, müssen Sie die Sichehreitslösung deaktivieren oder deinstallieren, mit der der Konflikt besteht.	**Lösung 1**: Wenn Sie den Echtzeitschutz von Acronis verwenden wollen, müssen Sie das Antivirenprogramm eines Drittanbieters von der Maschine deinstallieren. **Lösung 2**: Wenn Sie das Antiviren-Programm eines Drittanbieters verwenden wollen, müssen Sie den Echtzeitschutz von Acronis, die URL-Filterung und die Windows Defender Antivirus-Funktionalität im Schutzplan deaktivieren.
Die Quarantäne-Aktion ist fehlgeschlagen	Es wird ein Alarm generiert, wenn die	Überprüfen Sie die Fehlermeldung, um herauszufinden, warum die Quarantäne

Alarm	Beschreibung	So können Sie den Alarm auflösen
	Antimalware-Funktionalität eine erkannte Malware nicht unter Quarantäne stellen konnte.	fehlgeschlagen ist.
Es wurde ein schädlicher Prozess erkannt	Es wird ein Alarm generiert, wenn eine Malware (ein bestimmter Prozesstyp) von der Behavioral Engine erkannt wird. Die erkannte Malware wird unter Quarantäne gestellt.	Schließen Sie den Alarm manuell über die Konsole.
Es wurde ein schädlicher Prozess erkannt, aber nicht unter Quarantäne gestellt	Es wird ein Alarm generiert, wenn eine Malware (ein bestimmter Prozesstyp) von der Behavioral Engine erkannt wird. Die erkannte Malware wird nicht unter Quarantäne gestellt.	Schließen Sie den Alarm manuell über die Konsole.
Malware wurde erkannt und blockiert (ODS)	Es wird ein Alarm generiert, wenn bei einem geplanten Scan eine Malware erkannt wurde. Die erkannte Malware wird unter Quarantäne gestellt.	Schließen Sie den Alarm manuell über die Konsole.
Malware wurde erkannt und blockiert (RTP)	Es wird ein Alarm generiert, wenn eine Malware vom Echtzeitschutz erkannt wird. Die erkannte Malware wird unter Quarantäne gestellt.	Schließen Sie den Alarm manuell über die Konsole.
In einem Backup wurde eine Malware erkannt	Es wird ein Alarm generiert, wenn eine Malware beim Backup-Scanning erkannt wird.	Schließen Sie den Alarm manuell über die Konsole.
Es wurde ein Konflikt zwischen der Realtime Antimalware Protection und einem Sicherheitsprodukt erkannt	Es wird ein Alarm generiert, wenn die Antimalware-Funktionalität nicht im Windows-	Deaktivieren oder deinstallieren Sie das Drittanbieter-Sicherheitsprodukt – oder deaktivieren Sie die in Echtzeit arbeitende Antimalware Protection im Schutzplan.

Alarm	Beschreibung	So können Sie den Alarm auflösen
	Sicherheitscenter registriert werden konnte.	
Das Microsoft Security Essentials-Modul konnte nicht ausgeführt werden	Es wird ein Alarm generiert, wenn die Microsoft Security Essentials-Moduls nicht ausgeführt werden konnten.	Überprüfen Sie die Fehlermeldung, um zu ermitteln, warum das Microsoft Security Essentials-Modul nicht ausgeführt werden konnte.
Der Echtzeitschutz ist nicht verfügbar, da die Antiviren-Software eines Drittanbieters installiert ist	Es wird ein Alarm generiert, wenn der Echtzeitschutz nicht eingeschaltet werden konnte, weil der Antivirus-Echtzeitschutz eines Drittanbieters noch aktiviert ist.	Deaktivieren oder deinstallieren Sie das Drittanbieter-Sicherheitsprodukt – oder deaktivieren Sie die in Echtzeit arbeitende Antimalware Protection im Schutzplan.
Der Echtzeitschutz ist nicht verfügbar, weil ein Treiber fehlt oder eine Inkompatibilität vorliegt	Es wird ein Alarm generiert, wenn der Echtzeitschutz aufgrund eines inkompatiblen oder fehlenden Treibers nicht verfügbar ist.	Überprüfen Sie die Fehlermeldung, um festzustellen, warum Acronis den Treiber nicht auf dem Workload installieren konnte.
Der Cyber Protection (oder Active Protection) Service reagiert nicht	Es wird ein Alarm generiert, wenn der Cyber Protection Service von der Konsole auf einen Ping zur Integritätsprüfung antwortet.	Schließen Sie den Alarm manuell über die Konsole.
Das Sicherheitsdefinitionsupdate ist fehlgeschlagen	Es wird ein Alarm generiert, wenn das Update der Sicherheitsdefinitionen fehlgeschlagen ist.	Überprüfen Sie die Fehlermeldung, um herauszufinden, warum das Update der Sicherheitsdefinitionen fehlgeschlagen ist.
Der Manipulationsschutz ist aktiviert	Ein Alarm wird generiert, wenn die Microsoft Defender-Einstellungen nicht geändert werden können, weil der Manipulationsschutz aktiviert ist.	Deaktivieren Sie die Einstellungen für den Manipulationsschutz im Windows-Workload.
Die Ausführung des Windows	Ein wird ein Alarm	Überprüfen Sie die Fehlermeldung, um zu

Alarm	Beschreibung	So können Sie den Alarm auflösen
Defender-Moduls ist fehlgeschlagen	generiert, wenn die Ausführung des Windows Defender-Moduls fehlgeschlagen ist.	ermitteln, warum das Windows Defender-Modul nicht ausgeführt werden konnte.
Windows Defender wird durch die Antivirus-Software eines Drittanbieters blockiert	Es wird ein Alarm generiert, wenn der Windows Defender blockiert wird, weil die Antivirus-Software eines anderen Anbieters auf der Maschine installiert ist.	Deaktivieren oder deinstallieren Sie das Drittanbieter-Sicherheitsprodukt.
Gruppenrichtlinien-Konflikt	Es wird ein Alarm generiert, wenn die Microsoft Defender-Einstellungen nicht angepasst werden können, weil sie von einer Gruppenrichtlinie kontrolliert werden.	Deaktivieren Sie die Gruppenrichtlinien-Einstellungen im Windows-Workload.
Microsoft Security Essentials hat Maßnahmen ergriffen, um diese Maschine vor Malware zu schützen	Es wird ein Alarm generiert, wenn Microsoft Security Essential eine Malware gelöscht/unter Quarantäne gestellt hat.	Schließen Sie den Alarm manuell über die Konsole.
Microsoft Security Essentials hat eine Malware erkannt	Es wird ein Alarm generiert, wenn Microsoft Security Essentials eine Malware oder eine andere potentiell unerwünschte Software erkannt hat.	Schließen Sie den Alarm manuell über die Konsole.

Lizenzierungsalarmmeldungen

Alarm	Beschreibung	So können Sie den Alarm auflösen
Die Storage-Quota ist fast erreicht	Es wird ein Alarm generiert, wenn die Nutzung unter 80% fällt (nach einer Bereinigung oder einem Quota-Upgrade).	Erwägen Sie, zusätzlichen Speicherplatz zu kaufen oder Speicherplatz in Ihrem Cloud Storage freizugeben.
Die Storage-Quota wurde überschritten	Es wird ein Alarm generiert, wenn die Storage-Quota zu 100% verwendet	Kaufen Sie mehr Speicherplatz. Weitere Informationen darüber,

Alarm	Beschreibung	So können Sie den Alarm auflösen
	wird.	wie Sie das tun können, finden Sie im Abschnitt Mehr Cloud Storage kaufen.
Die Workload-Quota wurde erreicht	Es wird ein Alarm generiert, wenn die Nutzung für das Angebotselement > 0 ist und die Nutzung > die Quota ist, aber die Nutzung <= der Quota + Überschreitung ist.	
Die Workload-Quota wurde überschritten	Es wird ein Alarm generiert, wenn die Nutzung für das Angebotselement > die Quota + Überschreitung ist.	
Die Workload hat keine Quota, um einen Backup-Plan anwenden zu können (die Ressource hat keine Service-Quota)	Es wird ein Alarm generiert, wenn: • Die Quota manuell entfernt wurde: **Gerät** –> **Details** –> **Service-Quota** – klicken Sie dann auf **Ändern** und wählen Sie die Option **Keine Quota**. • Das Management-Konsole-Angebotselement ist deaktiviert. • Der Quota+Überschreitung-Wert der Management-Konsole für das Angebotselement ist unter die aktuelle Nutzung gesunken.	
Ein Workload mit zugewiesener Quota kann nicht geschützt werden	Es wird ein Alarm generiert, wenn das Angebotselement nicht ausreicht und Sie Folgendes haben müssen: • eine dynamische Gruppe. • einen Backup-Plan, der dieser Gruppe zugewiesen wurde. • Sie haben eine Ressource hinzugefügt, die zu dieser dynamischen Gruppe gehört, aber einige Eigenschaften hat, die es verbieten, dass derselbe Backup-Plan auf sie angewendet werden kann.	
Die Abonnementlizenz ist abgelaufen	Es wird ein Alarm generiert, wenn bei der täglichen Überprüfung auf Alarmmeldungen zu abgelaufenen Lizenzen/Wartungsverträgen der	Wenn ein Abonnement ausläuft, wird die gesamte Produktfunktionalität

Alarm	Beschreibung	So können Sie den Alarm auflösen
	License Server abgefragt wurde und dieser zurückgemeldet hat, dass die Lizenz abgelaufen ist.	(ausgenommen Wiederherstellungen) so lange blockiert, bis das Abonnement wieder erneuert wird. Bereits vorliegende Backup-Daten können aber weiterhin wiederhergestellt werden. Kaufen Sie eine neue Lizenz. **Hinweis** Wenn Sie erst kürzlich ein neues Abonnement erworben haben, diese Meldung aber weiterhin erhalten, müssen Sie das neue Abonnement aus Ihrem Acronis Konto importieren: Gehen Sie in der Management-Konsole zu Einstellungen -> Lizenzen und klicken Sie in der oberen rechten Ecke auf 'Sync'. Die Abonnements werden synchronisiert.
Die Abonnementlizenz wird bald ablaufen	Es wird ein Alarm generiert, wenn bei der täglichen Überprüfung auf Alarmmeldungen zu abgelaufenen Lizenzen/Wartungsverträgen der License Server abgefragt wurde und dieser zurückgemeldet hat, dass die Lizenz in weniger als 30 Tagen ablaufen wird.	Erwägen Sie, ein neues Abonnement zu kaufen.

URL-Filter-Alarmmeldungen

Alarm	Beschreibung	So können Sie den Alarm auflösen
Schädliche URL wurde blockiert	Es wird ein Alarm generiert, wenn eine schädliche URL durch die URL-Filterung blockiert wird.	Überprüfen Sie die Einstellungen für die URL-Filterung. Die URL-Filterung kann Webseiten blockieren, die gemäß den Einstellungen für die URL-Filterung blockiert werden sollen.

Alarm	Beschreibung	So können Sie den Alarm auflösen
Eine Warnung 'Schädliche URL' wurde ignoriert	Es wird ein Alarm generiert, wenn Sie ausgewählt haben, dass Sie mit der schädlichen URL fortfahren wollen, obwohl diese von der URL-Filterung blockiert wird.	Überprüfen Sie die Einstellungen für die URL-Filterung.
Es wurde ein Konflikt zwischen der URL-Filterung und einem Sicherheitsprodukt erkannt	Es wird ein Alarm generiert, wenn die URL-Filterung nicht aktiviert werden kann, weil es einen Konflikt mit einem anderen Sicherheitsprodukt gibt.	Überprüfen Sie die Einstellungen für die URL-Filterung.
Die Website-URL wurde blockiert	Es wird ein Alarm generiert, wenn eine URL alle Kriterien erfüllt, die in der blockierten Kategorie für die URL-Filterung spezifiziert wurden.	Überprüfen Sie die Einstellungen für die URL-Filterung.

EDR-Alarmmeldungen

Alarm	Beschreibung	So können Sie den Alarm auflösen
Vorfall erkannt	Es wird ein Alarm generiert, wenn ein Vorfall generiert wurde oder wenn der Status eines bestehenden Vorfalls aktualisiert wurde.	Mit diesem Alarm werden Sie über einen neuen Vorfall informiert oder wenn ein bestehender Vorfall aktualisiert wurde. Sie können sich den Alarm ansehen und diesen dann schließen. Bei Bedarf können Sie den Vorfall zur weiteren Untersuchung öffnen.
Kompromittierungsindikator (IoC) erkannt	Es wird ein Alarm generiert, wenn ein neuer Kompromittierungsindikator vom EDR IOC Threat Search Service erkannt wurde.	Mit diesem Alarm sollen Sie darüber informiert werden, dass in einem oder mehreren Workloads ein Kompromittierungsindikator (IoC) erkannt worden ist. Sie können den Alarm einsehen und dann auf den Link im Alarm klicken, um weitere Details über den Kompromittierungsindikator zu erfahren.
Die Isolierung des Workloads vom Netzwerk ist fehlgeschlagen	Es wird ein Alarm generiert, wenn	Ergreifen Sie die erforderlichen Maßnahmen.

Alarm	Beschreibung	So können Sie den Alarm auflösen
	der Benutzer eine Aktion auslöst, um die Maschine vom Netzwerk zu isolieren – und die Isolierungsaktion fehlschlägt.	
Die erneute Verbindung des Workloads mit dem Netzwerk ist fehlgeschlagen	Es wird ein Alarm generiert, wenn der Benutzer eine Aktion auslöst, um die Maschine wieder mit dem Netzwerk zu verbinden – und diese Aktion fehlgeschlagen ist.	Ergreifen Sie die erforderlichen Maßnahmen.
Die Windows Defender Firewall-Einstellungen wurden geändert	Es wird ein Alarm generiert, wenn die Einstellungen der Firewall auf der isolierten Maschine geändert wurden.	Mit diesem Alarm sollen Sie darüber informiert werden, dass bestimmte Firewall-Details auf der isolierten Maschine geändert wurden. Der Alarm dient nur der Information und Sie können ihn schließen, nachdem Sie ihn angesehen haben.

Gerätekontrolle-Alarmmeldungen

Alarm	Beschreibung	So können Sie den Alarm auflösen
Die Gerätekontrolle- und Data Loss Prevention-Funktionen werden mit eingeschränkter Funktionalität ausgeführt (inkompatible CPU erkannt).	Es wird ein Alarm generiert, wenn der DeviceLock Agent auf einer physischen Maschine mit einer CPU gestartet wird, die die CET-Technologie unterstützt.	Deaktivieren Sie diese Option auf den betroffenen Maschinen, um diese Alarmmeldungen zu vermeiden.
Die Gerätekontrolle-Funktionalität wird unter macOS Ventura noch nicht unterstützt	Es wird ein Alarm generiert, wenn der DeviceLock Agent auf einer physischen Maschine mit macOS Ventura gestartet wird und der Schutzplan mit der Gerätekontrolle-Funktionalität auf den Agenten angewendet wird. Gilt nur für Versionen, bei denen es ein Problem mit 'Kernel Panic'-Fehlern aufgrund des DeviceLock-Treibers gibt.	
Erlaubte Übertragung von sensiblen Daten	Es wird ein Alarm generiert, wenn die Übertragung von vertraulichen Inhalten erlaubt ist.	

Alarm	Beschreibung	So können Sie den Alarm auflösen
Gerechtfertigte Übertragung sensibler Daten	Es wird ein Alarm generiert, wenn die Übertragung von vertraulichen Inhalten gerechtfertigt wurde.	
Verweigerte Übertragung sensibler Daten	Es wird ein Alarm generiert, wenn die Übertragung von vertraulichen Inhalten blockiert wurde.	
Überprüfen Sie die Ergebnisse des Data Loss Prevention-Beobachtungsmodus	Es wird ein Alarm generiert, wenn es an der Zeit ist, die Beobachtungsergebnisse zu überprüfen: • Die Lizenz für das Advanced DLP-Paket wurde nicht angewendet. • Es ist ein Monat vergangen, seit der Beobachtungsmodus in einem Schutzplan aktiviert wurde, der auf mindestens einen Workload angewendet wurde. • Ein Monat ist vergangen, seit der letzte vergleichbare Alarm ausgelöst wurde, und es wurde eine Nutzung der DLP-Funktionalität im Beobachtungsmodus erkannt.	
Die Sicherheits-ID für den Benutzer wurde geändert	Es wird ein Alarm generiert, wenn eine Sicherheits-ID (SID) für einen bekannten Benutzernamen aktualisiert wird. Dies kann passieren, wenn das Betriebssystem auf einem PC ohne Domain neu installiert wird.	
Der Zugriff auf Peripheriegeräte ist blockiert	Es wird ein Alarm generiert, wenn bestimmte Aktionen (Lese-/Schreib-Operationen) für unterstützte Geräte blockiert sind.	
Verbindung zu einer entfernten SSL-Ressource nicht möglich.	Es wird ein Alarm erzeugt, wenn der Zugriff auf eine entfernte SSL-Ressource aufgrund zusätzlicher Handshake-Verhinderung, die bei der Ressource verwendet wird, blockiert ist.	Fügen Sie die Ressource zur Positivliste für Remote-Hosts hinzu.

System-Alarmmeldungen

Alarm	Beschreibung	So können Sie den Alarm auflösen
Der Agent ist nicht mehr aktuell	Es wird ein Alarm generiert, wenn die Agenten-Version veraltet ist.	Gehen Sie zur Liste der Agenten und starten Sie ein Update des Agenten.
Das automatische Update ist fehlgeschlagen	Es wird ein Alarm generiert, wenn die automatische Aktualisierung des Agenten fehlgeschlagen ist.	Versuchen Sie, ein manuelles Update durchzuführen.
Sie müssen das Gerät neu starten, nachdem ein neuer Agent installiert wurde	Es wird ein Alarm generiert, wenn nach erfolgreicher Remote-Installation ein Neustart erforderlich ist.	Starten Sie den Workload neu.
Aktivität fehlgeschlagen	Es wird ein Alarm generiert, wenn eine Aktivität fehlgeschlagen ist.	Starten Sie alle Dienste von Acronis auf der Maschine neu.
Die Aktivität wurde mit Warnungen abgeschlossen	Es wird ein Alarm generiert, wenn eine Aktivität erfolgreich abgeschlossen wurde, dabei aber einige Warnungen generiert wurden.	
Die Aktivität antwortet nicht mehr	Es wird ein Alarm generiert, wenn eine gerade ausgeführte Aktivität nicht mehr antwortet.	
Die Plan-Bereitstellung ist fehlgeschlagen	Es wird ein Alarm generiert, wenn die Bereitstellung des Schutzplans fehlgeschlagen ist.	
Die Konvertierung von Benutzername zu SID ist fehlgeschlagen	Es wird ein Alarm generiert, wenn die geplante SID-Konvertierung fehlgeschlagen ist.	

Alarm-Widgets

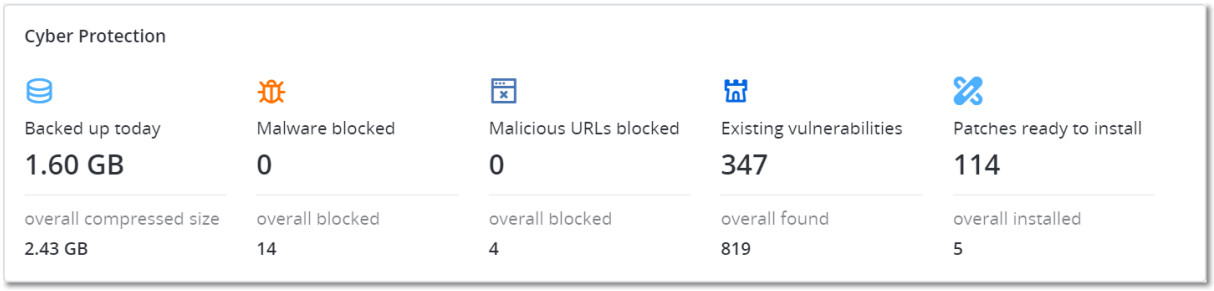
In den Alarm-Widgets werden, je nach Ihrem Workload, die folgenden Alarmmeldungsdetails angezeigt:

Feld	Beschreibung
5 neueste Alarmmeldungen	Eine Liste der fünf letzten Alarmmeldungen.

Feld	Beschreibung
Übersicht der historischen Alarmmeldungen	Ein grafisches Widget, das die Alarmmeldungen nach Schweregrad, Art und Zeitraum des Alarms anzeigt.
Aktive Alarmmeldungen – Übersicht	Ein grafisches Widget, das aktive Alarmmeldungen nach deren Schweregrad und Typ anzeigt – und zudem die Summe der aktiven Alarmmeldungen.
Alarmverlauf	Eine tabellarische Ansicht der bisherigen Alarmmeldungen.
Details 'Aktive Alarmmeldungen'	Eine tabellarische Ansicht der aktiven Alarmmeldungen.

Cyber Protection

Dieses Widget zeigt allgemeine Informationen über blockierte Malware, blockierte URLs, gefundene Schwachstellen, installierte Patches und die Größe von Backups an.



Die obere Zeile zeigt die aktuellen Statistiken an:

- **Heute gesichert** – die summierte Größe aller Recovery-Punkte für die letzten 24 Stunden
- **Malware blockiert** – die Anzahl der derzeit aktiven Alarmmeldungen über blockierte Malware
- **URLs blockiert** – die Anzahl der derzeit aktiven Alarmmeldungen über blockierte URLs
- **Vorhandene Schwachstellen** – die Anzahl der derzeit vorhandenen Schwachstellen
- **Patches bereit zur Installation** – die Anzahl der derzeit verfügbaren Patches, die installiert werden sollen

Die untere Zeile zeigt die Gesamtstatistiken an:

- Die komprimierte Größe aller Backups
- Die akkumulierte Anzahl der blockierten Malware auf allen Maschinen
- Die akkumulierte Anzahl der blockierten URLs auf allen Maschinen
- Die akkumulierte Anzahl der erkannten Schwachstellen auf allen Maschinen
- Die akkumulierte Anzahl der installierten Updates/Patches auf allen Maschinen

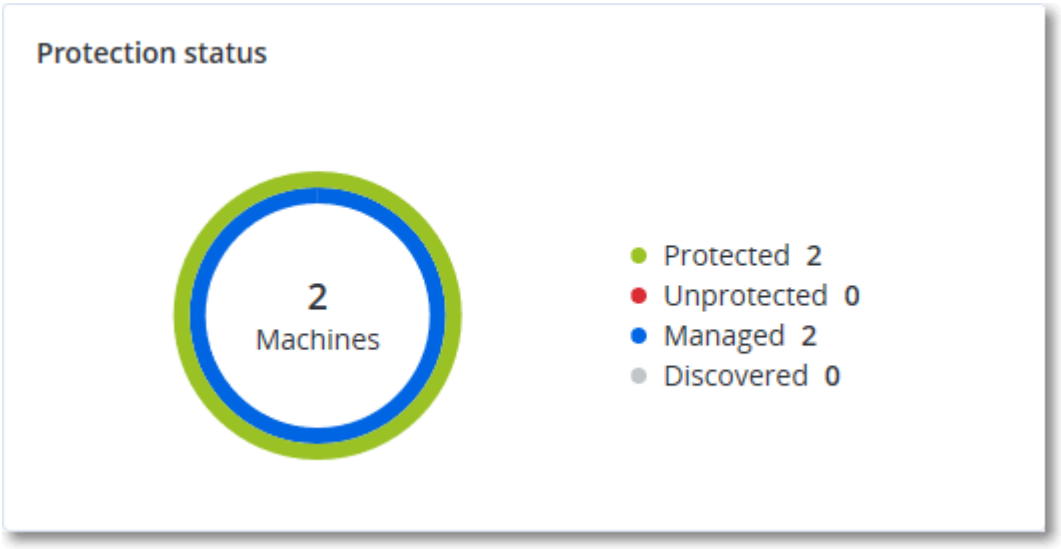
Schutzstatus

Dieses Widget zeigt den aktuellen Sicherungsstatus für alle Maschinen an.

Eine Maschine kann sich in einem der folgenden Statuszustände befinden:

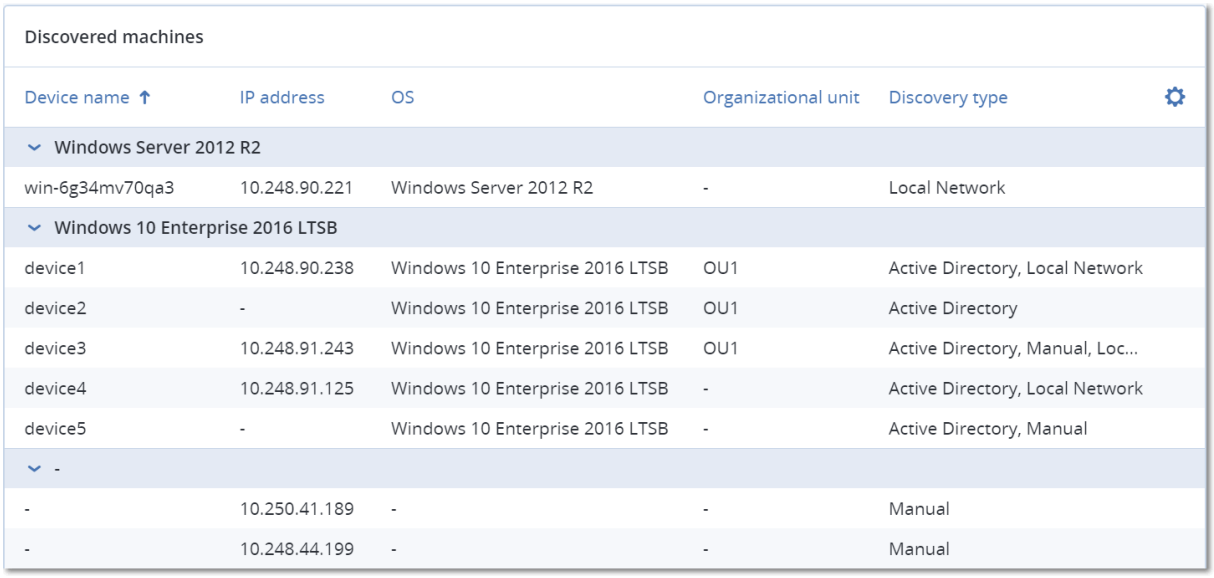
- **Geschützt** – Maschinen, auf die ein Schutzplan angewendet wurde.
- **Ungeschützt** – Maschinen, auf die noch kein Schutzplan angewendet wurde. Dazu gehören sowohl erkannte als auch verwaltete Maschinen, auf die noch kein Schutzplan angewendet wurde.
- **Verwaltet** – Maschinen, auf denen ein Protection Agent installiert ist.
- **Erkannt** – Maschinen, auf denen kein Protection Agent installiert ist.

Wenn Sie auf den Maschinenstatus klicken, werden Sie zu der Liste der Maschinen mit diesem Status weitergeleitet, um weitere Details zu erhalten.



Erkannte Maschinen

Dieses Widget zeigt die Liste der erkannten Maschinen während eines spezifizierten Zeitraums an.



Discovered machines

Device name	IP address	OS	Organizational unit	Discovery type
Windows Server 2012 R2				
win-6g34mv70qa3	10.248.90.221	Windows Server 2012 R2	-	Local Network
Windows 10 Enterprise 2016 LTSB				
device1	10.248.90.238	Windows 10 Enterprise 2016 LTSB	OU1	Active Directory, Local Network
device2	-	Windows 10 Enterprise 2016 LTSB	OU1	Active Directory
device3	10.248.91.243	Windows 10 Enterprise 2016 LTSB	OU1	Active Directory, Manual, Loc...
device4	10.248.91.125	Windows 10 Enterprise 2016 LTSB	-	Active Directory, Local Network
device5	-	Windows 10 Enterprise 2016 LTSB	-	Active Directory, Manual
-				
-	10.250.41.189	-	-	Manual
-	10.248.44.199	-	-	Manual

Endpoint Detection & Response (EDR)-Widgets

Das Endpoint Detection & Response (EDR)-Paket enthält sieben Widgets, auf die Sie über das Dashboard **Überblick** zugreifen können. Drei dieser Widgets werden außerdem standardmäßig innerhalb der EDR-Funktionalität angezeigt (siehe Abschnitt '"Vorfälle überprüfen" (S. 988)').

Die sieben verfügbaren Widgets sind:

- Spitzenverteilung der Vorfälle pro Workload
- Bedrohungsstatus (in der EDR-Funktionalität angezeigt)
- Vorfallschweregradverlauf (in der EDR-Funktionalität angezeigt)
- Sicherheitsvorfall-MTTR (Mittlere Problemlösungszeit)
- Sicherheitsvorfall-Burndown
- Erkennung anhand von Taktiken (in der EDR-Funktionalität angezeigt)
- Workload-Netzwerkstatus

Spitzenverteilung der Vorfälle pro Workload

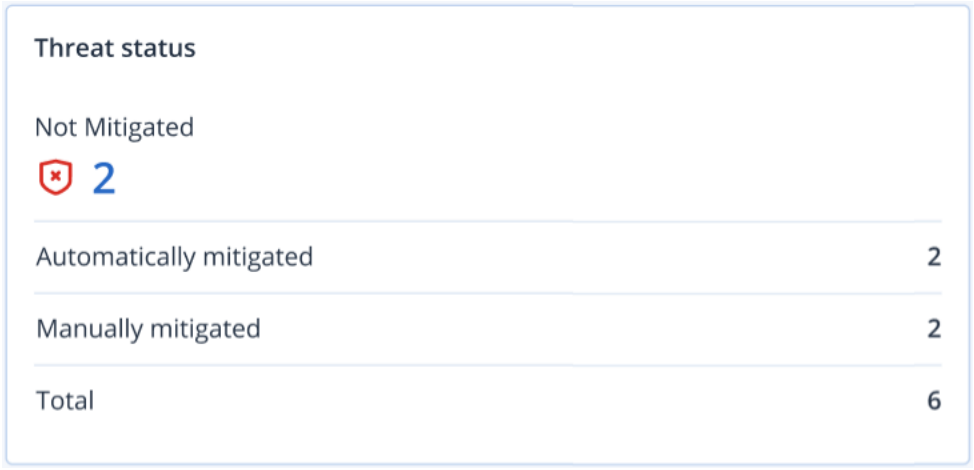
Dieses Widget zeigt die fünf Workloads mit den meisten Vorfällen an (klicken Sie auf **Alle anzeigen**, um zur Vorfallsliste zu gelangen, die entsprechend den Widget-Einstellungen gefiltert wird).

Bewegen Sie den Mauszeiger über eine Workload-Zeile, um eine Aufschlüsselung des aktuellen Untersuchungsstadiums für die Vorfälle angezeigt zu bekommen; die Untersuchungsstadien sind **Nicht gestartet**, **Wird untersucht**, **Geschlossen** und **Falsch positiv**. Klicken Sie anschließend auf den Workload, den Sie weiter analysieren wollen. Daraufhin wird die Vorfallsliste anhand der Widget-Einstellungen aktualisiert.

Bedrohungsstatus

In diesem Widget wird der aktuelle Bedrohungsstatus aller Workloads angezeigt. Dabei wird die Anzahl der Vorfälle hervorgehoben, die noch nicht abgeschwächt wurden und daher untersucht werden müssen. Das Widget gibt auch die Anzahl der Vorfälle an, die (manuell und/oder automatisch vom System) abgeschwächt wurden.

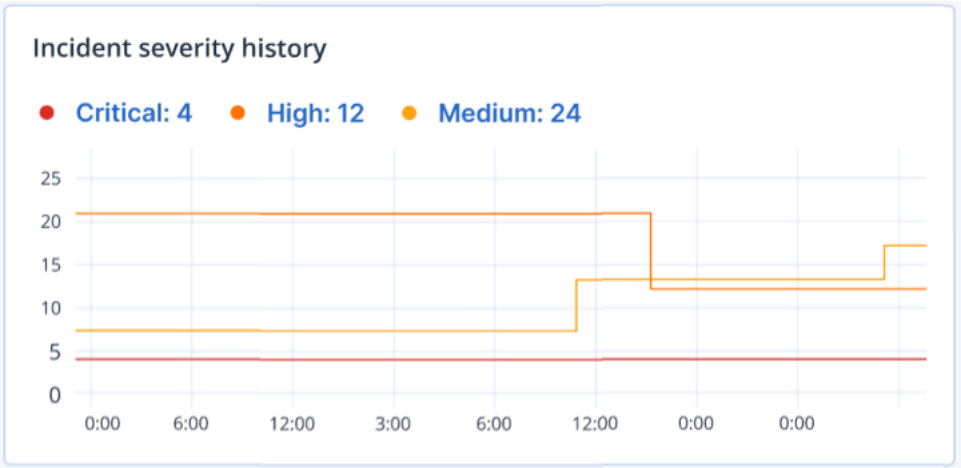
Klicken Sie auf die Nummer für **Nicht abgeschwächt**, damit die Vorfallsliste so gefiltert wird, dass nur noch Vorfälle angezeigt werden, die nicht abgeschwächt sind.



Vorfallschweregradverlauf

Dieses Widget zeigt die Angriffsentwicklung nach Schweregrad an und kann so helfen, Angriffskampagnen zu erkennen. Wenn Spitzen sichtbar werden, kann dies ein Hinweis darauf sein, dass die entsprechende Organisation angegriffen wird.

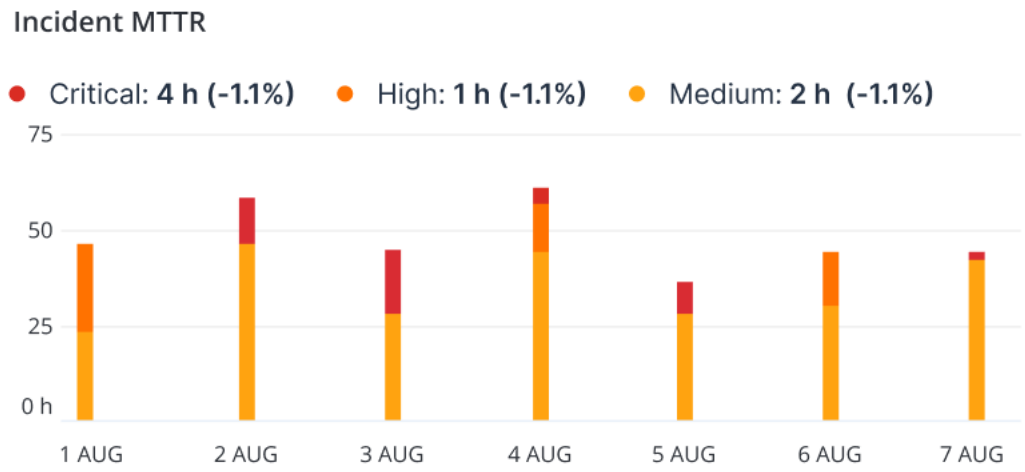
Bewegen Sie den Mauszeiger über das Diagramm, wenn Sie eine Aufschlüsselung des Vorfallverlaufs für einen bestimmten Zeitpunkt in den letzten 24 Stunden (der Standardzeitraum) einsehen wollen. Klicken Sie auf den jeweiligen Schweregrad (**Kritisch**, **Hoch** oder **Mittel**), wenn Sie eine Liste mit verwandten Vorfällen einsehen wollen. Sie werden daraufhin zur Vorfallsliste weitergeleitet, in der die Vorfälle nach dem ausgewählten Schweregrads vorgefiltert sind.



Sicherheitsvorfall-MTTR (Mittlere Problemlösungszeit)

Dieses Widget zeigt die durchschnittliche Problemlösungszeit für Sicherheitsvorfälle an. Sie gibt an, wie schnell Vorfälle untersucht und gelöst werden.

Klicken Sie auf eine Spalte, um die Vorfälle nach ihrem Schweregrad (**Kritisch**, **Hoch** und **Mittel**) aufzuschlüsseln und zu sehen, wie lange es dauerte, die verschiedenen Schweregrade zu beheben. Der in Klammern angegebene Prozentwert gibt den Anstieg bzw. den Rückgang im Vergleich zum vorherigen Zeitraum an.



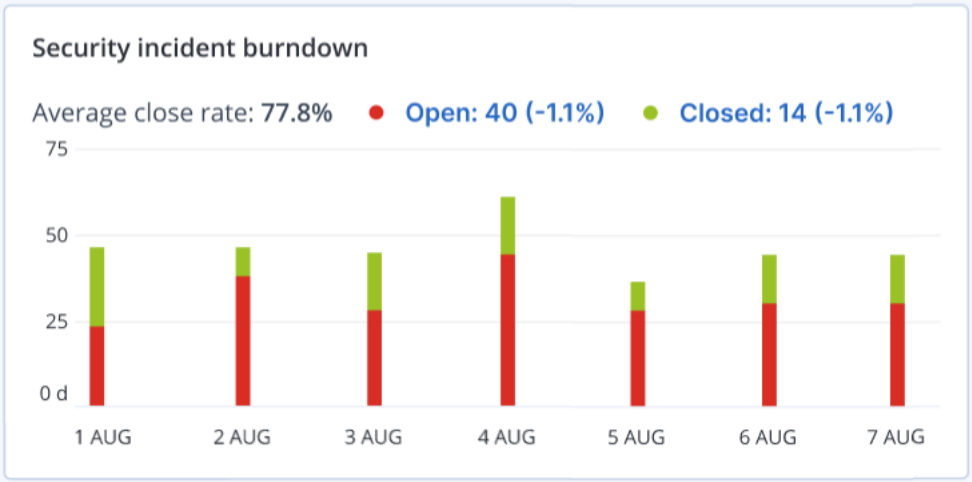
Sicherheitsvorfall-Burndown

Dieses Widget zeigt die Effizienzrate bei der Schließung von Vorfällen an; die Anzahl der offenen Vorfälle wird dabei mit der Anzahl der geschlossenen Vorfälle über einen bestimmten Zeitraum abgeglichen.

Bewegen Sie den Mauszeiger über eine Spalte, um eine Aufschlüsselung der geschlossenen und offenen Vorfälle für den jeweiligen Tag angezeigt zu bekommen. Wenn Sie auf den Wert 'Offen' klicken, wird die Vorfallsliste angezeigt und so gefiltert, dass alle derzeit offenen Vorfälle (also mit dem Stadium **Wird untersucht** oder **Nicht gestartet**) angezeigt werden. Wenn Sie auf den Wert

'Geschlossen' klicken, wird die Vorfallsliste angezeigt und so gefiltert, dass nur noch die Vorfälle angezeigt werden, die nicht mehr offen sind (die also das Stadium **Geschlossen** oder **Falsch positiv** haben).

Der in Klammern angegebene Prozentwert gibt den Anstieg bzw. den Rückgang im Vergleich zum vorherigen Zeitraum an.



Erkennung anhand von Taktiken

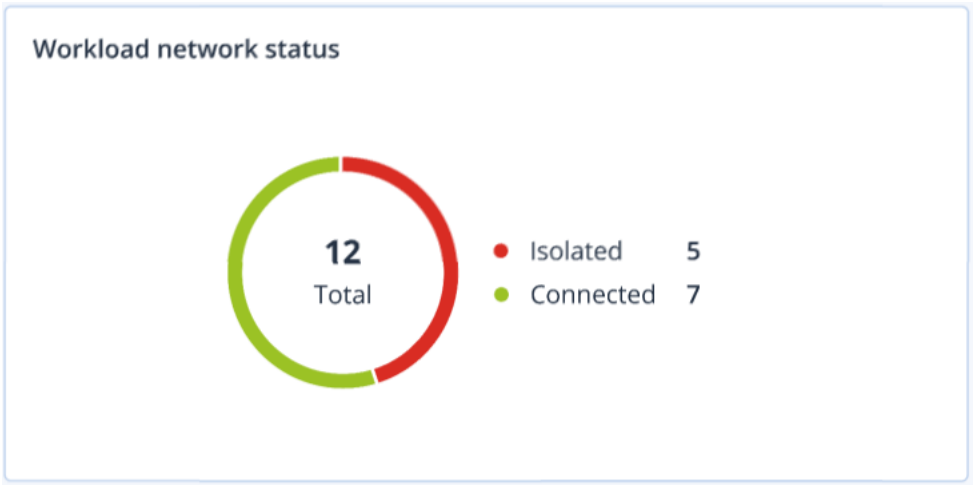
In diesem Widget wird angezeigt, wie oft bestimmte Angriffstechniken bei Vorfällen im ausgewählten Zeitraum aufgetreten sind.

Die grünen und roten Werte zeigen an, ob es (im Vergleich zum vorherigen Zeitraum) dabei zu einem Anstieg oder Abfall gekommen ist. Im unteren Beispiel ist es im Vergleich zum vorherigen Zeitraum zu einer Zunahme bei den Rechteausweitungs- und Command & Control-Angriffen gekommen. Dies kann ein Hinweis darauf sein, dass Ihre Credential Management-Lösung analysiert und die Sicherheit erhöht werden sollte.

Workload-Netzwerkstatus

Dieses Widget zeigt den aktuellen Netzwerkstatus für Ihre Workloads an und informiert darüber, wie viele Workloads isoliert und wie viele verbunden sind.

Klicken Sie auf den Wert 'Isoliert', damit Ihnen die Liste 'Workload mit Agenten' angezeigt wird (in der -Konsole unter dem Menü **Workloads**). Diese Liste ist so vorgefiltert, dass nur isolierte Workloads angezeigt werden. Wenn Sie auf den Wert 'Verbunden' klicken, wird die Liste 'Workload mit Agenten' angezeigt, die so gefiltert ist, dass die verbundenen Workloads angezeigt werden.



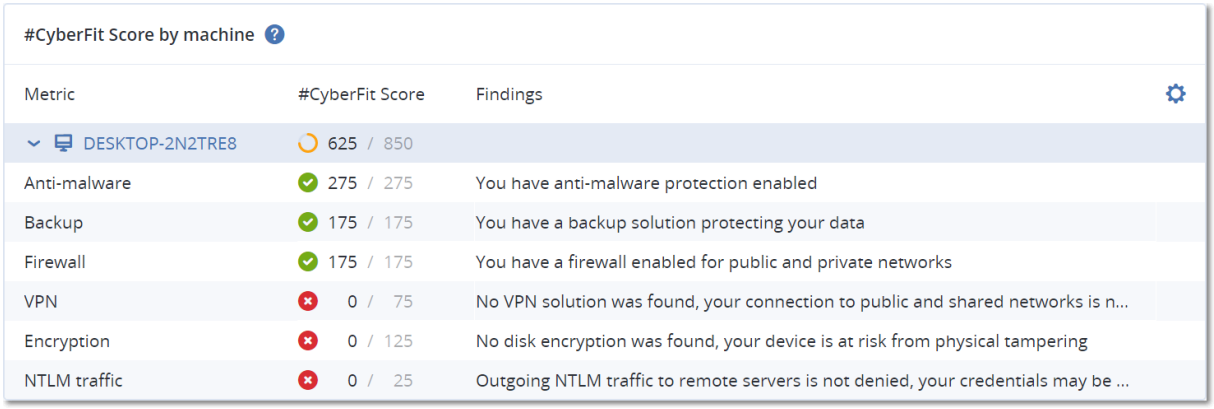
#CyberFit-Score pro Maschine

Dieses Widget zeigt für jede Maschine den #CyberFit-Gesamt-Score und die Einzel-Scores an, aus denen sich dieser Gesamtwert zusammensetzt – sowie die Ergebnisse für jede der bewerteten Metriken:

- Antimalware
- Backup
- Firewall
- VPN
- Verschlüsselung
- NTLM-Traffic

Wenn Sie den Score einer einzelnen Metrik verbessern wollen, können Sie die Empfehlungen einsehen, die in Form eines Berichts verfügbar sind.

Weitere Informationen über den #CyberFit-Score finden Sie im Abschnitt '#CyberFit-Score für Maschinen'.



Überwachung der Laufwerksintegrität

Die Überwachung der Laufwerksintegrität liefert Informationen über den aktuellen Laufwerksintegritätsstatus sowie eine Vorhersage über diesen. Dadurch können Sie Datenverluste vorab verhindern, die durch einen Laufwerksausfall verursacht werden könnten. Es werden sowohl Laufwerke vom Typ HDD (klassische Festplatten) als auch SSD (Flash-Speicher basierte Laufwerke) unterstützt.

Einschränkungen

- Die Vorhersage zur Laufwerksintegrität wird nur für Maschinen unterstützt, die unter Windows laufen.
- Es können nur Laufwerke von physischen Maschinen überwacht werden. Die Laufwerke von virtuellen Maschinen können nicht überwacht werden und werden daher auch nicht in den Laufwerksintegrität-Widgets angezeigt.
- RAID-Konfigurationen werden nicht unterstützt. Die Laufwerksintegrität-Widgets enthalten keine Informationen über Maschinen mit RAID-Implementierung.
- NVMe-SSDs werden nicht unterstützt.

Die Laufwerksintegrität wird durch folgende Statuszustände dargestellt:

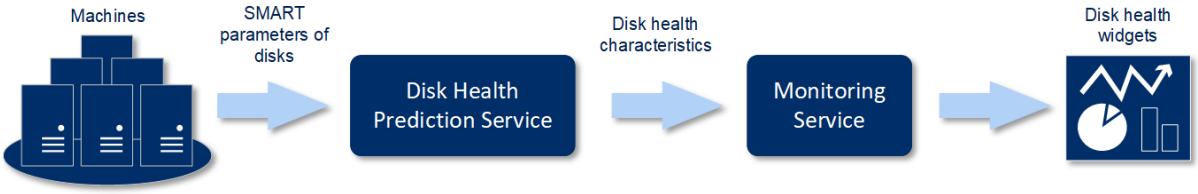
- **OK**
  Die Laufwerksintegrität liegt zwischen 70% und 100%.
- **Warnung**
  Die Laufwerksintegrität liegt zwischen 30% und 70%.
- **Kritisch**
  Die Laufwerksintegrität liegt zwischen 0% und 30%.
- **Laufwerksdaten werden berechnet**
  Der aktuelle Laufwerksstatus und die Vorhersage werden ermittelt.

Und so funktioniert es

Der Disk Health Prediction Service verwendet ein auf künstlicher Intelligenz (KI) basierendes Vorhersagemodell.

1. Der Protection Agent sammelt die SMART-Parameter der Laufwerke und übermittelt diese Daten an den Disk Health Prediction Service:
   - SMART 5 – Reallocated Sectors Count (Anzahl neu zugewiesener Sektoren).
   - SMART 9 – Power-On Hours (Einschaltzeit).
   - SMART 187 – Reported Uncorrectable Errors (Gemeldete unkorrigierbare Fehler).
   - SMART 188 – Command Timeout (Befehls-Timeout, wegen Zeitüberschreitung abgebrochene Befehle).
   - SMART 197 – Current Pending Sector Count (Anzahl derzeit ausstehender Sektoren).
   - SMART 198 – Offline Uncorrectable Sector Count (Anzahl nicht korrigierbarer Sektoren).
   - SMART 200 – Write Error Rate (Fehlerrate beim Schreiben).
2. Der Disk Health Prediction Service verarbeitet die empfangenen SMART-Parameter, trifft Vorhersagen und stellt dann folgende Laufwerksintegritätsmerkmale bereit:
   - Aktueller Laufwerksintegritätsstatus: OK, Warnung, Kritisch.
   - Vorhersage zur Laufwerksintegrität: negativ, stabil, positiv.
   - Vorhersage-Wahrscheinlichkeit der Laufwerksintegrität in Prozent.

   Der Vorhersagezeitraum beträgt ein Monat.
3. Der Monitoring Service empfängt diese Merkmale und zeigt die entsprechenden Informationen dann in den Laufwerksintegrität-Widgets der Cyber Protect-Konsole an.



Laufwerksintegrität-Widgets

Die Ergebnisse der Laufwerksintegritätsüberwachung werden in folgenden Widgets dargestellt, die in der Cyber Protect-Konsole verfügbar sind.

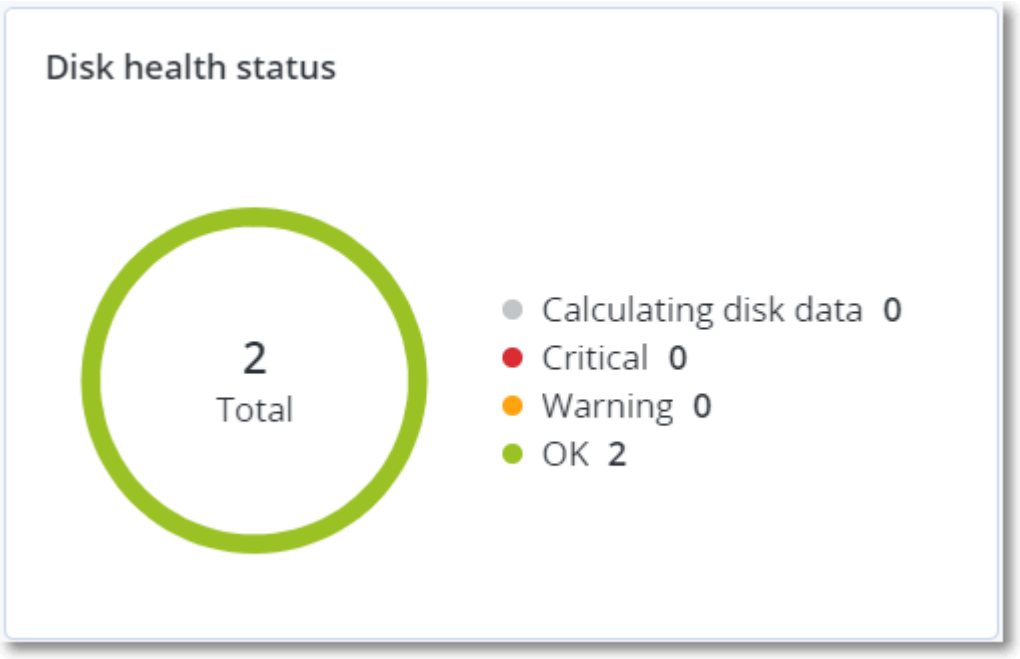
- **Überblick der Laufwerksintegrität** ist ein Treemap-Widget (Kacheldiagramm mit Baumstruktur) mit zwei Detailebenen, zwischen denen umgeschaltet werden kann.
  - Maschinenebene

    Zeigt zusammengefasste Informationen über den Laufwerksintegritätsstatus für die ausgewählten Kundenmaschinen an. Es werden nur die kritischsten Laufwerkstatuszustände angezeigt. Die anderen Statuszustände werden in einem Tooltip angezeigt, wenn Sie mit dem Mauszeiger über einen bestimmten Block fahren. Die Blockgröße der Maschine hängt von der Gesamtgröße aller Laufwerke dieser Maschine ab. Die Blockfarbe der Maschine hängt vom kritischsten Laufwerksstatus ab, der gefunden wurde.

- Laufwerksebene
  Zeigt den aktuellen Laufwerksintegritätsstatus aller Laufwerke für die ausgewählte Maschine an. Jeder Laufwerksblock zeigt eine der nachfolgenden Vorhersagen zur Laufwerksintegrität sowie die dazugehörige Wahrscheinlichkeit (in Prozent) an:
  - Wird heruntergestuft
  - Wird stabil bleiben

- Wird verbessert

- **Laufwerksintegritätsstatus** ist ein Kreisdiagramm-Widget, welches die Anzahl der Laufwerke für jeden Status anzeigt.



Alarmmeldungen zum Laufwerksintegritätsstatus

Die Laufwerksintegritätsprüfung wird alle 30 Minuten durchgeführt, während die entsprechende Alarmmeldung nur einmal täglich generiert wird. Wenn sich der Laufwerksintegritätsstatus von **Warnung** zu **Kritisch** ändert, wird immer ein Alarm generiert.

Alarmbezeichnung	Schweregrad	Laufwerksintegritätsstatus	Beschreibung
Laufwerksausfall ist möglich	Warnung	(30 – 70)	Das Laufwerk <Laufwerksname> auf dieser Maschine wird wahrscheinlich demnächst ausfallen. Sichern Sie das Laufwerk möglichst bald mit einem vollständigen Image-Backup. Bauen Sie dann ein Ersatzlaufwerk ein und stellen Sie das Image auf diesem wieder her.
Laufwerksausfall steht unmittelbar bevor	Kritisch	(0 – 30)	Das Laufwerk <Laufwerksname> auf dieser Maschine befindet sich in einem kritischen Zustand und wird höchstwahrscheinlich sehr bald ausfallen. Wir raten davon ab, jetzt noch ein Image-Backup des Laufwerks zu erstellen, da die zusätzliche Belastung zum endgültigen Laufwerksausfall führen könnte. Versuchen Sie, die wichtigsten Dateien auf dem Laufwerk umgehend zu sichern und es dann auszutauschen.

Data Protection-Karte

Hinweis
Diese Funktion ist über das Advanced Backup-Paket verfügbar.

Die Funktion 'Data Protection-Karte' ermöglicht es Ihnen, alle für Sie wichtigen Daten zu ermitteln sowie ausführliche Informationen über Anzahl, Größe, Speicherort und Sicherungsstatus aller

wichtigen Dateien in Form einer skalierbaren Treemap-Anzeige (Kacheldiagramm mit Baumstruktur) zu erhalten.

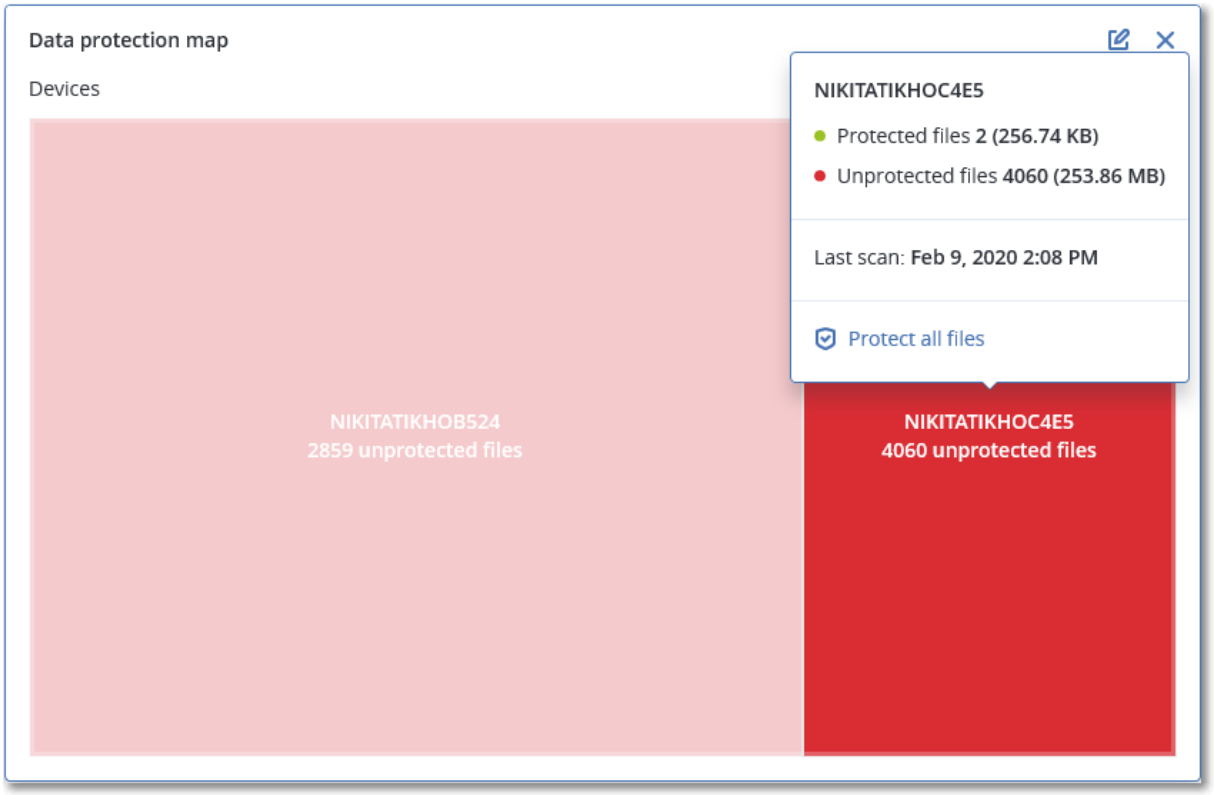
Jede Blockgröße hängt von der Gesamtzahl/Größe aller wichtigen Dateien ab, die zu einem Kunden/einer Maschine gehören.

Dateien können einen der folgenden Schutzstatus-Zustände haben:

- **Kritisch** – es gibt 1-20% ungeschützte Dateien mit den von Ihnen spezifizierten Erweiterungen, die für die/den ausgewählte(n) Maschine/Speicherort nicht per Backup gesichert wurden und mit den vorhandenen Backup-Einstellungen nicht gesichert werden.
- **Niedrig** – es gibt 21-50% ungeschützte Dateien mit den von Ihnen spezifizierten Erweiterungen, die für die/den ausgewählte(n) Maschine/Speicherort nicht per Backup gesichert wurden und mit den vorhandenen Backup-Einstellungen nicht gesichert werden.
- **Mittel** – es gibt 1-20% ungeschützte Dateien mit den von Ihnen spezifizierten Erweiterungen, die für die/den ausgewählte(n) Maschine/Speicherort nicht per Backup gesichert wurden und mit den vorhandenen Backup-Einstellungen nicht gesichert werden.
- **Hoch** – alle Dateien mit den von Ihnen spezifizierten Erweiterungen wurden für die/den ausgewählte(n) Maschine/Speicherort per Backup gesichert.

Alle Ergebnisse der Data Protection-Untersuchtung können auf dem Monitoring-Dashboard im Data Protection-Karten-Widget gefunden werden – einem Treemap-Widget, welches die Details auf Maschinenebene anzeigt:

- Maschinenebene – zeigt Informationen über den Schutzstatus wichtiger Dateien für die Maschinen des ausgewählten Kundens an.



Wenn Sie bisher noch ungesicherte Dateien schützen wollen, müssen Sie mit dem Mauszeiger über den Block fahren und dann auf den Befehl **Alle Dateien schützen** klicken. Im Dialogfenster finden Sie Informationen zur Anzahl der ungeschützten Dateien und zu deren Speicherort. Wenn Sie diese sichern wollen, klicken Sie auf **Alle Dateien schützen**.

Sie können außerdem einen ausführlichen Bericht im CSV-Format herunterladen.

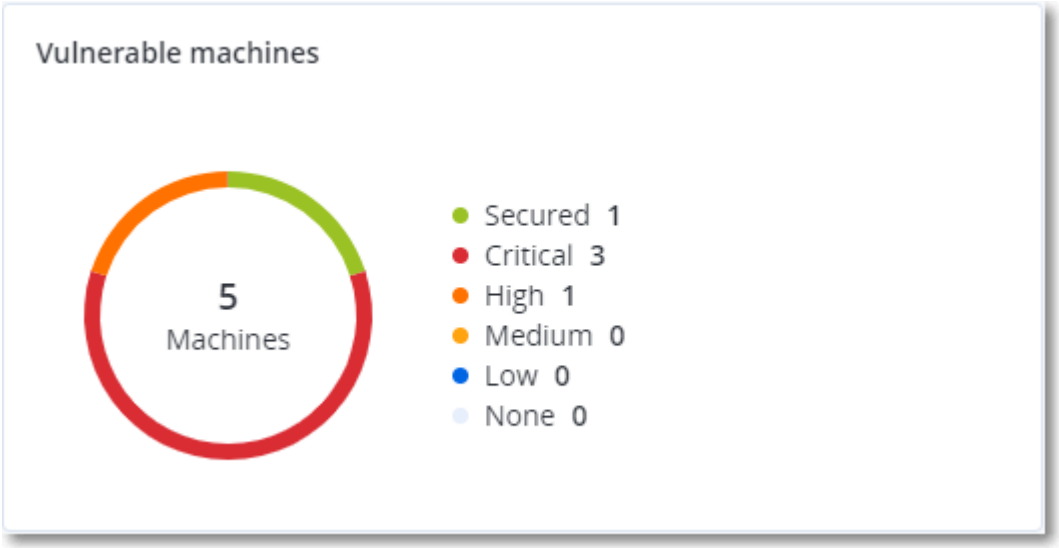
Widget für Schwachstellenbewertung

Verwundbare Maschinen

Dieses Widget zeigt die verwundbaren Maschinen nach dem Verwundbarkeitsgrad an.

Die gefundene Schwachstelle kann gemäß CVSS v3.0 (Common Vulnerability Scoring System) einen der folgenden Schweregrade haben:

- Gesichert: es wurden keine Schwachstellen gefunden
- Kritisch: 9.0 - 10.0 CVSS
- Hoch: 7.0 - 8.9 CVSS
- Mittel: 4.0 - 6.9 CVSS
- Niedrig: 0.1 - 3.9 CVSS
- Ohne: 0.0 CVSS

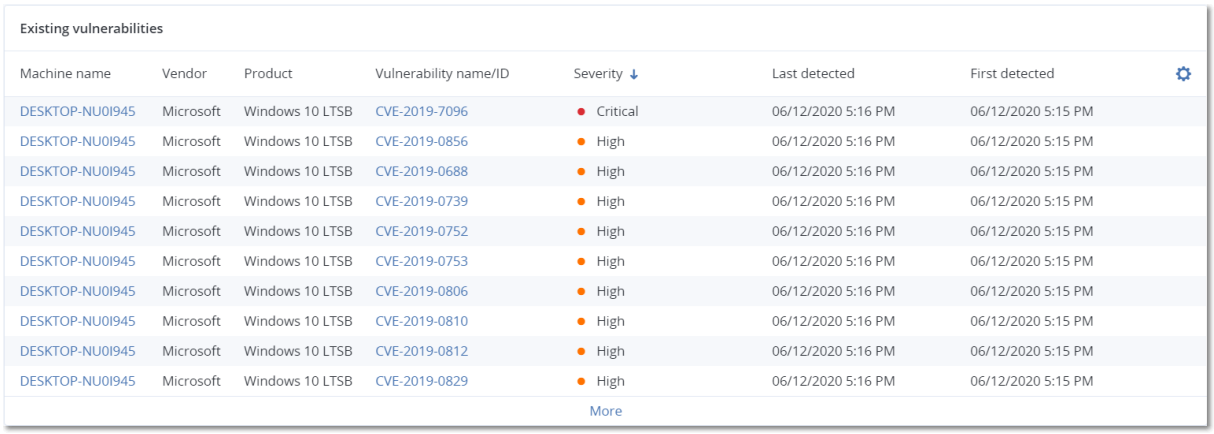


Vorhandene Schwachstellen

Dieses Widget zeigt die derzeit vorhandenen Schwachstellen auf Maschinen an. Im Widget **Vorhandene Schwachstellen** gibt es zwei Spalten mit Zeitstempeln:

- **Zuerst erkannt** – Datum und Uhrzeit, als die Schwachstelle erstmals auf der Maschine erkannt wurde.

- **Zuletzt erkannt** – Datum und Uhrzeit, als die Schwachstelle das letzte Mal auf der Maschine erkannt wurde.



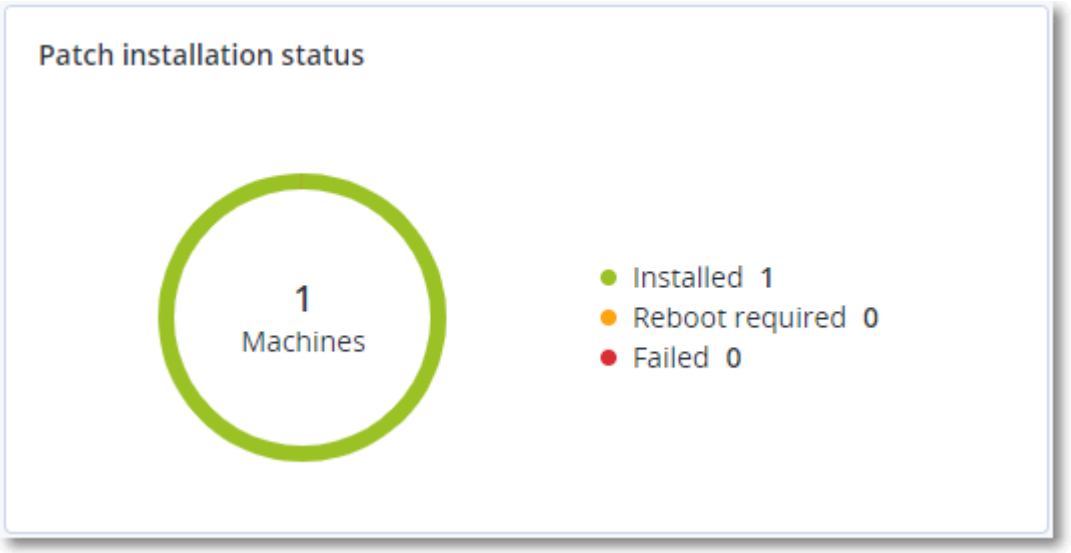
Widgets für Patch-Installation

Es gibt vier Widgets im Zusammenhang mit der Patch-Verwaltungsfunktionalität.

Status der Patch-Installation

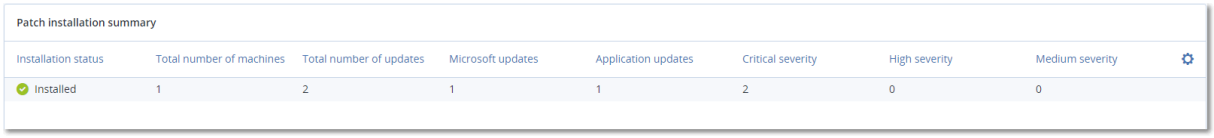
Dieses Widget zeigt die Anzahl der Maschinen gruppiert nach dem Status des Patch-Installation an.

- **Installiert** – alle verfügbaren Patches sind auf einer Maschine installiert
- **Neustart erforderlich** – nach einer Patch-Installation muss eine Maschine neu gestartet werden
- **Fehlgeschlagen** – die Patch-Installation ist auf einer Maschine fehlgeschlagen



Übersicht der Patch-Installation

Dieses Widget zeigt eine Übersicht der Patches auf den Maschinen an, gruppiert nach dem Status des Patch-Installation.



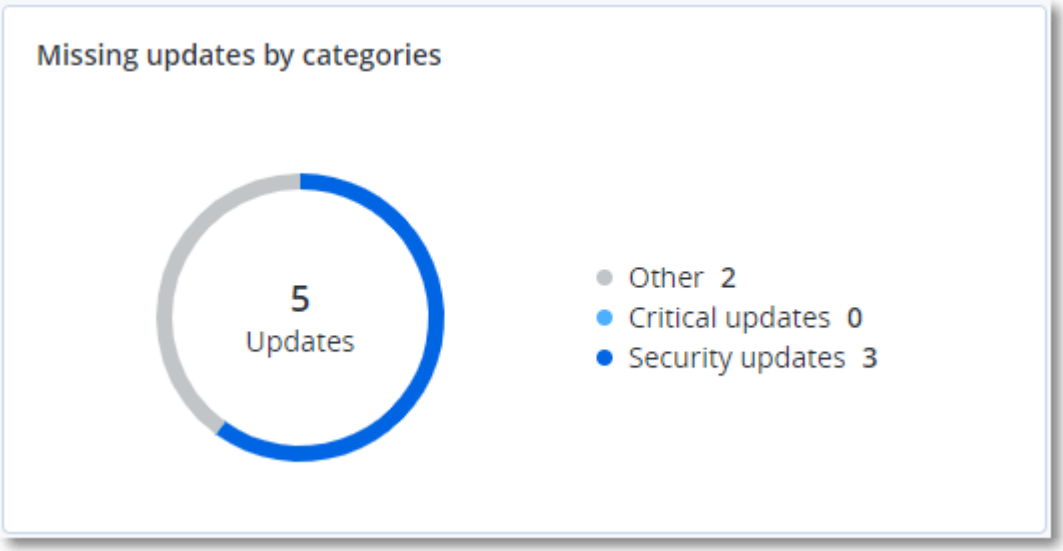
Verlauf der Patch-Installation

Dieses Widget zeigt ausführliche Informationen über die Patches auf den Maschinen an.

Fehlende Updates nach Kategorie

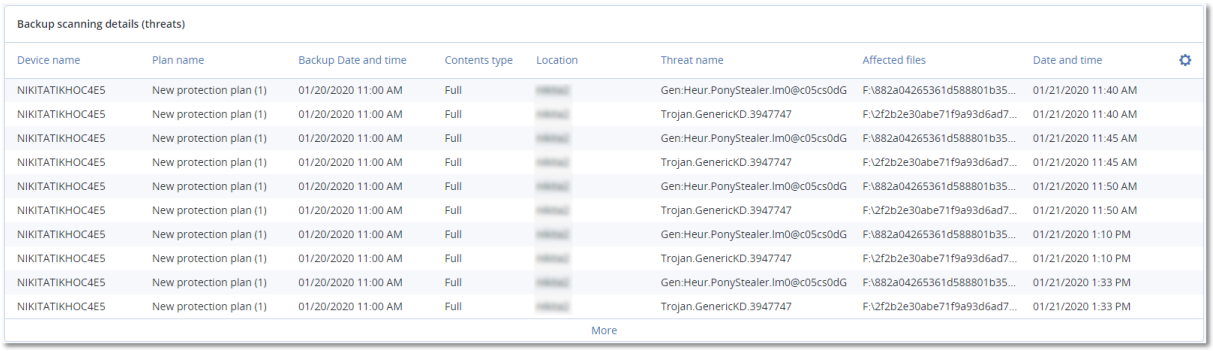
Dieses Widget zeigt die Anzahl der fehlenden Updates nach Kategorie an. Folgende Kategorien werden angezeigt:

- Sicherheitsupdates
- Kritische Updates
- Anderer



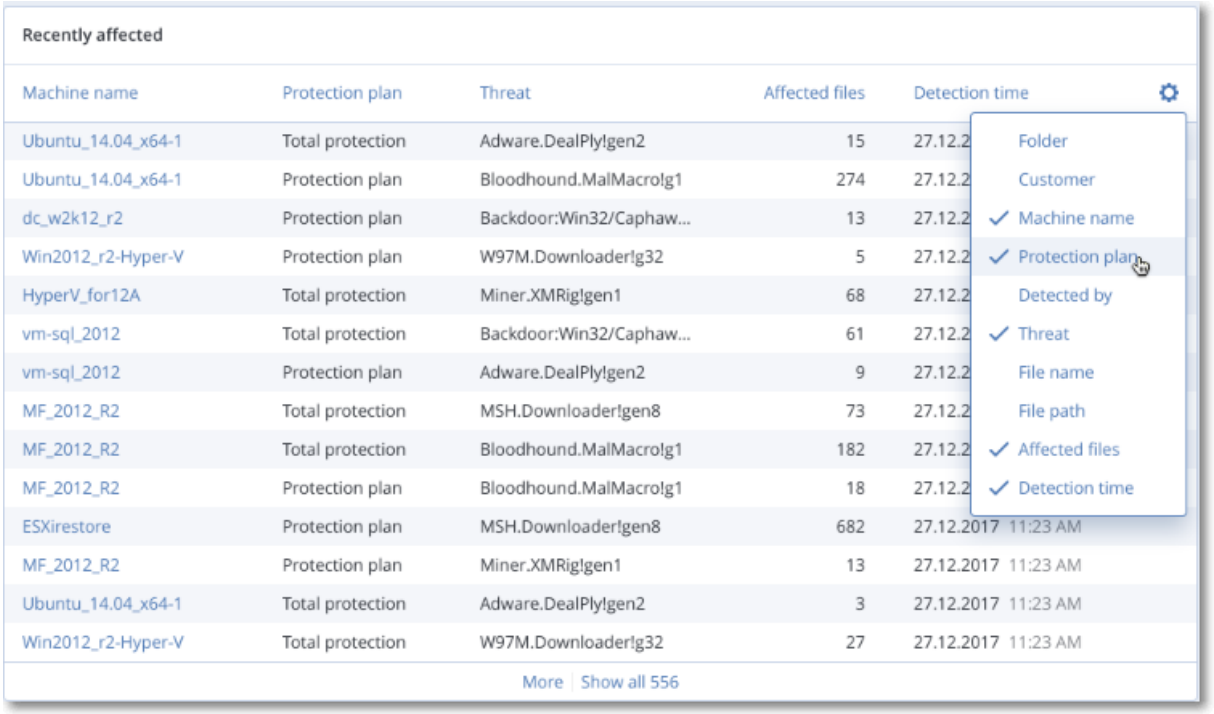
Backup-Scanning-Details

Dieses Widget zeigt ausführliche Informationen über erkannte Bedrohungen in den Backups an.



Kürzlich betroffen

Dieses Widget zeigt detaillierte Informationen über Workloads an, die von Bedrohungen wie Viren, Malware und Ransomware betroffen waren. Sie können hier Informationen über die erkannten Bedrohungen, den Zeitpunkt der Erkennung sowie die Anzahl der betroffenen Dateien finden.



Daten für kürzlich betroffene Workloads herunterladen

Sie können die Daten für kürzlich betroffene Workloads herunterladen, eine CSV-Datei generieren und diese dann an die von Ihnen spezifizierten Empfänger senden.

So laden Sie die Daten für kürzlich betroffene Workloads herunter

1. Klicken Sie im Widget **Kürzlich betroffen** auf den Befehl **Daten herunterladen**.
2. Geben Sie im Feld **Zeitraum** die Anzahl der Tage ein, für die Sie Daten herunterladen wollen. Die maximale Anzahl der Tage, die Sie eingeben können, beträgt 200.

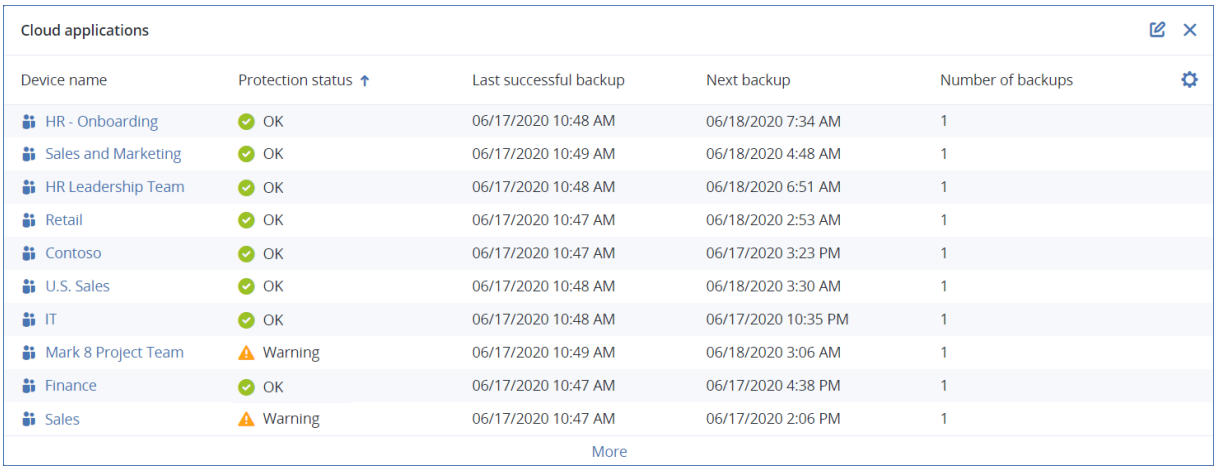
3. Geben Sie im Feld **Empfänger** die E-Mail-Adressen aller Personen ein, die eine E-Mail mit einem Link zum Herunterladen der CSV-Datei erhalten sollen.
4. Klicken Sie auf **Download**.

   Das System beginnt dann damit, die CSV-Datei mit den Daten für diejenigen Workloads zu generieren, die in dem von Ihnen spezifizierten Zeitraum betroffen waren. Wenn die CSV-Datei vollständig ist, sendet das System eine E-Mail an die Empfänger. Jeder Empfänger kann dann diese CSV-Datei herunterladen.

Cloud-Applikationen

Dieses Widget zeigt ausführliche Informationen über Cloud-zu-Cloud-Ressourcen an:

- Microsoft 365-Benutzer (Postfach, OneDrive)
- Microsoft 365-Gruppen (Postfach, Gruppen-Website)
- Öffentliche Microsoft 365-Ordner
- Microsoft 365-Website-Sammlungen
- Microsoft 365-Teams
- Google Workspace-Benutzer (Gmail, Google Drive)
- Google Workspace Shared Drives



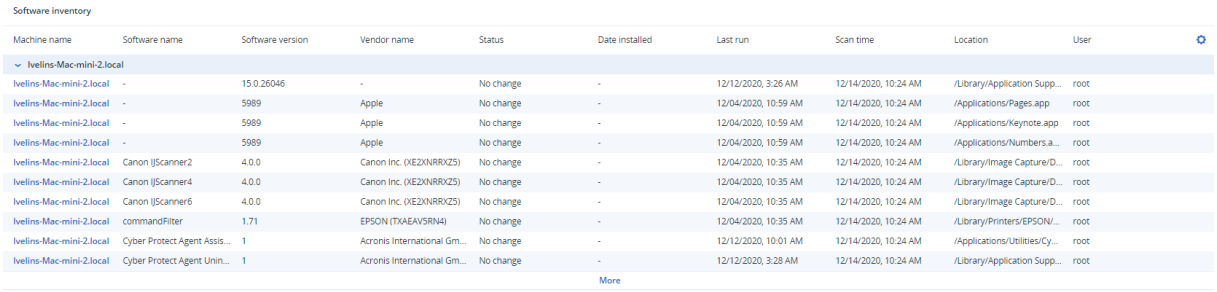
Weitere Informationen über Cloud-zu-Cloud-Ressourcen sind auch in folgenden Widgets verfügbar:

- Aktivitäten
- Aktivitätsliste
- 5 neueste Alarmmeldungen
- Alarmverlauf
- Aktive Alarmmeldungen – Übersicht
- Übersicht der historischen Alarmmeldungen

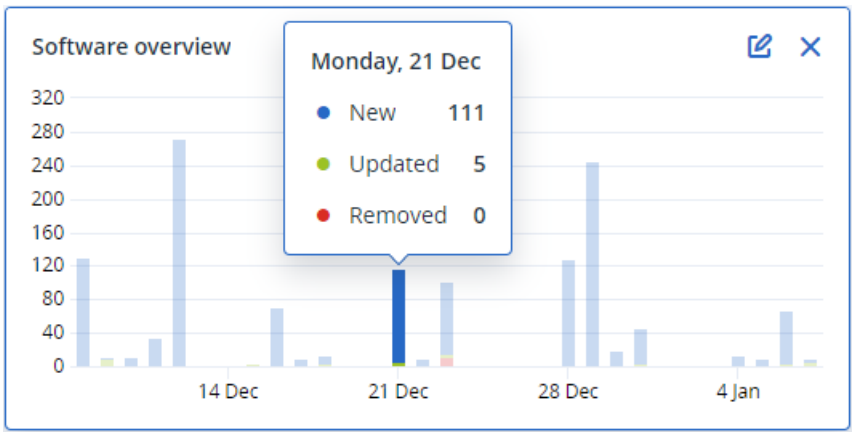
- Details 'Aktiver Alarm'
- Speicherorteübersicht

Widgets für Software-Inventarisierung

Das Tabellen-Widget **Software-Inventarisierung** zeigt ausführliche Informationen über die gesamte Software an, die auf den physischen Windows- und macOS-Geräten in Ihrem Unternehmen installiert ist.



Das Widget **Software-Überblick** zeigt die Anzahl der neuen, aktualisierten oder gelöschten Applikationen auf Windows- und macOS-Maschinen in Ihrem Unternehmen für einen spezifizierten Zeitraum (7 Tage, 30 Tage oder den aktuellen Monat) an.



Wenn Sie den Mauszeiger über einen bestimmten Balken im Diagramm halten, wird ein Tooltip mit folgenden Informationen angezeigt:

Neu – die Anzahl der neu installierten Applikationen.

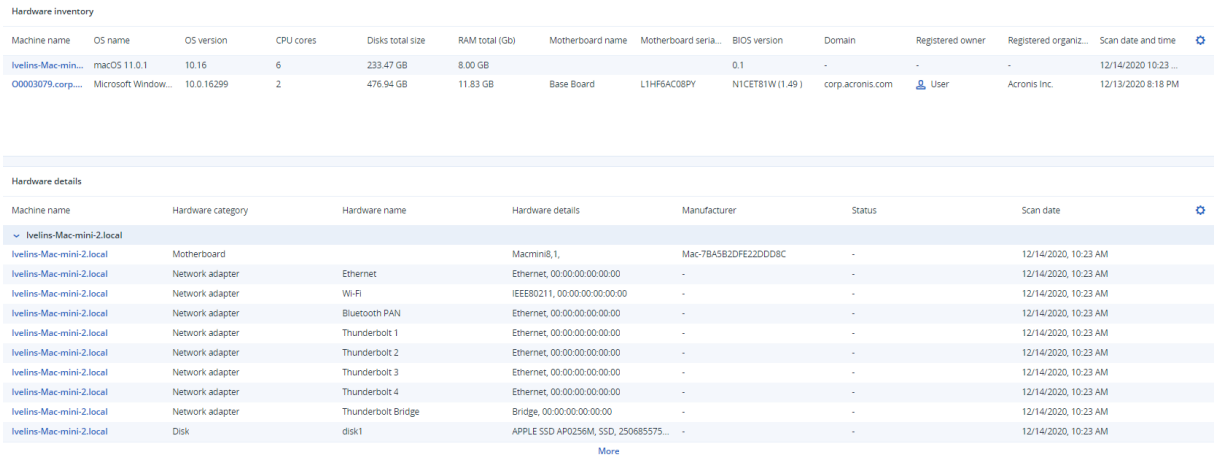
Aktualisiert – die Anzahl der aktualisierten Applikationen.

Entfernt – die Anzahl der entfernten Applikationen.

Wenn Sie auf den Balkenteil für einen bestimmten Status klicken, werden Sie zur Seite **Software-Verwaltung** –> **Software-Inventarisierung** weitergeleitet. Die Informationen auf dieser Seite werden nach dem entsprechenden Datum und Status gefiltert.

Widgets für Hardware-Inventarisierung

Die Tabellen-Widgets **Hardware-Inventarisierung** und **Hardware-Details** zeigen Informationen über alle Hardware an, die von den physischen und virtuellen Windows- sowie macOS-Geräten in Ihrem Unternehmen verwendet wird.



Hardware inventory

Machine name	OS name	OS version	CPU cores	Disks total size	RAM total (Gb)	Motherboard name	Motherboard seria...	BIOS version	Domain	Registered owner	Registered organiz...	Scan date and time
Ivelins-Mac-min...	macOS 11.0.1	10.16	6	233.47 GB	8.00 GB			0.1	-	-	-	12/14/2020 10:23 ...
O0003079.corp....	Microsoft Window...	10.0.16299	2	476.94 GB	11.83 GB	Base Board	L1HF6AC08PY	N1CET81W (1.49)	corp.acronis.com	User	Acronis Inc.	12/13/2020 8:18 PM

Hardware details

Machine name	Hardware category	Hardware name	Hardware details	Manufacturer	Status	Scan date
Ivelins-Mac-mini-2.local						
Ivelins-Mac-mini-2.local	Motherboard		Macmini8,1,	Mac-7BA5B2DFE22DDD8C	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Ethernet	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Wi-Fi	IEEE80211, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Bluetooth PAN	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt 1	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt 2	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt 3	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt 4	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt Bridge	Bridge, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Disk	disk1	APPLE SSD AP0256M, SSD, 250685575...	-	-	12/14/2020, 10:23 AM

More

Das Tabellen-Widget **Hardware-Änderungen** zeigt Informationen über hinzugefügte, entfernte oder geänderte Hardware auf physischen und virtuellen Windows- sowie macOS-Geräten in Ihrem Unternehmen für einen spezifizierten Zeitraum (7 Tage, 30 Tage oder den aktuellen Monat) an.

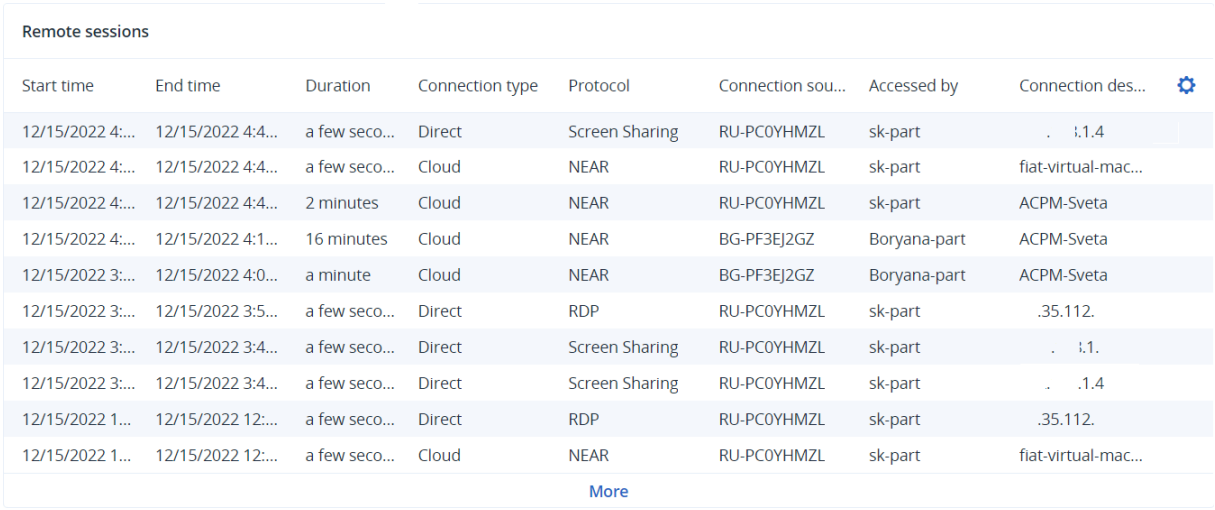
Hardware changes

Machine name	Hardware category	Status	Old value	New value	Modification date and time
DESKTOP-0FF9TTF					
DESKTOP-0FF9TTF	Network adapter	Changed	Oracle Corporation, Ethernet 802.3,...	Oracle Corporation, Ethernet 802.3, ...	01/11/2021 9:28 AM
DESKTOP-0FF9TTF	Network adapter	New	-	Realtek Semiconductor Corp., Ether...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Motherboard	New	-	LENOVO, Torronto 5C1, PF0PJB10	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	GPU	New	-	Intel(R) HD Graphics Family	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Disk	New	-	(Standard disk drives), WDC WD10JP...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Network adapter	New	-	Cisco Systems, Ethernet 802.3, 00:0...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Network adapter	New	-	Oracle Corporation, Ethernet 802.3, ...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	RAM	New	-	Samsung, 985D7122, 4.00 GB	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Network adapter	New	-	TAP-NordVPN Windows Provider V9...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	RAM	New	-	Micron, 00000000, 4.00 GB	01/04/2021 2:37 PM

More

Das Widget 'Remote-Sitzungen'

Dieses Widget zeigt detaillierte Informationen über die Remote-Desktop- und Dateiübertragungssitzungen an.



Smart Protection

Bedrohungsfeed

Das Acronis Cyber Protection Operations Center (CPOC) generiert Sicherheitsalarmmeldungen, die nur zu entsprechenden geographischen Regionen gesendet werden. Diese Sicherheitsmeldungen liefern Informationen über Malware, Schwachstellen, Naturkatastrophen, zu relevanten Aspekten der öffentlichen Gesundheit und anderen Arten von globalen Ereignissen, die Ihre Data Protection beeinträchtigen können. Der Bedrohungsfeed informiert Sie über potenzielle Bedrohungen und ermöglicht Ihnen so, diese abzuwenden.

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

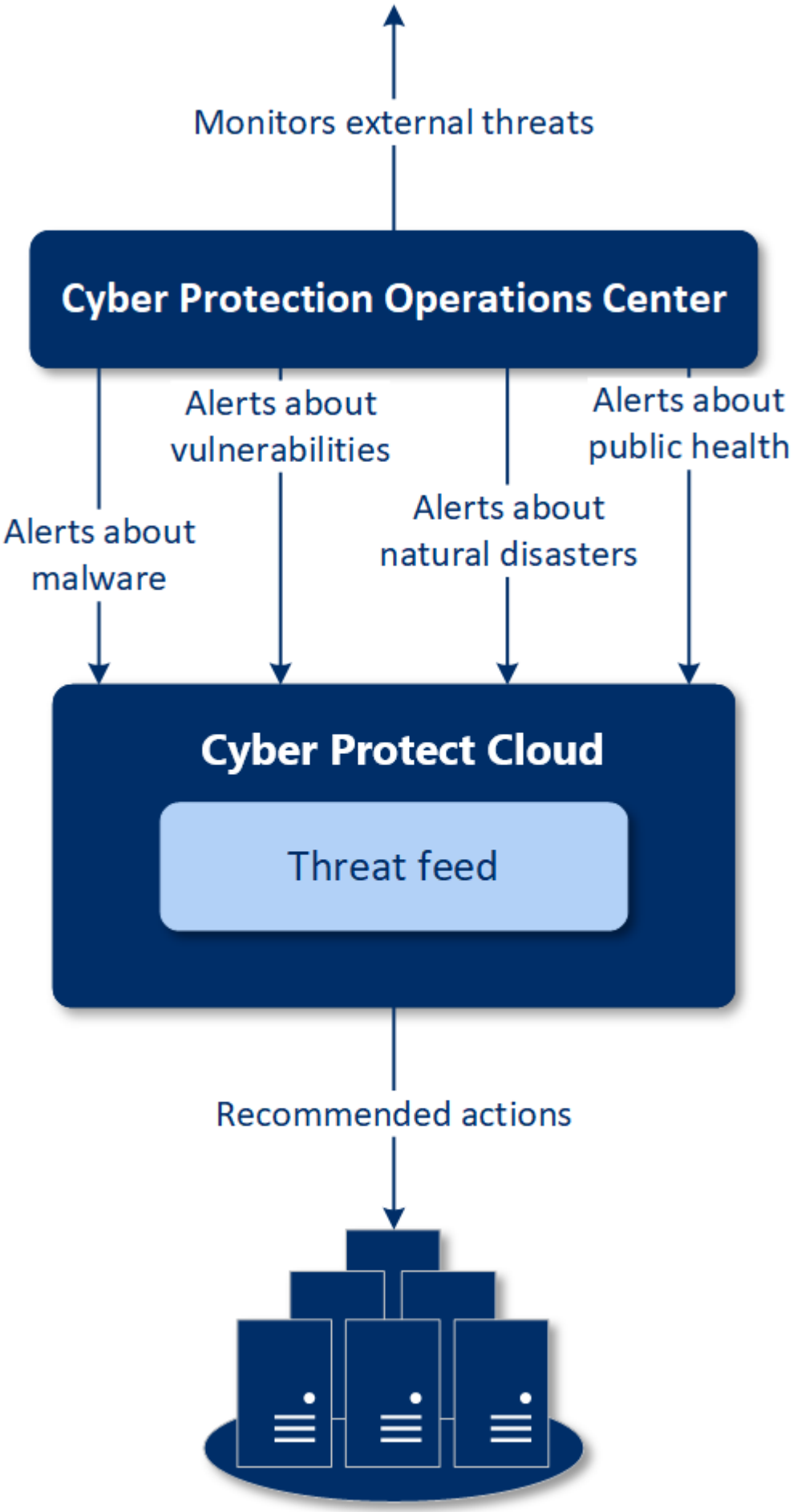
Einige Sicherheitsalarmmeldungen können durch eine Reihe spezifischer Aktionen behoben werden, die von entsprechenden Sicherheitsexperten bereitgestellt werden. Einige Alarmmeldungen dienen nur dazu, Sie über die bevorstehenden Bedrohungen zu informieren, ohne dass empfohlene Aktionen verfügbar sind.

Hinweis
Malware-Alarmmeldungen werden nur für Maschinen generiert, auf denen der Agent für die Antimalware Protection installiert ist.

Und so funktioniert es

Das Acronis Cyber Protection Operations Center überwacht externe Bedrohungen und generiert Alarmmeldungen zu Malware-Angriffen, auftauchenden Schwachstellen, natürlichen Desastern oder relevanten Gefährdungen der öffentlichen Gesundheit. Sie können all diese Alarmmeldungen im Bereich **Bedrohungsfeed** der Cyber Protect-Konsole einsehen. Abhängig von der Art des Alarms können Sie empfohlene Aktionen zur Behebung des Problems durchführen.

Der Hauptablauf des Bedrohungsfeeds ist in der nachfolgenden Abbildung dargestellt.



Gehen Sie folgendermaßen vor, um bei einem Alarm, den Sie über das Acronis Cyber Protection Operations Center empfangen haben, die empfohlenen Aktionen durchzuführen:

1. Gehen Sie in der Cyber Protect-Konsole zu **Monitoring** –> **Bedrohungsfeed**, um dort nach vorhandenen Sicherheitsalarmmeldungen zu schauen.
2. Wählen Sie einen Alarm aus der Liste aus und lassen Sie sich die bereitgestellten Details anzeigen.
3. Klicken Sie auf **Start**, um den Assistenten zu starten.
4. Aktivieren Sie die Aktionen, die Sie ausführen wollen, und wählen Sie die Maschinen aus, auf die diese Aktionen angewendet werden sollen. Folgende Aktionen können vorgeschlagen werden:
   - **Schwachstellenbewertung** – um die Maschinen nach Schwachstellen scannen zu lassen
   - **Patch-Verwaltung** – um auf den ausgewählten Maschinen Patches zu installieren
   - **Antimalware Protection** – um auf den ausgewählten Maschinen vollständige Scans auszuführen

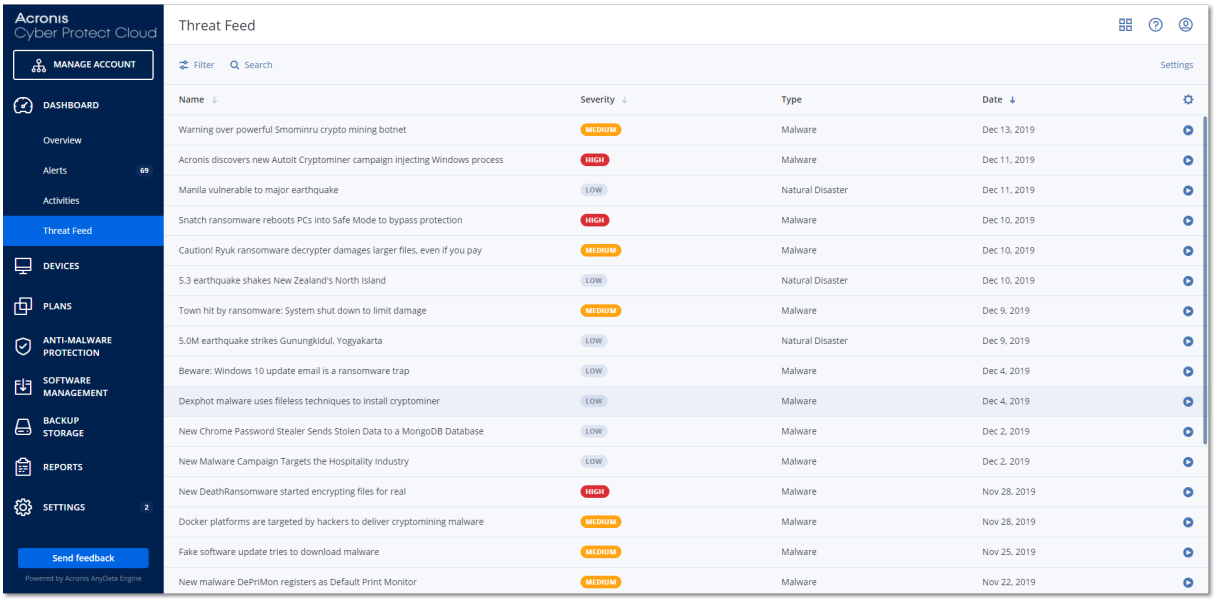
     Hinweis
     Diese Aktion ist nur für Maschinen verfügbar, auf denen der Agent für die Antimalware Protection installiert ist.

   - **Backup von geschützten oder ungeschützten Maschinen** – um geschützte und ungeschützte Workloads per Backup zu sichern
     Wenn es noch keine Backups für den Workload gibt (an allen verfügbaren Speicherorten - in der Cloud und lokal) oder die vorhandenen Backups verschlüsselt sind, wird das System ein vollständiges Backup mit folgendem Namensformat erstellen:

     ```
     %workload_name%-Remediation
     ```

     Das standardmäßige Backup-Ziel ist der Cyber Protect Cloud Storage. Sie können aber auch einen anderen Speicherort konfigurieren, bevor Sie die Aktion starten.

     Wenn es bereits ein nicht verschlüsseltes Backup gibt, wird das System ein inkrementelles Backup in dem vorhandenen Archiv erstellen.
5. Klicken Sie auf **Start**.
6. Überprüfen Sie auf der Registerkarte **Aktivitäten**, dass die entsprechende Aktivität erfolgreich durchgeführt wurde.



Alle Alarmmeldungen löschen

Nach folgenden Zeiträumen wird der Bedrohungsfeed automatisch bereinigt:

- Natürliche Disaster – 1 Woche
- Schwachstellen – 1 Monat
- Malware – 1 Monat
- Öffentliche Gesundheit – 1 Woche

Data Protection-Karte

Die Funktionalität 'Data Protection-Karte' bietet Ihnen folgende Möglichkeiten:

- Ausführliche Informationen über die auf Ihren Maschinen gespeicherten Daten (Klassifizierung, Speicherorte, Sicherungsstatus und weitere Informationen) zu erhalten.
- Zu ermitteln, ob Daten geschützt sind oder nicht. Daten werden als 'geschützt' angesehen, wenn diese per Backup (über einen Schutzplan mit aktiviertem Backup-Modul) gesichert wurden.
- Data Protection-Aktionen durchzuführen.

Und so funktioniert es

1. Zuerst müssen Sie einen Schutzplan erstellen, in dem das Modul Data Protection-Karte aktiviert ist.
2. Nachdem dieser Plan ausgeführt wurde und Ihre Daten erkannt und analysiert wurden, erhalten Sie im Widget Data Protection-Karte eine visuelle Darstellung der Data Protection-Analyse.
3. Alternativ können Sie auch zu **Geräte** –> **Data Protection-Karte** gehen, wo Ihnen Informationen über ungeschützte Dateien pro Gerät angezeigt werden.
4. Sie können Aktionen vornehmen, um die ungeschützten Dateien, die auf den Geräten gefunden wurden, zu schützen.

Erkannte ungeschützte Dateien verwalten

Gehen Sie folgendermaßen vor, um wichtige Dateien, die als ungeschützt erkannt wurden, zu sichern:

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte** –> **Data Protection-Karte**.
   Sie können in der Geräteliste allgemeine Informationen über die Anzahl der ungeschützten Dateien, deren Größe pro Gerät und über die letzte Datenerkennung finden.
   Wenn Sie die Dateien auf einer bestimmten Maschine sichern wollen, müssen Sie auf das Drei-Punkte-Symbol klicken und dann auf den Befehl **Alle Dateien schützen**. Sie werden zur Liste der Pläne weitergeleitet, wo Sie einen Schutzplan mit aktiviertem Backup-Modul erstellen können.
   Wenn Sie ein bestimmtes Gerät mit ungeschützten Dateien aus der Liste enfernen wollen, klicken Sie auf **Bis zur nächsten Datenerkennung verbergen**.
2. Wenn Sie ausführlichere Informationen über die ungeschützten Dateien auf einem bestimmten Gerät erhalten wollen, klicken Sie auf den Namen des entsprechenden Gerätes.
   Ihnen wird eine Liste mit ungeschützten Dateien angezeigt – aufgeschlüsselt nach Erweiterungen und Speicherort. Sie können im Suchfeld die Erweiterungen eingeben, für die Sie Informationen über ungeschützte Dateien erhalten wollen.
3. Wenn Sie alle ungeschützten Dateien sichern wollen, klicken Sie auf **Alle Dateien schützen**. Sie werden zur Liste der Pläne weitergeleitet, wo Sie einen Schutzplan mit aktiviertem Backup-Modul erstellen können.

Wenn Sie die Informationen über die ungeschützten Dateien in Form eines Berichts erhalten wollen, können Sie auf den Befehl **Ausführlichen Bericht im CSV-Format herunterladen** klicken.

Einstellungen für die Data Protection-Karte

Eine Anleitung zum Erstellen eines Schutzplans mit aktiviertem Modul für die Data Protection-Karte finden Sie im Abschnitt 'Einen Schutzplan erstellen'.

Für das Data Protection-Karten-Modul können folgende Einstellungen spezifiziert werden:

Planung

Sie können verschiedene Einstellungen für einen Zeitplan definieren, auf dessen Basis der Task für die Data Protection-Karte ausgeführt wird.

Feld	Beschreibung
Die Task-Ausführung auf Basis folgender Ereignisse planen	Diese Einstellung definiert, wann der Task ausgeführt werden soll. Folgende Werte sind verfügbar: • **Planung nach Zeit** – Dies ist die Standardeinstellung. Der Task wird gemäß der spezifizierten Zeit ausgeführt. • **Wenn sich ein Benutzer am System anmeldet** – Die Task-

Feld	Beschreibung
	Ausführung wird standardmäßig durch die Anmeldung eines (beliebigen) Benutzers ausgelöst. Sie können diese Einstellung so ändern, dass nur ein bestimmtes Benutzerkonto den Task auslösen kann. • **Wenn sich ein Benutzer vom System abmeldet** – Die Task-Ausführung wird standardmäßig durch die Abmeldung eines (beliebigen) Benutzers ausgelöst. Sie können diese Einstellung so ändern, dass nur ein bestimmtes Benutzerkonto den Task auslösen kann. **Hinweis** Der Task wird daher nicht beim Herunterfahren des Systems ausgeführt. Herunterfahren und Abmelden sind unterschiedliche Ereignisse in der Planungskonfiguration. • **Beim Systemstart** – Der Task wird ausgeführt, wenn das Betriebssystem startet. • **Beim Herunterfahren des Systems** – Der Task wird ausgeführt, wenn das Betriebssystem herunterfährt.
Planungstyp	Das Feld wird angezeigt, wenn Sie bei **Die Task-Ausführung auf Basis folgender Ereignisse planen** die Option **Planung nach Zeit** gewählt haben. Folgende Werte sind verfügbar: • **Monatlich** – Wählen Sie die Monate und dann die jeweiligen Wochen oder Tage des Monats, in denen der Task ausgeführt werden soll. • **Täglich** – Dies ist die Standardeinstellung. Wählen Sie die Wochentage aus, an denen der Task ausgeführt werden soll. • **Stündlich** – Wählen Sie die Wochentage, die Anzahl der Wiederholungen sowie das Zeitintervall aus, in dem der Task ausgeführt werden soll.
Starten um	Das Feld wird angezeigt, wenn Sie bei **Die Task-Ausführung auf Basis folgender Ereignisse planen** die Option **Planung nach Zeit** gewählt haben. Bestimmen Sie den genauen Zeitpunkt, an dem der Task ausgeführt werden soll.
Innerhalb eines Zeitraums ausführen	Das Feld wird angezeigt, wenn Sie bei **Die Task-Ausführung auf Basis folgender Ereignisse planen** die Option **Planung nach Zeit** gewählt haben. Bestimmten Sie einen Datumsbereich, innerhalb dessen die konfigurierte Planung gültig sein soll.

Feld	Beschreibung
Spezifizieren Sie einen Benutzer, dessen Anmeldung am Betriebssystem einen Task auslösen wird	Das Feld wird angezeigt, wenn Sie bei **Die Task-Ausführung auf Basis folgender Ereignisse planen** die Option **Wenn sich ein Benutzer am System anmeldet** gewählt haben. Folgende Werte sind verfügbar: • **Jeder Benutzer** – Verwenden Sie diese Option, wenn Sie wollen, dass der Task durch die Anmeldung eines beliebigen Benutzers ausgelöst wird. • **Der folgende Benutzer** – Verwenden Sie diese Option, wenn Sie wollen, dass der Task nur durch die Anmeldung eines bestimmten Benutzerkontos ausgelöst wird.
Spezifizieren Sie einen Benutzer, dessen Abmeldung vom Betriebssystem einen Task auslösen wird	Das Feld wird angezeigt, wenn Sie bei **Die Task-Ausführung auf Basis folgender Ereignisse planen** die Option **Wenn sich ein Benutzer vom System abmeldet** gewählt haben. Folgende Werte sind verfügbar: • **Jeder Benutzer** – Verwenden Sie diese Option, wenn Sie wollen, dass der Task durch die Abmeldung eines beliebigen Benutzers ausgelöst wird. • **Der folgende Benutzer** – Verwenden Sie diese Option, wenn Sie wollen, dass der Task nur durch die Abmeldung eines bestimmten Benutzerkontos ausgelöst wird.
Startbedingungen	Definieren Sie alle Bedingungen, die gleichzeitig zutreffen müssen, damit der Task ausgeführt werden kann. Die Startbedingungen für Antimalware-Scans sind ähnlich wie die Startbedingungen für das **Backup-Modul**, die wiederum im Abschnitt 'Startbedingungen' beschrieben sind. Sie können folgende zusätzliche Startbedingungen definieren: • **Task-Startzeit innerhalb eines Zeitfensters verteilen**– Diese Option ermöglicht es Ihnen, einen Zeitrahmen für den Task festzulegen, um Netzwerkengpässe zu vermeiden. Sie können die Verzögerung in Stunden oder Minuten spezifizieren. Wenn beispielsweise die Standardstartzeit 10:00 Uhr morgens ist und die Verzögerung 60 Minuten beträgt, dann beginnt der Task zwischen 10:00 und 11:00 Uhr morgens. • **Task bei Neustart der Maschine ausführen, wenn die Maschine zur geplanten Zeit ausgeschaltet war** • **Standby- oder Ruhezustandsmodus während der Task-Ausführung verhindern** – Diese Option gilt nur für Maschinen, die unter Windows laufen. • **Wenn die Startbedingungen nicht erfüllt sind, Task trotzdem ausführen nach** – Spezifizieren Sie einen Zeitraum, nach dem der

Feld	Beschreibung
	Task unabhängig von anderen Startbedingungen auf jeden Fall gestartet werden soll. **Hinweis** Für Linux werden keine Startbedingungen unterstützt.

Erweiterungen und Ausnahmeregeln

Auf der Registerkarte **Erweiterungen** können Sie eine Liste von Dateierweiterungen definieren, die bei der Datenerkennung als wichtig betrachtet und auf ihren Schutzstatus hin überprüft werden. Verwenden Sie folgendes Format, um die Erweiterungen zu definieren:

```
.html, .7z, .docx, .zip, .pptx, .xml
```

Auf der Registerkarte **Ausnahmeregeln** können Sie definieren, welche Dateien und Ordner bei der Datenerkennung nicht auf ihren Sicherungsstatus hin überprüft werden sollen.

- **Versteckte Dateien und Ordner** – wenn diese Option ausgewählt ist, werden versteckte Dateien/Ordner bei der Datenerkennung übersprungen.
- **Systemdateien und Systemordner** – wenn diese Option ausgewählt ist, werden Dateien/Ordner, die das Attribut 'System' haben, bei der Datenerkennung übersprungen.

Die Registerkarte 'Aktivitäten'

Die Registerkarte **Aktivitäten** bietet einen Überblick über die Aktivitäten der letzten 90 Tage.

So können Sie Aktivitäten auf dem Dashboard filtern

1. Spezifizieren Sie im Feld **Gerätename** die Maschine, auf welcher die Aktivität ausgeführt wird.
2. Wählen Sie im Listenfeld **Status** den gewünschten Status aus. Zum Beispiel: erfolgreich, fehlgeschlagen, wird ausgeführt, abgebrochen.
3. Wählen Sie im Listenfeld **Remote-Aktionen** die gewünschte Aktion aus. Zum Beispiel: Plan anwenden, Backups löschen, Software-Updates installieren.
4. Legen Sie im Feld **Neueste** den Zeitraum für die Aktivitäten fest. Zum Beispiel: die jüngsten Aktivitäten, die Aktivitäten der letzten 24 Stunden oder die Aktivitäten während eines bestimmten Zeitraums innerhalb der letzten 90 Tage.
5. Wenn Sie als Partner-Administrator auf die Registerkarte **Aktivitäten** zugreifen, können Sie die Aktivitäten für einen bestimmten Kunden filtern, den Sie verwalten.

Wenn Sie die Darstellung der Registerkarte **Aktivitäten** anpassen wollen, können Sie auf das Zahnradsymbol klicken und dann die Spalten auswählen, die angezeigt werden sollen. Wenn Sie den Aktivitätsfortschritt in Echtzeit sehen wollen, aktivieren Sie das Kontrollkästchen **Automatisch aktualisieren**.

Wenn Sie eine laufende Aktivität abbrechen wollen, müssen Sie zuerst auf deren Namen klicken und anschließend (auf der Anzeige **Details**) auf **Abbrechen** klicken.

Sie können die aufgelisteten Aktivitäten nach den folgenden Kriterien durchsuchen:

- Gerätename
  Dies ist die Maschine, auf welcher die Aktivität ausgeführt wird.
- Gestartet von
  Dies ist das Konto, welches die Aktivität gestartet hat.

Die Remote-Desktop-Aktivitäten können nach folgenden Eigenschaften gefiltert werden:

- Plan wird erstellt
- Plan wird angewendet
- Plan wird widerrufen
- Plan wird gelöscht
- Remote-Verbindung
  - Cloud-Remote-Desktop-Verbindung über RDP
  - Cloud-Remote-Desktop-Verbindung über NEAR
  - Cloud-Remote-Desktop-Verbindung über Apple Bildschirmfreigabe
  - Remote-Desktop-Verbindung über Webclient
  - Remote-Desktop-Verbindung über Quick Assist
  - Direkte Remote-Desktop-Verbindung über RDP
  - Direkte Remote-Desktop-Verbindung über Apple Bildschirmfreigabe
  - Dateiübertragung
  - Dateiübertragung über Quick Assist
- Remote-Aktion
  - Ein Workload wird heruntergefahren
  - Ein Workload wird neu gestartet
  - Remote-Benutzer wird auf dem Workload abgemeldet
  - Papierkorb für Benutzer wird auf dem Workload geleert
  - Ein Workload wird in den Energiesparmodus versetzt

Cyber Protect Monitor

Der Cyber Protect Monitor zeigt Informationen über den Schutzstatus derjenigen Maschine an, auf welcher der Agent für Windows oder der Agent für Mac installiert ist – und ermöglicht es den entsprechenden Anwendern, die Backup-Verschlüsselung und die Proxy-Server-Einstellungen zu konfigurieren.

Wenn der Agent für File Sync & Share auf der Maschine installiert ist, ermöglicht der Cyber Protect Monitor Zugriff auf den File Sync & Share Service. Die File Sync & Share-Funktionalität ist nach einem zwingend erforderlichen Onboarding zugänglich, bei dem sich die Benutzer an ihrem File Sync &

Share Konto anmelden und einen persönlichen Sync-Ordner auswählen. Weitere Informationen über den Agent für File Sync & Share finden Sie im Benutzeranleitung für Cyber Files Cloud.

Wichtig
Auf den Cyber Protect Monitor können auch Anwender zugreifen, die keine administrativen Rechte für Cyber Protection oder den File Sync & Share Service haben.

Die untenstehende Tabelle fasst die Aktionen zusammen, die für Benutzer ohne administrative Rechte verfügbar sind.

Installierte Agenten	Benutzer können	Benutzer können nicht
Der Agent für Windows oder der Agent für Mac	• Den Standard-Schutzplan auf ihre Maschinen anwenden • Den Schutzstatus ihrer Maschinen überprüfen • Benachrichtigungen von Active Protection erhalten • Die Backups ihrer Maschinen vorübergehend pausieren • Die Proxy-Server-Einstellungen konfigurieren • Die Einstellungen für die Backup-Verschlüsselung ändern **Warnung!** Eine Änderung der Verschlüsselungseinstellungen im Cyber Protect Monitor überschreibt die Einstellungen im Schutzplan und wirkt sich auf alle Backups der entsprechenden Maschine aus. Diese Aktion kann dazu führen, dass einige Schutzpläne fehlschlagen. Weitere Informationen dazu finden Sie unter "Verschlüsselung" (S. 484). Falls Sie Ihr Kennwort verlieren, gibt es keine Möglichkeit, Ihre verschlüsselten Backups wiederherzustellen!	• Benutzerdefinierten Schutzpläne anwenden • Bereits angewendete Schutzpläne verwalten
Der Agent für Windows und der Agent für Sync & Share	• Inhalte zwischen ihrem lokalen Sync-Ordner und ihrem File Sync & Share-Konto synchronisieren • Die Synchronisierungsaktionen pausieren	• Die Dateitypen bearbeiten, die nicht synchronisiert werden können

Installierte Agenten	Benutzer können	Benutzer können nicht
Der Agent für Mac und der Agent für Sync & Share	• Den Sync-Ordner ändern • Die Dateitypen überprüfen, die nicht synchronisiert werden können	

Proxy-Server-Einstellungen im Cyber Protect Monitor konfigurieren

Sie können Proxy-Server-Einstellungen im Cyber Protect Monitor konfigurieren. Diese Konfiguration wirkt sich auf alle Agenten aus, die auf der Maschine installiert sind.

So können Sie die Proxy-Server-Einstellungen konfigurieren

1. Öffnen Sie den Cyber Protect Monitor und klicken Sie dann in der rechten oberen Ecke auf das Zahnradsymbol.
2. Klicken Sie zuerst auf **Einstellungen** und dann auf **Proxy**.
3. Aktivieren Sie den Schalter **Proxy-Server verwenden** und geben Sie dann die Adresse und den Port des Proxy-Servers ein.
4. [Falls der Zugriff auf den Proxy-Server kennwortgeschützt ist] Aktivieren Sie den Schalter **Kennwort erforderlich** und geben Sie dann den Benutzernamen und das Kennwort für den Zugriff auf den Proxy-Server ein.
5. Klicken Sie auf **Speichern**.
   Die Proxy-Server-Einstellungen werden in der Datei `http-proxy.yaml` gespeichert.

Berichte

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Ein Bericht über Aktionen kann einen beliebigen Satz von Dashboard-Widgets enthalten. Alle Widgets zeigen zusammengefasste Informationen für die komplette Firma an.

Je nach Widget-Typ enthält der Bericht Daten für einen bestimmten Zeitraum oder für den Zeitpunkt des Durchsuchens oder der Berichtserstellung. Siehe Abschnitt '"Berichtsdaten je nach Widget-Typ" (S. 346)'.

Alle historischen Widgets zeigen Daten für den gleichen Zeitraum an. Sie können diesen Zeitraum in den Berichtseinstellungen ändern.

Sie können vorgegebene Berichte (Standardberichte) verwenden oder einen benutzerdefinierten Bericht erstellen.

Sie können einen Bericht herunterladen oder per E-Mail im XLSX-Format (Excel) oder PDF-Format versenden.

Der Satz der Standardberichte hängt von der Cyber Protection Service-Edition ab, die Sie haben. Die Standardberichte sind nachfolgend aufgelistet:

Berichtsname	Beschreibung
#CyberFit-Score pro Maschine	Zeigt den #CyberFit-Score, der auf der Evaluierung von Sicherheitsmetriken und Sicherheitskonfigurationen für jede Maschine basiert, und Empfehlungen für deren Verbesserungen an.
Alarmmeldungen	Zeigt Alarmmeldungen an, die während eines bestimmten Zeitraums aufgetreten sind.
Backup-Scanning-Details	Zeigt ausführliche Informationen über erkannte Bedrohungen in den Backups an.
Tägliche Aktivitäten	Zeigt Übersichtsinformationen zu Aktivitäten an, die während eines bestimmten Zeitraums durchgeführt wurden.
Data Protection-Karte	Zeigt ausführliche Informationen über Anzahl, Größe, Speicherort und Sicherungsstatus aller wichtigen Dateien auf den Maschinen an.
Erkannte Bedrohungen	Zeigt Details der betroffenen Maschinen anhand der Anzahl der blockierten Bedrohungen sowie der fehlerfreien und verwundbaren Maschinen an.
Erkannte Maschinen	Zeigt alle gefundene Maschinen im Organisationsnetzwerk an.
Vorhersage der Laufwerksintegrität	Zeigt den aktuellen Laufwerksstatus an sowie eine Prognose dazu, wann Ihre HDD/SSD vermutlich ausfallen wird.
Vorhandene Schwachstellen	Zeigt die existierenden Verwundbarkeiten des Betriebssystems und der Applikationen in Ihrem Unternehmen an. Der Bericht zeigt zudem Details der betroffenen Maschinen in Ihrem Netzwerk für jedes aufgelistete Produkt an.
Software-Inventarisierung	Zeigt Informationen über die Software an, die auf den Geräten Ihres Unternehmens installiert ist.
Hardware-Inventarisierung	Zeigt Informationen über die Hardware an, die auf den Geräten Ihres Unternehmens verfügbar ist.
Übersicht zur Patch-Verwaltung	Zeigt die Anzahl der fehlenden, installierten und anwendbaren Patches an. Sie können sich Detailinformationen zu den Berichten anzeigen lassen, um Informationen und Details zu den fehlenden/installierten Patches für alle Systeme zu erhalten.
Übersicht	Zeigt Übersichtsinformationen zu geschützten Geräten für einen bestimmten Zeitraum an.
Wöchentliche Aktivitäten	Zeigt Übersichtsinformationen zu Aktivitäten an, die während eines bestimmten Zeitraums durchgeführt wurden.
Remote-Sitzungen	Zeigt Informationen über die Remote-Desktop- und Dateiübertragungssitzungen an.

Aktionen mit Berichten

Wenn Sie einen Bericht einsehen wollen, klicken Sie auf dessen Namen.

So können Sie einen neuen Bericht hinzufügen

1. Gehen Sie in der Cyber Protect-Konsole zu **Berichte**.
2. Klicken Sie unter der Liste der verfügbaren Berichte auf **Bericht hinzufügen**.
3. [Um einen vordefinierten Bericht hinzuzufügen] Klicken Sie auf den Namen des vordefinierten Berichts.
4. [Um einen benutzerdefinierten Bericht hinzuzufügen] Klicken Sie auf **Benutzerdefiniert** und fügen Sie dann Widgets zum Bericht hinzu.
5. [Optional] Ordnen Sie die Widgets per Drag & Drop nach Ihren Vorstellungen neu an.

So können Sie eine Bericht bearbeiten

1. Gehen Sie in der Cyber Protect-Konsole zu **Berichte**.
2. Wählen Sie aus der Liste der Berichte denjenigen Bericht aus, den Sie bearbeiten wollen.
   Sie können Folgendes tun:
   - Den Bericht umbenennen.
   - Den Zeitraum für alle Widgets im Report ändern.
   - Die Berichtsempfänger spezifizieren sowie den Zeitpunkt, an dem der Bericht an diese gesendet werden soll. Die verfügbaren Formate sind PDF und XLSX.

So können Sie einen Bericht löschen

1. Gehen Sie in der Cyber Protect-Konsole zu **Berichte**.
2. Wählen Sie aus der Liste der Berichte denjenigen Bericht aus, den Sie löschen wollen.
3. Klicken Sie auf das Drei-Punkte-Symbol (...) und dann auf den Befehl **Löschen**.
4. Bestätigen Sie Ihre Auswahl, indem Sie auf **Löschen** klicken.

So können Sie eine Bericht planen

1. Gehen Sie in der Cyber Protect-Konsole zu **Berichte**.
2. Wählen Sie in der Liste der Berichte denjenigen Bericht aus, den Sie planen wollen, und klicken Sie anschließend auf **Einstellungen**.
3. Aktivieren Sie den Schalter **Geplant**.
   - Spezifizieren Sie die E-Mail-Adressen der Empfänger.
   - Bestimmen Sie das Format des Berichts.

Hinweis
Sie können bis zu 1000 Elemente in eine PDF-Datei und bis zu 10.000 Elemente in eine XLSX-Datei exportieren. Die Zeitstempel in den PDF- und XLSX-Dateien basieren auf der lokalen Zeit Ihrer Maschine.

- Bestimmen Sie die Sprache des Berichts.
- Konfigurieren Sie die Planung.

4. Klicken Sie auf **Speichern**.

So können Sie einen Bericht herunterladen

1. Gehen Sie in der Cyber Protect-Konsole zu **Berichte**.
2. Wählen Sie in der Liste der Berichte den gewünschten Bericht aus und klicken Sie dann auf **Download**.
3. Bestimmen Sie das Format des Berichts.

So können Sie einen Bericht senden

1. Gehen Sie in der Cyber Protect-Konsole zu **Berichte**.
2. Wählen Sie in der Liste der Berichte den gewünschten Bericht aus und klicken Sie dann auf **Senden**.
3. Spezifizieren Sie die E-Mail-Adressen der Empfänger.
4. Bestimmen Sie das Format des Berichts.
5. Klicken Sie auf **Senden**.

So können Sie die Berichtsstruktur exportieren

1. Gehen Sie in der Cyber Protect-Konsole zu **Berichte**.
2. Wählen Sie in der Liste der Berichte den gewünschten Bericht aus.
3. Klicken Sie auf das Drei-Punkte-Symbol (...) und dann auf den Befehl **Exportieren**.

Als Ergebnis wird die Berichtsstruktur als JSON-Datei auf Ihrer Maschine gespeichert.

So können Sie die Berichtsdaten sichern

Mit dieser Option können Sie alle Daten für einen benutzerdefinierten Zeitraum (ohne Filterung) in eine CSV-Datei exportieren und diese an einen E-Mail-Empfänger senden.

Hinweis
Sie können bis zu 150.000 Elemente in eine CSV-Datei exportieren. Die Zeitstempel in der CSV-Datei verwenden die koordinierte Weltzeit (UTC).

1. Gehen Sie in der Cyber Protect-Konsole zu **Berichte**.
2. Wählen Sie aus der Liste der Berichte denjenigen Bericht aus, dessen Daten Sie sichern wollen.

3. Klicken Sie auf das Drei-Punkte-Symbol (...) und dann auf **Sicherungsdaten**.
4. Spezifizieren Sie die E-Mail-Adressen der Empfänger.
5. Spezifizieren Sie bei **Zeitraum** den benutzerdefinierten Zeitraum, für den Sie die Daten sichern wollen.

   Hinweis
   CSV-Dateien für längere Zeiträume vorzubereiten, kostet mehr Zeit.

6. Klicken Sie auf **Senden**.

Berichtsdaten je nach Widget-Typ

Je nach dem Datenbereich, den sie anzeigen, gibt es zwei Arten von Widgets auf dem Dashboard:

- Widgets, die aktuelle Daten für den Zeitpunkt des Durchsuchens oder der Berichtserstellung anzeigen.
- Widgets, die historische Daten anzeigen.

Wenn Sie in den Berichtseinstellungen einen Datumsbereich konfigurieren, um Daten für einen bestimmten Zeitraum auszugeben, gilt der gewählte Zeitraum nur für Widgets, die historische Daten anzeigen. Für Widgets, die aktuelle Daten für den Zeitpunkt des Durchsuchens anzeigen, ist der Parameter Zeitraum nicht anwendbar.

Die nachfolgende Tabelle führt die verfügbaren Widgets und deren Datenbereiche auf.

Widget-Name	Daten, die im Widget und in Berichten angezeigt werden
#CyberFit-Score pro Maschine	Aktuell
5 neueste Alarmmeldungen	Aktuell
Details zu aktiven Alarmmeldungen	Aktuell
Aktive Alarmmeldungen – Übersicht	Aktuell
Aktivitäten	Historisch
Aktivitätsliste	Historisch
Alarmverlauf	Historisch
Statistik der Angriffstaktiken	Historisch
Backup-Scanning-Details (Bedrohungen)	Historisch
Backup-Status	Historisch – in den Spalten **Ausführungen insgesamt** und **Anzahl erfolgreiche Ausführungen** Aktuell – in allen anderen Spalten

Blockierte URLs	Aktuell
Cloud-Applikationen	Aktuell
Cyber protection	Aktuell
Data Protection-Karte	Historisch
Geräte	Aktuell
Erkannte Maschinen	Aktuell
Überblick der Laufwerksintegrität	Aktuell
Laufwerksintegritätstatus nach physischen Geräten	Aktuell
Vorhandene Schwachstellen	Historisch
Hardware-Änderungen	Historisch
Hardware-Details	Aktuell
Hardware-Inventarisierung	Aktuell
Übersicht der historischen Alarmmeldungen	Historisch
Vorfallschweregradverlauf	Historisch
Speicherorteübersicht	Aktuell
Fehlende Updates nach Kategorie	Aktuell
Nicht geschützt	Aktuell
Verlauf der Patch-Installation	Historisch
Status der Patch-Installation	Historisch
Übersicht der Patch-Installation	Historisch
Schutzstatus	Aktuell
Kürzlich betroffen	Historisch
Remote-Sitzungen	Historisch
Sicherheitsvorfall-Burndown	Historisch
Sicherheitsvorfall-MTTR (Mittlere Problemlösungszeit)	Historisch
Software-Inventarisierung	Aktuell
Software-Überblick	Historisch

Bedrohungsstatus	Aktuell
Verwundbare Maschinen	Aktuell
Workload-Netzwerkstatus	Aktuell

Workloads in der Cyber Protect-Konsole verwalten

In diesem Abschnitt wird erläutert, wie Sie Ihre Workloads in der Cyber Protect-Konsole verwalten können.

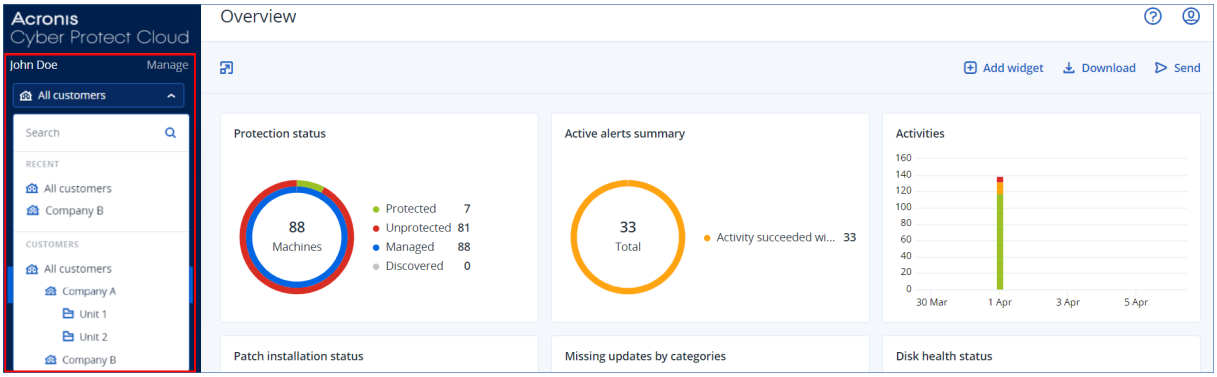
Die Cyber Protect-Konsole

Sie können in der Cyber Protect-Konsole Workloads und Pläne verwalten, die Schutzeinstellungen ändern, Berichte konfigurieren oder den Backup Storage überprüfen.

Die Cyber Protect-Konsole ermöglicht Ihnen Zugriff auf zusätzliche Services oder Funktionen – wie etwa File Sync & Share-Funktionen, Antivirus & Antimalware Protection, Patch-Verwaltung, Gerätekontrolle und Schwachstellenbewertung. Die Art und Anzahl dieser Services und Funktionen hängt von Ihrer jeweiligen Cyber Protection-Lizenz ab.

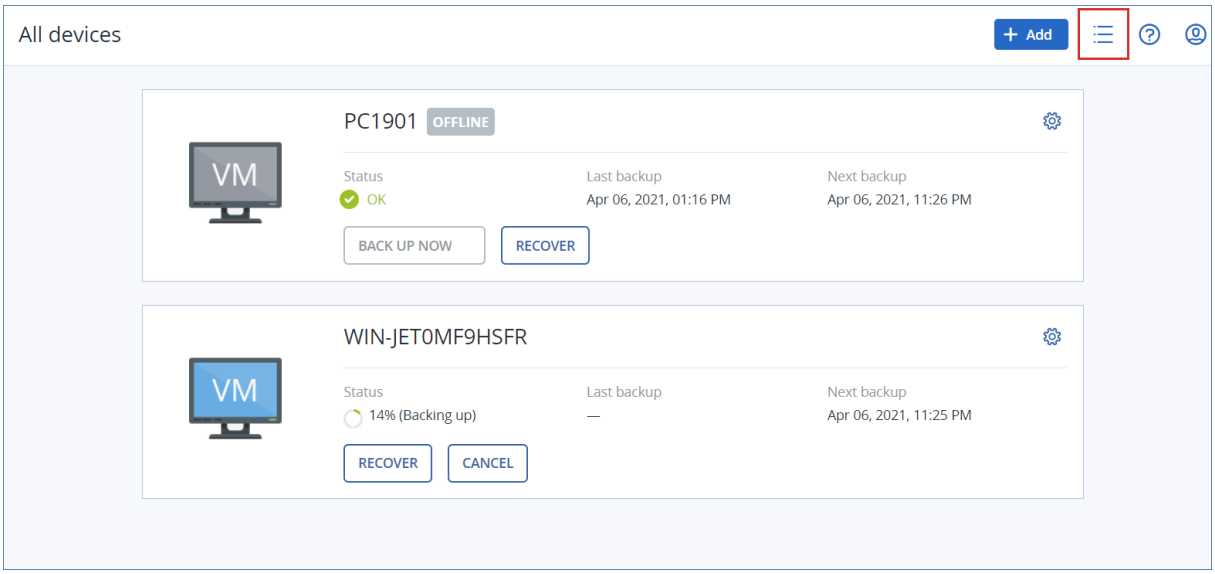
Wenn Sie sich das Dashboard mit den wichtigsten Informationen zu Ihrem Schutz ansehen wollen, gehen Sie zu **Monitoring** –> **Überblick**.

Abhängig von Ihren Zugriffsberechtigungen können Sie den Schutz für einen oder mehrere Kunden-Mandanten oder Abteilungen in einem Mandanten verwalten. Verwenden Sie das Listenfeld im Navigationsmenü, um die Hierarchie-Ebene zu wechseln. Es werden nur die Ebenen angezeigt, auf die Sie Zugriff haben. Wenn Sie zum Management-Portal gehen wollen, klicken Sie auf **Verwalten**.

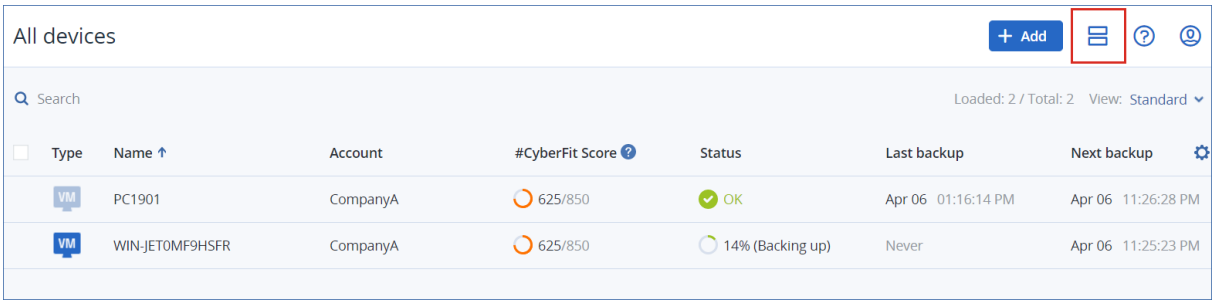


Der Bereich **Geräte** ist in einer einfachen Ansicht und einer Tabellenansicht verfügbar. Sie können zwischen diesen wechseln, wenn Sie in der oberen rechten Ecke auf das entsprechende Symbol klicken.

In der einfachen Ansicht werden nur einige wenige Workloads angezeigt.



Die Tabellenansicht wird automatisch aktiviert, wenn die Anzahl der Workloads größer wird.



Beide Ansichten stellen ansonsten dieselben Funktionen und Operationen bereit. In diesem Dokument wird die Tabellenansicht verwendet, um den Zugriff auf die Operationen zu beschreiben.

Wenn ein Workload online oder offline geht, dauert es einige Zeit, bis sich dessen Status in der Cyber Protect-Webkonsole ändert. Der Workload-Status wird jede Minute überprüft. Wenn der auf der entsprechenden Maschine installierte Agent keine Daten überträgt und bei fünf aufeinanderfolgenden Prüfungen keine Antwort gegeben hat, wird der Workload als offline angezeigt. Der Workload wird wieder als online angezeigt, wenn sie auf einen Status-Check antwortet oder mit einer Datenübertragung beginnt.

Die Neuerungen in der Cyber Protect-Konsole

Wenn neue Funktionen von Cyber Protect Cloud verfügbar sind, wird Ihnen bei der Anmeldung an der Cyber Protect-Konsole ein Pop-up-Fenster mit einer kurzen Beschreibung dieser Funktionen angezeigt.

Sie können die Beschreibung der neuen Funktionen auch einsehen, indem Sie in der linken unteren Ecke des Hauptfensters der -Konsole auf den Link **Neuerungen** klicken.

Wenn es keine neuen Funktionen gibt, wird auch der Link **Neuerungen** nicht angezeigt.

Die Cyber Protect-Konsole als Partner-Administrator verwenden

Als Partner-Administrator können Sie die Cyber Protect-Konsole auf der Partner-Mandanten-Ebene (**Alle Kunden**) oder auf der Kunden-Mandanten-Ebene verwenden.

Partner-Mandant-Ebene (**Alle Kunden**)

Auf der Partner-Mandanten-Ebene (**Alle Kunden**) können Sie folgende Aktionen ausführen:

- Skripting-Pläne für Workloads von all Ihren verwalteten Kunden-Mandanten verwalten.
  Sie können denselben Skripting-Plan auf Workloads von verschiedenen Kunden anwenden und Gerätegruppen mit Workloads von verschiedenen Kunden erstellen. Wie Sie eine statische oder dynamische Gerätegruppe auf Partner-Ebene erstellen können, erfahren Sie in den Abschnitten "Eine statische Gerätegruppe auf Partnerebene erstellen" (S. 354) und "Eine dynamische Gerätegruppe auf Partnerebene erstellen" (S. 354). Weitere Informationen über Skripte und Skripting-Pläne finden Sie im Abschnitt "Cyber Scripting" (S. 255).
- Monitoring-Pläne für Workloads von all Ihren verwalteten Kunden-Mandanten erstellen.
- Remote-Verwaltungspläne für Workloads von all Ihren verwalteten Kunden-Mandanten erstellen.
- Betrachten und verwalten Sie Endpoint Detection & Response (EDR)-Vorfälle für alle Kunden-Mandanten über eine einzige Konsole zur Vorfallsverwaltung, anstatt auf die Vorfallsanzeigen der einzelnen Kunden zugreifen zu müssen.
- Eine automatische Erkennung von Maschinen für all Ihre verwalteten Kunden-Mandanten durchführen.

Kunden-Mandanten-Ebene

Auf dieser Ebene haben Sie die gleichen Rechte wie der Firmenadministrator, in dessen Namen Sie handeln.

Eine Mandanten-Ebene auswählen

Sie können die Mandanten-Ebene auswählen, auf der Sie in der Cyber Protect-Konsole arbeiten möchten.

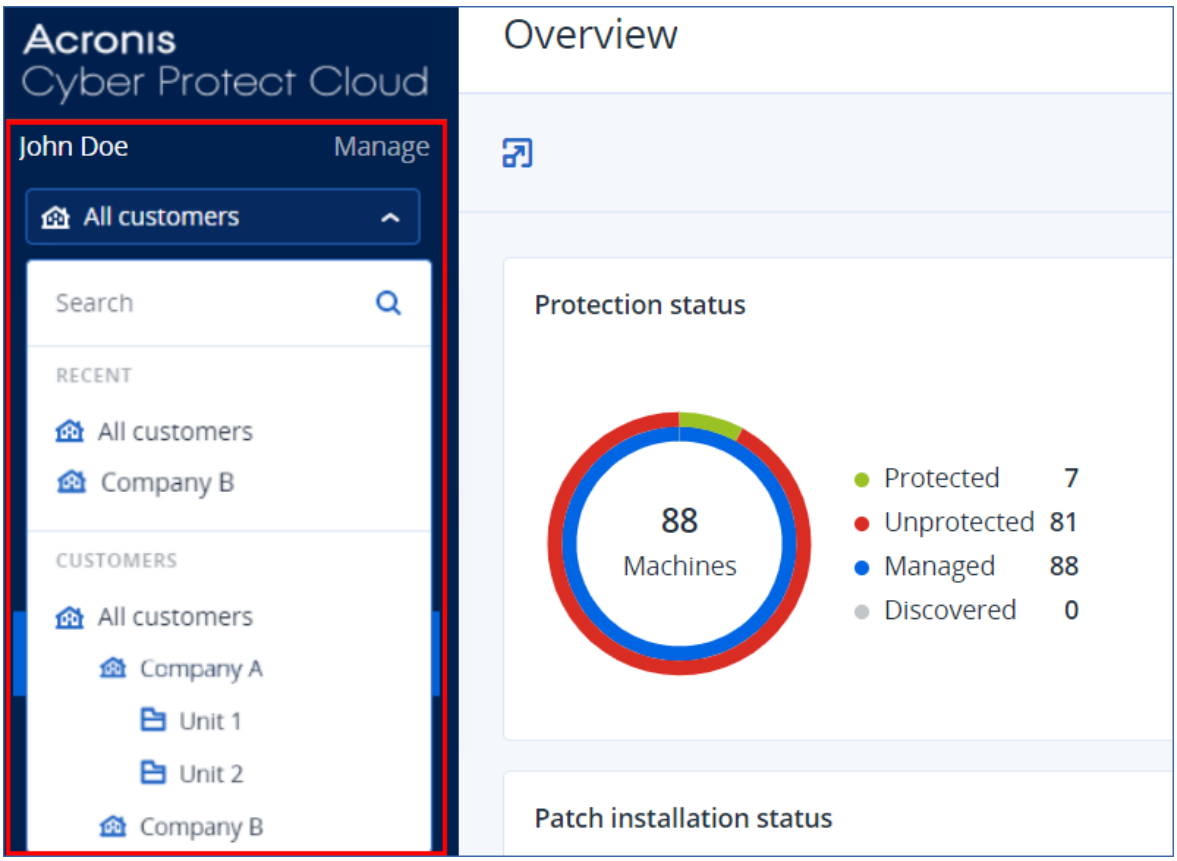
Voraussetzungen

- Sie haben sowohl Zugriffsrechte auf die Cyber Protect-Konsole als auch auf das Management-Portal.
- Sie können mehr als einen Mandanten oder eine Abteilung verwalten.

So können Sie eine Mandanten-Ebene in der Cyber Protect-Konsole auswählen

1. Klicken Sie im Navigationsmenü links auf den Pfeil neben dem Namen des Kunden-Mandanten.
2. Wählen Sie eine der folgenden Optionen:

- Wenn Sie auf der Partnerebene arbeiten wollen, wählen Sie **Alle Kunden**.
- Wenn Sie auf Kunden- oder Abteilungsebene arbeiten wollen, müssen Sie den Namen des betreffenden Kunden bzw. der betreffenden Abteilung auswählen.



Partner-Mandanten-Ebene in der Cyber Protect-Konsole

Wenn Sie die Cyber Protect-Konsole auf der Partner-Ebene (**Alle Kunden**) verwenden, ist eine angepasste Anzeige verfügbar.

Die Registerkarten **Alarmmeldungen** und **Aktivitäten** bieten zusätzliche partnerbezogene Filter, während die Registerkarten **Geräte** und **Verwaltung** nur Zugriff auf jene Funktionen oder Objekte bieten, die für Partner-Administratoren zugänglich sind.

Die Registerkarte 'Alarmmeldungen'

Hier können Sie die Alarmmeldungen aller von Ihnen verwalteten Kunden einsehen, diese durchsuchen und nach den folgenden Kriterien filtern:

- Gerät
- Kunde
- Plan

Sie können für jedes dieser Kriterien mehrere Elemente auswählen.

Die Registerkarte 'Aktivitäten'

Hier können Sie die Aktivitäten aller von Ihnen verwalteten Mandanten oder die Aktivitäten in einem bestimmten Kunden-Mandanten einsehen.

Sie können die Aktivitäten nach Kunde, Status, Zeit und Typ filtern.

Folgende Arten von Aktivitäten werden auf dieser Ebene automatisch vorausgewählt:

- Plan wird angewendet
- Schutzplan wird erstellt
- Schutzplan
- Plan wird widerrufen
- Skripting

Die Registerkarte 'Geräte'

Auf der Registerkarte **Maschinen mit Agenten** können Sie alle Workloads Ihrer verwalteten Kunden-Mandanten einsehen sowie Workloads von einem oder mehreren Mandanten auswählen. Sie können auch Gerätegruppen erstellen, die Workloads von verschiedenen Mandanten enthalten.

Wichtig
Wenn Sie auf der Partner-Ebene (**Alle Kunden**) arbeiten, können Sie nur eine begrenzte Anzahl von Aktionen mit Geräten durchführen. Beispielsweise können Sie keine der folgenden Aktionen ausführen:

- Vorhandene Schutzpläne auf Kunden-Geräten einsehen und verwalten.
- Neue Schutzpläne erstellen.
- Backups wiederherstellen.
- Disaster Recovery verwenden.
- Auf die Cyber Protection Desktop-Funktionen zugreifen.

Wenn Sie eine dieser Aktionen durchführen wollen, müssen Sie auf der Kunden-Ebene arbeiten.

Die Registerkarte 'Software-Verwaltung'

Wenn der Software-Inventarisierungsscan für Kunden-Workloads aktiviert ist, können Sie die Ergebnisse des Software-Scans einsehen.

Die Workloads von bestimmten Kunden einsehen

Als Partner-Administrator können Sie die Workloads der Kunden-Mandanten einsehen, die von Ihnen verwaltet werden.

So können Sie die Workloads eines bestimmten Kunden einsehen

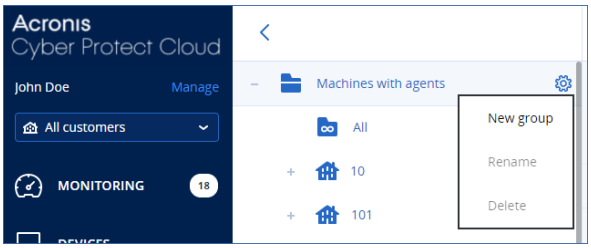
1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte** –> **Maschinen mit Agenten**.
2. Klicken Sie im Verzeichnisbaum auf **Maschinen mit Agenten**, um die Liste zu erweitern.
3. Klicken Sie auf den Namen desjenigen Kunden, dessen Workloads Sie einsehen und verwalten wollen.

Eine statische Gerätegruppe auf Partnerebene erstellen

Sie können statische Gerätegruppen auf der Partner-Ebene (**Alle Geräte**) erstellen.

So können Sie eine statische Gerätegruppe auf der Partnerebene erstellen

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte** –> **Maschinen mit Agenten**.
2. Klicken Sie auf das Zahnradsymbol neben dem Element '**Maschinen mit Agenten**' und klicken Sie dann auf **Neue Gruppe**.



3. Spezifizieren Sie den Gruppennamen.
4. [Optional] Fügen eine Beschreibung hinzu.
5. Klicken Sie auf **OK**.

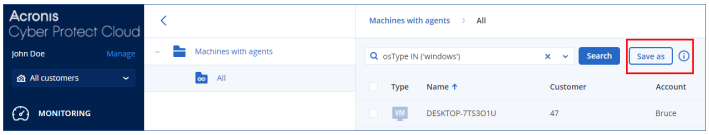
Eine dynamische Gerätegruppe auf Partnerebene erstellen

Sie können dynamische Gerätegruppen auf der Partner-Ebene (**Alle Geräte**) erstellen.

So können Sie eine dynamische Gerätegruppe auf der Partnerebene erstellen

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte** –> **Maschinen mit Agenten**.
2. Klicken Sie im Verzeichnisbaum auf **Maschinen mit Agenten**, um die Liste zu erweitern.
3. Klicken Sie auf **Alle**.
4. Spezifizieren Sie im Suchfeld die Kriterien, nach denen Sie eine dynamische Gerätegruppe erstellen wollen, und klicken Sie anschließend auf **Suchen**.

   Um mehr über die verfügbaren Suchkriterien zu erfahren, siehe "Suchattribute für Nicht-Cloud-zu-Cloud-Workloads" (S. 379) und "Suchattribute für Cloud-zu-Cloud-Workloads" (S. 378).
5. Klicken Sie auf **Speichern unter** und spezifizieren Sie dann den Gruppennamen.



6. [Optional] Fügen eine Beschreibung hinzu.
7. Klicken Sie auf **OK**.

Eine automatische Erkennung von Maschinen auf der Partner-Mandanten-Ebene durchführen

Sie können eine automatische Erkennung von Maschinen auf der Partner-Mandanten-Ebene (**Alle Kunden**) durchführen.

Voraussetzungen

Es gibt mindestens eine Maschine mit einem installierten Protection Agenten in Ihrem lokalen Netzwerk oder Active Directory-Domain Ihres Kunden.

Wichtig
Nur Agenten, die auf Windows-Maschinen installiert sind, können Discovery Agenten sein. Wenn es in der Umgebung Ihres Kunden keine Discovery Agenten gibt, können Sie nicht die Option **Mehrere Geräte** im Fensterbereich **Geräte hinzufügen** verwenden.

Beim Hinzufügen von Domain Controllern wird keine automatische Erkennung (Autodiscovery-Funktionalität) unterstützt, da zur Ausführung des Agenten-Dienstes zusätzliche Berechtigungen erforderlich sind.

Die Remote-Installation von Agenten wird nur für Maschinen unter Windows unterstützt (wobei Windows XP nicht mehr unterstützt wird). Um eine Remote-Installation auf einer Maschine mit Windows Server 2012 R2 durchführen zu können, muss das Windows-Update KB2999226 installiert sein.

So können Sie eine automatische Erkennung von Maschinen auf der Partner-Mandanten-Ebene durchzuführen

1. Wählen Sie in der Cyber Protect-Konsole die Option **Alle Kunden**.
2. Gehen Sie zu **Geräte**> **Alle Geräte**.
3. Klicken Sie auf **Hinzufügen**.
4. Klicken Sie bei **Mehrere Geräte** auf **Nur Windows**. Der Erkennungsassistent wird geöffnet.
5. Wählen Sie einen Kunden-Mandanten aus und wählen Sie dann den Discovery Agenten aus, der den Scan zur Erkennung der Maschinen durchführen soll.
6. Bestimmen Sie die Erkennungsmethode:
   - **Active Directory durchsuchen**. Stellen Sie sicher, dass die Maschine mit dem Discovery Agenten ein Mitglied der Active Directory-Domain ist.
   - **Lokales Netzwerk scannen**. Wenn der ausgewählte Discovery Agent keine Maschinen finden konnte, wählen Sie einen anderen Discovery Agenten aus.
   - **Manuell spezifizieren oder aus Datei importieren**. Definieren Sie die hinzuzufügenden Maschinen manuell oder importieren Sie diese aus einer Textdatei.
7. [Wenn die Erkennungsmethode 'Active Directory' ausgewählt wurde] Bestimmen Sie, wie nach den Maschinen gesucht werden soll:

- **In der Liste der Organisationseinheiten**. Wählen Sie die Gruppe der Maschinen aus, die hinzugefügt werden sollen.
- **Per LDAP-Dialekt-Abfrage**. Verwenden Sie die LDAP-Dialekt-Abfrage, um die Maschinen auszuwählen. Die **Such-Basis** definiert, wo gesucht werden soll, während Sie über den **Filter** die Kriterien zur Auswahl der Maschinen spezifizieren können.

8. Je nach der von Ihnen gewählten Erkennungsmethode können Sie eine der folgenden Aktionen durchführen:

Erkennungsmethode	Aktion
Active Directory durchsuchen	Wählen Sie aus der Liste der erkannten Maschinen diejenigen aus, die Sie hinzufügen wollen.
Lokales Netzwerk scannen	Wählen Sie aus der Liste der erkannten Maschinen diejenigen aus, die Sie hinzufügen wollen.

Manuell spezifizieren oder aus Datei importieren	Spezifizieren Sie die IP-Adressen oder Host-Namen der Maschinen – oder importieren Sie eine Liste der Maschinen aus einer Textdatei. Die Datei muss je eine IP-Adresse bzw. einen Host-Namen pro Zeile enthalten. Hier ist ein Beispiel für eine entsprechende Datei:
	`156.85.34.10`
	`156.85.53.32`
	`156.85.53.12`
	`EN-L00000100`
	`EN-L00000101`
	Nachdem die Adressen der Maschinen manuell hinzugefügt oder über eine Datei importiert wurden, versucht der Agent, die hinzugefügten Maschinen anzupingen und deren Verfügbarkeit zu ermitteln.

9. Bestimmen Sie, welche Aktionen nach der Erkennung durchgeführt werden sollen:

Option	Beschreibung
Agenten installieren und Maschinen registrieren	Sie können auswählen, welche Komponenten auf den Maschinen installiert werden sollen, indem Sie auf **Komponenten auswählen** klicken. Weitere Details finden Sie unter "Zu installierende Komponenten auswählen" (S. 144).
Anmeldekonto für den Agenten-Dienst	Diese Einstellung ist auf der Anzeige **Komponenten auswählen** verfügbar. Die Einstellung definiert das Konto, unter dem die Dienste ausgeführt werden. Sie können eine der folgenden Optionen auswählen: • **Service User-Konten verwenden** (Standard für den Agenten-Dienst) Service User-Konten sind Windows-System-Konten, die verwendet werden, um Dienste auszuführen. Der Vorteil dieser Einstellung ist, dass die Domänen-Sicherheitsrichtlinien keinen Einfluss auf die Benutzerrechte dieser Konten haben. Standardmäßig wird der Agent unter dem Konto **Lokales System** ausgeführt.

Option	Beschreibung
	• **Neues Konto erstellen** Der Kontoname für den Agenten lautet 'Agent User'. • **Folgendes Konto verwenden** Wenn Sie den Agenten auf einem Domain Controller installieren, wird Sie das System auffordern, für den Agenten vorhandene Konten (oder dasselbe Konto) zu spezifizieren. Das System erstellt aus Sicherheitsgründen nicht automatisch neue Konten auf einem Domain Controller. Wenn Sie die Option **Neues Konto erstellen** oder **Folgendes Konto verwenden** wählen, sollten Sie sicherstellen, dass die Domänen-Sicherheitsrichtlinien die Rechte der entsprechenden Konten nicht beeinträchtigen. Wenn einem Konto Benutzerrechte wieder entzogen werden, die diesem bei der Installation zugewiesen wurden, wird die Komponente möglicherweise fehlerhaft oder gar nicht funktioniert.
Maschinen mit installierten Agenten registrieren	Verwenden Sie diese Option, wenn der Agent bereits auf den Maschinen installiert ist und Sie diese nur in Cyber Protection registrieren müssen. Wenn auf den Maschinen kein Agent gefunden wird, werden diese als **Nicht verwaltete** Maschinen hinzugefügt.
Als nicht verwaltete Maschinen hinzufügen	Wenn Sie diese Option wählen, wird der Agent nicht auf den Maschinen installiert. Sie können sich die Maschinen in der Konsole anzeigen lassen und den Agenten später installieren oder registrieren.
Maschine bei Bedarf neu starten	Diese Option erscheint, wenn **Agenten installieren und Maschinen registrieren** ausgewählt wurde. Wenn Sie diese Option auswählen, wird die Maschine so oft neu gestartet, wie es zur Fertigstellung der Installation erforderlich ist. Ein Neustart der Maschine kann in einem der folgenden Fälle erforderlich sein: • Die Installation der Vorgaben ist abgeschlossen. Es ist ein Neustart erforderlich, um mit der Installation fortfahren zu können. • Die Installation ist abgeschlossen. Es ist jedoch ein Neustart erforderlich, weil einige Dateien während der Installation gesperrt wurden. • Die Installation ist abgeschlossen. Für andere, zuvor installierte Software ist jedoch ein Neustart erforderlich.
Nicht neu starten, wenn der Benutzer angemeldet ist	Diese Option erscheint, wenn **Maschine bei Bedarf neu starten** ausgewählt wurde. Wenn Sie diese Option auswählen, wird die Maschine nicht automatisch neu gestartet, solange der Benutzer im System angemeldet ist. Wenn ein Benutzer also beispielsweise arbeitet, während die Installation einen Neustart erfordert, wird das System nicht neu gestartet. Wenn die Voraussetzungen installiert wurden, aber die Maschine nicht neu gestartet wurde, weil ein Benutzer angemeldet war, müssen Sie zur Fertigstellung der Installation die Maschine neu starten und dann die Installation erneut starten.

Option	Beschreibung
	Wenn der Agent installiert wurde, aber der Computer dann nicht neu gestartet wurde, müssen Sie den Computer selbst neu starten.
Benutzer, bei dem die Maschinen registriert werden sollen	[Wenn es Abteilungen in Ihrer Organisation gibt] Wählen Sie das Benutzerkonto der Abteilung oder Unterabteilungen aus, unter dem Sie die Maschinen registrieren möchten. [Wenn Sie eine automatische Erkennung auf der Partner-Mandanten-Ebene durchführen] Erweitern Sie in der Liste der von Ihnen verwalteten Kunden-Mandanten die Verzeichnisstruktur und wählen Sie dann das Benutzerkonto aus, unter dem Sie die Maschinen registrieren wollen. [Wenn Sie eine automatische Erkennung als Kunden-Administrator durchführen] Wenn Sie **Agenten installieren und Maschinen registrieren** oder **Maschinen mit installierten Agenten registrieren** ausgewählt haben, gibt es auch die Option, den Schutzplan auf die Maschinen anwenden zu lassen. Wenn Sie mehrere Schutzpläne haben, können Sie auswählen, welchen Sie verwenden möchten.

10. Spezifizieren Sie die Anmeldedaten eines Benutzers mit administrativen Berechtigungen für all diese Maschinen.

Wichtig
Die Remote-Installation der Agenten funktioniert nur dann ohne Vorbereitungen, wenn Sie die Anmeldedaten des integrierten Administratorkontos (das erste Konto, das bei der Installation des Betriebssystems erstellt wird) spezifizieren. Wenn Sie einige benutzerdefinierte Administrator-Anmeldedaten definieren wollen, dann müssen Sie zusätzliche Vorbereitungen treffen, wie im Abschnitt '"Voraussetzungen" (S. 355)' erläutert.

11. Das System überprüft, ob eine Verbindung mit all diesen Maschinen möglich ist. Wenn mit einigen Maschinen keine Verbindung aufgebaut werden kann, können Sie die Anmeldedaten für diese Maschinen ändern.

Wenn die Erkennung für diese Maschinen initiiert wurde, können Sie den entsprechenden Task in der Aktivität **Monitoring** –> **Aktivitäten** –> **Maschinen erkennen** finden.

Unterstützung für mehrere Mandanten

Der Cyber Protection Service unterstützt Mandantenfähigkeit, was eine Verwaltung auf folgenden Ebenen impliziert:

- [Für Service Provider] Partner-Mandant-Ebene (**Alle Kunden**)
  Diese Stufe ist nur für Partner-Administratoren verfügbar, die Kunden-Mandanten verwalten.
- Kunden-Mandanten-Ebene
  Diese Ebene wird von Firmenadministratoren verwaltet.

Partner-Administratoren können auf dieser Ebene auch in den Kunden-Mandanten arbeiten, die von ihnen verwaltet werden. Auf dieser Ebene haben Partner-Administratoren die gleichen Rechte wie die Kunden-Administratoren, in deren Namen sie handeln.

- Abteilungsebene

  Diese Ebene wird von Abteilungsadministratoren und von Firmenadministratoren des übergeordneten Kunden-Mandanten verwaltet.

  Partner-Administratoren, die den übergeordneten Kunden-Mandanten verwalten, können ebenfalls auf die Abteilungsebene zugreifen. Auf dieser Ebene haben sie die gleichen Rechte wie die Kunden-Administratoren, in deren Namen sie handeln.

Administratoren können Objekte in ihrem eigenen Mandanten und in dessen Untermandanten verwalten. Sie können keine Objekte auf einer höheren Verwaltungsebene sehen oder auf diese zugreifen (sofern solche vorhanden sind).

So können beispielsweise Firmenadministratoren Schutzpläne sowohl auf der Ebene des Kunden-Mandanten als auch auf der Abteilungsebene verwalten. Abteilungsadministratoren können nur ihre eigenen Schutzpläne auf der Abteilungsebene verwalten. Sie können keine Schutzpläne auf der Kunden-Mandanten-Ebene verwalten und auch keine Schutzpläne, die vom Kunden-Administrator auf der Abteilungsebene erstellt wurden.

Außerdem können Partner-Administratoren Skripting-Pläne in denjenigen Kunden-Mandanten erstellen und anwenden, die von ihnen verwaltet werden. Die Firmenadministratoren in solchen Mandanten können nur auf Skripting-Pläne zugreifen, die von einem Partner-Administrator auf ihre Workloads angewendet werden – und das auch nur lesend. Kunden-Administratoren können jedoch eigene Skripting- oder Schutzpläne erstellen und anwenden.

Workloads

Unter einem Workload wird hier jede Art von geschützter Ressource verstanden – beispielsweise eine physische Maschine, eine virtuelle Maschine, ein Postfach oder eine Datenbank-Instanz. Der Workload wird in der Cyber Protect-Konsole als ein Objekt angezeigt, auf das Sie einen Plan (einen Schutzplan, Backup-Plan oder Skripting-Plan) anwenden können.

Für einige Workloads muss ein Protection Agent installiert oder eine virtuelle Appliance bereitgestellt werden. Sie können die Agenten über die grafische Benutzeroberfläche oder die Befehlszeilenschnittstelle (als unbeaufsichtigte Installation) installieren. Mithilfe einer unbeaufsichtigten Installation können Sie die Installationsprozedur automatisieren. Weitere Informationen zur Installation von Protection Agenten finden Sie im Abschnitt '"Cyber Protection Agenten installieren und bereitstellen" (S. 62)'.

Eine virtuelle Appliance (VA) ist eine vorgefertigte virtuelle Maschine, die bereits einen Protection Agenten enthält. Mithilfe einer virtuellen Appliance können Sie andere virtuelle Maschinen in derselben Umgebung sichern, ohne dass ein Protection Agent auf diesen Maschinen selbst installiert sein muss (sogenanntes „agentenloses Backup“). Die virtuellen Appliances liegen in Hypervisor-spezifischen Formaten vor (z.B. als .ovf-, .ova- oder .qcow-Dateien). Weitere

Informationen darüber, welche Virtualisierungsplattformen ein agentenloses Backup unterstützen, finden Sie im Abschnitt '"Unterstützte Virtualisierungsplattformen" (S. 33)'.

Wichtig
Die Agenten müssen mindestens einmal alle 30 Tage online sein. Anderenfalls werden ihre Pläne widerrufen und die Workloads sind dann nicht mehr geschützt.

In der nachfolgenden Tabelle werden die Workload-Typen und deren entsprechende Agenten zusammengefasst.

Workloadtyp	Agent	Beispiele (unvollständige Liste)
Physische Maschinen	Ein Protection Agent wird auf jeder geschützten Maschine installiert.	Workstation Laptop Server
Virtuelle Maschinen	Je nach Virtualisierungsplattform sind folgende Backup-Methoden verfügbar: • Agentenbasiertes Backup – Ein Protection Agent wird auf jeder geschützten Maschine installiert. • Agentenloses Backup – Ein Protection Agent wird nur auf dem Hypervisor-Host (auf einer dedizierten virtuellen Maschine) installiert oder als virtuelle Appliance bereitgestellt. Dieser Agent sichert alle virtuellen Maschinen in der Umgebung.	Virtuelle VMware-Maschine Virtuelle Hyper-V-Maschine Kernel-basierte virtuelle Maschinen (KVM), verwaltet von oVirt
Microsoft 365 Business-Workloads Google Workspace-Workloads	Diese Workloads werden von einem Cloud Agenten gesichert, der nicht installiert werden muss. Wenn Sie den Cloud Agenten verwenden wollen, müssen Sie Ihre Microsoft 365- bzw. Google Workspace-Organisation zur Cyber Protect-Konsole hinzufügen. Zusätzlich ist ein lokaler Agent für Office 365 verfügbar. Er erfordert eine Installation und kann nur zum Backup von Exchange Online-Postfächern verwendet werden. Weitere Informationen über die Unterschiede zwischen dem lokalen und dem Cloud Agenten finden Sie im Abschnitt '"Microsoft 365-Daten sichern" (S. 654)'. .	Microsoft 365-Postfach Microsoft 365 OneDrive Microsoft Teams SharePoint-Website Google-Postfach Google Drive
Applikationen	Die Daten spezifischer Applikationen werden durch spezielle Agenten gesichert, z.B. durch den Agenten für SQL, den Agenten für Exchange, den Agenten für MySQL/MariaDB oder den Agenten für Active Directory.	SQL-Server-Datenbanken MySQL/MariaDB-Datenbank

Workloadtyp	Agent	Beispiele (unvollständige Liste)
		Oracle-Datenbanken Active Directory
Mobilgeräte	Auf den zu schützenden Geräten wird eine Mobilgeräte-App installiert.	Android- oder iOS-Geräte
Websites	Die Websites werden von einem Cloud Agenten gesichert, der nicht installiert werden muss.	Websites, auf die über die Protokolle SFTP oder SSH zugegriffen wird

Weitere Informationen darüber, welchen Agenten Sie benötigen und wo Sie diesen installieren können, finden Sie im Abschnitt '"Welcher Agent wird wofür benötigt?" (S. 65)'

Workloads zur Cyber Protect-Konsole hinzufügen

Um mit dem Schutz Ihrer Workloads beginnen zu können, müssen Sie diese zuerst zur Cyber Protect-Konsole hinzufügen.

Hinweis
Die Workload-Typen, die Sie hinzufügen können, hängen davon ab, welche Service-Quotas für Ihr Konto zur Verfügung stehen. Wenn ein bestimmter Workload-Typ fehlt, wird er im Fensterbereich **Geräte hinzufügen** ausgegraut dargestellt.

Ein Partner-Administrator kann die benötigten Service-Quotas im Management-Portal aktivieren. Weitere Informationen finden Sie hier: "Informationen für Partner-Administratoren" (S. 366).

So können Sie einen Workload hinzufügen

1. Melden Sie sich an der Cyber Protect-Konsole an.
2. Gehen Sie zu **Geräte** –> **Alle Geräte** und klicken Sie dann auf **Hinzufügen**.
   Der Fensterbereich **Geräte hinzufügen** wird auf der rechten Seite geöffnet.
3. Wählen Sie den Release-Kanal.
4. Klicken Sie auf den Workload-Typ, den Sie hinzufügen wollen, und befolgen Sie dann die Anweisungen für den von Ihnen ausgewählten Workload.

In der nachfolgenden Tabelle werden die Workload-Typen und die erforderlichen Aktionen zusammengefasst.

Hinzufügende Workloads	Erforderliche Aktion	Zu befolgende Prozedur
Mehrere Windows-Maschinen	Führen Sie eine automatische Erkennung in Ihrer Umgebung durch. Um eine automatische Erkennung durchführen zu können, benötigen Sie mindestens eine Maschine in Ihrem lokalen Netzwerk oder Ihrer Active Directory-Domain, auf der ein Protection Agent installiert ist. Dieser Agent wird dann als sogenannter Discovery Agent verwendet.	"Automatische und manuelle Erkennung durchführen" (S. 138)
Windows-Workstations Windows-Server	Installieren Sie den Agenten für Windows.	"Protection Agenten in Windows installieren" (S. 82) oder "Unbeaufsichtigte Installation oder Deinstallation unter Windows" (S. 93)
macOS-Workstations	Installieren Sie den Agenten für macOS.	"Protection Agenten in macOS installieren" (S. 87) oder "Unbeaufsichtigte Installation oder Deinstallation unter macOS" (S. 119)
Linux-Server	Installieren Sie den Agenten für Linux.	"Protection Agenten in Linux installieren" (S. 84) oder "Unbeaufsichtigte Installation oder Deinstallation unter Linux" (S. 113)
Mobilgeräte (iOS, Android)	Installieren Sie die App für Mobilgeräte.	"Mobilgeräte sichern" (S. 645)
Cloud-zu-Cloud-Workloads		
Microsoft 365 Business	Fügen Sie Ihre Microsoft 365-Organisation zur Cyber Protect-Konsole hinzu und verwenden Sie den Cloud Agenten, um Exchange Online-Postfächer, OneDrive-Dateien, Microsoft-Teams und SharePoint-	"Microsoft 365-Daten sichern" (S. 654)

Hinzufügende Workloads	Erforderliche Aktion	Zu befolgende Prozedur
	Websites zu schützen. Alternativ können Sie auch den lokalen Agenten für Office 365 installieren. Mit diesem können Sie jedoch nur Exchange Online-Postfächer per Backup sichern. Weitere Informationen über die Unterschiede zwischen dem lokalen und dem Cloud Agenten finden Sie im Abschnitt '"Microsoft 365-Daten sichern" (S. 654)'.	
Google Workspace	Fügen Sie Ihre Google Workspace-Organisation zur Cyber Protect-Konsole hinzu und verwenden Sie den Cloud Agenten, um Google Mail-Postfächer und Google Drive-Dateien zu schützen.	"Google Workspace-Daten sichern" (S. 703)
Virtuelle Maschinen		
VMware ESXi	Stellen Sie den Agenten für VMware (Virtuelle Appliance) in Ihrer Umgebung bereit.	"Den Agenten für VMware (Virtuelle Appliance) bereitstellen" (S. 147)
	Installieren Sie den Agent für VMware (Windows) installieren.	"Protection Agenten in Windows installieren" (S. 82) oder "Unbeaufsichtigte Installation oder Deinstallation unter Windows" (S. 93)
Virtuozzo Hybrid Infrastructure	Stellen Sie den Agenten für Virtuozzo Hybrid Infrastructure (Virtuelle Appliance) in Ihrer Umgebung bereit.	"Den Agenten für Virtuozzo Hybrid Infrastructure (Virtuelle Appliance) bereitstellen" (S. 157)
Hyper-V	Installieren Sie den Agenten für Hyper-V.	"Protection Agenten in Windows installieren" (S. 82) oder "Unbeaufsichtigte Installation oder Deinstallation unter Windows" (S. 93)
Virtuozzo	Installieren Sie den Agenten für Virtuozzo.	"Protection Agenten in Linux installieren" (S. 84)

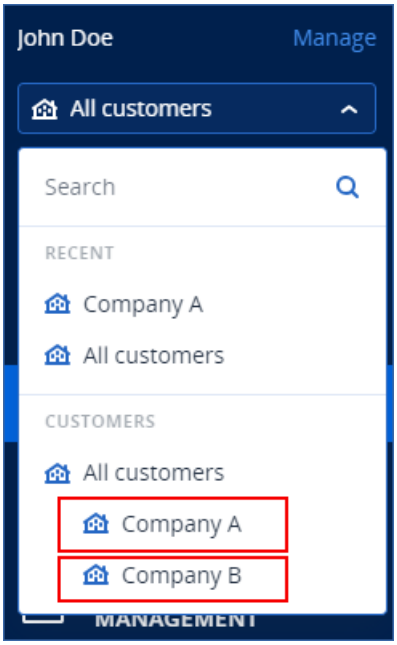
Hinzufügende Workloads	Erforderliche Aktion	Zu befolgende Prozedur
		oder "Unbeaufsichtigte Installation oder Deinstallation unter Linux" (S. 113)
KVM	Installieren Sie den Agenten für Windows.	"Protection Agenten in Windows installieren" (S. 82) oder "Unbeaufsichtigte Installation oder Deinstallation unter Windows" (S. 93)
	Installieren Sie den Agenten für Linux.	"Protection Agenten in Linux installieren" (S. 84) oder "Unbeaufsichtigte Installation oder Deinstallation unter Linux" (S. 113)
Red Hat Virtualization (oVirt)	Stellen Sie den Agenten für oVirt (Virtuelle Appliance) in Ihrer Umgebung bereit.	"Den Agenten für oVirt (Virtuelle Appliance) bereitstellen" (S. 166)
Citrix XenServer	Installieren Sie den Agenten für Windows.	"Protection Agenten in Windows installieren" (S. 82) oder "Unbeaufsichtigte Installation oder Deinstallation unter Windows" (S. 93)
	Installieren Sie den Agenten für Linux.	"Protection Agenten in Linux installieren" (S. 84) oder "Unbeaufsichtigte Installation oder Deinstallation unter Linux" (S. 113)
Nutanix AHV	Installieren Sie den Agenten für Windows.	"Protection Agenten in Windows installieren" (S. 82) oder "Unbeaufsichtigte Installation oder Deinstallation unter Windows" (S. 93)
	Installieren Sie den Agenten für Linux.	"Protection Agenten in Linux

Hinzufügende Workloads	Erforderliche Aktion	Zu befolgende Prozedur
		installieren" (S. 84) oder "Unbeaufsichtigte Installation oder Deinstallation unter Linux" (S. 113)
Oracle VM	Installieren Sie den Agenten für Windows.	"Protection Agenten in Windows installieren" (S. 82) oder "Unbeaufsichtigte Installation oder Deinstallation unter Windows" (S. 93)
	Installieren Sie den Agenten für Linux.	"Protection Agenten in Linux installieren" (S. 84) oder "Unbeaufsichtigte Installation oder Deinstallation unter Linux" (S. 113)
Scale Computing HC3	Stellen Sie den Agenten für Scale Computing HC3 (Virtuelle Appliance) in Ihrer Umgebung bereit.	"Den Agenten für Scale Computing HC3 (Virtuelle Appliance) bereitstellen" (S. 151)
NAS-Gerät (Network Attached Storage)		
Synology	Stellen Sie den Agenten für Synology (Virtuelle Appliance) in Ihrer Umgebung bereit.	"Den Agenten für Synology bereitstellen" (S. 173)
Applikationen		
Microsoft SQL Server	Installieren Sie den Agenten für SQL.	"Protection Agenten in Windows installieren" (S. 82) oder "Unbeaufsichtigte Installation oder Deinstallation unter Windows" (S. 93)
Microsoft Exchange Server	Installieren Sie den Agenten für Exchange.	
Microsoft Active Directory	Installieren Sie den Agenten für Active Directory.	
Oracle Database	Installieren Sie den Agenten für Oracle.	"Oracle Database sichern" (S. 732)
Website	Konfigurieren Sie die Verbindung zur Website.	"Websites und Webhosting-Server sichern" (S. 740)

Weitere Informationen über die verfügbaren Protection Agenten und wo Sie diesen installieren können, finden Sie im Abschnitt '"Welcher Agent wird wofür benötigt?" (S. 65)'

Informationen für Partner-Administratoren

- Es kann vorkommen, dass im Fensterbereich **Geräte hinzufügen** ein Workload-Typ fehlt, wenn eine erforderliche Service-Quota nicht im Management-Portal aktiviert wurde. Weitere Informationen darüber, welche Service-Quotas für welche Workloads erforderlich sind, finden Sie im Abschnitt Angebotselemente aktivieren oder deaktivieren in der Anleitung für Partner-Administratoren.
- Als Partner-Administrator können Sie keine Workloads auf der Ebene **Alle Kunden** hinzufügen. Wenn Sie einen Workload hinzufügen wollen, müssen Sie einen einzelnen Kunden-Mandanten auswählen.



Workloads aus der Cyber Protect-Konsole entfernen

Sie können Workloads, die Sie nicht mehr schützen müssen, aus der Cyber Protect-Konsole entfernen. Die Prozedur hängt vom jeweiligen Workload-Typ ab.

Alternativ dazu können Sie den Agenten auf dem geschützten Workload auch deinstallieren. Wenn Sie einen Agenten deinstallieren, wird der geschützte Workload automatisch aus der Cyber Protect-Konsole entfernt.

Wichtig
Wenn Sie einen Workload aus der Cyber Protect-Konsole entfernen, werden alle Pläne, die auf diesen Workload angewendet wurden, widerrufen. Durch das Entfernen eines Workloads werden jedoch keine Pläne oder Backups gelöscht. Und auch der Protection Agent wird nicht deinstalliert.

In der nachfolgenden Tabelle werden die Workload-Typen und die erforderlichen Aktionen zusammengefasst.

Zu entfernende Workloads	Erforderliche Aktionen	Zu befolgende Prozedur
Physische und virtuelle Maschinen		
Physische oder virtueelle Maschinen, auf denen ein Protection Agent installiert ist.	1. Entfernen Sie den Workload aus der Cyber Protect-Konsole. 2. [Optional] Deinstallieren Sie den Protection Agenten.	"So können Sie einen Workload aus der Cyber Protect-Konsole entfernen" (S. 369) (Workload mit Protection Agent)
Virtuelle Maschinen, die auf Hypervisor-Ebene gesichert werden (agentenloses Backup)	1. Entfernen Sie in der Cyber Protect-Konsole diejenige Maschine, auf welcher der Protection Agent installiert ist. Alle virtuellen Maschinen, die von diesem Agenten gesichert werden, werden automatisch aus der Konsole entfernt. 2. [Optional] Deinstallieren Sie den Protection Agenten.	"So können Sie einen Workload aus der Cyber Protect-Konsole entfernen" (S. 369) (Workload ohne einen Protection Agenten)
Cloud-zu-Cloud-Workloads		
Microsoft 365 Business-Workloads Google Workspace-Workloads	Löschen Sie die Microsoft 365- oder Google Workspace-Organisation aus der Cyber Protect-Konsole. Alle Ressourcen in	"So können Sie einen Workload aus der Cyber Protect-Konsole entfernen" (S. 369) (Cloud-zu-Cloud-Workload)

Zu entfernende Workloads	Erforderliche Aktionen	Zu befolgende Prozedur
	dieser Organisation werden automatisch aus der Konsole entfernt.	
Mobilgeräte		
Android-Geräte iOS-Geräte	1. Entfernen Sie das Mobilgerät aus der Cyber Protect-Konsole. 2. [Optional] Deinstallieren Sie die App auf dem Mobilgerät.	"So können Sie einen Workload aus der Cyber Protect-Konsole entfernen" (S. 369) (Mobilgerät)
NAS-Gerät (Network Attached Storage)		
Synology	1. Entfernen Sie den Workload aus der Cyber Protect-Konsole. 2. [Optional] Deinstallieren Sie den Protection Agenten.	"So können Sie einen Workload aus der Cyber Protect-Konsole entfernen" (S. 369) (Workload mit einem Protection Agenten)
Applikationen		
Microsoft SQL Server Microsoft Exchange Server Microsoft Active Directory Oracle Database	1. Entfernen Sie in der Cyber Protect-Konsole diejenige Maschine, auf welcher der Protection Agent installiert ist. Die Objekte, die von diesem Agenten gesichert werden, werden automatisch aus der Konsole	"So können Sie einen Workload aus der Cyber Protect-Konsole entfernen" (S. 369) (Workload ohne einen Protection Agenten)

Zu entfernende Workloads	Erforderliche Aktionen	Zu befolgende Prozedur
	entfernt. 2. [Optional] Deinstallieren Sie den Protection Agenten.	
Websites	Entfernen Sie die Website aus der Cyber Protect-Konsole.	"So können Sie einen Workload aus der Cyber Protect-Konsole entfernen" (S. 369) (Website)

So können Sie einen Workload aus der Cyber Protect-Konsole entfernen

Workload mit einem Protection Agenten

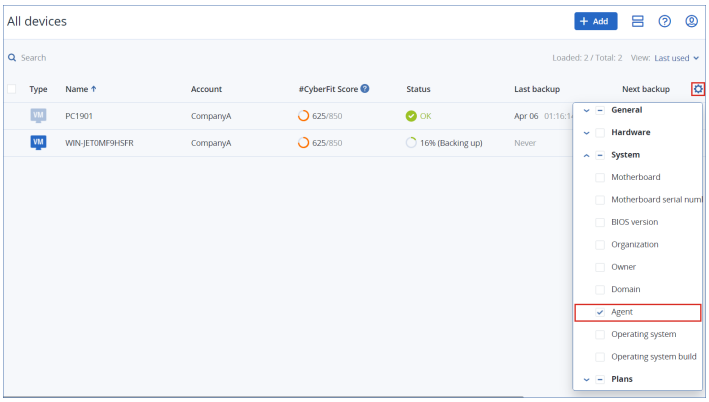
Sie können diese Art von Workload direkt entfernen.

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte** –> **Alle Geräte**.
2. Aktivieren Sie das jeweilige Kontrollkästchen neben einem oder mehreren Workloads, den/die Sie entfernen wollen.
3. Klicken Sie im Fensterbereich **Aktionen** auf den Befehl **Löschen**.
4. Bestätigen Sie Ihre Auswahl, indem Sie auf **Löschen** klicken.
5. [Optional] Deinstallieren Sie den Agenten wie im Abschnitt '"Agenten deinstallieren" (S. 196)' beschrieben.

Workload ohne einen Protection Agenten

Wenn Sie diesen Workload-Typ entfernen wollen, müssen Sie die Maschine entfernen, auf welcher der Protection Agent installiert ist.

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte** –> **Alle Geräte**.
2. Klicken Sie in der rechten oberen Ecke auf das Zahnradsymbol und aktivieren Sie dann das Kontrollkästchen für **Agent**.



Die Spalte **Agent** wird angezeigt.

3. Aktivieren Sie in der Spalte **Agent** das Kontrollkästchen für den Namen der Maschine, auf welcher der Protection Agent installiert ist.
4. Aktivieren Sie in der Cyber Protect-Konsole das Kontrollkästchen neben derjenigen Maschine, auf welcher der Protection Agent installiert ist.
5. Klicken Sie im Fensterbereich **Aktionen** auf den Befehl **Löschen**.
6. Bestätigen Sie Ihre Auswahl, indem Sie auf **Löschen** klicken.
7. [Optional] Deinstallieren Sie den Agenten wie im Abschnitt '"Agenten deinstallieren" (S. 196)' beschrieben.

Cloud-zu-Cloud-Workload

Wenn Sie Workloads entfernen wollen, die durch den Cloud Agenten gesichert werden, müssen Sie Ihre Microsoft 365- oder Google Workspace-Organisation aus der Cyber Protect-Konsole löschen.

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte** –> **Microsoft 365** oder **Geräte** –> **Google Workspace**.
2. Klicken Sie auf den Namen Ihrer Microsoft 365- oder Google Workspace-Organisation.
3. Klicken Sie im Fensterbereich **Aktionen** auf den Befehl **Gruppe löschen**.
4. Klicken Sie auf **Löschen**, um Ihre Aktion zu bestätigen.

Mobilgerät

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte** –> **Alle Geräte**.
2. Aktivieren Sie das Kontrollkästchen neben dem Workload, den Sie löschen wollen.
3. Klicken Sie im Fensterbereich **Aktionen** auf den Befehl **Löschen**.
4. Bestätigen Sie Ihre Auswahl, indem Sie auf **Löschen** klicken.
5. [Optional] Deinstallieren Sie die App vom Mobilgerät.

Website

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte** –> **Alle Geräte**.
2. Aktivieren Sie das Kontrollkästchen neben dem Workload, den Sie löschen wollen.
3. Klicken Sie im Fensterbereich **Aktionen** auf den Befehl **Löschen**.
4. Bestätigen Sie Ihre Auswahl, indem Sie auf **Löschen** klicken.

Gerätegruppen

Mit Gerätegruppen können Sie mehrere Workloads, die sich in bestimmten Aspekten ähneln, mit einem Gruppenplan schützen. Der Plan wird auf die Gruppe als Ganzes angewendet und kann von keinem Mitglied der Gruppe widerrufen werden.

Ein Workload kann mehreren Gruppen angehören. Ein Workload, der zu einer Gerätegruppe gehört, kann dennoch auch durch individuelle Pläne geschützt werden.

Sie können nur Workloads zu einer Gerätegruppe hinzufügen, die demselben Typ angehören. Beispiel: Sie können unter **Hyper-V** nur Gruppen von virtuellen Hyper-V-Maschinen erstellen. Unter **Maschinen mit Agenten** können Sie nur Gruppen von Maschinen erstellen, auf denen Agenten installiert sind.

Sie können keine Gerätegruppen innerhalb einer Gruppe vom Typ **Alle** (wie der Stammgruppe **Alle Geräte**) oder innerhalb von integrierten Gruppen wie **Maschinen mit Agenten** –> **Alle**, **Microsoft 365** –> Ihre Organisation –> **Benutzer** –> **Alle Benutzer** erstellen.

Integrierte Gruppen und benutzerdefinierte Gruppen

Vorgegebene Gruppen

Nachdem Sie einen Workload in der Cyber Protect-Konsole registriert haben, wird der Workload in einer der integrierten Stammgruppen auf der Registerkarte **Geräte** angezeigt – z.B. **Maschinen mit Agenten**, **Microsoft 365** oder **Hyper-V**.

Auch alle registrierten Nicht-Cloud-zu-Cloud-Workloads werden in der Stammgruppe **Alle Geräte** aufgeführt. Eine separate integrierte Stammgruppe, die nach Ihrem Mandanten benannt ist, enthält alle Nicht-Cloud-zu-Cloud-Workloads und alle Abteilungen in diesem Mandanten.

Sie können Stammgruppen weder löschen noch bearbeiten und auch keine Pläne auf diese anwenden.

Einige der Stammgruppen enthalten eine oder mehrere Ebenen von integrierten Untergruppen – z.B. **Maschinen mit Agenten** –> **Alle**, **Microsoft 365** –> Ihre Organisation –> **Teams** –> **Alle Teams**, **Google Workspace** –> Ihre Organisation –> **Shared Drives** –> **Alle Shared Drives**.

Sie können integrierte Untergruppen weder bearbeiten noch löschen.

Benutzerdefinierte Gruppen

Alle Workloads in einer integrierten Gruppe zu schützen, ist möglicherweise nicht zweckmäßig, weil es Workloads geben könnte, die andere Schutzeinstellungen oder eine andere Planung benötigen.

In einigen Stammgruppen (z.B. in **Maschinen mit Agenten**, **Microsoft 365** oder **Google Workspace**) können Sie eigene Untergruppen erstellen. Diese Untergruppen können statisch oder dynamisch sein.

Sie können jede benutzerdefinierte Gruppe bearbeiten, umbenennen oder löschen.

Statische Gruppen und dynamische Gruppen

Sie können folgende Arten von benutzerdefinierten Gruppen erstellen:

- Statisch
- Dynamisch

Statische Gruppen

Statische Gruppen enthalten manuell hinzugefügte Workloads.

Der Inhalt einer statischen Gruppe ändert sich nur dann, wenn Sie einen Workload explizit hinzufügen oder entfernen.

Beispiel: Sie erstellen eine statische Gruppe für die Buchhaltung in Ihrem Unternehmen und fügen dann die Maschinen der jeweiligen Buchhalter manuell zu dieser Gruppe hinzu. Wenn Sie einen Gruppenplan anwenden, werden die Maschinen in dieser Gruppe geschützt. Wenn ein neuer Buchhalter eingestellt wird, so müssen Sie dessen Maschine manuell zu der statischen Gruppe hinzufügen.

Dynamische Gruppen

Dynamische Gruppen enthalten Workloads, die bestimmte Kriterien erfüllen. Sie können diese Kriterien im Voraus definieren, indem Sie eine Suchanfrage erstellen, die bestimmte Attribute (z.B. `osType`), deren Werte (z.B. `Windows`) und Suchoperatoren (z.B. `IN`) enthält.

So können Sie beispielsweise eine dynamische Gruppe für alle Maschinen erstellen, die unter Windows laufen, oder eine dynamische Gruppe, die alle Benutzer in Ihrer Microsoft 365-Organisation enthält, deren E-Mail-Adressen mit dem Namen `john` beginnen.

Alle Workloads, die die erforderlichen Attribute und Werte aufweisen, werden der Gruppe automatisch hinzugefügt – während alle Workloads, die ein erforderliches Attribut oder einen Wert verlieren, wieder automatisch aus der Gruppe entfernt werden.

Beispiel 1: Die Host-Namen der Maschinen, die zur Buchhaltungsabteilung gehören, enthalten alle den Begriff Buchhaltung. Sie suchen nach den Maschinen, die den Begriff Buchhaltung im Namen enthalten, und speichern die Suchergebnisse dann als dynamische Gruppe. Dann wenden Sie einen Schutzplan auf die Gruppe an. Wenn ein neuer Buchhalter eingestellt wird, wird dessen Maschine den Begriff Buchhaltung im Namen haben und daher automatisch zur dynamischen Gruppe hinzugefügt, sobald Sie diese Maschine in der Cyber Protect-Konsole registrieren.

Beispiel 2: Die Buchhaltungsabteilung bildet eine eigene Active Directory-Organisationseinheit (Organizational Unit, OU). Sie spezifizieren die Buchhaltungs-Organisationseinheit als erforderliches Attribut und speichern dann die Suchergebnisse als dynamische Gruppe. Dann wenden Sie einen Schutzplan auf die Gruppe an. Wenn ein neuer Buchhalter eingestellt wird, wird dessen Maschine der dynamischen Gruppe hinzugefügt, sobald sie der Active Directory-Organisationseinheit hinzugefügt und in der Cyber Protect-Konsole registriert wird (unabhängig davon, was zuerst eintritt).

Cloud-zu-Cloud-Gruppen und Nicht-Cloud-zu-Cloud-Gruppen

Cloud-zu-Cloud-Gruppen enthalten Microsoft 365- oder Google Workspace-Workloads, die von einem Cloud Agenten gesichert werden.

Nicht-Cloud-zu-Cloud-Gruppen enthalten alle anderen Workload-Typen.

Unterstützte Pläne für Gerätegruppen

In der nachfolgenden Tabelle werden die Pläne zusammengefasst, die Sie auf eine Gerätegruppe anwenden können.

Gruppe	Verfügbare Pläne	Plan-Standort
Cloud-zu-Cloud-Workloads (Microsoft 365- und Google Workspace-Workloads)	Backup-Plan	**Verwaltung** –> **Cloud-Applikationen-Backup**
Nicht-Cloud-zu-Cloud-Workloads	Schutzplan	**Verwaltung** –> **Schutzpläne**
	Remote-Verwaltungsplan	**Verwaltung** –> **Remote-Verwaltungspläne**
	Skripting-Plan	**Verwaltung** –> **Skripting-Pläne**

Cloud-Ressourcen (wie Microsoft 365- oder Google Workspace-Benutzer, OneDrive- und Google Drive-Freigaben, Microsoft Teams oder Azure AD-Gruppen) werden mit der Cyber Protect-Konsole synchronisiert, gleich nachdem Sie eine Microsoft 365- oder Google Workspace-Organisation zur Konsole hinzugefügt haben. Alle weiteren Änderungen in einer Organisation werden einmal pro Tag synchronisiert.

Wenn Sie eine Änderung sofort synchronisieren wollen, gehen Sie in der Cyber Protect-Konsole zu **Geräte** –> **Microsoft 365** oder zu **Geräte** –> **Google Workspace**, wählen Sie die gewünschte Organisation aus und klicken Sie anschließend auf **Aktualisieren**.

Eine statische Gruppe erstellen

Sie können eine leere statische Gruppe erstellen und dieser dann Workloads hinzufügen.

Sie können auch Workloads auswählen und anhand Ihrer Auswahl eine neue statische Gruppe erstellen.

Sie können keine Gerätegruppen innerhalb einer Gruppe vom Typ **Alle** (wie der Stammgruppe **Alle Geräte**) oder innerhalb von integrierten Gruppen wie **Maschinen mit Agenten** –> **Alle**, **Microsoft 365** –> Ihre Organisation –> **Benutzer** –> **Alle Benutzer** erstellen.

So können Sie eine statische Gruppe erstellen

Im Hauptfenster

1. Klicken Sie auf **Geräte** und wählen Sie die Stammgruppe aus, die die Workloads enthält, für die Sie eine statische Gruppe erstellen wollen.
2. [Optional] Wenn Sie eine verschachtelte Gruppe erstellen möchten, gehen Sie zunächst zu einer bestehenden statischen Gruppe.

Hinweis
Das Erstellen von verschachtelten statischen Gruppen ist für Cloud-zu-Cloud-Workloads nicht verfügbar.

3. Klicken Sie unter dem Gruppen-Verzeichnisbaum auf **+ Neue statische Gruppe** oder klicken Sie im Fensterbereich **Aktionen** auf **Neue statische Gruppe**.
4. Spezifizieren Sie einen Namen für die neue Gruppe.
5. [Optional] Geben Sie einen Kommentar für die Gruppe ein.
6. Klicken Sie auf **OK**.

Im Gruppen-Verzeichnisbaum

1. Klicken Sie auf **Geräte** und wählen Sie die Stammgruppe aus, die die Workloads enthält, für die Sie eine statische Gruppe erstellen wollen.
2. Klicken Sie neben dem Namen der Gruppe, in der Sie eine neue statische Gruppe erstellen wollen, auf das Zahnradsymbol.

Hinweis
Das Erstellen von verschachtelten statischen Gruppen ist für Cloud-zu-Cloud-Workloads nicht verfügbar.

3. Klicken Sie auf **Neue statische Gruppe**.
4. Spezifizieren Sie einen Namen für die neue Gruppe.
5. [Optional] Geben Sie einen Kommentar für die Gruppe ein.
6. Klicken Sie auf **OK**.

Über die Auswahl

1. Klicken Sie auf **Geräte** und wählen Sie die Stammgruppe aus, die die Workloads enthält, für die Sie eine statische Gruppe erstellen wollen.

Hinweis
Sie können keine Gerätegruppen innerhalb einer Gruppe vom Typ **Alle** (wie der Stammgruppe **Alle Geräte**) oder innerhalb von integrierten Gruppen wie **Maschinen mit Agenten** –> **Alle**, **Microsoft 365** –> Ihre Organisation –> **Benutzer** –> **Alle Benutzer** erstellen.

2. Aktivieren Sie die Kontrollkästchen neben den Workloads, für die Sie eine neue Gruppe erstellen wollen, und klicken Sie anschließend auf **Zur Gruppe hinzufügen**.
3. Wählen Sie im Verzeichnisbaum die übergeordnete Ebene für die neue Gruppe und klicken Sie anschließend auf **Neue statische Gruppe**.

Hinweis
Das Erstellen von verschachtelten statischen Gruppen ist für Cloud-zu-Cloud-Workloads nicht verfügbar.

4. Spezifizieren Sie einen Namen für die neue Gruppe.
5. [Optional] Geben Sie einen Kommentar für die Gruppe ein.
6. Klicken Sie auf **OK**.
   Die neue Gruppe erscheint im Verzeichnisbaum.
7. Klicken Sie auf **Fertig**.

Workloads zu einer statischen Gruppe hinzufügen

Sie können zuerst die Zielgruppe auswählen und ihr dann Workloads hinzufügen.

Alternativ können Sie auch zuerst die Workloads auswählen und diese dann einer Gruppe hinzufügen.

So können Sie Workloads zu einer statischen Gruppe hinzufügen

Zuerst die Zielgruppe auswählen

1. Klicken Sie auf **Geräte** und gehen Sie dann zu Ihrer Zielgruppe.
2. Wählen Sie die Zielgruppe und klicken Sie anschließend auf **Geräte hinzufügen**.
3. Wählen Sie im Verzeichnisbaum die Gruppe aus, die die gewünschten Workloads enthält.
4. Aktivieren Sie die Kontrollkästchen neben den Workloads, die Sie hinzufügen wollen, und klicken Sie anschließend auf **Hinzufügen**.

Zuerst die Workloads auswählen

1. Klicken Sie auf **Geräte** und wählen Sie dann die Stammgruppe aus, die die gewünschten Workloads enthält.
2. Aktivieren Sie die Kontrollkästchen neben den Workloads, die Sie hinzufügen wollen, und klicken Sie anschließend auf **Zur Gruppe hinzufügen**.
3. Wählen Sie im Verzeichnisbaum die Zielgruppe aus und klicken Sie anschließend auf **Fertig**.

Eine dynamische Gruppe erstellen

Sie können eine dynamische Gruppe erstellen, indem Sie nach Workloads suchen, die bestimmte Attribute aufweisen, deren Werte Sie wiederum in einer Suchabfrage definieren. Dann speichern Sie die Suchergebnisse als dynamische Gruppe.

Die Attribute, die für die Suche und Erstellung dynamischer Gruppen unterstützt werden, unterscheiden sich für Cloud-zu-Cloud-Workloads und Nicht-Cloud-zu-Cloud-Workloads. Weitere Informationen zu unterstützten Attributen finden Sie unter "Suchattribute für Nicht-Cloud-zu-Cloud-Workloads" (S. 379) und "Suchattribute für Cloud-zu-Cloud-Workloads" (S. 378).

Dynamische Gruppen werden in ihren jeweiligen Stammgruppen erstellt. Verschachtelte dynamische Gruppen werden nicht unterstützt.

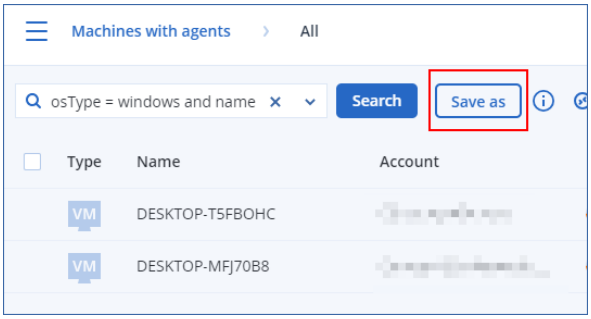
Sie können keine Gerätegruppen innerhalb einer Gruppe vom Typ **Alle** (wie der Stammgruppe **Alle Geräte**) oder innerhalb von integrierten Gruppen wie **Maschinen mit Agenten** –> **Alle**, **Microsoft 365** –> Ihre Organisation –> **Benutzer** –> **Alle Benutzer** erstellen.

So können Sie eine dynamische Gruppe erstellen

Nicht-Cloud-zu-Cloud-Workloads

1. Klicken Sie auf **Geräte** und wählen Sie die Gruppe aus, die die Workloads enthält, für die Sie eine neue dynamische Gruppe erstellen wollen.
2. Sie können nach Workloads suchen, indem Sie die unterstützten Suchattribute und Operatoren verwenden.

   Sie können mehrere Attribute und Operatoren in einer einzigen Abfrage verwenden. Weitere Informationen zu den unterstützten Attributen finden Sie unter "Suchattribute für Nicht-Cloud-zu-Cloud-Workloads" (S. 379).
3. Klicken Sie neben dem Suchfeld auf **Speichern unter**.



Hinweis
Die Schaltfläche **Speichern unter** ist nicht verfügbar, wenn Sie keine dynamische Gruppe auf einer bestimmten Ebene erstellen dürfen. Zum Beispiel in der Hauptgruppe **Geräte** > **Alle Geräte**.

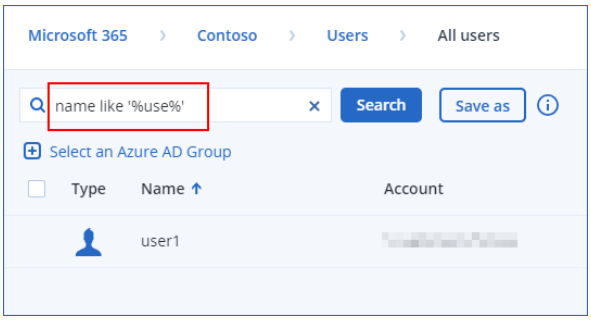
Wählen Sie eine andere Ebene (zum Beispiel: **Geräte** > **Maschinen mit Agenten** > **Alle**) und wiederholen Sie dann die oben genannten Schritte. Mit dieser Suche können Sie eine dynamische Gruppe innerhalb von **Maschinen mit Agenten** erstellen und nicht innerhalb von **Maschinen mit Agenten** > **Alle**.

4. Spezifizieren Sie einen Namen für die neue Gruppe.
5. [Optional] Geben Sie im Feld **Kommentar** eine Beschreibung für die neue Gruppe ein.
6. Klicken Sie auf **OK**.

Cloud-zu-Cloud-Workloads

1. Klicken Sie auf **Geräte** und wählen Sie dann **Microsoft 365** oder **Google Workspace**.
2. Wählen Sie die Gruppe aus, die die Workloads enthält, für die Sie eine neue dynamische Gruppe erstellen möchten. Zum Beispiel, **Benutzer** > **Alle Benutzer**.
3. Sie können nach Workloads suchen, indem Sie die unterstützten Suchattribute und Operatoren verwenden oder indem Sie Microsoft 365-Benutzer aus einer bestimmten Active Directory-Gruppe auswählen.

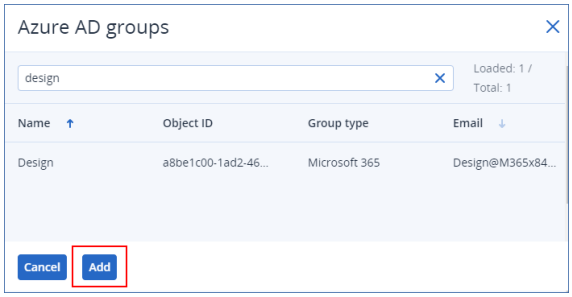
   Sie können mehrere Attribute und Operatoren in einer einzigen Abfrage verwenden. Weitere Informationen zu den unterstützten Attributen finden Sie unter "Suchattribute für Cloud-zu-Cloud-Workloads" (S. 378).



4. [Nur für **Microsoft 365** > **Benutzer**] Um Benutzer aus einer bestimmten Active Directory-Gruppe auszuwählen, gehen Sie wie folgt vor:
   a. Navigieren Sie zu **Benutzer** > **Alle Benutzer**.
   b. Klicken Sie auf **Wählen Sie eine Azure AD-Gruppe**.

      Es wird eine Liste der Active Directory-Gruppen in Ihrer Organisation geöffnet.

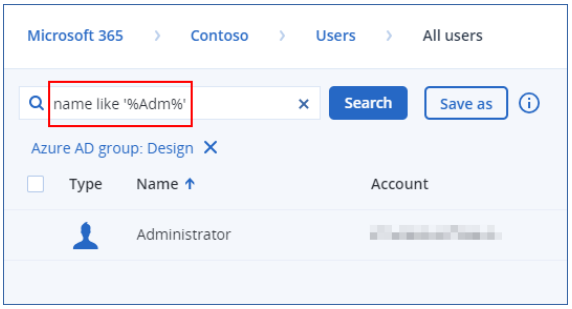
      Sie können in dieser Liste nach einer bestimmten Gruppe suchen oder die Gruppen nach Namen oder E-Mail sortieren.
   c. Wählen Sie die gewünschte Active Directory-Gruppe aus und klicken Sie anschließend auf **Hinzufügen**.



   d. [Optional] Wenn Sie bestimmte Benutzer in die ausgewählte Active Directory-Gruppe aufnehmen oder von dieser ausschließen wollen, können Sie eine Suchabfrage erstellen, indem Sie die unterstützten Suchattribute und Operatoren verwenden.

      Sie können mehrere Attribute und Operatoren in einer einzigen Abfrage verwenden. Weitere Informationen zu den unterstützten Attributen finden Sie unter "Suchattribute für Cloud-zu-

Cloud-Workloads" (S. 378).



5. Klicken Sie neben dem Suchfeld auf **Speichern unter**.

Hinweis
Die Schaltfläche **Speichern unter** ist nicht verfügbar, wenn Sie keine dynamische Gruppe auf einer bestimmten Ebene erstellen dürfen. Zum Beispiel in **Microsoft 365** > Ihre Organisation > **Benutzer**.

Wählen Sie eine andere Ebene (zum Beispiel: **Microsoft 365** > Ihre Organisation > **Benutzer** > **Alle**) und wiederholen Sie dann die oben genannten Schritte. Mit dieser Suche können Sie eine dynamische Gruppe innerhalb von **Microsoft 365** > Ihre Organisation > **Benutzer** > erstellen und nicht innerhalb von **Benutzer** > **Alle**.

6. Spezifizieren Sie einen Namen für die neue Gruppe.
7. [Optional] Geben Sie im Feld **Kommentar** eine Beschreibung für die neue Gruppe ein.
8. Klicken Sie auf **OK**.

Suchattribute für Cloud-zu-Cloud-Workloads

In der nachfolgenden Tabelle sind die Attribute zusammengefasst, die Sie in Ihren Suchanfragen für Microsoft 365- und Google Workspace-Workloads verwenden können.

Informationen darüber, welche Attribute Sie in Suchabfragen für andere Workload-Typen verwenden können, finden Sie im Abschnitt '"Suchattribute für Nicht-Cloud-zu-Cloud-Workloads" (S. 379)'.

Attribut	Bedeutung	Kann verwendet werden in	Beispiele für Suchanfragen	Für Gruppenerstellung unterstützt
`name`	Anzeigename eines Microsoft 365- oder Google Workspace-Workloads	Alle Cloud-zu-Cloud-Ressourcen	`name = 'My Name'` `name LIKE '*nam*'`	Ja
`email`	E-Mail-Adresse	Microsoft 365 –> Gruppen	`email = 'my_group_email@mycompany.com'`	Ja

Attribut	Bedeutung	Kann verwendet werden in	Beispiele für Suchanfragen	Für Gruppenerstellung unterstützt
	für einen Microsoft 365-Benutzer bzw. eine -Gruppe oder einen Google Workspace-Benutzer	Microsoft 365 –> Benutzer Google Workspace –> Benutzer	`email LIKE '*@company*'` `email NOT LIKE '*enterprise.com'`	
`siteName`	Name einer Site, die mit einer Microsoft 365-Gruppe verbunden ist	Microsoft 365 –> Gruppen	`siteName = 'my_site'` `siteName LIKE '*company.com*support*'`	Ja
`url`	Webadresse für eine Microsoft 365-Gruppe oder -SharePoint-Website	Microsoft 365 –> Gruppen Microsoft 365 –> Website-Sammlungen	`url = 'https://www.mycompany.com/'` `url LIKE '*www.mycompany.com*'`	Ja

Suchattribute für Nicht-Cloud-zu-Cloud-Workloads

In der nachfolgenden Tabelle sind die Attribute zusammengefasst, die Sie in Ihren Suchanfragen für Nicht-Cloud-zu-Cloud-Workloads verwenden können.

Informationen darüber, welche Attribute Sie in Suchabfragen für Cloud-zu-Cloud-Workloads verwenden können, finden Sie im Abschnitt '"Suchattribute für Cloud-zu-Cloud-Workloads" (S. 378)'.

Attribut	Bedeutung	Beispiele für Suchanfragen	Für Gruppenerstellung unterstützt
Allgemein			
`name`	Workload-Name, wie etwa: • Host-Name für physische Maschinen • Name für virtuelle Maschinen • Datenbankname • E-Mail-Adresse für	`name = 'en-00'`	Ja

Attribut	Bedeutung	Beispiele für Suchanfragen	Für Gruppenerstellung unterstützt
	Postfächer		
`id`	Geräte-ID. So können Sie die Geräte-ID einsehen: Wählen Sie bei **Geräte** das gewünschte Gerät aus und klicken Sie dann auf **Details** –> **Alle Eigenschaften**. Die ID wird im Feld `id` angezeigt.	`id != '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Ja
`resourceType`	Workload-Typ. Mögliche Werte: • `'machine'` • `'exchange'` • `'mssql_server'` • `'mssql_instance'` • `'mssql_database'` • `'mssql_database_folder'` • `'msexchange_database'` • `'msexchange_storage_group'` • `'msexchange_mailbox.msexchange'` • `'msexchange_mailbox.office365'` • `'mssql_aag_group'` • `'mssql_aag_database'` • `'virtual_machine.vmww'` • `'virtual_machine.vmwesx'` • `'virtual_host.vmwesx'` • `'virtual_cluster.vmwesx'` • `'virtual_appliance.vmwesx'`	`resourceType = 'machine'` `resourceType in ('mssql_aag_database', 'mssql_database')`	Ja

Attribut	Bedeutung	Beispiele für Suchanfragen	Für Gruppenerstellung unterstützt
	• 'virtual_application.vmwesx' • 'virtual_resource_pool.vmwesx' • 'virtual_center.vmwesx' • 'datastore.vmwesx' • 'datastore_cluster.vmwesx' • 'virtual_network.vmwesx' • 'virtual_data_center.vmwesx' • 'virtual_machine.vmww' • 'virtual_cluster.mshyperv' • 'virtual_machine.mshyperv' • 'virtual_host.mshyperv' • 'virtual_network.mshyperv' • 'virtual_folder.mshyperv' • 'virtual_data_center.mshyperv' • 'datastore.mshyperv' • 'virtual_machine.msvs' • 'virtual_machine.parallelsw' • 'virtual_host.parallelsw' • 'virtual_cluster.parallelsw' • 'virtual_machine.rhev' • 'virtual_machine.kvm' • 'virtual_machine.xen' • 'bootable_media'		

Attribut	Bedeutung	Beispiele für Suchanfragen	Für Gruppenerstellung unterstützt
`chassis`	Gehäusetyp. Mögliche Werte: • `laptop` • `desktop` • `server` • `other` • `unknown`	`chassis = 'laptop'` `chassis IN ('laptop', 'desktop')`	Ja
`ip`	IP-Adresse (nur für physische Maschinen).	`ip RANGE ('10.250.176.1','10.250.176.50')`	Ja
`comment`	Kommentar für ein Gerät. Er kann automatisch oder manuell spezifiziert werden. Standardwert: • Bei physischen Maschinen, die unter Windows laufen, wird die Computer-Beschreibung in Windows automatisch als Kommentar übernommen. Dieser Wert wird alle 15 Minuten synchronisiert. • Leer für andere Geräte.	`comment = 'important machine'` `comment = ''` (alle Maschinen ohne Kommentar)	Ja

Attribut	Bedeutung	Beispiele für Suchanfragen	Für Gruppenerstellung unterstützt

	Hinweis
	Die automatische Synchronisierung wird deaktiviert, wenn im Kommentarfeld manuell Text hinzugefügt wird. Wenn Sie die Synchronisierung wieder aktivieren wollen, müssen Sie den Text löschen.
	
	Um die automatisch synchronisierten Kommentare für Ihre Workloads aktualisieren zu können, müssen Sie den Managed Machine Service in den **Windows-Diensten** neu starten oder folgende Befehle in der Eingabeaufforderung ausführen:
	`net stop mms`
	`net start mms`
	
	Wenn Sie einen Gerätekommentar einsehen wollen, wählen Sie unter **Geräte** das entsprechende Geräte aus, klicken Sie dann auf **Details** und suchen Sie anschließend den Abschnitt **Kommentar**.
	
	Wenn Sie einen Kommentar manuell hinzufügen oder ändern wollen, klicken Sie auf **Hinzufügen** oder		

Attribut	Bedeutung	Beispiele für Suchanfragen	Für Gruppenerstellung unterstützt
	Bearbeiten. Bei Geräten, auf denen ein Protection Agent installiert ist, gibt es zwei separate Kommentarfelder: • Agenten-Kommentar ◦ Bei physischen Maschinen, die unter Windows laufen, wird die Computer-Beschreibung in Windows automatisch als Kommentar übernommen. Dieser Wert wird alle 15 Minuten synchronisiert. ◦ Leer für andere Geräte. **Hinweis** Die automatische Synchronisierung wird deaktiviert, wenn im Kommentarfeld manuell Text hinzugefügt wird. Wenn Sie die Synchronisierung wieder aktivieren wollen, müssen Sie den Text löschen. • Geräte-Kommentar ◦ Wenn der Agenten-Kommentar automatisch spezifiziert wird, wird er als Geräte-		

Attribut	Bedeutung	Beispiele für Suchanfragen	Für Gruppenerstellung unterstützt
	Kommentar kopiert. Manuell hinzugefügte Agenten-Kommentare werden nicht als Geräte-Kommentare kopiert. ◦ Geräte-Kommentare werden nicht als Agenten-Kommentare kopiert. Für ein Gerät können einer oder beide Kommentare spezifiziert werden – oder beide können auch leer bleiben. Wenn beide Kommentare spezifiziert sind, hat der Geräte-Kommentar die höhere Priorität. Wenn Sie einen Agenten-Kommentar einsehen wollen, wählen Sie unter **Einstellungen** – > **Agenten** das Geräte mit dem Agenten aus, klicken Sie dann auf **Details** und suchen Sie anschließend den Bereich **Kommentar**. Wenn Sie einen Gerätekommentar einsehen wollen, wählen Sie unter **Geräte** das entsprechende Geräte aus, klicken Sie dann auf		

Attribut	Bedeutung	Beispiele für Suchanfragen	Für Gruppenerstellung unterstützt
	Details und suchen Sie anschließend den Abschnitt **Kommentar**. Wenn Sie einen Kommentar manuell hinzufügen oder ändern wollen, klicken Sie auf **Hinzufügen** oder **Bearbeiten**.		
`isOnline`	Workload-Verfügbarkeit. Mögliche Werte: • `true` • `false`	`isOnline = true`	Nein
`hasAsz`	Secure Zone-Verfügbarkeit. Mögliche Werte: • `true` • `false`	`hasAsz = true`	Ja

`tzOffset`	Abweichung der Zeitzone von der Koordinierten Weltzeit (UTC) in Minuten.	`tzOffset = 120`
		`tzOffset > 120`
		`tzOffset < 120`
			Ja

CPU, Arbeitsspeicher, Laufwerke			
`cpuArch`	CPU-Architektur. Mögliche Werte: • `'x64'` • `'x86'`	`cpuArch = 'x64'`	Ja
`cpuName`	CPU-Name.	`cpuName LIKE '%XEON%'`	Ja
`memorySize`	RAM-Größe in Megabytes.	`memorySize < 1024`	Ja
`diskSize`	Die Laufwerksgröße in Gigabyte oder Megabyte (nur für physische Maschinen).	`diskSize < 300GB` `diskSize >= 3000000MB`	Nein

Attribut	Bedeutung	Beispiele für Suchanfragen	Für Gruppenerstellung unterstützt
Betriebssystem			
`osName`	Betriebssystemname.	`osName LIKE '%Windows XP%'`	Ja
`osType`	Betriebssystemtyp. Mögliche Werte: • `'windows'` • `'linux'` • `'macosx'`	`osType = 'windows'` `osType IN ('linux', 'macosx')`	Ja
`osArch`	Betriebssystem-Architektur. Mögliche Werte: • `'x64'` • `'x86'`	`cpuArch = 'x86'`	Ja
`osProductType`	Betriebssystem-Produkttyp. Mögliche Werte: • `'dc'` Steht für Domain Controller. **Hinweis** Wenn die Rolle des Domain-Controllers auf einem Windows-Server zugewiesen wird, ändert sich der `osProductType` (Betriebssystem-Produkttyp) von `server` zu `dc`. Solche Maschinen werden in Suchergebnissen mit dem Filter `osProductType='server'` nicht berücksichtigt. • `'server'`	`osProductType = 'server'`	Ja

Attribut	Bedeutung	Beispiele für Suchanfragen	Für Gruppenerstellung unterstützt
	• `'workstation'`		
`osSp`	Service Pack des Betriebssystems.	`osSp = 1`	Ja
`osVersionMajor`	Hauptversion des Betriebssystems.	`osVersionMajor = 1`	Ja
`osVersionMinor`	Nebenversion des Betriebssystems.	`osVersionMinor > 1`	Ja
Agent			
`agentVersion`	Version des installierten Protection Agenten.	`agentVersion LIKE '12.0.*'`	Ja
`hostId`	Interne ID des Protection Agenten. So können Sie die ID des Protection Agenten einsehen: Wählen Sie bei **Geräte** das gewünschte Gerät aus und klicken Sie dann auf **Details** –> **Alle Eigenschaften**. Überprüfen Sie den Wert `id` der Eigenschaft `agent`.	`hostId = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Ja
`virtualType`	Typ der virtuellen Maschine. Mögliche Werte: • `'vmwesx'` Virtuelle VMware-Maschinen. • `'mshyperv'` Virtuelle Hyper-V-Maschinen. • `'pcs'` Virtuelle Virtuozzo-Maschinen. • `'hci'` Virtuelle Virtuozzo Hybrid Infrastructure-	`virtualType = 'vmwesx'`	Ja

Attribut	Bedeutung	Beispiele für Suchanfragen	Für Gruppenerstellung unterstützt
	Maschinen. • `'scale'` Virtuelle Scale Computing HC3-Maschinen. • `'ovirt'` Virtuelle oVirt-Maschinen		
`insideVm`	Virtuelle Maschine, die einen Agenten enthält. Mögliche Werte: • `true` • `false`	`insideVm = true`	Ja
Speicherort			
`tenant`	Der Name des Mandanten, zu dem das Gerät gehört.	`tenant = 'Unit 1'`	Ja
`tenantId`	Die Kennung (ID) des Mandanten, zu dem das Gerät gehört. So können Sie die Mandanten-ID einsehen: Wählen Sie bei **Geräte** das gewünschte Gerät aus und klicken Sie dann auf **Details** –> **Alle Eigenschaften**. Die ID wird im Feld `ownerId` angezeigt.	`tenantId = '3bfe6ca9-9c6a-4953-9cb2-a1323f454fc9'`	Ja
`ou`	Geräte, die zu der spezifizierten Active Directory-Organisationseinheit gehören.	`ou IN ('RnD', 'Computers')`	Ja
Status			
`state`	Gerätestadium.	`state = 'backup'`	Nein

Attribut	Bedeutung	Beispiele für Suchanfragen	Für Gruppenerstellung unterstützt
	Mögliche Werte: • `'idle'` • `'interactionRequired'` • `'canceling'` • `'backup'` • `'recover'` • `'install'` • `'reboot'` • `'failback'` • `'testReplica'` • `'run_from_image'` • `'finalize'` • `'failover'` • `'replicate'` • `'createAsz'` • `'deleteAsz'` • `'resizeAsz'`		
Status	Schutzstatus. Mögliche Werte: • `ok` • `warning` • `error` • `critical` • `protected` • `notProtected`	`status = 'ok'` `status IN ('error', 'warning')`	Nein
`protectedByPlan`	Geräte, die durch einen Schutzplan mit einer bestimmten ID gesichert werden. Wenn Sie die Plan-ID einsehen wollen, wählen Sie zuerst unter **Verwaltung** –> **Schutzpläne** einen Plan aus. Klicken Sie anschließend auf den Balken in der Spalte **Status** und schließlich	`protectedByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Nein

Attribut	Bedeutung	Beispiele für Suchanfragen	Für Gruppenerstellung unterstützt
	auf den Statusnamen. Es wird eine neue Suche mit der Plan-ID erstellt.		
`okByPlan`	Geräte, die durch einen Schutzplan mit einer angegebenen ID gesichert werden und den Status **OK** haben.	`okByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Nein
`errorByPlan`	Geräte, die durch einen Schutzplan mit einer angegebenen ID gesichert werden und den Status **Fehler** haben.	`errorByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Nein
`warningByPlan`	Geräte, die durch einen Schutzplan mit einer angegebenen ID gesichert werden und den Status **Warnung** haben.	`warningByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Nein
`runningByPlan`	Geräte, die durch einen Schutzplan mit einer angegebenen ID gesichert werden und den Status **Wird ausgeführt** haben.	`runningByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Nein
`interactionByPlan`	Geräte, die durch einen Schutzplan mit einer angegebenen ID gesichert werden und den Status **Benutzereingriff erforderlich** haben.	`interactionByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Nein

`lastBackupTime`*	Datum und Zeitpunkt des letzten erfolgreichen Backups.
	Das Format ist `'YYYY-MM-DD HH:MM'`.
		`lastBackupTime > '2023-03-11'`
		`lastBackupTime <= '2023-03-11 00:15'`
		`lastBackupTime is null`
			Nein

`lastBackupTryTim`	Zeitpunkt des letzten	`lastBackupTryTime >= '2023-03-`	Nein

Attribut	Bedeutung	Beispiele für Suchanfragen	Für Gruppenerstellung unterstützt
e*	Backup-Versuchs. Das Format ist 'YYYY-MM-DD HH:MM'.	11'	
nextBackupTime*	Zeitpunkt des nächsten Backups. Das Format ist 'YYYY-MM-DD HH:MM'.	nextBackupTime >= '2023-08-11'	Nein
lastVAScanTime*	Datum und Zeitpunkt des letzten erfolgreichen Schwachstellenbewertung. Das Format ist 'YYYY-MM-DD HH:MM'.	lastVAScanTime > '2023-03-11' lastVAScanTime <= '2023-03-11 00:15' lastVAScanTime is null	Ja
lastVAScanTryTime*	Der Zeitpunkt des letzten Versuchs zur Schwachstellenbewertung. Das Format ist 'YYYY-MM-DD HH:MM'.	lastVAScanTimeTryTime >= '2022-03-11'	Ja
nextVAScanTime*	Der Zeitpunkt der nächsten Schwachstellenbewertung. Das Format ist 'YYYY-MM-DD HH:MM'.	nextVAScanTime <= '2023-08-11'	Ja
network_status	Der Status der Netzwerk-Isolation für die Endpoint Detection & Response (EDR)-Funktionalität. Mögliche Werte: • connected • isolated	network_status= 'connected'	Ja

Hinweis
Wenn Sie den Wert für Stunde und Minuten überspringen, wird 'YYYY-MM-DD 00:00:00' als Startzeitpunkt und 'YYYY-MM-DD 23:59:59' als Endzeitpunkt angenommen. Beispiel: `lastBackupTime = 2023-01-20` bedeutet, dass die Suchergebnisse alle Backups aus dem Zeitraum `lastBackupTime >= 2023-01-20 00:00` und `lastBackup time <= 2023-01-20 23:59:59` enthalten werden.

Suchoperatoren

In der nachfolgenden Tabelle sind die Operatoren zusammengefasst, die Sie in Ihren Suchanfragen verwenden können.

Sie können mehr als einen Operator in einer Abfrage verwenden.

Operator	Unterstützt für	Bedeutung	Beispiele
`AND`	Alle Workloads	Operator für logische Konjunktion	`name like 'en-00' AND tenant = 'Unit 1'`
`OR`	Alle Workloads	Operator für logische Disjunktion	`state = 'backup' OR state = 'interactionRequired'`
`NOT`	Alle Workloads	Operator für logische Negation	`NOT(osProductType = 'workstation')`
`IN (<value1>,... <valueN>)`	Alle Workloads	Dieser Operator überprüft, ob ein Ausdruck mit irgendeinem Wert in einer Liste von Werten übereinstimmt.	`osType IN ('windows', 'linux')`
`NOT IN`	Alle Workloads	Dieser Operator ist das Gegenteil des Operators `IN`.	`NOT osType IN ('windows', 'linux')`

`LIKE 'wildcard pattern'`	Alle Workloads	Dieser Operator überprüft, ob ein Ausdruck mit dem Platzhalter-Muster übereinstimmt.
		Sie können die folgenden Platzhalter-Operatoren verwenden:
		• * oder %. Der
			`name LIKE 'en-00'`
			`name LIKE '*en-00'`
			`name LIKE '*en-00*'`
			`name LIKE 'en-00_'`

Operator	Unterstützt für	Bedeutung	Beispiele
		Asterisk und das Prozentzeichen stehen für kein, ein oder oder mehrere Zeichen. • _. Das Unterstrichzeichen repräsentiert ein einzelnes Zeichen	

`NOT LIKE 'wildcard pattern'`	Alle Workloads	Dieser Operator ist das Gegenteil des Operators `LIKE`.
		Sie können die folgenden Platzhalter-Operatoren verwenden:
		• * oder %. Der Asterisk und das Prozentzeichen stehen für kein, ein oder oder mehrere Zeichen.
		• _. Das Unterstrichzeichen repräsentiert ein einzelnes Zeichen
			`NOT name LIKE 'en-00'`
			`NOT name LIKE '*en-00'`
			`NOT name LIKE '*en-00*'`
			`NOT name LIKE 'en-00_'`

`RANGE (<starting_value>, <ending_value>)`	Alle Workloads	Dieser Operator überprüft, ob sich ein Ausdruck innerhalb eines Wertebereichs befindet.
		Suchanfragen mit alphanumerischen Zeichenfolgen verwenden die ASCII-Sortierreihenfolge, wobei Groß- und Kleinschreibung jedoch nicht beachtet werden.
			`ip RANGE('10.250.176.1','10.250.176.50')`
			`name RANGE('a','d')`
			Mit dieser Abfrage können Sie alle Namen herausfiltern, die mit A, B und C beginnen, wie beispielsweise `Alice`, `Bob` und `Claire`. Allerdings erfüllt nur der einzelne Buchstabe D die Anforderungen. Daher werden Namen mit mehr Buchstaben (wie `Diana` oder `Don`) nicht berücksichtigt.
			Dasselbe Ergebnis können Sie auch mit folgender Abfrage erzielen:
			`name >= 'a' AND name <= 'd'`

= oder ==	Alle Workloads	*Ist gleich*-Operator	`osProductType = 'server'`

Operator	Unterstützt für	Bedeutung	Beispiele
!= oder <>	Alle Workloads	*Ist nicht gleich*-Operator	`id != '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`
<	Nicht-Cloud-zu-Cloud-Workloads	*Kleiner als*-Operator	`memorySize < 1024`
>	Nicht-Cloud-zu-Cloud-Workloads	*Größer als*-Operator	`diskSize > 300GB`
<=	Nicht-Cloud-zu-Cloud-Workloads	*Kleiner als- oder Ist gleich*-Operator	`lastBackupTime <= '2022-03-11 00:15'`
>=	Nicht-Cloud-zu-Cloud-Workloads	*Größer als- oder Ist gleich*-Operator	`nextBackupTime >= '2022-08-11'`

Eine dynamische Gruppe bearbeiten

Sie können eine dynamische Gruppe bearbeiten, indem Sie die Suchabfrage ändern, die den Gruppeninhalt definiert.

Bei dynamischen Gruppen, die auf dem Active Directory basieren, können Sie auch die Active Directory-Gruppe ändern.

So können Sie eine dynamische Gruppe bearbeiten

Indem Sie die Suchanfrage ändern

1. Klicken Sie auf **Geräte**, gehen Sie zu der dynamischen Gruppe, die Sie bearbeiten wollen, und wählen Sie diese aus.
2. Klicken Sie neben dem Namen der Gruppe auf das Zahnradsymbol und anschließend auf den Befehl **Bearbeiten**. Alternativ können Sie auch im Fensterbereich **Aktionen** auf **Bearbeiten** klicken.
3. Ändern Sie die Suchanfrage, indem Sie die Suchattribute, deren Werte oder die Suchoperatoren ändern, und klicken Sie anschließend auf **Suchen**.
4. Klicken Sie neben dem Suchfeld auf **Speichern**.

Indem Sie die Active Directory-Gruppe ändern

Hinweis
Diese Prozedur gilt für dynamische Gruppen, die auf dem Active Directory basieren. Gruppen, die auf dem Active Directory basieren, sind nur unter **Microsoft 365** –> **Benutzer** verfügbar.

1. Klicken Sie auf **Geräte**, gehen Sie zu **Geräte** –> **Microsoft 365** –> Ihre Organisation –> **Benutzer**.
2. Wählen Sie die dynamische Gruppe aus, die Sie bearbeiten wollen.
3. Klicken Sie neben dem Namen der Gruppe auf das Zahnradsymbol und anschließend auf den Befehl **Bearbeiten**. Alternativ können Sie auch im Fensterbereich **Aktionen** auf **Bearbeiten** klicken.
4. Ändern Sie den Gruppeninhalt, indem Sie einen der folgenden Schritte ausführen:
   - Ändern Sie die bereits ausgewählte Active Directory-Gruppe, indem Sie auf deren Namen klicken und dann eine neue Active Directory-Gruppe aus der sich öffnenden Liste auswählen.
   - Bearbeiten Sie die Suchanfrage und klicken Sie anschließend auf **Suchen**.
     Die Suchabfrage ist auf die aktuell ausgewählte Active Directory-Gruppe beschränkt.
5. Klicken Sie neben dem Suchfeld auf **Speichern**.

Sie können Ihre Bearbeitungen außerdem speichern, ohne die aktuelle Gruppe zu überschreiben. Wenn Sie die bearbeitete Konfiguration als neue Gruppe speichern wollen, dann klicken Sie zuerst neben dem Suchfeld auf die Pfeilschaltfläche und anschließend auf **Speichern unter**.

Eine Gruppe löschen

Wenn Sie eine Gerätegruppe löschen, werden alle Pläne, die auf diese Gruppe angewendet wurden, widerrufen. Die Workloads in der Gruppe verlieren ihren Schutz, wenn keine anderen (neuen) Pläne auf sie angewendet werden.

So können Sie eine Gerätegruppe löschen

1. Klicken Sie auf **Geräte** und gehen Sie dann zu der Gruppe, die Sie löschen wollen.
2. Klicken Sie neben dem Namen der Gruppe auf das Zahnradsymbol und anschließend auf den Befehl **Löschen**.
3. Bestätigen Sie Ihre Auswahl, indem Sie auf **Löschen** klicken.

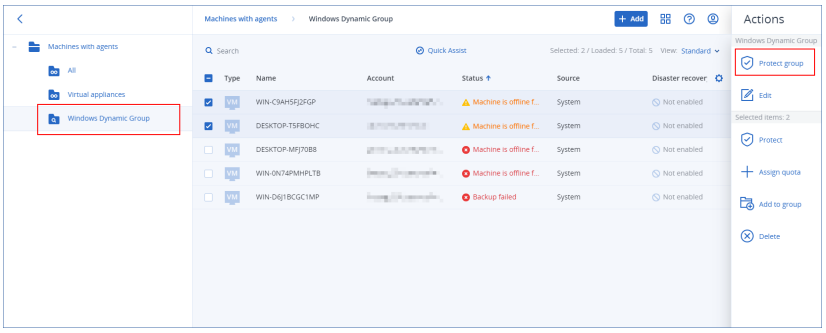
Einen Plan auf eine Gruppe anwenden

Sie können einen Plan auf eine Gruppe anwenden, indem Sie zuerst die Gruppe auswählen und dieser dann einen Plan zuweisen.

Alternativ können Sie einen Plan auch zur Bearbeitung öffnen und diesem dann eine Gruppe hinzufügen.

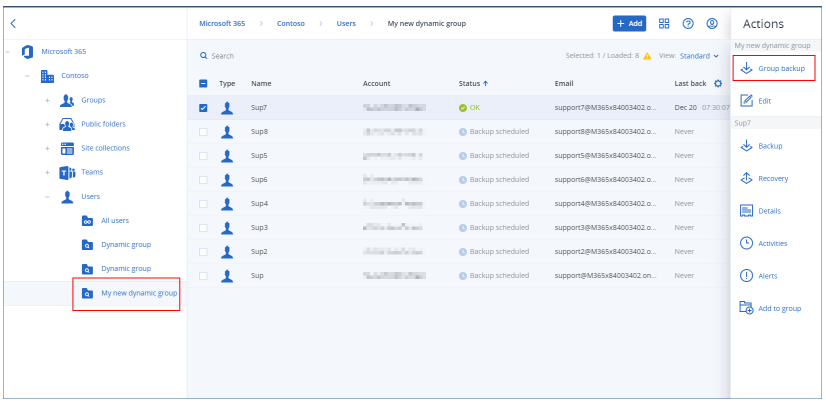
So können Sie einen Plan auf eine Gruppe anwenden

1. Klicken Sie auf **Geräte** und gehen Sie dann zu der Gruppe, auf die Sie einen Plan anwenden wollen.
2. [Für Nicht-Cloud-zu-Cloud-Workloads] Klicken Sie auf **Gruppe schützen**.



Es wird eine Liste der Pläne angezeigt, die angewendet werden können.

3. [Für Cloud-zu-Cloud-Workloads] Klicken Sie auf **Gruppen-Backup**.



Es wird eine Liste der Backup-Pläne angezeigt, die angewendet werden können.

4. [Um einen vorhandenen Plan anzuwenden] Wählen Sie den Plan aus und klicken Sie anschließend auf **Anwenden**.
5. [Um einen neuen Plan zu erstellen] Klicken Sie auf **Plan erstellen**, wählen Sie den Plantyp aus und erstellen Sie dann den neuen Plan.

   Weitere Informationen über die verfügbaren Plantypen und wie Sie diese erstellen können, finden Sie im Abschnitt '"Unterstützte Pläne für Gerätegruppen" (S. 373)'.

Hinweis

Backup-Pläne, die auf Cloud-zu-Cloud-Gerätegruppen angewendet werden, werden automatisch so geplant, dass sie einmal pro Tag ausgeführt werden. Sie können diese Pläne nicht bei Bedarf manuell ausführen, indem Sie auf **Jetzt ausführen** klicken.

Einen Plan von einer Gruppe widerrufen

Sie können einen Plan von einer Gruppe widerrufen, indem Sie zuerst die Gruppe auswählen und dann den Plan von dieser Gruppe widerrufen.

Alternativ können Sie den Plan auch zur Bearbeitung öffnen und dann die Gruppe aus dem Plan entfernen.

So können Sie einen Plan von einer Gruppe widerrufen

1. Klicken Sie auf **Geräte** und gehen Sie dann zu der Gruppe, von der Sie einen Plan widerrufen wollen.

2. [Für Nicht-Cloud-zu-Cloud-Workloads] Klicken Sie auf **Gruppe schützen**.
   Es wird eine Liste der Pläne angezeigt, die auf die Gruppe angewendet werden.
3. [Für Cloud-zu-Cloud-Workloads] Klicken Sie auf **Gruppen-Backup**.
   Es wird eine Liste der Backup-Pläne angezeigt, die auf die Gruppe angewendet werden.
4. Wählen Sie den Plan aus, den Sie widerrufen wollen.
5. [Für Nicht-Cloud-zu-Cloud-Workloads] Klicken Sie auf das Drei-Punkte-Symbol (...) und anschließend auf **Widerrufen**.
6. [Für Cloud-zu-Cloud-Workloads] Klicken Sie auf das Zahnradsymbol und anschließend auf **Widerrufen**.

Mit dem Gerätekontrolle-Modul arbeiten

Als Bestandteil der Cyber Protection Service-Schutzpläne verwendet das Modul Gerätekontrolle[1] eine funktionale Teilmenge des Agenten für Data Loss Prevention[2] auf jedem entsprechend geschützten Computer, um unautorisierte Zugriffe auf und Übertragungen von Daten über lokale Computer-Datenkanäle zu erkennen und zu unterbinden. Das Gerätekontrolle-Modul ermöglicht eine feinstufige Kontrolle über eine Vielzahl von Data Leackage-Pfaden – wozu beispielsweise Datenübertragungen über Wechselmedien, Drucker, virtuelle und umgeleitete Geräte oder die Windows-Zwischenablage gehören.

Das Modul ist für die Cyber Protect Essentials-, Cyber Protect Standard- und Cyber Protect Advanced-Editionen verfügbar, die 'pro Workload' lizenziert werden.

Hinweis
Auf Windows Maschinen muss der Agent für Data Loss Prevention installiert sein, um die Funktionen der Gerätekontrolle nutzen zu können. Dieser wird bei geschützten Workloads automatisch installiert, wenn das Modul für die **Gerätekontrolle** in den Schutzplänen der Maschinen aktiviert wird.

[1]Als Bestandteil eines Schutzplans verwendet das Modul 'Gerätekontrolle' eine funktionale Teilmenge des Data Loss Prevention Agenten auf jedem entsprechend geschützten Computer, um unautorisierte Zugriffe auf und Übertragungen von Daten über lokale Computer-Datenkanäle zu erkennen und zu unterbinden. Dazu gehören Benutzerzugriffe auf Peripheriegeräte und Ports, das Ausdrucken von Dokumenten, Zwischenablage-Aktionen (Kopieren, Einfügen), bestimmte Aktionen mit Medien (Formatieren, Auswerfen) und die Synchronisierung von Daten mit lokal angeschlossenen Mobilgeräten. Das Modul 'Gerätekontrolle' bietet granulare, kontextbezogene Kontrollmöglichkeiten über die Art der Geräte und Ports, auf die Benutzer auf dem geschützten Computer zugreifen dürfen, sowie über die Aktionen, die Benutzer auf diesen Geräten ausführen können.
[2]Die Client-Komponente eines Data Loss Prevention-Systems, die den jeweiligen Host-Computer vor der unbefugten Nutzung, Übertragung und Speicherung von vertraulichen, geschützten oder sensiblen Daten schützt, indem sie eine Kombination aus kontext- und inhaltsbezogenen Analysetechniken anwendet und zentral verwaltete Data Loss Prevention-Richtlinien durchsetzt. Zur Cyber Protection-Funktionalität gehört ein vollwertiger Data Loss Prevention Agent. Die tatsächliche Funktionalität des Agenten auf einem geschützten Computer ist jedoch auf denjenigen Satz von Data Loss Prevention-Funktionen beschränkt, der in der jeweiligen Cyber Protection-Lösung je nach Lizenzierung verfügbar ist – und sie hängt zudem von dem Schutzplan ab, der auf den betreffenden Computer angewendet wird.

Das Gerätekontrolle-Modul greift auf die Data Loss Prevention[1]-Funktionen des Agenten zurück, um eine kontextbezogene Kontrolle über Datenzugriffe und Datenübertragungen auf dem jeweils geschützten Computer durchzusetzen. Dazu gehören Benutzerzugriffe auf Peripheriegeräte und Ports, das Ausdrucken von Dokumenten, Zwischenablage-Aktionen (Kopieren, Einfügen), bestimmte Aktionen mit Medien (Formatieren, Auswerfen) und die Synchronisierung von Daten mit lokal angeschlossenen Mobilgeräten. Der Agent für Data Loss Prevention stellt ein Framework für alle zentralen Verwaltungs- und Administrationskomponenten des Gerätekontrolle-Moduls bereit. Er muss daher auf jedem Computer installiert sein, der mit dem Gerätekontrolle-Modul geschützt werden soll. Dieser Agent kann Benutzeraktionen erlauben, einschränken oder unterbinden. Dies erfolgt auf Basis der Gerätekontrolle-Einstellungen, die er von demjenigen Schutzplan übermittelt bekommt, der auf den geschützten Computer angewendet wurde.

Das Gerätekontrolle-Modul kann Zugriff auf unterschiedlichste Peripheriegeräte steuern – egal, ob diese direkt auf geschützten Computern verwendet oder in Virtualisierungsumgebungen umgeleitet werden, wo geschützte Computer gehostet werden. Die Gerätekontrolle erkennt Geräte, die im Microsoft Remote Desktop Server, in Citrix XenDesktop / XenApp / XenServer oder in VMware Horizon umgeleitet werden. Sie kann außerdem Datenkopieraktionen zwischen der Windows-Zwischenablage eines Gast-Betriebssystems (welches unter VMware Workstation, VMware Player, Oracle VM, VirtualBox oder Windows Virtual PC läuft) und der Zwischenablage des entsprechenden Host-Betriebssystems (welches auf einem geschützten Computer läuft) kontrollieren.

Das Gerätekontrolle-Modul kann Computer mit folgenden Betriebssystemen schützen:

Gerätekontrolle

- Microsoft Windows 7 Service Pack 1 und höher
- Microsoft Windows Server 2008 R2 und höher
- macOS 10.15 (Catalina)
- macOS 11.2.3 (Big Sur)
- macOS 12 (Monterey)
- macOS 13 (Ventura)

Hinweis
Der Agent für Data Loss Prevention für macOS unterstützt nur x64-Prozessoren. ARM-basierte Apple Silicon-Prozessoren werden nicht unterstützt.

Data Loss Prevention

- Microsoft Windows 7 Service Pack 1 und höher
- Microsoft Windows Server 2008 R2 und höher

[1]Ein System integrierter Technologien und organisatorischer Maßnahmen, das darauf abzielt, versehentliche oder absichtliche Offenlegungen/Zugriffe auf vertrauliche, geschützte oder sensible Daten durch unberechtigte Entitäten außerhalb oder innerhalb des Unternehmens oder die Übertragung solcher Daten zu nicht vertrauenswürdigen Umgebungen zu erkennen und zu unterbinden.

Hinweis
Der Agent für Data Loss Prevention kann auf nicht-unterstützten macOS-Systemen installiert werden, da er ein integraler Bestandteil von Agent für Mac ist. In diesem Fall wird die Cyber Protect-Konsole anzeigen, dass der Agent für Data Loss Prevention auf dem Computer installiert ist, aber die Gerätekontrolle-Funktionalität wird nicht funktionieren. Die Gerätekontrolle-Funktionalität funktioniert nur auf macOS-Systemen, die vom Agenten für Data Loss Prevention unterstützt werden.

Einschränkungen bei der Verwendung des Agenten für Data Loss Prevention mit Hyper-V

Sie sollten den Agenten für Data Loss Prevention nicht auf Hyper-V-Hosts in Hyper-V-Clustern installieren, da dies Abstürze (Bluescreens) verursachen kann – hauptsächlich in Hyper-V-Clustern mit freigegebenen Cluster-Volumes (CSVs).

Wenn Sie eine der nachfolgenden Versionen des Agenten für Hyper-V verwenden, müssen Sie den Agenten für Data Loss Prevention manuell entfernen:

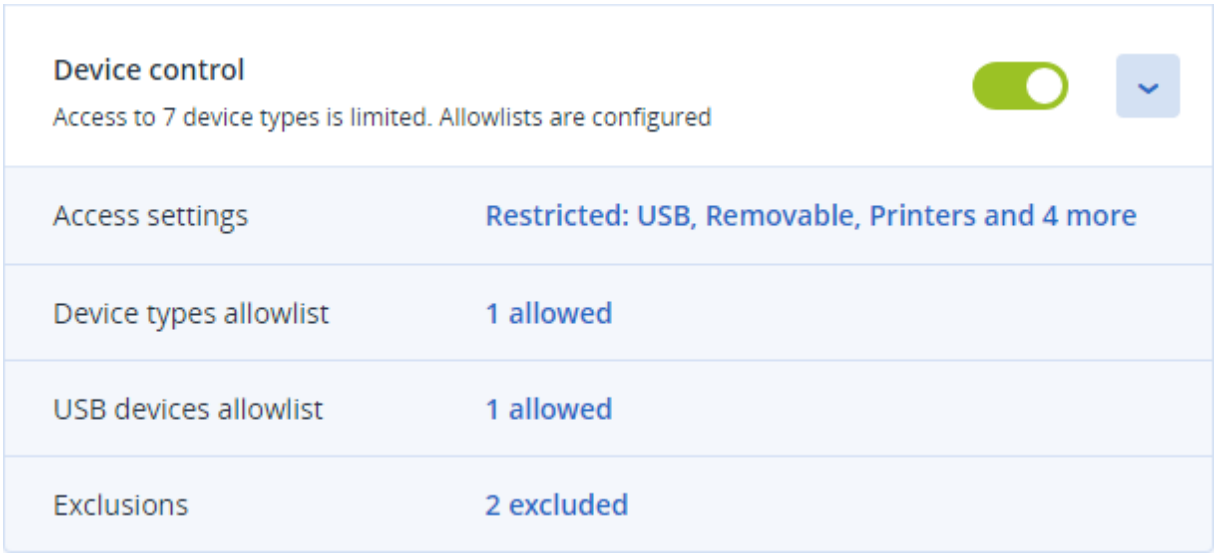
- 15.0.26473 (C21.02)
- 15.0.26570 (C21.02 HF1)
- 15.0.26653 (C21.03)
- 15.0.26692 (C21.03 HF1)
- 15.0.26822 (C21.04)

Wenn Sie den Agenten für Data Loss Prevention entfernen wollen, können Sie auf dem Hyper-V Host den Installer manuell ausführen und das Kontrollkästchen des Agenten für Data Loss Prevention deaktivieren – oder folgenden Befehl ausführen:

```
<installer_name> --remove-components=agentForDlp -quiet
```

Sie können das Gerätekontrolle-Modul in der Cyber Protect-Konsole im Bereich **Gerätekontrolle** des jeweiligen Schutzplans aktivieren und konfigurieren. Zu weiteren Anweisungen siehe die Schritte zum Aktivieren oder Deaktivieren der Gerätekontrolle.

Im Bereich **Gerätekontrolle** wird eine Zusammenfassung über die Konfiguration des Moduls angezeigt:



- Zugriffseinstellungen – Zeigt (sofern zutreffend) eine Zusammenfassung der Gerätetypen und Ports mit eingeschränktem Zugriff (schreibgeschützt oder komplett verweigert) an. Anderenfalls wird angezeigt, dass die Zugriffe auf alle Gerätetypen erlaubt sind. Klicken Sie auf diese Zusammenfassung, wenn Sie die Zugriffseinstellungen einsehen oder ändern wollen (siehe auch die Schritte zum Anzeigen oder Ändern der Zugriffseinstellungen).
- Positivliste für Gerätetypen – Zeigt an (sofern zutreffend), wie viele Geräteunterklassen durch Ausschluss von der Gerätezugriffskontrolle erlaubt wurden. Anderenfalls wird angezeigt, dass die Positivliste leer ist. Klicken Sie auf die Zusammenfassung, wenn Sie die Auswahl der erlaubten Geräteunterklassen einsehen oder ändern wollen (siehe auch die Schritte, um Geräteunterklassen von der Zugriffskontrolle auszuschließen).
- Positivliste für USB-Geräte – Zeigt an (sofern zutreffend), wie viele USB-Geräte/-Modelle durch Ausschluss von der Gerätezugriffskontrolle erlaubt wurden. Anderenfalls wird angezeigt, dass die Positivliste leer ist. Klicken Sie auf die Zusammenfassung, wenn Sie die Liste der erlaubten USB-Geräte/-Modelle einsehen oder ändern wollen (siehe auch die Schritte, um einzelne USB-Geräte von der Zugriffskontrolle auszuschließen).
- Ausschlüsse – Zeigt an, wie viele Ausschlüsse von der Zugriffskontrolle für die Windows-Zwischenablage, Screenshot-Aufnahmen, Drucker und Mobilgeräte festgelegt wurden.

Die Gerätekontrolle verwenden

Dieser Abschnitt enthält Schritt-für-Schritt-Anweisungen, wie Sie grundlegende Aufgaben zur Verwendung des Gerätekontrolle-Moduls durchgeführt können.

Die Gerätekontrolle aktivieren oder deaktivieren

Sie können die Gerätekontrolle aktivieren, wenn Sie einen Schutzplan erstellen. Sie können auch einen bereits vorhandenen Schutzplan ändern, um die Gerätekontrolle zu aktivieren oder zu

deaktivieren.

So können Sie die Gerätekontrolle aktivieren oder deaktivieren

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte** –> **Alle Geräte**.
2. Gehen Sie folgendermaßen vor, um das Schutzplan-Panel zu öffnen:
   - Wählen einen neuen Schutzplan erstellen wollen: wählen Sie die zu schützende Maschine aus, klicken Sie dann auf **Schützen** und anschließend auf **Plan erstellen**.
   - Wenn Sie einen vorhandenen Schutzplan ändern wollen: wählen Sie eine geschützte Maschine aus und klicken Sie dann auf **Schützen**. Klicken Sie anschließend neben dem Namen des Schutzplans auf das Drei-Punkte-Symbol (...) und wählen Sie abschließend den Befehl **Bearbeiten**.
3. Gehen Sie im Schutzplan-Panel zum Bereich **Gerätekontrolle** und aktivieren oder deaktivieren Sie die Option **Gerätekontrolle**.
4. Gehen Sie folgendermaßen vor, um Ihre Änderungen zu übernehmen:
   - Wenn Sie einen Schutzplan erstellen, dann klicken Sie auf **Erstellen**.
   - Wenn Sie einen Schutzplan bearbeiten, dann klicken Sie auf **Speichern**.

Sie können auch über die Registerkarte Verwaltung auf das Schutzplan-Panel zugreifen. Diese Möglichkeit ist jedoch nicht in allen Editionen des Cyber Protection Service verfügbar.

Die Verwendung des Gerätekontrolle-Moduls unter macOS aktivieren

Die Gerätekontrolle-Einstellungen eines Schutzplans werden erst wirksam, nachdem der entsprechende Treiber für die Gerätekontrolle auf den geschützten Workload geladen wurde. Dieser Abschnitt beschreibt, wie Sie den Treiber für die Gerätekontrolle laden können, um die Verwendung des Gerätekontrolle-Moduls unter macOS zu aktivieren. Dies ist eine einmalige Aktion, für die jedoch Administrator-Berechtigungen auf der Endpunkt-Maschine erforderlich sind.

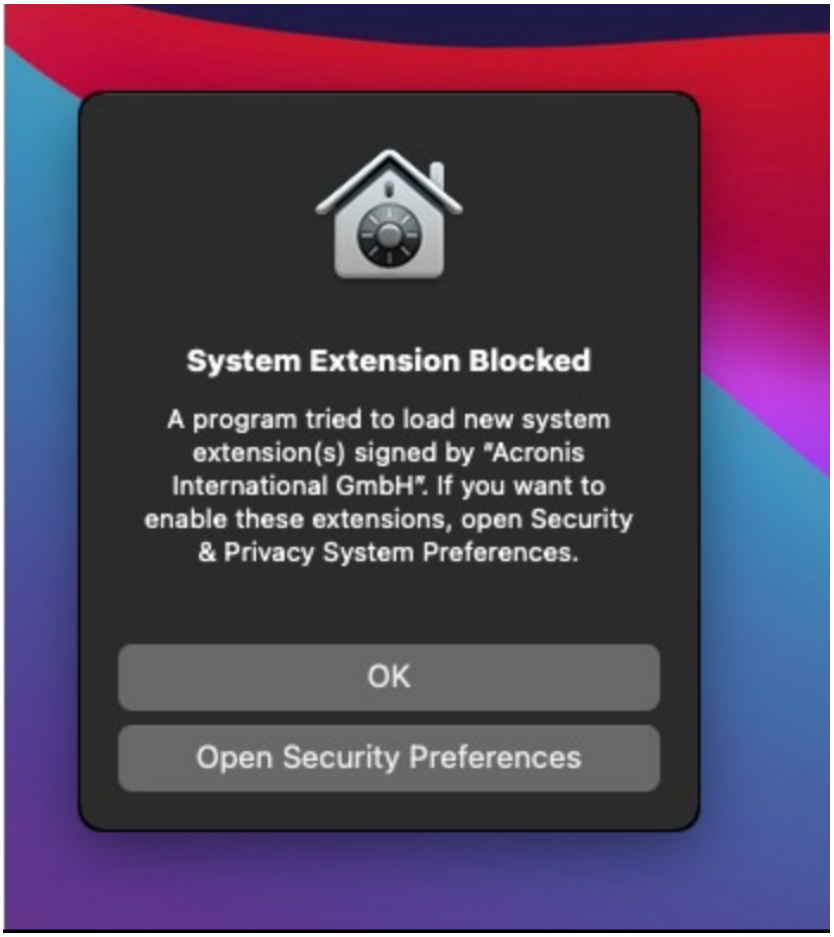
Unterstützte macOS-Versionen:

- macOS 10.15 (Catalina) und höher
- macOS 11.2.3 (Big Sur) und höher
- macOS 12.2 (Monterey) und höher
- macOS 13.2 (Ventura) und höher

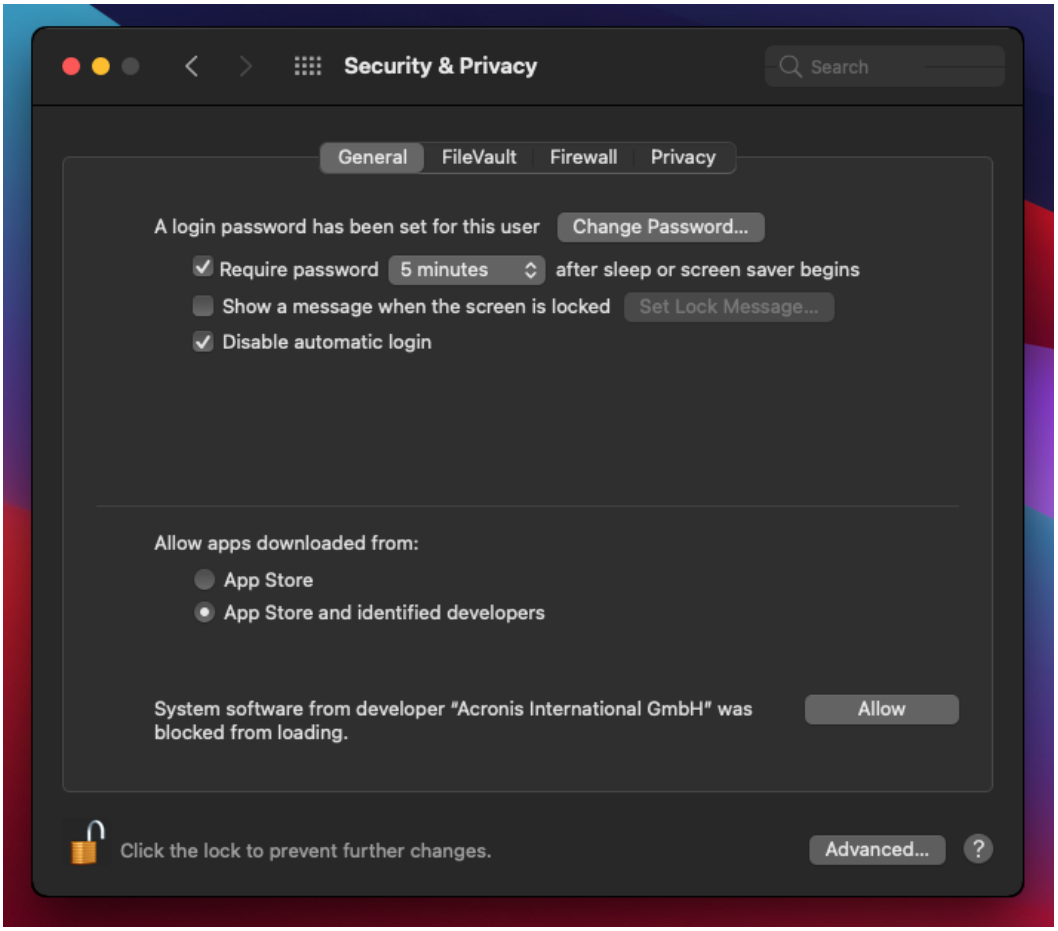
So können Sie die Verwendung des Gerätekontrolle-Moduls unter macOS aktivieren

1. Installieren Sie den Agenten für Mac auf der Maschine, die Sie schützen wollen.
2. Aktivieren Sie die Gerätekontrolle-Einstellungen im Schutzplan.
3. Wenden Sie den Schutzplan an.

4. Die Warnmeldung „Systemerweiterung blockiert“ wird auf dem geschützten Workload angezeigt. Klicken Sie auf **Sicherheitseinstellungen öffnen**.



5. Wählen Sie im angezeigten Fenster **Sicherheit & Datenschutz** (in der Registerkarte 'Allgemein') die Option **App Store und verifizierte Entwickler** und klicken Sie dann auf **Erlauben**.



6. Klicken Sie im dann angezeigten Dialog auf **Neustart**, damit der Workload neu gestartet und die Gerätekontrolle-Einstellungen aktiviert werden.

Hinweis
Sie müssen diese Schritte nicht wiederholen, falls die Gerätekontrolle-Einstellungen einmal deaktiviert und dann wieder aktiviert werden sollten.

Die Zugriffseinstellungen anzeigen oder ändern

Sie können die Zugriffseinstellungen für das Gerätekontrolle-Modul im Schutzplan-Fensterbereich verwalten. Dabei können Sie den Zugriff auf bestimmte Gerätetypen erlauben oder verweigern sowie Benachrichtigungen und Alarmmeldungen aktivieren oder deaktivieren.

So können Sie die Zugriffseinstellungen anzeigen oder ändern

1. Öffnen Sie das Schutzplan-Panel eines Schutzplans und aktivieren Sie die Gerätekontrolle in diesem Plan (siehe die Schritte zum Aktivieren oder Deaktivieren der Gerätekontrolle).
2. Klicken Sie zuerst neben dem **Gerätekontrolle**-Schalter auf das Pfeilsymbol, damit die Einstellungen erweitert werden, und dann auf den Link neben dem Eintrag **Zugriffseinstellungen**.

3. Auf der dann angezeigten Seite zur Verwaltung der Zugriffseinstellungen können Sie die Zugriffseinstellungen anzeigen oder ändern.

Hinweis
Die in der Gerätekontrolle konfigurierten Zugriffseinstellungen werden möglicherweise überschrieben, wenn Sie zum Schutz eines Workloads sowohl die Gerätekontroll- als auch Advanced DLP-Funktionalität verwenden. Siehe Abschnitt '"Die Advanced Data Loss Prevention-Funktionalität in Schutzplänen aktivieren" (S. 962)'.

Betriebssystem-Benachrichtigung und Service-Alarmmeldungen aktivieren oder deaktivieren

Bei der Verwaltung der Zugriffseinstellungen können Sie die Betriebssystem-Benachrichtigung und Service-Alarmmeldungen aktivieren oder deaktivieren, die über Versuche von Anwendern informieren, unerlaubte Aktionen durchzuführen.

So können Sie die Betriebssystem-Benachrichtigung aktivieren oder deaktivieren

1. Befolgen Sie die Schritte zum Anzeigen oder Ändern der Zugriffseinstellungen.
2. Aktivieren bzw. deaktivieren Sie (je nach Bedarf) auf der Seite zur Verwaltung der Zugriffseinstellungen das Kontrollkästchen **Betriebssystem-Benachrichtigung für Endbenutzer anzeigen, wenn diese versuchen, einen blockierten Gerätetyp oder Anschluss zu verwenden**.

So können Sie die Service-Alarmmeldungen aktivieren oder deaktivieren

1. Befolgen Sie die Schritte zum Anzeigen oder Ändern der Zugriffseinstellungen.
2. Aktivieren bzw. deaktivieren Sie (je nach Bedarf) auf der Seite zur Verwaltung der Zugriffseinstellungen das Kontrollkästchen **Alarm anzeigen** für den/die gewünschten Gerätetyp (en).

Das Kontrollkästchen **Alarm anzeigen** ist nur für Gerätetypen mit eingeschränktem Zugriff (Schreibgeschützt oder verweigerter Zugriff) verfügbar – ausgenommen Screenshot-Aufnahmen.

Geräteunterklassen von der Zugriffskontrolle ausschließen

Sie können über das Schutzplan-Panel Geräteunterklassen auswählen, die von der Zugriffskontrolle ausgeschlossen werden sollen. Dadurch wird der Zugriff auf diese Geräte erlaubt – unabhängig von den sonstigen Zugriffseinstellungen in der Gerätekontrolle.

So können Sie Geräteunterklassen von der Zugriffskontrolle ausschließen

1. Öffnen Sie das Schutzplan-Panel eines Schutzplans und aktivieren Sie die Gerätekontrolle in diesem Plan (siehe die Schritte zum Aktivieren oder Deaktivieren der Gerätekontrolle).
2. Klicken Sie zuerst neben dem **Gerätekontrolle**-Schalter auf das Pfeilsymbol, damit die Einstellungen erweitert werden, und dann auf den Link neben der **Positivliste für Gerätetypen**.

3. Auf der angezeigten Seite zur Verwaltung der Positivliste können Sie dann die Auswahl der Geräteunterklassen einsehen oder ändern, die von der Zugriffskontrolle ausgeschlossen werden sollen.

Einzelne USB-Geräte von der Zugriffskontrolle ausschließen

Sie können über das Schutzplan-Panel einzelne USB-Geräte oder USB-Gerätemodelle spezifizieren, die von der Zugriffskontrolle ausgeschlossen werden sollen. Dadurch wird der Zugriff auf diese Geräte erlaubt – unabhängig von den sonstigen Zugriffseinstellungen in der Gerätekontrolle.

So können Sie ein USB-Gerät von der Zugriffskontrolle ausschließen

1. Öffnen Sie das Schutzplan-Panel eines Schutzplans und aktivieren Sie die Gerätekontrolle in diesem Plan (siehe die Schritte zum Aktivieren oder Deaktivieren der Gerätekontrolle).
2. Klicken Sie zuerst neben dem **Gerätekontrolle**-Schalter auf das Pfeilsymbol, damit die Einstellungen erweitert werden, und dann auf den Link neben dem Eintrag **Positivliste für USB-Geräte**.
3. Klicken Sie auf der dann angezeigten Seite zur Verwaltung der Positivliste auf den Befehl **Aus Datenbank hinzufügen**.
4. Wählen Sie auf der dann angezeigten Seite zur Auswahl von USB-Geräten das/die gewünschte(n) Gerät(e) aus, die in der USB-Geräte-Datenbank registriert sind.
5. Klicken Sie auf die Schaltfläche **Zur Positivliste hinzufügen**.

So können Sie den Ausschluss eines USB-Geräts von der Zugriffskontrolle aufheben

1. Öffnen Sie das Schutzplan-Panel eines Schutzplans und aktivieren Sie die Gerätekontrolle in diesem Plan (siehe die Schritte zum Aktivieren oder Deaktivieren der Gerätekontrolle).
2. Klicken Sie zuerst neben dem **Gerätekontrolle**-Schalter auf das Pfeilsymbol, damit die Einstellungen erweitert werden, und dann auf den Link neben dem Eintrag **Positivliste für USB-Geräte**.
3. Klicken Sie auf der dann angezeigten Seite zur Verwaltung der Positivliste auf das Löschen-Symbol am Ende des Listenelements, welches das gewünschte USB-Gerät repräsentiert.

USB-Geräte zur Datenbank hinzufügen oder aus dieser entfernen

Wenn Sie ein bestimmtes USB-Gerät von der Zugriffskontrolle ausschließen wollen, müssen Sie es zuerst zur USB-Geräte-Datenbank hinzufügen. Anschließend können Sie Geräte in die Positivliste aufnehmen, indem Sie diese aus der Datenbank auswählen.

Folgende Prozeduren gelten für Schutzpläne, für die die Funktion 'Gerätekontrolle' aktiviert wurde.

So können Sie USB-Geräte zur Datenbank hinzufügen

1. Öffnen Sie den Schutzplan eines Geräts, um diesen zu bearbeiten:
   Klicken Sie neben dem Namen des Schutzplans auf das Drei-Punkte-Symbol (...) und wählen Sie anschließend den Befehl **Bearbeiten**.

Hinweis
Die Gerätekontrolle muss im Plan aktiviert worden sein, damit Sie auf die Einstellungen der Gerätekontrolle zugreifen können.

2. Klicken Sie zuerst neben dem **Gerätekontrolle**-Schalter auf das Pfeilsymbol, damit die Einstellungen erweitert werden, und dann auf den Link neben dem Eintrag **Positivliste für USB-Geräte**.
3. Klicken Sie auf der dann angezeigten **Positivliste für USB-Geräte** auf den Befehl **Aus Datenbank hinzufügen**.
4. Klicken Sie auf der dann angezeigten Verwaltungsseite für die USB-Geräte-Datenbank auf den Befehl **Zur Datenbank hinzufügen**.
5. Klicken Sie im angezeigten Dialog **USB-Gerät hinzufügen** die Maschine aus, mit der das USB-Gerät verbunden ist.
   Es werden nur Maschinen in der Liste der Computer angezeigt, die online sind.
   Die Liste der USB-Geräte wird nur für solche Maschinen angezeigt, auf denen der Agent für Data Loss Prevention installiert ist.
   Die USB-Geräte werden in der Baumansicht aufgelistet. Die erste Ebene des Verzeichnisbaums repräsentiert ein Gerätemodell. Die zweite Ebene repräsentiert ein bestimmtes Gerät dieses Modells.
   Ein blaues Symbol neben der Beschreibung des Geräts signalisiert, dass das Gerät aktuell mit dem Computer verbunden ist. Das Symbol ist ausgegraut, wenn das Gerät nicht an den Computer angeschlossen ist.
6. Aktivieren Sie die Kontrollkästchen für diejenigen USB-Geräte, die Sie in die Datenbank aufnehmen wollen, und klicken Sie anschließend auf **Zur Datenbank hinzufügen**.
   Die ausgewählten USB-Geräte werden in die Datenbank aufgenommen.
7. Schließen oder speichern Sie den Schutzplan.

So können Sie USB-Geräte über das Fenster 'Details' des Computers zur Datenbank hinzufügen

Hinweis
Diese Prozedur gilt nur für Geräte, die online sind und auf denen der Agent für Data Loss Prevention installiert ist. Bei Computern, die offline sind oder auf denen kein Agent für Data Loss Prevention installiert ist, können Sie auch keine Liste der USB-Geräte einsehen.

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte** –> **Alle Geräte**.
2. Wählen Sie einen Computer aus, an den das gewünschte USB-Gerät schon einmal angeschlossen war, und klicken Sie dann im rechten Menü auf **Inventarisierung**.
   Das Fenster 'Details' des Computers wird geöffnet.
3. Klicken Sie im Fenster 'Details' des Computers auf die Registerkarte **USB-Geräte**.
   Es wird eine Liste mit allen USB-Geräten geöffnet, die auf dem ausgewählten Computer bekannt sind.

Die USB-Geräte werden in der Baumansicht aufgelistet. Die erste Ebene des Verzeichnisbaums repräsentiert ein Gerätemodell. Die zweite Ebene repräsentiert ein bestimmtes Gerät dieses Modells.

Ein blaues Symbol neben der Beschreibung des Geräts signalisiert, dass das Gerät aktuell mit dem Computer verbunden ist. Das Symbol ist ausgegraut, wenn das Gerät nicht an den Computer angeschlossen ist.

4. Aktivieren Sie die Kontrollkästchen für diejenigen USB-Geräte, die Sie in die Datenbank aufnehmen wollen, und klicken Sie anschließend auf **Zur Datenbank hinzufügen**.

So können Sie USB-Geräte von Service-Alarmmeldungen aus zur Datenbank hinzufügen

1. Gehen Sie in der Cyber Protect-Konsole zu **Monitoring** –> **Alarmmeldungen**.
2. Suchen Sie nach einer Gerätekontrolle-Alarmmeldung, die darüber informiert, dass der Zugriff auf das betreffende USB-Gerät verweigert wurde.
3. Klicken Sie in der einfachen Ansicht der Alarmmeldung auf den Befehl **Dieses USB-Gerät erlauben**.

   Dadurch wird das USB-Gerät von der Zugriffskontrolle ausgenommen und außerdem zur weiteren Verwendung noch in die Geräte-Datenbank aufgenommen.

So können Sie USB-Geräte durch Importieren einer Geräteliste in die Datenbank aufnehmen

Sie können eine JSON-Datei mit einer Liste von USB-Geräten in die Datenbank importieren. Siehe '"Eine Liste von USB-Geräten in die Datenbank importieren" (S. 420)'.

So können Sie USB-Geräte aus der Datenbank entfernen

1. Öffnen Sie den Schutzplan eines Geräts, um diesen zu bearbeiten:

   Klicken Sie neben dem Namen des Schutzplans auf das Drei-Punkte-Symbol (...) und wählen Sie anschließend den Befehl **Bearbeiten**.

   Hinweis
   Die Gerätekontrolle muss im Plan aktiviert worden sein, damit Sie auf die Einstellungen der Gerätekontrolle zugreifen können.

2. Klicken Sie zuerst neben dem **Gerätekontrolle**-Schalter auf das Pfeilsymbol, damit die Einstellungen erweitert werden, und dann auf die Zeile **Positivliste für USB-Geräte**.
3. Klicken Sie auf der dann angezeigten Seite zur Verwaltung der Positivliste auf den Befehl **Aus Datenbank hinzufügen**.
4. Klicken Sie auf der Seite zur Auswahl von USB-Geräten aus der Datenbank auf das Drei-Punkte-Symbol (...) am Ende des Listenelement, welches das Gerät repräsentiert. Klicken Sie anschließend auf den Befehl **Löschen** und bestätigen Sie die gewünschte Aktion.
   Die USB-Geräte werden aus der Datenbank entfernt.
5. Schließen oder speichern Sie den Schutzplan.

Gerätekontrolle-Alarmmeldungen anzeigen

Das Gerätekontrolle-Modul kann so konfiguriert werden, dass Alarmmeldungen darüber informieren, wenn die Versuche von Anwendern blockiert wurden, bestimmte Gerätetypen zu verwenden (siehe den Abschnitt 'Betriebssystem-Benachrichtigung und Service-Alarmmeldungen aktivieren oder deaktivieren'). Gehen Sie folgendermaßen vor, wenn Sie diese Alarmmeldungen einsehen wollen.

So können Sie die Gerätekontrolle-Alarmmeldungen einsehen

1. Gehen Sie in der Cyber Protect-Konsole zu **Monitoring** –> **Alarmmeldungen**.
2. Suchen Sie nach Alarmmeldungen mit folgendem Status: „Der Zugriff auf Peripheriegeräte ist blockiert“.

Weitere Informationen finden Sie im Abschnitt Gerätekontrolle-Alarmmeldungen.

Zugriffseinstellungen

Auf der Seite **Zugriffseinstellungen** können Sie den Zugriff auf bestimmte Gerätetypen erlauben/unterbinden sowie die Betriebssystem-Benachrichtigung und Gerätekontrolle-Alarmmeldungen aktivieren/deaktivieren.

Hinweis
Die in der Gerätekontrolle konfigurierten Zugriffseinstellungen werden möglicherweise überschrieben, wenn Sie zum Schutz eines Workloads sowohl die Gerätekontroll- als auch Advanced DLP-Funktionalität verwenden. Siehe Abschnitt '"Die Advanced Data Loss Prevention-Funktionalität in Schutzplänen aktivieren" (S. 962)'.

Mit den Zugriffseinstellungen können Sie Benutzerzugriffe auf folgende Gerätetypen und Anschlüsse (Ports) einschränken:

- **Entfernbar** (Zugriffskontrolle nach Gerätetyp) – Geräte mit einer beliebigen Schnittstelle zum Anschließen an einen Computer (USB, FireWire, PCMCIA, IDE, SATA, SCSI usw.), die vom Betriebssystem als Wechsellaufwerke erkannt werden (z.B. USB-Sticks, Kartenleser, magneto-optische Laufwerke usw.). Die Gerätekontrolle stuft alle Festplatten, die über USB, FireWire und PCMCIA angeschlossen werden, als entfernbare Geräte (Wechsellaufwerke) ein. Einige Festplatten (in der Regel mit SATA- und SCSI-Schnittstelle) werden ebenfalls als entfernbare Wechsellaufwerke eingestuft, wenn sie die Hot-Plug-Funktion unterstützen und das gerade laufende Betriebssystem nicht auf ihnen installiert ist.

  Sie können Vollzugriffe oder Nur-Lesen-Zugriffe zulassen oder Zugriffe auf Wechsellaufwerke ganz unterbinden, um auf geschützten Computern zu kontrollieren, ob Daten auf Wechsellaufwerke übertragen oder von diesen kopiert werden dürfen. Die Zugriffsrechte wirken sich nicht auf Geräte aus, die mit BitLocker oder FileVault (nur HFS+-Dateisystem) verschlüsselt werden.

  Dieser Gerätetyp wird sowohl unter Windows als auch unter macOS unterstützt.

- **Verschlüsseltes Wechsellaufwerk** (Zugriffskontrolle nach Gerätetyp) – Wechsellaufwerke, die mit der Laufwerksverschlüsselung BitLocker (unter Windows) oder FileVault (unter macOS) verschlüsselt werden.

  Unter macOS werden nur solche verschlüsselten Wechsellaufwerke unterstützt, die das Dateisystem HFS+ (auch als HFS Plus, Mac OS Extended oder HFS Extended bekannt) verwenden. Verschlüsselte Wechsellaufwerke, die das APFS-Dateisystem verwenden, werden wie normale Wechsellaufwerke behandelt.

  Sie können Vollzugriffe oder Nur-Lesen-Zugriffe zulassen oder Zugriffe auf verschlüsselte Wechsellaufwerke ganz unterbinden, um auf geschützten Computern zu kontrollieren, ob Daten auf verschlüsselte Wechsellaufwerke übertragen oder von diesen kopiert werden dürfen. Die Zugriffsrechte wirken sich nur auf Geräte aus, die mit BitLocker oder FileVault (nur HFS+-Dateisystem) verschlüsselt werden.

  Dieser Gerätetyp wird sowohl unter Windows als auch unter macOS unterstützt.
- **Drucker** (Zugriffskontrolle nach Gerätetyp) – Physische Drucker mit einer beliebigen Schnittstelle zum Anschließen an einen Computer (USB, LPT, Bluetooth usw.) sowie Drucker, auf die von einem Computer im Netzwerk zugegriffen wird.

  Sie können Zugriffe auf Drucker zulassen oder unterbinden, um auf geschützten Computern zu kontrollieren, ob Dokumente auf einem beliebigen Drucker gedruckt werden dürfen.

  Hinweis
  Wenn Sie die Zugriffseinstellung für Drucker auf **Verweigern** ändern, müssen die Applikationen und Prozesse, die auf die Drucker zugreifen, neu gestartet werden, damit die neu konfigurierten Zugriffseinstellungen durchgesetzt werden. Wenn Sie sicherstellen wollen, dass die Zugriffseinstellungen ordnungsgemäß durchgesetzt werden, können Sie auch die geschützten Workloads neu starten.

  Dieser Gerätetyp wird nur unter Windows unterstützt.
- **Zwischenablage** (Zugriffskontrolle nach Gerätetyp) – Windows-Zwischenablage.

  Sie können den Zugriff auf die Zwischenablage zulassen oder unterbinden, um auf geschützten Computern zu kontrollieren, ob Daten über die Windows-Zwischenablage kopiert oder eingefügt werden dürfen.

  Hinweis
  Wenn Sie die Zugriffseinstellung für die Zwischenablage auf **Verweigern** ändern, müssen die Applikationen und Prozesse, die auf die Zwischenablage zugreifen, neu gestartet werden, damit die neu konfigurierten Zugriffseinstellungen durchgesetzt werden. Wenn Sie sicherstellen wollen, dass die Zugriffseinstellungen ordnungsgemäß durchgesetzt werden, können Sie auch die geschützten Workloads neu starten.

  Dieser Gerätetyp wird nur unter Windows unterstützt.
- **Screenshot-Aufnahme** (Zugriffskontrolle nach Gerätetyp) – Ermöglicht es, Screenshots des kompletten Bildschirms, eines aktiven Fensters oder eines ausgewählten Bildschirmbereichs zu machen.

Sie können Zugriffe auf die Screenshot-Aufnahmefunktion erlauben oder verweigern, um Screenshot-Aufnahmen auf geschützten Computern zu kontrollieren.

Hinweis
Wenn Sie die Zugriffseinstellung für Screenshot-Aufnahmen auf **Verweigern** ändern, müssen die Applikationen und Prozesse, die auf die Screenshot-Aufnahmefunktion zugreifen, neu gestartet werden, damit die neu konfigurierten Zugriffseinstellungen durchgesetzt werden. Wenn Sie sicherstellen wollen, dass die Zugriffseinstellungen ordnungsgemäß durchgesetzt werden, können Sie auch die geschützten Workloads neu starten.

Dieser Gerätetyp wird nur unter Windows unterstützt.

- **Mobilgeräte** (Zugriffskontrolle nach Gerätetyp) – Geräte (wie Android-basierte Smartphones), die über das Media-Transfer-Protokoll (MTP) und eine geeignete Schnittstelle/Verbindung (USB, IP, Bluetooth) mit einem Computer kommunizieren.
  Sie können Vollzugriffe oder Nur-Lesen-Zugriffe zulassen oder Zugriffe auf Mobilgeräte ganz unterbinden, um auf geschützten Computern zu kontrollieren, ob Daten auf MTP-basierte Mobilgeräte übertragen oder von diesen kopiert werden dürfen.

  Hinweis
  Wenn Sie die Zugriffseinstellung für Mobilgeräte auf **Nur Lesen** oder **Verweigern** ändern, müssen die Applikationen und Prozesse, die auf die Mobilgeräte zugreifen, neu gestartet werden, damit die neu konfigurierten Zugriffseinstellungen durchgesetzt werden. Wenn Sie sicherstellen wollen, dass die Zugriffseinstellungen ordnungsgemäß durchgesetzt werden, können Sie auch die geschützten Workloads neu starten.

  Dieser Gerätetyp wird nur unter Windows unterstützt.
- **Bluetooth** (Zugriffskontrolle nach Gerätetyp) – Externe und interne Bluetooth-Geräte mit einer beliebigen Schnittstelle zum Anschließen an einen Computer (USB, PCMCIA usw.). Diese Einstellung kontrolliert die grundsätzliche Verwendung von Geräten diesen Typs und nicht den Datenaustausch mit solchen Geräten.
  Sie können Zugriffe über Bluetooth zulassen oder unterbinden, um die Verwendung von Bluetooth-Geräten auf geschützten Computern zu kontrollieren.

  Hinweis
  Unter macOS wirken sich die Zugriffsrechte für Bluetooth nicht auf Bluetooth-HID-Geräte aus. Zugriffe auf diese Geräte sind immer erlaubt, um zu verhindern, dass drahtlose HID-Geräte (Mäuse und Tastaturen) auf iMac- und Mac Pro-Hardware deaktiviert werden können.

  Dieser Gerätetyp wird sowohl unter Windows als auch unter macOS unterstützt.
- **Optische Laufwerke** (Zugriffskontrolle nach Gerätetyp) – Externe und interne CD-/DVD-/BD-Laufwerke mit einer beliebigen Schnittstelle zum Anschließen an einen Computer (IDE, SATA, USB, FireWire, PCMCIA usw.).

Sie können Vollzugriffe oder Nur-Lesen-Zugriffe zulassen oder Zugriffe auf optische Laufwerke ganz unterbinden, um auf geschützten Computern zu kontrollieren, ob Daten auf optische Laufwerke übertragen oder von diesem kopiert werden dürfen.

Dieser Gerätetyp wird sowohl unter Windows als auch unter macOS unterstützt.

- **Diskettenlaufwerke** (Zugriffskontrolle nach Gerätetyp) – Externe und interne Diskettenlaufwerke mit einer beliebigen Schnittstelle zum Anschließen an einen Computer (IDE, USB, PCMCIA usw.). Es gibt einige Diskettenlaufwerksmodelle, die vom Betriebssystem als entfernbare Laufwerke (Wechsellaufwerke) erkannt werden. In diesem Fall wird die Gerätekontrolle auch diese Laufwerke als Wechsellaufwerke identifizieren.

  Sie können Vollzugriffe oder Nur-Lesen-Zugriffe zulassen oder Zugriffe auf Diskettenlaufwerke ganz unterbinden, um auf geschützten Computern zu kontrollieren, ob Daten auf Diskettenlaufwerke übertragen oder von diesem kopiert werden dürfen.

  Dieser Gerätetyp wird nur unter Windows unterstützt.
- **USB** (Zugriffskontrolle nach Geräteschnittstelle) – Alle Geräte (außer Hubs), die über einen USB-Port angeschlossen sind.

  Sie können Vollzugriffe oder Nur-Lesen-Zugriffe zulassen oder Zugriffe auf USB-Ports ganz unterbinden, um auf geschützten Computern zu kontrollieren, ob Daten auf Geräte, die per USB angeschlossen werden, übertragen oder von diesen kopiert werden dürfen.

  Dieser Gerätetyp wird sowohl unter Windows als auch unter macOS unterstützt.
- **FireWire** (Zugriffskontrolle nach Geräteschnittstelle) – Alle Geräte (außer Hubs), die über einen FireWire-Port (IEEE 1394) angeschlossen sind.

  Sie können Vollzugriffe oder Nur-Lesen-Zugriffe zulassen oder Zugriffe auf FireWire-Ports ganz unterbinden, um auf geschützten Computern zu kontrollieren, ob Daten auf Geräte, die per FireWire angeschlossen werden, übertragen oder von diesen kopiert werden dürfen.

  Dieser Gerätetyp wird sowohl unter Windows als auch unter macOS unterstützt.
- **Umgeleitete Geräte** (Zugriffskontrolle nach Geräteschnittstelle) – Zugeordnete Laufwerke (Festplatten, Wechsellaufwerke und optische Laufwerke), USB-Geräte und die Zwischenablage, die zu virtuellen Applikationen/Desktop-Sitzungen umgeleitet werden.

  Die Gerätekontrolle erkennt Geräte, die über bestimmte Remoting-Protokolle (Microsoft RDP, Citrix ICA, VMware PCoIP, HTML5/WebSockets) in bestimmten Virtualisierungsumgebungen (Microsoft RDS, Citrix XenDesktop, Citrix XenApp, Citrix XenServer, VMware Horizon) umgeleitet werden, wo geschützte Computer gehostet werden. Sie kann außerdem Datenkopieraktionen zwischen der Windows-Zwischenablage eines Gast-Betriebssystems (welches unter VMware Workstation, VMware Player, Oracle VM, VirtualBox oder Windows Virtual PC läuft) und der Zwischenablage des entsprechenden Host-Betriebssystems (welches auf einem geschützten Windows-Computer läuft) kontrollieren.

  Dieser Gerätetyp wird nur unter Windows unterstützt.

  Sie können Zugriffe auf umgeleitete Geräte folgendermaßen konfigurieren:

  - **Zugeordnete Laufwerke** – Sie können Vollzugriffe oder Nur-Lesen-Zugriffe zulassen oder Zugriffe ganz unterbinden, um zu kontrollieren, ob Daten auf Festplattenlaufwerke, Wechsellaufwerke oder optische Laufwerke, die zu der Sitzung umgeleitet werden, die auf einem geschützten Computer gehostet wird, übertragen oder von diesen kopiert werden

dürfen.

- **Eingehende Zwischenablage** – Sie können Zugriffe zulassen oder unterbinden, um zu kontrollieren, ob Daten über die Zwischenablage zu der Sitzung kopiert werden dürfen, die auf einem geschützten Computer gehostet wird.

  Hinweis
  Wenn Sie die Zugriffseinstellung für die eingehende Zwischenablage auf **Verweigern** ändern, müssen die Applikationen und Prozesse, die auf die Zwischenablage zugreifen, neu gestartet werden, damit die neu konfigurierten Zugriffseinstellungen durchgesetzt werden. Wenn Sie sicherstellen wollen, dass die Zugriffseinstellungen ordnungsgemäß durchgesetzt werden, können Sie auch die geschützten Workloads neu starten.

- **Ausgehende Zwischenablage** – Sie können Zugriffe zulassen oder unterbinden, um zu kontrollieren, ob Daten über die Zwischenablage von der Sitzung kopiert werden dürfen, die auf einem geschützten Computer gehostet wird.

  Hinweis
  Wenn Sie die Zugriffseinstellung für die ausgehende Zwischenablage auf **Verweigern** ändern, müssen die Applikationen und Prozesse, die auf die Zwischenablage zugreifen, neu gestartet werden, damit die neu konfigurierten Zugriffseinstellungen durchgesetzt werden. Wenn Sie sicherstellen wollen, dass die Zugriffseinstellungen ordnungsgemäß durchgesetzt werden, können Sie auch die geschützten Workloads neu starten.

- **USB-Anschlüsse** – Sie können Zugriffe zulassen oder unterbinden, um zu kontrollieren, ob Daten auf/von Geräten kopiert werden dürfen, die an einen USB-Port angeschlossen sind, der zu der Sitzung umgeleitet wird, die auf einem geschützten Computer gehostet wird.

Die Einstellungen der Gerätekontrolle wirken sich auf alle Benutzer gleichermaßen aus. Wenn Sie beispielsweise Zugriffe auf Wechsellaufwerke verbieten, darf kein Benutzer auf diesem geschützten Computer irgendwelche Daten auf ein solches Wechsellaufwerk übertragen oder von diesem kopieren. Es ist jedoch möglich, Zugriffe auf einzelne USB-Geräte selektiv zuzulassen, indem Sie diese von der Zugriffskontrolle ausschließen (siehe auch die Abschnitte 'Positivliste für Gerätetypen und 'Positivliste für USB-Geräte').

Wenn Zugriffe auf ein Gerät sowohl über dessen Typ als auch über dessen Schnittstelle kontrolliert werden, haben die Zugriffseinschränkungen auf der Schnittstellenebene Vorrang. Wenn beispielsweise Zugriffe auf USB-Ports (als Geräteschnittstelle) verboten sind, werden Zugriffe auf Mobilgeräte, die per USB angeschlossen sind, grundsätzlich unterbunden – und das auch dann, wenn Zugriffe auf Mobilgeräte an sich (als Gerätetyp) erlaubt sind. Um Zugriffe auf ein solches Gerät zu erlauben, müssen Sie sowohl dessen Schnittstelle als auch dessen Typ zulassen.

Hinweis
Wenn der unter macOS verwendete Schutzplan Einstellungen für Gerätetypen enthält, die nur unter Windows unterstützt werden, dann werden die entsprechenden Einstellungen für diese Gerätetypen unter macOS ignoriert.

Wichtig
Wenn ein Wechsellaufwerk, ein verschlüsseltes Wechsellaufwerk, ein Drucker oder ein Bluetooth-Gerät an einen USB-Port angeschlossen ist und es Zugriffseinschränkung auf USB-Schnittstellenebene gibt, so werden diese außer Kraft gesetzt, wenn Zugriffe auf eines dieser Geräte zugelassen werden. Wenn Sie also den entsprechenden Gerätetyp zulassen, werden alle Zugriffe auf das jeweilige Gerät auch dann erlaubt, wenn Zugriffe auf USB-Ports untersagt sind.

Betriebssystem-Benachrichtigung und Service-Alarmmeldungen

Sie können die Gerätekontrolle so konfigurieren, dass den Endanwendern eine Betriebssystem-Benachrichtigung angezeigt wird, wenn sie versuchen, auf einem geschützten Computer einen blockierten Gerätetyp zu verwenden. Wenn das Kontrollkästchen **Betriebssystem-Benachrichtigung für Endbenutzer anzeigen, wenn diese versuchen, einen blockierten Gerätetyp oder Anschluss zu verwenden** in den Zugriffseinstellungen aktiviert ist, wird der Agent eine Popup-Meldung im Infobereich der Taskleiste des geschützten Computers anzeigen, falls eines der folgenden Ereignisse eintritt:

- Ein verweigerter Versuch, ein Gerät an einem USB- oder FireWire-Port zu verwenden. Diese Benachrichtigung wird immer dann angezeigt, wenn der Anwender ein USB- oder FireWire-Gerät anschließt, dem der Zugriff auf Schnittstellenebene (z.B. blockerter Zugriff auf USB Ports) oder auf Typebene (z.B. blockerter Zugriff auf Wechselmedien) verweigert wird. Die Benachrichtigung informiert den Anwender darüber, dass er nicht auf das spezifizierte Gerät/Laufwerk zugreifen darf.
- Ein verweigerter Versuch, ein Datenobjekt (z.B. eine Datei) von einem bestimmten Gerät zu kopieren. Diese Benachrichtigung erscheint, wenn Lesezugriffe auf folgende Geräte verweigert werden: Diskettenlaufwerke, optische Laufwerke, Wechsellaufwerke, verschlüsselte Wechsellaufwerke, Mobilgeräte, umgeleitete Netzlaufwerke und umgeleitete eingehende Zwischenablage-Daten. Die Benachrichtigung informiert den Anwender darüber, dass er das spezifizierte Datenobjekt nicht vom spezifizierten Gerät abrufen darf.
  Die Benachrichtigung über den verweigerten Lesezugriff wird auch angezeigt, wenn Lese-/Schreibzugriffe auf Bluetooth-, FireWire-, USB- oder umgeleitete USB-Anschlüsse verweigert werden.
- Ein verweigerter Versuch, ein Datenobjekt (z.B. eine Datei) zu einem bzw. auf ein bestimmtes Gerät zu kopieren. Diese Benachrichtigung erscheint, wenn Schreibzugriffe auf folgende Geräte verweigert werden: Diskettenlaufwerke, optische Laufwerke, Wechsellaufwerke, verschlüsselte Wechsellaufwerke, Mobilgeräte, lokale Zwischenablage, Screenshot-Aufnahmen, Drucker, umgeleitete Netzlaufwerke und umgeleitete ausgehende Zwischenablage-Daten. Die Benachrichtigung informiert den Anwender darüber, dass er das spezifizierte Datenobjekt nicht zu dem spezifizierten Gerät übertragen darf.

Wenn ein Anwender versucht, auf die blockierten Geräte eines geschützten Computers zuzugreifen, können Alarmmeldungen ausgelöst werden, die in der Cyber Protect-Konsole protokolliert werden. Sie können für jeden Gerätetyp (außer Screenshot-Aufnahmen) oder Port separate Alarmmeldungen aktivieren, wenn Sie in den entsprechenden Zugriffseinstellungen das

Kontrollkästchen **Alarm anzeigen** aktivieren. Wenn z.B. für Wechsellaufwerke die Zugriffsbeschränkung mit 'schreibgeschützt' festgelegt wurde und für diesen Gerätetyp zusätzlich das Kontrollkästchen **Alarm anzeigen** aktiviert wurde, wird jedes Mal eine Alarmmeldung protokolliert, wenn ein Anwender auf dem entsprechend geschützten Computer versucht, Daten zu einem Wechsellaufwerk zu kopieren. Weitere Informationen finden Sie im Abschnitt Gerätekontrolle-Alarmmeldungen.

Sieh auch Schritte zum Aktivieren oder Deaktivieren von Betriebssystem-Benachrichtigung und Service-Alarmmeldungen.

Positivliste für Gerätetypen

Auf der Seite **Positivliste für Gerätetypen** können Sie Geräteunterklassen auswählen, die von der Gerätezugriffskontrolle ausgeschlossen werden sollen. Dadurch wird der Zugriff auf diese Geräte erlaubt – unabhängig von den Zugriffseinstellungen im Gerätekontrolle-Modul.

Das Gerätekontrolle-Module bietet die Möglichkeit, innerhalb eines eigentlich eingeschränkten Gerätetypes den Zugriff auf bestimmte Geräteunterklassen dennoch zu erlauben. Mit dieser Option können Sie alle Geräte eines bestimmten Typs einschränken und dann Ausnahmen für bestimmte Geräteunterklassen definieren, die zu diesem Gerätetyp gehören. Dies kann beispielsweise nützlich sein, wenn Sie den Zugriff auf alle USB-Ports verweigern möchten, dabei aber die Verwendung einer USB-Tastatur und -Maus weiter zulassen wollen.

Beim Konfigurieren des Gerätekontrolle-Moduls können Sie spezifizieren, welche Geräteunterklassen von der Gerätezugriffskontrolle ausgeschlossen werden sollen. Wenn ein Gerät zu einer ausgeschlossenen Unterklasse gehört, ist der Zugriff auf dieses Gerät erlaubt, unabhängig davon, ob der jeweilige Gerätetyp oder Port eingeschränkt ist oder nicht. Sie können folgende Geräteunterklassen selektiv von der Gerätezugriffskontrolle ausschließen:

- **USB-HID (Eingabegeräte wie Maus, Tastatur etc.)** – Wenn diese Option ausgewählt ist, wird der Zugriff auf Eingabegeräte (wie Maus oder Tastatur), die per USB angeschlossen werden, auch dann erlaubt, wenn alle USB-Anschlüsse gesperrt sind. Dieses Element ist standardmäßig ausgewählt, damit Mäuse und Tastaturen auch weiterhin funktionieren, wenn Sie den Zugriff auf USB-Anschlüsse unterbinden.
  Wird sowohl unter Windows als auch macOS unterstützt.
- **USB- und FireWire-Netzwerkkarten** – Wenn diese Option ausgewählt ist, wird der Zugriff auf Netzwerkkarten, die per USB oder FireWire (IEEE 1394) angeschlossen werden, auch dann erlaubt, wenn alle USB- bzw. FireWire-Ports gesperrt sind.
  Wird sowohl unter Windows als auch macOS unterstützt.
- **USB-Scanner und -Standbildgeräte** – Wenn diese Option ausgewählt ist, wird der Zugriff auf Scanner und ähnliche Bildgeräte, die per USB angeschlossen werden, auch dann erlaubt, wenn alle USB-Anschlüsse gesperrt sind.
  Wird nur unter Windows unterstützt.
- **USB-Audio-Geräte** – Wenn diese Option ausgewählt ist, wird der Zugriff auf Audiogeräte (wie Headsets oder Mikrofone), die per USB angeschlossen werden, auch dann erlaubt, wenn alle

USB-Anschlüsse gesperrt sind.
Wird nur unter Windows unterstützt.

- **USB-Kameras** – Wenn diese Option ausgewählt ist, wird der Zugriff auf Webcams, die per USB angeschlossen werden, auch dann erlaubt, wenn alle USB-Anschlüsse gesperrt sind.
  Wird nur unter Windows unterstützt.
- **Bluetooth-HID (Eingabegeräte wie Maus, Tastatur etc.)** – Wenn diese Option ausgewählt ist, wird der Zugriff auf Eingabegeräte (wie Maus oder Tastatur), die per Bluetooth angeschlossen werden, auch dann erlaubt, wenn Bluetooth-Geräte gesperrt sind.
  Wird nur unter Windows unterstützt.
- **Applikationsinterne Zwischenablage-Aktionen (Kopieren/Einfügen)** – Wenn diese Option ausgewählt ist, wird das Kopieren/Einfügen von Daten über die Zwischenablage innerhalb ein und derselben Applikation erlaubt, auch wenn Zwischenablage-Übertragungen ansonsten grundsätzlich gesperrt sind.
  Wird nur unter Windows unterstützt.

Hinweis
Einstellungen für nicht unterstützte Geräteunterklassen werden ignoriert, wenn diese Einstellungen im angewendeten Schutzplan konfiguriert sind.

Wenn Sie Gerätetypen in eine Positivliste aufnehmen, sollten Sie Folgendes beachten:

- Sie können bei einer Positivliste für Gerätetypen nur jeweils eine komplette Geräteunterklasse zulassen. Sie können also nicht den Zugriff auf ein bestimmtes Gerätemodell zulassen, während Sie gleichzeitig alle Geräte derselben Unterklasse einschränken. Wenn Sie beispielsweise USB-Kameras von der Gerätezugriffskontrolle ausschließen, wird dadurch die Verwendung jeder USB-Kamera zugelassen (egal welches Modell und Hersteller). Wie Sie individuelle Geräte/Modelle zulassen können, finden Sie im Abschnitt 'Positivliste für USB-Geräte' erläutert.
- Gerätetypen können nur aus einer geschlossenen Liste von Geräteunterklassen ausgewählt werden. Wenn das zuzulassende Gerät zu einer anderen Unterklasse gehört, kann es nicht über eine Positivliste für Gerätetypen erlaubt werden. So kann beispielsweise eine Unterklasse wie 'USB-Smartcard-Lesegerät' nicht in die Positivliste aufgenommen werden. Anweisungen darüber, wie Sie ein USB-Smartcard-Lesegerät erlauben können, wenn alle USB-Anschlüsse gesperrt sind, finden Sie im Abschnitt 'Positivliste für USB-Geräte'.
- Die Positivliste für Gerätetypen funktioniert nur bei Geräten, die Standard-Windows-Treiber verwenden. Denn bei manchen USB-Geräten mit proprietären Treibern kann es vorkommen, dass die Gerätekontrolle die Unterklasse nicht erkennt. Daher können Sie den Zugriff auf solche USB-Geräte nicht über die Positivliste für Gerätetypen erlauben In diesem Fall können Sie den Zugriff auf Basis einer pro-Gerät/pro-Modell-Ausnahme erlauben (siehe 'Positivliste für Gerätetypen').

Positivliste für USB-Geräte

Die Positivliste dient dazu, die Verwendung bestimmter USB-Geräte unabhängig von anderen Einstellungen der Gerätekontrolle zu erlauben. Sie können einzelne Geräte oder Gerätemodelle zur

Positivliste hinzufügen, um die Zugriffskontrolle für diese Geräte zu deaktivieren. Wenn Sie beispielsweise ein Mobilgerät mithilfe seiner eindeutigen ID zur Positivliste hinzufügen, wird die Verwendung dieses einen Geräts erlaubt, obwohl alle anderen USB-Geräte gesperrt sind.

Sie können auf der Seite **Positivliste für USB-Geräte** einzelne USB-Geräte oder USB-Gerätemodelle spezifizieren, die von der Gerätezugriffskontrolle ausgeschlossen werden sollen. Dadurch wird der Zugriff auf diese Geräte erlaubt – unabhängig von den Zugriffseinstellungen im Gerätekontrolle-Modul.

Es gibt zwei Möglichkeiten, Geräte in der Positivliste zu identifizieren:

- Das Modell des Geräts – identifiziert alle Geräte, die zu einem bestimmten Modell gehören. Jedes Gerätemodell wird anhand einer Anbieter-ID (VID, V für Vendor) sowie einer Produkt-ID (PID) identifiziert – beispielsweise USB\VID_0FCE&PID_E19E.

  Diese Kombination aus VID und PID identifiziert jedoch nicht ein einzelnes Gerät, sondern ein ganzes Gerätemodell. Wenn Sie also ein Gerätemodell zur Positivliste hinzufügen, wird dadurch der Zugriff auf alle Geräte dieses Modells erlaubt. Auf diese Weise können Sie z.B. die Verwendung von USB-Druckern eines bestimmten Modells zulassen.
- Eine eindeutige Gerätekennung – identifiziert ein bestimmtes Gerät. Jede eindeutige Gerätekennung wird durch eine Anbieter-ID (VID, V für Vendor) eine Produkt-ID (PID) und eine Seriennummer identifiziert – beispielsweise USB\VID_0FCE&PID_E19E\D55E7FCA.

  Nicht allen USB-Geräten erhalten eine Seriennummer. Sie können ein Gerät jedoch nur dann als eindeutiges Gerät in eine Positivliste aufnehmen, wenn dem Gerät bei seiner Herstellung eine Seriennummer zugewiesen wurde. Ein Beispiel wäre ein USB-Stick, der eine eindeutige Seriennummer hat.

Wenn Sie ein Gerät zur Positivliste hinzufügen wollen, müssen Sie es zunächst in die USB-Geräte-Datenbank aufnehmen. Anschließend können Sie Geräte in die Positivliste aufnehmen, indem Sie diese aus der Datenbank auswählen.

Die Positivliste wird auf einer separaten Konfigurationsseite verwaltet, die **Positivliste für USB-Geräte** heißt. Jedes Element in der Liste steht für ein Gerät oder ein Gerätemodell und verfügt über folgende Felder:

- **Beschreibung** – Das Betriebssystem vergibt für ein USB-Gerät, wenn dieses angeschlossen wird, eine bestimmte Beschreibung. Sie können die Beschreibung des jeweiligen Geräts in der USB-Geräte-Datenbank ändern (siehe den Abschnitt 'Verwaltungsseite für die USB-Datenbank').
- **Gerätetyp** – Zeigt 'Eindeutig' an, wenn das Listenelement für ein eindeutiges Gerät steht, oder 'Modell', wenn es für ein Gerätemodell steht.
- **Nur lesen** – Wenn dies ausgewählt wurde, können nur Daten vom Gerät abgerufen werden (aber nicht auf dieses geschrieben). Wenn ein Gerät keinen Nur-Lesen-Zugriff unterstützt, wird der Zugriff auf das Gerät vollständig gesperrt. Deaktivieren Sie dieses Kontrollkästchen, wenn Sie den vollen Zugriff auf das Gerät erlauben wollen.
- **Erneut initialisieren** – Wenn diese Option ausgewählt ist, wird das Gerät bei der Anmeldung eines neuen Benutzers eine Trennen-/Erneut-Verbinden-Aktion simulieren. Einige USB-Geräte benötigen eine Neuinitialisierung, um richtig zu funktionieren. Daher empfehlen wir, bei solchen

Geräten (Mäuse, Tastaturen usw.) dieses Kontrollkästchen zu aktivieren. Bei Datenspeichergeräten (wie USB-Sticks, optischen Laufwerken oder externen Festplatten) empfehlen wir jedoch, dieses Kontrollkästchen zu deaktivieren.
Bei manchen USB-Geräten mit proprietären Treibern kann es vorkommen, dass die Gerätekontrolle die Geräte nicht neu initialisieren kann. Wenn auf ein solches Gerät nicht zugegriffen werden kann, müssen Sie das USB-Gerät aus dem USB-Port entfernen und dann wieder einstecken.

Hinweis
Das Feld **Erneut initialisieren** ist standardmäßig ausgeblendet. Um es in der Tabelle anzuzeigen, klicken Sie in der rechten oberen Ecke der Tabelle auf das Zahnradsymbol und aktivieren Sie dann das Kontrollkästchen **Erneut initialisieren**.

Hinweis
Die Felder **Nur Lesen** und **Erneut initialisieren** werden unter macOS nicht unterstützt. Wenn diese Felder im angewendeten Schutzplan konfiguriert sind, werden sie ignoriert.

Sie können Geräte/Modelle folgendermaßen zur Positivliste hinzufügen oder aus dieser entfernen:

- Klicken Sie über der Liste auf den Befehl **Aus Datenbank hinzufügen** und wählen Sie dann das/die gewünschte(n) Gerät(e) aus, die in der USB-Geräte-Datenbank registriert sind. Das ausgewählte Gerät wird in die Liste aufgenommen, wo Sie noch dessen Einstellungen konfigurieren und die Änderungen bestätigen können.
- Klicken Sie in einer Alarmmeldung, die anzeigt, dass der Zugriff auf ein USB-Gerät gesperrt ist, auf den Befehl **Dieses USB-Gerät erlauben** (siehe den Abschnitt 'Gerätekontrolle-Alarmmeldungen'). Dadurch wird das Gerät zur Positivliste (und gleichzeitig auch zur USB-Geräte-Datenbank) hinzugefügt.
- Klicken Sie auf das Symbol 'Löschen' am Ende eines Listenelements. Dadurch wird das entsprechende Gerät/Modell aus der Positivliste entfernt.

USB-Geräte-Datenbank

Das Gerätekontrolle-Modul verwaltet eine Datenbank mit USB-Geräten, aus der Sie Geräte in eine Ausschlussliste aufnehmen können (siehe den Abschnitt 'Positivliste für USB-Geräte'). Ein USB-Gerät kann auf eine der folgenden Arten in der Datenbank registriert werden:

- Ein Gerät auf der Seite hinzufügen, die angezeigt wird, wenn ein Gerät in die Ausschlussliste aufgenommen wird (siehe den Abschnitt 'Verwaltungsseite für die USB-Geräte-Datenbank').
- Ein Gerät über die Registerkarte 'USB-Geräte' im Fensterbereich 'Inventarisierung' eines Computers in der Cyber Protect-Konsole hinzufügen (siehe den Abschnitt 'Liste der USB-Geräte auf einem Computer').
- Das Gerät über eine Alarmmeldung zulassen, die darüber informiert, dass der Zugriff auf das USB-Gerät eingeschränkt wurde (siehe den Abschnitt 'Gerätekontrolle-Alarmmeldungen').

Siehe auch die Schritte, um USB-Geräte zur Datenbank hinzuzufügen oder aus dieser zu entfernen.

Verwaltungsseite für die USB-Geräte-Datenbank

Wenn Sie die Positivliste für USB-Geräte konfigurieren, können Sie ein Gerät aus der Datenbank hinzufügen. Wenn Sie diese Option wählen, wird eine Verwaltungsseite mit einer Geräteliste angezeigt. Auf dieser Seite können Sie die Liste aller Geräte einsehen, die in der Datenbank registriert sind. Sie können dann Geräte auswählen, die in die Positivliste aufgenommen werden sollen, und folgende Aktionen durchführen:

Ein Gerät in der Datenbank registrieren

1. Klicken Sie im oberen Bereich der Seite auf **Zur Datenbank hinzufügen**.
2. Wählen Sie im angezeigten Dialog **USB-Gerät hinzufügen** die Maschine aus, mit der das USB-Gerät verbunden ist.
   Es werden nur Maschinen in der Liste der Computer angezeigt, die online sind.
   Die Liste der USB-Geräte wird nur für solche Maschinen angezeigt, auf denen der Agent für Data Loss Prevention installiert ist.
   Die USB-Geräte werden in der Baumansicht aufgelistet. Die erste Ebene des Verzeichnisbaums repräsentiert ein Gerätemodell. Die zweite Ebene repräsentiert ein bestimmtes Gerät dieses Modells.
   Ein blaues Symbol neben der Beschreibung des Geräts signalisiert, dass das Gerät aktuell mit dem Computer verbunden ist. Das Symbol ist ausgegraut, wenn das Gerät nicht an den Computer angeschlossen ist.
3. Aktivieren Sie das Kontrollkästchen für dasjenige USB-Gerät, welches Sie registrieren wollen, und klicken Sie anschließend auf **Zur Datenbank hinzufügen**.

Die Beschreibung eines Geräts ändern

1. Klicken Sie auf der Seite **USB-Geräte-Datenbank** zuerst auf das Drei-Punkte-Symbol (...) am Ende des Listenelements, welches das Gerät repräsentiert, und dann auf **Bearbeiten**.
2. Nehmen Sie im angezeigten Dialogfenster die gewünschten Änderungen an der Beschreibung vor.

Ein Gerät aus der Datenbank entfernen

1. Klicken Sie auf das Drei-Punkte-Symbol (...) am Ende des Listenelements, welches das Gerät repräsentiert.
2. Klicken Sie auf **Löschen** und bestätigen Sie die Löschaktion.

Die Liste auf der Seite stellt für jedes Gerät folgende Informationen bereit:

- **Beschreibung** – Eine lesbare lesbare Kennung für das Gerät. Sie können die Beschreibung bei Bedarf ändern.
- **Gerätetyp** – Zeigt 'Eindeutig' an, wenn das Listenelement für ein eindeutiges Gerät steht, oder 'Modell', wenn es für ein Gerätemodell steht. Ein eindeutiges Gerät muss eine Seriennummer zusammen mit einer Hersteller-ID (VID) und einer Produkt-ID (PID) haben. Ein Gerätemodell wird dagegen nur durch eine Kombination aus VID und PID identifiziert.

- **Hersteller-ID**, **Produkt-ID**, **Seriennummer** – Diese Werte ergeben zusammen die Geräte-ID in der Form 'USB\VID_<Hersteller-ID>&PID_<Produkt-ID>\<Seriennummer>'.
- **Konto** – Kennzeichnet den Mandanten, zu dem dieses Gerät gehört. Das ist der Mandant, der das Benutzerkonto enthält, mit dem das Gerät in der Datenbank registriert wurde.

Hinweis
Diese Spalte ist standardmäßig ausgeblendet. Um es in der Tabelle anzuzeigen, klicken Sie in der rechten oberen Ecke der Tabelle auf das Zahnradsymbol und wählen Sie dann **Konto**.

Die Spalte ganz links ist zur Auswahl der Geräte gedacht, die in die Positivliste aufgenommen werden sollen: Aktivieren Sie das Kontrollkästchen für jedes Gerät, das Sie hinzufügen wollen, und klicken Sie dann auf die Schaltfläche **Zur Positivliste hinzufügen**. Wenn Sie alle Kontrollkästchen (de)aktivieren wollen, müssen Sie auf das Kontrollkästchen in der Spaltenüberschrift klicken.

Sie können die Geräteliste durchsuchen oder filtern:

- Klicken Sie im oberen Bereich der Seite auf **Suchen** und geben Sie den gewünschten Suchbegriff ein. In der Liste werden diejenigen Geräte angezeigt, deren Beschreibung der eingegebenen Zeichenfolge entspricht.
- Klicken Sie auf **Filter**, um dann im angezeigten Dialogfenster einen Filter konfigurieren und anwenden zu können. Die Liste wird auf die Geräte mit dem Typ, der Hersteller-ID, der Produkt-ID oder dem Konto eingegrenzt, die Sie beim Konfigurieren des Filters ausgewählt haben. Wenn Sie den Filter zurücksetzen wollen, damit wieder alle Geräte aufgelistet werden, dann klicken Sie auf **Auf Standard zurücksetzen**.

Die Liste der USB-Geräte in der Datenbank exportieren

Sie können die Liste der USB-Geräte, die in die Datenbank aufgenommen wurden, exportieren.

1. Öffnen Sie den Schutzplan eines Geräts, um diesen zu bearbeiten.
2. Klicken Sie zuerst neben dem **Gerätekontrolle**-Schalter auf das Pfeilsymbol, damit die Einstellungen erweitert werden, und dann auf die Zeile **Positivliste für USB-Geräte**.
3. Klicken Sie auf der Seite mit der Positivliste für USB-Geräte auf den Befehl **Aus Datenbank hinzufügen**.
4. Klicken Sie auf der dann angezeigten Verwaltungsseite für die USB-Geräte-Datenbank auf den Befehl **Exportieren**.
   Der Standard-Dialog zum Durchsuchen wird geöffnet.
5. Bestimmen Sie, wo die Datei gespeichert werden soll, geben Sie bei Bedarf einen neuen Dateinamen ein und klicken Sie anschließend auf **Speichern**.

Die Liste der USB-Geräte wird als JSON-Datei exportiert.

Sie können die resultierende JSON-Datei mit einem Text-Editor bearbeiten, um Geräte hinzuzufügen, zu entfernen oder die Gerätebeschreibungen in größerem Umfang zu ändern.

Eine Liste von USB-Geräten in die Datenbank importieren

Anstatt USB-Geräte über die Cyber Protect-Konsole hinzuzufügen, können Sie auch eine Liste von USB-Geräten importieren. Die Liste ist eine Datei im JSON-Format.

Hinweis
Sie können JSON-Dateien in eine Datenbank importieren, die die in der Datei beschriebenen Geräte nicht enthält. Wenn Sie eine geänderte Datei in die Datenbank importieren wollen, aus der sie zuvor exportiert wurde, müssen Sie die Datenbank zuerst löschen, weil Sie keine doppelten Einträge importieren dürfen. Wenn Sie eine Liste der USB-Geräte exportieren, diese bearbeiten und dann versuchen, die Liste wieder zurück in dieselbe Datenbank zu übernehmen, ohne dass Sie die Datenbank zuvor bereinigt haben, wird der Import fehlschlagen.

1. Öffnen Sie den Schutzplan eines Geräts, um diesen zu bearbeiten.
2. Klicken Sie zuerst neben dem **Gerätekontrolle**-Schalter auf das Pfeilsymbol, damit die Einstellungen erweitert werden, und dann auf die Zeile **Positivliste für USB-Geräte**.
3. Klicken Sie auf der Seite mit der Positivliste für USB-Geräte auf den Befehl **Aus Datenbank hinzufügen**.
4. Klicken Sie auf der dann angezeigten Verwaltungsseite für die USB-Geräte-Datenbank auf den Befehl **Importieren**.
   Das Dialogfenster 'USB-Geräte aus Datei importieren' wird geöffnet.
5. Verwenden Sie Drag & Drop oder suchen Sie nach der Datei, die Sie importieren wollen.

Die Cyber Protect-Konsole überprüft, ob die Liste doppelte Einträge enthält, die bereits in der Datenbank vorhanden sind, und überspringt diese. Die USB-Geräte, die nicht in der Datenbank gefunden werden konnten, werden an dann in die Datenbank übernommen.

Liste der USB-Geräte auf einem Computer

Der Fensterbereich 'Inventarisierung' eines Computers in der Cyber Protect-Konsole enthält die Registerkarte **USB-Geräte**. Wenn der Computer online ist und der Agent für Data Loss Prevention auf diesem installiert ist, wird auf der Registerkarte **USB-Geräte** eine Liste mit allen USB-Geräten angezeigt, die jemals mit diesem Computer verbunden waren.

Die USB-Geräte werden in der Baumansicht aufgelistet. Die erste Ebene des Verzeichnisbaums repräsentiert ein Gerätemodell. Die zweite Ebene repräsentiert ein bestimmtes Gerät dieses Modells.

In der Liste werden für jedes Gerät folgende Informationen bereitgestellt:

- **Beschreibung** – Das Betriebssystem vergibt für ein USB-Gerät, wenn dieses angeschlossen wird, eine Beschreibung. Diese Beschreibung kann als lesbare Gerätekennung dienen.
  Ein blaues Symbol neben der Beschreibung des Geräts signalisiert, dass das Gerät aktuell mit dem Computer verbunden ist. Das Symbol ist ausgegraut, wenn das Gerät nicht an den Computer angeschlossen ist.
- **Geräte-ID** – Die Kennung (Identifier), die das Betriebssystem dem Gerät zugewiesen hat. Diese ID hat folgendes Format: USB\VID_<Anbieter-ID>&PID_<Produkt-ID>\<Seriennummer> – wobei die

<Seriennummer> optional ist. Beispiele: USB\VID_0FCE&PID_ADDE\D55E7FCA (Gerät mit Seriennummer); USB\VID_0FCE&PID_ADDE (Gerät ohne Seriennummer).

Wenn Sie Geräte in die USB-Geräte-Datenbank aufnehmen wollen, müssen Sie die Kontrollkästchen der gewünschten Geräte aktivieren und dann auf die Schaltfläche **Zur Datenbank hinzufügen** klicken.

Prozesse von der Zugriffskontrolle ausschließen

Der Zugriff auf die Windows-Zwischenablage, Screenshot-Aufnahmen, Drucker und Mobilgeräte wird über sogenannte „Hooks“ gesteuert, die in Prozesse injiziert werden. Ein Hook kann grob mit dem Wort Einschubmethode übersetzt werden und ist eine Art Schnittstelle, um fremden Programmcode in vorhandene Applikationen einfügen zu können. Wenn Prozesse nicht „gehookt“ sind (kein Hook aufgerufen werden kann), kann der Zugriff auf die entsprechenden Geräte nicht kontrolliert werden.

Hinweis
Das Ausschließen von Prozessen von der Zugriffskontrolle wird unter macOS nicht unterstützt. Wenn im angewendeten Schutzplan eine Liste mit ausgeschlossenen Prozessen konfiguriert ist, wird diese ignoriert.

Sie können auf der Seite **Ausschlüsse** eine Liste von Prozessen spezifizieren, die nicht gehookt werden sollen. Das bedeutet, dass auf solche Prozesse keine Zugriffskontrollen für die Zwischenablage (lokal oder umgeleitet), Screenshot-Aufnahmen, Drucker oder Mobilgeräte angewendet werden können.

Ein Beispiel: Sie haben einen Schutzplan angewendet, der Zugriffe auf Drucker verweigert, und dann die Applikation Microsoft Word gestartet. Wenn ein entsprechender Anwender versucht, von dieser Applikation aus zu drucken, wird dies blockiert. Wenn Sie jedoch den Microsoft Word-Prozess zur Liste der Ausschlüsse hinzufügen, wird die Applikation nicht mehr gehookt. Infolgedessen wird auch das Drucken aus Microsoft Word nicht mehr blockiert. Aus anderen Applikationen heraus kann aber auch weiterhin nicht mehr gedruckt werden.

So können Sie Prozesse zu den Ausschlüssen hinzufügen

1. Öffnen Sie den Schutzplan eines Geräts, um diesen zu bearbeiten:
   Klicken Sie neben dem Namen des Schutzplans auf das Drei-Punkte-Symbol (...) und wählen Sie anschließend den Befehl **Bearbeiten**.

   Hinweis
   Die Gerätekontrolle muss im Plan aktiviert worden sein, damit Sie auf die Einstellungen der Gerätekontrolle zugreifen können.

2. Klicken Sie zuerst neben dem **Gerätekontrolle**-Schalter auf das Pfeilsymbol, damit die Einstellungen erweitert werden, und dann auf die Zeile **Ausschlüsse**.

3. Klicken Sie auf der Seite **Ausschlüsse** und in der Zeile **Prozesse und Ordner** auf den Befehl **+Hinzufügen**.
4. Geben Sie die Prozesse ein, die Sie von der Zugriffskontrolle ausschließen wollen.
   Beispiel: `C:\Ordner\Unterordner\prozess.exe`.
   Sie können Platzhalterzeichen (Wildcards) verwenden:
   - * steht für eine beliebige Anzahl von Zeichen.
   - ? ersetzt ein einzelnes Zeichen.

   Beispiel:

   ```
   C:\Ordner\*
   *\Ordner\Unterordner?\*
   *\prozess.exe
   ```
5. Klicken Sie zuerst auf das Häkchensymbol und dann auf **Fertig**.
6. Klicken Sie im Schutzplan auf **Speichern**.
7. Starten Sie die ausgeschlossenen Prozesse neu, um sicherzustellen, dass die Hooks richtig entfernt wurden.

Die ausgeschlossenen Prozesse haben nun Zugriff auf die Zwischenablage, Screenshot-Aufnahmen, Drucker und Mobilgeräte – unabhängig von den Zugriffseinstellungen für diese Geräte.

So können Sie einen Prozess von der Ausschlussliste entfernen

Öffnen Sie den Schutzplan eines Geräts, um diesen zu bearbeiten:

Klicken Sie neben dem Namen des Schutzplans auf das Drei-Punkte-Symbol (...) und wählen Sie anschließend den Befehl **Bearbeiten**.

Hinweis
Die Gerätekontrolle muss im Plan aktiviert worden sein, damit Sie auf die Einstellungen der Gerätekontrolle zugreifen können.

1. Klicken Sie zuerst neben dem **Gerätekontrolle**-Schalter auf das Pfeilsymbol, damit die Einstellungen erweitert werden, und dann auf die Zeile **Ausschlüsse**.
2. Klicken Sie auf der Seite **Ausschlüsse** auf das Papierkorb-Symbol neben dem Prozess, den Sie aus der Ausschlussliste entfernen wollen.
3. Klicken Sie auf **Fertig**.
4. Klicken Sie im Schutzplan auf **Speichern**.
5. Starten Sie den Prozess neu, um sicherzustellen, dass die Hooks richtig injiziert werden.

Die Zugriffseinstellungen des Schutzplans werden wieder auf diejenigen Prozesse angewendet, die Sie aus den Ausschlüssen entfernt haben.

So können Sie einen Prozess in den Ausschlüssen bearbeiten

1. Öffnen Sie den Schutzplan eines Geräts, um diesen zu bearbeiten:

   Klicken Sie neben dem Namen des Schutzplans auf das Drei-Punkte-Symbol (...) und wählen Sie anschließend den Befehl **Bearbeiten**.

   Hinweis
   Die Gerätekontrolle muss im Plan aktiviert worden sein, damit Sie auf die Einstellungen der Gerätekontrolle zugreifen können.

2. Klicken Sie zuerst neben dem **Gerätekontrolle**-Schalter auf das Pfeilsymbol, damit die Einstellungen erweitert werden, und dann auf die Zeile **Ausschlüsse**.
3. Klicken Sie auf der Seite **Ausschlüsse** auf das Symbol **Bearbeiten** neben dem Prozess, den Sie ändern wollen.
4. Übernehmen Sie die Änderungen und klicken Sie zu deren Bestätigung auf das Häkchen.
5. Klicken Sie auf **Fertig**.
6. Klicken Sie im Schutzplan auf **Speichern**.
7. Starten Sie die betroffenen Prozesse neu, um sicherzustellen, dass Ihre Änderungen korrekt übernommen werden.

Gerätekontrolle-Alarmmeldungen

Die Gerätekontrolle verwaltet ein Ereignisprotokoll, in dem die Versuche des Anwenders erfasst werden, auf kontrollierte Gerätetypen, Ports oder andere Schnittstellen zuzugreifen. Bestimmte Ereignisse können Alarmmeldungen auslösen, die dann in der Cyber Protect-Konsole protokolliert werden. Die Gerätekontrolle kann z.B. so konfiguriert werden, dass die Verwendung von Wechsellaufwerken verhindert wird und jeweils ein Alarmmeldungen protokolliert wird, wenn ein Anwender versucht, Daten zu oder von einem solchen Gerät zu kopieren.

Wenn Sie das Gerätekontrolle-Modul konfigurieren, können Sie für die meisten Elemente, die unter Gerätetyp (außer Screenshot-Aufnahmen) oder Ports aufgeführt sind, Alarmmeldungen aktivieren. Falls die Alarmmeldungen aktiviert sind, wird jedes Mal ein Benachrichtigung ausgelöst, wenn ein Benutzer versucht, eine nicht erlaubte Aktion durchzuführen. Wenn z.B. für Wechsellaufwerke die Zugriffsbeschränkung mit 'schreibgeschützt' festgelegt wurde und für diesen Gerätetyp zusätzlich die Option **Alarm anzeigen** aktiviert wurde, wird jedes Mal eine Alarmmeldung generiert, wenn ein Anwender auf dem entsprechend geschützten Computer versucht, Daten zu einem Wechsellaufwerk zu kopieren.

Wenn Sie die Alarmmeldungen in der Cyber Protect-Konsole einsehen wollen, gehen Sie zu **Monitoring** –> **Alarmmeldungen**. Die Konsole stellt bei jeder Alarmmeldung der Gerätekontrolle folgende Informationen über das jeweilige Ereignis zur Verfügung:

- **Typ** – Warnung.
- **Status** – Zeigt die Information „Der Zugriff auf Peripheriegeräte ist blockiert“ an
- **Nachricht** – Zeigt die Information „Der Zugriff auf '<Gerätetyp oder Port>' auf '<Computername>' ist blockiert“ an. Beispiel: „Der Zugriff auf 'Wechsellaufwerk' auf 'Buchhaltungs-PC' ist blockiert“.

- **Datum und Zeit** – Das Datum und die Uhrzeit, als das Ereignis stattfand.
- **Gerät** – Der Name des Computers, auf dem das Ereignis stattgefunden hat.
- **Plan-Name** – Der Name des Schutzplans, der das Ereignis verursacht hat.
- **Quelle** – Der Gerätetyp oder Port, der an dem Ereignis beteiligt war. Beispiel: wenn ein Benutzer auf ein Wechsellaufwerk zugreifen wollte und dies verweigert wurde, steht in diesem Feld 'Wechsellaufwerk'.
- **Aktion** – Die Aktion, die das Ereignis verursacht hat. Beispiel: wenn ein Benutzer Daten auf ein Gerät kopieren wollte und dies verweigert wurde, steht in diesem Feld 'Schreiben'. Zu weiteren Informationen siehe 'Werte für das Feld 'Aktion''.
- **Name** – Der Name des Zielobjekts bei dem Ereignis (z.B. die Datei, die der Benutzer kopieren wollte, oder das Gerät, das der Benutzer verwenden wollte). Wenn das Zielobjekt nicht identifiziert werden kann, wird keine Information angezeigt.
- **Informationen** – Zusätzliche Informationen über das Zielgerät bei dem Ereignis (z.B. die Geräte-ID bei einem USB-Gerät). Wenn keine zusätzlichen Informationen über das Zielgerät verfügbar sind, wird nichts angezeigt.
- **Benutzer** – Der Name des Benutzers, der das Ereignis verursacht hat.
- **Prozess** – Der vollqualifizierte Pfad zu der ausführbaren Datei der Applikation, die das Ereignis verursacht hat. In einigen Fällen wird möglicherweise der Prozessname anstelle des Pfades angezeigt. Wenn keine Prozessinformationen verfügbar sind, wird nichts angezeigt.

Wenn ein Alarm auf ein USB-Gerät (inkl. Wechsellaufwerke und verschlüsselte Wechsellaufwerke) zutrifft, kann der Administrator das Gerät direkt aus der Alarmmeldung heraus in die Positivliste aufnehmen. Dadurch kann verhindert werden, dass das Gerätekontrolle-Modul den Zugriff auf dieses spezielle Gerät einschränkt. Wenn Sie auf **Dieses USB-Gerät erlauben** klicken, wird es in die 'Positivliste für USB-Geräte' aufgenommen, die zur Konfiguration der Gerätekontrolle gehört. Das USB-Geräte wird dabei außerdem auch noch für weitere Verwendungsmöglichkeiten in die USB-Geräte-Datenbank aufgenommen.

Siehe außerdem auch die die Schritte, um die Gerätekontrolle-Alarmmeldungen einzusehen.

Werte für das Feld 'Aktion'

Das Feld **Aktion** für die Alarmmeldungen kann folgende Werte enthalten:

- **Lesen** – Daten vom Gerät oder Port erhalten.
- **Schreiben** – Daten zum Gerät oder Port senden.
- **Formatieren** – Direkter Zugriff auf das Gerät (z.B. um ein Laufwerk zu formatieren oder überprüfen). Bei Ports gilt dies für die Geräte, die über diesen Port angeschlossen sind.
- **Auswerfen** – Das Gerät aus dem System entfernen oder ein Medium aus dem Gerät auswerfen. Bei Ports gilt dies für die Geräte, die über diesen Port angeschlossen sind.
- **Drucken** – Ein Dokument an den Drucker senden.
- **Audio kopieren** – Audiodaten über die lokale Zwischenablage kopieren/einfügen.

- **Datei kopieren** – Eine Datei über die lokale Zwischenablage kopieren/einfügen.
- **Bild kopieren** – Ein Bild über die lokale Zwischenablage kopieren/einfügen.
- **Text kopieren** – Text über die lokale Zwischenablage kopieren/einfügen.
- **Unbekannter Inhalt kopieren** – Andere, nicht erkannte Daten über die lokale Zwischenablage kopieren/einfügen.
- **RTF-Daten kopieren (Bild)** – Ein Bild per „Rich Text Format" über die lokale Zwischenablage kopieren/einfügen.
- **RTF-Daten kopieren (Datei)** – Eine Datei per „Rich Text Format" über die lokale Zwischenablage kopieren/einfügen.
- **RTF-Daten kopieren (Text, Bild)** – Text zusammen mit einem Bild per „Rich Text Format" über die lokale Zwischenablage kopieren/einfügen.
- **RTF-Daten kopieren (Text, Datei)** – Text zusammen mit einer Datei per „Rich Text Format" über die lokale Zwischenablage kopieren/einfügen.
- **RTF-Daten kopieren (Bild, Datei)** – Ein Bild zusammen mit einer Datei per „Rich Text Format" über die lokale Zwischenablage kopieren/einfügen.
- **RTF-Daten kopieren (Text, Bild, Datei)** – Text zusammen mit einem Bild und einer Datei per „Rich Text Format" über die lokale Zwischenablage kopieren/einfügen.
- **Löschen** – Daten vom Gerät löschen (z.B. von einem Wechsellaufwerk, einem Mobilgerät usw.).
- **Gerätezugriff** – Zugriff auf ein Gerät oder einen Port (z.B. auf ein Bluetooth-Gerät, einen USB-Port usw.).
- **Eingehendes Audio** – Audiodaten vom Client-Computer über die umgeleitete Zwischenablage zur gehosteten Sitzung kopieren/einfügen.
- **Eingehende Datei** – Eine Datei vom Client-Computer über die umgeleitete Zwischenablage zur gehosteten Sitzung kopieren/einfügen.
- **Eingehendes Bild** – Ein Bild vom Client-Computer über die umgeleitete Zwischenablage zur gehosteten Sitzung kopieren/einfügen.
- **Eingehender Text** – Text vom Client-Computer über die umgeleitete Zwischenablage zur gehosteten Sitzung kopieren/einfügen.
- **Eingehender unbekannter Inhalt** – Andere, nicht erkannte Daten vom Client-Computer über die umgeleitete Zwischenablage zur gehosteten Sitzung kopieren/einfügen.
- **Eingehende RTF-Daten (Bild)** – Ein Bild vom Client-Computer über die umgeleitete Zwischenablage per „Rich Text Format" zur gehosteten Sitzung kopieren/einfügen.
- **Eingehende RTF-Daten (Datei)** – Eine Datei vom Client-Computer über die umgeleitete Zwischenablage per „Rich Text Format" zur gehosteten Sitzung kopieren/einfügen.
- **Eingehende RTF-Daten (Text, Bild)** – Text zusammen mit einem Bild vom Client-Computer über die umgeleitete Zwischenablage per „Rich Text Format" zur gehosteten Sitzung kopieren/einfügen.
- **Eingehende RTF-Daten (Text, Datei)** – Text zusammen mit einer Datei vom Client-Computer über die umgeleitete Zwischenablage per „Rich Text Format" zur gehosteten Sitzung kopieren/einfügen.

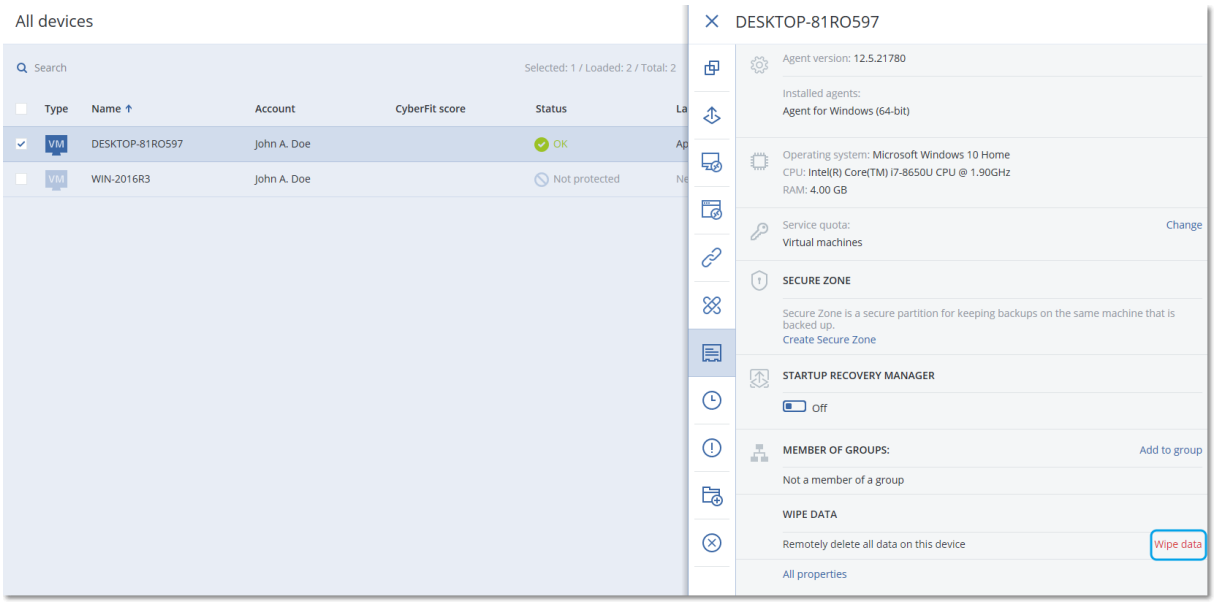
- **Eingehende RTF-Daten (Bild, Datei)** – Ein Bild zusammen mit einer Datei vom Client-Computer über die umgeleitete Zwischenablage per „Rich Text Format“ zur gehosteten Sitzung kopieren/einfügen.
- **Eingehende RTF-Daten (Text, Bild, Datei)** – Text zusammen mit einem Bild und einer Datei vom Client-Computer über die umgeleitete Zwischenablage per „Rich Text Format“ zur gehosteten Sitzung kopieren/einfügen.
- **Einlegen** – Ein USB- oder FireWire-Gerät anschließen oder ein Medium in ein Wechsellaufwerk einlegen
- **Ausgehendes Audio** – Audiodaten von der gehosteten Sitzung über die umgeleitete Zwischenablage zum Client-Computer kopieren/einfügen.
- **Ausgehende Datei** – Eine Datei von der gehosteten Sitzung über die umgeleitete Zwischenablage zum Client-Computer kopieren/einfügen.
- **Ausgehendes Bild** – Ein Bild von der gehosteten Sitzung über die umgeleitete Zwischenablage zum Client-Computer kopieren/einfügen.
- **Ausgehender Text** – Text von der gehosteten Sitzung über die umgeleitete Zwischenablage zum Client-Computer kopieren/einfügen.
- **Ausgehender unbekannter Inhalt** – Andere, nicht erkannte Daten von der gehosteten Sitzung über die umgeleitete Zwischenablage zum Client-Computer kopieren/einfügen.
- **Ausgehende RTF-Daten (Bild)** – Ein Bild von der gehosteten Sitzung über die umgeleitete Zwischenablage per „Rich Text Format“ zum Client-Computer kopieren/einfügen.
- **Ausgehende RTF-Daten (Datei)** – Eine Datei von der gehosteten Sitzung über die umgeleitete Zwischenablage per „Rich Text Format“ zum Client-Computer kopieren/einfügen.
- **Ausgehende RTF-Daten (Text, Bild)** – Text zusammen mit einem Bild von der gehosteten Sitzung über die umgeleitete Zwischenablage per „Rich Text Format“ zum Client-Computer kopieren/einfügen.
- **Ausgehende RTF-Daten (Text, Datei)** – Text zusammen mit einer Datei von der gehosteten Sitzung über die umgeleitete Zwischenablage per „Rich Text Format“ zum Client-Computer kopieren/einfügen.
- **Ausgehende RTF-Daten (Bild, Datei)** – Ein Bild zusammen mit einer Datei von der gehosteten Sitzung über die umgeleitete Zwischenablage per „Rich Text Format“ zum Client-Computer kopieren/einfügen.
- **Ausgehende RTF-Daten (Text, Bild, Datei)** – Text zusammen mit einem Bild und einer Datei von der gehosteten Sitzung über die umgeleitete Zwischenablage per „Rich Text Format“ zum Client-Computer kopieren/einfügen.
- **Umbenennen** – Dateien auf einem Gerät umbenennen (z.B. auf Wechsellaufwerken, Mobilgeräten und anderen).

Daten von einem verwalteten Workload löschen

Hinweis
Die Funktion zur Remote-Löschung ist über das Advanced Security-Paket verfügbar.

Über die Remote-Löschung kann ein Cyber Protection Service-Administrator oder der Besitzer einer Maschine die Daten auf einer verwalteten Maschine löschen – beispielsweise, weil diese gestohlen oder anderweitig verloren ging. Auf diese Weise wird verhindert, dass Unbefugte Zugriff auf sensible Informationen erhalten.

Die Funktion zur Remote-Löschung ist nur für Maschinen verfügbar, die unter Windows (Version 10 und höher) laufen. Damit die Maschine den Löschbefehl erhalten kann, muss Sie eingeschaltet und mit dem Internet verbunden sein.



So können Sie die Daten einer Maschine löschen

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte** –> **Alle Geräte**.
2. Wählen Sie die Maschine aus, deren Daten Sie vollständig löschen wollen.

   Hinweis
   Sie können nur jeweils die Daten einer Maschine gleichzeitig löschen.

3. Klicken Sie auf **Details** und dann auf den Befehl **Daten löschen**.
   Die Option **Daten löschen** ist nicht verfügbar, wenn die von Ihnen ausgewählte Maschine offline ist.
4. Bestätigen Sie Ihre Wahl.
5. Geben Sie die Anmeldedaten des lokalen Administrators dieser Maschine ein und klicken Sie dann auf den Befehl **Daten löschen**.

   Hinweis
   Über **Monitoring** –> **Aktivitäten** können Sie Details zum Löschvorgang und wer diesen gestartet einsehen.

Workloads anzeigen, die von RMM-Integrationen verwaltet werden

Hinweis
Diese Funktion ist nur verfügbar, wenn der Advanced Automation Service aktiviert ist.

Wenn Sie eine RMM-Plattform als Teil des Advanced Automation Service integrieren, können Sie Informationen von Geräten anzeigen und überwachen, die von der RMM-Plattform verwaltet werden. Diese Informationen können Sie in der Cyber Protect-Konsole einsehen, wenn Sie zu **Geräte** gehen.

So können Sie Workloads anzeigen, die von RMM-Integrationen verwaltet werden

1. Gehen Sie zu **Geräte –> Alle Geräte**.
2. (Optional) Sie können die Spalte **RMM-Integration** sortieren lassen, um relevante Integrationen zu finden.
3. Wählen Sie den gewünschten Workload aus.
4. Wählen Sie im Fensterbereich **Aktionen** die Option **Details** aus.
5. In dem angezeigten Fensterbereich wird, je nach Ihrem konfigurierten Workload, eine von drei Optionen angezeigt:
   - Wenn die Acronis Services für den Workload ohne RMM-Integration definiert sind: Wenn der Workload so konfiguriert wurde, dass er nur mit den Acronis Services arbeitet, werden keine Informationen zur RMM-Integration angezeigt.
   - Wenn für den Workload sowohl Acronis Services als auch eine RMM-Integration konfiguriert sind: Die Details zu den Acronis Services und der RMM-Integration befinden sich auf zwei Registerkarten, nämlich **Überblick** und **RMM-Integration** Klicken Sie auf **RMM-Integration**, um die Integrationsdetails einzusehen. Dazu gehören beispielsweise der Name und Typ des Workloads (von der RMM-Plattform bereitgestellt), die Beschreibung und der Speicherort. Außerdem werden hier auch alle installierten und aktivierten Add-ons für den RMM Agenten angezeigt.
   - Wenn der Workload nur mit einer RMM-Integration konfiguriert ist: Die Details zur RMM-Integration werden angezeigt. Dazu gehören beispielsweise der Name und Typ des Workloads (von der RMM-Plattform bereitgestellt), die Beschreibung und der Speicherort. Außerdem werden hier auch alle installierten und aktivierten Add-ons für den RMM Agenten angezeigt.

   Beachten Sie: Wenn der Workload mit RMM-Integration konfiguriert ist (entweder in Verbindung mit Acronis Services oder nur mit einer RMM-Integration), können Sie Folgendes tun:
   - Eine Remote-Verbindung initiieren (für Datto RMM-, N-able N-central- und N-able RMM-Integrationen verfügbar)
   - Die installierten Add-ons auf dem RMM-Gerät eines Drittanbieters überprüfen (nur für N-able RMM verfügbar)

- Direkt auf die Details des RMM-Geräts eines Drittanbieters zugreifen (für Datto RMM, N-able N-central, NinjaOne verfügbar)

CyberApp-Workloads

CyberApp-Workloads werden von ISVs (Independent Software Vendors) erstellt und erscheinen in der Cyber Protect-Konsole, nachdem Sie eine CyberApp-Integration aktiviert haben. Die folgenden Bedingungen müssen erfüllt sein:

- Der Erweiterungspunkt **Workloads und Aktionen** muss in der CyberApp aktiviert sein.
- In der CyberApp muss mindestens ein **Workload-Typ** definiert sein.
- Der vom ISV gehostete Connector Service muss gewährleisten, dass die CyberApp-Workloads der Acronis Plattform hinzugefügt und dort aktualisiert werden.

Weitere Informationen über das Vendor Portal und das Erstellen von CyberApps finden Sie in der Benutzeranleitung für das Vendor Portal.

Aggregierte Workloads

Auf einem physischen Workload können der Cyber Protect Agent sowie ein oder mehrere CyberApp-Agenten gleichzeitig installiert sein. In diesem Fall wird ein und derselbe Workload auf der Anzeige **Alle Geräte** mehr als einmal angezeigt – es wird jeweils ein separater Eintrag für den Workload von Acronis und für jeden CyberApp-Workload angezeigt. Wenn die automatische Zusammenführung von Workloads aktiviert und über das Vendor Portal oder die Cyber Protect-Konsole konfiguriert wurde, wird das System die Host- und MAC-Adressen der Workloads von Acronis und der CyberApp-Workloads vergleichen und alle Repräsentationen zu einem einzigen aggregierten Workload zusammenführen. Sie können Workloads auch manuell in der Cyber Protect-Konsole zusammenführen und die Zusammenführung wieder aufheben.

Mit aggregierten CyberApp-Workloads arbeiten

Neben den in der Cyber Protect-Konsole integrierten Standardaktionen können Sie außerdem folgende Aktionen durchführen, die verfügbar werden, sobald die CyberApp-Workloads in der Konsole angezeigt werden: Workloads manuell zu einem aggregierten Workload zusammenführen und benutzerdefinierte Aktionen durchführen, die in der CyberApp konfiguriert wurden.

Zusammenführen

Voraussetzungen

- Für den Mandanten sind Workloads aus verschiedenen Quellen verfügbar.

Sie können einen Workload von Acronis manuell mit einem oder mehreren CyberApp-Workloads zu einem einzelnen aggregierten Workload zusammenführen.

So können Sie Workloads manuell zu einem aggregierten Workload zusammenführen

1. Wählen Sie auf der Anzeige **Alle Geräte** diejenigen Workloads aus, die Sie zusammenführen wollen.

   Hinweis
   Die Aktion 'Zusammenführen' wird angezeigt, wenn Sie Workloads von verschiedenen Quellen auswählen – wie etwa einen Acronis-Workload und einen CyberApp-Workload.

2. Klicken Sie auf **Workloads zusammenführen**.

Benutzerdefinierte Aktionen durchführen

Voraussetzungen

- Für den Mandanten wurde eine CyberApp-Integration aktiviert, für die **Workload-Aktionen** definiert sind.

Benutzerdefinierte Aktionen sind Aktionen, die in der CyberApp konfiguriert werden und dann für den entsprechenden CyberApp-Workload verfügbar sind, wenn Sie die CyberApp-Integration für den entsprechenden Mandanten aktivieren.

So können Sie benutzerdefinierte Aktionen durchführen

1. Klicken Sie in der Anzeige **Alle Geräte** auf den Workload.
2. Klicken Sie auf **Integrierte App-Aktionen**.
3. Klicken Sie auf die Aktion.

Mit aggregierten Workloads arbeiten

Neben den Standardaktionen, die in der Cyber Protect-Konsole integriert sind, können Sie noch folgende Aktionen mit aggregierten Workloads durchführen: Details anzeigen, die Zusammenführung von Quell-Workloads wieder aufheben und benutzerdefinierte Aktionen durchführen, die in den CyberApps konfiguriert wurden.

Details anzeigen

Voraussetzungen

- Es ist mindestens ein aggregierter Workload für den Mandanten verfügbar.

So können Sie die Details eines aggregierten Workloads einsehen

1. Klicken Sie in der Anzeige **Alle Geräte** auf den aggregierten Workload.
2. Klicken Sie auf **Details**.
   Die Details des aggregierten Workloads sind auf Registerkarten aufgeteilt. Auf jeder Registerkarte werden die Details für jede Workload-Repräsentation angezeigt.

Zusammenführung aufheben

Voraussetzungen

- Es ist mindestens ein aggregierter Workload für den Mandanten verfügbar.

Wenn Sie die Zusammenführung eines aggregierten Workloads wieder aufheben, wird dieser nicht mehr in der Geräteliste angezeigt. Stattdessen wird für jeden Quell-Workload, der im aggregierten Workload zusammengeführt wurde, ein separater Eintrag angezeigt.

So können Sie die Zusammenführung eines aggregierten Workloads wieder aufheben

1. Klicken Sie in der Anzeige **Alle Geräte** auf den aggregierten Workload, dessen Zusammenführung Sie aufheben wollen.
2. Klicken Sie auf **Zusammenführung der Quell-Workloads aufheben**.
3. Klicken Sie im Bestätigungsfenster auf **Zusammenführung aufheben**.

Benutzerdefinierte Aktionen durchführen

Voraussetzungen

- Für den Mandanten wurde mindestens eine CyberApp-Integration aktiviert, für die **Workload-Aktionen** definiert sind.

Benutzerdefinierte Aktionen sind Aktionen, die in den CyberApps konfiguriert werden und dann für den entsprechenden CyberApp-Workload verfügbar sind, wenn Sie die CyberApp-Integration für den entsprechenden Mandanten aktivieren.

So können Sie benutzerdefinierte Aktionen durchführen

1. Klicken Sie in der Anzeige **Alle Geräte** auf den Workload.
2. Klicken Sie auf **Integrierte App-Aktionen**.
3. Gehen Sie, abhängig vom verfügbaren benutzerdefinierten Aktionen, folgendermaßen vor:
   - Wenn der aggregierte Workload einen einzelnen CyberApp-Workload enthält, klicken Sie auf die entsprechende Aktion.
   - Wenn der aggregierte Workload mehrere CyberApp-Workload enthält, klicken Sie auf den Namen der CyberApp und dann auf die entsprechende Aktion.

Workloads mit bestimmten Benutzern verknüpfen

Hinweis
Diese Funktion ist nur verfügbar, wenn der Advanced Automation Service aktiviert ist.

Indem Sie einen Workload mit einem bestimmten Benutzer verknüpfen, können Sie den Workload automatisch mit neuen Service Desk-Tickets verknüpfen, die von diesem Benutzer erstellt oder ihm zugewiesen wurden.

So können Sie einen Workload mit einem Benutzer verknüpfen

1. Gehen Sie zu **Geräte –> Alle Geräte** und wählen Sie dann den gewünschten Workload.
2. Wählen Sie im Fensterbereich **Aktionen** den Befehl **Mit einem Benutzer verknüpfen**.
3. Wählen Sie den gewünschten Benutzer aus.
   Bei Bedarf können Sie auch für bereits verknüpfte Workloads den ausgewählten Benutzer ändern.
4. Klicken Sie auf **Fertig**. Der ausgewählte Benutzer wird nun in der Spalte **Verknüpfter Benutzer** angezeigt.

So können Sie die Verknüpfung eines Workloads mit einem Benutzer wieder aufheben

1. Gehen Sie zu **Geräte –> Alle Geräte** und wählen Sie dann den gewünschten Workload.
2. Wählen Sie im Fensterbereich **Aktionen** den Befehl **Mit einem Benutzer verknüpfen**.
3. Klicken Sie auf **Verknüpfung des Benutzers aufheben**.
4. Klicken Sie auf **Fertig**.

Den zuletzt angemeldeten Benutzer finden

Damit die Administratoren Geräte verwalten können, müssen sie auch ermitteln können, welcher Benutzer an einem Gerät angemeldet ist und war. Diese Informationen werden im Dashboard oder in den Workload-Details angezeigt.

Sie können festlegen, ob die letzten Anmeldeinformationen in den Remote-Verwaltungsplänen angezeigt werden sollen oder nicht.

Im Dashboard:

1. Klicken Sie auf **Geräte**. Das Fenster **Alle Geräte** wird angezeigt.
2. In der Spalte **Letzte Anmeldung** wird für jedes Gerät anzeigt, welcher Benutzer sich das letzte Mal angemeldet hat.
3. In der Spalte **Letzte Anmeldezeit** wird für jedes Gerät angezeigt, wann sich der Benutzer das letzte Mal angemeldet hat.

In den Geräte-Details:

1. Klicken Sie auf **Geräte**. Das Fenster **Alle Geräte** wird angezeigt.
2. Klicken Sie auf das Gerät, dessen Details Sie überprüfen wollen.
3. Klicken Sie auf Symbol **Details**. Im Bereich **Zuletzt angemeldete Benutzer** werden für das ausgewählte Gerät jeweils der Name des Benutzers sowie das Datum und die Uhrzeit der letzten Anmeldungen angezeigt.

Hinweis
Im Bereich **Zuletzt angemeldete Benutzer**werden bis zu 5 verschiedene Benutzer angezeigt, die sich am Gerät angemeldet haben.

So können Sie die Spalten Letzte Anmeldung und Letzte Anmeldezeit im Dashboard ein- oder ausblenden

1. Klicken Sie auf **Geräte**. Das Fenster **Alle Geräte** wird angezeigt.
2. Klicken Sie in der rechten oberen Ecke auf das Zahnradsymbol und führen Sie im Bereich **Allgemeine** einen der folgenden Schritte aus:
   - Aktivieren Sie die Spalten **Letzte Anmeldung** und **Letzte Anmeldezeit**, wenn Sie wollen, dass diese im Dashboard angezeigt werden.
   - Deaktivieren Sie die Spalten **Letzte Anmeldung** und **Letzte Anmeldezeit**, wenn Sie wollen, dass diese im Dashboard ausgeblendet werden.

Die Backups und Wiederherstellungen von Workloads und Dateien verwalten

Mit dem Backup-Modul können Sie physische und virtuelle Maschinen, Dateien und Datenbanken per Backup sichern und wiederherstellen – und dabei sowohl lokale Storages wie auch einen Cloud Storage als Backup-Ziel verwenden.

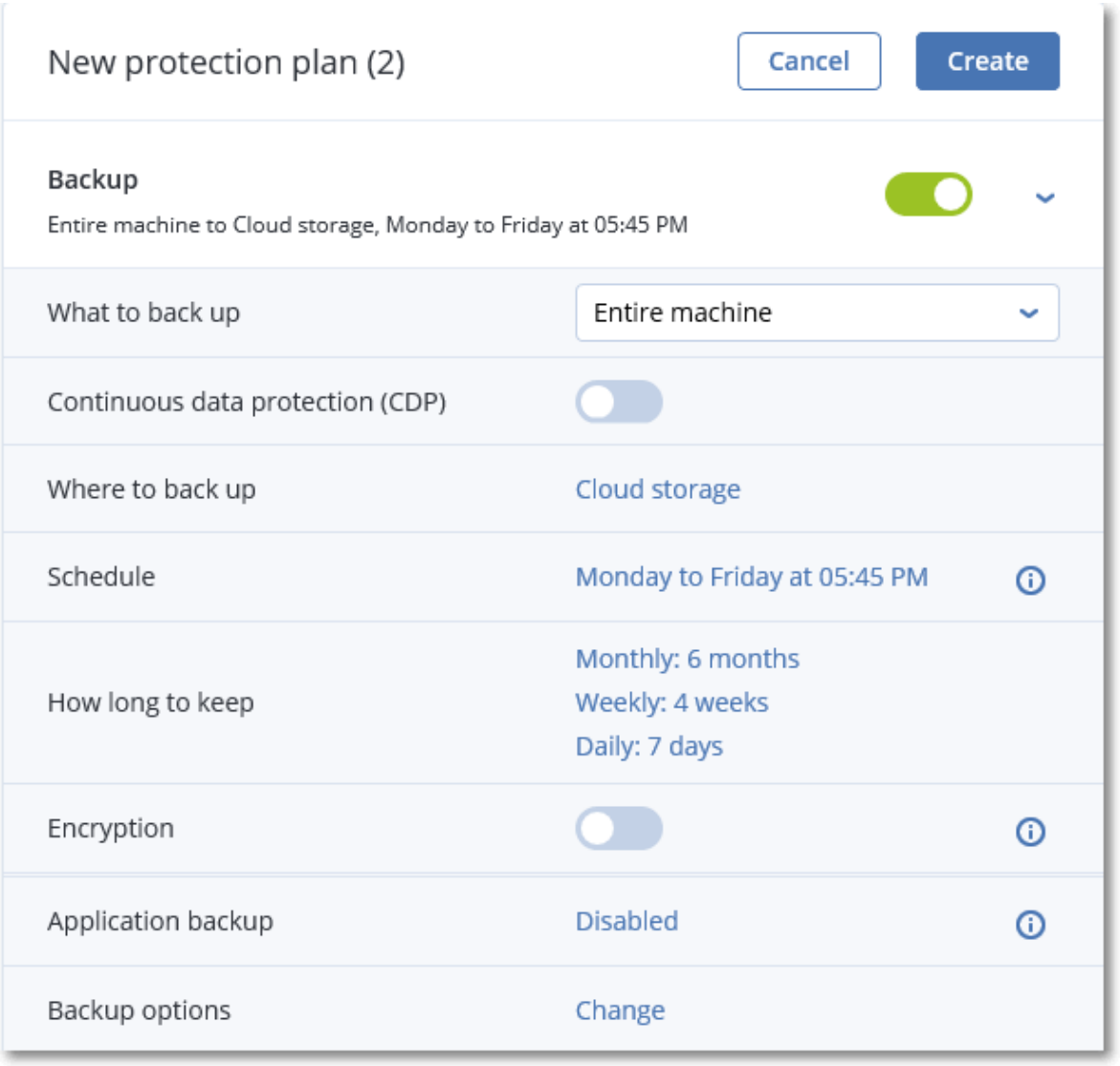
Backup

Ein Schutzplan mit einem aktivierten Backup-Modul ist ein Satz von Regeln, die spezifizieren, wie bestimmte Daten auf einer bestimmten Maschine gesichert werden sollen.

Ein Schutzplan kann zum Zeitpunkt seiner Erstellung (oder später) auf mehrere Maschinen angewendet werden.

So können Sie den ersten Schutzplan mit aktiviertem Backup-Modul erstellen

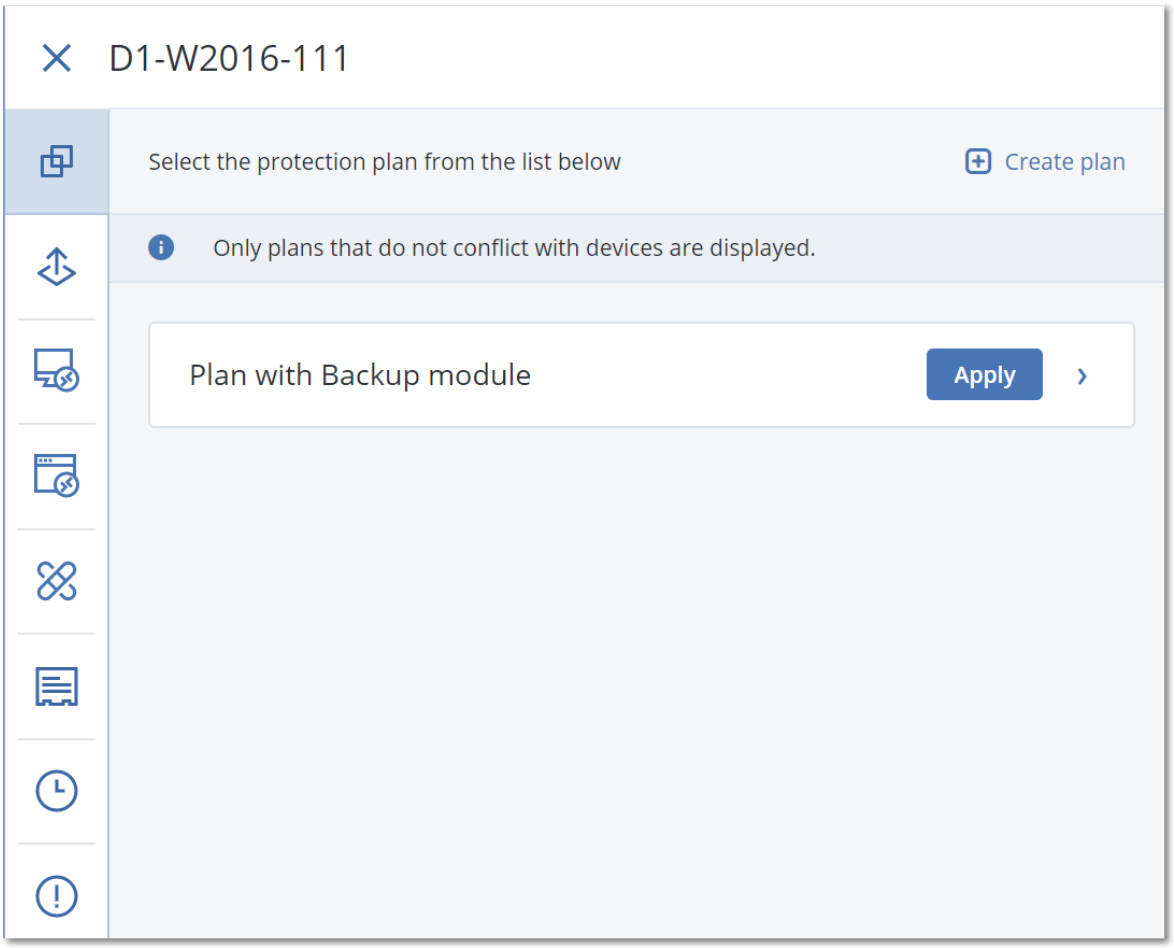
1. Wählen Sie Maschinen, die Sie per Backup sichern wollen.
2. Klicken Sie auf den Befehl **Schützen**.
   Es werden die Schutzpläne angezeigt, die auf die Maschine angewendet wurden. Wenn der Maschine noch keine Pläne zugewiesen wurden, wird Ihnen der Standard-Schutzplan angezeigt, der angewendet werden kann. Sie können die Einstellungen nach Bedarf anpassen und den Plan dann anwenden – oder auch einen neuen erstellen.
3. Klicken Sie auf **Plan erstellen**, wenn Sie einen neuen Plan erstellen wollen. Aktivieren Sie das **Backup**-Modul und rollen Sie die Einstellungen aus.



4. [Optional] Wenn Sie den Namen des Schutzplans ändern wollen, klicken Sie auf den vorgegebenen Standardnamen.
5. [Optional] Wenn Sie Parameter des Backup-Moduls ändern wollen, klicken Sie im Fensterbereich des Schutzplans auf die gewünschte Einstellung.
6. [Optional] Wenn Sie die Backup-Optionen ändern wollen, klicken Sie neben den **Backup-Optionen** auf **Ändern**.
7. Klicken Sie auf **Erstellen**.

So können Sie einen vorhandenen Schutzplan anwenden

1. Wählen Sie Maschinen, die Sie per Backup sichern wollen.
2. Klicken Sie auf den Befehl **Schützen**. Sollte auf die ausgewählten Maschinen bereits ein allgemeiner Schutzplan angewendet worden sein, dann klicken Sie auf **Plan hinzufügen**.
   Die Software zeigt die bisher erstellten Schutzpläne an.



3. Wählen Sie einen Schutzplan aus, der angewendet werden soll.
4. Klicken Sie auf **Anwenden**.

Schutzplan-Spickzettel

Die nachfolgende Tabelle fasst alle verfügbaren Schutzplan-Parameter zusammen. Verwenden Sie diese Tabelle, um einen Schutzplan zu erstellen, der am besten zu Ihren Bedürfnissen passt.

BACKUP-QUELLE	**Elemente für das Backup** **Auswahlmethoden**	**Backup-Ziel**	**Planung** **Backup-Schemata**	**Aufbewahrungsdauer**
Laufwerke/Volumes (physische Maschinen[1])	Direkte Auswahl Richtlinienregeln Dateifilter	Cloud Lokaler Ordner Netzwerkordner	Nur inkrementell (Einzeldatei) Nur vollständig	Nach Backup-Alter (einzelne Regel/per Backup-Set) Nach Backup-Anzahl

[1]Eine Maschine, die von einem Agenten gesichert wird, der im Betriebssystem installiert ist.

		NFS* Secure Zone**	Wöchentlich vollständig, täglich inkrementell Monatlich vollständig, wöchentlich differentiell, täglich inkrementell (GFS) Benutzerdefiniert (V-D-I)	Nach der Gesamtgröße der Backups*** Unbegrenzt aufbewahren
Laufwerke/Volumes (virtuelle Maschinen[1])	Richtlinienregeln Dateifilter	Cloud Lokaler Ordner Netzwerkordner NFS*		
Dateien (nur physische Maschinen[2])	Direkte Auswahl Richtlinienregeln Dateifilter	Cloud Lokaler Ordner Netzwerkordner NFS* Secure Zone**	Nur inkrementell (Einzeldatei) Nur vollständig Wöchentlich vollständig, täglich inkrementell Monatlich vollständig, wöchentlich differentiell, täglich inkrementell (GFS) Benutzerdefiniert (V-D-I)	
ESXi-Konfiguration	Direkte Auswahl	Lokaler Ordner Netzwerkordner NFS*		
Websites (Dateien und MySQL-Datenbanken)	Direkte Auswahl	Cloud	—	

[1]Eine virtuelle Maschine, die auf Hypervisor-Ebene von einem externen Agenten (wie dem Agenten für VMware oder dem Agenten für Hyper-V) gesichert wird. Eine virtuelle Maschine, in der ein Agent installiert ist, wird aus Backup-Sicht wie eine physische Maschine behandelt.
[2]Eine Maschine, die von einem Agenten gesichert wird, der im Betriebssystem installiert ist.

<table>
<tr><td colspan="2">Systemzustand</td><td rowspan="3">Direkte Auswahl</td><td rowspan="2">Cloud
Lokaler Ordner
Netzwerkordner</td><td rowspan="2">Nur vollständig
Wöchentlich vollständig, täglich inkrementell
Benutzerdefiniert (V-I)</td><td rowspan="6"></td></tr>
<tr><td colspan="2">SQL-Datenbanken</td></tr>
<tr><td colspan="2">Exchange-Datenbanken</td></tr>
<tr><td rowspan="7">Microsoft 365</td><td>Postfächer
(lokaler Agent für Microsoft 365)</td><td>Direkte Auswahl</td><td>Cloud
Lokaler Ordner
Netzwerkordner</td><td>Nur inkrementell (Einzeldatei)
Nur inkrementell (Einzeldatei) – nur für SQL-Datenbanken</td></tr>
<tr><td>Postfächer
(Cloud Agent für Microsoft 365)</td><td rowspan="3">Direkte Auswahl</td><td rowspan="4">Cloud</td><td rowspan="3">Bis zu 6 Backups pro Tag</td></tr>
<tr><td>Öffentliche Ordner</td></tr>
<tr><td>Teams</td></tr>
<tr><td>OneDrive-Dateien</td><td rowspan="2">Direkte Auswahl
Richtlinienregeln</td></tr>
<tr><td>SharePoint Online-Daten</td></tr>
<tr><td rowspan="3">Google Workspace</td><td>Gmail-Postfächer</td><td>Direkte Auswahl</td><td rowspan="3">Cloud</td><td rowspan="3">Bis zu 6 Backups pro Tag</td></tr>
<tr><td>Google Drive-Dateien</td><td rowspan="2">Direkte Auswahl
Richtlinienregeln</td></tr>
<tr><td>Shared Drive-Dateien</td></tr>
</table>

* Backups zu NFS-Freigaben sind unter Windows nicht verfügbar.

** Eine Secure Zone kann nicht auf einem Mac erstellt werden.

*** Die Aufbewahrungsregel **Nach der Gesamtgröße der Backups** ist nicht zusammen mit dem Backup-Schema **Nur inkrementell (Einzeldatei)** verfügbar oder wenn Sie Backups in den Cloud Storage erstellen.

Daten für ein Backup auswählen

Eine komplette Maschine auswählen

Unter dem 'Backup einer kompletten Maschine' versteht man ein Backup, das alle festeingebauten Laufwerke (interne „Nicht-Wechsellaufwerke“) der betreffenden Maschine umfasst. Weitere Informationen über Laufwerk-Backups finden Sie im Abschnitt '"Laufwerke oder Volumes auswählen" (S. 440)'.

Einschränkungen

- Für verschlüsselte APFS-Volumes, die gesperrt sind, werden keine Backups auf Laufwerkebene unterstützt. Wenn ein Backup einer kompletten Maschine erstellt wird, werden solche Volumes übersprungen.
- Das OneDrive-Stammverzeichnis wird standardmäßig von Backup-Aktionen ausgeschlossen. Wenn Sie jedoch festlegen, dass bestimmte OneDrive-Dateien und -Ordner gesichert werden sollen, dann werden diese auch in das Backup aufgenommen. Dateien, die nicht auf dem Gerät vorhanden sind, werden im Backup-Satz ungültige Inhalte haben.

Laufwerke oder Volumes auswählen

Ein Backup auf Laufwerksebene (kurz 'Laufwerk-Backup') enthält eine Kopie der Daten eines Laufwerks/Volumes – und zwar in 'gepackter' Form. Aus einem Backup auf Laufwerksebene können Sie Laufwerke, Volumes, Ordner und Dateien wiederherstellen.

Sie können für jeden einzelnen Workload im Schutzplan die zu sichernden Laufwerke oder Volumes auswählen (direkte Auswahl) oder Richtlinienregeln für mehrere Workloads konfigurieren. Außerdem können Sie durch die Verwendung von Dateifiltern festlegen, dass nur bestimmte Dateien in ein Backup aufgenommen oder von einem Backup ausgeschlossen werden. Weitere Informationen finden Sie im Abschnitt '"Dateifilter (Ausschlüsse/Einschlüsse)" (S. 504)'.

So können Sie Laufwerke oder Volumes auswählen

Direkte Auswahl

Eine direkte Auswahl ist nur für physische Maschinen verfügbar.

1. Wählen Sie bei **Backup-Quelle** die Option **Laufwerke/Volumes**.
2. Klicken Sie auf **Elemente für das Backup**.
3. Wählen Sie bei **Elemente für das Backup auswählen** die Option **Direkt**.
4. Aktivieren Sie für jeden der im Schutzplan enthaltenen Workloads die entsprechenden Kontrollkästchen neben den zu sichernden Laufwerken/Volumes.
5. Klicken Sie auf **Fertig**.

Nach Richtlinienregeln

1. Wählen Sie bei **Backup-Quelle** die Option **Laufwerke/Volumes**.
2. Klicken Sie auf **Elemente für das Backup**.
3. Wählen Sie bei **Elemente für das Backup auswählen** die Option **Richtlinienregeln verwenden**.
4. Wählen Sie eine der vordefinierten Regeln aus oder geben Sie Ihre eigenen Regeln ein (oder kombinieren Sie beides).

   Weitere Informationen über die verfügbaren Richtlinienregeln finden Sie im Abschnitt '"Richtlinienregeln für Laufwerke und Volumes" (S. 443)'.

   Die Richtlinienregeln werden auf alle Workloads angewendet, die im Schutzplan enthalten sind.

   Wenn keine der spezifizierten Regeln auf einen Workload angewendet werden kann, wird das Backup dieses Workloads fehlschlagen.
5. Klicken Sie auf **Fertig**.

Einschränkungen

- Für verschlüsselte APFS-Volumes, die gesperrt sind, werden keine Backups auf Laufwerkebene unterstützt. Wenn ein Backup einer kompletten Maschine erstellt wird, werden solche Volumes übersprungen.
- Das OneDrive-Stammverzeichnis wird standardmäßig von Backup-Aktionen ausgeschlossen. Wenn Sie jedoch festlegen, dass bestimmte OneDrive-Dateien und -Ordner gesichert werden sollen, dann werden diese auch in das Backup aufgenommen. Dateien, die nicht auf dem Gerät vorhanden sind, werden im Backup-Satz ungültige Inhalte haben.
- Sie können Laufwerke sichern, die per iSCSI-Protokoll an eine physische Maschine angeschlossen sind. Es gelten jedoch Einschränkungen, wenn Sie den Agenten für VMware oder den Agenten für Hyper-V verwenden, um die per iSCSI angeschlossenen Laufwerke zu sichern. Weitere Informationen finden Sie im Abschnitt '"Beschränkungen" (S. 35)'.

Was wird im Backup eines Laufwerks oder Volumes gespeichert?

Ein Laufwerk- bzw. Volume-Backup speichert das **Dateisystem** des entsprechenden Laufwerks bzw. Volumes 'als Ganzes'. Dabei werden auch alle zum Booten des Betriebssystems erforderlichen Informationen eingeschlossen. Aus solchen Backups können Laufwerke oder Volumes komplett wiederhergestellt werden – aber auch einzelne Dateien oder Ordner.

Wenn die Backup-Option '**Sektor-für-Sektor (Raw-Modus)**' aktiviert ist, werden in einem Laufwerk-Backup alle Sektoren des Laufwerks gespeichert. Das Sektor-für-Sektor-Backup kann verwendet werden, um Laufwerke mit nicht erkannten oder nicht unterstützten Dateisystemen sowie anderen proprietären Datenformaten zu sichern.

Windows

Ein Volume-Backup speichert alle Dateien und Ordner des gewählten Volumes, unabhängig von ihren Attributen (inkl. versteckter oder System-Dateien), den Boot-Record, die FAT (File Allocation

Table) und – sofern vorhanden – auch das Stammverzeichnis (Root) und die Spur Null (Track Zero), inkl. Master Boot Record (MBR).

Ein Laufwerk-Backup speichert alle Volumes des betreffenden Laufwerks (inkl. versteckter Volumes wie Wartungs-Volumes von Herstellern) und die Spur Null (Track Zero) mit dem Master Boot Record (MBR).

Folgende Elemente sind *nicht* in einem Laufwerk- oder Volume-Backup enthalten (und genauso wenig in einem Backup auf Dateiebene):

- Die Auslagerungsdatei (pagefile.sys) und die Datei, die ein Abbild des Hauptspeichers ist, wenn der Computer in den Ruhezustand wechselt (hiberfil.sys). Nach einer Wiederherstellung werden die Dateien an passender Position mit einer Größe von Null erneut erzeugt.
- Wenn das Backup unter dem Betriebssystem durchgeführt wird (und nicht mit einem Boot-Medium oder durch Sicherung von virtuellen Maschinen auf Hypervisor-Ebene):
  - Windows Schattenspeicher (Shadow Storage). Der auf diesen verweisende Pfad wird über den Registry-Wert **VSS Default Provider** bestimmt, der im Registry-Schlüssel **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup** gefunden werden kann. Das bedeutet, dass bei Betriebssystemen ab Windows Vista keine Windows-Systemwiederherstellungspunkte gesichert werden.
  - Wenn die Backup-Option **VSS (Volume Shadow Copy Service)** aktiviert ist, werden alle Dateien und Ordner, die im Registry-Schlüssel **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToSnapshot** spezifiziert sind, nicht per Backup gesichert.

Linux

Ein Volume-Backup speichert alle Dateien und Verzeichnisse des gewählten Laufwerkes (unabhängig von ihren Attributen), einen Boot-Record und den Dateisystem-Super-Block.

Ein Laufwerk-Backup speichert alle Volumes des Laufwerks, inkl. der Spur Null (Track Zero) mit dem 'Master Boot Record' (MBR).

Mac

Ein Laufwerk oder Volume-Backup speichert alle Dateien und Verzeichnisse des ausgewählten Laufwerks oder Volumes – plus einer Beschreibung des Volume-Layouts.

Folgende Elemente werden dabei ausgeschlossen:

- System-Metadaten, wie etwa das Dateisystem-Journal und der Spotlight-Index.
- Der Papierkorb
- Time Machine-Backups

Laufwerke und Volumes auf einem Mac werden physisch auf Dateiebene gesichert. Bare Metal Recovery (Wiederherstellung auf fabrikneuer Hardware) von Laufwerk- und Volume-Backups ist möglich, aber der Backup-Modus 'Sektor-für-Sektor' ist nicht verfügbar.

Richtlinienregeln für Laufwerke und Volumes

Wenn Sie Laufwerke oder Volumes für ein Backup auswählen, können Sie je nach Betriebssystem des geschützten Workloads die nachfolgenden Richtlinien verwenden.

Windows

- `[All Volumes]` – wählt alle Volumes auf der Maschine aus.
- Ein Laufwerksbuchstabe (beispielsweise `C:\`) wählt das Volume mit eben diesem Laufwerksbuchstaben aus.
- `[Fixed Volumes (physical machines)]` – wählt bei einer physischen Maschine alle Volumes aus, die keine Wechselmedien sind. Fest eingebaute Volumes schließen auch solche Volumes ein, die auf SCSI-, ATAPI-, ATA-, SSA-, SAS- und SATA-Geräten sowie auf RAID-Arrays liegen.
- `[BOOT+SYSTEM]` – wählt die System- und Boot-Volumes aus. Dies ist die minimale Kombination, mit der Sie ein Betriebssystem wiederherstellen können.
- `[Disk 1]` – wählt das erste Laufwerk der Maschine aus, einschließlich aller Volumes auf diesem Laufwerk. Um ein anderes Laufwerk auszuwählen, müssen Sie nur die entsprechende Laufwerksnummer eingeben.

Linux

- `[All Volumes]` – wählt alle gemounteten Volumes auf der Maschine aus.
- `/dev/hda1` – wählt das erste Volume auf dem ersten IDE-Laufwerk aus.
- `/dev/sda1` – wählt das erste Volume auf dem ersten SCSI-Laufwerk aus.
- `/dev/md1` – wählt das erste Software-RAID-Laufwerk aus.
- Verwenden Sie zur Auswahl anderer Basis-Volumes den Parameter '`/dev/xdyN`', wobei:
  - 'x' dem Laufwerkstyp entspricht
  - 'y' der Laufwerksnummer entspricht ('a' für das erste Laufwerk, 'b' für das zweite usw.)
  - 'N' der Volume-Nummer entspricht.
- Wenn Sie ein logisches Volume auswählen wollen, müssen Sie dessen Pfad so spezifizieren, wie er nach dem Ausführen des Befehls `ls /dev/mapper` (unter dem root-Konto) angezeigt wird.
  Beispiel:

  ```
  [root@localhost ~]# ls /dev/mapper/
  control vg_1-lv1 vg_1-lv2
  ```

  Diese Ausgabe zeigt zwei logische Volumes an, `lv1` und `lv2`, die zur Volume-Gruppe `vg_1` gehören. Spezifizieren Sie Folgendes, um diese Volumes per Backup zu sichern:

  `/dev/mapper/vg_1-lv1`
  `/dev/mapper/vg-l-lv2`

macOS

- `[All Volumes]` – wählt alle gemounteten Volumes auf der Maschine aus.
- `[Disk 1]` – wählt das erste Laufwerk der Maschine aus, einschließlich aller Volumes auf diesem Laufwerk. Wenn Sie ein anderes Laufwerk auswählen wollen, müssen Sie die entsprechende Laufwerksnummer spezifizieren.

Dateien und Ordner auswählen

Verwenden Sie ein Backup auf Dateiebene, wenn Sie nur bestimmte Daten (wie etwa Dateien, die zu einem aktuellen Projekt gehören) schützen wollen. Datei-Backups sind kleiner als Laufwerk-Backups und belegen daher weniger Speicherplatz.

Wichtig
Sie können aus einem Datei-Backup kein Betriebssystem wiederherstellen.

Sie können für jeden einzelnen Workload im Schutzplan die zu sichernden Dateien und Ordner auswählen (direkte Auswahl) oder Richtlinienregeln für mehrere Workloads konfigurieren. Außerdem können Sie durch die Verwendung von Dateifiltern festlegen, dass nur bestimmte Dateien in ein Backup aufgenommen oder von einem Backup ausgeschlossen werden. Weitere Informationen finden Sie im Abschnitt '"Dateifilter (Ausschlüsse/Einschlüsse)" (S. 504)'.

So können Sie Dateien oder Ordner auswählen

Direkte Auswahl

1. Wählen Sie bei **Backup-Quelle** die Option **Dateien/Ordner**.
2. Klicken Sie unter **Elemente für das Backup** auf **Spezifizieren**.
3. Wählen Sie bei **Elemente für das Backup auswählen** die Option **Direkt**.
4. Spezifizieren Sie für jeden Workload im Schutzplan, welche Dateien oder Ordner gesichert werden sollen.
   a. Klicken Sie auf **Dateien und Ordner auswählen**.
   b. Klicken Sie auf **Lokaler Ordner** oder **Netzwerkordner**.
      Wenn Netzwerkordner verwendet werden, müssen diese von der ausgewählten Maschine aus zugänglich sein.
      Wenn Sie **Netzwerkordner** als Quelle auswählen, können Sie Daten von NAS-Geräten (Network Attached Storages), wie z.B. NetApp-Geräten, sichern. Es werden NAS-Geräte aller Hersteller unterstützt.
   c. Gehen Sie im Verzeichnisbaum zu den gewünschten Dateien oder Ordnern.
      Alternativ können Sie den jeweiligen Pfad zu den Dateien/Ordnern spezifizieren und dann auf die Pfeilschaltfläche klicken.
   d. [Bei freigegebenen Ordnern] Spezifizieren Sie bei Aufforderung die Anmeldedaten, um auf den freigegebenen Ordner zugreifen zu können.
      Ein Backup von Ordnern mit anonymem Zugriff wird nicht unterstützt.

e. Wählen Sie die gewünschten Dateien bzw. Ordner aus.

f. Klicken Sie auf **Fertig**.

Nach Richtlinienregeln

1. Wählen Sie bei **Backup-Quelle** die Option **Dateien/Ordner**.
2. Klicken Sie unter **Elemente für das Backup** auf **Spezifizieren**.
3. Wählen Sie bei **Elemente für das Backup auswählen** die Option **Richtlinienregeln verwenden**.
4. Wählen Sie eine der vordefinierten Regeln aus oder geben Sie Ihre eigenen Regeln ein (oder kombinieren Sie beides).

   Weitere Informationen über die verfügbaren Richtlinienregeln finden Sie im Abschnitt '"Richtlinienregeln für Dateien und Ordner" (S. 445)'.

   Die Richtlinienregeln werden auf alle Workloads angewendet, die im Schutzplan enthalten sind.

   Wenn keine der spezifizierten Regeln auf einen Workload angewendet werden kann, wird das Backup dieses Workloads fehlschlagen.
5. Klicken Sie auf **Fertig**.

Einschränkungen

- Sie können Dateien und Ordner auswählen, wenn Sie physische oder virtuelle Maschinen sichern, auf denen ein Agent installiert ist (agentenbasiertes Backup). Bei virtuellen Maschinen, die Sie im agentenlosen Modus sichern, ist kein Datei-Backup möglich. Weitere Informationen über die Unterschiede zwischen diesen Backup-Typen finden Sie im Abschnitt '"Agentenbasiertes und agentenloses Backup" (S. 69)'.
- Das OneDrive-Stammverzeichnis wird standardmäßig von Backup-Aktionen ausgeschlossen. Wenn Sie jedoch festlegen, dass bestimmte OneDrive-Dateien und -Ordner gesichert werden sollen, dann werden diese auch in das Backup aufgenommen. Dateien, die nicht auf dem Gerät vorhanden sind, werden im Backup-Satz ungültige Inhalte haben.
- Sie können Dateien und Ordner sichern, die sich auf Laufwerken befinden, die per iSCSI-Protokoll an eine physische Maschine angeschlossen sind. Es gelten jedoch bestimmte Einschränkungen, wenn Sie den Agenten für VMware oder den Agenten für Hyper-V verwenden, um Daten auf den per iSCSI angeschlossenen Laufwerke zu sichern.

Richtlinienregeln für Dateien und Ordner

Wenn Sie Dateien oder Ordner für ein Backup auswählen, können Sie je nach Betriebssystem des geschützten Workloads die nachfolgenden Richtlinien verwenden.

Windows

- Vollständiger Pfad für eine Datei oder einen Ordner. Beispielsweise: `D:\Work\Text.doc` oder `C:\Windows`.

- Vordefinierte Regeln:
  - `[All Files]` – wählt alle Dateien auf allen Volumes der betreffenden Maschine aus.
  - `[All Profiles Folder]` – wählt den Ordner aus, in dem sich alle Benutzerprofile befinden. Beispielsweise `C:\Benutzer` oder `C:\Dokumente und Einstellungen`.
- Umgebungsvariablen:
  - `%ALLUSERSPROFILE%` – wählt den Ordner aus, in dem sich die gemeinsamen Daten aller Benutzerprofile befinden. Beispielsweise `C:\ProgramData` oder `C:\Dokumente und Einstellungen\Alle Benutzer`.
  - `%PROGRAMFILES%` – wählt den Ordner `Programme` aus. Beispielsweise `C:\Programme`.
  - `%WINDIR%` – wählt den `Windows`-Ordner aus. Beispielsweise `C:\Windows`.

  Sie können auch andere Umgebungsvariablen oder eine Kombination von Umgebungsvariablen und Text verwenden. Spezifizieren Sie beispielsweise Folgendes, wenn Sie den Ordner 'Java' im Systemordner 'Programme' auswählen wollen: `%PROGRAMFILES%\Java`.

Linux

- Vollständiger Pfad für eine Datei oder ein Verzeichnis.
  Ein Beispiel: Wenn Sie die Datei `datei.txt` auf dem Volume `/dev/hda3` sichern wollen, welches wiederum unter `/home/usr/docs` gemountet ist, müssen Sie `/dev/hda3/datei.txt` oder `/home/usr/docs/datei.txt` spezifizieren.
- Vordefinierte Regeln:
  - `[All Profiles Folder]` – wählt `/home` aus. Standardmäßig werden alle Benutzerprofile in diesem Ordner gespeichert.
  - `/home` – wählt das Home-Verzeichnis der allgemeinen Benutzer aus.
  - `/root` – wählt das Home-Verzeichnis des Benutzers 'root' aus.
  - `/usr` – wählt das Verzeichnis für alle benutzerbezogenen Programme aus.
  - `/etc` – wählt das Verzeichnis der Systemkonfigurationsdateien aus.

macOS

- Vollständiger Pfad für eine Datei oder ein Verzeichnis.
  Beispiel:
  - Wenn Sie `datei.txt` auf dem Desktop eines Benutzers sichern wollen, müssen Sie `/Users/<Benutzername>/Desktop/datei.txt` spezifizieren.
  - Wenn Sie die Ordner `Desktop`, `Dokumente` und `Downloads` eines Benutzers sichern wollen, müssen Sie `/Users/<Benutzername>/Desktop`, `/Users/<Benutzername>/Documents` und `/Users/<Benutzername>/Downloads` spezifizieren.
  - Wenn Sie die Basis-Ordner aller Benutzer sichern wollen, die ein Konto auf dieser Maschine haben, spezifizieren Sie `/Users`.
  - Spezifizieren Sie `/Applications`, wenn Sie den Ordner sichern wollen, in dem die Anwendungen installiert sind.
- Vordefinierte Regeln

- `[All Profiles Folder]` – wählt `/Users` aus. Standardmäßig werden alle Benutzerprofile in diesem Ordner gespeichert.

Einen Systemzustand auswählen

Hinweis
Ein Backup des Systemzustands ist für Maschinen mit Windows 7 oder höher verfügbar, auf denen der Agent für Windows installiert ist. Ein Backup des Systemzustands ist nicht für virtuelle Maschinen verfügbar, die auf Hypervisor-Ebene gesichert werden (agentenloses Backup).

Um einen Systemzustand sichern zu können, müssen Sie bei **Backup-Quelle** die Option **Systemzustand** auswählen.

Ein Backup des Systemzustands setzt sich aus Dateien folgender Windows-Komponenten/-Funktionen zusammen:

- Konfigurationsinformationen für die Aufgabenplanung
- VSS-Metadatenspeicher
- Konfigurationsinformationen für die Leistungsindikatoren
- MSSearch-Dienst
- Intelligenter Hintergrundübertragungsdienst (BITS)
- Die Registry
- Windows-Verwaltungsinstrumentation (WMI)
- Registrierungsdatenbank der Komponentendienste-Klasse

Eine ESXi-Konfiguration auswählen

Mit dem Backup einer ESXi-Host-Konfiguration können Sie einen ESXi-Host auf fabrikneuer Hardware wiederherstellen (Bare Metal Recovery). Die Wiederherstellung wird von einem Boot-Medium aus durchgeführt.

Evtl. auf dem Host laufende virtuelle Maschinen werden nicht in das Backup eingeschlossen. Sie können diese jedoch separat per Backup sichern und wiederherstellen.

Das Backup einer ESXi-Host-Konfiguration beinhaltet:

- Den Boot-Loader und die Boot-Bank-Partition des Hosts.
- Den Host-Zustand (virtuelle Netzwerk- und Storage-Konfiguration, SSL-Schlüssel, Server-Netzwerkeinstellungen und Informationen zu den lokalen Benutzern).
- Auf dem Host installierte oder bereitgestellte Erweiterungen und Patches.
- Protokolldateien.

Voraussetzungen

- SSH muss im **Sicherheitsprofil** der ESXi-Host-Konfiguration aktiviert sein.
- Sie müssen das Kennwort des 'root'-Kontos auf dem ESXi-Host kennen.

Einschränkungen

- ESXi-Konfigurations-Backups werden nicht für Hosts unterstützt, die unter VMware vSphere 7.0 und höher laufen.
- Eine ESXi-Konfiguration kann nicht in den Cloud Storage (als Backup-Ziel) gesichert werden.

So können Sie eine ESXi-Konfiguration auswählen

1. Klicken Sie auf **Geräte** –> **Alle Geräte** und bestimmen Sie den ESXi-Host, den Sie per Backup sichern wollen.
2. Klicken Sie auf den Befehl **Schützen**.
3. Wählen Sie bei **Backup-Quelle** die Option **ESXi-Konfiguration**.
4. Spezifizieren Sie bei **'root'-Kennwort für ESXi** das Kennwort für das jeweilige 'root'-Konto auf jedem der ausgewählten ESXi-Hosts – oder verwenden Sie dasselbe Kennwort für alle Hosts.

Kontinuierliche Datensicherung (CDP)

Die kontinuierliche Datensicherung (CDP) ist Bestandteil des Advanced Backup-Pakets. Sie kann geschäftskritische Daten umgehend sichern, sobald diese geändert werden, damit keine Änderungen verloren gehen, wenn Ihr System einmal zwischen zwei geplanten Backups ausfallen sollte. Sie können die kontinuierliche Datensicherung für folgende Daten konfigurieren:

- Dateien oder Ordner an bestimmten Speicherorten
- Dateien, die von bestimmten Applikationen verändert wurden

Die kontinuierliche Datensicherung wird nur für das Dateisystem NTFS und folgende Betriebssysteme unterstützt:

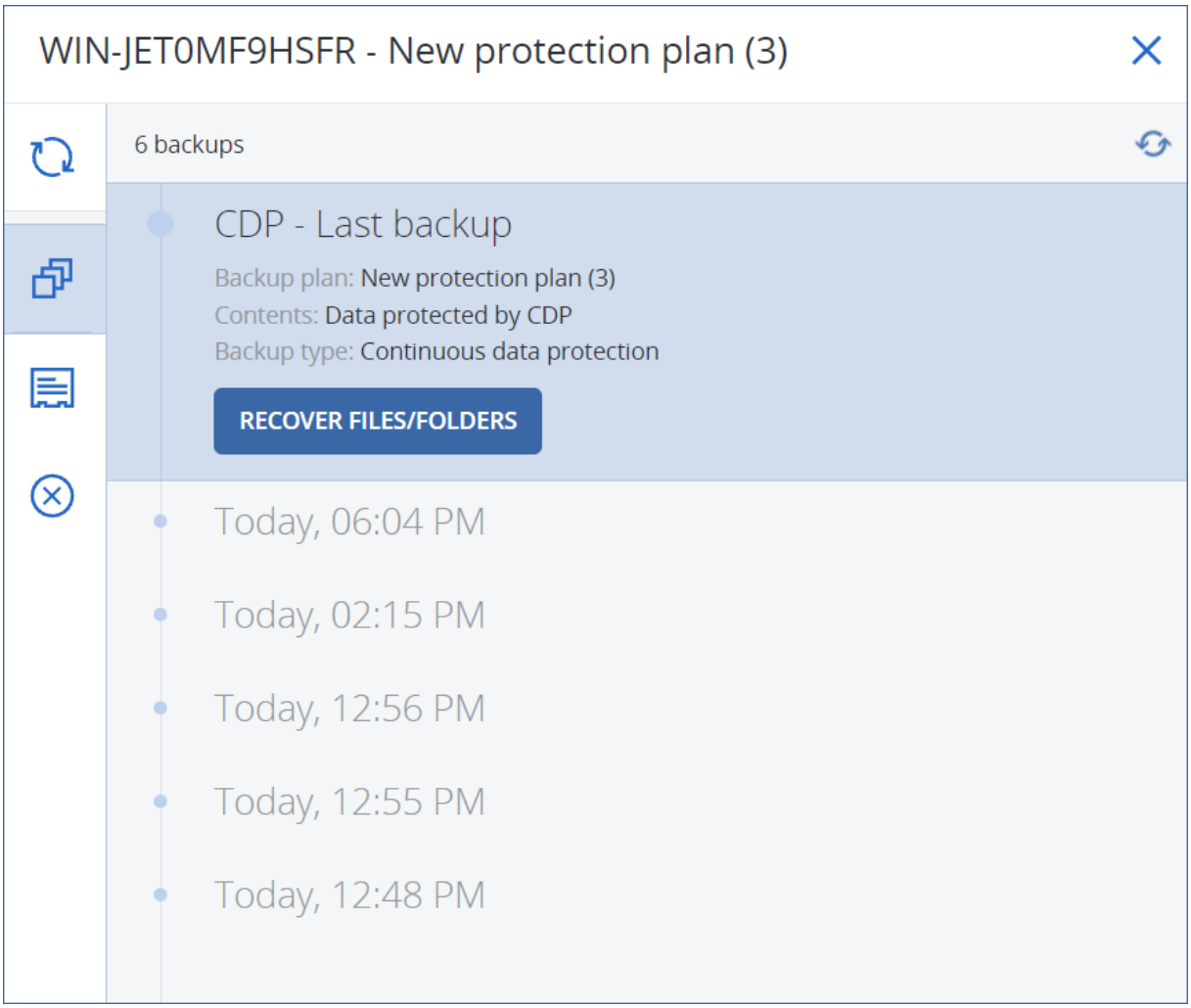
- Desktop: Windows 7 und höher
- Server: Windows Server 2008 R2 und höher

Es werden nur lokale Ordner unterstützt. Es können keine Netzwerkordner für eine kontinuierliche Datensicherung ausgewählt werden.

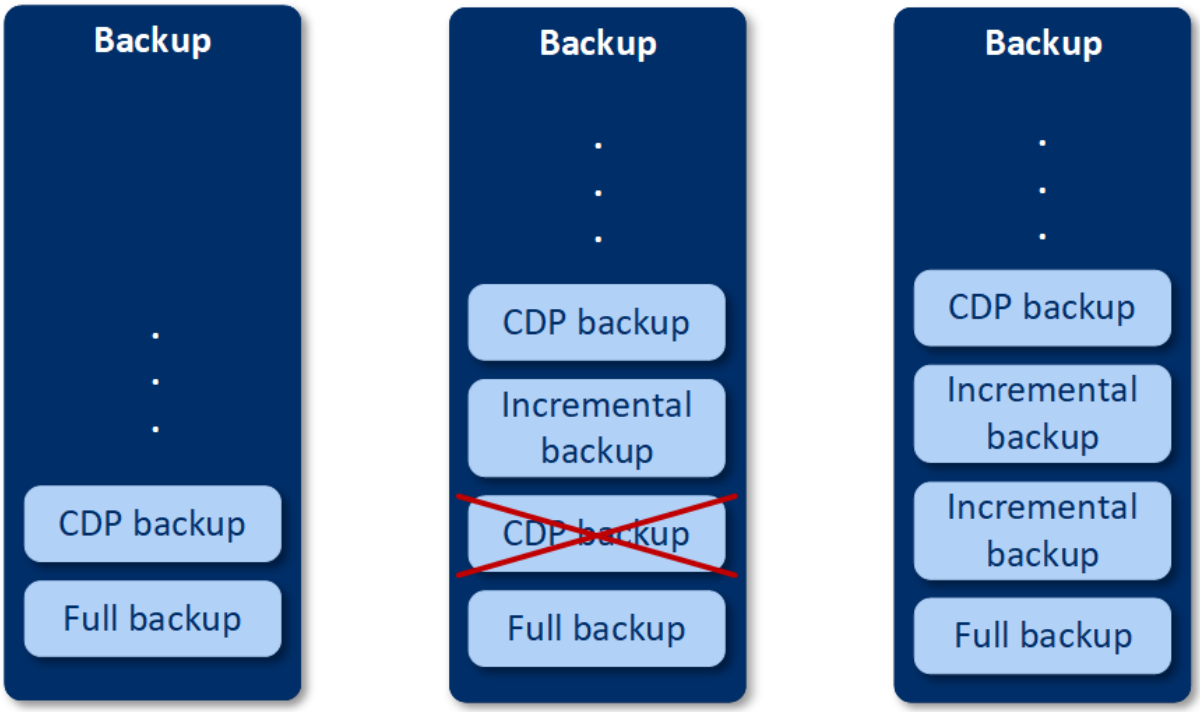
Die kontinuierliche Datensicherung (CDP) ist nicht mit der Option **Applikations-Backup** kompatibel.

Und so funktioniert es

Änderungen an Dateien und Ordnern, die von der kontinuierlichen Datensicherung (CDP) überwacht werden, werden umgehend in einem speziellen CDP-Backup gesichert. Es gibt immer nur ein CDP-Backup in einem Backup-Set – und es ist immer das letzte (neueste).



Wenn ein geplantes reguläres Backup gestartet wird, wird die kontinuierliche Datensicherung (CDP) angehalten, weil die neuesten Daten jetzt in dem geplanten Backup aufgenommen werden. Sobald das geplante Backup abgeschlossen wurde, wird die kontinuierliche Datensicherung wieder aufgenommen, das alte (vorherige) CDP-Backup gelöscht und ein neues CDP-Backup erstellt. Auf diese Weise bleibt das CDP-Backup immer die letzte Sicherung innerhalb des Backup-Sets und enthält immer den jeweils aktuellsten Stand der überwachten Dateien oder Ordner.



Wenn Ihre Maschine während eines regulären Backups abstürzt, wird die kontinuierliche Datensicherung nach dem Neustart der Maschine automatisch fortgesetzt und ein CDP-Backup zusätzlich zum letzten erfolgreichen geplanten Backup erstellt.

Für die kontinuierliche Datensicherung ist es erforderlich, dass vor dem CDP-Backup mindestens ein reguläres Backup erstellt wurde. Aus diesem Grund wird bei der ersten Ausführung eines Schutzplans, für den die kontinuierlicher Datensicherung aktiviert wurde, zuerst ein vollständiges Backup erstellt, dem direkt anschließend ein CDP-Backup hinzugefügt wird. Wenn Sie die Option **Kontinuierliche Datensicherung (CDP)** für einen bereits bestehenden Schutzplan aktivieren, wird das CDP-Backup zum schon vorhandenen Backup-Set hinzugefügt.

Hinweis
Die kontinuierliche Datensicherung (CDP) ist standardmäßig für alle Schutzpläne aktiviert, die Sie über die Registerkarte **Geräte** erstellen, wenn die Advanced Backup-Funktionalität für Sie aktiviert wurde und wenn Sie keine anderen Advanced Backup-Funktionen für die ausgewählten Maschinen verwenden. Wenn Sie bereits einen Plan mit kontinuierlicher Datensicherung (CDP) für eine ausgewählte Maschine haben, wird die kontinuierliche Datensicherung für diese Maschine bei neu erstellten Plänen nicht standardmäßig aktiviert.
Bei Plänen, die für Gerätegruppen erstellt werden, ist die kontinuierliche Datensicherung (CDP) nicht standardmäßig aktiviert.

Unterstützte Datenquellen

Sie können die kontinuierliche Datensicherung (CDP) für folgende Datenquellen konfigurieren:

- Komplette Maschine
- Laufwerke/Volumes
- Dateien/Ordner

Nachdem Sie im Bereich **Backup-Quelle** des Schutzplans die gewünschte Datenquelle ausgewählt haben, müssen Sie im Bereich **Elemente, die kontinuierlich geschützt werden sollen** diejenigen Dateien, Ordner oder Applikationen auswählen, die für die kontinuierliche Datensicherung (CDP) verwendet werden sollen. Weitere Informationen darüber, wie Sie die kontinuierliche Datensicherung (CDP) konfigurieren können, finden Sie im Abschnitt '"Ein CDP-Backup konfigurieren" (S. 451)'.

Unterstützte Zielorte

Sie können die kontinuierliche Datensicherung (CDP) mit folgenden Zielorten konfigurieren:

- Lokaler Ordner
- Netzwerkordner
- Cloud Storage
- Acronis Cyber Infrastructure
- Per Skript festgelegter Speicherort

Hinweis
Sie können per Skript nur die oben aufgeführten Speicherorte definieren.

Ein CDP-Backup konfigurieren

Sie können die kontinuierliche Datensicherung (CDP) im Modul **Backup** eines Schutzplans konfigurieren. Weitere Informationen darüber, wie Sie einen Schutzplan erstellen können, finden Sie im Abschnitt '"Einen Schutzplan erstellen" (S. 232)'.

So können Sie die Einstellungen für die kontinuierliche Datensicherung (CDP) konfigurieren

1. Aktivieren Sie im Modul **Backup** eines Schutzplans den Schalter für die **Kontinuierliche Datensicherung (CDP)**.
   Dieser Schalter ist nur bei folgenden Datenquellen verfügbar:
   - Komplette Maschine
   - Laufwerke/Volumes
   - Dateien/Ordner
2. Konfigurieren Sie bei **Elemente, die kontinuierlich geschützt werden sollen** die kontinuierliche Datensicherung für **Applikationen** oder **Dateien/Ordner** oder beides.
   - Klicken Sie auf **Applikationen**, um das CDP-Backup für Dateien zu konfigurieren, die von bestimmten Applikationen verändert werden.

Sie können Applikationen aus vordefinierten Kategorien auswählen oder weitere Applikationen hinzufügen, indem Sie den Pfad zu deren ausführbarer Datei spezifizieren. Beispielsweise:

- `C:\Program Files\Microsoft Office\Office16\WINWORD.EXE`
- `*:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE`

- Klicken Sie auf **Dateien/Ordner**, um das CDP-Backup für Dateien zu konfigurieren, die sich an bestimmten Speicherorten befinden.

  Sie können diese Speicherorte mithilfe von Auswahlregeln definieren oder indem Sie die Dateien bzw. Ordner direkt (manuell) auswählen.

  - [Für alle Maschinen] Wenn Sie eine Auswahlregel erstellen wollen, verwenden Sie das Textfeld.

    Sie können die vollständigen Pfade zu den Dateien eingeben oder auch Platzhalterzeichen (* und ?) für die Pfadangaben verwenden. Der Asterisk (*) ersetzt null bis mehrere Zeichen. Das Fragezeichen entspricht genau einem einzelnen Zeichen.

    Wichtig
    Wenn Sie ein CDP-Backup für einen Ordner erstellen wollen, müssen Sie dessen Inhalt mit einem Asterisk (*) als Platzhalterzeichen spezifizieren:

    Richtige Pfadangabe: `D:\Daten\*`

    Falsche Pfadangabe: `D:\Daten\`

  - [Für Online-Maschinen] So können Sie Dateien und Ordner direkt auswählen:
    - Wählen Sie bei **Von dieser Maschine aus durchsuchen** diejenige Maschine, auf der sich die Dateien oder Ordner befinden.
    - Klicken Sie auf **Dateien und Ordner auswählen**, um die ausgewählte Maschine zu durchsuchen.

      Ihre direkte Auswahl erstellt eine Auswahlregel. Wenn Sie den Schutzplan auf mehrere Maschinen anwenden und eine Auswahlregel auf einer Maschine nicht zutrifft, wird sie auf dieser Maschine übersprungen.

3. Klicken Sie im Fensterbereich des Schutzplans auf **Erstellen**.

Als Ergebnis werden die Daten, die Sie spezifiziert haben, zwischen den geplanten Backups kontinuierlich gesichert.

Ein Ziel auswählen

Klicken Sie auf **Backup-Ziel** und wählen Sie dann eine der folgenden Möglichkeiten:

- **Cloud Storage**

  Die Backups werden im Cloud-Datacenter gespeichert.
- **Lokale Ordner**

Wenn Sie nur eine einzelne Maschine ausgewählt haben, dann bestimmen Sie auf der ausgewählten Maschine über 'Durchsuchen' den gewünschten Ordner – oder geben Sie den Ordnerpfad manuell ein.

Wenn Sie mehrere Maschinen ausgewählt haben, geben Sie den Ordnerpfad manuell ein. Die Backups werden in genau diesem Ordner auf jeder der ausgewählten physischen Maschinen gespeichert – oder auf der Maschine, wo der Agent für virtuelle Maschinen installiert ist. Falls der Ordner nicht existiert, wird er automatisch erstellt.

- **Netzwerkordner**

  Dies ist ein Ordner, der per SMB/CIFS/DFS freigegeben ist.

  Bestimmen Sie (per 'Durchsuchen') den gewünschten Freigabe-Ordner oder geben Sie den Pfad im folgenden Format manuell ein:

  - Für SMB-/CIFS-Freigaben: `\\<Host-Name>\<Pfad>\` oder `smb://<Host-Name>/<Pfad>/`
  - Für DFS-Freigabe: `\\<vollständiger DNS-Domain-Name>\<DFS-Stammverzeichnis>\<Pfad>`

    Beispielsweise: `\\beispiel.firma.com\freigabe\dateien`

  Klicken Sie anschließend auf die Schaltfläche mit dem Pfeil. Spezifizieren Sie bei Aufforderung die Anmeldedaten (Benutzernamen, Kennwort), um auf den freigegebenen Ordner zugreifen zu können. Sie können diese Anmeldedaten jederzeit ändern, indem Sie neben dem Ordnernamen auf das Schlüsselsymbol klicken.

  Backups zu einem Ordner mit anonymem Zugriff werden nicht unterstützt.

- **Public Cloud**

  Diese Option ist als Bestandteil des Advanced Backup-Pakets verfügbar.

  Es ermöglicht Ihnen, ein direktes Backup zu einem kompatiblen Public Cloud Storage zu konfigurieren, ohne zusätzliche Komponenten (wie Microsoft Azure oder andere virtuelle Maschinen als Gateways) bereitstellen zu müssen. Wählen Sie bei Bedarf die entsprechende Public Cloud aus und stellen Sie eine Verbindung zu dieser her.

  Weitere Informationen finden Sie im Abschnitt '"Workloads zu Public Clouds sichern" (S. 591)'.

- **NFS-Ordner** (auf Maschinen verfügbar, die mit Linux oder macOS laufen)

  Überprüfen Sie, dass das nfs-utils-Paket auf dem Linux-Server installiert ist, auf dem der Agent für Linux installiert ist.

  Bestimmen Sie (per 'Durchsuchen') den gewünschten NFS-Ordner oder geben Sie den Pfad im folgenden Format manuell ein:

  `nfs://<Host-Name>/<exportierter Ordner>:/<Unterordner>`

  Klicken Sie anschließend auf die Schaltfläche mit dem Pfeil.

  Hinweis
  Ein NFS-Ordner, der per Kennwort geschützt ist, kann nicht als Backup-Ziel verwendet werden.

- **Secure Zone** (verfügbar, falls auf jeder der ausgewählten Maschinen eine verfügbar ist)

  Die 'Secure Zone' ist ein spezielles, geschütztes Volume (Partition), das auf einem Laufwerk der zu sichernden Maschine liegt. Dieses Volume bereits muss vor der Konfiguration eines entsprechenden Backups manuell erstellt worden sein. Weitere Informationen über die

Erstellung einer Secure Zone sowie deren Vorteile und Beschränkungen finden Sie im Abschnitt '"Über Secure Zone" (S. 455)'.

Erweiterte Storage-Option

Hinweis
Diese Funktionalität ist nur in der Advanced Edition des Cyber Protection Service verfügbar.

Per Skript festgelegt (nur für unter Windows laufende Maschinen)

Sie können die Backups einer jeden Maschine in einem per Skript festgelegten Ordner speichern lassen. Die Software unterstützt Skripte, die in JScript, VBScript oder Python 3.5 geschrieben sind. Wenn der Schutzplan bereitgestellt wird, führt die Software das Skript auf jeder Maschine aus. Die Skript-Ausgabe für jede Maschine sollte ein Ordnerpfad (lokal oder im Netzwerk) sein. Falls ein entsprechender Ordner nicht existiert, wird er automatisch erstellt (Einschränkung: Skripte, die in Python geschrieben sind, können keine Ordner auf Netzwerkfreigaben erstellen). In der Registerkarte **Backup Storage** wird jeder Ordner als separater Backup-Speicherort angezeigt.

Wählen Sie bei **Skript-Typ** die Skript-Sprache (**JScript**, **VBScript** oder **Python**). Dann können Sie das Skript importieren, kopieren oder über die Zwischenablage einfügen. Spezifizieren Sie für Netzwerkordner die Zugriffsanmeldedaten mit den Lese-/Schreibberechtigungen.

Beispiele:

- Folgendes JScript-Skript gibt den Backup-Speicherort für eine Maschine im Format `\\bkpsrv\<Maschinenname>` aus:

  ```
  WScript.Echo("\\\\bkpsrv\\" + WScript.CreateObject("WScript.Network").ComputerName);
  ```

  Als Ergebnis dieser Aktion werden die Backups einer jeden Maschine in einem Ordner gleichen Namens auf dem Server **bkpsrv** gespeichert.
- Folgendes JScript-Skript gibt den Backup-Speicherort als Ordner auf derjenigen Maschine aus, wo das Skript ausgeführt wird:

  ```
  WScript.Echo("C:\\Backup");
  ```

  Als Ergebnis werden die Backups dieser Maschine im Ordner `C:\Backup` auf eben dieser Maschine gespeichert.

  Hinweis
  Bei der Pfadangabe für den Speicherort in diesen Skripten wird zwischen Groß- und Kleinschreibung unterschieden. Daher werden `C:\Backup` und `C:\backup` in der Cyber Protect-Konsole als unterschiedliche Speicherorte angezeigt. Sie müsse außerdem auch einen Großbuchstaben für den Laufwerksbuchstaben verwenden.

Über Secure Zone

Die 'Secure Zone' ist ein spezielles, geschütztes Volume (Partition), das auf einem Laufwerk der zu sichernden Maschine liegt. Sie kann verwendet werden, um die Backups von Laufwerken oder Dateien der jeweiligen Maschine zu speichern.

Sollte das betreffende Laufwerk jedoch aufgrund eines physischen Fehlers ausfallen, gehen alle in der Secure Zone gespeicherten Backups verloren. Aus diesem Grund sollten Sie ein Backup nicht alleine nur in der Secure Zone speichern, sondern möglichst noch an einem oder sogar mehreren anderen Speicherorten. In Unternehmensumgebungen kann eine Secure Zone beispielsweise als praktischer Zwischenspeicher für Backups dienen, wenn ein normalerweise verwendeter Speicherort temporär nicht verfügbar ist (z.B. aufgrund einer fehlenden oder zu langsamen Daten- oder Netzwerkanbindung).

Wann ist die Verwendung der Secure Zone sinnvoll?

Secure Zone:

- Ermöglicht es, bei einer Laufwerkswiederherstellung dasselbe Laufwerk als Recovery-Ziel zu verwenden, auf dem das entsprechende Laufwerk-Backup selbst gespeichert ist.
- Bietet eine kosteneffektive und praktische Methode, um Ihre Daten leicht gegen Software-Fehler, Virusangriffe und Bedienungsfehler abzusichern.
- Ermöglicht es, dass bei Backup- oder Recovery-Aktionen die gesicherten Daten nicht unbedingt auf einem anderen Medium liegen oder über eine Netzwerkverbindung bereitgestellt werden müssen. Diese Funktion ist besonders für Benutzer von Mobilgeräten nützlich.
- Eignet sich gut als primäres Backup-Ziel, wenn Backups per Replikation noch an anderen Speicherorten gesichert werden.

Einschränkungen

- Auf dem Mac ist die Einrichtung bzw. Verwendung einer Secure Zone nicht möglich.
- Die Secure Zone kann nur als normales Volume auf einem Laufwerk vom Typ 'Basis' angelegt/verwendet werden. Sie kann weder auf einem dynamischen Datenträger liegen, noch als logisches Volume (einem per LVM verwalteten Volume) erstellt werden.
- Die Secure Zone verwendet FAT32 als Dateisystem. Da FAT32 eine Dateigrößenbeschränkung von 4 GB hat, werden größere Backups bei der Speicherung in der Secure Zone entsprechend aufgeteilt. Dies hat jedoch keinen Einfluss auf die Geschwindigkeit oder spätere Wiederherstellungsprozesse.

Wie die Erstellung der Secure Zone ein Laufwerk umwandelt

- Die Secure Zone wird immer am Ende des entsprechenden Laufwerks erstellt.
- Sollte der 'nicht zugeordnete' Speicherplatz am Ende des Laufwerks nicht ausreichen, jedoch zwischen den Volumes (Partitionen) noch weiterer 'nicht zugeordneter' Speicherplatz vorhanden

sein, so werden die entsprechenden Volumes so verschoben, dass der benötigte 'nicht zugeordnete' Speicherplatz demjenigen am Endes des Laufwerkes hinzugefügt wird.

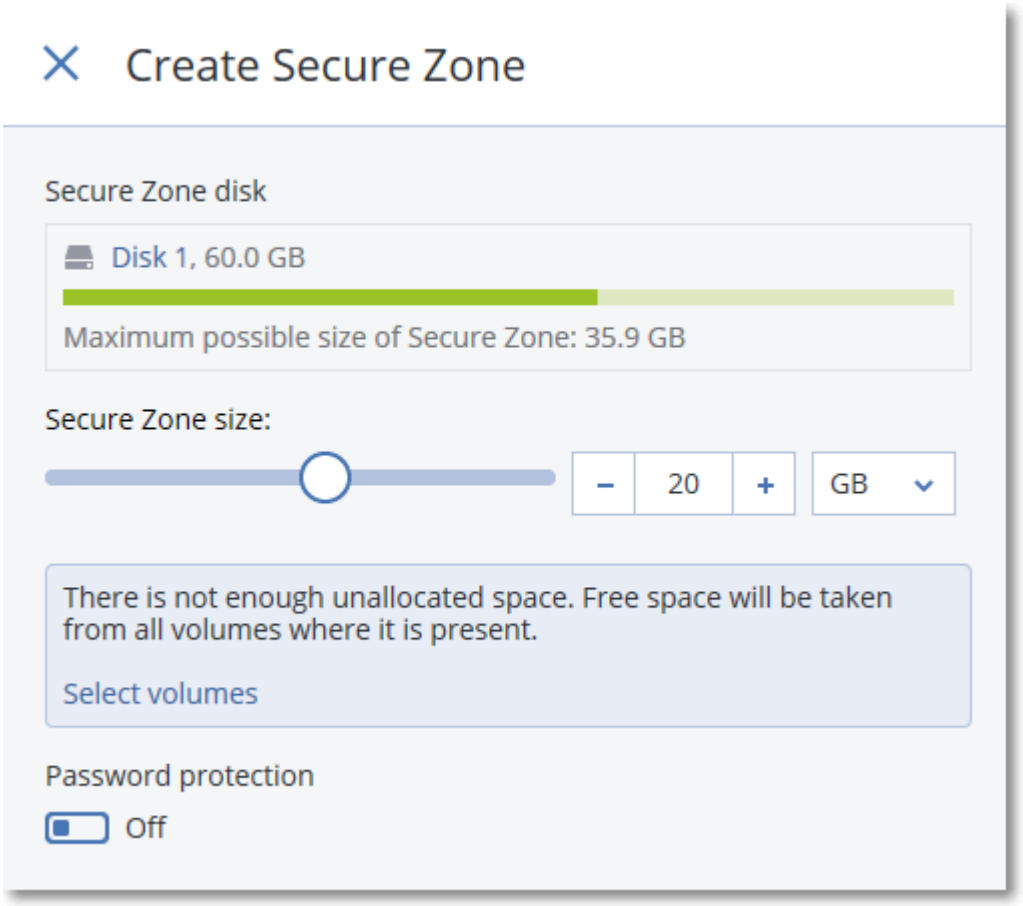
- Wenn der so zusammengestellte Speicherplatz immer noch nicht ausreicht, wird die Software freien Speicherplatz von denjenigen Volumes entnehmen, die Sie dafür festgelegt haben. Die Größe dieser Volumes wird bei diesem Prozess entsprechend proportional verkleinert.
- Auf jedem Volume sollte jedoch eine gewisse Menge freier Speicherplatz vorhanden sein/bleiben, um weiter damit arbeiten zu können. Auf einem Volume mit Betriebssystem und Applikationen müssen beispielsweise temporäre Dateien angelegt werden können. Ein Volume, dessen freier Speicherplatz weniger als 25 Prozent der Gesamtgröße des Volumes entspricht – oder durch den Prozess unter diesen Wert kommen würde – wird von der Software überhaupt nicht verkleinert. Nur wenn alle entsprechenden Volumes des Laufwerks mindestens 25 Prozent freien Speicherplatz haben, wird die Software mit der proportionalen Verkleinerung der Volumes fortfahren.

Daraus ergibt es sich, dass es normalerweise nicht ratsam ist, der Secure Zone die maximal mögliche Größe zuzuweisen. Am Ende haben Sie sonst auf keinem Volume mehr ausreichend freien Speicherplatz, was dazu führen kann, dass Betriebssystem und Applikationen nicht mehr starten oder fehlerhaft arbeiten.

Wichtig
Wenn Sie das Volume, von dem das System gegenwärtig bootet, verschieben oder in der Größe ändern, ist ein Neustart erforderlich.

So können Sie eine Secure Zone erstellen

1. Wählen Sie die Maschine aus, auf der Sie die Secure Zone erstellen wollen.
2. Klicken Sie auf **Details** –> **Secure Zone erstellen**.
3. Klicken Sie unter **Laufwerk für die Secure Zone** auf **Auswahl** und wählen Sie ein Laufwerk aus (sofern mehrere vorhanden sind), auf welchem Sie die Zone erstellen wollen.
   Die Software berechnet dann die maximal mögliche Größe für die Secure Zone.
4. Geben Sie die gewünschte Größe der Secure Zone ein oder ziehen Sie am Schieber, um eine Größe zwischen dem minimalen und maximalen Wert zu wählen.
   Die minimale Größe beträgt ca. 50 MB, abhängig von der Geometrie der Festplatte. Die maximale Größe ist identisch mit dem 'nicht zugeordneten' Speicherplatz plus der Größe des freien Speicherplatz auf allen Volumes des Laufwerks.
5. Sollte es für die von Ihnen spezifizierte Größe zu wenig 'nicht zugeordneten' Speicherplatz geben, wird die Software freien Speicherplatz von den vorhandenen Volumes entnehmen. Standardmäßig werden dafür alle Volumes ausgewählt. Falls Sie einige Volumes ausschließen wollen, klicken Sie auf **Volumes wählen**. Ansonsten können Sie diesen Schritt überspringen.



6. [Optional] Aktivieren Sie den Schalter **Kennwortschutz** und geben Sie ein Kennwort ein.
   Das Kennwort ist dann immer erforderlich, um auf die Backups in der Secure Zone zugreifen zu können. Um ein Backup in die Secure Zone zu erstellen, ist kein Kennwort erforderlich – außer die Backup-Ausführung erfolgt von einem Boot-Medium aus.
7. Klicken Sie auf **Erstellen**.
   Die Software zeigt das zu erwartende Partitionslayout an. Klicken Sie auf **OK**.
8. Warten Sie, bis die Software die Secure Zone erstellt hat.

Die Secure Zone kann nun unter **Backup-Ziel** ausgewählt werden, wenn Sie einen Schutzplan erstellen.

So können Sie eine Secure Zone löschen

1. Wählen Sie eine Maschine aus, auf der sich eine Secure Zone befindet.
2. Klicken Sie auf **Details**.
3. Klicken Sie auf das Zahnradsymbol neben dem Element **Secure Zone** und klicken Sie dann auf **Löschen**.
4. [Optional] Spezifizieren Sie die Volumes, denen der freiwerdende Speicherplatz aus der Zone zugewiesen werden soll. Standardmäßig werden dafür alle Volumes ausgewählt.

Der Speicherplatz wird gleichmäßig auf die ausgewählten Volumes verteilt. Wenn Sie keine Volumes auswählen, wird der freiwerdende Speicherplatz in 'nicht zugeordneten' Speicherplatz umgewandelt.

Wenn Sie das Volume, von dem das System gegenwärtig bootet, in der Größe ändern, ist ein Neustart erforderlich.

5. Klicken Sie auf **Löschen**.

Als Ergebnis dieser Aktion wird die Secure Zone komplett gelöscht – inklusive aller Backups, die in ihr gespeichert waren.

Backup-Planung

Sie können ein Backup so konfigurieren, dass es automatisch zu einem bestimmten Zeitpunkt, in bestimmten Intervallen oder bei einem bestimmten Ereignis ausgeführt wird.

Geplante Backups für Nicht-Cloud-zu-Cloud-Ressourcen werden nach den Zeitzoneneinstellungen des Workloads ausgeführt, auf dem der Protection Agent installiert ist. Wenn Sie beispielsweise denselben Schutzplan auf Workloads mit unterschiedlichen Zeitzoneneinstellungen anwenden, werden die Backups auf Basis der lokalen Zeitzone des jeweiligen Workloads gestartet.

Zur Planung eines Backups gehören folgende Aktionen:

- Ein Backup-System auswählen
- Den Zeitpunkt der Backup-Ausführung festlegen oder das Ereignis auswählen, welches das Backup auslösen soll
- Optionale Einstellungen und Startbedingungen konfigurieren

Backup-Schemata

Ein Backup-Schema ist derjenige Teil eines Schutzplans, der definiert, wann und welche Art von Backup (vollständig, differentiell oder inkrementell) erstellt werden soll. Sie können eines der vordefinierten Backup-Schemata auswählen oder ein benutzerdefiniertes Schema erstellen.

Die verfügbaren Backup-Schemata und -Typen hängen vom Backup-Speicherort und der Datenquelle für das Backup ab. Ein differentielles Backup ist beispielsweise nicht verfügbar, wenn Sie SQL-Daten, Exchange-Daten oder einen Systemzustand sichern wollen. Das Schema **Nur inkrementell (Einzeldatei)** wird nicht für Bandlaufwerke unterstützt.

Backup-Schema	Beschreibung	Konfigurierbare Elemente
Nur inkrementell (Einzeldatei)	Das erste Backup ist ein Voll-Backup und kann eine längere Zeit in Anspruch nehmen. Die nachfolgenden Backups sind inkrementell und bedeutend schneller.	• Planungstyp: monatlich, wöchentlich, täglich, stündlich

Backup-Schema	Beschreibung	Konfigurierbare Elemente
	Die Backups verwenden das Backup-Format 'Einzeldatei'[1]*. Die standardmäßig Planung für die Durchführung von Backups ist 'täglich' und zwar von Montag bis Freitag. Wir empfehlen die Verwendung dieses Schemas, wenn Sie Ihre Backups im Cloud Storage speichern wollen, weil inkrementelle Backups schneller sind und weniger Netzwerkverkehr verursachen.	• Backup-Auslöser: Zeit oder Ereignis • Startzeit • Startbedingungen • Zusätzliche Optionen
Nur vollständig	Alle Backups im Backup-Satz sind Voll-Backups. Die standardmäßig Planung für die Durchführung von Backups ist 'täglich' und zwar von Montag bis Freitag.	• Planungstyp: monatlich, wöchentlich, täglich, stündlich • Backup-Auslöser: Zeit oder Ereignis • Startzeit • Startbedingungen • Zusätzliche Optionen
Wöchentlich vollständig, täglich inkrementell	Ein Voll-Backup wird einmal pro Woche erstellt, während alle anderen Backups inkrementell sind. Das erste Backup ist ein Voll-Backup, die weiteren Backups im Verlauf der Woche sind inkrementell. Danach wiederholt sich der Zyklus. Wenn Sie den Tag bestimmen wollen, an dem das wöchentliche Voll-Backup erstellt werden soll, klicken Sie im Schutzplan auf das Zahnradsymbol und gehen Sie dann zu **Backup-Optionen** –> **Wöchentliches Backup**. Die standardmäßig Planung für die Durchführung von Backups ist 'täglich' und zwar von Montag bis Freitag.	• Backup-Auslöser: Zeit oder Ereignis • Startzeit • Startbedingungen • Zusätzliche Optionen

[1]Ein Backup-Format, in dem das anfängliche Voll-Backup sowie alle nachfolgenden inkrementellen Backups gemeinsam in Form einer einzigen/einzelnen tibx-Datei gespeichert werden. Dieses Format nutzt die Geschwindigkeit der inkrementellen Backup-Methode und vermeidet dabei gleichzeitig deren größten Nachteil: das schwierige Löschen veralteter Backups. Die Software kennzeichnet diejenigen Blöcke, die von veralteten Backups verwendet werden, als 'frei' und schreibt neue Backups in diese neuen Blöcke. Dies führt zu einer extrem schnellen Bereinigung, bei gleichzeitig minimalem Ressourcenverbrauch. Das Backup-Format 'Einzeldatei' ist nicht verfügbar, wenn als Backup-Ziel ein Storage (wie beispielsweise ein Bandlaufwerk) verwendet wird, der keine wahlfreien Lese- und Schreib-Zugriffe (Random Access Read and Write) zulässt.

Backup-Schema	Beschreibung	Konfigurierbare Elemente
Monatlich vollständig, wöchentlich differentiell, täglich inkrementell (GFS)	Standardmäßig werden inkrementelle Backups erstellt und zwar täglich von Montag bis Freitag. Differentielle Backups werden an jedem Samstag durchgeführt. Voll-Backups werden am ersten Tag eines jeden Monats durchgeführt. **Hinweis** Dies ist ein vordefiniertes benutzerdefiniertes Schema. Es wird im Schutzplan als **Benutzerdefiniert** angezeigt.	• Ändern Sie die vorhandene Planung pro Backup-Typ: ◦ Planungstyp: monatlich, wöchentlich, täglich, stündlich ◦ Backup-Auslöser: Zeit oder Ereignis ◦ Startzeit ◦ Startbedingungen ◦ Zusätzliche Optionen • Neue Planungen pro Backup-Typ hinzufügen
Benutzerdefiniert	Sie müssen die Backup-Typen (vollständig, differentiell und inkrementell) auswählen sowie für jeden von diesen eine eigene Planung konfigurieren*.	• Ändern Sie die vorhandene Planung pro Backup-Typ: ◦ Planungstyp: monatlich, wöchentlich, täglich, stündlich ◦ Backup-Auslöser: Zeit oder Ereignis ◦ Startzeit ◦ Startbedingungen ◦ Zusätzliche Optionen • Neue Planungen pro Backup-Typ hinzufügen

* Nachdem Sie einen Schutzplan erstellt haben, können Sie nicht mehr zwischen dem Backup-Schema **Nur inkrementell (Einzeldatei)** und einem der anderen Backup-Schemata wechseln (bzw. umgekehrt). **Nur inkrementell (Einzeldatei)** ist immer ein Einzeldatei-Format-Schema, während die übrigen Schemata Multidatei-Format-Schemata sind. Wenn Sie zwischen den Formaten wechseln wollen, müssen Sie einen neuen Schutzplan erstellen.

Backup-Typen

Folgende Backup-Typen sind verfügbar:

- Vollständig – ein Voll-Backup enthält alle Quelldaten. Dieses Backup ist eigenständig. Sie müssen auf keine anderen Backups zugreifen, um Daten aus einem Voll-Backup wiederherstellen zu können.

  Hinweis
  Das erste Backup, welches ein Schutzplan erstellt, ist immer ein Voll-Backup.

- Inkrementell – bei einem inkrementellen Backup werden nur solche Daten gespeichert, die seit dem letzten Backup geändert wurden, unabhängig davon, ob dieses ein vollständiges, differentielles oder inkrementelles Backup war. Um Daten aus diesem Backup wiederherstellen zu können, benötigen Sie die komplette Backup-Kette, auf der das inkrementelle Backup basiert – und zwar zurück bis zum anfänglichen Voll-Backup.
- Differentiell – ein differenzielles Backup speichert nur solche Daten, die seit dem letzten Voll-Backup geändert wurden. Um Daten aus diesem Backup wiederherstellen zu können, benötigen Sie sowohl das differentielle Backup als auch das entsprechende Voll-Backup, auf dem das differentielle Backup basiert.

Ein Backup nach Planung ausführen

Wenn Sie ein Backup automatisch zu einem bestimmten Zeitpunkt oder bei einem bestimmten Ereignis ausführen lassen wollen, müssen Sie im Schutzplan eine entsprechende Planung aktivieren.

So können Sie eine Planung aktivieren

1. Erweitern Sie im Schutzplan das **Backup**-Modul.
2. Klicken Sie auf **Planung**.
3. Aktivieren Sie den Schalter für 'Planung'.
4. Wählen Sie das Backup-Schema.
5. Konfigurieren Sie die Planung nach Ihren Anforderungen und klicken Sie anschließend auf **Fertig**.
   Weitere Informationen über die verfügbaren Planungsoptionen finden Sie in den Abschnitten '"Planung nach Zeit" (S. 462)' und '"Planung nach Ereignissen" (S. 464)'.
6. [Optional] Konfigurieren Sie die Startbedingungen oder zusätzliche Planungsoptionen.
7. Speichern Sie den Schutzplan.

Als Ergebnis wird jedes Mal eine Backup-Aktion gestartet, wenn die entsprechenden Bedingungen für die Planung erfüllt sind.

So können Sie eine Planung deaktivieren

1. Erweitern Sie im Schutzplan das **Backup**-Modul.
2. Klicken Sie auf **Planung**.
3. Stellen Sie den Schalter für 'Planung' auf aus.
4. Speichern Sie den Schutzplan.

Als Ergebnis wird nur dann ein Backup ausgeführt, wenn Sie es manuell starten.

Hinweis
Wenn die Planung deaktiviert ist, werden auch die Aufbewahrungsregeln nicht automatisch angewendet. Wenn Sie diese anwenden wollen, müssen Sie das Backup manuell ausführen.

Planung nach Zeit

In der nachfolgenden Tabelle werden die Planungsoptionen zusammengefasst, die sich auf Zeiteinstellungen beziehen. Die Verfügbarkeit dieser Optionen hängt vom jeweiligen Backup-Schema ab. Weitere Informationen finden Sie im Abschnitt '"Backup-Schemata" (S. 458)'.

Option	Beschreibung	Beispiele
Monatlich	Wählen Sie die Monate, die Monatstage oder die Wochentage und bestimmen Sie anschließend den Startzeitpunkt des Backups.	Ein Backup am 1. Januar und 3. Februar um 12:00 Uhr ausführen. Ein Backup am ersten Tag eines jeden Monats um 10:00 Uhr ausführen. Ein Backup am 1. März, 5. März, 1. April und 5. April, jeweils um 09:00 Uhr, ausführen. Ein Backup an jedem zweiten und dritten Freitag eines jeden Monats um 11:00 Uhr ausführen. Ein Backup am letzten Mittwoch des Monats um 22:30 Uhr ausführen.
Wöchentlich	Wählen Sie die Wochentage aus und bestimmen Sie dann den Startzeitpunkt des Backups.	Ein Backup von Montag bis Freitag um 10:00 Uhr ausführen. Ein Backup am Montag um 23:00 Uhr ausführen. Ein Backup am Dienstag und Samstag um 08:00 Uhr ausführen.
Täglich	Wählen Sie die Tage aus (täglich oder nur wochentags) und bestimmen Sie dann den Startzeitpunkt des Backups.	Ein Backup jeden Tag um 11:45 Uhr ausführen. Ein Backup von Montag bis Freitag um 21:30 Uhr ausführen.
Stündlich	Wählen Sie die Wochentage und bestimmen Sie anschließend das Zeitintervall zwischen zwei aufeinanderfolgenden Backups sowie den Zeitraum, in dem die Backups ausgeführt werden sollen.	Ein Backup stündlich zwischen 08:00 Uhr und 18:00 Uhr, von Montag bis Freitag, ausführen. Ein Backup alle 3 Stunden zwischen 01:00 Uhr und 18:00 Uhr, am Samstag und Sonntag, ausführen.

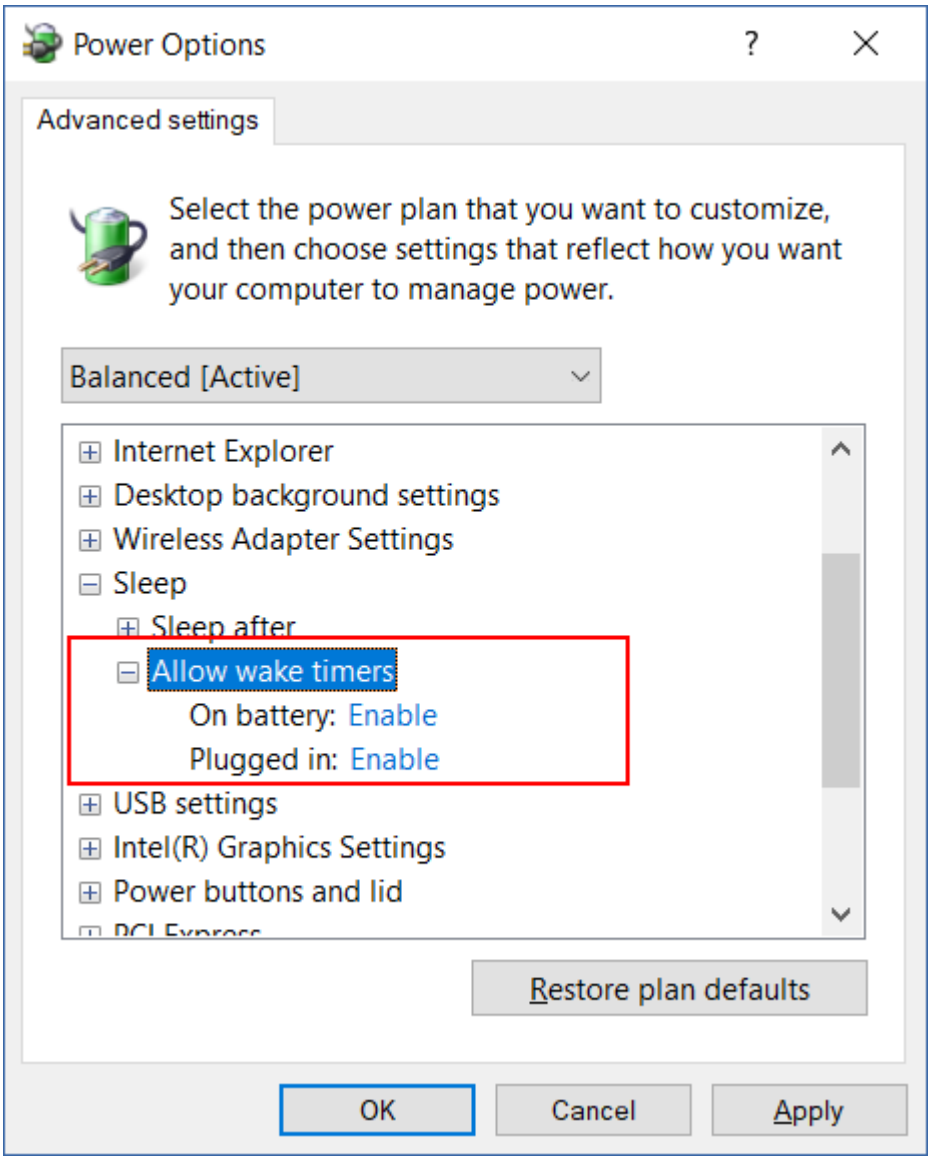
Option	Beschreibung	Beispiele
	Wenn Sie das Intervall in Minuten konfigurieren, können Sie ein vorgeschlagenes Intervall zwischen 10 und 60 Minuten wählen oder alternativ ein benutzerdefiniertes Intervall (wie 45 oder 75 Minuten) spezifizieren.	

Zusätzliche Optionen

Wenn Sie ein Backup nach Zeit planen, sind die folgenden zusätzlichen Planungsoptionen verfügbar.

Wenn Sie auf diese zugreifen wollen, klicken Sie im Fensterbereich **Planung** auf **Mehr anzeigen**.

- **Task bei Neustart der Maschine ausführen, wenn die Maschine zur geplanten Zeit ausgeschaltet war**
  Standardeinstellung: Deaktiviert.
- **Standby- oder Ruhezustandsmodus während des Backups verhindern**
  Diese Option ist nur auf Maschinen anwendbar, die unter Windows laufen.
  Standardeinstellung: Aktiviert.
- **Aus Standby- oder Ruhezustandsmodus aufwecken, um ein geplantes Backup zu starten**
  Diese Option gilt nur für Maschinen mit Windows, in deren Energiesparplänen die Option **Zeitgeber zur Aktivierung zulassen** aktiviert ist.



Diese Option verwendet nicht die Wake-on-LAN-Funktionalität und kann daher nicht auf ausgeschaltete Maschinen angewendet werden.

Standardeinstellung: Deaktiviert.

Planung nach Ereignissen

Wenn Sie ein Backup konfigurieren wollen, das bei einem bestimmten Ereignis ausgeführt wird, müssen Sie eine der nachfolgenden Optionen wählen.

Option	Beschreibung	Beispiele
Zeit seit letztem Backup	Ein Backup wird nach einem spezifizierten Zeitraum nach dem letzten erfolgreichen Backup gestartet.	Backup einen Tag nach dem letzten erfolgreichen Backup ausführen. Backup vier Stunden nach dem letzten erfolgreichen Backup ausführen.

Option	Beschreibung	Beispiele
	Hinweis Diese Option hängt davon ab, wie das vorherige Backup abgeschlossen wurde. Falls ein Backup fehlgeschlagen ist, wird das nächste Backup nicht automatisch ausgeführt. In diesem Fall müssen Sie das Backup manuell ausführen und sicherstellen, dass es erfolgreich abgeschlossen wurde, damit die Planung zurückgesetzt wird.	
Wenn sich ein Benutzer am System anmeldet	Ein Backup wird gestartet, wenn sich ein Benutzer an der Maschine anmeldet. Sie können diese Option für jede beliebige Anmeldung oder für die Anmeldung eines bestimmten Benutzers konfigurieren. **Hinweis** Es wird kein Backup gestartet, wenn Sie sich mit einem temporären Benutzerprofil anmelden.	Backup ausführen, wenn sich der Benutzer John Doe anmeldet.
Wenn sich ein Benutzer vom System abmeldet	Es wird ein Backup gestartet, wenn sich ein Benutzer von der Maschine abmeldet. Sie können diese Option für jede beliebige Abmeldung oder für die Abmeldung eines bestimmten Benutzers konfigurieren. **Hinweis** Es wird kein Backup gestartet, wenn Sie sich mit einem temporären Benutzerprofil abmelden. Es wird kein Backup gestartet, wenn eine Maschine heruntergefahren wird.	Backup ausführen, wenn sich jeder Benutzer abmeldet.
Beim Systemstart	Ein Backup wird ausgeführt, wenn die geschützte Maschine hochfährt.	Backup ausführen, wenn ein Benutzer die Maschine startet.
Beim Herunterfahren des Systems	Ein Backup wird ausgeführt, wenn die geschützte Maschine herunterfährt.	Backup ausführen, wenn ein Benutzer die Maschine herunterfährt.

Option	Beschreibung	Beispiele
Bei Ereignis im Windows-Ereignisprotokoll	Ein Backup wird ausgeführt, wenn ein von Ihnen spezifiziertes Windows-Ereignis eintritt.	Backup ausführen, wenn das Ereignis 7 mit dem Typ Fehler und der Quelle disk im Windows-Systemprotokoll aufgenommen wird.

Die Verfügbarkeit dieser Optionen ist von der Backup-Quelle und dem Betriebssystem der geschützten Workloads abhängig. In der nachfolgenden Tabelle werden die verfügbaren Optionen für Windows, Linux und macOS zusammengefasst.

Ereignis	Backup-Quelle					
	Komplette Maschine, Laufwerke/Volumes oder Dateien/Ordner (physische Maschinen)	**Komplette Maschinen oder Laufwerke/Volumes (virtuelle Maschinen)**	**ESXi-Konfiguration**	**Microsoft 365-Postfächer**	**Exchange-Datenbanken und -Postfächer**	**SQL-Datenbanken**
Zeit seit letztem Backup	Windows, Linux, macOS	Windows, Linux	Windows, Linux	Windows	Windows	Windows
Wenn sich ein Benutzer am System anmeldet	Windows	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar
Wenn sich ein Benutzer vom System abmeldet	Windows	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar
Beim Systemstart	Windows, Linux, macOS	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar
Beim Herunterfahren des Systems	Windows	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar
Bei Ereignis im Windows-Ereignisprotokoll	Windows	Nicht verfügbar	Nicht verfügbar	Windows	Windows	Windows

Bei Ereignis im Windows-Ereignisprotokoll

Sie können automatisch ein Backup ausführen lassen, wenn ein bestimmtes Ereignis in einem Windows-Ereignisprotokoll (wie dem Anwendungsprotokoll, dem Sicherheitsprotokoll oder dem Systemprotokoll) aufgezeichnet wird.

Hinweis
Sie können die Ereignisse durchsuchen und (in Windows) deren Eigenschaften unter **Computerverwaltung** –> **Ereignisanzeige** einsehen. Wenn Sie das Sicherheitsprotokoll öffnen wollen, benötigen Sie Administratorrechte.

Ereignis-Parameter

In der nachfolgenden Tabelle werden die Parameter zusammengefasst, die Sie spezifizieren müssen, wenn Sie die Option **Bei Ereignis im Windows-Ereignisprotokoll** konfigurieren.

Parameter	Beschreibung
Protokollname	Der Name des Protokolls. Wählen Sie den Namen eines Standardprotokolls (Applikation, Sicherheit, System) oder spezifizieren Sie einen anderen Protokollnamen. Beispielsweise Microsoft Office-Sitzungen.
Ereignisquelle	Die Ereignisquelle verweist auf das Programm oder die Systemkomponente, welche(s) das Ereignis verursacht hat. Beispielsweise Laufwerk. Jede Ereignisquelle, die die spezifizierte Textzeichenfolge enthält, wird das geplante Backup auslösen. Bei diesem Option wird nicht zwischen Groß-/Kleinschreibung unterschieden. Wenn Sie beispielsweise die Zeichenfolge `service` spezifizieren, werden sowohl die Ereignisquellen Service Control Manager als auch Time-Service ein Backup auslösen.
Ereignistyp	Typ des Ereignisses: Fehler, Warnung, Informationen, Überwachung erfolgreich oder Überwachung fehlgeschlagen.
Ereignis-ID	Die Ereignis-ID identifiziert eine bestimmte Art von Ereignis innerhalb einer Ereignisquelle. So tritt z.B. ein Fehler-Ereignis mit der Ereignisquelle Laufwerk und der Ereignis-ID 7 auf, wenn Windows einen fehlerhaften Block auf einem Festplattenlaufwerk entdeckt – während ein Fehler-Ereignis mit der Ereignisquelle Laufwerk und der Ereignis-ID 15 auftritt, wenn ein Laufwerk nicht zugriffsbereit ist.

Beispiel: Ein Notfall-Backup, wenn auf dem Laufwerk fehlerhafte Blöcke gefunden werden

Ein oder mehrere fehlerhafte Blöcke auf einem Laufwerk können ein Indiz für einen bevorstehenden Ausfall sein. Deshalb wollen Sie möglicherweise ein Backup erstellen, wenn ein

fehlerhafter Block erkannt wird.

Wenn Windows auf einem Laufwerk einen fehlerhaften Block entdeckt, wird ein Fehlerereignis mit der Ereignisquelle disk und der Ereignisnummer 7 im Systemprotokoll aufgezeichnet. Konfigurieren Sie im Schutzplan die folgende Planung:

- Planung: Bei Ereignis im Windows-Ereignisprotokoll
- Protokollname: System
- Ereignisquelle: disk
- Ereignistyp: Fehler
- Ereignis-ID: 7

Wichtig
Wenn Sie sicherstellen wollen, dass das Backup trotz der fehlerhaften Blöcke abgeschlossen werden kann, gehen Sie in den **Backup-Optionen** zum Unterpunkt **Fehlerbehandlung** und aktivieren das Kontrollkästchen **Fehlerhafte Sektoren ignorieren**.

Startbedingungen

Wenn Sie wollen, dass ein Backup nur dann ausgeführt wird, wenn bestimmte Bedingungen erfüllt sind, müssen Sie eine oder mehrere Startbedingungen konfigurieren. Wenn Sie mehrere Bedingungen konfigurieren, müssen diese alle gleichzeitig erfüllt sein, damit das Backup ausgeführt wird. Sie können einen Zeitraum spezifizieren, nach dem die Backups ausgeführt werden, unabhängig davon, ob die Bedingungen erfüllt sind. Weitere Informationen über diese Backup-Option finden Sie im Abschnitt '"Task-Startbedingungen" (S. 536)'.

Die Startbedingungen gelten nicht, wenn Sie ein Backup manuell ausführen.

Die untere Tabelle zeigt die Startbedingungen an, die für verschiedene Daten unter Windows, Linux und macOS verfügbar sind.

Startbedingung	Backup-Quelle					
	Komplette Maschine, Laufwerke/Volumes oder Dateien/Ordner (physische Maschinen)	**Komplette Maschinen oder Laufwerke/Volumes (virtuelle Maschinen)**	**ESXi-Konfiguration**	**Microsoft 365-Postfächer**	**Exchange-Datenbanken und -Postfächer**	**SQL-Datenbanken**
Benutzer ist inaktiv	Windows	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar
Der Host des Backup-	Windows, Linux, macOS	Windows, Linux	Windows, Linux	Windows	Windows	Windows

Startbedingung	Backup-Quelle					
	Komplette Maschine, Laufwerke/Volumes oder Dateien/Ordner (physische Maschinen)	**Komplette Maschinen oder Laufwerke/Volumes (virtuelle Maschinen)**	**ESXi-Konfiguration**	**Microsoft 365-Postfächer**	**Exchange-Datenbanken und -Postfächer**	**SQL-Datenbanken**
Speicherorts ist verfügbar						
Benutzer sind abgemeldet	Windows	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar
Entspricht dem Zeitintervall	Windows, Linux, macOS	Windows, Linux	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar
Akkubelastung senken	Windows	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar
Nicht starten, wenn eine getaktete Verbindung besteht	Windows	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar
Nicht starten, wenn eine Verbindung mit folgenden WLANs besteht	Windows	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar
IP-Adresse des Gerätes überprüfen	Windows	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar

Benutzer ist inaktiv

'Benutzer ist inaktiv' bedeutet, dass auf der Maschine ein Bildschirmschoner läuft oder die Maschine gesperrt ist.

Beispiel

Starte ein Backup täglich um 21:00 Uhr, möglichst, wenn der Benutzer inaktiv ist. Wenn der Benutzer um 23:00 Uhr immer noch aktiv, starte den Task trotzdem.

- Planung: **Täglich**, **Jeden Tag ausführen**. Starten um: **21:00:00 Uhr**.
- Bedingung: **Benutzer ist inaktiv**.
- Backup-Startbedingungen: **Warten, bis die Bedingungen erfüllt sind**, **Task trotzdem ausführen nach 2** Stunden.

Ergebnis:

- Wenn der Benutzer vor 21:00 Uhr inaktiv ist, wird das Backup um 21:00 Uhr gestartet.
- Wenn der Benutzer zwischen 21:00 und 23:00 Uhr inaktiv wird, wird das Backup sofort gestartet.
- Wenn der Benutzer um 23 Uhr immer noch aktiv ist, wird das Backup um 23:00 Uhr gestartet.

Der Host des Backup-Speicherorts ist verfügbar

'Der Host des Backup-Speicherorts ist verfügbar' bedeutet, dass die Maschine, die den Backup-Speicherort hostet, über das Netzwerk verfügbar ist.

Diese Bedingung gilt für Netzwerkordner, den Cloud Storage und Speicherorte, die von einem Storage Node verwaltet werden.

Diese Bedingung sagt nichts über die Verfügbarkeit des Speicherorts selbst aus – nur über die Verfügbarkeit des Hosts. Wenn beispielsweise der Host verfügbar ist, der Netzwerkordner auf diesem Host aber nicht freigegeben ist oder die Anmeldedaten für den Ordner nicht mehr gültig sind, trifft die Bedingung dennoch weiterhin zu.

Beispiel

Sie führen Backups an jedem Werktag um 21:00 Uhr zu einem Netzwerkordner durch. Wenn die Maschine, die den Ordner hostet, gerade nicht verfügbar ist (z.B. wegen Wartungsarbeiten), soll das Backup übersprungen werden und auf den nächsten geplanten Start am nächsten Werktag gewartet werden.

- Planung: **Täglich**, **Montag bis Freitag ausführen**. Starten um: **21:00 Uhr**.
- Bedingung: **Der Host des Backup-Speicherorts ist verfügbar**.
- Backup-Startbedingungen: **Das geplante Backup überspringen**.

Ergebnis:

- Wenn der Host um 21:00 Uhr verfügbar ist, wird das Backup sofort gestartet.
- Wenn der Host nicht um 21:00 Uhr verfügbar ist, wird das Backup am nächsten Werktag gestartet (sofern der Host an diesem Tag um 21:00 Uhr verfügbar ist).
- Wenn der Host niemals an Werktagen um 21:00 Uhr verfügbar ist, wird das Backup niemals gestartet.

Benutzer sind abgemeldet

Verwenden Sie diese Startbedingung, um ein Backup solange zu verschieben, bis sich alle Benutzer von der betreffenden Windows Maschine abgemeldet haben.

Beispiel

Sie starten ein Backup jeden Freitag um 20:00 Uhr, möglichst wenn alle Benutzer abgemeldet sind. Wenn einer der Benutzer um 23:00 Uhr immer noch angemeldet ist, starte das Backup trotzdem.

- Planung: **Wöchentlich**, immer freitags. Starten um: **20:00:00 Uhr**.
- Bedingung: **Benutzer sind abgemeldet**.
- Backup-Startbedingungen: **Warten, bis die Bedingungen erfüllt sind**, **Backup trotzdem ausführen nach 3** Stunden.

Ergebnis:

- Wenn alle Benutzer um 20:00 Uhr abgemeldet sind, wird das Backup um 20:00 Uhr gestartet.
- Wenn sich der letzte Benutzer zwischen 20:00 und 23:00 Uhr abmeldet, wird das Backup sofort ausgeführt.
- Wenn um 23:00 Uhr noch Benutzer angemeldet sind, wird das Backup um 23:00 Uhr gestartet.

Entspricht dem Zeitintervall

Verwenden Sie diese Startbedingung, um einen Backup-Start auf ein bestimmtes Intervall zu beschränken.

Beispiel

Eine Firma verwendet unterschiedliche Speicherorte auf demselben NAS-Gerät (Network Attached Storage), um Benutzerdaten und Server zu sichern.

Der Werktag beginnt um 08:00 Uhr und endet um 17:00 Uhr. Die Benutzerdaten sollen gesichert werden, sobald sich die Benutzer abmelden, jedoch nicht vor 16:30 Uhr.

Die Server der Firma werden täglich um 23:00 Uhr gesichert. Die Benutzerdaten sollen möglichst vor 23:00 Uhr gesichert werden, damit genügend Netzwerkbandbreite für die Server-Backups verfügbar ist.

Das Backup der Benutzerdaten dauert nicht länger als eine Stunde, sodass der späteste Backup-Startzeitpunkt 22:00 Uhr ist. Wenn ein Benutzer innerhalb des spezifizierten Zeitintervalls immer noch angemeldet ist oder sich zu einem anderen Zeitpunkt abmeldet, soll das Backup der Benutzerdaten übersprungen werden.

- Ereignis: **Wenn sich ein Benutzer vom System abmeldet**. Spezifizieren Sie das Benutzerkonto: **Jeder Benutzer**.
- Bedingung: **Entspricht dem Zeitintervall**: von **16:30:00 Uhr** bis **22:00:00 Uhr**.
- Backup-Startbedingungen: **Das geplante Backup überspringen**.

Ergebnis:

- Wenn sich der Benutzer zwischen 16:30 und 22:00 Uhr abmeldet, wird das Backup umgehend ausgeführt.

- Wenn sich der Benutzer zu einem anderen Zeitpunkt abmeldet, wird das Backup übersprungen.

Akkubelastung senken

Verwenden Sie diese Startbedingung, um ein Backup zu unterbinden, wenn eine Maschine (wie etwa ein Laptop oder ein Tablet) an keine externe Stromquelle angeschlossen ist. In Abhängigkeit vom Wert der Option Backup-Startbedingungen, wird das übersprungene Backup (nicht) gestartet, wenn die Maschine wieder an eine externe Stromquelle angeschlossen wird.

Folgende Optionen sind verfügbar:

- **Nicht starten, wenn im Akkubetrieb**
  Ein Backup wird nur gestartet, wenn die Maschine mit einer externen Stromquelle verbunden wird.
- **Im Akkubetrieb starten, wenn Akkustand höher ist als**
  Ein Backup wird gestartet, wenn die Maschine mit einer externen Stromquelle verbunden wird oder der Akkustand über dem spezifizierten Wert liegt.

Beispiel

Sie sichern Ihre Daten jeden Werktag um 21:00 Uhr. Wenn Ihre Maschine an keine externe Stromquelle angeschlossen ist, soll das Backup übersprungen werden, um Akkuladung zu sparen und stattdessen darauf gewartet werden, dass Sie die Maschine wieder an eine Stromversorgung anschließen.

- Planung: **Täglich**, **Montag bis Freitag ausführen**. Starten um: **21:00:00 Uhr**.
- Bedingung: **Akkubelastung senken**, **Nicht starten, wenn im Akkubetrieb**.
- Backup-Startbedingungen: **Warten, bis die Bedingungen erfüllt sind**.

Ergebnis:

- Wenn die Maschine um 21:00 Uhr an eine externe Stromquelle angeschlossen ist, wird das Backup umgehend gestartet.
- Wenn die Maschine um 21:00 Uhr im Akkubetrieb läuft, wird das Backup gestartet, sobald Sie die Maschine wieder an eine externe Stromquelle anschließen.

Nicht starten, wenn eine getaktete Verbindung besteht

Verwenden Sie diese Startbedingung, um ein Backup (auch ein Backup zu einem lokalen Laufwerk) zu unterbinden, wenn die Maschine eine Internetverbindung verwendet, die von Windows als 'getaktet' eingestuft wird (z.B. eine Mobilfunkverbindung). Weitere Informationen über getaktete Verbindungen in Windows finden Sie in diesem Artikel: https://support.microsoft.com/de-de/help/17452/windows-metered-internet-connections-faq.

Die zusätzliche Startbedingung **Nicht starten, wenn eine Verbindung mit folgenden WLANs besteht** wird automatisch aktiviert, wenn Sie die Bedingung **Nicht starten, wenn eine getaktete Verbindung besteht** aktivieren. Dies ist eine zusätzliche Maßnahme, um Backups über Mobilfunk-

Hotspots unterbinden zu können. Folgende Netzwerknamen sind standardmäßig eingetragen: android, phone, mobile und modem.

Wenn Sie diese Namen aus der Liste entfernen wollen, klicken Sie auf das X-Zeichen. Wenn Sie einen neuen Namen hinzufügen wollen, geben Sie diesen in das leere Feld ein.

Beispiel

Sie sichern Ihre Daten jeden Werktag um 21:00 Uhr. Wenn die Maschine über eine getaktete Verbindung mit dem Internet verbunden ist, soll das Backup übersprungen werden, um Netzwerkverkehr/Gebühren zu sparen, und stattdessen auf den geplanten Start am nächsten Werktag gewartet werden.

- Planung: **Täglich**, **Montag bis Freitag ausführen**. Starten um: **21:00:00 Uhr**.
- Bedingung: **Nicht starten, wenn eine getaktete Verbindung besteht**.
- Backup-Startbedingungen: **Das geplante Backup überspringen**.

Ergebnis:

- Wenn die Maschine um 21:00 Uhr nicht über eine getaktete Verbindung mit dem Internet verbunden ist, wird das Backup umgehend gestartet.
- Wenn die Maschine um 21:00 Uhr nicht über eine getaktete Verbindung mit dem Internet verbunden ist, wird das Backup am nächsten Werktag gestartet.
- Wenn die Maschine werktags um 21:00 Uhr immer über eine getaktete Verbindung mit dem Internet verbunden ist, wird das Backup niemals gestartet.

Nicht starten, wenn eine Verbindung mit folgenden WLANs besteht

Verwenden Sie diese Startbedingung, um ein Backup (auch ein Backup zu einem lokalen Laufwerk) zu unterbinden, wenn die Maschine mit einem der spezifizierten drahtlosen Netzwerke (WLANs) verbunden ist (wenn Sie beispielsweise unterbinden wollen, dass Backups über Mobilfunk-Hotspots durchgeführt werden).

Sie können als WLAN-Name die sogenannte SSID (Service Set Identifier) spezifizieren. Die Sperre gilt für alle Netzwerke, die den angegebenen Namen als Teilzeichenfolge in ihrer Netzwerknamen enthalten (unabhängig von Groß-/Kleinschreibung). Beispiel: wenn Sie `phone` als Netzwerkname spezifizieren, wird das Backup nicht gestartet, wenn die Maschine mit einem der folgenden Netzwerke verbunden ist: `Johns iPhone`, `phone_wlan` oder `mein_PHONE_wlan`.

Die Startbedingung **Nicht starten, wenn eine Verbindung mit folgenden WLANs besteht** wird automatisch aktiviert, wenn Sie die Bedingung **Nicht starten, wenn eine getaktete Verbindung besteht** aktivieren. Die folgenden Netzwerknamen sind standardmäßig spezifiziert: android, `phone`, `mobile` und modem.

Wenn Sie diese Namen aus der Liste entfernen wollen, klicken Sie auf das X-Zeichen. Wenn Sie einen neuen Namen hinzufügen wollen, geben Sie diesen in das leere Feld ein.

Beispiel

Sie sichern Ihre Daten jeden Werktag um 21:00 Uhr. Wenn die Maschine über einen Mobilfunk-Hotspot mit dem Internet verbunden ist, soll das Backup übersprungen und auf den planmäßigen Start am nächsten Werktag gewartet werden.

- Planung: **Täglich**, **Montag bis Freitag ausführen**. Starten um: **21:00:00 Uhr**.
- Bedingung: **Nicht starten, wenn eine Verbindung mit folgenden WLANs besteht**, **Netzwerkname**: `<SSID des Hotspot-Netzwerks>`.
- Backup-Startbedingungen: **Das geplante Backup überspringen**.

Ergebnis:

- Wenn die Maschine um 21:00 Uhr nicht mit dem spezifizierten Netzwerk verbunden ist, wird das Backup umgehend gestartet.
- Wenn die Maschine um 21:00 Uhr mit dem spezifizierten Netzwerk verbunden ist, wird das Backup am nächsten Werktag gestartet.
- Wenn die Maschine werktags um 21:00 Uhr immer mit dem spezifizierten Netzwerk verbunden ist, wird das Backup niemals gestartet.

IP-Adresse des Gerätes überprüfen

Verwenden Sie diese Startbedingung, um ein Backup (auch ein Backup zu einem lokalen Laufwerk) zu unterbinden, wenn eine der Maschinen-IP-Adressen innerhalb oder außerhalb des angegebenen IP-Adressbereichs liegt. So können Sie z.B. hohe Datenübertragungsgebühren vermeiden, wenn Sie Maschinen von Benutzern sichern, die sich im fernen Ausland befinden – oder unterbinden, dass Backups über VPN-Verbindungen (Virtual Private Network) durchgeführt werden.

Folgende Optionen sind verfügbar:

- **Starten, wenn außerhalb des IP-Bereichs**
- **Starten, wenn innerhalb des IP-Bereichs**

Sie können mit beiden Optionen mehrere Bereiche spezifizieren. Es werden nur IPv4-Adressen unterstützt.

Beispiel

Sie sichern Ihre Daten jeden Werktag um 21:00 Uhr. Wenn die Maschine über einen VPN-Tunnel mit dem Unternehmensnetzwerk verbunden ist, soll das Backup ausgelassen werden.

- Planung: **Täglich**, **Montag bis Freitag ausführen**. Start um **21:00 Uhr**.
- Bedingung: **IP-Adresse des Gerätes überprüfen**, **Starten, wenn außerhalb des IP-Bereichs**, **Von**: `<Anfang des VPN-IP-Adressbereichs>`, **Bis**: `<Ende des VPN-IP-Adressbereichs>`.
- Backup-Startbedingungen: **Warten, bis die Bedingungen erfüllt sind**.

Ergebnis:

- Wenn sich die IP-Adresse der Maschine um 21:00 Uhr nicht im spezifizierten Bereich befindet, wird das Backup umgehend gestartet.
- Wenn sich die IP-Adresse der Maschine um 21:00 Uhr im spezifizierten Bereich befindet, wird das Backup gestartet, wenn die Maschine eine Nicht-VPN-IP-Adresse erhält.
- Wenn die IP-Adresse der Maschine werktags um 21:00:00 Uhr immer im spezifizierten Bereich liegt, wird das Backup niemals gestartet.

Zusätzliche Planungsoptionen

Sie können die Backups so konfigurieren, dass sie nur dann ausgeführt werden, wenn bestimmte Bedingungen erfüllt sind. Oder dass sie nur während eines bestimmten Zeitraums ausgeführt werden. Oder dass sie mit einer bestimmten Verzögerung zur Planung ausgeführt werden.

So können Sie die Startbedingungen konfigurieren

1. Erweitern Sie im Schutzplan das **Backup**-Modul.
2. Klicken Sie auf **Planung**.
3. Klicken Sie im Fensterbereich **Planung** auf **Mehr anzeigen**.
4. Aktivieren Sie die Kontrollkästchen neben den Startbedingungen, die Sie verwenden wollen – und klicken Sie anschließend auf **Fertig**.
   Weitere Informationen zu den verfügbaren Startbedingungen und deren Konfiguration finden Sie im Abschnitt '"Startbedingungen" (S. 468)'.
5. Speichern Sie den Schutzplan.

So können Sie einen Zeitraum konfigurieren

1. Erweitern Sie im Schutzplan das **Backup**-Modul.
2. Klicken Sie auf **Planung**.
3. Aktivieren Sie das Kontrollkästchen **Den Plan innerhalb eines Zeitraums ausführen**.
4. Spezifizieren Sie den Zeitraum nach Ihren Anforderungen und klicken Sie anschließend auf **Fertig**.
5. Speichern Sie den Schutzplan.

Als Ergebnis werden die Backups nur während des spezifizierten Zeitraums ausgeführt.

So können Sie eine Verzögerung konfigurieren

Um eine übermäßige Netzwerkauslastung zu vermeiden, wenn Sie mehrere Workloads zu einem Netzwerkspeicherort sichern wollen, können Sie über eine Backup-Option eine kleine zufällige Verzögerung konfigurieren. Sie können die Option deaktivieren oder deren Einstellung ändern.

1. Erweitern Sie im Schutzplan das **Backup**-Modul.
2. Klicken Sie auf **Backup-Optionen** und wählen Sie dann **Planung**.

Der Verzögerungswert für jeden Workload wird zufällig bestimmt und kann zwischen Null und einem maximalen, von Ihnen spezifizierten Wert liegen. Der maximale Wert beträgt standardmäßig 30 Minuten.

Weitere Informationen über diese Backup-Option finden Sie im Abschnitt '"Planung" (S. 534)'

Der Verzögerungswert für jeden Workload wird berechnet, wenn Sie den Schutzplan auf diesen Workload anwenden – und er bleibt so lange gleich, bis Sie den maximalen Verzögerungswert wieder ändern.

3. Spezifizieren Sie den Zeitraum nach Ihren Anforderungen und klicken Sie anschließend auf **Fertig**.
4. Speichern Sie den Schutzplan.

Ein Backup manuell ausführen

Sie können sowohl geplante als auch ungeplante Backups manuell ausführen.

So können Sie ein Backup manuell ausführen

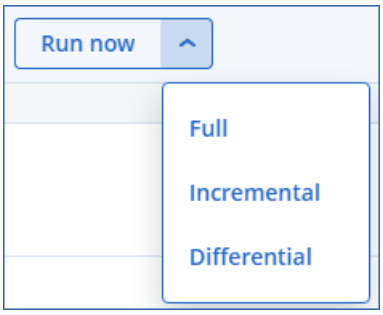
1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte**.
2. Wählen Sie den Workload aus, für den Sie ein Backup ausführen wollen, und klicken Sie anschließend auf **Schützen**.
3. Wählen Sie den Schutzplan aus, mit dem Sie das Backup erstellen wollen.

   Wenn auf den Workload kein Schutzplan angewendet wurde, können Sie einen bereits vorhandenen Plan anwenden oder einen neuen erstellen.

   Weitere Informationen darüber, wie Sie einen Schutzplan erstellen können, finden Sie im Abschnitt '"Einen Schutzplan erstellen" (S. 232)'.
4. [Wenn Sie den vorgegebenen Backup-Typ erstellen wollen] Klicken Sie im Schutzplan auf das Symbol **Jetzt ausführen**.

   Alternativ können Sie auch im Schutzplan das **Backup**-Modul erweitern und dann auf die Schaltfläche **Jetzt ausführen** klicken.
5. [Wenn Sie eine bestimmte Backup-Typ erstellen wollen] Erweitern Sie im Schutzplan das **Backup**-Modul, klicken Sie auf den Pfeil neben der Schaltfläche **Jetzt ausführen** und bestimmen Sie anschließend den gewünschten Backup-Typ.



Hinweis
Bei Backup-Schemata, die nur eine Backup-Methode verwenden (z.B. **Nur inkrementell (Einzeldatei)** oder **Nur vollständig**), kann kein Backup-Typ ausgewählt werden.

Daraufhin wird die Backup-Aktion gestartet. Sie können deren Fortschritt und Ergebnis auf der Registerkarte **Geräte** in der Spalte **Status** überprüfen.

Aufbewahrungsregeln

Wenn Sie ältere Backups automatisch löschen lassen wollen, konfigurieren Sie die Backup-Aufbewahrungsregeln im Schutzplan.

Sie können die Aufbewahrungsregeln auf eine der folgenden Backup-Eigenschaften basieren lassen:

- Nummer
- Alter
- Größe

Die verfügbaren Aufbewahrungsregeln und ihre Optionen hängen vom jeweiligen Backup-Schema ab. Die Regeln sind auch für Agenten, Workloads und Cloud-zu-Cloud-Backups relevant. Weitere Informationen finden Sie im Abschnitt '"Aufbewahrungsregeln je nach Backup-Schema" (S. 478)'.

Sie können die automatische Bereinigung von älteren Backups deaktivieren, indem Sie bei der Konfiguration der Aufbewahrungsregeln die Option **Backups unbegrenzt behalten** aktivieren. Dies kann zu einer erhöhten Speicherbelegung führen, sodass Sie nicht mehr benötigte alte Backups manuell löschen müssen.

Wichtige Tipps

- Aufbewahrungsregeln sind Bestandteil des jeweiligen Schutzplans. Wenn Sie einen Plan widerrufen oder löschen, werden die Aufbewahrungsregeln dieses Plans nicht mehr länger angewendet. Weitere Informationen darüber, wie Sie nicht mehr benötigte Backups löschen können, finden Sie im Abschnitt '"Backups löschen" (S. 584)'.
- Wenn gemäß dem Backup-Schema und Backup-Format jedes Backup als separate Datei gespeichert wird, können Sie ein Backup, von dem noch weitere inkrementelle oder differentielle Backups abhängen, nicht löschen. Dieses Backup wird gemäß den Aufbewahrungsregeln gelöscht, die für die entsprechenden abhängigen Backups gelten. Diese Konfiguration kann zu

einer erhöhten Speicherbelegung führen, weil die Löschung einiger Backups aufgeschoben wird. Es kann daher auch vorkommen, dass die von Ihnen spezifizierten Werte für Backup-Alter, Backup-Größe und Backup-Anzahl überschritten werden. Weitere Informationen darüber, wie Sie dieses Verhalten ändern können, finden Sie im Abschnitt '"Backup-Konsolidierung" (S. 492)'.

- Standardmäßig wird das neueste Backup, das ein Schutzplan erstellt, niemals gelöscht. Wenn Sie jedoch eine Aufbewahrungsregel konfigurieren, damit die Backups vor dem Start einer neuen Backup-Aktion bereinigt werden, und Sie die Anzahl der aufzubewahrenden Backups mit Null festlegen, wird auch das neueste Backup gelöscht.

Warnung!
Wenn Sie diese Aufbewahrungsregel auf einen Backup-Satz mit einem einzelnen Backup anwenden und die Backup-Aktion fehlschlägt, können Sie Ihre Daten nicht mehr wiederherstellen, weil das vorhandene Backup gelöscht wird, bevor ein neues erstellt wird.

Aufbewahrungsregeln je nach Backup-Schema

Die verfügbaren Aufbewahrungsregeln und deren Einstellungen hängen von dem Backup-Schema ab, das Sie im Schutzplan verwenden. Weitere Informationen über die Backup-Schemata finden Sie im Abschnitt '"Backup-Schemata" (S. 458)'.

In der nachfolgenden Tabelle werden die verfügbaren Aufbewahrungsregeln und deren Einstellungen zusammengefasst.

Backup-Schema	Planung	Verfügbare Aufbewahrungsregeln und -Einstellungen
Nur inkrementell (Einzeldatei)	Monatlich Wöchentlich Täglich Stündlich Durch Ereignisse ausgelöste Backups	Nach Backup-Anzahl Nach Backup-Alter (separate Einstellungen für monatliche, wöchentliche, tägliche und stündliche Backups) Backups unbegrenzt aufbewahren
Nur vollständig	Monatlich Wöchentlich Täglich Stündlich Durch Ereignisse ausgelöste Backups	Nach Backup-Anzahl Nach Backup-Alter (separate Einstellungen für monatliche, wöchentliche, tägliche und stündliche Backups) Nach der Gesamtgröße der Backups Backups unbegrenzt aufbewahren
Wöchentlich vollständig, täglich inkrementell	Täglich Durch Ereignisse ausgelöste Backups	Nach Backup-Anzahl Nach Backup-Alter (separate Einstellungen für wöchentliche und tägliche Backups)

Backup-Schema	Planung	Verfügbare Aufbewahrungsregeln und -Einstellungen
		Nach der Gesamtgröße der Backups Backups unbegrenzt aufbewahren
Monatlich vollständig, wöchentlich differentiell, täglich inkrementell	Monatlich Wöchentlich Täglich Stündlich Durch Ereignisse ausgelöste Backups	Nach Backup-Anzahl Nach Backup-Alter (separate Einstellungen für vollständige, differentielle und inkrementelle Backups) Nach der Gesamtgröße der Backups Backups unbegrenzt aufbewahren
Benutzerdefiniert	Monatlich Wöchentlich Täglich Stündlich Durch Ereignisse ausgelöste Backups	Nach Backup-Anzahl Nach Backup-Alter (separate Einstellungen für vollständige, differentielle und inkrementelle Backups) Nach der Gesamtgröße der Backups Backups unbegrenzt aufbewahren

Warum gibt es monatliche Backups bei einem stündlichen Schema?

Je nach Backup-Schema können Sie die Option **Nach Backup-Alter** für eines der folgenden Backups konfigurieren:

- Monatliche, wöchentliche, tägliche und stündliche Backups.
  Diese Einstellungen sind bei allen nicht benutzerdefinierten Backup-Schemata verfügbar und basieren auf zeitlichen Einstellungen. Alle diese Backups (monatlich, wöchentlich, täglich und stündlich) sind verfügbar, auch wenn Sie Ihre Backups so konfigurieren, dass diese stündlich ausgeführt werden. Siehe das nachfolgende Beispiel.

Backup	Beschreibung
Monatlich	Ein monatliches Backup ist das erste Backup, das jeden Monat erstellt wird.
Wöchentlich	Ein wöchentliches Backup ist das erste Backup, das an dem Wochentag erstellt wird, den Sie in der Option Wöchentliches Backup spezifizieren. Dieser Tag wird im Sinne der Aufbewahrungsregeln als Wochenbeginn betrachtet. Wenn ein wöchentliches Backup gleichzeitig das erste Backup des Monats ist, wird es als monatliches Backup betrachtet. In diesem Fall wird ein wöchentliches Backup an dem ausgewählten Tag in der folgenden Woche erstellt.

Backup	Beschreibung
Täglich	Ein tägliches Backup ist das erste Backup eines Tages, es sei denn, dieses Backup fällt unter die Definition eines monatlichen oder wöchentlichen Backups. In diesem Fall wird ein tägliches Backup am folgenden Tag erstellt.
Stündlich	Ein stündliches Backup ist das erste Backup einer Stunde, es sei denn, dieses Backup fällt unter die Definition eines monatlichen, wöchentlichen oder täglichen Backups. In diesem Fall wird ein stündliches Backup in der nächsten Stunde erstellt.

- Vollständige, differentielle und inkrementelle Backups.

  Diese Einstellungen sind für das Backup-Schema **Benutzerdefiniert** verfügbar und hängen von der Backup-Methode ab. Das benutzerdefinierte Schema **Monatlich vollständig, wöchentlich differentiell, täglich inkrementell** ist vorkonfiguriert.

Beispiel

Sie verwenden das Backup-Schema **Nur inkrementell (Einzeldatei)** mit der Standardeinstellung für stündliche Backups:

- Nach Zeit geplant.
- Backups werden stündlich ausgeführt: Montag bis Freitag, jede Stunde, von 08:00 Uhr bis 18:00 Uhr.
- Die Option **Wöchentliches Backup** ist auf Montag festgelegt.

Sie können im Bereich **Aufbewahrungsdauer** des Schutzplans Aufbewahrungsregeln auf monatliche, wöchentliche, tägliche und stündliche Backups anwenden.

In der nachfolgenden Tabelle werden die Backup-Typen zusammengefasst, die in einem Zeitraum von 8 Tagen erstellt werden.

Datum	Wochentag	Beschreibung
1. Juli	Montag	Das erste Backup eines jeden Monats ist monatlich, also ist das erste Backup am heutigen Tag ein monatliches Backup. Die anderen Backups während des Tages sind stündliche. Diese Woche wird das erste Backup als monatliches Backup betrachtet. Deshalb gibt es kein wöchentliches Backup. Das erste Backup in der nächsten Woche wird ein wöchentliches Backup sein.
2. Juli	Dienstag	Das erste Backup ist ein tägliches, die anderen Backups während des Tages sind stündliche.
3. Juli	Mittwoch	Das erste Backup ist ein tägliches, die anderen Backups während des Tages sind stündliche.

Datum	Wochentag	Beschreibung
4. Juli	Donnerstag	Das erste Backup ist ein tägliches, die anderen Backups während des Tages sind stündliche.
5. Juli	Freitag	Das erste Backup ist ein tägliches, die anderen Backups während des Tages sind stündliche.
6. Juli	Samstag	Das erste Backup ist ein tägliches, die anderen Backups während des Tages sind stündliche.
7. Juli	Sonntag	Das erste Backup ist ein tägliches, die anderen Backups während des Tages sind stündliche.
8. Juli	Montag	Das erste Backup ist ein wöchentliches, die anderen Backups während des Tages sind stündliche.

Aufbewahrungsregeln konfigurieren

Die Aufbewahrungsregeln sind Bestandteil eines Schutzplans, wobei ihre Verfügbarkeit und Optionen vom jeweiligen Backup-Schema abhängen. Weitere Informationen finden Sie im Abschnitt '"Aufbewahrungsregeln je nach Backup-Schema" (S. 478)'.

So können Sie die Aufbewahrungsregeln konfigurieren

1. Erweitern Sie im Schutzplan das **Backup**-Modul.
2. Klicken Sie auf **Aufzubewahrende Anzahl**.
3. Wählen Sie eine der folgenden Optionen:
   - **Nach Backup-Anzahl**
   - **Nach Backup-Alter**

     Es sind separate Einstellungen für monatliche, wöchentliche, tägliche und stündliche Backups verfügbar. Der Höchstwert für alle Backup-Typen ist 9999.

     Sie können auch eine einzelne Einstellung für alle Backups verwenden.
   - **Nach der Gesamtgröße der Backups**

     Diese Einstellung ist nicht für das Backup-Schema **Nur inkrementell (Einzeldatei)** verfügbar.
   - **Backups unbegrenzt aufbewahren**
4. [Wenn Sie nicht die Option **Backups unbegrenzt aufbewahren** gewählt haben] Konfigurieren Sie die Werte für die ausgewählte Option.
5. [Wenn Sie nicht die Option **Backups unbegrenzt aufbewahren** gewählt haben] Legen Sie fest, wann die Aufbewahrungsregeln angewendet werden sollen:
   - Nach dem Backup
   - Vor dem Backup

     Diese Option ist beim Backup von Microsoft SQL Server-Clustern oder Microsoft Exchange Server-Clustern nicht verfügbar.

6. Klicken Sie auf **Fertig**.
7. Speichern Sie den Schutzplan.

Replikation

Bei einer Replikation wird jedes neue Backup automatisch zu einem Replikationsspeicherort kopiert. Die Backups am Replikationsspeicherort sind unabhängig von den Backups am Quellspeicherort (was für letztere auch umgekehrt gilt).

Es wird nur das letzte Backup im Quellverzeichnis repliziert. Wenn frühere Backups jedoch nicht repliziert wurden (z.B. aufgrund eines Problems mit der Netzwerkverbindung), werden bei der Replikationsaktion alle Backups berücksichtigt, die nach der letzten erfolgreichen Replikation erstellt wurden.

Wenn eine Replikationsaktion unterbrochen wird, werden die bis dahin verarbeiteten Daten bei der nächsten Replikationsaktion wieder verwendet.

Hinweis
In diesem Thema wird die Replikation als Teil eines Schutzplans beschrieben. Sie können auch einen separaten Backup-Replikationsplan erstellen. Weitere Informationen finden Sie im Abschnitt '"Backup-Replikation" (S. 215)'.

Anwendungsbeispiele

- Zuverlässige Wiederherstellungen sicherstellen

  Speichern Sie Ihre Backups sowohl 'on-site' (lokal, zur sofortigen Wiederherstellung) wie auch 'off-site' (extern, um die Backups vor Ausfall des lokalen Speichers oder natürlichen Desastern zu schützen, die den primären Standort betreffen können).
- Den Cloud Storage nutzen, um Daten vor natürlichen Desastern zu schützen

  Replizieren Sie die Backups zum Cloud Storage, indem lediglich geänderte Daten übertragen werden.
- Nur die jüngsten Recovery-Punkte aufbewahren

  Konfigurieren Sie Aufbewahrungsregeln, um aus Kosteneinsparungsgründen dafür zu sorgen, dass ältere Backups aus einem schnellen Storage gelöscht werden.

Unterstützte Speicherorte

Speicherort	Als Quellspeicherort	Als Replikationsspeicherort
Lokaler Ordner	+	+
Netzwerkordner	+	+
Cloud Storage	-	+

Speicherort	Als Quellspeicherort	Als Replikationsspeicherort
Secure Zone	+	–
Public Cloud	+	+

So können Sie die Replikation aktivieren

1. Erweitern Sie in einem Schutzplan das **Backup**-Modul und klicken Sie anschließend auf **Speicherort hinzufügen**.

   Hinweis
   Die Option **Speicherort hinzufügen** ist nicht verfügbar, wenn Sie den Cloud Storage bei der Option **Backup-Ziel** auswählen.

2. Wählen Sie aus der Liste der verfügbaren Speicherorte den Replikationsspeicherort aus.
   Der Speicherort wird im Schutzplan als **2. Speicherort**, **3. Speicherort**, **4. Speicherort** oder **5. Speicherort** angezeigt, je nachdem, wie viele Speicherorte Sie zur Replikation hinzugefügt haben.
3. [Optional] Klicken Sie auf das Zahnradsymbol, um die Optionen für den Replikationsspeicherort zu konfigurieren.
   - **Performance und Backup-Fenster** – bestimmen Sie das Backup-Fenster für den gewählten Speicherort (wie im Abschnitt '"Performance und Backup-Fenster" (S. 523)' beschrieben). Diese Einstellung bestimmt die Replikations-Performance.
   - **Speicherort entfernen** – löschen Sie den aktuell ausgewählten Speicherort.
   - [Nur für den Cloud Storage] **Physischer Datenversand** – speichern Sie das erste, einleitende Backup auf einem Wechseldatenträger (wie einer externen Festplatte) und versenden Sie es an das Datacenter zum Upload in den Cloud Storage, anstatt es selbst über das Internet zu replizieren.
     Diese Option eignet sich für Speicherorte mit langsamer Netz- bzw. Internetverbindung – oder wenn Sie bei der Übertragung großer Dateien über das Internet Bandbreite sparen wollen. Für die Aktivierung dieser Option sind keine erweiterten Cyber Protect-Service-Quotas erforderlich, aber Sie benötigen eine Quota für den Service 'Physischer Datenversand' (Physical Data Shipping), um einen Versandauftrag erstellen zu können und diesen verfolgen zu können. Siehe Abschnitt '"Physischer Datenversand" (S. 527)'.

     Hinweis
     Diese Option wird mit der Protection Agenten-Version ab Release C21.06 oder höher unterstützt.

4. [Optional] Ändern Sie in der Zeile **Aufzubewahrende Anzahl** unter dem Replikationsspeicherort die Aufbewahrungsregeln für den gewählten Speicherort (wie im Abschnitt '"Aufbewahrungsregeln" (S. 477)' beschrieben).
5. [Optional] Wiederholen Sie die Schritte 1–4, um weitere Replikationsspeicherorte hinzuzufügen.

Sie können bis zu vier Replikationsspeicherorte konfigurieren (**2. Speicherort**, **3. Speicherort**, **4. Speicherort**, und **5. Speicherort**). Wenn Sie **Cloud Storage** wählen, können Sie keine weiteren Replikationsorte hinzufügen.

Wichtig
Wenn Sie Backup und Replikation im selben Schutzplan aktivieren, müssen Sie sicherstellen, dass die Replikation abgeschlossen wird, bevor das nächste geplante Backup ausgeführt wird. Wenn die Replikation noch läuft, wird das geplante Backup nicht gestartet. Beispiel: Ein geplantes Backup, das alle 24 Stunden einmal ausgeführt wird, wird nicht gestartet, wenn es 26 Stunden dauert, bis die Replikation abgeschlossen ist.

Wenn Sie diese Abhängigkeit vermeiden wollen, müssen Sie einen separaten Plan für die Backup-Replikation verwenden. Weitere Informationen zu diesem speziellen Plan finden Sie im Abschnitt '"Backup-Replikation" (S. 215)'.

Verschlüsselung

Der kryptografische AES-Algorithmus (Advanced Encryption Standard) arbeitet im Galois/Counter-Modus (GCM) und verwendet einen zufällig erstellten Schlüssel mit einer benutzerdefinierten Größe von 256 Bit. Der Codierungsschlüssel ist dann mit dem AES-256-Algorithmus verschlüsselt, wobei ein SHA-2-Hash-Wert (256 Bit) des Kennworts als Schlüssel dient. Das Kennwort selbst wird weder auf dem Laufwerk noch in den Backups gespeichert; stattdessen wird der Kennwort-Hash zur Verifikation verwendet.

Mit dieser zweistufigen Methode sind die gesicherten Daten vor unberechtigtem Zugriff geschützt – ein verlorenes Kennwort kann daher auch nicht wiederhergestellt werden.

Hinweis
Die Verwendung des AES-256-Algorithmus mit einem starken Kennwort sorgt für eine quantensichere Verschlüsselung. Es ist sicher gegen kryptoanalytische Angriffe, die sich auf Quantencomputer stützen.

Wir empfehlen Ihnen, alle Backups zu verschlüsseln, die im Cloud Storage gespeichert werden – insbesondere, wenn Ihr Unternehmen gesetzlichen Bestimmungen (zum Datenschutz u. Ä.) unterliegt.

Sie können die Verschlüsselung auf folgende Weise konfigurieren:

- Im Schutzplan
- Als eine Maschineneigenschaft, indem Sie den Cyber Protect Monitor oder die Befehlszeilenschnittstelle verwenden

Die Verschlüsselung im Schutzplan konfigurieren

In einem Schutzplan ist die Verschlüsselung standardmäßig aktiviert. Dabei wird der AES-256-Algorithmus verwendet.

Mit einem starken Kennwort bietet der AES-256-Algorithmus eine quantensichere Verschlüsselung.

Für Konten im Compliance-Modus können Sie die Verschlüsselung im Schutzplan nicht konfigurieren. Weitere Informationen zur Konfiguration der Verschlüsselung auf dem geschützten Gerät finden Sie unter "Verschlüsselung als Maschineneigenschaft konfigurieren" (S. 485).

So können Sie die Verschlüsselung konfigurieren

1. Erweitern Sie in einem Schutzplan das **Backup**-Modul.
2. Klicken Sie bei **Verschlüsselung** auf **Kennwort spezifizieren**.
3. Spezifizieren und bestätigen Sie das Verschlüsselungskennwort.
4. Klicken Sie auf **OK**.

Warnung!
Falls Sie Ihr Kennwort verlieren, gibt es keine Möglichkeit, Ihre verschlüsselten Backups wiederherzustellen!

Sie können die Verschlüsselungseinstellungen nicht mehr ändern, nachdem Sie den Schutzplan angewendet haben. Erstellen Sie einen neuen Plan, wenn Sie andere Verschlüsselungseinstellungen verwenden wollen.

Verschlüsselung als Maschineneigenschaft konfigurieren

Sie können die Backup-Verschlüsselung über die Eigenschaften einer Maschine konfigurieren. In diesem Fall wird die Backup-Verschlüsselung nicht im Schutzplan, sondern auf dem geschützten Workload selbst konfiguriert. Die Verschlüsselung als Eigenschaft einer Maschine nutzt den AES-Algorithmus mit einem 256-Bit-Schlüssel (AES-256).

Hinweis
Die Verwendung des AES-256-Algorithmus mit einem starken Kennwort sorgt für eine quantensichere Verschlüsselung. Es ist sicher gegen kryptoanalytische Angriffe, die sich auf Quantencomputer stützen.

Wenn Sie die Verschlüsselung als Maschineneigenschaft konfigurieren, wirkt sich dies folgendermaßen auf die Schutzpläne aus:

- **Bei Schutzplänen, die bereits auf die Maschine angewendet wurden.** Wenn die Verschlüsselungseinstellungen in einem Schutzplan anders sind, wird das Backup fehlschlagen.
- **Bei Schutzplänen, die später auf die Maschine angewendet werden.** Die auf der Maschine gespeicherten Verschlüsselungseinstellungen überschreiben die Verschlüsselungseinstellungen des Schutzplans. Jedes Backup wird verschlüsselt – selbst dann, wenn die Verschlüsselung in den Backup-Modul-Einstellungen deaktiviert ist.

Für Konten im Compliance-Modus ist nur die Verschlüsselung als Maschineneigenschaft verfügbar.

Wenn Sie mehr als einen Agenten für VMware mit demselben vCenter Server verbunden haben und die Verschlüsselung als Maschineneigenschaft konfigurieren, müssen Sie wegen des Load Balancing

zwischen den Agenten auf allen Maschinen mit dem Agenten für VMware das gleiche Verschlüsselungskennwort verwenden.

Sie können die Verschlüsselung als Maschineneigenschaft auf folgende Arten konfigurieren:

- Über die Befehlszeile
- Über den Cyber Protect Monitor (nur für Windows und macOS verfügbar)

So können Sie die Verschlüsselung konfigurieren

Über die Befehlszeile

1. Melden Sie sich als Administrator (unter Windows) oder als Benutzer 'root' (unter Linux) an.
2. Führen Sie in der Kommandozeile den nachfolgenden Befehl aus:
   - Für Windows:

     ```
     <installation_path>\PyShell\bin\acropsh.exe -m manage_creds --set-password
     <encryption_password>
     ```

     Der standardmäßige Installationspfad ist '`%ProgramFiles%\BackupClient`'.
   - Für Linux:

     ```
     /usr/sbin/acropsh -m manage_creds --set-password <encryption_password>
     ```

   - Für eine virtuelle Appliance:

     ```
      /./sbin/acropsh -m manage_creds --set-password <encryption_password>
     ```

   Warnung!
   Falls Sie Ihr Kennwort verlieren, gibt es keine Möglichkeit, Ihre verschlüsselten Backups wiederherzustellen!

Im Cyber Protect Monitor

1. Melden Sie sich als Administrator an.
2. Klicken Sie im Infobereich der Taskleiste (Windows) oder in der Menüleiste (macOS) auf das Symbol für den Cyber Protect Monitor.
3. Klicken Sie auf das Zahnradsymbol und anschließend auf **Einstellungen** –> **Verschlüsselung**.
4. Wählen Sie den Befehl **Legen Sie ein Kennwort für diese Maschine fest**. Spezifizieren und bestätigen Sie das Verschlüsselungskennwort.
5. Klicken Sie auf **Speichern**.

Warnung!
Falls Sie Ihr Kennwort verlieren, gibt es keine Möglichkeit, Ihre verschlüsselten Backups wiederherzustellen!

So können Sie die Verschlüsselungseinstellungen zurücksetzen

1. Melden Sie sich als Administrator (unter Windows) oder als Benutzer 'root' (unter Linux) an.
2. Führen Sie in der Kommandozeile den nachfolgenden Befehl aus:
   - Für Windows:

     ```
     <installation_path>\PyShell\bin\acropsh.exe -m manage_creds --reset
     ```

     Der standardmäßige Installationspfad ist '`%ProgramFiles%\BackupClient`'.
   - Für Linux:

     ```
     /usr/sbin/acropsh -m manage_creds --reset
     ```

   - Für eine virtuelle Appliance:

     ```
     /./sbin/acropsh -m manage_creds --reset
     ```

Wichtig
Wenn Sie die Verschlüsselung als Maschineneigenschaft zurücksetzen oder das Verschlüsselungskennwort ändern, nachdem ein Schutzplan ein Backup erstellt hat, wird die nächste Backup-Aktion fehlschlagen. Wenn Sie weiterhin den Workload per Backup sichern wollen, müssen Sie einen neuen Schutzplan erstellen.

Beglaubigung (Notarization)

Hinweis
Diese Funktion ist über das Advanced Backup-Paket verfügbar.

Mit der Beglaubigungsfunktion können Sie überprüfen und belegen, ob und dass Ihre gesicherten Dateien seit dem Backup authentisch und unverändert geblieben sind. Wir empfehlen die Nutzung dieser Funktion, wenn Sie wichtige Dateien (wie rechtlich relevante Dokumente) sichern, deren Authentizität Sie später einmal überprüfen wollen/müssen.

Die Beglaubigungsfunktion ist nur für Backups auf Dateiebene verfügbar. Dateien, die über eine digitale Signatur verfügen, werden übersprungen, da diese nicht beglaubigt werden müssen.

Die Beglaubigungsfunktion ist *nicht* verfügbar:

- Wenn das Backup-Format auf **Version 11** festgelegt ist
- Wenn die Secure Zone als Backup-Ziel verwendet wird

So können Sie die Beglaubigungsfunktion verwenden

Um die Beglaubigungsfunktion für alle Dateien, die für ein Backup ausgewählt wurden (ausgenommen Dateien mit digitalen Signaturen), zu aktivieren, müssen Sie beim Erstellen des entsprechenden Schutzplans den Schalter **Beglaubigung (Notarization)** einschalten.

Wenn Sie eine Wiederherstellung konfigurieren, werden die beglaubigten Dateien durch ein spezielles Symbol gekennzeichnet. Das bedeutet, dass Sie die Authentizität dieser Dateien überprüfen können.

Und so funktioniert es

Der Agent berechnet während eines Backups die Hash-Werte der gesicherten Dateien, erstellt einen Hash-Baum (basierend auf der Ordnerstruktur), speichert diesen Hash-Baum mit im Backup und sendet dann das Stammverzeichnis (Root) des Hash-Baums an den Notary Service. Der Notary Service speichert das Wurzelverzeichnis des Hash-Baums in der Blockchain-Datenbank von Ethereum. Damit wird sichergestellt, dass dieser Wert nicht mehr geändert werden kann.

Wenn die Authentizität einer Datei überprüft werden soll, berechnet der Agent den Hash-Wert der Datei und vergleicht diesen dann mit dem Hash-Wert, der im Hash-Baum innerhalb des Backups gespeichert ist. Sollten diese Hash-Werte nicht übereinstimmen, wird die Datei als 'nicht authentisch' eingestuft. Im anderen Fall ist die Authentizität der Datei durch den Hash-Baum verbürgt.

Um zu verifizieren, dass der Hash-Baum selbst nicht kompromittiert wurde, sendet der Agent den Wert des Hash-Baum-Wurzelverzeichnisses an den Notary Service. Der Notary Service vergleicht diesen Wert mit dem, der in der Blockchain-Datenbank gespeichert ist. Wenn die Hash-Werte übereinstimmen, ist die ausgewählte Datei garantiert authentisch. Falls nicht, zeigt die Software über eine Nachricht an, dass die Datei nicht authentisch ist.

Standardoptionen für Backup

Die Standardwerte der Backup-Optionen sind auf der Firmen-, Abteilungs- und Benutzerebene vorhanden. Wenn eine Abteilung oder ein Benutzerkonto innerhalb einer Firma oder innerhalb einer Abteilung erstellt wird, übernimmt sie/es die für die Firma oder Abteilung festgelegten Standardwerte.

Firmenadministratoren, Abteilungsadministratoren und jeder Benutzer ohne Administratorrechte können einen Standardoptionswert gegen einen vordefinierten Wert ersetzen. Der neue Wert wird dann als Vorgabe in allen Schutzpläne verwendet, die nach der Änderung auf der jeweiligen Ebene neu erstellt werden.

Beim Erstellen eines Schutzplans kann ein Benutzer einen Standardwert mit einem benutzerdefinierten Wert überschreiben, welcher dann nur für diesen Plan gilt.

So können Sie einen Standardoptionswert ändern

1. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Um den Standardwert für eine Firma zu ändern, melden Sie sich als Firmenadministrator an der Cyber Protect-Konsole an.
   - Um den Standardwert für eine Abteilung zu ändern, melden Sie sich als ein Administrator für die Abteilung an der Cyber Protect-Konsole an.

- Um den Standardwert für Sie selbst zu ändern, melden Sie sich an der Cyber Protect-Konsole an, indem Sie ein Konto ohne Administratorrechte verwenden.

2. Klicken Sie auf **Einstellungen** –> **Systemeinstellungen**.
3. Erweitern Sie den Bereich **Standardoptionen für Backup**.
4. Wählen Sie die Option aus und führen Sie die benötigten Änderungen durch.
5. Klicken Sie auf **Speichern**.

Backup-Optionen

Wenn Sie die Backup-Optionen eines Schutzplans ändern wollen, müssen Sie im **Backup**-Modul im Feld **Backup-Optionen** auf **Ändern** klicken.

Welche Backup-Optionen verfügbar sind

Art und Umfang der verfügbaren Backup-Optionen sind abhängig von:

- Der Umgebung, in welcher der Agent arbeitet (Windows, Linux, macOS).
- Der Art der zu sichernden Daten (Laufwerke, Dateien, virtuelle Maschinen, Applikationsdaten).
- Dem Backup-Ziel (Cloud Storage, lokaler Ordner, Netzwerkordner).

Die nachfolgende Tabelle fasst die Verfügbarkeit der Backup-Optionen zusammen:

	Backup auf Laufwerksebene			**Backup auf Dateiebene**			**Virtuelle Maschinen**			**SQL und Exchange**
	Windows	**Linux**	**macOS**	**Windows**	**Linux**	**macOS**	**ESXi**	**Hyper-V**	**Virtuozzo**	**Windows**
Alarmmeldungen	+	+	+	+	+	+	+	+	+	+
Backup-Konsolidierung	+	+	+	+	+	+	+	+	+	-
Backup-Dateiname	+	+	+	+	+	+	+	+	+	+
Backup-Format	+	+	+	+	+	+	+	+	+	+
Backup-Validierung	+	+	+	+	+	+	+	+	+	+
CBT (Changed Block Tracking)	+	-	-	-	-	-	+	+	-	-
Cluster-Backup-Modus	-	-	-	-	-	-	-	-	-	+
Komprimierungsgra	+	+	+	+	+	+	+	+	+	+

d										
Fehlerbehandlung										
Erneut versuchen, wenn ein Fehler auftritt	+	+	+	+	+	+	+	+	+	+
Während der Durchführung keine Meldungen bzw. Dialoge anzeigen (Stiller Modus)	+	+	+	+	+	+	+	+	+	+
Fehlerhafte Sektoren ignorieren	+	-	+	+	-	+	+	+	+	-
Erneut versuchen, wenn bei der VM-Snapshot-Erstellung ein Fehler auftritt	-	-	-	-	-	-	+	+	+	-
Schnelles inkrementelles/differentielles Backup	+	+	+	-	-	-	-	-	-	-
Snapshot für Datei-Backups	-	-	-	+	+	+	-	-	-	-
Dateifilter	+	+	+	+	+	+	+	+	+	-
Forensische Daten	+	-	-	-	-	-	-	-	-	-
Protokollabschneidung	-	-	-	-	-	-	+	+	-	Nur SQL
LVM-Snapshot-Erfassung	-	+	-	-	-	-	-	-	-	-
Mount-Punkte	-	-	-	+	-	-	-	-	-	-
Multi-Volume-Snapshot	+	+	-	+	+	-	-	-	-	-
One-Click Recovery	+	+	-	-	-	-	-	-	-	-
Performance und Backup-Fenster	+	+	+	+	+	+	+	+	+	+
Physischer Datenversand	+	+	+	+	+	+	+	+	+	-
Vor-/Nach-Befehle	+	+	+	+	+	+	+	+	+	+

Befehle vor/nach der Datenerfassung	+	+	+	+	+	+	-	-	-	+
Planung										
Startzeiten in einem Zeitfenster verteilen	+	+	+	+	+	+	+	+	+	+
Die Anzahl gleichzeitig ausgeführter Backups begrenzen	-	-	-	-	-	-	+	+	+	-
Sektor-für-Sektor-Backup	+	+	-	-	-	-	+	+	+	-
Aufteilen	+	+	+	+	+	+	+	+	+	+
Task-Fehlerbehandlung	+	+	+	+	+	+	+	+	+	+
Task-Startbedingungen	+	+	-	+	+	-	+	+	+	+
VSS (Volume Shadow Copy Service)	+	-	-	+	-	-	-	+	-	+
VSS (Volume Shadow Copy Service) für virtuelle Maschinen	-	-	-	-	-	-	+	+	-	-
Wöchentliche Backups	+	+	+	+	+	+	+	+	+	+
Windows-Ereignisprotokoll	+	-	-	+	-	-	+	+	-	+

Alarmmeldungen

Keine erfolgreichen Backups für eine spezifizierte Anzahl aufeinanderfolgender Tage

Die Voreinstellung ist: **Deaktiviert**.

Diese Option bestimmt, ob eine Alarmmeldung generiert wird, wenn der Schutzplan innerhalb des spezifizierten Zeitraums kein erfolgreiches Backup durchgeführt hat. Zusätzlich zu fehlgeschlagenen Backups zählt die Software hier auch Backups, die nicht planungsgemäß ausgeführt wurden (verpasste Backups).

Die Alarmmeldungen werden pro Maschine generiert und in der Registerkarte **Alarmmeldungen** angezeigt.

Sie können spezifizieren, ab wie vielen aufeinanderfolgenden Tagen ohne Backups eine Alarmmeldung generiert wird.

Backup-Konsolidierung

Diese Option bestimmt, ob Backups während einer Bereinigung konsolidiert oder komplette Backup-Ketten gelöscht werden sollen.

Die Voreinstellung ist: **Deaktiviert**.

Konsolidierung ist ein Prozess, bei dem zwei oder mehr aufeinander folgende, abhängige Backups zu einem einzelnen Backup kombiniert werden.

Eine Aktivierung dieser Option bewirkt, dass ein Backup, welches während einer Bereinigung gelöscht werden soll, zusammen mit dem nächsten abhängigen Backup (inkrementell oder differentiell) konsolidiert wird.

Bei deaktivierter Option wird das Backup solange aufbewahrt, bis alle abhängigen Backups gelöscht werden. Dieser hilft, die potenziell zeitaufwendige Konsolidierung zu vermeiden, benötigt aber extra Speicherplatz für von der Löschung zurückgestellte Backups. Das Alter oder die Anzahl der Backups kann daher die Werte überschreiten, die in den entsprechenden Aufbewahrungsregeln spezifiziert wurden.

Wichtig
Beachten Sie, dass eine Konsolidierung nur eine bestimmte Art der Datenbereinigung ist, jedoch keine Alternative zu einer richtigen Löschung ist. Das resultierende Backup wird keine Daten enthalten, die im gelöschten Backup vorlagen, die jedoch im aufbewahrten inkrementellen oder differentiellen Backup fehlten.

Diese Option ist *nicht* wirksam, wenn einer der folgenden Umstände zutrifft:

- Der Cloud-Storage wird als Backup-Ziel verwendet.
- Als Backup-Schema wurde **Nur inkrementell (Einzeldatei)** festgelegt.
- Als Backup-Format wurde '**Version 12**' festgelegt.

Backups, die im Cloud Storage gespeichert sind, sowie Backups vom Typ 'Einzeldatei' (mit dem Backup-Format Version 11 oder Version 12) werden immer konsolidiert, da ihre innere Struktur eine schnelle und einfache Konsolidierung ermöglicht.

Wenn jedoch das Backup-Format 'Version 12' verwendet wird und mehrere Backup-Ketten vorliegen (jede Kette wird als separate .tibx-Datei gespeichert), dann funktioniert die Konsolidierung nur innerhalb der letzten Kette. Alle anderen Ketten werden als Ganzes gelöscht, mit Ausnahme der ersten Kette, die auf minimale Größe verkleinert wird, um die Metainformationen zu bewahren (ca. 12 KB). Diese Metainformationen sind erforderlich, um bei gleichzeitigen Lese- und Schreibaktionen für Datenkonsistenz zu sorgen. Die in diesen Ketten enthaltenen Backups verschwinden aus der Benutzeroberfläche, sobald die Aufbewahrungsregel angewendet wird. Diese Backups existieren jedoch physisch solange weiter, bis die gesamte Kette gelöscht wurde.

In allen anderen Fällen werden Backups, deren Löschung verschoben wurde, in der Benutzeroberfläche mit einem Mülleimer-Symbol () gekennzeichnet. Wenn Sie ein solches Backup löschen, indem Sie auf das X-Symbol klicken, wird die Konsolidierung durchgeführt.

Backup-Dateiname

Diese Option definiert die Namen der Backup-Dateien, die vom Schutzplan oder vom Backup-Plan für Cloud-Applikationen erstellt werden.

Für Backup-Dateien, die von Schutzplänen erstellt werden, können Sie diese Namen in einem Dateimanager (wie dem Windows Explorer) einsehen, wenn Sie den Backup-Speicherort durchsuchen.

Was ist ein Backup-Datei?

Jeder Schutzplan erstellt eine oder mehrere Dateien am Backup-Speicherort – abhängig davon, welches Backup-Schema und welches Backup-Format verwendet wird. Die folgende Tabelle listet die Dateien auf, die pro Maschine oder Postfach erstellt werden können.

	Nur inkrementell (Einzeldatei)	**Andere Backup-Schemata**
Backup-Format **Version 11**	Eine TIB-Datei und eine XML-Metadaten-Datei	Mehrere TIB-Dateien und eine XML-Metadaten-Datei
Backup-Format **Version 12**	Eine TIBX-Datei pro Backup-Kette (ein vollständiges oder differentielles Backup und alle davon abhängigen inkrementellen Backups). Wenn die Größe einer Datei, die in einem lokalen Ordner oder einem Netzwerkordner (SMB) gespeichert wurde, 200 GB überschreitet, wird die Datei standardmäßig in Dateien von je 200 GB aufgeteilt.	

Alle Dateien haben den gleichen Namen, mit oder ohne eine Erweiterung um einen Zeitstempel oder eine fortlaufende Nummer (Sequenznummer). Sie können diesen Namen (auch als 'Backup-Dateiname' bezeichnet) festlegen, wenn Sie einen Schutzplan oder einen Backup-Plan für Cloud-Applikationen erstellen oder bearbeiten.

Hinweis
Der Zeitstempel wird nur beim Backup-Format 'Version 11' dem Backup-Dateinamen hinzugefügt.

Wenn Sie einen Backup-Dateinamen in einem Schutzplan oder einem Backup-Plan für Cloud-Applikationen ändern, wird bei der nächsten Ausführung ein Voll-Backup erstellt.

Wenn Sie den Dateinamen eines vorhandenen Backups derselben Maschine spezifizieren, wird – gemäß der vorliegenden Planung – ein vollständiges, ein inkrementelles oder ein differentielles Backup erstellt.

Hinweis
Wenn Sie Backup-Dateien (.tibx) aus ihrem ursprünglichen Storage verschieben, benennen Sie diese nicht um. Umbenannte Dateien werden als beschädigt erscheinen – und Sie werden keine Daten aus diesen wiederherstellen können.

Sie können auch Backup-Dateinamen für Speicherorte festzulegen, die nicht per Datei-Manager durchsuchbar sind (wie etwa der Cloud Storage). Dann können Sie die benutzerdefinierten Namen auf der Registerkarte **Backup Storage** einsehen.

Wo kann ich Backup-Dateinamen einsehen?

Wählen Sie für Schutzpläne auf der Registerkarte **Backup Storage** zuerst den Speicherort und dann das Backup-Archiv aus.

- Der Standard-Backup-Dateiname wird im Fensterbereich **Details** angezeigt.
- Wenn Sie einen eigenen statt dem Standard-Backup-Dateinamen festlegen, wird dieser direkt auf der Registerkarte **Backup Storage** angezeigt (in der Spalte **Name**).

Wählen Sie für Backup-Pläne von Cloud-Applikationen auf der Registerkarte **Backup Storage** zuerst den Speicherort und dann das Backup-Archiv aus und klicken Sie anschließend auf das Zahnradsymbol.

Beschränkungen für Backup-Dateinamen

- Ein Backup-Dateiname darf nicht mit einer Ziffer enden.
  Um beim Standard-Backup-Dateinamen zu verhindern, dass dieser mit einer Zahl enden könnte, wird ihm immer der Buchstabe 'A' angehängt. Wenn Sie einen benutzerdefinierten Namen erstellen, sollten Sie immer überprüfen, dass dieser nicht mit einer Zahl endet. Wenn Sie Variablen verwenden, darf der Name nicht mit einer Variable enden, weil eine Variable selbst wiederum mit einer Zahl enden könnte.
- Ein Backup-Dateiname darf keine der folgenden Symbole enthalten: **()&?*$<>":\|/#**, Zeilenendzeichen (**\n**) und Tabulatorzeichen (**\t**).

Hinweis
Wählen Sie benutzerfreundliche Backup-Dateinamen. Dies erleichtert Ihnen, die Backups zu unterscheiden, wenn Sie den Backup-Speicherort mit einem Datei-Manager (wie dem Windows Explorer) durchsuchen.

Standard-Backup-Dateiname

Der Standarddateiname für Backups von kompletten physischen/virtuellen Maschinen, Laufwerken/Volumes, Dateien/Ordnern, Microsoft SQL Server-Datenbanken, Microsoft Exchange Server-Datenbanken und ESXi-Konfigurationen lautet: `[Machine Name]-[Plan ID]-[Unique ID]A`.

Der Standardname für Backups von Exchange-Postfächern und Microsoft 365-Postfächern, die von einem lokalen Agenten für Microsoft 365 erstellt wurden, lautet: `[Mailbox ID]_mailbox_[Plan ID]A`.

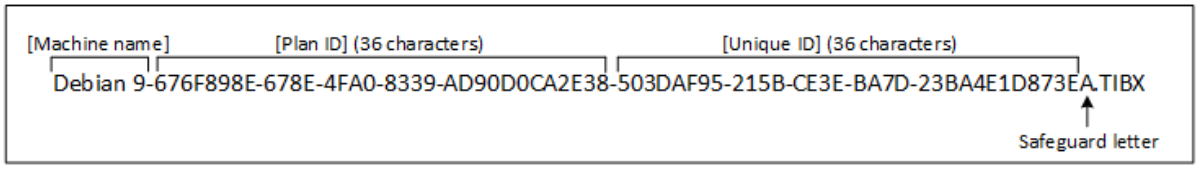
Der Standardname für Microsoft Azure-Backups wird mit dem Präfix `[Mailbox ID]_` versehen. Das Präfix kann nicht entfernt werden.

Der Standardname für Backups von Cloud-Applikationen, die von Cloud Agenten erstellt wurden, lautet: `[Resource Name]_[Resource Type]_[Resource Id]_[Plan Id]A`.

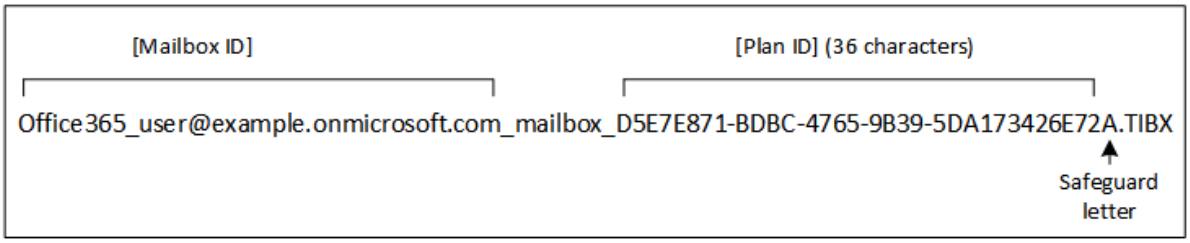
Der Standardname setzt sich aus folgenden Variablen zusammen:

- `[Machine Name]` – Diese Variable wird mit dem Namen der Maschine ersetzt (derselbe Name, der in der Cyber Protect-Konsole angezeigt wird).
- `[Plan ID]`, `[Plan Id]` – Diese Variablen werden durch den eindeutigen Bezeichner (die ID) des Schutzplans ersetzt. Der Wert dieser ID ändert sich auch dann nicht, wenn der Plan umbenannt wird.
- `[Unique ID]` – Diese Variable wird durch den eindeutigen Bezeichner (die ID) der ausgewählten Maschine ersetzt. Der Wert dieser ID ändert sich auch dann nicht, wenn die Maschine umbenannt wird.
- `[Mailbox ID]` – Diese Variable wird durch den UPN (User Principal Name, Benutzerprinzipalnamen) des Postfachs ersetzt.
- `[Resource Name]` – Diese Variable wird durch den Namen der Cloud-Datenquelle ersetzt, wie z.B. den UPN (User Principal Name, Benutzerprinzipalnamen) des Benutzers, die URL der SharePoint-Website oder den Shared Drive-Namen.
- `[Resource Type]` – Diese Variable wird durch den Cloud-Datenquellentyp ersetzt, wie z.B. `mailbox`, `O365Mailbox`, `O365PublicFolder`, `OneDrive`, `SharePoint`, `GDrive`.
- `[Resource ID]` – Diese Variable wird durch den eindeutigen Bezeichner (die ID) der Cloud-Datenquelle ersetzt. Der Wert ändert sich auch dann nicht, wenn die Cloud-Datenquelle umbenannt wird.
- `"A"` – dient als „Schutzbuchstabe“, da dieser an den Namen angehängt wird, um zu verhindern, dass der Dateiname mit einer Zahl endet.

Das untere Diagramm verdeutlicht den Standard-Backup-Dateinamen.



Das untere Diagramm zeigt den Standard-Backup-Dateinamen für Microsoft 365-Postfach-Backups an, die von einem lokalen Agenten erstellt wurden.



Namen ohne Variablen

Die nachfolgenden Beispiele illustrieren, welche finalen Backup-Dateien sich ergeben, wenn Sie für ein Backup den Dateinamen '`MyBackup`' festlegen. Für beide Beispiele wird folgende Backup-Planung angenommen: Die Backup-Erstellung beginnt am 13.09.2016, mit nachfolgenden täglichen inkrementellen Backups um 14:40 Uhr.

Beim Backup-Format 'Version 12' mit dem Backup-Schema **Nur inkrementell (Einzeldatei)**:

```
MyBackup.tibx
```

Beim Backup-Format 'Version 12' mit anderen Backup-Schemata:

```
MyBackup.tibx
MyBackup-0001.tibx
MyBackup-0002.tibx
...
```

Verwendung von Variablen

Neben den standardmäßig verwendeten Variablen können Sie außerdem noch folgende Variablen verwenden:

- Die Variable `[Plan name]`, die durch den Namen des Schutzplans ersetzt wird.
- Die Variable `[Virtualization Server Type]`, die durch 'vmwesx' ersetzt wird, wenn die virtuellen Maschinen durch den Agenten für VMware gesichert werden – oder durch 'mshyperv', wenn die virtuellen Maschinen durch den Agenten für Hyper-V gesichert werden.

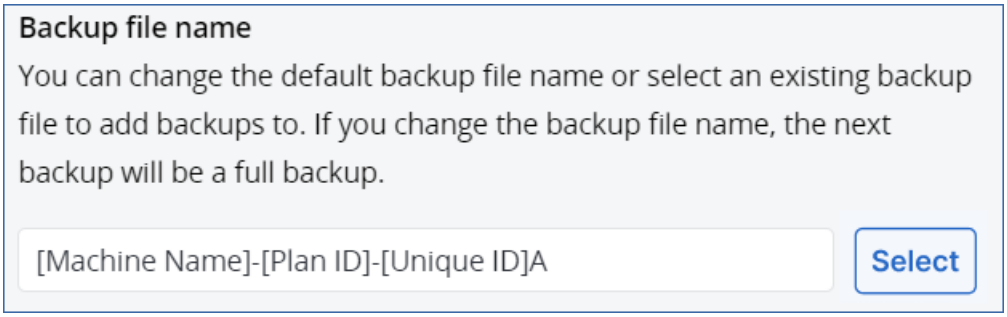
Sind mehrere Maschinen oder Postfächer zum Backup ausgewählt, muss der Backup-Dateiname die Variable `[Machine Name]`, `[Unique ID]`, `[Mailbox ID]`, `[Resource Name]` oder `[Resource Id]`.

Backups in einem vorhandenen Backup-Archiv erstellen

Sie können die Backups eines Workloads so konfigurieren, dass diese einem bestehenden Backup-Archiv hinzugefügt werden.

Diese Option könnte beispielsweise nützlich sein, wenn ein Schutzplan auf eine einzelne Maschine angewendet wird und Sie diese Maschine aus der Cyber Protect-Konsole entfernen oder den Agenten zusammen mit dessen Konfigurationseinstellungen deinstallieren müssen. Nachdem Sie

die Maschine erneut hinzugefügt oder den Agenten erneut installiert haben, können Sie den Schutzplan dazu zwingen, das Backup im ursprünglichen Archiv fortzusetzen.



So können Sie konfigurieren, dass die Backups eines Workloads einem bestehenden Backup-Archiv hinzugefügt werden

Nicht-Cloud-zu-Cloud-Workloads

1. Klicken Sie in der Anzeige **Alle Geräte** auf den Workload und dann auf **Schützen**.
2. Erweitern Sie in den Einstellungen des Schutzplans das **Backup**-Modul.
3. Klicken Sie auf **Backup-Optionen** und dann auf **Ändern**.
4. Klicken Sie in der Registerkarte **Backup-Dateiname** auf **Auswahl**.
   Die Schaltfläche **Auswahl** zeigt die Backups an dem Speicherort an, der im Schutzplan unter **Backup-Ziel** festgelegt wurde.

   Hinweis
   Die Schaltfläche **Auswahl** ist nur bei Schutzplänen verfügbar, die für einen einzelnen Workload erstellt oder auf einen solchen angewendet werden.

5. Wählen Sie ein Archiv aus und klicken Sie dann auf **Fertig**.
6. Klicken Sie auf **Fertig** und dann auf **Anwenden**.

Cloud-zu-Cloud-Workloads

1. Wählen Sie in der Registerkarte **Verwaltung** > **Cloud-Applikationen-Backup** den entsprechenden Plan aus.
2. Klicken Sie zuerst auf **Bearbeiten** und dann auf das Zahnrad-Symbol neben dem Namen des Plans.
3. Klicken Sie auf der Registerkarte **Backup-Dateiname** auf **Auswahl**.

   Hinweis
   Die Schaltfläche **Auswahl** ist nur bei Backup-Plänen verfügbar, die für einen einzelnen Workload erstellt und auf diesen angewendet wurden.

4. Wählen Sie ein Backup-Archiv aus und klicken Sie dann auf **Fertig**.
5. Klicken Sie auf **Fertig** und dann auf **Änderungen speichern**.

Backup-Format

Die Option **Backup-Format** bestimmt das Format der Backups, die vom Schutzplan erstellt werden. Diese Option ist nur für Schutzpläne verfügbar, die bereits das Backup-Format 'Version 11' verwenden. Sie können in diesem Fall das Backup-Format auf 'Version 12' ändern. Wenn Sie das Backup-Format auf 'Version 12' umgestellt haben, ist die Option nicht mehr verfügbar.

- **Version 11**

  Das frühere Format (Legacy-Format), welches aus Gründen der Abwärtskompatibilität beibehalten wurde.

  Hinweis
  Sie können Datenbankverfügbarkeitsgruppen (DAG) nicht im Backup-Format 'Version 11' sichern. Die Sicherung der DAG wird nur im Backup-Format 'Version 12' unterstützt.

- **Version 12**

  Das Backup-Format, das mit Acronis Backup 12 für schnellere Backups und Wiederherstellungen eingeführt wurde. Jede Backup-Kette (ein vollständiges oder differentielles Backup und alle davon abhängigen inkrementellen Backups) wird als einzelne TIBX-Datei gespeichert.

Backup-Format und Backup-Dateien

Bei Backup-Speicherorten, die mit einem Datei-Manager durchsucht werden können (wie etwa lokale Ordner oder Netzwerklaufwerke), bestimmt das Backup-Format die Anzahl der Dateien und ihrer Erweiterung. Die folgende Tabelle listet die Dateien auf, die pro Maschine oder Postfach erstellt werden können.

	Nur inkrementell (Einzeldatei)	**Andere Backup-Schemata**
Backup-Format **Version 11**	Eine TIB-Datei und eine XML-Metadaten-Datei	Mehrere TIB-Dateien und eine XML-Metadaten-Datei
Backup-Format **Version 12**	Eine TIBX-Datei pro Backup-Kette (ein vollständiges oder differentielles Backup und alle davon abhängigen inkrementellen Backups). Wenn die Größe einer Datei, die in einem lokalen Ordner oder einem Netzwerkordner (SMB) gespeichert wurde, 200 GB überschreitet, wird die Datei standardmäßig in Dateien von je 200 GB aufgeteilt.	

Das Backup-Format auf 'Version 12' (TIBX) ändern

Wenn Sie das Backup-Format von 'Version 11' (TIB-Format) zu 'Version 12' (TIBX-Format) ändern, hat dies folgende Auswirkungen:

- Das nächste ausgeführte Backup wird ein Voll-Backup sein.
- Bei Backup-Speicherorten, die mit einem Datei-Manager durchsucht werden können (wie etwa lokale Ordner oder Netzwerklaufwerke), wird eine neue TIBX-Datei erstellt. Die neue Datei übernimmt den Namen der Originaldatei, wird jedoch mit dem Suffix **_v12A** erweitert.
- Aufbewahrungsregeln und Replikationen werden nur auf neue Backups angewendet.
- Die alten Backups werden nicht gelöscht, sondern bleiben über die Registerkarte **Backup Storage** weiter verfügbar. Sie können diese jedoch auch manuell löschen.
- Die alten Cloud Backups werden nicht auf die Quota **Cloud Storage** angerechnet.
- Die alten lokalen Backups werden solange auf die Quota **Lokales Backup** angerechnet, bis diese von Ihnen gelöscht werden.

Archiv-interne Deduplizierung

Das TIBX-Backup-Format 'Version 12' unterstützt eine innerhalb des Archivs erfolgende Deduplizierung (Archiv-interne Deduplizierung), die folgende Vorteile bietet:

- Deutlich reduzierte Backup-Größe, mit integrierter Deduplizierung auf Block-Ebene für jede Art von Daten
- Eine effiziente Handhabung von festen NTFS-Links (Hard Links) stellt sicher, dass es keine Duplikate auf dem Storage gibt
- Hash-basiertes Chunking (Blockerstellung)

Hinweis
Die Archiv-interne Deduplizierung ist standardmäßig für alle Backups im TIBX-Format aktiviert. Sie müssen diese nicht extra in den Backup-Optionen aktivieren – und Sie können sie auch nicht deaktivieren.

Backup-Format-Kompatibilität zwischen verschiedenen Produktversionen

Informationen zur Kompatibilität der Backup-Formate finden Sie im Knowlegde Base-Artikel 'Backup archive compatibility across different product versions (1689)'.

Backup-Validierung

Validierung ist eine Aktion, mit der geprüft wird, ob es grundsätzlich möglich ist, dass Daten, die in einem Backup gespeichert sind, wiederhergestellt werden können. Wenn diese Option aktiviert ist, wird jedes von einem entsprechenden Schutzplan erstellte Backup sofort nach dessen Erstellung mithilfe der Methode 'Prüfsummen-Verifizierung' validiert. Diese Aktion wird vom Protection Agenten durchgeführt.

Die Voreinstellung ist: **Deaktiviert**.

Weitere Informationen zur Validierung mittels Prüfsummen-Verifizierung finden Sie im Abschnitt '"Prüfsummen-Verifizierung" (S. 222)'.

Hinweis
Abhängig von den Einstellungen, die Ihr Service Provider vorgenommen hat, kann es sein, dass keine Validierung verfügbar ist, wenn Sie ein Backup auf dem Cloud Storage erstellen. Die Validierung ist auch nicht für Backup-Standorte in Public Clouds verfügbar.

CBT (Changed Block Tracking)

Diese Option ist für folgende Backups wirksam:

- Laufwerk-Backups von virtuellen Maschinen
- Laufwerk-Backups von physischen Maschinen, die unter Windows laufen
- Backups von Microsoft SQL Server-Datenbanken
- Backups von Microsoft Exchange-Server-Datenbanken

Voreinstellung ist: **Aktiviert**.

Diese Option bestimmt, ob CBT (Changed Block Tracking) verwendet werden soll, wenn ein inkrementelles oder differentielles Backup durchgeführt wird.

CBT ist eine Technologie, mit der Backup-Prozesse beschleunigt werden können. Dabei werden entsprechende Laufwerke oder Datenbanken kontinuierlich auf Blockebene überwacht, ob vorhandene Dateninhalte geändert wurden. Wenn dann ein Backup durchgeführt wird, können die zuvor bereits ermittelten Änderungen direkt im Backup gespeichert werden.

Cluster-Backup-Modus

Hinweis
Diese Funktion ist über das Advanced Backup-Paket verfügbar.

Diese Optionen gelten für Datenbank-Backups von Microsoft SQL Server und Microsoft Exchange Server.

Diese Optionen gelten nur dann, wenn der Cluster selbst (Microsoft SQL Server-AlwaysOn-Verfügbarkeitsgruppe (AAG) oder Microsoft Exchange Server-Datenbankverfügbarkeitsgruppe (DAG)) als Backup-Quelle ausgewählt ist, statt einzelner Knoten oder Datenbanken innerhalb des Clusters. Wenn Sie einzelne Elemente innerhalb des Clusters auswählen, wird das Backup nicht Cluster-konform sein und es werden nur die ausgewählten Kopien der Elemente gesichert.

Microsoft SQL Server

Diese Option bestimmt den Backup-Modus für die SQL Server-AlwaysOn-Verfügbarkeitsgruppen (AAG). Damit diese Option wirksam werden kann, muss der Agent für SQL auf allen entsprechenden AAG-Knoten installiert sein. Weitere Informationen über das Backup von AlwaysOn-Verfügbarkeitsgruppen finden Sie im Abschnitt 'AlwaysOn-Verfügbarkeitsgruppen (AAG) sichern'.

Die Voreinstellung ist: **Sekundäres Replikat, falls möglich.**

Sie können eine der folgenden Varianten wählen:

- **Sekundäres Replikat, falls möglich**
  Falls alle sekundären Replikate offline sind, wird das primäre Replikat gesichert. Eine Sicherung des primären Replikats kann die Performance des SQL Servers ausbremsen, dafür sind die Backup-Daten aber auf dem neuesten Stand.
- **Sekundäres Replikat**
  Falls alle sekundären Replikate offline sind, wird das Backup fehlschlagen. Backups von sekundären Replikaten haben keinen Einfluss auf die SQL Server-Performance und ermöglichen Ihnen, das Backup-Fenster zu erweitern. Passive Replikate können jedoch Informationen enthalten, die nicht mehr aktuell sind, da solche Replikate oft so eingestellt sind, dass sie asynchron (verzögert) aktualisiert werden.
- **Primäres Replikat**
  Falls das primäre Replikat offline ist, wird das Backup fehlschlagen. Eine Sicherung des primären Replikats kann die Performance des SQL Servers ausbremsen, dafür sind die Backup-Daten aber auf dem neuesten Stand.

Unabhängig vom Wert dieser Option und zur Gewährleistung der Datenbankkonsistenz überspringt die Software solche Datenbanken, die sich beim Start des Backups *nicht* im Stadium **SYNCHRONISIERT** oder **WIRD SYNCHRONISIERT** befinden. Falls alle Datenbanken übersprungen werden, schlägt das Backup fehl.

Microsoft Exchange Server

Diese Option bestimmt den Backup-Modus für die Exchange Server-Datenbankverfügbarkeitsgruppen (DAG). Damit diese Option wirksam werden kann, muss der Agent für Exchange auf allen entsprechenden DAG-Knoten installiert sein. Weitere Informationen über das Backup von Datenbankverfügbarkeitsgruppen finden Sie im Abschnitt 'Datenbankverfügbarkeitsgruppen (DAG) sichern'.

Die Voreinstellung ist: **Passive Kopie, falls möglich.**

Sie können eine der folgenden Varianten wählen:

- **Passive Kopie, falls möglich**
  Falls alle passiven Kopien offline sind, wird die aktive Kopie gesichert. Eine Sicherung der aktiven Kopie kann die Performance des Exchange Servers ausbremsen, dafür sind die Backup-Daten aber auf dem neuesten Stand.
- **Passive Kopie**
  Falls alle passiven Kopien offline sind, wird das Backup fehlschlagen. Backups von passiven Kopien haben keinen Einfluss auf die Exchange-Server-Performance und ermöglichen Ihnen, das Backup-Fenster zu erweitern. Passive Kopien können jedoch Informationen enthalten, die nicht mehr aktuell sind, da diese oft so eingestellt sind, dass sie asynchron (verzögert) aktualisiert werden.
- **Aktive Kopie**

Falls die aktive Kopie offline ist, wird das Backup fehlschlagen. Eine Sicherung der aktiven Kopie kann die Performance des Exchange Servers ausbremsen, dafür sind die Backup-Daten aber auf dem neuesten Stand.

Unabhängig vom Wert dieser Option und zur Gewährleistung der Datenbankkonsistenz überspringt die Software solche Datenbanken, die sich beim Start des Backups *nicht* im Stadium **FEHLERFREI** oder **AKTIV** befinden. Falls alle Datenbanken übersprungen werden, schlägt das Backup fehl.

Komprimierungsgrad

Hinweis
Diese Option ist nicht für Cloud-zu-Cloud-Backups verfügbar. Die Komprimierung für diese Backups ist standardmäßig aktiviert und auf einen festen Grad eingestellt, der dem üblichen Komprimierungsgrad **Normal** entspricht.

Diese Option definiert den Grad der Komprimierung für die zu sichernden Daten. Folgende Stufen sind verfügbar: **Ohne**, **Normal**, **Hoch**, **Maximum**.

Die Voreinstellung ist: **Normal**.

Ein höherer Komprimierungsgrad verlängert die Dauer des Backup-Prozesses, verkleinert aber den benötigten Backup-Speicherplatz. Derzeit funktionieren die Komprimierungsgrade **Hoch** und **Maximum** ähnlich.

Der optimale Komprimierungsgrad hängt von der Art der Daten ab, die gesichert werden sollen. So wird z.B. eine maximale Komprimierung die Größe einer Backup-Datei nicht wesentlich beeinflussen, wenn Dateien im Backup erfasst werden, die bereits stark komprimiert sind (wie .jpg-, .pdf- oder .mp3-Dateien). Andere Typen, wie z.B. doc- oder xls-Dateien, werden dagegen stark komprimiert.

Fehlerbehandlung

Mit diesen Optionen können Sie festlegen, wie eventuell auftretende Fehler beim Backup behandelt werden.

Erneut versuchen, wenn ein Fehler auftritt

Die Voreinstellung ist: **Aktiviert. Anzahl der Versuche: 10. Intervall zwischen den Versuchen: 30 Sekunden.**

Wenn ein behebbarer Fehler auftritt, versucht das Programm, die erfolglose Aktion erneut durchzuführen. Sie können das Zeitintervall und die Anzahl der Versuche einstellen. Die Versuche werden aufgegeben, wenn entweder die Aktion erfolgreich ist oder die angegebene Anzahl an Versuchen erreicht wurde, je nachdem, was zuerst eintritt.

Wenn beispielsweise während einer Backup-Ausführung der Zielspeicherort des Backups im Netzwerk plötzlich nicht mehr verfügbar/erreichbar ist, wird die Software versuchen, den Ort alle 30 Sekunden erneut zu erreichen – jedoch nicht mehr als 30 Mal. Die Versuche werden aufgegeben,

wenn entweder die Verbindung gelingt oder die angegebene Zahl der Versuche erreicht ist – je nachdem, was zuerst eintritt.

Wenn das Backup-Ziel jedoch beim Start des Backups nicht verfügbar ist, werden nur 10 Versuche unternommen.

Während der Durchführung keine Meldungen bzw. Dialoge anzeigen (Stiller Modus)

Die Voreinstellung ist: **Aktiviert**.

Wenn der stille Modus eingeschaltet ist, kann das Programm Situationen automatisch behandeln, die eine Benutzeraktion erfordern (außer der Behandlung von fehlerhaften Sektoren, die mit einer eigenen Option gesteuert wird). Falls eine Aktion nicht ohne Benutzereingriff fortfahren kann, wird sie fehlschlagen. Detaillierte Informationen über die Aktion, einschließlich eventueller Fehler, finden Sie im Log der Aktion.

Fehlerhafte Sektoren ignorieren

Die Voreinstellung ist: **Deaktiviert**.

Ist diese Option deaktiviert, dann wird der Backup-Aktivität jedes Mal der Status **Benutzereingriff erforderlich** zugewiesen, wenn das Programm auf einen fehlerhaften Sektor trifft. Wenn Sie z.B. vorhaben, die Informationen von einer 'sterbenden' Festplatte zu retten, aktivieren Sie diese Funktion. Die restlichen Daten werden in diesem Fall noch gesichert und Sie werden das entstandene Laufwerk-Backup mounten und die noch gültigen Daten auf ein anderes Laufwerk kopieren können.

Hinweis
Das Überspringen fehlerhafter Sektoren wird unter Linux nicht unterstützt. Sie können Linux-Systeme mit fehlerhaften Sektoren im Offline-Modus sichern, indem Sie den Bootable Media Builder in der On-Premise-Version von Cyber Protect (lokale Version) verwenden. Für die Verwendung des Bootable Media Builders der On-Premise-Version ist eine separate Lizenz erforderlich. Kontaktieren Sie den Support, um Unterstützung zu erhalten.

Erneut versuchen, wenn bei der VM-Snapshot-Erstellung ein Fehler auftritt

Die Voreinstellung ist: **Aktiviert. Anzahl der Versuche: 3. Intervall zwischen den Versuchen: 5 Minuten.**

Wenn die Snapshot-Erfassung einer virtuellen Maschine fehlschlägt, versucht das Programm, die Aktion zu wiederholen. Sie können das Zeitintervall und die Anzahl der Versuche einstellen. Die Versuche werden aufgegeben, wenn entweder die Aktion erfolgreich ist ODER die angegebene Anzahl an Versuchen erreicht wurde, je nachdem, was zuerst eintritt.

Schnelles inkrementelles/differentielles Backup

Diese Option gilt für inkrementelle und differentielle Backups auf Laufwerksebene.

Diese Option gilt nicht (ist immer deaktiviert) für Volumes, die mit den Dateisystemen JFS, ReiserFS3, ReiserFS4, ReFS oder XFS formatiert sind.

Die Voreinstellung ist: **Aktiviert**.

Inkrementelle oder differentielle Backups erfassen nur jeweils geänderte Daten. Um das Backup-Verfahren zu beschleunigen, ermittelt das Programm, ob eine Datei geändert wurde oder nicht – und zwar anhand von Dateigröße und Zeitstempel der jeweils letzten Änderung. Ist diese Funktion ausgeschaltet, so vergleicht das Programm die Quelldateien und die Dateien, die bereits im Backup gespeichert sind, stattdessen anhand des kompletten Dateiinhaltes.

Dateifilter (Ausschlüsse/Einschlüsse)

Verwenden Sie Dateifiltern um festzulegen, dass nur bestimmte Dateien bzw. Ordner in ein Backup aufgenommen oder von einem Backup ausgeschlossen werden.

Dateifilter stehen, sofern nicht anders angegeben, für Backups auf Maschinen-, Laufwerk- oder Dateiebene zur Verfügung.

Dateifilter sind bei den Dateisystemen XFS, JFS, exFAT und ReiserFS4 nicht verfügbar. Weitere Informationen finden Sie im Abschnitt '"Unterstützte Dateisysteme" (S. 56)'.

Dateifilter können nicht auf dynamische Laufwerke (LVM- oder LDM-Volumes) von virtuellen Maschinen angewendet werden, die im agentenlosen Modus (z.B. von einem Agenten für VMware, einem Agenten für Hyper-V oder einem Agenten für Scale Computing) gesichert werden.

So können Sie Dateifilter aktivieren

1. Erweitern Sie in einem Schutzplan das **Backup**-Modul.
2. Klicken Sie in den **Backup-Optionen** auf den Befehl **Ändern**.
3. Wählen Sie **Dateifilter (Ausschlüsse/Einschlüsse)**.
4. Verwenden Sie eine der nachfolgend beschriebenen Optionen.

Einschluss- und Ausschluss-Filter

Es gibt zwei Arten von Filter – Einschluss- und Ausschlussfilter.

- **Nur Dateien einschließen, die folgende Kriterien erfüllen**

  Wenn Sie `C:\File.exe` im Einschlussfilter spezifizieren, wird ausschließlich diese Datei gesichert – auch wenn Sie ausgewählt haben, dass ein Backup der kompletten Maschine erstellt werden soll.

  Hinweis
  Dieser Filter wird nicht für Backups auf Dateiebene unterstützt, wenn **Version 11** als Backup-Format verwendet wird und das Backup-Ziel nicht der Cloud Storage ist.

- **Dateien ausschließen, die folgende Kriterien erfüllen**

Wenn Sie `C:\File.exe` im Ausschlussfilter spezifizieren, wird diese Datei bei einem Backup übersprungen – auch wenn Sie ausgewählt haben, dass ein Backup der kompletten Maschine erstellt werden soll.

Sie können beide Filter gleichzeitig verwenden. Der Ausschlussfilter hat eine höhere Priorität als der Einschlussfilter – was bedeutet: Wenn Sie `C:\File.exe` in beiden Feldern spezifizieren, wird die Datei beim Backup übersprungen.

Filterkriterien

Sie können Datei- und Ordnernamen, vollständige Pfade zu Dateien und Ordnern sowie Masken mit Platzhalterzeichen (Wildcards) als Filterkriterien verwenden.

Bei den Filterkriterien wird nicht zwischen Groß- und Kleinschreibung unterschieden. Wenn Sie beispielsweise `C:\Temp` spezifizieren, wird sowohl `C:\TEMP` als auch `C:\temp` ausgewählt.

- Name

  Spezifizieren Sie den Namen der Datei oder des Ordners (Beispiel: `Dokument.txt`). Es werden alle Dateien und Ordner mit diesem Namen ausgewählt.
- Vollständiger Pfad

  Spezifizieren Sie den vollständigen Pfad zu der Datei oder dem Ordner, indem Sie mit dem Laufwerksbuchstaben (bei Backups unter Windows) oder dem Stammverzeichnis (bei Backups unter Linux oder macOS) beginnen. Unter Windows, Linux und macOS können Sie normale Schrägstriche verwenden (wie in `C:/Temp/File.tmp`). Unter Windows können Sie zudem den herkömmlichen, nach links geneigten Schrägstrich (Backslash) verwenden (Beispiel: `C:\Temp\File.tmp`).

  Wichtig

  Wenn das Betriebssystem einer gesicherten Maschine während eines Laufwerk-Backups nicht korrekt erkannt wird, funktionieren keine Dateifilter mit vollständigem Pfad. Bei einem Ausschlussfilter wird eine Warnung angezeigt. Wenn ein Einschlussfilter vorhanden ist, wird das Backup fehlschlagen.

  Ein Beispiel für einen vollständigen Dateipfad wäre `C:\Temp\File.tmp`. Ein Filter mit einem vollständigen Pfad, der einen Laufwerksbuchstaben oder ein Stammverzeichnis enthält – zum Beispiel `C:\Temp\File.tmp` oder `C:\Temp\*` – wird zu einer Warnung- oder Fehlermeldung führen.

  Ein Filter, der keinen Laufwerksbuchstaben oder kein Stammverzeichnis verwendet (z.B. `Temp\*` oder `Temp\File.tmp`), oder ein Filter, der mit einem Sternchen (*) beginnt (z.B. `*C:\`), wird keine Warnung- oder Fehlermeldung verursachen. Wenn das Betriebssystem der gesicherten Maschine jedoch nicht korrekt erkannt wird, werden auch diese Filter nicht funktionieren.

- Maske

  Sie können folgende Platzhalterzeichen (Wildcards) für Namen und vollständige Pfade verwenden: Sternchen (*), Doppelsternchen (**) , und Fragezeichen (?).

  Das Sternchen (*), das auch Asterisk genannt wird, steht für keine (null) oder mehr Zeichen. So beinhaltet beispielsweise das Filterkriterium **Doc*.txt** Dateien wie `Doc.txt` und `Document.txt`.

Das Doppelsternchen (**) steht für keine (null) oder mehrere Zeichen, einschließlich des normalen Schrägstrichs. Beispielweise schließt ****/Docs/**.txt** alle .txt-Dateien in allen Unterordnern von allen Ordnern mit der Bezeichnung `Docs` ein. Sie können das Doppelsternchen (**) als Platzhalterzeichen nur für Backups im Format 'Version 12' verwenden.

Das Fragezeichen (?) steht für genau ein beliebiges anderes Zeichen. Beispielsweise schließt **Doc?.txt** Dateien wie `Doc1.txt` und `Docs.txt` ein – während Dateien wie `Doc.txt` oder `Doc11.txt` ausgeschlossen werden.

Snapshot für Datei-Backups

Diese Option gilt nur für Backups auf Dateiebene.

Diese Option definiert, ob die Dateien bei einem Backup nacheinander gesichert oder mithilfe eines einmaligen Daten-Snapshots erfasst werden.

Hinweis
Dateien, die auf Netzwerkfreigaben gespeichert sind, werden immer nacheinander gesichert.

Die Voreinstellung ist:

- Wenn nur Maschinen zum Backup ausgewählt wurden, die unter Linux laufen: **Keinen Snapshot erstellen.**
- Ansonsten: **Snapshot erstellen, sofern möglich.**

Sie können eine der folgenden Optionen wählen:

- **Snapshot erstellen, sofern möglich**
  Dateien direkt sichern, sofern kein Snapshot möglich ist.
- **Snapshot immer erstellen**
  Der Snapshot ermöglicht es, alle Dateien zu sichern – auch solcher, die mit einem exklusiven Zugriff geöffnet sind. Die gesicherten Dateien haben alle den gleichen Backup-Zeitpunkt. Wählen Sie diese Einstellung nur, wenn diese Faktoren kritisch sind, d.h. ein Backup der Dateien ohne den vorhergehenden Snapshot keinen Sinn macht. Wenn kein Snapshot erstellt werden kann, wird das Backup fehlschlagen.
- **Keinen Snapshot erstellen**
  Dateien immer direkt sichern. Der Versuch, Dateien zu sichern, die per exklusivem Zugriff geöffnet sind, führt hier zu einem Fehler. Außerdem ist die Backup-Zeit der Dateien nicht gleich.

Forensische Daten

Schadprogramme (wie Computerviren, Malware oder Ransomware) können bösartige Aktivitäten durchführen, wie etwa Daten zu stehlen oder zu verändern. Diese Aktivitäten müssen möglicherweise untersucht werden, was jedoch nur möglich ist, wenn digitale Beweisdaten verfügbar sind. Es kann jedoch vorkommen, dass Teile der digitalen Beweisdaten (wie z.B. bestimmte Dateien oder Aktivitätsspuren) gelöscht werden – oder dass die Maschine, auf der die schädliche Aktivität stattfand, nicht mehr verfügbar ist.

Backups mit forensischen Daten („Forensik-Backups“) ermöglichen Ermittlern, auch solche Laufwerksbereiche zu untersuchen, die normalerweise in einem herkömmlichen Laufwerk-Backup nicht enthalten sind. Die Backup-Option **Forensische Daten** ermöglicht es Ihnen, folgende digitale Beweisdaten zu sammeln, die dann für forensische Untersuchungen herangezogen werden können: Snapshots von nicht verwendetem Laufwerksspeicherplatz, Speicherabbilder (Memory Dumps) sowie Snapshots von laufenden Prozessen.

Backups mit forensischen Daten werden automatisch digital beglaubigt.

Die Option **Forensische Daten** ist nur für 'Backups der kompletten Maschine' von Windows-Maschinen verfügbar, die mit einem der nachfolgenden Betriebssysteme laufen:

- Windows 8.1, Windows 10
- Windows Server 2012 R2 – Windows Server 2019

Für folgende Maschinen sind keine Backups mit forensischen Daten verfügbar:

- Maschinen, die per VPN mit Ihrem Netzwerk verbunden sind und keinen direkten Zugriff auf das Internet haben
- Maschinen mit Laufwerken, die per BitLocker verschlüsselt sind

Hinweis
Sie können die 'Forensische Daten'-Einstellungen nicht mehr nachträglich ändern, nachdem Sie einen Schutzplan mit aktiviertem **Backup**-Modul auf eine Maschine angewendet haben. Erstellen Sie einen neuen Schutzplan, wenn Sie andere 'Forensische Daten'-Einstellungen verwenden wollen.

Sie können Backups mit forensischen Daten zu folgenden Speicherorten sichern:

- Cloud Storage
- Lokaler Ordner

  Hinweis
  Ein lokaler Ordner als Speicherort wird nur unterstützt, wenn sich dieser auf einer per USB angeschlossenen Festplatte befindet.
  Lokale dynamische Datenträger werden nicht als Speicherort für Forensik-Backups unterstützt.

- Netzwerkordner

Forensik-Backup-Prozess

Bei der Erstellung eines Forensik-Backups werden vom System folgende Aktionen durchgeführt:

1. Es wird ein Speicherabbild im Rohdaten-Format (Raw Memory Dump) sowie eine Liste der laufenden Prozesse erfasst.
2. Die Maschine wird automatisch neu gestartet und mit einem Boot-Medium gebootet.
3. Es wird ein Backup erstellt, in welchem sowohl der belegte als auch der 'nicht zugeordnete' Speicherplatz des Laufwerks enthalten ist.

4. Die gesicherten Laufwerksdaten werden digital beglaubigt.
5. Das Live-Betriebssystem wird neu gebootet und vorhandene Planausführungen werden fortgesetzt (beispielsweise Replikation, Aufbewahrung, Validierung).

So können Sie das Erfassen von forensischen Daten konfigurieren

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte** –> **Alle Geräte**. Alternativ können Sie den Schutzplan auch über die Registerkarte **Verwaltung** erstellen.
2. Wählen Sie das gewünschte Gerät aus und klicken Sie auf **Schützen**.
3. Aktivieren Sie im Schutzplan das **Backup**-Modul.
4. Wählen Sie bei **Backup-Quelle** die Option **Komplette Maschine**.
5. Klicken Sie in den **Backup-Optionen** auf den Befehl **Ändern**.
6. Suchen Sie die Option **Forensische Daten**.
7. Aktivieren Sie die **Forensische Daten sammeln**. Das System wird automatisch ein Speicherabbild (Memory Dump) erfassen und einen Snapshot der laufenden Prozesse erstellen.

   Hinweis
   Ein vollständiges Speicherabbild kann auch sensible Daten wie Kennwörter enthalten.

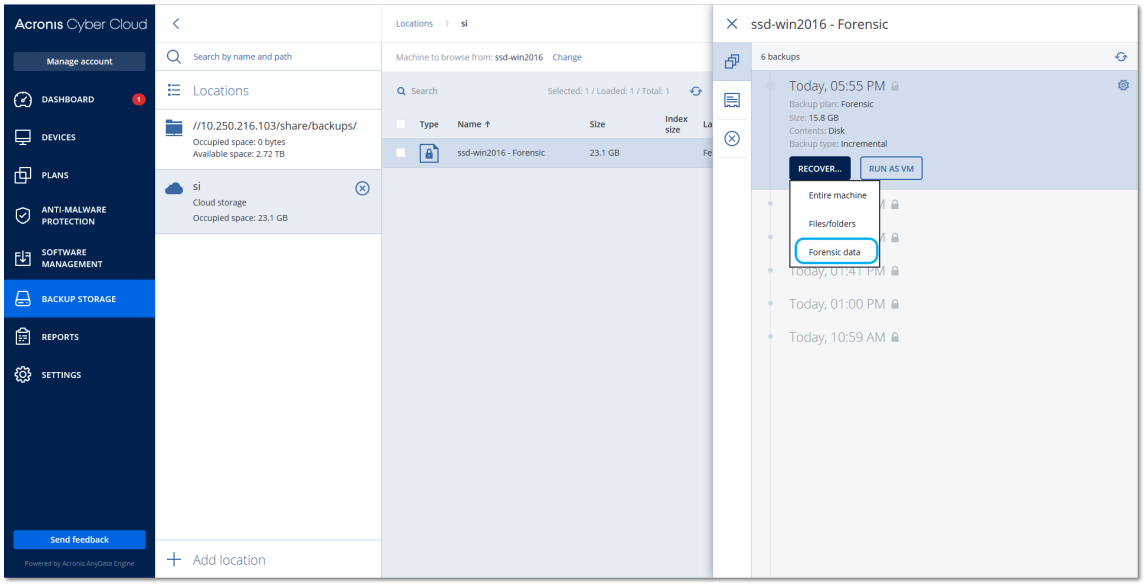
8. Spezifizieren Sie den Speicherort.
9. Klicken Sie auf **Jetzt ausführen**, wenn Sie wollen, dass das Forensik-Backup direkt erstellt wird – oder warten Sie, bis das Backup gemäß seiner Planung ausgeführt wird.
10. Gehen Sie zu **Monitoring** –> **Aktivitäten** und überprüfen Sie, dass das Backup mit den forensischen Daten erfolgreich erstellt wurde.

Als Ergebnis wird das resultierende Backup forensische Daten enthalten, die Sie dann in Ruhe analysieren (lassen) können. Backups mit forensischen Daten sind gekennzeichnet und können daher unter den anderen/allgemeinen Backups (im Bereich **Backup Storage** –> **Speicherorte**) über die Option **Nur mit forensischen Daten** herausgefiltert werden.

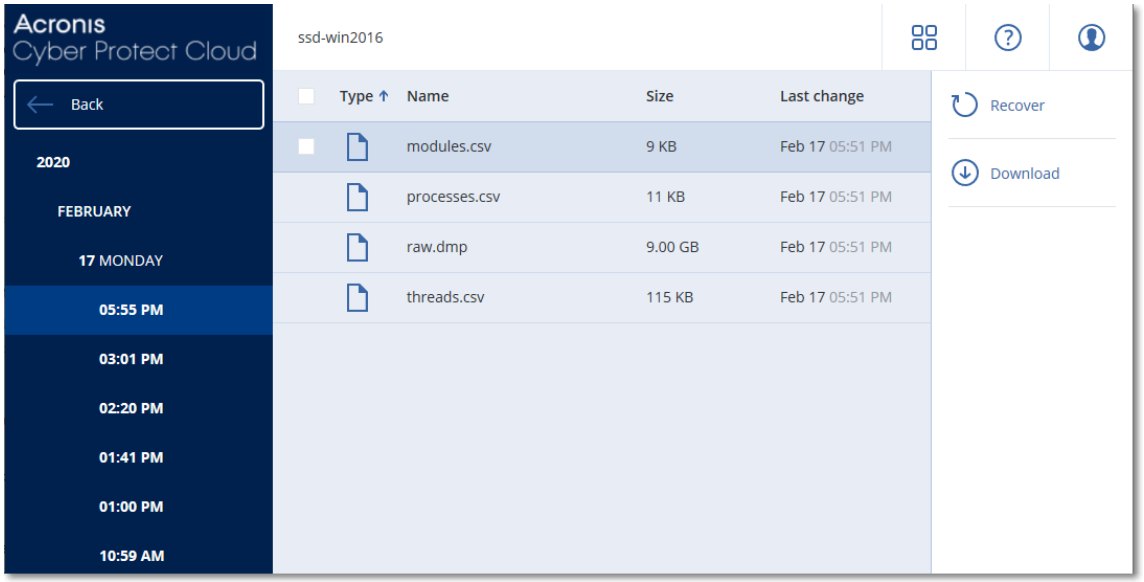
Wie können Sie die forensischen Daten aus einem Backup abrufen?

1. Gehen Sie in der Cyber Protect-Konsole zum Bereich **Backup Storage** und wählen Sie den Speicherort mit den Backups, die forensische Daten enthalten.
2. Wählen Sie das gewünschte Backup mit den forensischen Daten aus und klicken Sie auf **Backups anzeigen**.
3. Klicken Sie auf **Recovery** für das Backup mit den forensischen Daten.

- Wenn Sie nur die forensischen Daten erhalten wollen, klicken Sie auf **Forensische Daten**.



Das System wird einen Ordner mit den forensischen Daten anzeigen. Wählen Sie eine Speicherabbildsdatei oder eine andere forensische Datei aus und klicken Sie dann auf **Download**.



- Klicken Sie auf **Komplette Maschine**, wenn Sie das vollständige Forensik-Backup wiederherstellen wollen. Das System wird das Backup ohne den Boot-Modus wiederherstellen. So können Sie überprüfen, dass das Laufwerk nicht verändert wurde.

Sie können das bereitgestellte Speicherabbild (Memory Dump) für diverse Forensik-Programme von Drittherstellern verwenden. Ein Beispiel ist die Software Volatility Framework (https://www.volatilityfoundation.org/), mit der Sie Speicheranalysen durchführen können.

Beglaubigung von Backups mit forensischen Daten

Um sicherzustellen, dass ein Forensik-Backup wirklich genau dem erfassten Image entspricht und dass dieses nicht kompromittiert wurde, führt das Backup-Modul bei Backups mit forensischen

Daten eine Beglaubigung (Notarization) durch.

Und so funktioniert es

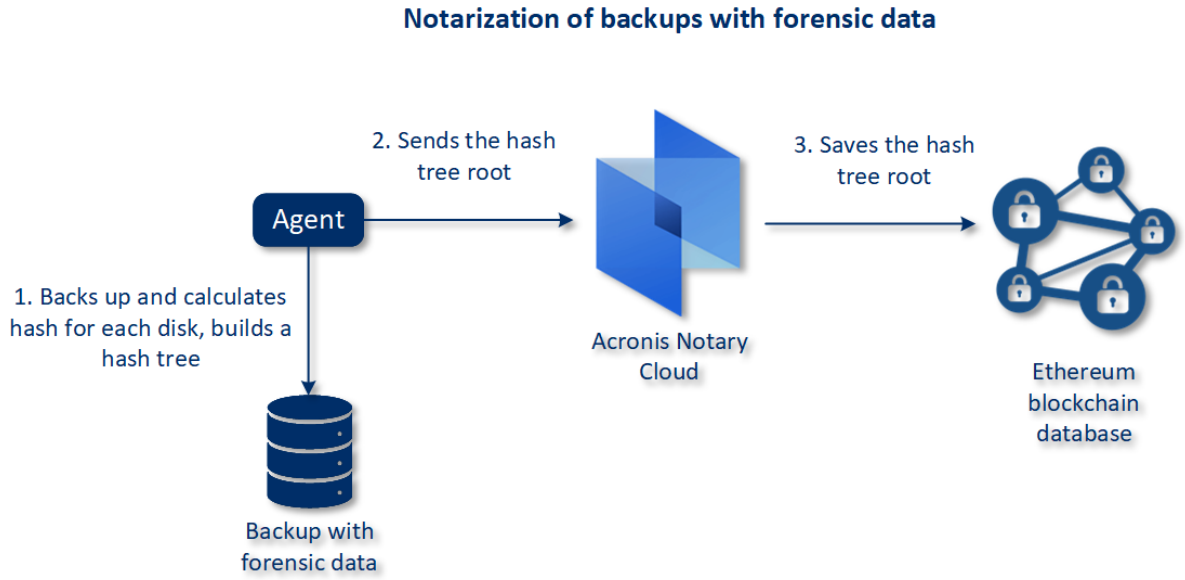
Mit der Beglaubigungsfunktion können Sie überprüfen und belegen, dass ein Laufwerk mit forensischen Daten authentisch ist und die entsprechenden Daten seit der ursprünglichen Backup-Erfassung nicht geändert wurden.

Der Agent berechnet während eines Backups die Hash-Werte der gesicherten Laufwerke, erstellt einen Hash-Baum, speichert diesen Hash-Baum mit im Backup und sendet dann das Stammverzeichnis (Root) des Hash-Baums an den Notary Service. Der Notary Service speichert das Wurzelverzeichnis des Hash-Baums in der Blockchain-Datenbank von Ethereum. Damit wird sichergestellt, dass dieser Wert nicht mehr geändert werden kann.

Wenn die Authentizität des Laufwerks mit den forensischen Daten überprüft werden soll, berechnet der Agent den Hash-Wert des Laufwerks und vergleicht diesen dann mit dem Hash-Wert, der im Hash-Baum innerhalb des Backups gespeichert ist. Sollten diese Hash-Werte nicht übereinstimmen, wird das Laufwerk als 'nicht authentisch' eingestuft. Im anderen Fall ist die Authentizität des Laufwerks durch den Hash-Baum verbürgt.

Um zu verifizieren, dass der Hash-Baum selbst nicht kompromittiert wurde, sendet der Agent den Wert des Hash-Baum-Wurzelverzeichnisses an den Notary Service. Der Notary Service vergleicht diesen Wert mit dem, der in der Blockchain-Datenbank gespeichert ist. Wenn die Hash-Werte übereinstimmen, ist das ausgewählte Laufwerk garantiert authentisch. Falls nicht, zeigt die Software über eine Nachricht an, dass das Laufwerk nicht authentisch ist.

Das untere Schema soll den Beglaubigungsprozess für Backups mit forensischen Daten verdeutlichen.



Wenn Sie das beglaubigte Laufwerk-Backup manuell verifizieren wollen, können Sie dessen Zertifikat abrufen und die mit dem Zertifikat angezeigte Verifizierungsprozedur befolgen (mithilfe des Tools tibxread).

Das Zertifikat für Backups mit forensischen Daten abrufen

Gehen Sie folgendermaßen vor, um das Zertifikat eines Backups mit forensischen Daten von der Konsole aus abzurufen:

1. Gehen Sie zu **Backup Storage** und wählen Sie das gewünschte Backup mit forensischen Daten aus.
2. Stellen Sie die komplette Maschine wieder her.
3. Das System öffnet die Anzeige **Laufwerkszuordnung**.
4. KlickenSie auf das Symbol **Zertifikat abrufen** für das entsprechende Laufwerk.
5. Das System wird das Zertifikat generieren und das Zertifikat in einem neuen Browser-Fenster öffnen. Unter dem Zertifikat wird Ihnen eine Anweisung angezeigt, wie Sie das beglaubigte Laufwerk-Backup manuell verifizieren können.

Das Tool "tibxread" zum Abrufen von Backup-Daten

Cyber Protection stellt ein Tool namens `tibxread` bereit, mit dem Sie die Integrität eines per Backup gesicherten Laufwerks manuell überprüfen können. Mit dem Tool können Sie die Daten aus einem Backup abrufen und den Hash-Wert des entsprechenden Laufwerks berechnen. Das Tool wird automatisch zusammen mit folgenden Komponenten installiert: dem Agenten für Windows, dem Agent für Linux und dem Agenten für Mac.

Der Installationspfad: derselbe Ordner, den auch der Agent verwendet (z.B. `C:\Programme\BackupClient\BackupAndRecovery`).

Folgende Speicherorte werden unterstützt:

- Ein lokales Laufwerk
- Ein Netzwerkordner (CIFS/SMB), auf den ohne Anmeldedaten zugegriffen werden kann.
  Bei einem kennwortgeschützten Netzwerkordner können Sie diesen mithilfe von Betriebssystemtools als lokalen Ordner mounten – und diesen lokalen Ordner dann als Datenquelle für das Tool verwenden.
- Der Cloud Storage
  Sie müssen die URL, den Port und das Zertifikat angeben. Die URL und der Port können aus dem entsprechenden Windows-Registry-Schlüssel oder bei Linux-/Mac-Maschinen aus den entsprechenden Konfigurationsdateien ermittelt werden.
  Für Windows:

```
HKEY_LOCAL_
MACHINE\SOFTWARE\Acronis\BackupAndRecovery\Settings\OnlineBackup\FesAddressCache\Defa
ult\<Mandanten-Anmeldename>\FesUri
```

Für Linux:

```
/etc/Acronis/BackupAndRecovery.config
```

Für MacOS:

```
/Library/Application Support/Acronis/Registry/BackupAndRecovery.config
```

Das Zertifikat kann an folgenden Speicherorten gefunden werden:

Für Windows:

```
%allusersprofile%\Acronis\BackupAndRecovery\OnlineBackup\Default
```

Für Linux:

```
/var/lib/Acronis/BackupAndRecovery/OnlineBackup/Default
```

Für MacOS:

```
/Library/Application Support/Acronis/BackupAndRecovery/OnlineBackup/Default
```

Das Tool verfügt über folgenden Befehle:

- `list backups`
- `list content`
- `get content`
- `calculate hash`

list backups

Listet die Recovery-Punkte in einem Backup auf.

ÜBERSICHT:

```
tibxread list backups --loc=URI --arc=BACKUP_NAME --raw
```

Optionen

```
--loc=URI
--arc=BACKUP_NAME
--raw
--utc
--log=PATH
```

```
Ausgabevorlage:
```

```
GUID   Date   Date timestamp
----   ------ --------------
<guid> <date> <timestamp>
```

<guid> – die GUID eines Backups.

<date> – das Erstellungsdatum des Backups. Das Format ist 'DD.MM.YYYY HH24:MM:SS'. Standardmäßig in der lokalen Zeitzone (kann mit der Option --utc geändert werden).

Ausgabebeispiel:

```
GUID   Date   Date timestamp
----   ------ --------------
516FCE73-5E5A-49EF-B673-A9EACB4093B8 18.12.2019 16:01:05 1576684865
516FCE73-5E5A-49EF-B673-A9EACB4093B9 18.12.2019 16:02:05 1576684925
```

list content

Listet die Inhalte eines Recovery-Punktes auf.

ÜBERSICHT:

```
tibxread list content --loc=URI --arc=BACKUP_NAME --password --backup=RECOVERY_POINT_ID
--raw --log=PATH
```

Optionen

```
--loc=URI
--arc=BACKUP_NAME
--password
--backup=RECOVERY_POINT_ID
--raw
--log=PATH
```

Ausgabevorlage:

```
Disk     Size   Notarization status
-------- ------ --------------------
<number> <size> <notarization_status>
```

<number> – Bezeichner (ID) des Laufwerks.

<size> – Größe in Byte.

<notarization_status> – folgende Statuszustände sind möglich: Ohne Beglaubigung, Beglaubigt, Nächstes Backup.

Ausgabebeispiel:

```
Disk     Size   Notary status
-------- ------ --------------
```

```
1        123123465798 Notarized
2        123123465798 Notarized
```

get content

Schreibt die Inhalte des speziellen Laufwerks im Recovery-Punkt in die Standardausgabe (stdout).

ÜBERSICHT:

```
tibxread get content --loc=URI --arc=BACKUP_NAME --password --backup=RECOVERY_POINT_ID -
-disk=DISK_NUMBER --raw --log=PATH --progress
```

Optionen

```
--loc=URI
--arc=BACKUP_NAME
--password
--backup=RECOVERY_POINT_ID
--disk=DISK_NUMBER
--raw
--log=PATH
--progress
```

calculate hash

Berechnet den Hash-Wert des speziellen Laufwerks im Recovery-Punkt mithilfe des SHA-2-Algorithmus (256 Bit) und schreibt diesen in die Standardausgabe (stdout).

ÜBERSICHT:

```
tibxread calculate hash --loc=URI --arc=BACKUP_NAME --password --backup=RECOVERY_POINT_
ID --disk=DISK_NUMBER --raw --log=PATH --progress
```

Optionen

```
--loc=URI
--arc=BACKUP_NAME
--password
--backup=RECOVERY_POINT_ID
--disk=DISK_NUMBER
--raw
--log=PATH
```

Beschreibung der Optionen

Option	Beschreibung
--arc=BACKUP_NAME	Der Name der Backup-Datei, den Sie über die Backup-Eigenschaften in der Cyber

	Protect-Konsole ermitteln können. Die Backup-Datei muss mit der Erweiterung .tibx spezifiziert werden.
--backup=RECOVERY_POINT_ID	Bezeichner (ID) des Recovery-Punkts.
--disk=DISK_NUMBER	Die Laufwerksnummer (dieselbe, die über den Befehl 'get content' in die Ausgabe geschrieben wurde)

--loc=URI	Der URI des Backup-Speicherortes. Folgende Formate sind für die Option '--loc' möglich:
	• Name des lokalen Pfads (in Windows)
	`c:/upload/backups`
	• Name des lokalen Pfads (in Linux)
	`/var/tmp`
	• SMB/CIFS
	`\\server\ordner`
	• Cloud Storage
	`--loc=<IP_address>:443 --cert=<Pfad_zum_Zertifikat> [--storage_path=/1]`
	`<IP_address>` – Sie können die IP-Adresse unter Windows im folgenden Registry-Schlüssel finden: HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\BackupAndRecovery\Settings\OnlineBackup\FesAddressCache\Default\<Mandanten-Anmeldename>\FesUri
	`<path_to_certificate>` – der Pfad zur Zertifikatsdatei, um auf Cyber Protect Cloud zugreifen zu können. Unter Windows lautet der Pfad für das Zertifikat: `C:\ProgramData\Acronis\BackupAndRecovery\OnlineBackup\Default\<Benutzername>.crt` – wobei <Benutzername> Ihrem Kontonamen entspricht, den Sie für den Zugriff auf Cyber Protect Cloud verwenden.

--log=PATH	Ermöglicht es, die Protokolle (Logs) zu dem spezifizierten Pfad (PATH) schreiben zu lassen (nur lokale Pfade, das Format ist dasselbe wie beim Parameter `--loc=URI`). Der Log-Level ist DEBUG.
--password=PASSWORD	Das Verschlüsselungskennwort für Ihre Backup. Wenn das Backup nicht verschlüsselt ist, lassen Sie diesen Wert einfach leer.

--raw	Blendet die Header (die ersten zwei Zeilen) in der Befehlsausgabe aus. Wird verwendet, wenn die Befehlsausgabe analysiert bzw. weiterverwendet werden soll.
	Ausgabebeispiel ohne '`--raw`':
	`GUID Date Date timestamp`
	`---- ------ --------------`
	`516FCE73-5E5A-49EF-B673-A9EACB4093B8 18.12.2019 16:01:05 1576684865`
	`516FCE73-5E5A-49EF-B673-A9EACB4093B9 18.12.2019 16:02:05 1576684925`
	Ausgabebeispiel mit '`--raw`':

	516FCE73-5E5A-49EF-B673-A9EACB4093B8 18.12.2019 16:01:05 1576684865 516FCE73-5E5A-49EF-B673-A9EACB4093B9 18.12.2019 16:02:05 1576684925
--utc	Zeigt die Zeitangaben im UTC-Format an.
--progress	Zeigt den Fortschritt der Aktion an. Beispiel: 1% 2% 3% 4% ... 100%

Protokollabschneidung

Diese Option gilt für Backups von Microsoft SQL Server-Datenbanken und für Laufwerk-Backups mit aktiviertem Microsoft SQL Server-Applikations-Backup.

Diese Option bestimmt, ob die SQL Server-Transaktionsprotokolle nach einem erfolgreichen Backup abgeschnitten werden.

Die Voreinstellung ist: **Aktiviert**.

Wenn diese Option aktiviert ist, kann eine Datenbank nur auf einen Zeitpunkt zurückgesetzt (wiederhergestellt) werden, zu dem es ein von der Software erstelltes Backup gibt. Deaktivieren Sie diese Option, wenn Sie die Transaktionsprotokolle mithilfe der integrierten Backup-Engine des Microsoft SQL Servers sichern. Sie können die Transaktionsprotokolle nach der Wiederherstellung anwenden – und damit eine Datenbank auf einen beliebigen Zeitpunkt zurücksetzen (wiederherstellen).

LVM-Snapshot-Erfassung

Diese Option gilt nur für physische Maschinen.

Diese Option gilt für Laufwerk-Backups von Volumes, die vom Linux Logical Volume Manager (LVM) verwaltet werden. Solche Volumes werden auch als 'logische Volumes' bezeichnet.

Diese Option definiert, wie der Snapshot eines logischen Volumes erfasst wird. Die Backup-Software kann dies eigenständig tun oder den Linux Logical Volume Manager (LVM) beanspruchen.

Die Voreinstellung ist: **Durch die Backup-Software**.

- **Durch die Backup-Software**. Die Snapshot-Daten werden überwiegend im RAM gehalten. Das Backup ist schneller und es wird kein nicht zugeordneter Speicherplatz auf der Volume-Gruppe benötigt. Wir empfehlen, die Voreinstellung nur dann zu ändern, wenn es zu Problemen beim Backup von logischen Volumes kommt.

- **Durch den LVM**. Der Snapshot wird auf 'nicht zugeordnetem' Speicherplatz der Volume-Gruppe gespeichert. Falls es keinen 'nicht zugeordneten' Speicherplatz gibt, wird der Snapshot durch die Backup-Software erfasst.

Der Snapshot wird nur während der Backup-Aktion verwendet und wird automatisch wieder gelöscht, sobald die Backup-Aktion abgeschlossen wurde. Es werden keine temporären Dateien aufbewahrt.

Mount-Punkte

Diese Option ist nur unter Windows und für ein Datei-basiertes Backup wirksam, dessen Datenquelle gemountete Volumes oder freigegebene Cluster-Volumes enthält.

Diese Option ist nur wirksam, wenn Sie einen Ordner als Backup-Quelle auswählen, der in der Verzeichnishierarchie höher als der Mount-Punkt liegt. (Ein Mount-Punkt ist ein Ordner, an den ein zusätzliches Volume logisch angeschlossen ist).

- Wenn ein solcher Ordner (oder ein übergeordneter Ordner) als Backup-Quelle ausgewählt wird – und die Option **Mount-Punkte** aktiviert wurde – dann werden alle auf dem gemounteten Volume liegenden Dateien in das Backup aufgenommen. Wenn die Option **Mount-Punkte** deaktiviert wurde, bleibt der Mount-Punkt im Backup leer.

  Bei der Wiederherstellung eines übergeordneten Ordners hängt die Frage, ob auch der Inhalt des Mount-Punktes wiederhergestellt wird (oder nicht) davon ab, ob die Option **Mount-Punkte** für die Recovery-Aktion aktiviert oder deaktiviert wurde.
- Wenn Sie den Mount-Punkt direkt auswählen oder einen Ordner innerhalb des gemounteten Volumes, dann werden die gewählten Ordner wie herkömmliche Ordner betrachtet. Sie werden unabhängig vom Status der Backup-Option **Mount-Punkte** gesichert – genauso, wie sie unabhängig vom Status der entsprechenden Recovery-Option **Mount-Punkte** wiederhergestellt werden.

Die Voreinstellung ist: **Deaktiviert**.

Hinweis
Sie können virtuelle Maschinen vom Typ Hyper-V sichern, die auf einem freigegebenen Cluster-Volume liegen, indem Sie die benötigten Dateien oder das komplette Volume per Datei-basiertem Backup sichern. Fahren Sie die virtuellen Maschinen herunter, um zu gewährleisten, dass sie in einem konsistenten Zustand gesichert werden.

Beispiel

Angenommen, der Ordner **C:\Daten1** ist der Mount-Punkt für ein gemountetes Volume. Das Volume enthält die Verzeichnisse **Ordner1** und **Ordner2**. Sie erstellen einen Schutzplan für ein Datei-Backup Ihrer Daten.

Wenn Sie das Volume C per Kontrollkästchen auswählen und dafür die Option **Mount-Punkte** aktivieren, wird der Ordner **C:\Daten1** in Ihrem Backup auch die Verzeichnisse **Ordner1** und

Ordner2 enthalten. Wenn Sie die gesicherten Daten dann später wiederherstellen, sollten Sie an die entsprechende, gewünschte Einstellung der Option **Mount-Punkte** für Recovery-Aktionen denken.

Wenn Sie das Volume C per Kontrollkästchen auswählen und die Option **Mount-Punkte** jedoch deaktivieren, wird der Ordner **C:\Daten1** in Ihrem Backup leer sein.

Wenn Sie die Verzeichnisse **Daten1**, **Ordner1** oder **Ordner2** direkt selbst per Kontrollkästchen zum Backup auswählen, werden diese markierten Ordner wie herkömmliche Ordners in Backup aufgenommen – unabhängig vom Status der Option **Mount-Punkte**.

Multi-Volume-Snapshot

Diese Option gilt nur für Backups von physischen Maschinen, die mit Windows oder Linux laufen.

Diese Option gilt für Laufwerk-Backups. Diese Option gilt auch für Backups auf Dateiebene, wenn diese unter Verwendung eines Snapshots erstellt werden. (Die Option Snapshot für Datei-Backups bestimmt, ob bei einem solchen Backup ein Snapshot benutzt wird oder nicht.)

Diese Option bestimmt, ob die Snapshots bei mehreren Volumes gleichzeitig oder nacheinander erfasst werden sollen.

Die Voreinstellung ist:

- Wenn mindestens eine Maschine, die mit Windows läuft, zum Backup ausgewählt wurde: **Aktiviert**.
- Ansonsten: **Deaktiviert**.

Wenn diese Option aktiviert ist, werden die Snapshots aller zu sichernden Volumes gleichzeitig erstellt. Verwenden Sie diese Option, um ein zeitkonsistentes Backup von Daten zu erstellen, die über mehrere Volumes verteilt sind (z.B. für eine Oracle-Datenbank).

Wenn diese Option deaktiviert ist, werden die Snapshots der Volumes nacheinander erfasst. Falls sich die Daten also über mehrere Volumes erstrecken, werden diese zu unterschiedlichen Zeiten gesichert. Das resultierende Backup ist daher möglicherweise nicht konsistent.

One-Click Recovery

Hinweis
Diese Funktion ist über das Advanced Backup-Paket verfügbar.

Mit One-Click Recovery können Sie automatisch eine Laufwerk-Backup Ihrer Windows- oder Linux-Maschine wiederherstellen. Diess Backup kann das Backup einer kompletten Maschine oder bestimmter Laufwerke bzw. Volumes von dieser Maschine sein.

Die One-Click Recovery-Funktion unterstützt folgende Aktionen:

- Automatische Wiederherstellung aus dem letzten Backup
- Wiederherstellung von einem spezifischen Backup (auch Recovery-Punkt genannt) innerhalb des Backup-Archivs

Die One-Click Recovery-Funktion unterstützt folgende Backup Storages:

- Secure Zone
- Lokaler Ordner
- Netzwerkordner
- Cloud Storage

Wichtig
Setzen Sie die BitLocker-Verschlüsselung aus, bis zum nächsten Neustart Ihres Geräts, wenn Sie eine der folgenden Aktionen durchführen:

- Eine Secure Zone erstellen, ändern oder löschen.
- Den Startup Recovery Manager aktivieren oder deaktivieren.
- [Nur wenn der Startup Recovery Manager nicht bereits aktiviert ist] Wenn Sie das erste Backup ausführen, nachdem Sie im Schutzplan die Option One-Click Restore aktiviert haben. Denn bei dieser Aktion wird der Startup Recovery Manager automatisch aktiviert.
- Startup Recovery Manager aktualisieren, etwa indem Sie den Schutz aktualisieren.

Wenn die BitLocker-Verschlüsselung während dieser Aktionen nicht pausiert wurde, müssen Sie nach dem Neustart Ihres Geräts Ihre BitLocker-PIN angeben.

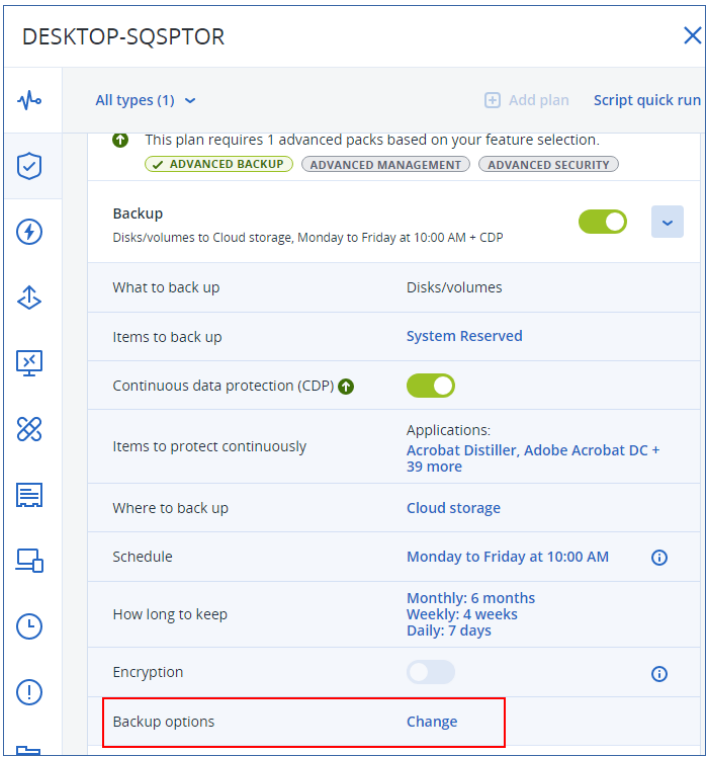
One-Click Recovery aktivieren

One-Click Recovery ist eine Backup-Option im Schutzplan. Für weitere Informationen zur Erstellung eines Plans siehe "Einen Schutzplan erstellen" (S. 232).

Hinweis
Wenn Sie One-Click Recovery aktiviert, wird auf dem Zielcomputer auch Startup Recovery Manager aktiviert. Wenn Startup Recovery Manager nicht aktiviert werden kann, wird die Backup-Aktion, die One-Click-Recovery-Backups erstellt, fehlschlagen. Weitere Informationen dazu Startup Recovery Manager finden Sie unter "Startup Recovery Manager" (S. 801).

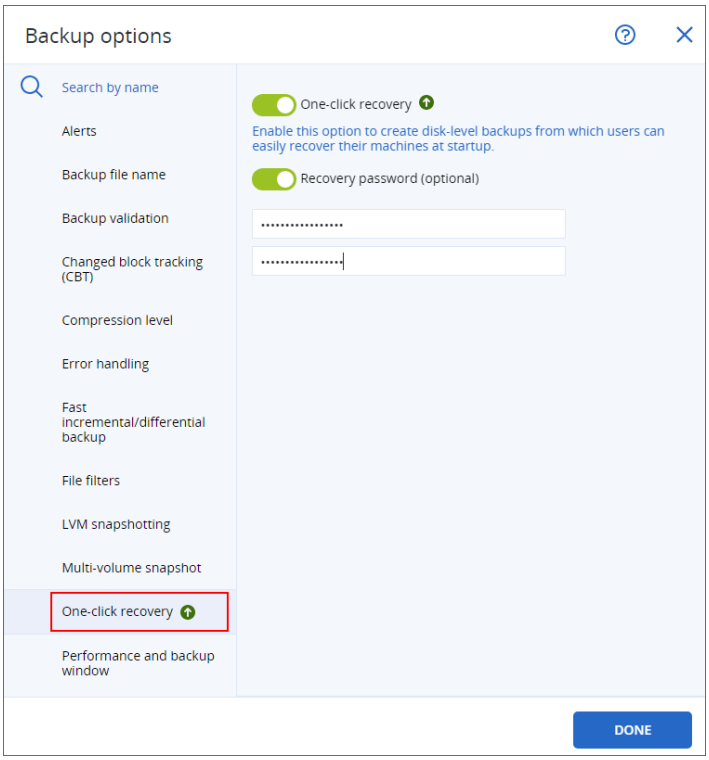
So können Sie One-Click Recovery aktivieren

1. Erweitern Sie im Schutzplan das **Backup**-Modul.
2. Wählen Sie bei **Backup-Quelle** die Option **Komplette Maschine** oder or **Laufwerke/Volumes**.
3. [Wenn Sie die Option **Laufwerke/Volumes** ausgewählt haben]. Spezifizieren Sie bei **Elemente für das Backup** das Laufwerk oder die Volumes, die gesichert werden sollen.
4. Klicken Sie bei **Backup-Optionen** zuerst auf **Ändern** und wählen Sie dann die Option **One-Click Recovery**.



5. Aktivieren Sie den Schalter **One-Click Recovery**.
6. [Optional] Aktivieren Sie den Schalter **Kennwort für die Wiederherstellung** und spezifizieren Sie ein Kennwort.

Wichtig
Wir empfehlen Ihnen dringend, dass Sie ein Kennwort für die Wiederherstellung spezifizieren. Stellen Sie sicher, dass der Anwender, der eine One-Click Recovery-Aktion auf der Zielmaschine durchführen wird, dieses Kennwort kennt.



7. Klicken Sie auf **Fertig**.
8. Konfigurieren Sie die anderen Elemente des Schutzplans nach Ihren jeweiligen Anforderungen und speichern Sie dann den Plan.

Nachdem der Schutzplan ausgeführt wurde und ein Backup erstellt hat, haben die Benutzer der geschützten Maschine Zugriff auf die One-Click Recovery-Möglichkeit.

Wichtig
Die One-Click-Recovery-Funktion ist vorübergehend nicht mehr verfügbar, wenn Sie den Protection Agenten aktualisieren. Wenn Sie die One-Click-Recovery-Funktion wieder aktivieren wollen, müssen Sie ein Backup durchführen. Nach Abschluss des Backups können Sie wieder One-Click-Recovery-Aktionen durchführen.

Die Funktion One-Click Recovery deaktivieren

Sie können die One-Click-Recovery-Funktion für einen bestimmten Workload auf folgende Weisen deaktivieren:

- Deaktivieren Sie die Option **One-Click Recovery** im Schutzplan, der auf den Workload angewendet wurde.
- Widerrufen Sie den Schutzplan, in dem die Option **One-Click Recovery** aktiviert ist.
- Löschen Sie den Schutzplan, in dem die Option **One-Click Recovery** aktiviert ist.

Eine Maschine per One-Click Recovery wiederherstellen

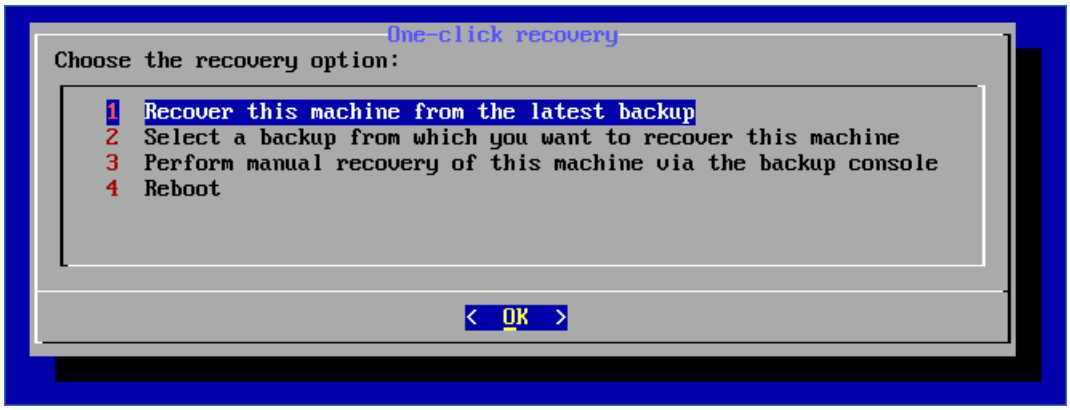
Voraussetzungen

- Es wird ein Schutzplan auf die Maschine angewendet, bei dem die Backup-Option **One-Click Recovery** aktiviert ist.
- Es gibt mindestens ein Laufwerk-Backup der Maschine.

So können Sie eine Maschine wiederherstellen

1. Starten Sie die Maschine neu, die Sie wiederherstellen wollen.
2. Drücken Sie während des Neustarts die Taste F11, um zum Startup Recovery Manager zu gelangen.

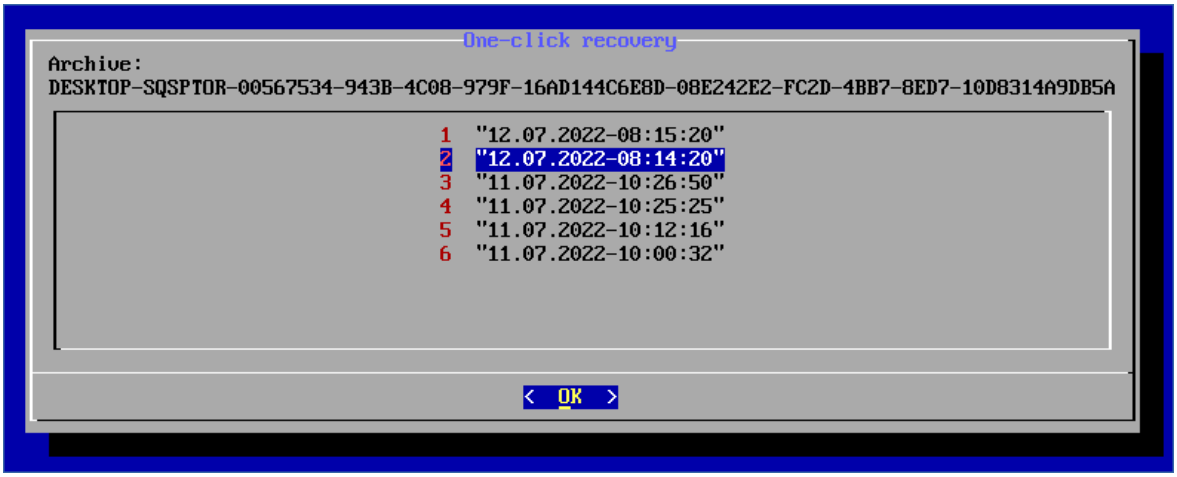
   Das Boot-Medium-Fenster wird geöffnet.
3. Wählen Sie **Acronis Cyber Protect**.
4. [Falls im Schutzplan ein Kennwort für die Wiederherstellung spezifiziert wurde] Geben Sie das Kennwort für die Wiederherstellung ein und klicken Sie anschließend auf **OK**.
5. Wählen Sie eine One-Click Recovery-Option aus.
   - Wenn Sie das letzte (neueste) Backup automatisch wiederherstellen wollen, wählen Sie die erste Option aus und klicken dann auf **OK**.
   - Wenn Sie ein weiteres Backup aus dem Backup-Archiv wiederherstellen wollen, müssen Sie die zweite Option wählen und dann auf **OK** klicken.



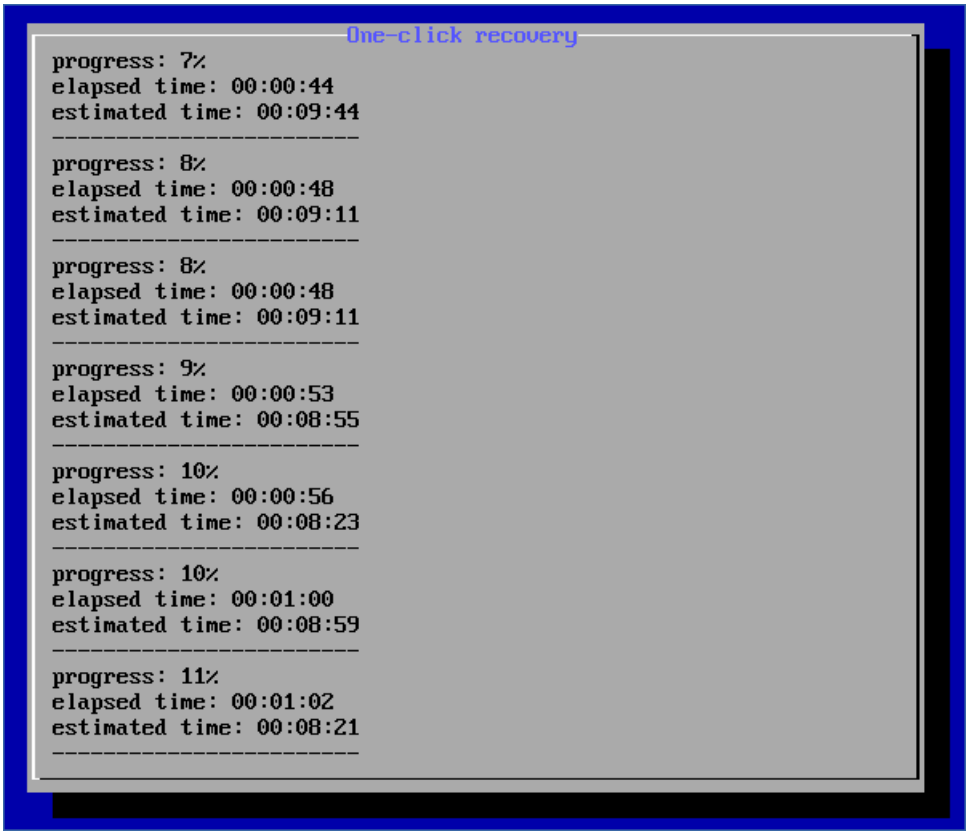
6. Bestätigen Sie Ihre Wahl durch Klicken auf **Ja**.

   Das Boot-Medium-Fenster wird geöffnet und verschwindet dann wieder. Die Recovery-Prozedur wird ohne sie fortgesetzt.
7. [Wenn Sie sich ein bestimmtes Backup wiederherstellen wollen] Wählen Sie das Backup aus, das

Sie wiederherstellen wollen, und klicken Sie dann auf **OK**.



Die Wiederherstellung wird nach einer kurzen Zeit gestartet und dann deren Fortschritt angezeigt. Wenn die Wiederherstellung abgeschlossen wurde, wird Ihre Maschine neu gestartet.



Performance und Backup-Fenster

Mit dieser Option können Sie für jede Stunde innerhalb einer Woche eine von drei Backup-Performance-Stufen (hoch, niedrig, verboten) festlegen. Auf diese Weise können Sie ein Zeitfenster definieren, in dem Backups gestartet und ausgeführt werden dürfen. Die hohen und niedrigen Performane-Stufen sind in Bezug auf Prozesspriorität und Ausgabegeschwindigkeit konfigurierbar.

Diese Option ist nicht verfügbar für Backups, die von Cloud Agenten ausgeführt werden – wie z.B. Website-Backups oder Backups von Servern, die sich auf einer Cloud-Recovery-Site befinden.

Diese Option gilt nur für Backup- und Backup-Replikationsprozesse. 'Nach-Backup'-Befehle und andere Aktionen, die in einem Schutzplan enthalten sind (wie etwa eine Validierung), werden unabhängig von dieser Option ausgeführt.

Voreinstellung ist: **Deaktiviert**.

Wenn diese Option deaktiviert ist, können Backups jederzeit mit folgenden Parametern ausgeführt werden (unabhängig davon, ob die Parameter gegenüber dem Standardwert geändert wurden):

- CPU-Priorität: **Niedrig** (in Windows entspricht dies **Niedriger als normal**)
- Ausgabegeschwindigkeit: **Unbegrenzt**

Wenn diese Option aktiviert ist, werden geplante Backups entsprechend der für die aktuelle Stunde spezifizierten Performance-Parameter zugelassen oder blockiert. Zu Beginn einer Stunde, in der Backups blockiert sind, wird ein Backup-Prozess automatisch angehalten und ein Alarm generiert. Auch wenn geplante Backups blockiert sind, kann ein Backup manuell gestartet werden. Dabei werden die Performance-Parameter der letzten Stunde verwendet, in der Backups erlaubt waren.

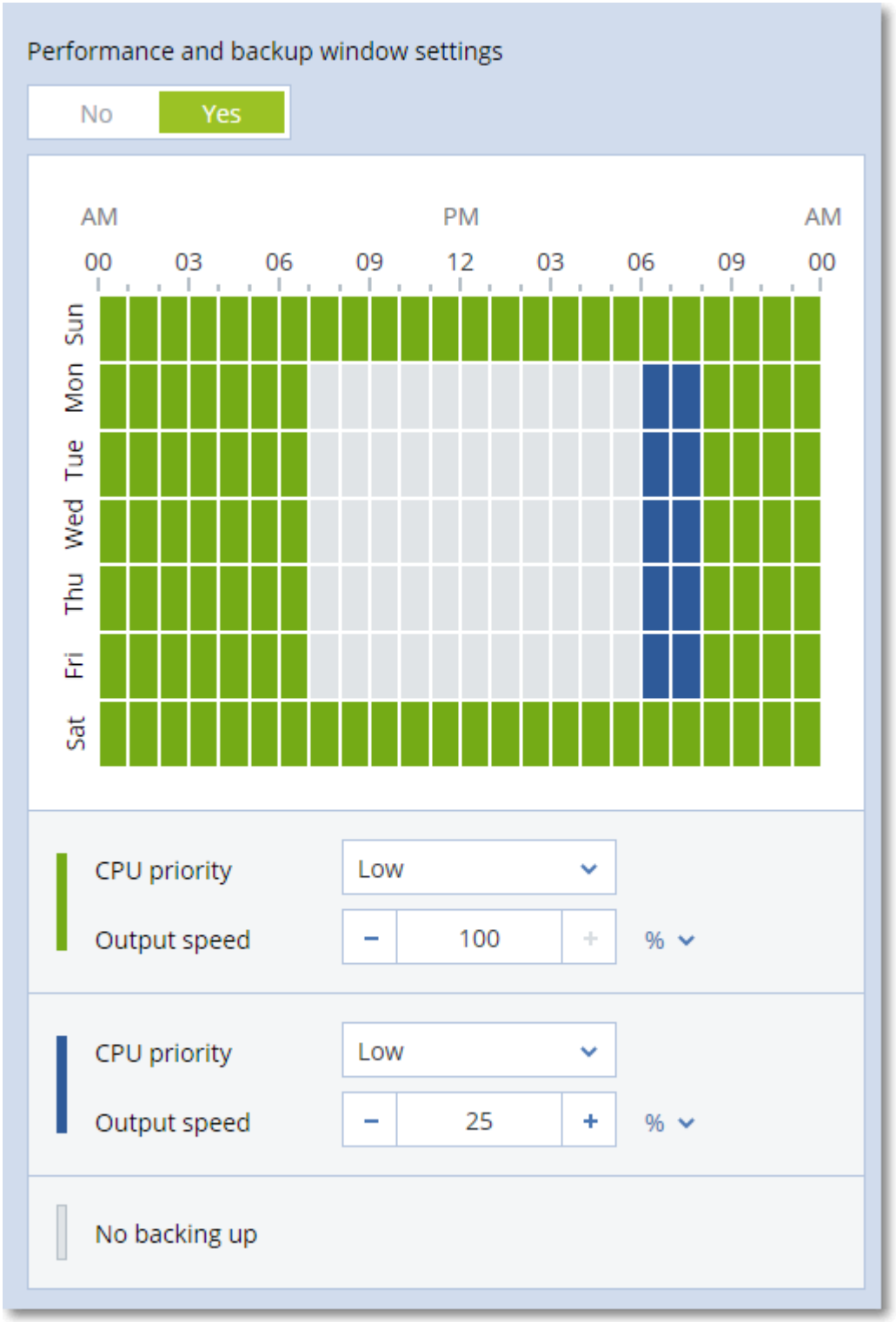
Hinweis
Sie können die Performance und das Backup-Fenster für jeden Replikationsort individuell konfigurieren. Wenn Sie auf die Einstellungen des Replikationsorts zugreifen möchten, klicken Sie im Schutzplan auf das Zahnradsymbol neben dem Namen des Speicherorts und dann auf **Performance und Backup-Fenster**.

Backup-Fenster

Jedes Rechteck repräsentiert eine Stunde innerhalb eines Wochentages. Klicken Sie auf ein Rechteck, um zwischen folgenden Zustände zu wechseln:

- **Grün:** Backup ist mit den Parametern erlaubt, die im unteren grünen Abschnitt spezifiziert sind.
- **Blau:** Backup ist mit den Parametern erlaubt, die im unteren blauen Abschnitt spezifiziert sind. Dieser Zustand ist nicht verfügbar, wenn das Backup-Format auf **Version 11** festgelegt ist.
- **Grau:** Backup ist blockiert.

Sie können mit der Maus klicken und ziehen, um den Zustand mehrerer Rechtecke gleichzeitig zu ändern.



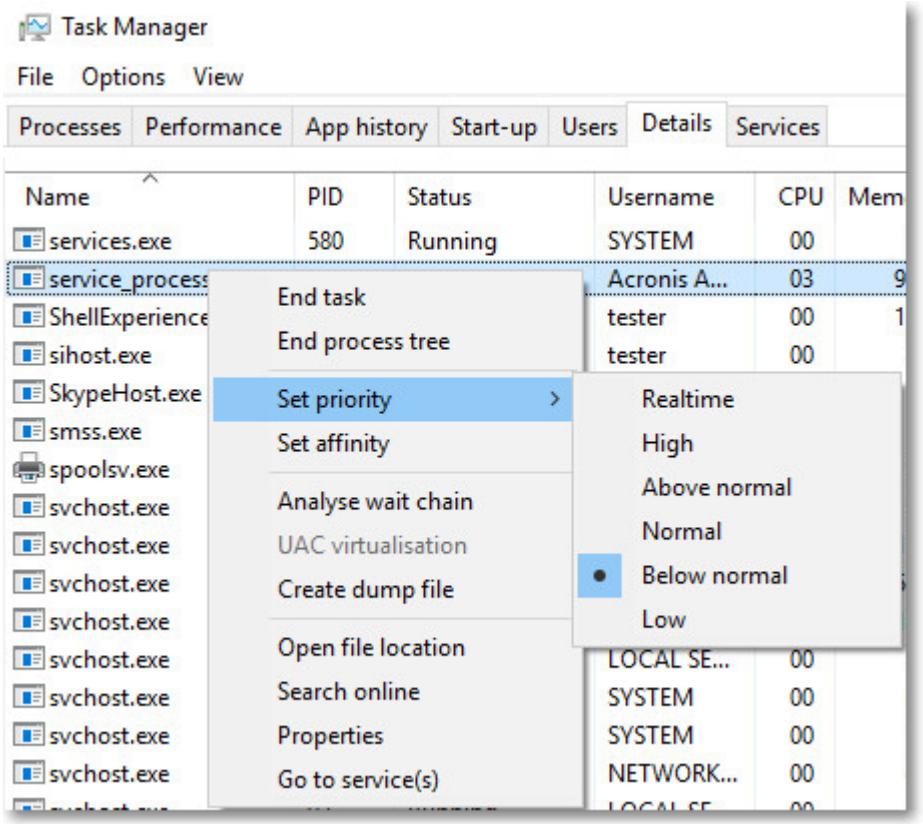
CPU-Priorität

Dieser Parameter bestimmt, welche Priorität dem Backup-Prozess innerhalb des Betriebssystems zugewiesen wird.

Die verfügbaren Einstellungen sind: **Niedrig**, **Normal**, **Hoch**.

Die Priorität eines Prozesses, der in einem System ausgeführt wird, bestimmt, wie viele CPU-und System-Ressourcen ihm zugewiesen werden. Durch das Herabsetzen der Backup-Priorität stehen mehr Ressourcen für andere Applikationen zur Verfügung. Das Heraufsetzen der Backup-Priorität kann den Backup-Prozess beschleunigen, indem z.B. CPU-Ressourcen von anderen gleichzeitig laufenden Prozessen abgezogen werden. Der Effekt ist aber abhängig von der totalen CPU-Auslastung und anderen Faktoren (wie etwa der Schreibgeschwindigkeit der Festplatte oder dem Datenverkehr im Netzwerk).

Diese Option bestimmt die Priorität des Backup-Prozesses (**service_process.exe**) unter Windows und die Priorität ('niceness') des Prozeses (**service_process**) unter Linux und macOS.



Die nachfolgende Tabelle fasst die Zuordnung für diese Einstellung in Windows, Linux und macOS zusammen.

Cyber Protection Priorität	Windows Priorität	Linux und macOS Nettigkeit (Niceness)
Niedrig	Niedriger als normal	10
Normal	Normal	0
Hoch	Hoch	-10

Die Ausgabegeschwindigkeit beim Backup

Mit diesem Parameter können Sie die Geschwindigkeit begrenzen, mit der die Backup-Daten auf die Festplatte geschrieben werden (wenn das Backup-Ziel ein lokaler Ordner ist) – oder mit der die Backup-Daten durch ein Netzwerk übertragen werden (wenn das Backup-Ziel eine Netzwerkfreigabe oder der Cloud Storage ist).

Wenn die Option aktiviert ist, können Sie eine maximal zulässige Ausgabegeschwindigkeit festlegen:

- Als Prozentwert der geschätzten Schreibgeschwindigkeit des Ziellaufwerks (Backup-Ziel ist ein lokaler Ordner) oder als geschätzte maximale Netzwerkverbindungsgeschwindigkeit (Backup-Ziel ist eine Netzwerkfreigabe oder der Cloud Storage).

  Diese Einstellung gilt nur, wenn der Agent unter Windows läuft.
- In KB/Sekunde (für alle Zielorte).

Physischer Datenversand

Diese Option ist verfügbar, wenn das Backup- oder Replikationsziel der Cloud Storage ist und das Backup-Format auf **Version 12** eingestellt ist.

Diese Option gilt für Laufwerk- und Datei-Backups, die von einem Agenten für Windows, Agenten für Linux, Agenten für Mac, Agenten für VMware, Agenten für Hyper-V und Agenten für Virtuozzo erstellt wurden.

Verwenden Sie diese Option, um das erste Voll-Backup, welches durch einen entsprechenden Schutzplan erstellt wurde, mithilfe des Service 'Physischer Datenversand' (Physical Data Shipping) auf einem Festplattenlaufwerk zum Cloud Storage zu senden. Alle dazugehörigen, nachfolgenden inkrementellen Backups können dann über das Netzwerk/Internet durchgeführt werden.

Bei lokalen Backups, die in die Cloud repliziert werden, werden inkrementelle Backups weiter fortgeführt und erst einmal lokal gespeichert, bis das anfängliche Voll-Backup in den Cloud Storage hochgeladen wurde. Dann werden alle inkrementellen Änderungen in die Cloud repliziert und die Replikation gemäß dem Backup-Zeitplan fortgesetzt.

Die Voreinstellung ist: **Deaktiviert.**

Über den Service 'Physische Datenversand'

Die Weboberfläche für den Service 'Physische Datenversand' ist nur für Administratoren verfügbar.

Eine ausführliche Anleitung, wie Sie den Service 'Physischer Datenversand' und das entsprechende Auftragserstellungstool verwenden, finden Sie in der Anleitung für Administratoren zum 'Physischen Datenversand'. Sie können auf dieses Dokument zugreifen, wenn Sie Weboberfläche für den Service 'Physische Datenversand' auf das Fragezeichen-Symbol klicken.

Ein Überblick zum Ablauf des physischen Datenversandes

1. [So können Sie Backups versenden, die den Cloud Storage als primären Speicherort verwenden]
   a. Erstellen Sie einen neuen Schutzplan mit einem Backup in die Cloud.
   b. Klicken Sie in der Zeile **Backup-Optionen** auf den Befehl **Ändern**.
   c. Klicken Sie in der Liste der verfügbaren Optionen auf **Physischer Datenversand**.

   Sie können das Backup direkt auf dem für den Versand verwendeten externen Laufwerk (Wechsellaufwerk) erstellen lassen – oder zuerst in einen lokalen Ordner oder Netzwerkordner speichern und das Backup anschließend auf das Laufwerk kopieren.
2. [So können Sie lokale Backups versenden, die in die Cloud repliziert werden]

   Hinweis
   Diese Option wird mit der Protection Agenten-Version ab Release C21.06 oder höher unterstützt.

   a. Erstellen Sie einen neuen Schutzplan, bei dem das Backup zu einem lokalen oder Netzwerk-Speicherort durchgeführt wird.
   b. Klicken Sie auf **Speicherort hinzufügen** und wählen Sie dort **Cloud Storage**.
   c. Klicken Sie in der Speicherort-Zeile **Cloud Storage** auf das Zahnradsymbol und wählen Sie **Physischer Datenversand**.
3. Klicken Sie bei **Physischen Datenversand verwenden** auf **Ja** und **Fertig**.
   Die Option 'Verschlüsselung' wird automatisch im Schutzplan aktiviert, da alle versendeten Backups verschlüsselt sein müssen.
4. Klicken Sie in der Zeile **Verschlüsselung** auf **Spezifizieren Sie ein Kennwort** und geben Sie dann ein Kennwort für die Verschlüsselung ein.
5. Wählen Sie in der Zeile **Physischer Datenversand** das Wechsellaufwerk (wie eine externe Festplatte) aus, wo das anfängliche Voll-Backup gespeichert werden soll.
6. Klicken Sie auf **Erstellen**, um den Schutzplan zu speichern.
7. Nachdem das anfängliche Backup abgeschlossen wurde, können Sie über die Weboberfläche für den Service 'Physischer Datenversand' das Auftragserstellungstool herunterladen, um mit diesem die Bestellung durchzuführen.
   Sie können auf diese Weboberfläche zugreifen, wenn Sie sich am Management-Portal anmelden. Klicken Sie dort dann zuerst auf **Überblick** –> **Nutzung** – und anschließend unter **Physischer Datenversand** auf den Befehl **Service verwalten**.

   Wichtig
   Wenn das anfängliche Voll-Backup erstellt wurde, müssen alle nachfolgenden Backups weiterhin mit demselben Schutzplan durchgeführt werden. Jeder andere Schutzplan, selbst wenn er die gleichen Parameter und die gleiche Maschine verwenden sollte, benötigt einen neuen/anderen physischen Datenversand.

8. Verpacken Sie das Laufwerk sorgfältig und versenden Sie es dann per Post an das entsprechende Datacenter.

   Wichtig
   Stellen Sie sicher, dass Sie die Verpackungsanweisungen befolgen, wie sie in der Anleitung für Administratoren zum 'Physischen Datenversand' beschrieben sind.

9. Sie können den Auftragsstatus über die Weboberfläche für den Service verfolgen. Beachten Sie, dass alle nachfolgenden Backups solange noch fehlschlagen werden, bis das anfängliche Voll-Backup vom Festplattenlaufwerk in den Cloud Storage hochgeladen wurde.

Vor-/Nach-Befehle

Diese Option ermöglicht die Definition von Befehlen, die automatisch vor oder nach einem Backup durchgeführt werden.

Das folgende Schema zeigt, wann diese Befehle ausgeführt werden.

Befehl vor dem Backup	Backup	'Nach-Backup'-Befehl

So können Sie diese Vor- bzw. Nach-Befehle verwenden:

- Löschen Sie bestimmte temporäre Dateien von der Festplatte, bevor ein Backup gestartet wird.
- Konfiguration Sie das Antivirenprodukt eines Drittanbieters so, dass es vor jedem Start des Backups ausgeführt wird.
- Kopieren Sie Backups selektiv zu einem anderen Speicherort. Diese Option kann nützlich sein, weil die in einem Schutzplan konfigurierte Replikation *jedes* Backup zu den nachfolgenden Speicherorten kopiert.

Der Agent führt die Replikation *nach* Ausführung des Nach-Backup-Befehls aus.

Das Programm unterstützt keine interaktiven Befehle, d.h. Befehle, die eine Reaktion des Benutzers erfordern, wie z.B. 'Pause'.

Befehl vor dem Backup

So spezifizieren Sie einen Befehl bzw. eine Stapelverarbeitungsdatei, die vor dem Start des Backups ausgeführt wird

1. Aktivieren Sie den Schalter **Einen Befehl vor dem Backup ausführen**.
2. Geben Sie im Feld **Befehl** ein Kommando ein oder wählen Sie eine vorbereitete Stapelverarbeitungsdatei aus dem Dateisystem aus. Das Programm unterstützt keine interaktiven Befehle, d.h. Befehle, die eine Reaktion des Benutzers erfordern (wie z.B. 'Pause').
3. Spezifizieren Sie im Eingabefeld **Arbeitsverzeichnis** einen Pfad zu einem Verzeichnis, in dem der Befehl bzw. die Stapelverarbeitungsdatei durchgeführt werden soll.
4. Tragen Sie Argumente für die Befehlsausführung in das Feld **Argumente** ein, wenn das erforderlich ist.

5. Wählen Sie in der unteren Tabelle die passenden Optionen, abhängig vom Ergebnis, das Sie erreichen wollen.
6. Klicken Sie auf **Fertig**.

Kontrollkästchen	**Auswahl**			
Backup scheitern lassen, wenn die Befehlsausführung fehlschlägt*	Ausgewählt	Deaktiviert	Ausgewählt	Deaktiviert
Backup erst ausführen, wenn die Befehlsausführung abgeschlossen ist	Ausgewählt	Ausgewählt	Deaktiviert	Deaktiviert
Ergebnis				
	Voreinstellung Backup nur ausführen, nachdem der Befehl erfolgreich durchgeführt wurde. Backup scheitern lassen, wenn die Befehlsausführung fehlschlägt.	Backup nach Befehlsausführung fortsetzen, unabhängig vom Erfolg oder Misserfolg der Ausführung.	Nicht verfügbar	Backup gleichzeitig mit Befehlsausführung durchführen, unabhängig vom Ergebnis der Befehlssausführung.

* Ein Befehl wird als 'fehlgeschlagen' betrachtet, wenn sein Exit-Code ungleich Null ist.

Hinweis
Wenn ein Skript aufgrund eines Konflikts im Zusammenhang mit einer erforderlichen Bibliotheksversion unter Linux fehlschlägt, schließen Sie die Umgebungsvariablen `LD_LIBRARY_PATH` und `LD_PRELOAD` aus, indem Sie folgende Zeilen in Ihr Skript aufnehmen:

```
#!/bin/sh
unset LD_LIBRARY_PATH
unset LD_PRELOAD
```

'Nach-Backup'-Befehl

So spezifizieren Sie einen Befehl bzw. eine Stapelverarbeitungsdatei, die ausgeführt wird, wenn ein Backup erfolgreich abgeschlossen wurde.

1. Aktivieren Sie den Schalter **Einen Befehl nach dem Backup ausführen**.
2. Geben Sie im Feld **Befehl** ein Kommando ein oder wählen Sie eine vorbereitete Stapelverarbeitungsdatei aus dem Dateisystem aus.
3. Spezifizieren Sie im Eingabefeld **Arbeitsverzeichnis** einen Pfad zu einem Verzeichnis, in dem der Befehl bzw. die Stapelverarbeitungsdatei durchgeführt werden soll.
4. Tragen Sie, sofern erforderlich, in das Feld **Argumente** entsprechende Parameter für die Befehlsausführung ein.
5. Aktivieren Sie das Kontrollkästchen **Backup scheitern lassen, wenn die Befehlsausführung fehlschlägt**, sofern eine erfolgreiche Ausführung des Befehls besonders wichtig für Sie ist. Der Befehl wird als 'fehlgeschlagen' betrachtet, wenn sein Exit-Code ungleich Null ist. Sollte die Befehlsausführung fehlschlagen, erhält der Backup-Status den Wert '**Fehler**'.

   Wenn das Kontrollkästchen deaktiviert ist, hat das Ergebnis der Befehlsausführung keinen Einfluss darauf, ob die Backup-Ausführung als erfolgreich oder fehlgeschlagen eingestuft wird. Sie können das Ergebnis der Befehlsausführung in der Registerkarte **Aktivitäten** überwachen.
6. Klicken Sie auf **Fertig**.

Befehle vor/nach der Datenerfassung

Diese Option ermöglicht die Definition von Befehlen, die automatisch vor oder nach der Datenerfassung (also Erstellung des Daten-Snapshots) ausgeführt werden. Die Datenerfassung wird zu Beginn der Backup-Prozedur durchgeführt.

Das folgende Schema zeigt, wann diese Befehle ausgeführt werden.

	<---------- **Backup** ---------->				
Befehl vor dem Backup	Befehl vor Datenerfassung	Datenerfassung	Befehl nach Datenerfassung	Daten in das Backup-Set schreiben	'Nach-Backup'-Befehl

Interaktion mit anderen Backup-Optionen

Die Ausführung der Befehle vor/nach der Datenerfassung kann durch andere Backup-Optionen verändert werden.

Wenn die Option **Multi-Volume-Snapshot** aktiviert ist, werden die Befehle vor/nach der Datenerfassung nur einmal ausgeführt, weil die Snapshots für alle Volumes gleichzeitig erstellt werden. Wenn die Option **Multi-Volume-Snapshot** deaktiviert ist, werden die Befehle vor/nach der Datenerfassung für jedes Volume, das gesichert wird, einzeln ausgeführt, weil die Snapshots nacheinander erstellt werden.

Wenn die Option **VSS (Volume Shadow Copy Service)** aktiviert ist, werden die Befehle vor/nach der Datenerfassung und die Microsoft VSS-Aktionen folgendermaßen ausgeführt:

Befehle vor der Datenerfassung –> VSS anhalten –> Datenerfassung –> VSS fortsetzen –> Befehle nach Datenerfassung

Mithilfe der Befehle vor/nach der Datenerfassung können Sie Datenbanken, die nicht mit VSS kompatibel sind, vor der Datenerfassung anhalten und nach der Datenerfassung wieder fortsetzen. Da die Datenerfassung nur einige Sekunden benötigt, werden die Datenbanken oder Applikationen nur für kurze Zeit pausiert.

Befehl vor Datenerfassung

So spezifizieren Sie einen Befehl bzw. eine Stapelverarbeitungsdatei, die vor der Datenerfassung ausgeführt wird

1. Aktivieren Sie den Schalter **Einen Befehl vor der Datenerfassung ausführen**.
2. Geben Sie im Feld **Befehl** ein Kommando ein oder wählen Sie eine vorbereitete Stapelverarbeitungsdatei aus dem Dateisystem aus. Das Programm unterstützt keine interaktiven Befehle, d.h. Befehle, die eine Reaktion des Benutzers erfordern (wie z.B. 'Pause').
3. Spezifizieren Sie im Eingabefeld **Arbeitsverzeichnis** einen Pfad zu einem Verzeichnis, in dem der Befehl bzw. die Stapelverarbeitungsdatei durchgeführt werden soll.
4. Tragen Sie Argumente für die Befehlsausführung in das Feld **Argumente** ein, wenn das erforderlich ist.
5. Wählen Sie in der unteren Tabelle die passenden Optionen, abhängig vom Ergebnis, das Sie erreichen wollen.
6. Klicken Sie auf **Fertig**.

Kontrollkästchen	**Auswahl**			
Backup scheitern lassen, wenn die Befehlsausführung fehlschlägt*	Ausgewählt	Deaktiviert	Ausgewählt	Deaktiviert
Datenerfassung erst ausführen, wenn die Befehlsausführung abgeschlossen ist	Ausgewählt	Ausgewählt	Deaktiviert	Deaktiviert
Ergebnis				
	Voreinstellung Datenerfassung nur ausführen, nachdem der Befehl erfolgreich durchgeführt wurde. Backup	Datenerfassung nach Befehlsausführung fortsetzen, unabhängig vom Erfolg oder Misserfolg der	Nicht verfügbar	Datenerfassung gleichzeitig mit Befehlsausführung durchführen, unabhängig vom Ergebnis der Befehlssausführung.

	scheitern lassen, wenn die Befehlsausführung fehlschlägt.	Ausführung.		

* Ein Befehl wird als 'fehlgeschlagen' betrachtet, wenn sein Exit-Code ungleich Null ist.

Hinweis
Wenn ein Skript aufgrund eines Konflikts im Zusammenhang mit einer erforderlichen Bibliotheksversion unter Linux fehlschlägt, schließen Sie die Umgebungsvariablen `LD_LIBRARY_PATH` und `LD_PRELOAD` aus, indem Sie folgende Zeilen in Ihr Skript aufnehmen:

```
#!/bin/sh
unset LD_LIBRARY_PATH
unset LD_PRELOAD
```

Befehl nach Datenerfassung

So spezifizieren Sie einen Befehl bzw. eine Stapelverarbeitungsdatei, die nach der Datenerfassung ausgeführt wird

1. Aktivieren Sie den Schalter **Einen Befehl nach der Datenerfassung ausführen**.
2. Geben Sie im Feld **Befehl** ein Kommando ein oder wählen Sie eine vorbereitete Stapelverarbeitungsdatei aus dem Dateisystem aus. Das Programm unterstützt keine interaktiven Befehle, d.h. Befehle, die eine Reaktion des Benutzers erfordern (wie z.B. 'Pause').
3. Spezifizieren Sie im Eingabefeld **Arbeitsverzeichnis** einen Pfad zu einem Verzeichnis, in dem der Befehl bzw. die Stapelverarbeitungsdatei durchgeführt werden soll.
4. Tragen Sie Argumente für die Befehlsausführung in das Feld **Argumente** ein, wenn das erforderlich ist.
5. Wählen Sie in der unteren Tabelle die passenden Optionen, abhängig vom Ergebnis, das Sie erreichen wollen.
6. Klicken Sie auf **Fertig**.

Kontrollkästchen	**Auswahl**			
Backup scheitern lassen, wenn die Befehlsausführung fehlschlägt*	Ausgewählt	Deaktiviert	Ausgewählt	Deaktiviert
Backup erst ausführen, wenn die Befehlsausführung abgeschlossen ist	Ausgewählt	Ausgewählt	Deaktiviert	Deaktiviert

	Ergebnis			
	Voreinstellung Backup nur fortsetzen, nachdem der Befehl erfolgreich durchgeführt wurde.	Backup nach Befehlsausführung fortsetzen, unabhängig vom Erfolg oder Misserfolg der Ausführung.	Nicht verfügbar	Backup gleichzeitig mit Befehlsausführung fortsetzen, unabhängig vom Ergebnis der Befehlssausführung.

***** Ein Befehl wird als 'fehlgeschlagen' betrachtet, wenn sein Exit-Code ungleich Null ist.

Planung

Mit dieser Option können Sie festlegen, ob Backups genau nach Planung oder mit einer Verzögerung starten sollen – und wie viele virtuelle Maschinen gleichzeitig gesichert werden.

Weitere Informationen über die Konfiguration einer Backup-Planung finden Sie im Abschnitt '"Ein Backup nach Planung ausführen" (S. 461)'.

Die Voreinstellung ist: **Backup-Startzeiten in einem Zeitfenster verteilen**. **Maximale Verzögerung**: **30 Minuten**.

Sie können eine der folgenden Optionen wählen:

- **Alle Backups genau nach Planung starten**
  Die Backups von physischen Maschinen werden wie im Plan definiert gestartet. Virtuelle Maschinen werden nacheinander gesichert.
- **Startzeiten in einem Zeitfenster verteilen**
  Die Backups von physischen Maschinen werden mit einer Verzögerung (bezogen auf die geplante Zeit) gestartet. Der Verzögerungswert für jede Maschine wird zufällig bestimmt und reicht von Null bis einem maximalen, von Ihnen spezifizierten Wert. Sie können diese Einstellung bei Bedarf verwenden, wenn Sie mehrere Maschinen per Backup zu einem Netzwerkspeicherort sichern, um eine übermäßige Netzwerklast zu vermeiden. Der Verzögerungswert für jede Maschinen wird bestimmt, wenn der Schutzplan auf die Maschine angewendet wird – und er bleibt so lange gleich, bis Sie den Schutzplan erneut bearbeiten und den maximalen Verzögerungswert ändern.
  Virtuelle Maschinen werden nacheinander gesichert.
- **Die Anzahl gleichzeitig ausgeführter Backups begrenzen**
  Verwenden Sie diese Option, um parallele Backups von virtuellen Maschinen zu verwalten, die auf Hypervisor-Ebene gesichert werden (mit einem agentenlosen Backup).
  Schutzpläne, bei denen diese Option ausgewählt ist, können zusammen mit anderen Schutzplänen ausgeführt werden, sofern diese gleichzeitig von demselben Agenten durchgeführt werden. Wenn Sie diese Option auswählen, müssen Sie die Anzahl der parallelen Backups pro Plan spezifizieren. Die Gesamtzahl der Maschinen, die von allen Plänen gleichzeitig gesichert werden können, ist auf 10 pro Agent begrenzt. Informationen darüber, wie Sie die

Standardbegrenzung ändern können, finden Sie im Abschnitt '"Die Gesamtzahl der gleichzeitig gesicherten virtuellen Maschinen begrenzen" (S. 770)'.

Bei Schutzplänen, in denen diese Option deaktiviert ist, werden die Backup-Aktionen nacheinander durchgeführt, also eine virtuelle Maschine nach der anderen.

Sektor-für-Sektor-Backup

Die Option gilt nur für Backups auf Laufwerksebene.

Diese Option definiert, ob von einem Laufwerk/Volume eine exakte Kopie auf physischer Ebene erstellt werden soll.

Die Voreinstellung ist: **Deaktiviert**.

Wenn diese Option aktiviert ist, werden beim Backup eines Laufwerks/Volumes alle vorhandenen Sektoren gesichert – einschließlich der Sektoren von 'nicht zugeordnetem' und 'freiem' Speicherplatz. Das resultierende Backup wird die gleiche Größe wie das gesicherte Laufwerk haben (sofern die Option 'Komprimierungsgrad' auf **Ohne** eingestellt ist). Die Software schaltet automatisch auf den Sektor-für-Sektor-Modus um, wenn ein Laufwerk ein Dateisystem verwendet, welches nicht erkannt oder nicht unterstützt wird.

Hinweis
Es wird unmöglich sein, eine Wiederherstellung der Anwendungsdaten aus den Backups durchzuführen, die im Sektor-für-Sektor-Modus erstellt wurden.

Aufteilen

Mit dieser Option können Sie festlegen, ob und wie große Backups in kleinere Dateien aufgeteilt werden sollen.

Hinweis
Die Möglichkeit zur Backu-Aufteilung ist bei Schutzplänen, die den Cloud Storage als Backup-Speicherort verwenden, nicht verfügbar.

Die Voreinstellung ist:

- Wenn der Backup-Speicherort ein lokaler Ordner oder Netzwerkordner (SMB) ist und das Backup-Format der Version 12 entspricht: **Feste Größe – 200 GB**

  Durch diese Einstellung kann die Backup-Software mit großen Datenmengen auf dem NTFS-Dateisystem arbeiten, ohne dass es zu negativen Auswirkungen durch Dateifragmentierungen kommt.
- Ansonsten: **Automatisch**

Es stehen folgende Einstellungen zur Verfügung:

- **Automatisch**
  Das Backup wird aufgeteilt, wenn es die maximale Dateigröße überschreitet, die vom Dateisystem des Zielspeicherortes/Datenträgers noch unterstützt wird.
- **Feste Größe**
  Geben Sie die gewünschte Dateigröße manuell ein oder wählen Sie diese mit dem Listenfeld aus.

Task-Fehlerbehandlung

Diese Option bestimmt das Programmverhalten, wenn die geplante Ausführung eines Schutzplans fehlschlägt oder Ihre Maschine während der Durchführung eines Backups neu gestartet wird. Diese Option gilt nicht, wenn ein Schutzplan manuell gestartet wird.

Wenn diese Option aktiviert ist, wird das Programm versuchen, die Ausführung des Schutzplans zu wiederholen. Sie können festlegen, wie oft und mit welchem Zeitintervall die Ausführung wiederholt werden soll. Die Versuche werden aufgegeben, wenn die Aktion gelingt – oder die festgelegte Anzahl der Versuche erreicht ist (je nachdem, was zuerst eintritt).

Wenn diese Option aktiviert ist und Ihre Maschine während einer Backup-Ausführung neu gestartet wird, wird die Backup-Aktion nicht fehlschlagen. Die Backup-Aktion wird einige Minuten nach dem Neustart automatisch fortgesetzt und die Backup-Datei mit den noch fehlenden Daten vervollständigt. In diesem Anwendungsfall ist die Option **Intervall zwischen den Versuchen** nicht relevant.

Die Voreinstellung ist: **Aktiviert**.

Hinweis
Diese Option ist bei Forensik-Backups nicht wirksam.

Task-Startbedingungen

Diese Option gilt nur für Windows- und Linux-Betriebssysteme.

Diese Option bestimmt, wie sich das Programm verhalten soll, wenn ein Task eigentlich starten sollte (weil der vorgegebene Zeitpunkt erreicht ist oder das spezifizierte Startereignis eingetreten ist), die festgelegte Bedingung (oder eine von mehreren Bedingungen) jedoch nicht erfüllt ist. Weitere Informationen zu den Bedingungen finden Sie im Abschnitt '"Startbedingungen" (S. 468)'.

Die Voreinstellung ist: **Warten, bis die Bedingungen der Planung erfüllt sind.**

Warten, bis die Bedingungen der Planung erfüllt sind

Mit dieser Einstellung beginnt der Scheduler, die Bedingungen zu überwachen, und startet den Task, sobald die Bedingung(en) erfüllt sind. Wenn die Bedingungen nie erfüllt werden, wird der Task auch nie gestartet.

Wenn die Bedingung(en) über einen zu langen Zeitraum nicht erfüllt wurde(n), könnte ein weiteres Aufschieben des Tasks zu kritisch werden. Um zu bestimmen, was in so einem Fall passieren soll, können Sie ein Zeitintervall festlegen, nach dessen Ablauf der Task auf jeden Fall ausgeführt wird –

egal ob die Bedingung(en) erfüllt wurde(n) oder nicht. Aktivieren Sie das Kontrollkästchen **Task trotzdem ausführen nach** und geben Sie dann das Zeitintervall an. Der Task wird gestartet, sobald die Bedingungen erfüllt sind ODER die festgelegte maximale Zeitverzögerung abgelaufen ist – je nachdem, welche dieser Vorgaben als erstes gültig wird.

Task-Ausführung überspringen

Einen Task aufzuschieben kann unter gewissen Umständen inakzeptabel sein. Beispielsweise, wenn Sie einen Task unbedingt zu einem ganz bestimmten Zeitpunkt ausführen müssen. Dann macht es eher Sinn, diesen Task zu übergehen, anstatt auf die Erfüllung der Bedingungen zu warten – insbesondere, wenn die Tasks verhältnismäßig oft ausgeführt werden.

VSS (Volume Shadow Copy Service)

Diese Option gilt nur für Windows-Betriebssysteme.

Sie legt fest, ob ein Backup abgeschlossen werden kann, wenn ein oder mehrere VSS Writer (Volume Shadow Copy Service) fehlschlagen sollten und welcher VSS Provider die VSS-konforme Applikationen benachrichtigen muss, dass das Backup gestartet wird.

Die Verwendung des VSS (Volume Shadow Copy Service, Volumenschattenkopie-Dienst) gewährleistet, dass die von den entsprechenden Applikationen verwendeten und dann im Backup gespeicherten Daten in einem konsistenten Zustand gesichert werden. Beispielsweise, dass alle Datenbanktransaktionen in dem Augenblick abgeschlossen werden, in dem die Backup-Software den Snapshot erfasst. Die Datenkonsistenz gewährleistet dann wiederum, dass die Applikationen auch in einem korrekten Zustand wiederhergestellt werden können und somit unmittelbar nach der Wiederherstellung einsatzbereit sind.

Der Snapshot wird nur während der Backup-Aktion verwendet und wird automatisch wieder gelöscht, sobald die Backup-Aktion abgeschlossen wurde. Es werden keine temporären Dateien aufbewahrt.

Sie können außerdem Befehle vor/nach der Datenerfassung verwenden, um sicherstellen, dass die Daten in einem konsistenten Zustand gesichert wurden. Sie können z.B. bestimmte Befehle vor der Datenerfassung spezifizieren, mit denen eine Datenbank pausiert und alle Zwischenspeicher-Inhalte geleert werden. Damit kann sichergestellt werden, dass alle offenen Datenbank-Transaktionen vor dem Backup abgeschlossen werden. Und anschließend können Sie Befehle nach der Datenerfassung spezifizieren, mit denen die Datenbank nach der Snapshot-Erstellung wieder in Betrieb genommen wird.

Hinweis
Dateien und Ordner, die im Registry-Schlüssel **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToSnapshot** spezifiziert werden, werden nicht gesichert. Es werden insbesondere keine offline Outlook-Datendateien (.ost) gesichert, da diese im Wert '**OutlookOST**' dieses Schlüssels spezifiziert sind.

Fehlgeschlagene VSS Writer ignorieren

Sie können eine der folgenden Optionen wählen:

- **Fehlgeschlagene VSS Writer ignorieren**

  Mit dieser Option können Sie erreichen, dass Backups auch dann abgeschlossen werden, wenn ein oder mehrere VSS Writer ausfallen sollten.

  Wichtig
  Applikationskonforme Backups schlagen immer fehl, wenn der applikationsspezifische VSS Writer fehlschlägt. Wenn Sie beispielsweise ein applikationskonformes Backup von SQL Server-Daten erstellen und **SqlServerWriter** fehlschlägt, wird auch die Backup-Aktion fehlschlagen.

  Wenn diese Option aktiviert ist, werden für einen VSS-Snapshot bis zu drei aufeinanderfolgende Versuche unternommen.

  Im ersten Versuch werden alle VSS-Schreiber benötigt. Wenn dieser Versuch fehlschlägt, wird er wiederholt. Wenn auch der zweite Versuch fehlschlägt, werden die fehlgeschlagenen VSS Writer von der Backup-Aktion ausgeschlossen. Anschließend erfolgt ein dritter Versuch. Wenn der dritte Versuch erfolgreich ist, wird das Backup mit einer Warnung abgeschlossen, dass die VSS Writer fehlgeschlagen sind. Wenn auch der dritte Versuch nicht erfolgreich ist, wird das Backup fehlschlagen.

- **Erfolgreiche Verarbeitung für alle VSS Writer anfordern**

  Wenn einer der VSS Writer ausfällt, wird auch die Backup-Aktion fehlschlagen.

Wählen Sie den Snapshot Provider

Sie können eine der folgenden Optionen wählen:

- **Snapshot Provider automatisch auswählen**

  Automatisch zwischen Hardware Snapshot Provider, Software Snapshot Provider und Microsoft Software Shadow Copy Provider (Microsoft-Softwareschattenkopie-Anbieter) wählen.
- **Microsoft Software Shadow Copy Provider verwenden**

  Wir empfehlen Ihnen, dass Sie diese Option verwenden, wenn Sie Applikationsserver (Microsoft Exchange Server, Microsoft SQL Server, Microsoft SharePoint oder Active Directory) sichern.

VSS-Voll-Backup aktivieren

Falls diese Option aktiviert ist, werden die Protokolle des Microsoft Exchange Servers und anderer VSS-konformer Applikationen (mit Ausnahme des Microsoft SQL Servers) nach jedem erfolgreichen vollständigen, inkrementellen oder differentiellen Laufwerk-Backup abgeschnitten.

Die Voreinstellung ist: **Deaktiviert**.

Lassen Sie diese Option in folgenden Fällen deaktiviert:

- Falls Sie den Agenten für Exchange oder eine Drittanbieter-Software zum Backup von Exchange Server-Daten verwenden. Hintergrund ist, dass die Protokollabschneidung die aufeinanderfolgenden Transaktionsprotokoll-Backups beeinträchtigt.
- Falls Sie eine Drittanbieter-Software zum Backup der SQL Server-Daten verwenden. Hintergrund ist, dass die Drittanbieter-Software das resultierende Laufwerk-Backup als sein eigenes Voll-Backup ansehen wird. Als Folge wird das nächste differentielle Backup der SQL Server-Daten fehlschlagen. Die Backups werden solange fehlschlagen, bis die Drittanbieter-Software das nächste eigene Voll-Backup erstellt.
- Falls andere VSS-kompatible Applikationen auf der Maschine laufen und es aus irgendwelchen Gründen notwendig ist, deren Protokolle zu behalten.

Wichtig
Eine Aktivierung dieser Option bewirkt kein Abschneiden von Microsoft SQL Server-Protokollen. Wenn Sie das SQL Server-Protokoll nach einem Backup abschneiden lassen wollen, müssen Sie die Backup-Option 'Protokollabschneidung aktivieren.

VSS (Volume Shadow Copy Service) für virtuelle Maschinen

Diese Option definiert, ob die virtuellen Maschinen mit stillgelegten (quiesced) Snapshots erfasst werden sollen.

Die Voreinstellung ist: **Aktiviert**.

Wenn diese Option deaktiviert ist, wird ein 'nicht stillgelegter' (non-quiesced) Snapshot erstellt. Die Maschine wird dann in einem 'crash-konsistenten' Zustand gesichert.

Eine Aktivierung dieser Option bewirkt, dass die Transaktionen aller VSS-konformen Applikationen, die in der virtuellen Maschine ausgeführt werden, abgeschlossen werden und anschließend ein stillgelegter („quiesced“) Snapshot erstellt wird.

Wenn nach der einer bestimmten Anzahl von Wiederholungsversuchen, die in der Option Fehlerbehandlung spezifiziert wurde, kein stillgelegter Snapshot erstellt werden konnte und zudem das Applikations-Backup aktiviert ist, wird das Backup fehlschlagen.

Wenn nach der einer bestimmten Anzahl von Wiederholungsversuchen, die in der Option 'Fehlerbehandlung' spezifiziert wurde, kein stillgelegter Snapshot erstellt werden konnte und zudem das Applikations-Backup deaktiviert ist, wird ein crash-konsistentes Backup erstellt. Wenn Sie wollen, dass das Backup fehlschlägt, anstatt ein crash-konsistentes Backup zu erstellen, müssen Sie das Kontrollkästchen **Backup fehlschlagen lassen, wenn die Erstellung eines stillgelegten Snapshots nicht möglich ist** aktivieren.

In der nachfolgenden Tabelle werden die verfügbaren Einstelliungen und deren Auswirkungen zusammengefasst.

Einstellungen	Stillgelegter Snapshot wurde erfolgreich erstellt		Es wurde kein stillgelegter Snapshot erstellt	
	Applikations-Backup aktiviert	**Applikations-Backup deaktiviert**	**Applikations-Backup aktiviert**	**Applikations-Backup deaktiviert**
VSS (Volume Shadow Copy Service) für virtuelle Maschinen deaktiviert **Backup fehlschlagen lassen, wenn die Erstellung eines stillgelegten Snapshots nicht möglich ist** nicht ausgewählt	Stillgelegter Snapshot wird erstellt. Applikationskonsistentes Backup wird erstellt.	Stillgelegter Snapshot wird erstellt. Applikationskonsistentes Backup wird erstellt.	Backup schlägt fehl.	Nicht stillgelegter Snapshot wird erstellt. Crash-konsistentes Backup wird erstellt.
VSS (Volume Shadow Copy Service) für virtuelle Maschinen deaktiviert **Backup fehlschlagen lassen, wenn die Erstellung eines stillgelegten Snapshots nicht möglich ist** ausgewählt	Stillgelegter Snapshot wird erstellt. Applikationskonsistentes Backup wird erstellt.	Stillgelegter Snapshot wird erstellt. Applikationskonsistentes Backup wird erstellt.	Backup schlägt fehl.	Backup schlägt fehl.
VSS (Volume Shadow Copy Service) für virtuelle Maschinen deaktiviert	Nicht stillgelegter Snapshot wird erstellt. Crash-konsistentes Backup wird erstellt.	Nicht stillgelegter Snapshot wird erstellt. Crash-konsistentes Backup wird erstellt.	Nicht stillgelegter Snapshot wird erstellt. Crash-konsistentes Backup wird erstellt.	Nicht stillgelegter Snapshot wird erstellt. Crash-konsistentes Backup wird erstellt.

Das Aktivieren von **VSS (Volume Shadow Copy Service) für virtuelle Maschinen** löst auch die Pre-Freeze- und Post-Thaw-Skripte aus, die Sie möglicherweise für Backups der virtuellen Maschine

angelegt haben. Weitere Informationen über diese Skripte finden Sie hier: "Pre-Freeze- und Post-Thaw-Skripte automatisch ausführen" (S. 763).

Um einen stillgelegten Snapshot zu erfassen, wendet die Backup-Software den VSS (Volumenschattenkopiedienst) innerhalb der virtuellen Maschine an – und zwar mithilfe der VMware Tools, der Hyper-V-Integrationsdienste, der Virtuozzo Guest Tools, Red Hat Virtualization Guest Tools oder der QEMU Guest Tools.

Hinweis
Für virtuelle Maschinen von Red Hat Virtualization (oVirt) empfehlen wir, dass Sie statt der Red Hat Virtualization Guest Tools die QEMU Guest Tools installieren. Einige Versionen der Red Hat Virtualization Guest Tools unterstützen keine applikationskonsistenten Snapshots.

Diese Option hat keinen Einfluss auf virtuelle Scale Computing HC3-Maschinen. Bei diesen hängt das Stilllegen (Quiescing) davon ab, ob die Scale-Tools auf der virtuellen Maschine installiert sind.

Wöchentliche Backups

Diese Option bestimmt, welche Backups in Aufbewahrungsregeln und Backup-Schemata als 'wöchentlich' betrachtet werden. Ein 'wöchentliches' Backup ist dasjenige Backup, das als erstes in einer Woche erstellt wird.

Die Voreinstellung ist: **Montag**.

Windows-Ereignisprotokoll

Diese Option gilt nur für Windows-Betriebssysteme.

Diese Option definiert, ob die Agenten für alle Backup-Aktionen entsprechende Ereigniseinträge im Windows-Anwendungsereignisprotokoll hinterlegen sollen. Sie können die Protokolleinträge über die Windows-Ereignisanzeige einsehen, die per Eingabebefehl (eventvwr.exe) oder per Menü (**Systemsteuerung** –> **Verwaltung** –> **Ereignisanzeige**) aufgefrufen werden kann. Sie können die Ereignisse filtern, die geloggt werden.

Die Voreinstellung ist: **Deaktiviert**.

Recovery

Spickzettel für Wiederherstellungen

Die nachfolgende Tabelle fasst alle verfügbaren Recovery-Methoden zusammen. Verwenden Sie diese Tabelle, um diejenige Recovery-Methode zu finden, die am besten zu Ihren Bedürfnissen passt.

Hinweis
Bei Mandanten, die sich im Compliance-Modus befinden, können Sie keine Backups in der Cyber Protect-Konsole wiederherstellen. Weitere Informationen darüber, wie Sie solche Backups wiederherstellen können, finden Sie in Abschnitt "Backups für Mandanten im Compliance-Modus wiederherstellen" (S. 1196).

Recovery-Quelle	Recovery-Methode
Physische Maschine (Windows oder Linux)	Die Cyber Protect-Konsole verwenden Boot-Medium verwenden
Physische Maschine (Mac)	Boot-Medium verwenden
Virtuelle Maschine (VMware, Hyper-V, Red Hat Virtualization (oVirt) oder Scale Computing HC3)	Die Cyber Protect-Konsole verwenden Boot-Medium verwenden
Virtuelle Maschine oder Container (Virtuozzo, Virtuozzo Hybrid Server oder Virtuozzo Hybrid Infrastructure)	Die Cyber Protect-Konsole verwenden
ESXi-Konfiguration	Boot-Medium verwenden
Dateien/Ordner	Die Cyber Protect-Konsole verwenden Dateien aus dem Cloud Storage herunterladen Boot-Medium verwenden Dateien aus lokalen Backups extrahieren
Systemzustand	Die Cyber Protect-Konsole verwenden
SQL-Datenbanken	Die Cyber Protect-Konsole verwenden
Exchange-Datenbanken	Die Cyber Protect-Konsole verwenden
Exchange-Postfächer	Die Cyber Protect-Konsole verwenden
Websites	Die Cyber Protect-Konsole verwenden
Microsoft 365	
Postfächer (lokaler Agent für Microsoft 365)	Die Cyber Protect-Konsole verwenden
Postfächer	Die Cyber Protect-Konsole verwenden

(Cloud Agent für Microsoft 365)	
Öffentliche Ordner	Die Cyber Protect-Konsole verwenden
OneDrive-Dateien	Die Cyber Protect-Konsole verwenden
SharePoint Online-Daten	Die Cyber Protect-Konsole verwenden
Google Workspace	
Postfächer	Die Cyber Protect-Konsole verwenden
Google Drive-Dateien	Die Cyber Protect-Konsole verwenden
Shared Drive-Dateien	Die Cyber Protect-Konsole verwenden

Plattform-übergreifende Wiederherstellungen

Plattform-übergreifende Wiederherstellungen sind für Backups von kompletten Maschinen sowie für Backups von Laufwerken möglich, die ein Betriebssystem enthalten.

Eine Plattform-übergreifende Wiederherstellung wird in folgenden Fällen durchgeführt:

- Es wird ein Backup von einem bestimmten Agenten-Typ erstellt, aber von einem anderen Agenten-Typ wiederhergestellt.
- Es wird ein agentenbasiertes Backup auf Hypervisor-Ebene wiederhergestellt (agentenlose Wiederherstellung) oder es wird ein agentenloses Backup durch einen Agenten wiederhergestellt (agentenbasierte Wiederherstellung).
- Es wird ein Backup auf abweichender Hardware (kann auch virtuelle Hardware sein) wiederhergestellt.

Hinweis
Wenn Sie eine Plattform-übergreifende Wiederherstellung durchführen, werden einige Peripheriegeräte (wie z.B. Drucker) möglicherweise nicht korrekt wiederhergestellt.

Die nachfolgende Tabelle zeigt einige Beispiele für Plattform-übergreifende Wiederherstellungen.

Plattform-übergreifend Wiederherstellung	
Agentenloses Backup	Agentenbasierte Wiederherstellung
Agentenbasiertes Backup	Agentenlose Wiederherstellung
Backup durch den Agenten für Windows	Wiederherstellung durch den Agenten für VMware
Backup durch den Agenten für VMware	Wiederherstellung durch den Agenten für Hyper-V
Backup durch den Agenten für Windows, der auf einer virtuellen VMware ESXi-Maschine installiert ist	Wiederherstellung durch den Agenten für VMware (agentenlos) auf demselben VMware ESXi-Host

Plattform-übergreifend Wiederherstellung	
(agentenbasiert)	
Backup durch den Agenten für Windows	Wiederherstellung durch den Agenten für Windows, der auf einer Maschine mit abweichender Hardware installiert ist
Backup einer physischen Maschine	Wiederherstellung als virtuelle Maschine

Hinweis für Mac-Benutzer

- Ab Mac OS X 10.11 El Capitan werden bestimmte System-Dateien/-Ordner/-Prozesse mit dem erweiterten Datei-Attribut 'com.apple.rootless' gekennzeichnet und so besonders geschützt. Diese Funktion zur Wahrung der Systemintegrität wird auch SIP (System Integrity Protection) genannt. Zu den geschützten Dateien gehörten vorinstallierte Applikationen sowie die meisten Ordner in /system, /bin, /sbin, /usr.

  Solchermaßen geschützte Dateien und Ordner können bei einer Recovery-Aktion nicht überschrieben werden, wenn die Wiederherstellung unter dem Betriebssystem selbst ausgeführt wird. Wenn es notwendig ist, diese geschützten Dateien zu überschreiben, müssen Sie die Wiederherstellung stattdessen mit einem Boot-Medium durchführen.
- Ab macOS Sierra 10.12 können selten verwendete Dateien mit der Funktion 'In iCloud speichern' in die Cloud verschoben werden. Von diesen Dateien werden im Dateisystem kleine 'Fußabdrücke' gespeichert. Bei einem Backup werden dann diese Datenfußabdrücke statt der Originaldateien gesichert.

  Wenn Sie einen solchen Datenfußabdruck an ursprünglichen Speicherort wiederherstellen, wird er mit der iCloud synchronisiert und die Originaldatei ist wieder verfügbar. Wenn Sie einen Datenfußabdruck an einem anderen Speicherort wiederherstellen, ist keine Synchronisierung möglich und ist die Originaldatei daher nicht verfügbar.

Safe Recovery

Verwenden Sie die Safe Recovery-Funktion mit Windows-Workload-Backups vom Typ **Komplette Maschine** oder **Laufwerke/Volumes**, um sicherzustellen, dass Sie nur Daten wiederherstellen, die frei von Malware sind – was selbst dann gilt, falls eines dieser Backups mal infizierte Dateien enthalten sollte.

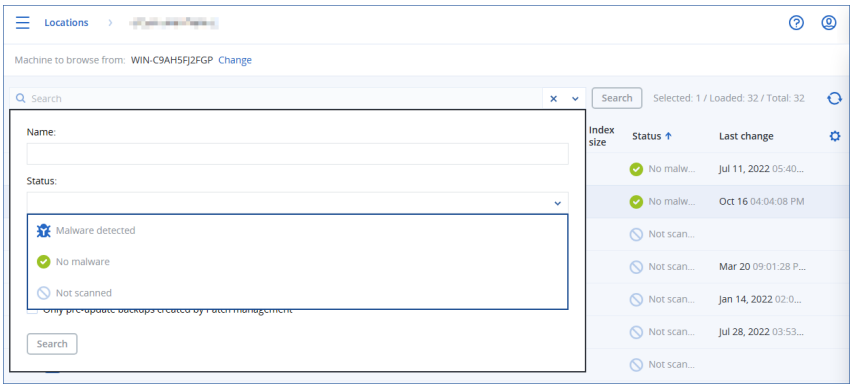
Das Backup wird während einer Safe Recovery-Aktion automatisch auf Malware gescannt. Anschließend stellt der Protection Agent das Backup auf dem Ziel-Workload wieder her und löscht bei diesem Vorgang alle möglicherweise infizierten Dateien. Als Ergebnis wird ein Malware-freies Backup wiederhergestellt.

Dem Backup wird außerdem einer der folgenden Statuszustände zugewiesen:

- Malware erkannt
- Keine Malware

- Nicht gescannt

Sie können die Backup-Archive nach dem jeweiligen Status filtern.



Einschränkungen

- Safe Recovery wird für physische und virtuelle Windows Maschinen unterstützt, auf denen ein Protection Agent installiert ist.
- Safe Recovery wird für Backups vom Typ **Komplette Maschine** und **Laufwerke/Volumes** unterstützt.
- Es werden nur NTFS-Volumes auf Malware gescannt. Nicht-NTFS-Volumes werden ohne einen Antimalware-Scan wiederhergestellt.
- Safe Recovery wird nicht für Backups vom Typ 'Kontinuierliche Datensicherung (CDP)' unterstützt, die in dem Archiv enthalten sind. Wenn Sie Daten aus CDP-Backups wiederherstellen wollen, müssen Sie eine zusätzliche Wiederherstellung vom Typ **Dateien/Ordnern** ausführen. Weitere Informationen über Aktionen mit CDP-Backups finden Sie im Abschnitt '"Kontinuierliche Datensicherung (CDP)" (S. 448)'.

Recovery einer Maschine

Physische Maschinen wiederherstellen

Dieser Abschnitt erläutert, wie Sie physische Maschinen mithilfe der Weboberfläche wiederherstellen können.

Für die Wiederherstellung folgender Systeme müssen Sie ein Boot-Medium (statt der Weboberfläche) verwenden:

- Eine Maschine, die unter macOS läuft
- Eine Maschine von einem Mandanten im Compliance-Modus
- Ein beliebiges Betriebssystem, das auf fabrikneuer Hardware (Bare Metal Recovery) oder zu einer Offline-Maschine wiederhergestellt werden soll
- Die Struktur logischer Volumes (Volumes, die mit dem Logical Volume Manager unter Linux erstellt wurden). Das Medium ermöglicht Ihnen, die logische Volume-Struktur automatisch neu erstellen zu lassen.

Hinweis
Sie können keine Laufwerk-Backups von Intel-basierten Macs auf Macs wiederherstellen, die einen Apple Silicon-Prozessor verwenden (oder umgekehrt). Sie können jedoch einzelne Dateien und Ordner wiederherstellen.

Recovery mit Neustart

Die Wiederherstellung eines Betriebssystems und die Wiederherstellung von Volumes, die per BitLocker verschlüsselt wurden, erfordert einen Neustart. Sie können wählen, ob die Maschine automatisch neu gestartet werden soll – oder ob Ihr der Status **Benutzereingriff erforderlich** zugewiesen werden soll. Das wiederhergestellte System geht automatisch online.

Wichtig
Verschlüsselte Volumes, die per Backup gesichert wurden, werden als unverschlüsselte Volumes wiederhergestellt.

Die Wiederherstellung von Volumes, die bei der Sicherung per BitLocker verschlüsselt waren, setzt voraus, dass sich auf derselben Maschine ein unverschlüsseltes Volume befindet. Dieses Volume muss außerdem über mindestens 1 GB freien Speicherplatz verfügen. Wenn eine dieser beiden Bedingungen nicht erfüllt ist, wird die Wiederherstellung fehlschlagen.

Für die Wiederherstellung eines verschlüsselten System-Volumes sind keine weiteren Maßnahmen erforderlich. Wenn Sie ein verschlüsseltes Nicht-System-Volume wiederherstellen wollen, müssen Sie es zunächst sperren. Beispielsweise, indem Sie eine Datei öffnen, die sich auf diesem Volume befindet. Anderenfalls wird die Wiederherstellung ohne einen Neustart fortgesetzt, wodurch es passieren kann, dass das wiederhergestellte Volume von Windows nicht erkannt wird.

Hinweis
Falls die Wiederherstellung fehlschlägt und Ihre Maschine mit der Fehlermeldung `Datei kann nicht von der Partition abgerufen werden` neu startet, sollten Sie versuchen, die Secure Boot-Funktion zu deaktivieren. Weitere Informationen dazu finden Sie im Abschnitt Deaktivieren des sicheren Starts („Disabling Secure Boot“) in der Microsoft-Dokumentation.

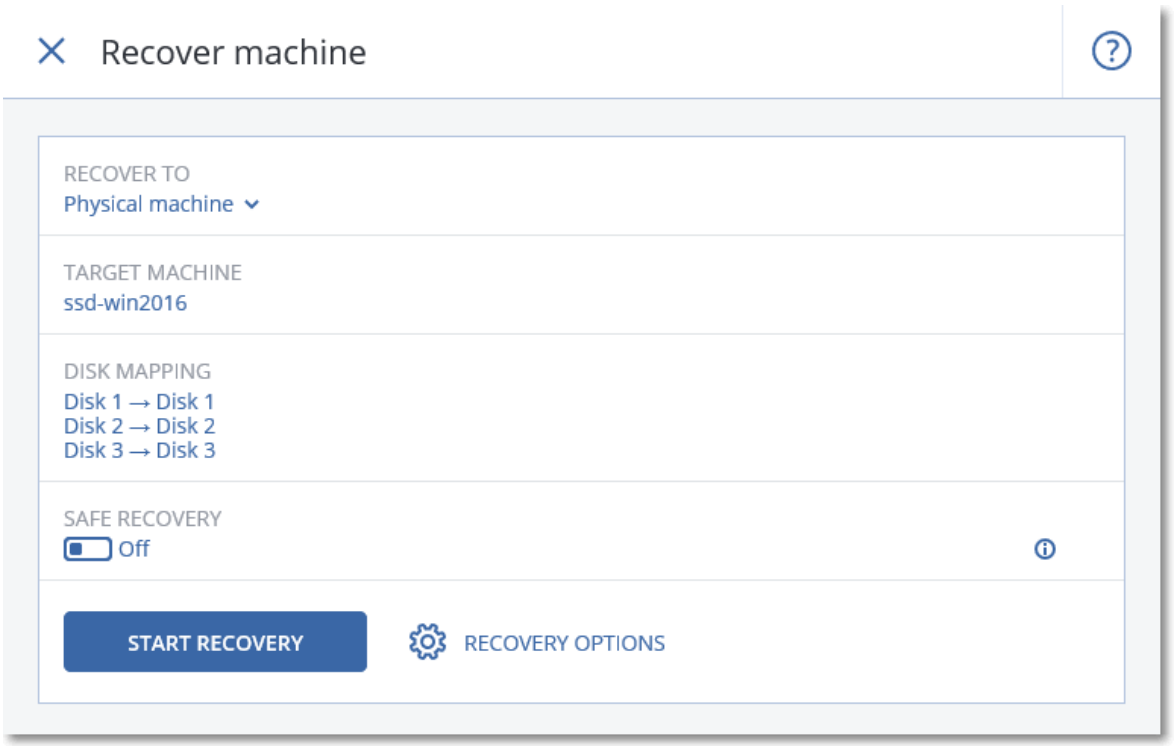
So können Sie eine physische Maschine wiederherstellen

1. Wählen Sie die Maschine aus, die per Backup gesichert wurde.
2. Klicken Sie auf **Recovery**.
3. Wählen Sie einen Recovery-Punkt. Beachten Sie dabei, dass Recovery-Punkte nach Speicherorten gefiltert werden.
   Falls die Maschine offline ist, werden keine Recovery-Punkte angezeigt. Gehen Sie nach einer der folgenden Möglichkeiten vor:
   - Sollte sich das Backup im Cloud Storage oder einem freigegebenen Storage befinden (d.h., dass andere Agenten auf diesen zugreifen können), dann klicken Sie zuerst auf den Befehl **Maschine auswählen**. Wählen Sie anschließend eine Zielmaschine, die online ist, und dann

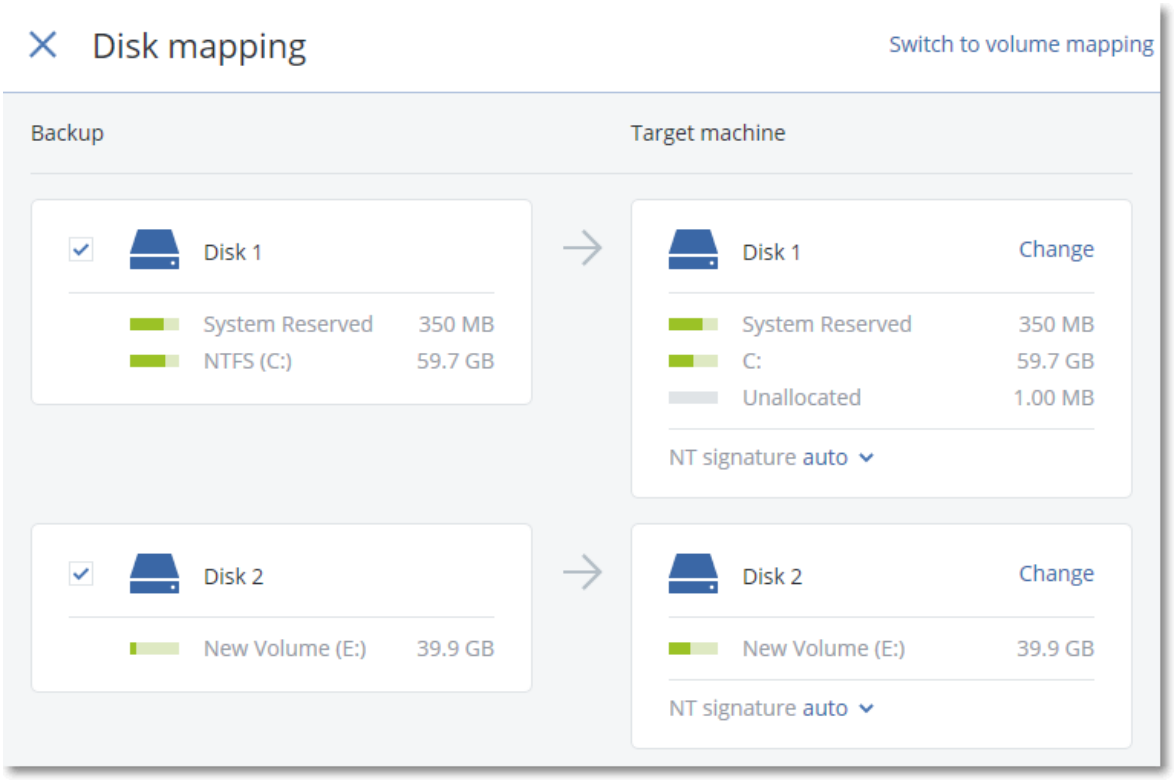
den gewünschten Recovery-Punkt.

- Wählen Sie einen Recovery-Punkt auf der Registerkarte 'Backup Storage'.
- Stellen Sie die Maschine so wieder her, wie es im Abschnitt 'Laufwerke mithilfe eines Boot-Mediums wiederherstellen' beschrieben ist.

4. Klicken Sie auf **Recovery** –> **Komplette Maschine**.
   Die Software weist die Laufwerke im Backup automatisch den Laufwerken der Zielmaschine zu.
   Wenn Sie eine andere physische Maschine als Recovery-Ziel verwenden wollen, klicken Sie auf **Zielmaschine** und wählen Sie dann eine Zielmaschine aus, die online ist.



5. Falls die Zuordnung erfolglos war oder falls Sie mit dem Zuordnungsergebnis unzufrieden sind, können Sie auf **Volume-Zuordnung** klicken, um die Laufwerke manuell zuzuordnen.
   Der Zuordnungsbereich ermöglicht Ihnen außerdem, bestimmte Laufwerke oder Volumes für die Wiederherstellung auszuwählen. Mit dem Link **Wechseln zu...** (in der oberen rechten Ecke) können Sie zwischen Wiederherstellung von Laufwerken und Volumes wechseln.



6. [Nur für Windows-Maschinen verfügbar, auf denen ein Protection Agent installiert ist] Aktivieren Sie den Schalter **Safe Recovery**, um sicherzustellen, dass die wiederhergestellten Daten frei von Malware sind. Weitere Informationen darüber, wie Safe Recovery funktioniert, finden Sie im Abschnitt '"Safe Recovery" (S. 544)'.
7. Klicken Sie auf **Recovery starten**.
8. Bestätigen Sie, dass die Daten auf den Laufwerken durch die Datenversionen überschrieben werden sollen, die im Backup vorliegen. Bestimmen Sie, ob ein automatischer Neustart der Maschine erfolgen soll.

Der Recovery-Fortschritt wird auf der Registerkarte **Aktivitäten** angezeigt.

Physische Maschinen als virtuelle Maschinen wiederherstellen

Sie können eine physische Maschine zu einer virtuellen Maschine auf einem der unterstützten Hypervisors wiederherstellen. Dies ist auch ein Mechanismus, mit dem eine physische zu einer virtuellen Maschine migriert werden kann. Weitere Informationen zu unterstützten P2V-Migrationspfaden finden Sie im Abschnitt 'Migration von Maschinen'.

Dieser Abschnitt erläutert, wie Sie eine physische Maschine über die Weboberfläche als virtuelle Maschine wiederherstellen können. Diese Aktion kann durchgeführt werden, wenn mindestens ein Agent für den entsprechenden Hypervisor installiert und im Acronis Management Server registriert ist. Zum Beispiel erfordert eine Wiederherstellung zu VMware ESXi mindestens einen Agenten für VMware, eine Wiederherstellung zu Hyper-V erfordert mindestens einen Agenten für Hyper-V, der in der jeweiligen Umgebung installiert und registriert ist.

Wiederherstellungen über die Weboberfläche sind für Mandanten im Compliance-Modus nicht verfügbar.

Hinweis
Sie können keine virtuellen Maschinen mit macOS zu einem Hyper-V-Host wiederherstellen, weil macOS von Hyper-V nicht unterstützt wird. Sie können virtuelle Maschinen mit macOS zu einem VMware-Host wiederherstellen, wenn dieser auf Mac-Hardware installiert ist.

Sie können außerdem keine Backups von physischen macOS-Maschinen als virtuelle Maschinen wiederherstellen.

So können Sie eine physische Maschine als virtuelle Maschine wiederherstellen

1. Wählen Sie die Maschine aus, die per Backup gesichert wurde.
2. Klicken Sie auf **Recovery**.
3. Wählen Sie einen Recovery-Punkt. Beachten Sie dabei, dass Recovery-Punkte nach Speicherorten gefiltert werden.
   Falls die Maschine offline ist, werden keine Recovery-Punkte angezeigt. Gehen Sie nach einer der folgenden Möglichkeiten vor:
   - Sollte sich das Backup im Cloud Storage oder einem freigegebenen Storage befinden (d.h., dass andere Agenten auf diesen zugreifen können), dann klicken Sie zuerst auf den Befehl **Maschine auswählen**. Wählen Sie anschließend eine Maschine aus, die online ist, und dann den gewünschten Recovery-Punkt.
   - Wählen Sie einen Recovery-Punkt auf der Registerkarte 'Backup Storage'.
   - Stellen Sie die Maschine so wieder her, wie es im Abschnitt 'Laufwerke mithilfe eines Boot-Mediums wiederherstellen' beschrieben ist.
4. Klicken Sie auf **Recovery** –> **Komplette Maschine**.
5. Wählen Sie unter **Recovery zu** die Option **Virtuelle Maschine**.
6. Klicken Sie auf **Zielmaschine**.
   a. Wählen Sie den Hypervisor.

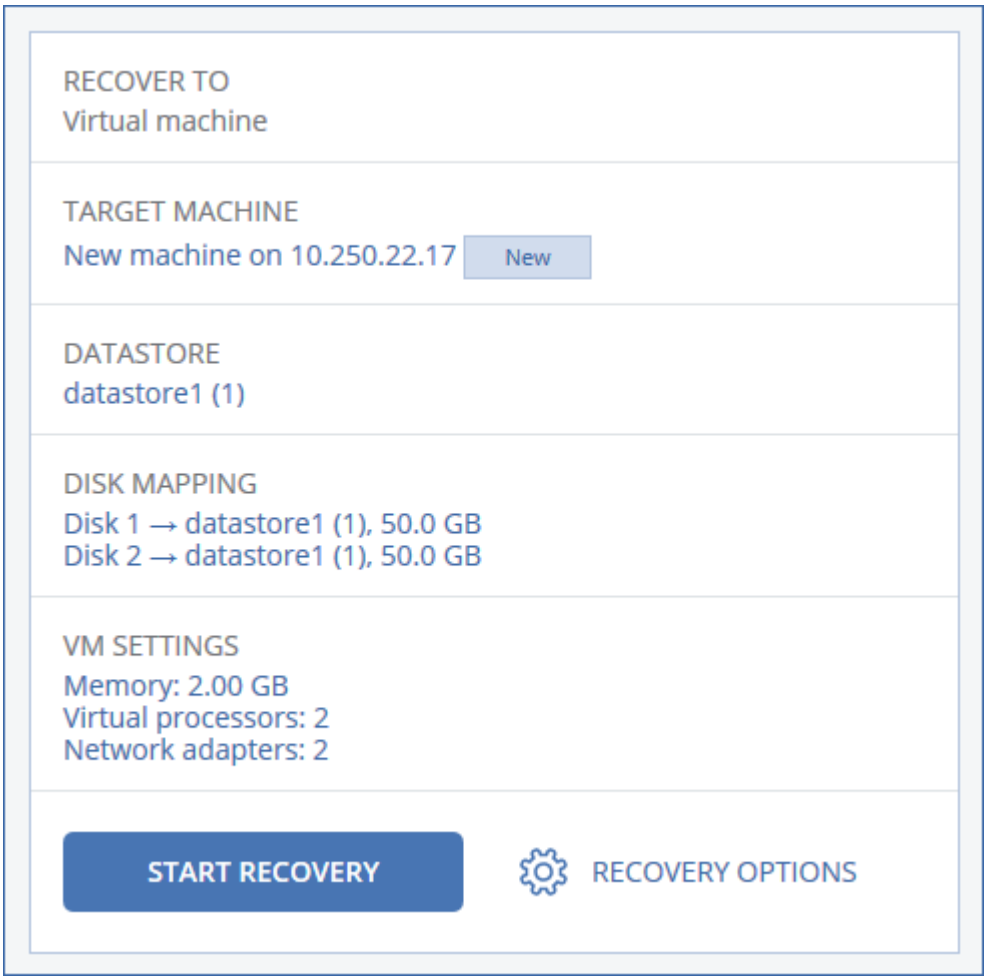
      Hinweis
      Mindestens ein Agent für den jeweiligen Hypervisor muss installiert und im Acronis Management Server registriert sein.

   b. Bestimmen Sie, ob eine neue oder eine vorhandene Maschine als Recovery-Ziel verwendet werden soll. Die Option 'Neue Maschine' ist vorteilhafter, da hier die Laufwerkskonfiguration im Backup nicht mit der Laufwerkskonfiguration der Zielmaschine exakt übereinstimmen muss.
   c. Wählen Sie den Host und spezifizieren Sie einen Namen für die neue Maschine – oder wählen Sie eine bereits vorhandene Zielmaschine aus.
   d. Klicken Sie auf **OK**.

7. [Für Virtuozzo Hybrid Infrastructure] Klicken Sie auf **VM-Einstellungen**, um eine **Variante** (Englisch: Flavor) auszuwählen. Sie können optional die Größe des Arbeitsspeichers, die Anzahl der Prozessoren und die Netzwerkverbindungen für die virtuelle Maschine ändern.

   Hinweis
   Für Virtuozzo Hybrid Infrastructure ist die Auswahl des Variante (Flavor) ein notwendiger Schritt.

8. [Optional] Konfigurieren Sie zusätzliche Recovery-Optionen:
   - [Nicht für Virtuozzo Hybrid Infrastructure verfügbar] Klicken Sie auf **Datenspeicher** für ESXi oder **Pfad** für Hyper-V – und bestimmten Sie dann den Datenspeicher (Storage) für die neue virtuelle Maschine.
   - Klicken Sie auf **Laufwerkszuordnung**, um den Datenspeicher (Storage), die Oberfläche und den Provisioning-Modus für jedes virtuelle Laufwerk auszuwählen. Der Zuordnungsbereich ermöglicht Ihnen außerdem, bestimmte Laufwerke für die Wiederherstellung auszuwählen.
     Für Virtuozzo Hybrid Infrastructure können Sie nur die Storage-Richtlinie für die Ziellaufwerke auswählen. Wählen Sie dafür das gewünschte Ziellaufwerk aus und klicken Sie dann auf 'Ändern'. Klicken Sie in dem sich öffnenden Blatt auf das Zahnradsymbol, wählen Sie die Storage-Richtlinie aus und klicken Sie dann auf 'Fertig'.
   - [Bei VMware ESXi, Hyper-V und Red Hat Virtualization/oVirt] Klicken Sie auf **VM-Einstellungen**, um die Größe des Arbeitsspeichers, die Anzahl der Prozessoren und die Netzwerkverbindungen für die virtuelle Maschine zu ändern.



9. [Nur für Windows-Maschinen verfügbar, auf denen ein Protection Agent installiert ist] Aktivieren Sie den Schalter **Safe Recovery**, um sicherzustellen, dass die wiederhergestellten Daten frei von Malware sind. Weitere Informationen darüber, wie Safe Recovery funktioniert, finden Sie im Abschnitt '"Safe Recovery" (S. 544)'.
10. Klicken Sie auf **Recovery starten**.
11. Wenn Sie eine vorhandene virtuelle Maschine als Recovery-Ziel verwenden, müssen Sie noch bestätigen, dass deren Laufwerke überschrieben werden.

Der Recovery-Fortschritt wird auf der Registerkarte **Aktivitäten** angezeigt.

Eine virtuelle Maschine wiederherstellen

Sie können virtuelle Maschinen aus deren Backups wiederherstellen.

Hinweis
Bei Mandanten, die sich im Compliance-Modus befinden, können Sie keine Backups in der Cyber Protect-Konsole wiederherstellen. Weitere Informationen darüber, wie Sie solche Backups wiederherstellen können, finden Sie in Abschnitt "Backups für Mandanten im Compliance-Modus wiederherstellen" (S. 1196).

Voraussetzungen

- Eine virtuelle Maschine, die als Recovery-Ziel dient, muss während der Wiederherstellung gestoppt werden. Standardmäßig stoppt die Software die Maschine ohne weitere Nachfrage. Wenn die Wiederherstellung abgeschlossen wurde, müssen Sie die Maschine manuell wieder starten. Sie können dieses vorgegebene Verhalten mithilfe der Recovery-Option für die VM-Energieverwaltung ändern (klicken Sie dafür auf **Recovery-Optionen** –> **VM-Energieverwaltung**).

Vorgehensweise

1. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Wählen Sie eine zu sichernde Maschine, klicken Sie auf **Recovery** und wählen Sie dann einen Recovery-Punkt.
   - Wählen Sie einen Recovery-Punkt auf der Registerkarte 'Backup Storage'.
2. Klicken Sie auf **Recovery** –> **Komplette Maschine**.
3. Wenn Sie die Wiederherstellung zu einer physischen Maschine durchführen wollen, wählen Sie bei **Recovery zu** das Element **Physische Maschine**. Ansonsten können Sie diesen Schritt überspringen.

   Eine Wiederherstellung auf einer physischen Maschine ist nur dann möglich, wenn die Laufwerkskonfiguration im Backup exakt mit der Laufwerkskonfiguration der Zielmaschine übereinstimmt.

   Falls dies zutrifft, fahren Sie mit Schritt 4 im Abschnitt 'Physische Maschine' fort. Falls dies nicht zutrifft, empfehlen wir Ihnen, eine V2P-Migration mithilfe eines Boot-Mediums durchzuführen.
4. [Optional] Die Software wählt standardmäßig automatisch die ursprüngliche Maschine als Zielmaschine aus. Wenn Sie die Wiederherstellung auf eine andere virtuelle Maschine durchführen wollen, müssen Sie auf **Zielmaschine** klicken und dann Folgendes tun:
   a. Wählen Sie den Hypervisor (**VMware ESXi**, **Hyper-V**, **Virtuozzo**, **Virtuozzo Hybrid Infrastructure**, **Scale Computing HC3** oder **oVirt**).

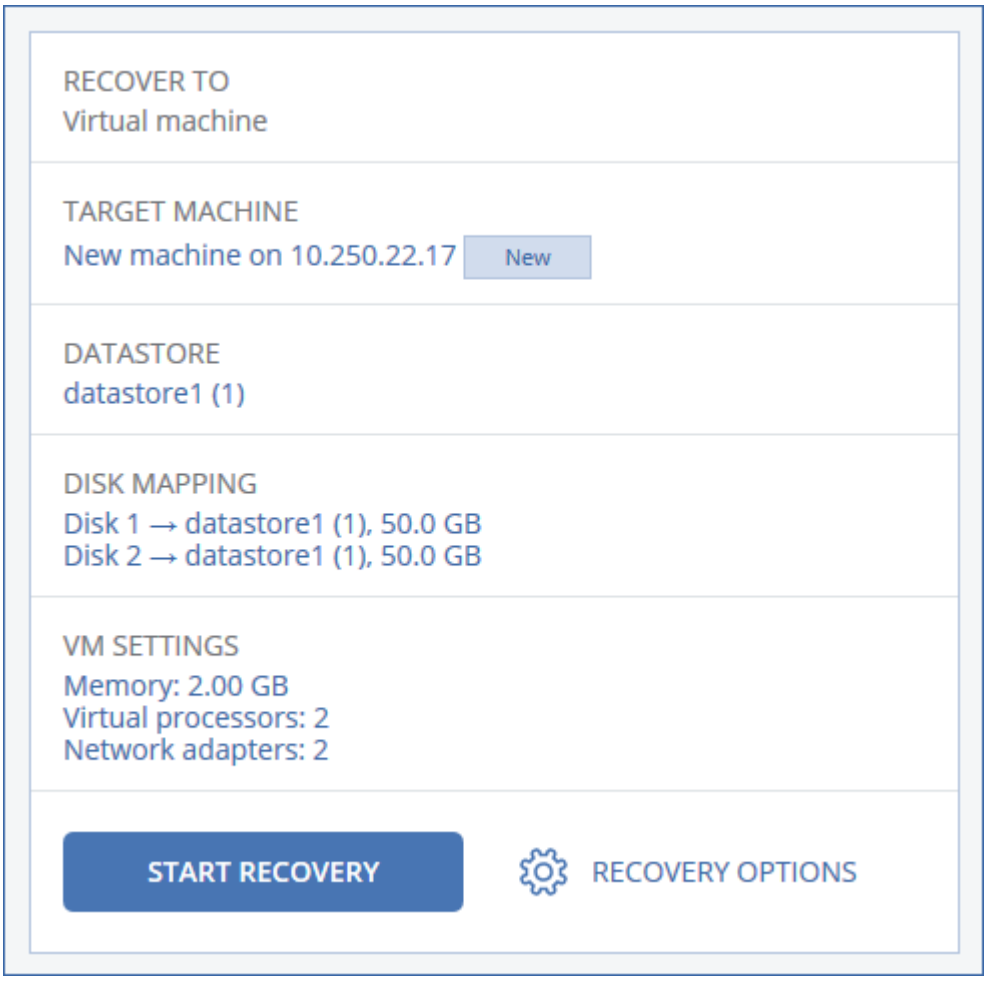
      Nur virtuelle Virtuozzo-Maschinen können zu Virtuozzo wiederhergestellt werden. Weiter Informationen zu V2V-Migrationen finden Sie im Abschnitt 'Migration von Maschinen'.
   b. Bestimmen Sie, ob eine neue oder eine vorhandene Maschine als Recovery-Ziel verwendet werden soll.
   c. Wählen Sie den Host und spezifizieren Sie einen Namen für die neue Maschine – oder wählen Sie eine bereits vorhandene Zielmaschine aus.
   d. Klicken Sie auf **OK**.
5. Richten Sie die zusätzlichen Recovery-Optionen ein, die Sie benötigen.
   - [Optional] [Nicht für Virtuozzo Hybrid Infrastructure und Scale Computing HC3 verfügbar] Wenn Sie das Speicherziel für die virtuelle Maschine auswählen wollen, klicken Sie auf **Datenspeicher** für ESXi, **Pfad** für Hyper-V bzw. Virtuozzo oder **Storage-Domain** für Red Hat Virtualization (oVirt) – und bestimmten Sie dann den Datenspeicher (Storage) für die virtuelle Maschine.
   - [Optional] Klicken Sie auf **Laufwerkszuordnung**, um den Datenspeicher (Storage), die Schnittstelle und den Provisioning-Modus für jedes virtuelle Laufwerk einzusehen. Sie können

diese Einstellungen ändern, außer Sie stellen einen Virtuozzo-Container oder eine virtuelle Maschine für Virtuozzo Hybrid Infrastructure wieder her.

Für Virtuozzo Hybrid Infrastructure können Sie nur die Storage-Richtlinie für die Ziellaufwerke auswählen. Wählen Sie dafür das gewünschte Ziellaufwerk aus und klicken Sie dann auf **Ändern**. Klicken Sie in dem sich öffnenden Blatt auf das Zahnradsymbol, wählen Sie die Storage-Richtlinie aus und klicken Sie dann **Fertig**.

Der Zuordnungsbereich ermöglicht Ihnen außerdem, bestimmte Laufwerke für die Wiederherstellung auszuwählen.

- [Optional] [Für VMware ESXi, Hyper-V und Virtuozzo verfügbar] Klicken Sie auf **VM-Einstellungen**, um die Größe des Arbeitsspeichers, die Anzahl der Prozessoren und die Netzwerkverbindungen für die virtuelle Maschine zu ändern.
- [Für Virtuozzo Hybrid Infrastructure] Wählen Sie **Variante**, um die Speichergröße sowie die Anzahl der Prozessoren der virtuellen Maschine zu ändern.



6. [Nur für Windows-Maschinen verfügbar, auf denen ein Protection Agent installiert ist] Aktivieren Sie den Schalter **Safe Recovery**, um sicherzustellen, dass die wiederhergestellten Daten frei von Malware sind. Weitere Informationen darüber, wie Safe Recovery funktioniert, finden Sie im Abschnitt '"Safe Recovery" (S. 544)'.
7. Klicken Sie auf **Recovery starten**.

8. Wenn Sie eine vorhandene virtuelle Maschine als Recovery-Ziel verwenden, müssen Sie noch bestätigen, dass deren Laufwerke überschrieben werden.

Der Recovery-Fortschritt wird auf der Registerkarte **Aktivitäten** angezeigt.

Laufwerke mithilfe eines Boot-Mediums wiederherstellen

Informationen über die Erstellung eines Boot-Mediums finden Sie im Abschnitt '"Ein physisches Boot-Medium erstellen" (S. 778)'.

Hinweis

Sie können keine Laufwerk-Backups von Intel-basierten Macs auf Macs wiederherstellen, die einen Apple Silicon-Prozessor verwenden (oder umgekehrt). Sie können jedoch einzelne Dateien und Ordner wiederherstellen.

So stellen Sie Laufwerke mithilfe eines Boot-Mediums wieder her

1. Booten Sie die Zielmaschine mit einem Boot-Medium.
2. [Nur bei Wiederherstellung eines Macs] Wenn Sie APFS-formatierte Laufwerke/Volumes zu einer anderen als der ursprünglichen (wie einer fabrikneuen) Maschine wiederherstellen, müssen Sie die ursprüngliche Laufwerkskonfiguration manuell neu erstellen:
   a. Klicken Sie auf **Festplattendienstprogramm**.
   b. Löschen und formatieren Sie das Laufwerk im APFS-Format. Weitere Informationen dazu finden Sie unter https://support.apple.com/de-de/HT208496#erasedisk.
   c. Stellen Sie die ursprüngliche Laufwerkskonfiguration wieder her. Weitere Informationen dazu finden Sie unter https://support.apple.com/guide/disk-utility/add-erase-or-delete-apfs-volumes-dskua9e6a110/19.0/mac/10.15.
   d. Klicken Sie auf **Festplattendienstprogramm** > **Festplattendienstprogramm beenden**.
3. Klicken Sie entweder auf **Diese Maschine lokal verwalten** oder zweimal auf **Rescue Bootable Media** (abhängig vom verwendeten Typ des Mediums).
4. Falls in Ihrem Netzwerk ein Proxy-Server verwendet wird, klicken Sie auf **Tools** –> **Proxy-Server** und spezifizieren Sie dann den Host-Namen/die IP-Adresse, den Port und die Anmeldedaten des Proxy-Servers. Ansonsten können Sie diesen Schritt überspringen.
5. [Optional] Klicken Sie bei der Wiederherstellung von Windows oder Linux auf **Tools** –> **Medium im Cyber Protection Service registrieren** und spezifizieren Sie dann das Registrierungstoken, welches Sie beim Download des Mediums erhalten haben. Wenn Sie dies tun, müssen Sie keine Anmeldedaten oder keinen Registrierungscode eingeben, um auf den Cloud Storage zuzugreifen (wie in Schritt 8 beschrieben).
6. Klicken Sie innerhalb der Willkommensseite auf **Recovery**.
7. Klicken Sie auf **Daten wählen** und dann auf **Durchsuchen**.
8. Spezifizieren Sie den Backup-Speicherort:
   - Wählen Sie das Element **Cloud Storage**, um Dateien aus dem Cloud Storage wiederherzustellen. Geben Sie die Anmeldedaten des Kontos ein, dem die gesicherte

Maschine zugewiesen wird.

Bei der Wiederherstellung von Windows oder Linux haben Sie die Möglichkeit, einen Registrierungscode anzufordern und diesen statt der Anmeldeinformationen zu verwenden. Klicken Sie auf **Registrierungscode verwenden** –> **Den Code anfordern**. In der Software werden der Registrierungslink und Registrierungscode angezeigt. Sie können diese kopieren und die Registrierungsschritte dann auf einer anderen Maschine durchführen. Der Registrierungscode ist für eine (1) Stunde gültig.

- Um eine Wiederherstellung von einem lokalen Ordner oder einem Netzwerkordner aus durchzuführen, wählen Sie den entsprechenden Ordner über das Element **Lokale Ordner** oder **Netzwerkordner** aus.
- Wenn Sie Wiederherstellungen von Backup-Speicherorten auf einem Public Cloud Storage (wie Microsoft Azure, Amazon S3, Wasabi oder andere S3-kompatible Storages) durchführen wollen, müssen Sie zuerst auf **Medium im Cyber Protection Service registrieren** klicken und dann die Wiederherstellung über die Weboberfläche konfigurieren. Weitere Informationen darüber, wie Sie die entsprechenden Medien remote über die Weboberfläche verwalten können, finden Sie unter "Remote-Aktionen mit einem Boot-Medium" (S. 797).

Klicken Sie auf **OK**, um Ihre Auswahl zu bestätigen.

9. Wählen Sie das Backup, aus dem die Daten wiederhergestellt werden sollen. Geben Sie das Kennwort für das Backup an, falls Sie dazu aufgefordert werden.
10. Wählen Sie bei **Backup-Inhalte** die wiederherzustellenden Laufwerke. Klicken Sie auf **OK**, um Ihre Auswahl zu bestätigen.
11. Die Software ordnet unter **Recovery-Ziel** die ausgewählten Laufwerke automatisch den Ziellaufwerken zu.

    Falls die Zuordnung erfolglos ist oder falls Sie mit dem Zuordnungsergebnis unzufrieden sind, können Sie die Laufwerke auch manuell zuordnen.

    Hinweis
    Eine Änderung des Laufwerk-Layouts kann die Bootfähigkeit des Betriebssystems beeinflussen. Verwenden Sie möglichst das ursprüngliche Laufwerkslayout der Maschine, außer Sie sind sich über das Ergebnis der Änderung absolut sicher.

12. [Bei einer Wiederherstellung von Linux] Falls die gesicherte Maschine logische Volumes hatte (LVM) und Sie die ursprüngliche LVM-Struktur nachbilden wollen:
    a. Stellen Sie sicher, dass die Anzahl der Laufwerke der Zielmaschine und jede Laufwerkskapazität der der ursprünglichen Maschine entspricht oder diese übersteigt – und klicken Sie dann auf **RAID/LVM anwenden**.
    b. Überprüfen Sie die Volume-Struktur und klicken Sie dann auf **RAID/LVM anwenden** um sie zu erstellen.
13. [Optional] Klicken Sie auf **Recovery-Optionen**, um zusätzliche Einstellungen zu spezifizieren.
14. Wählen Sie **OK**, um die Wiederherstellung zu starten.

Universal Restore verwenden

Moderne Betriebssysteme behalten normalerweise ihre Bootfähigkeit, wenn sie auf abweichender Hardware (beinhaltet auch VMware- und Hyper-V-Maschinen) wiederhergestellt werden. Falls ein Betriebssystem nach einer Wiederherstellung dennoch nicht mehr bootet, können Sie das Tool 'Universal Restore' verwenden, um diejenigen Treiber und Module zu aktualisieren, die das Betriebssystem zum Starten auf der neuen Hardware/Maschine benötigt.

Universal Restore kann für Windows und Linux verwendet werden.

So verwenden Sie Universal Restore

1. Booten Sie die Maschine mithilfe eines Boot-Mediums.
2. Klicken Sie auf den Befehl **Universal Restore anwenden**.
3. Sollte es mehrere Betriebssysteme auf der Maschine geben, dann wählen Sie dasjenige System aus, welches von Universal Restore angepasst werden soll.
4. [Nur bei Windows] Konfigurieren Sie die 'Erweiterten Einstellungen'.
5. Klicken Sie auf **OK**.

Universal Restore unter Windows

Vorbereitung

Treiber vorbereiten

Bevor Sie Universal Restore auf ein Windows-Betriebssystem anwenden, sollten Sie sicherstellen, dass Sie über die passenden Treiber für den neuen Festplatten-Controller und den Chipsatz des Mainbords verfügen. Diese Treiber sind für den Start des Betriebssystem unerlässlich. Verwenden Sie (sofern vorhanden) die Treiber-CD/-DVD, die der Hardware-Hersteller Ihrem Computer/Mainboard beigelegt hat – oder laden Sie benötigten Treiber von der Website des Herstellers herunter. Die Treiber sollten die Dateierweiterung *.inf verwenden. Wenn Sie die Treiber im Format *.exe, *.cab oder *.zip herunterladen, extrahieren Sie diese mit einer entsprechenden Dritthersteller-Anwendung.

Eine empfehlenswerte Vorgehensweise ist es, die benötigten Treiber (für die in Ihrer Organisation verwendete Hardware) an einem zentralen Aufbewahrungsort ('Repository') zu speichern und dabei nach Gerätetyp oder Hardware-Konfiguration zu sortieren. Sie können eine Kopie des Treiber-Repositorys zur leichteren Verwendung auch auf DVD oder USB-Stick vorhalten. Suchen Sie daraus die benötigten Treiber aus, um diese dem bootfähigen Medium hinzufügen zu können. Erstellen Sie dann für jeden Ihrer Server ein benutzerdefiniertes Boot-Medium mit den benötigten Treibern (und der benötigten Netzwerk-Konfiguration). Alternativ können Sie den Pfad zum Repository auch bei jeder Verwendung von Universal Restore spezifizieren.

Überprüfen Sie, dass auf die Treiber in der bootfähigen Umgebung zugegriffen werden kann.

Überprüfen Sie, dass Sie beim Arbeiten mit dem bootfähigen Medium auf das Gerät mit den Treibern zugreifen können. Ein WinPE-basiertes Medium sollte dann zum Einsatz kommen, wenn ein Gerät unter Windows verfügbar ist, von einem Linux-basierten Medium aber nicht erkannt wird.

Universal Restore-Einstellungen

Automatische Suche nach Treibern

Spezifizieren Sie, wo das Programm nach Treibern für die Hardware-Abstraktionsschicht (HAL, Hardware Abstraction Layer) sowie für Festplatten-Controller und Netzwerkkarten suchen soll:

- Befinden sich die Treiber auf einem Datenträger (CD/DVD) des Herstellers oder einem anderen Wechselmedium, dann aktivieren Sie **Wechselmedien durchsuchen**.
- Liegen die Treiber in einem Netzwerkordner oder auf einem bootfähigen Medium, so spezifizieren Sie den Pfad zu diesem Ordner durch Anklicken von **Ordner durchsuchen**.

Zusätzlich wird Universal Restore den Standardspeicherort (Ordner) für Treiber durchsuchen. Dessen genaue Position ist über den Registry-Wert **DevicePath** definiert, der im Registry-Schlüssel **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion** gefunden werden kann. Üblicherweise befindet sich dieser Speicherordner im Unterverzeichnis 'WINDOWS/inf'.

Universal Restore führt im spezifizierten Ordner und seinen Unterordnern eine rekursive Suche durch, ermittelt dann unter allen verfügbaren Festplatten-Controller- und HAL-Treibern diejenigen, die am besten geeignet sind, und installiert diese Treiber schließlich im System. Universal Restore sucht außerdem nach Treibern für Netzwerkkarten. Der Pfad zu einem gefundenen Treiber wird dem Betriebssystem dann von Universal Restore mitgeteilt. Falls die Hardware über mehrere Netzwerkkarten verfügt, versucht Universal Restore, die Treiber für alle Karten zu konfigurieren.

Auf jeden Fall zu installierende Massenspeichertreiber

Sie benötigen diese Einstellung falls:

- Die Hardware einen speziellen Massenspeicher-Controller verwendet – z.B. einen RAID- (insbesondere NVIDIA RAID) oder Fibre Channel-Adapter.
- Sie ein System zu einer virtuellen Maschine migriert haben, die einen SCSI-Festplatten-Controller verwendet. Verwenden Sie diejenigen SCSI-Treiber, die zusammen mit Ihrer Virtualisierungssoftware ausgeliefert werden. Alternativ können Sie die neueste Treiberversion vermutlich auch von der Website des betreffenden Software-Herstellers herunterladen.
- Falls die automatische Suche nach Treibern nicht hilft, das System zu booten.

Spezifizieren Sie die entsprechenden Treiber, indem Sie auf den Befehl **Treiber hinzufügen** klicken. Treiber, die hier definiert werden, werden auch dann (mit entsprechenden Warnmeldungen) installiert, wenn das Programm einen besseren Treiber findet.

Der Universal Restore-Prozess

Klicken Sie auf **OK**, nachdem Sie die benötigten Einstellungen spezifiziert haben.

Falls Universal Restore an den angegebenen Speicherorten keinen kompatiblen Treiber findet, zeigt es eine Eingabeaufforderung für das Problemgerät an. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:

- Fügen Sie den Treiber einem der zuvor spezifizierten Speicherorte hinzu und klicken Sie dann auf **Wiederholen**.
- Klicken Sie auf **Ignorieren**, falls Sie sich nicht mehr an den Speicherort erinnern können, damit der Prozess fortgesetzt wird. Sollte das Ergebnis nicht zufriedenstellend sein, dann wenden Sie Universal Restore erneut an. Spezifizieren Sie bei Konfiguration der Aktion den benötigten Treiber.

Sobald Windows bootet, wird es die Standardprozedur zur Installation neuer Hardware initialisieren. Der Treiber für die Netzwerkkarte wird ohne weitere Nachfrage installiert, sofern er eine passende Microsoft Windows-Signatur hat. Anderenfalls verlangt Windows eine Bestätigung, dass der unsignierte Treiber installiert werden soll.

Danach können Sie die Netzwerk-Verbindung konfigurieren und weitere Treiber spezifizieren (beispielsweise für die Grafikkarte und USB-Geräte).

Universal Restore unter Linux

Universal Restore kann auf Linux-Betriebssysteme mit der Kernel-Version 2.6.8 (oder höher) angewendet werden.

Wenn Universal Restore auf ein Linux-Betriebssystem angewendet wird, aktualisiert es ein temporäres Dateisystem, das auch als 'Initial RAM-Disk' (initrd) bekannt ist. Dadurch wird gewährleistet, dass das Betriebssystem auch auf neuer, abweichender Hardware booten kann.

Universal Restore kann dieser 'Initial RAM-Disk' benötigte Module für die neue Hardware hinzufügen (einschließlich Gerätetreiber). Es findet die benötigten Module normalerweise im Verzeichnis **/lib/modules**. Falls Universal Restore ein benötigtes Modul nicht finden kann, schreibt es den Dateinamen des Moduls in das Log.

Universal Restore kann unter Umständen die Konfiguration des GRUB-Boot-Loaders ändern. Dies kann beispielsweise notwendig sein, um die Bootfähigkeit des Systems zu gewährleisten, falls die neue Maschine ein anderes Volume-Layout als die ursprüngliche hat.

Universal führt keine Änderungen am Linux-Kernel durch!

Zur ursprünglichen 'Initial RAM-Disk' zurücksetzen

Sie können bei Bedarf zur ursprünglichen 'Initial RAM-Disk' zurücksetzen.

Die 'Initial RAM-Disk' ist auf der Maschine in Form einer Datei gespeichert. Bevor Universal Restore die 'Initial RAM-Disk' zum ersten Mal aktualisiert, speichert es diese als Kopie ab – und zwar im gleichen Verzeichnis. Der Name dieser Kopie entspricht dem Dateinamen, ergänzt um das Suffix _ **acronis_backup.img**. Diese Kopie wird auch dann nicht überschrieben, wenn Sie Universal Restore mehrmals ausführen (beispielsweise nachdem Sie fehlende Treiber hinzugefügt haben).

Sie können folgendermaßen vorgehen, um zur ursprünglichen 'Initial RAM-Disk' zurückzukehren:

- Benennen Sie die Kopie passend um. Führen Sie beispielsweise einen Befehl, der ungefähr so aussieht:

  ```
  mv initrd-2.6.16.60-0.21-default_acronis_backup.img initrd-2.6.16.60-0.21-default
  ```

- Spezifizieren Sie die Kopie in der Zeile **initrd** der GRUB-Boot-Loader-Konfiguration.

Dateien wiederherstellen

Dateien in der Cyber Protect-Konsole wiederherstellen

Hinweis
Bei Mandanten, die sich im Compliance-Modus befinden, können Sie keine Backups in der Cyber Protect-Konsole wiederherstellen. Weitere Informationen darüber, wie Sie solche Backups wiederherstellen können, finden Sie in Abschnitt "Backups für Mandanten im Compliance-Modus wiederherstellen" (S. 1196).

1. Wählen Sie diejenige Maschine aus, auf der sich die wiederherzustellenden Daten ursprünglich befunden haben.
2. Klicken Sie auf **Recovery**.
3. Wählen Sie den gewünschten Recovery-Punkt aus. Beachten Sie dabei, dass Recovery-Punkte nach Speicherorten gefiltert werden.

   Falls es sich bei der ausgewählten Maschine um eine physische Maschine handelt und diese offline ist, werden keine Recovery-Punkte angezeigt. Gehen Sie nach einer der folgenden Möglichkeiten vor:
   - [Empfohlen] Sollte sich das Backup im Cloud Storage oder einem freigegebenen Storage befinden (d.h., dass andere Agenten auf diesen zugreifen können), dann klicken Sie zuerst auf den Befehl **Maschine auswählen**. Wählen Sie anschließend eine Zielmaschine, die online ist, und dann den gewünschten Recovery-Punkt.
   - Wählen Sie einen Recovery-Punkt auf der Registerkarte 'Backup Storage'.
   - Laden Sie die Dateien aus dem Cloud Storage herunter.
   - Verwenden Sie ein Boot-Medium.
4. Klicken Sie auf **Wiederherstellen** –> **Dateien/Ordner**.
5. Wechseln Sie zum benötigten Ordner oder verwenden Sie die Suchleiste, um eine Liste der gewünschten Dateien und Ordner abzurufen.

Die Suche ist sprachunabhängig.

Sie können ein oder mehrere Platzhalterzeichen (* und ?) verwenden. Ausführlichere Informationen über die Verwendung von Platzhalterzeichen finden Sie im Abschnitt '"Maske" (S. 505)'.

Hinweis
Für Laufwerk-Backups, die im Cloud Storage gespeichert sind, ist keine Suchfunktion verfügbar.

6. Wählen Sie die Dateien, die Sie wiederherstellen wollen.
7. Falls Sie die Dateien als .zip-Archiv speichern wollen, müssen Sie zuerst auf **Download** klicken, dann den Zielspeicherort für die Daten bestimmen und schließlich auf **Speichern** klicken. Ansonsten können Sie diesen Schritt überspringen.

   Ein Download ist nicht möglich, weil die Gesamtgröße der ausgewählten Dateien 100 MB überschreitet oder weil in Ihrer Auswahl Ordner enthalten sind. Um größere Datenmengen aus der Cloud abzurufen, verwenden Sie die hier Prozedur '"Dateien aus dem Cloud Storage herunterladen" (S. 561)'.
8. Klicken Sie auf **Recovery**.

   Bestimmen Sie bei **Recovery zu** das Ziel für die Wiederherstellungsaktion oder übernehmen Sie das vorgegebene Ziel. Das Standardziel variiert je nach der Datenquelle für das Backup.

   Folgende Ziele sind verfügbar:
   - Die Quellmaschine (falls auf dieser ein Protection Agent installiert ist).

     Dies ist die Maschine, auf der sich die wiederherzustellenden Dateien ursprünglich befunden haben.
   - Andere Maschinen, auf denen ein Protection Agent installiert ist – physische Maschinen, virtuelle Maschinen und Virtualisierungshosts, auf denen ein Protection Agent installiert ist, oder virtuelle Appliances.

     Sie können Dateien zu physischen Maschinen, virtuellen Maschinen und Virtualisierungshosts wiederherstellen, auf denen ein Protection Agent installiert ist. Sie können keine Dateien zu virtuellen Maschinen wiederherstellen, auf denen kein Protection Agent installiert ist (mit Ausnahme von virtuellen Virtuozzo-Maschinen).
   - Virtuozzo-Container oder virtuelle Maschinen.

     Sie können Dateien zu Virtuozzo-Containern und virtuellen Maschinen wiederherstellen, wobei es einige Einschränkungen gibt. Weitere Informationen dazu finden Sie im Abschnitt '"Einschränkungen bei der Wiederherstellung von Dateien in der Cyber Protect-Konsole" (S. 566)'.
9. Wählen Sie bei **Pfad** das gewünschte Ziel für die Wiederherstellung. Sie können eine der folgenden Optionen wählen:
   - [Bei Wiederherstellungen zur ursprünglichen Maschine] Der ursprüngliche Standort.
   - Ein lokaler Ordner oder ein lokal angeschlossener Storage auf der Zielmaschine.

Hinweis
Symbolische Links werden nicht unterstützt.

- Ein Netzwerkordner, auf von der Zielmaschine aus verfügbar ist.

10. Klicken Sie auf **Recovery starten**.
11. Wählen Sie eine der folgenden Optionen zum Überschreiben:
    - **Vorhandene Dateien überschreiben**
    - **Vorhandene Datei überschreiben, wenn diese älter ist**
    - **Vorhandene Dateien nicht überschreiben**

Der Recovery-Fortschritt wird auf der Registerkarte **Aktivitäten** angezeigt.

Dateien aus dem Cloud Storage herunterladen

In der Web Restore-Konsole können Sie den Cloud Storage durchsuchen, den Inhalt der Backups einsehen und gesicherte Dateien und Ordner herunterladen.

Hinweis
Sie können nur auf die Web Restore-Konsole zugreifen, wenn Sie ein Cyber Protection Kunden-Administrator oder ein Kunden-Mandant-Benutzer sind. Die Partnerebenen-Benutzerrollen sind nicht erlaubt.

Einschränkungen

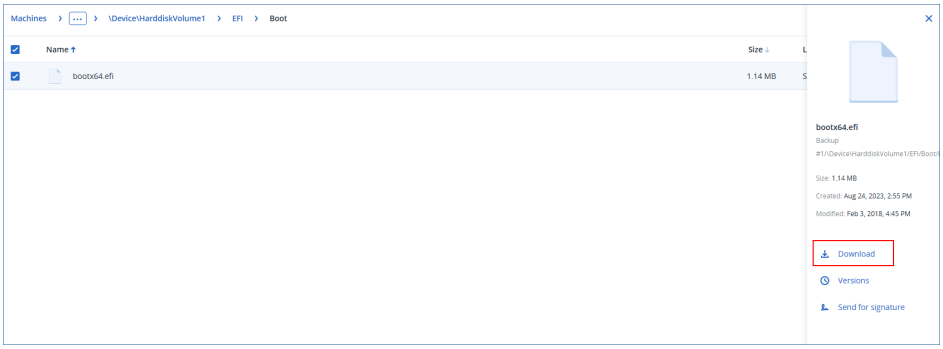
- Sie können keine gesicherten Laufwerke, Volumes oder ganze Recovery-Punkte herunterladen.
- Wenn Sie Backups auf Laufwerksebene (Images) durchsuchen, werden keine logischen Volumes (wie LVM und LDM) angezeigt.
- Sie können keine Backups von Systemzuständen, SQL-Datenbanken und Exchange-Datenbanken durchsuchen.

So können Sie Dateien und Ordner aus dem Cloud Storage herunterladen

1. Wählen Sie in der Cyber Protection-Konsole das gewünschte Laufwerk aus und klicken Sie dann auf **Recovery**.
2. [Wenn mehrere Backup-Speicherorte verfügbar sind] Wählen Sie den Backup-Speicherort aus und klicken Sie dann auf **Weitere Wiederherstellungsmöglichkeiten**.
3. Klicken Sie auf **Dateien herunterladen**.
4. Klicken Sie unter **Maschinen** zuerst auf den Workload-Namen und dann auf das Backup-Archiv. Ein Backup-Archiv enthält ein oder mehrere Backups (Recovery-Punkte).
5. Klicken Sie auf die Backup-Nummer (Recovery-Punkt), aus dem Sie Dateien oder Ordner herunterladen wollen – und navigieren Sie dann zu den gewünschten Elementen.
6. Aktivieren Sie die Kontrollkästchen derjenigen Elemente, die Sie herunterladen wollen.

Hinweis
Wenn Sie mehrere Elemente auswählen, werden diese in einer ZIP-Datei heruntergeladen.

7. Klicken Sie auf **Download**.



Die Authentizität von Dateien mit dem Notary Service überprüfen

Falls die Beglaubigungsfunktion (Notarization) während eines Backups aktiviert wurde, können Sie später bei Bedarf die Authentizität einer gesicherten Datei überprüfen.

So können Sie die Authentizität von Dateien überprüfen

1. Wählen Sie die gewünschte Datei aus, wie es in den Schritten 1-6 des Abschnitts 'Dateien über die Weboberfläche wiederherstellen' oder in den Schritten 1-5 des Abschnitts 'Dateien aus dem Cloud Storage herunterladen' beschrieben ist.
2. Überprüfen Sie, dass die ausgewählte Datei mit dem folgenden Symbol gekennzeichet ist:  . Das bedeutet, dass die Datei 'beglaubigt' (notarized) ist.
3. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Klicken Sie auf **Verifizieren**.
     Die Software überprüft die Authentizität der Datei und zeigt das Ergebnis an.
   - Klicken Sie auf **Zertifikat abrufen**.
     Ein Zertifikat, das die Dateibeglaubigung bestätigt, wird in einem Webbrowser-Fenster geöffnet. In dem Fenster werden außerdem Anweisungen angezeigt, wie Sie die Dateiauthentizität manuell überprüfen können.

Eine Datei mit ASign signieren

Hinweis
Diese Funktion ist über das Advanced Backup-Paket verfügbar.

ASign ist ein Service, der es ermöglicht, dass mehrere Personen eine per Backup gesicherte Datei elektronisch unterschreiben (signieren) können. Diese Funktion ist nur für Backups auf Dateiebene verfügbar, die im Cloud Storage gespeichert sind.

Es kann nur je eine Dateiversion gleichzeitig signiert werden. Wenn eine Datei also zu mehreren Zeitpunkten gesichert wurde, müssen Sie die gewünschte Version bestimmten, die signiert werden soll – und nur diese Version wird dann signiert.

ASign kann beispielsweise verwendet werden, um folgende Dateien elektronisch zu signieren:

- Miet- oder Leasing-Verträge
- Kaufverträge
- Kaufvereinbarungen für Wertgegenstände
- Kreditverträge
- Berechtigungsscheine
- Finanzdokumente
- Versicherungsdokumente
- Haftungsverzichtserklärungen
- Gesundheitsdokumente
- Forschungsunterlagen
- Authentizitätzertifikate für Produkte
- Geheimhaltungsvereinbarungen
- Schriftliche Angebote
- Vertraulichkeitsvereinbarungen
- Vereinbarungen mit unabhängigen Vertragspartnern

So können Sie eine Dateiversion signieren

1. Wählen Sie die gewünschte Datei aus, wie es in den Schritten 1-6 des Abschnitts 'Dateien über die Weboberfläche wiederherstellen' oder in den Schritten 1-5 des Abschnitts 'Dateien aus dem Cloud Storage herunterladen' beschrieben ist.
2. Überprüfen Sie im linken Fensterbereich, dass der korrekte Zeitpunkt (Datum, Uhrzeit) ausgewählt wurde.
3. Klicken Sie auf **Diese Dateiversion signieren**.
4. Spezifizieren Sie das Kennwort für das Cloud Storage-Konto, unter dem das Backup gespeichert wurde. Der Anmeldename des Kontos wird im Eingabeaufforderungsfenster angezeigt.
   Die Benutzeroberfläche des ASign Service wird in einem Webbrowser-Fenster geöffnet.
5. Fügen Sie bei Bedarf weitere Unterzeichner hinzu, indem Sie deren E-Mail-Adressen spezifizieren. Nach dem Versenden der Einladungen können keine weiteren Unterzeichner mehr hinzugefügt oder entfernt werden. Überprüfen Sie daher, dass auch wirklich alle Personen in der Liste sind, deren Signatur erforderlich ist.
6. Klicken Sie auf **Zum Signieren einladen**, damit die Einladung an die Unterzeichner versendet wird.

Jeder Unterzeichner erhält eine E-Mail-Nachricht mit der Signatur-Aufforderung. Wenn alle angeforderten Unterzeichner die Datei signiert haben, wird diese noch vom Notary Service beglaubigt und signiert.

Sie erhalten jeweils Benachrichtigungen, wenn ein Unterzeichner die Datei signiert hat und wenn der komplette Prozess abgeschlossen wurde. Sie können auf die ASign-Webseite zugreifen, indem Sie in einer der E-Mail-Nachrichten, die Sie erhalten, auf **Details anzeigen** klicken.

7. Gehen Sie nach Abschluss des Prozesses zur ASign-Webseite und klicken Sie auf **Dokument abrufen**, um ein .pdf-Dokument herunterzuladen, welches folgende Informationen enthält:
   - Eine Signaturzertifikatsseite mit den zusammengestellten Signaturen.
   - Eine Audit-Trail-Seite mit einem Verlauf folgender Aktivitäten: wann die Einladung an die Unterzeichner gesendet wurde, wann der Unterzeichner die Datei signiert hat usw.

Dateien mit einem Boot-Medium wiederherstellen

Genau Informationen über die Erstellung eines Boot-Mediums finden Sie im Abschnitt 'Ein Boot-Medium erstellen'.

So können Sie Dateien mithilfe eines Boot-Mediums wiederherstellen

1. Booten Sie die Zielmaschine mit dem Boot-Medium.
2. Klicken Sie entweder auf **Diese Maschine lokal verwalten** oder zweimal auf **Rescue Bootable Media** (abhängig vom verwendeten Typ des Mediums).
3. Falls in Ihrem Netzwerk ein Proxy-Server verwendet wird, klicken Sie auf **Tools** –> **Proxy-Server** und spezifizieren Sie dann den Host-Namen/die IP-Adresse, den Port und die Anmeldedaten des Proxy-Servers. Ansonsten können Sie diesen Schritt überspringen.
4. [Optional] Klicken Sie bei der Wiederherstellung von Windows oder Linux auf **Tools** –> **Medium im Cyber Protection Service registrieren** und spezifizieren Sie dann das Registrierungstoken, welches Sie beim Download des Mediums erhalten haben. Wenn Sie dies tun, müssen Sie keine Anmeldedaten oder keinen Registrierungscode eingeben, um auf den Cloud Storage zuzugreifen (wie in Schritt 7 beschrieben).
5. Klicken Sie innerhalb der Willkommensseite auf **Recovery**.
6. Klicken Sie auf **Daten wählen** und dann auf **Durchsuchen**.
7. Spezifizieren Sie den Backup-Speicherort:
   - Wählen Sie das Element **Cloud Storage**, um Dateien aus dem Cloud Storage wiederherzustellen. Geben Sie die Anmeldedaten des Kontos ein, dem die gesicherte Maschine zugewiesen wird.

     Bei der Wiederherstellung von Windows oder Linux haben Sie die Möglichkeit, einen Registrierungscode anzufordern und diesen statt der Anmeldeinformationen zu verwenden. Klicken Sie auf **Registrierungscode verwenden** –> **Den Code anfordern**. In der Software werden der Registrierungslink und Registrierungscode angezeigt. Sie können diese kopieren und die Registrierungsschritte dann auf einer anderen Maschine durchführen. Der Registrierungscode ist für eine (1) Stunde gültig.

- Um eine Wiederherstellung von einem lokalen Ordner oder einem Netzwerkordner aus durchzuführen, wählen Sie den entsprechenden Ordner über das Element **Lokale Ordner** oder **Netzwerkordner** aus.
- Wenn Sie Wiederherstellungen von Backup-Speicherorten auf einem Public Cloud Storage (wie Microsoft Azure, Amazon S3, Wasabi oder andere S3-kompatible Storages) durchführen wollen, müssen Sie zuerst auf **Medium im Cyber Protection Service registrieren** klicken und dann die Wiederherstellung über die Weboberfläche konfigurieren. Weitere Informationen darüber, wie Sie die entsprechenden Medien remote über die Weboberfläche verwalten können, finden Sie unter "Remote-Aktionen mit einem Boot-Medium" (S. 797).

Klicken Sie auf **OK**, um Ihre Auswahl zu bestätigen.

8. Wählen Sie das Backup, aus dem die Daten wiederhergestellt werden sollen. Geben Sie das Kennwort für das Backup an, falls Sie dazu aufgefordert werden.
9. Wählen Sie bei **Backup-Inhalte** das Element **Ordner/Dateien**.
10. Wählen Sie Daten, die Sie wiederherstellen wollen. Klicken Sie auf **OK**, um Ihre Auswahl zu bestätigen.
11. Spezifizieren Sie bei **Recovery-Ziel** einen gewünschten Ordner. Optional können Sie neuere Dateiversionen vor Überschreibung schützen oder einige Dateien von der Wiederherstellung ausschließen.
12. [Optional] Klicken Sie auf **Recovery-Optionen**, um zusätzliche Einstellungen zu spezifizieren.
13. Wählen Sie **OK**, um die Wiederherstellung zu starten.

Dateien aus lokalen Backups extrahieren

Sie können Backups nach bestimmten Inhalten durchsuchen und gewünschte Dateien extrahieren.

Anforderungen

- Diese Funktionalität steht nur unter Windows und bei Verwendung des Windows Datei-Explorers zur Verfügung.
- Folgende, im Backup gesicherte Dateisysteme werden dabei unterstützt: FAT16, FAT32, NTFS, ReFS, Ext2, Ext3, Ext4, XFS oder HFS+.

Voraussetzungen

- Auf der Maschine, von der aus Sie ein Backup durchsuchen wollen, muss ein Protection Agent installiert sein.
- Das Backup selbst muss entweder in einem lokalen Ordner oder in einer Netzwerkfreigabe (SMB/CIFS) gespeichert sein.

So können Sie Dateien aus einem Backup extrahieren

1. Verwenden Sie den Windows Datei-Explorer, um den Speicherort des Backups aufzurufen.
2. Klicken Sie doppelt auf die Backup-Datei. Die Dateinamen basieren auf folgender Vorlage:
   `<Maschinenname> - <Schutzplan-GUID>`

3. Wenn das Backup verschlüsselt ist, müssen Sie das entsprechende Kennwort eingeben. Ansonsten können Sie diesen Schritt überspringen.
   Der Windows Datei-Explorer zeigt die Recovery-Punkte an.
4. Klicken Sie doppelt auf einen gewünschten Recovery-Punkt.
   Der Windows Datei-Explorer zeigt die im Backup gespeicherten Daten an.
5. Wählen Sie den gewünschten Ordner aus.
6. Kopieren Sie die benötigten Dateien zu einem beliebigen Ordner im Dateisystem.

Einschränkungen bei der Wiederherstellung von Dateien in der Cyber Protect-Konsole

Mandanten im Compliance-Modus

Bei Mandanten, die sich im Compliance-Modus befinden, können Sie keine Backups in der Cyber Protect-Konsole wiederherstellen. Weitere Informationen darüber, wie Sie solche Backups wiederherstellen können, finden Sie in Abschnitt "Backups für Mandanten im Compliance-Modus wiederherstellen" (S. 1196).

Wiederherstellungen zu Virtuozzo-Containern oder virtuellen Virtuozzo-Maschinen

- Der QEMU-Gast-Agent muss auf der virtuellen Zielmaschine installiert sein.
- [Nur bei Wiederherstellungen zu Containern anwendbar] Mount-Punkte innerhalb von Containern können nicht als Wiederherstellungsziel verwendet werden. Sie können beispielsweise keine Dateien zu einem zweiten Laufwerk oder einer NFS-Freigabe wiederherstellen, die in einem Container gemountet ist.
- Wenn Sie Dateien zu einer virtuellen Windows-Maschine wiederherstellen und die Recovery-Option '"Dateisicherheitseinstellungen" (S. 572)' aktiviert ist, wird für die wiederhergestellten Dateien das Dateiattribut 'Archiv' festgelegt.
- Dateien, die Nicht-ANSI-Zeichen in ihrem Namen enthalten, werden auf Maschinen mit Windows Server 2012 (oder höher) und auf Maschinen mit Windows 7 (oder höher) mit falschen Namen wiederhergestellt.
- Wenn Sie Dateien zu virtuellen CentOS- oder Red Hat Enterprise Linux-Maschinen wiederherstellen möchten, die auf einem Virtuozzo Hybrid Server laufen, müssen Sie die Datei `qemu-ga` folgendermaßen bearbeiten:
  - Gehen Sie auf der virtuellen Zielmaschine zu `/etc/sysconfig/` und öffnen Sie dort die Datei `qemu-ga` zur Bearbeitung.
  - Gehen Sie in die folgende Zeile und löschen Sie alles nach dem Gleichheitszeichen (=):

    ```
    BLACKLIST_RPC=
    ```

  - Starten Sie den QEMU-Gast-Agenten neu, indem Sie folgenden Befehl ausführen:

    ```
    systemctl restart qemu-guest-agent
    ```

Systemzustand wird wiederhergestellt

Hinweis
Bei Mandanten, die sich im Compliance-Modus befinden, können Sie keine Backups in der Cyber Protect-Konsole wiederherstellen. Weitere Informationen darüber, wie Sie solche Backups wiederherstellen können, finden Sie in Abschnitt "Backups für Mandanten im Compliance-Modus wiederherstellen" (S. 1196).

1. Wählen Sie diejenige Maschine, deren Systemzustand Sie wiederherstellen wollen.
2. Klicken Sie auf **Recovery**.
3. Wählen Sie einen Systemzustand-Recovery-Punkt. Beachten Sie dabei, dass Recovery-Punkte nach Speicherorten gefiltert werden.
4. Klicken Sie auf **Systemzustand wiederherstellen**.
5. Bestätigen Sie, dass der vorliegende Systemzustand mit der Version überschrieben werden soll, die im Backup vorliegt.

Der Recovery-Fortschritt wird auf der Registerkarte **Aktivitäten** angezeigt.

Eine ESXi-Konfiguration wiederherstellen

Um eine ESXi-Konfiguration wiederherstellen zu können, benötigen Sie ein Linux-basiertes Boot-Medium. Informationen über die Erstellung eines Boot-Mediums finden Sie im Abschnitt '"Ein physisches Boot-Medium erstellen" (S. 778)'.

Wenn Sie für die Wiederherstellung einer ESXi-Konfiguration einen anderen als den ursprünglichen Host als Ziel verwenden wollen und der ursprüngliche ESXi-Host noch mit dem vCenter Server verbunden ist, sollten Sie diesen ursprünglichen Host vom vCenter Server trennen und entfernen, um unerwartete Probleme bei der Wiederherstellung zu vermeiden. Wenn Sie den ursprünglichen Host gemeinsam mit dem wiederhergestellten Host weiter behalten/verwenden wollen, können Sie ihn nach Abschluss der Wiederherstellung wieder hinzufügen.

Evtl. auf dem Host laufende virtuelle Maschinen werden nicht in das ESXi-Konfigurations-Backup eingeschlossen. Sie können diese jedoch separat per Backup sichern und wiederherstellen.

So stellen Sie eine ESXi-Konfiguration wieder her

1. Booten Sie die Zielmaschine mit dem Boot-Medium.
2. Klicken Sie auf **Diese Maschine lokal verwalten**.
3. Klicken Sie innerhalb der Willkommensseite auf **Recovery**.
4. Klicken Sie auf **Daten wählen** und dann auf **Durchsuchen**.
5. Spezifizieren Sie den Backup-Speicherort:
   - Wählen Sie den gewünschten Ordner unter **Lokale Ordner** oder **Netzwerkordner** aus.

   Klicken Sie auf **OK**, um Ihre Auswahl zu bestätigen.

6. Wählen Sie bei **Anzeigen** das Element **ESXi-Konfiguration**.
7. Wählen Sie das Backup, aus dem die Daten wiederhergestellt werden sollen. Geben Sie das Kennwort für das Backup an, falls Sie dazu aufgefordert werden.
8. Klicken Sie auf **OK**.
9. Bei **Für neue Datenspeicher zu verwendende Laufwerke** gehen Sie folgendermaßen vor:
   - Wählen Sie bei **ESXi wiederherstellen zu** dasjenige Laufwerk, auf dem die Host-Konfiguration wiederhergestellt werden soll. Wenn Sie den ursprünglichen Host als Ziel für die Wiederherstellung der Konfiguration verwenden, wird das ursprüngliche Laufwerk standardmäßig vorausgewählt.
   - [Optional] Wählen Sie bei **Für neue Datenspeicher verwenden** die Laufwerke, auf denen die neuen Datenspeicher erstellt werden sollen. Beachten Sie, dass dabei alle (möglicherweise bereits vorhandenen) Daten auf den ausgewählten Laufwerken verloren gehen. Falls Sie die virtuellen Maschinen in den vorhandenen Datenspeichern bewahren wollen, wählen Sie kein Laufwerk aus.
10. Falls Sie Laufwerke für neue Datenspeicher auswählen, bestimmen Sie auch die Methode, wie diese erstellt werden sollen. Verwenden Sie dazu die Befehle **Einen Datenspeicher auf allen ausgewählten Laufwerken erstellen: Einen Datenspeicher pro Laufwerk erstellen** oder **Einen Datenspeicher auf allen ausgewählten Laufwerken erstellen**.
11. [Optional] Ändern Sie gegebenenfalls bei **Netzwerkzuordnung**, wie die automatische Zuordnung die (im Backup vorliegenden) virtuellen Switche den physischen Netzwerkadaptern zugeordnet hat.
12. [Optional] Klicken Sie auf **Recovery-Optionen**, um zusätzliche Einstellungen zu spezifizieren.
13. Wählen Sie **OK**, um die Wiederherstellung zu starten.

Recovery-Optionen

Wenn Sie die Recovery-Optionen ändern wollen, klicken Sie während der Konfiguration der Wiederherstellung auf **Recovery-Optionen**.

Verfügbarkeit der Recovery-Optionen

Art und Umfang der verfügbaren Recovery-Optionen sind abhängig von:

- Der Umgebung, in welcher der Agent seine Recovery-Aktionen durchführt (Windows, Linux, macOS oder ein Boot-Medium).
- Die Art der wiederherzustellenden Daten (Laufwerke, Dateien, virtuelle Maschinen, Applikationsdaten).

Die nachfolgende Tabelle fasst die Verfügbarkeit der Recovery-Optionen zusammen:

	Laufwerke	Dateien	Virtuelle Maschinen	SQL und Exchange

	Windows	Linux	Boot-Medium	Windows	Linux	macOS	Boot-Medium	ESXi, Hyper-V und Virtuozzo	Windows
Backup-Validierung	+	+	+	+	+	+	+	+	+
Boot-Modus	+	-	-	-	-	-	-	+	-
Zeitstempel für Dateien	-	-	-	+	+	+	+	-	-
Fehlerbehandlung	+	+	+	+	+	+	+	+	+
Dateifilter (Ausschluss)	-	-	-	+	+	+	+	-	-
Dateisicherheitseinstellungen	-	-	-	+	-	-	-	-	-
Flashback	+	+	+	-	-	-	-	+	-
Wiederherstellung mit vollständigem Pfad	-	-	-	+	+	+	+	-	-
Mount-Punkte	-	-	-	+	-	-	-	-	-
Performance	+	+	-	+	+	+	-	+	+
Vor-/Nach-Befehle	+	+	-	+	+	+	-	+	+
SID ändern	+	-	-	-	-	-	-	-	-
VM-Energieverwaltung	-	-	-	-	-	-	-	+	-
Windows-Ereignisprotokoll	+	-	-	+	-	-	-	Nur Hyper-V	+

Backup-Validierung

Diese Option definiert, ob ein Backup vor der Wiederherstellung der darin enthaltenen Daten zu validieren ist, um sicherzustellen, dass das Backup nicht beschädigt ist. Diese Aktion wird vom Protection Agenten durchgeführt.

Die Voreinstellung ist: **Deaktiviert**.

Weitere Informationen zur Validierung mittels Prüfsummen-Verifizierung finden Sie im Abschnitt '"Prüfsummen-Verifizierung" (S. 222)'.

Hinweis
Abhängig von den Einstellungen, die Ihr Service Provider vorgenommen hat, kann es sein, dass keine Validierung verfügbar ist, wenn Sie ein Backup auf dem Cloud Storage erstellen.

Boot-Modus

Diese Option ist nur wirksam, wenn Sie eine physische oder virtuelle Maschine aus einem Laufwerk-Backup wiederherstellen, welches ein Windows-Betriebssystem enthält.

Mit dieser Option können Sie den Boot-Modus (BIOS oder UEFI) festlegen, den Windows nach der Wiederherstellung verwenden soll. Wenn der Boot-Modus der ursprünglichen Maschine anders als der ausgewählte Boot-Modus ist, wird die Software:

- Das Laufwerk, auf dem Sie das System-Volume wiederherstellen, entsprechend dem ausgewählten Boot-Modus initialisieren (MBR für BIOS, GPT für UEFI).
- Das Windows-Betriebssystem so anpassen, dass es mit dem ausgewählten Boot-Modus starten kann.

Die Voreinstellung ist: **Wie bei der Zielmaschine.**

Sie können eine der folgenden Varianten wählen:

- **Wie bei der Zielmaschine**
  Der Agent, der auf dem Zielmaschine läuft, erkennt den aktuell von Windows verwendeten Boot-Modus und nimmt dann die Einstellungen entsprechend dem erkannten Boot-Modus vor.
  Dies ist der sicherste Wert, der automatisch zu einem bootfähigen System führt – außer die unten aufgeführten Einschränkungen treffen zu. Da die Option **Boot-Modus** unter einem Boot-Medium nicht verfügbar ist, verhält sich der Agent des Boot-Mediums immer so, als wäre dieser Wert ausgewählt worden.
- **Wie bei der gesicherten Maschine**
  Der Agent, der auf dem Zielmaschine läuft, liest den Boot-Modus aus dem Backup aus und nimmt dann die Einstellungen so vor, dass sie zu diesem Boot-Modus passen. Damit können Sie ein System auch auf einer anderen Maschine wiederherstellen, wenn diese Maschine einen anderen Boot-Modus verwendet, und dann das Laufwerk in der gesicherten Maschine austauschen.
- **BIOS**
  Der Agent, der auf der Zielmaschine läuft, nimmt die Einstellungen zur Verwendung des BIOS-Modus vor.
- **UEFI**
  Der Agent, der auf der Zielmaschine läuft, nimmt die Einstellungen zur Verwendung des UEFI-Modus vor.

Sobald eine Einstellung geändert wurde, wird die Laufwerkszuordnungsprozedur wiederholt. Dies wird einige Zeit benötigen.

Empfehlungen

Wenn Sie Windows zwischen UEFI und BIOS migrieren müssen:

- Stellen Sie das komplette Laufwerk, auf dem sich das System-Volume befindet, wieder her. Wenn Sie nur das System-Volume über ein vorhandenes Volume wiederherstellen, wird der Agent das Ziellaufwerk nicht richtig initialisieren können.
- Beachten Sie, dass Sie mit dem BIOS-Standard den Speicherplatz auf Festplatten nur bis zu einer Grenze von 2 TB ansprechen können.

Einschränkungen

- Eine Migration zwischen UEFI und BIOS wird unterstützt für:
  - Die 64-Bit-Versionen aller Windows-Betriebssysteme, beginnend mit Windows 7
  - Die 64-Bit-Versionen aller Windows-Betriebssysteme, beginnend mit Windows Server 2008 SP1
- Eine Migration zwischen UEFI und BIOS wird nicht unterstützt, wenn sich das Backup auf einem Bandgerät befindet.

Wenn die Migration eines Systems zwischen UEFI und BIOS nicht unterstützt wird, verhalten sich die Agenten so, als wäre die Einstellung **Wie bei der gesicherten Maschine** ausgewählt worden. Wenn die Zielmaschine sowohl UEFI als auch BIOS unterstützen, müssen Sie den Boot-Modus manuell aktivieren, der der ursprünglichen Maschine entspricht. Anderenfalls wird das System nicht mehr booten.

Zeitstempel für Dateien

Diese Option gilt nur für die Wiederherstellung von Dateien.

Diese Option bestimmt, ob wiederhergestellte Dateien den ursprünglichen Zeitstempel aus dem Backup übernehmen – oder ob ihnen das Datum/die Zeit des aktuellen Wiederherstellungszeitpunkts zugewiesen wird.

Wenn diese Option aktiviert ist, werden den Dateien die aktuelle Zeit und das aktuelle Datum zugewiesen.

Die Voreinstellung ist: **Aktiviert**.

Fehlerbehandlung

Diese Optionen ermöglichen Ihnen vorzugeben, wie auftretende Fehler während einer Recovery-Aktion behandelt werden.

Erneut versuchen, wenn ein Fehler auftritt

Die Voreinstellung ist: **Aktiviert. Anzahl der Versuche: 30. Intervall zwischen den Versuchen: 30 Sekunden.**

Wenn ein behebbarer Fehler auftritt, versucht das Programm, die erfolglose Aktion erneut durchzuführen. Sie können das Zeitintervall und die Anzahl der Versuche einstellen. Die Versuche werden aufgegeben, wenn entweder die Aktion erfolgreich ist ODER die angegebene Anzahl an Versuchen erreicht wurde, je nachdem, was zuerst eintritt.

Während der Durchführung keine Meldungen bzw. Dialoge anzeigen (Stiller Modus)

Die Voreinstellung ist: **Deaktiviert**.

Wenn der stille Modus eingeschaltet ist, kann das Programm Situationen automatisch behandeln, die einen Benutzereingriff erfordern, falls das möglich ist. Falls eine Aktion nicht ohne Benutzereingriff fortfahren kann, wird sie fehlschlagen. Detaillierte Informationen über die Aktion, einschließlich eventueller Fehler, finden Sie im Log der Aktion.

Systeminformationen speichern, wenn eine Wiederherstellung mit Neustart fehlschlägt

Diese Option gilt für Wiederherstellungen von Laufwerken/Volumes zu einer physischen Maschine, die unter Windows oder Linux läuft.

Die Voreinstellung ist: **Deaktiviert**.

Wenn diese Option aktiviert ist, können Sie einen Ordner auf einem lokalen Laufwerk (einschließlich an die Zielmaschine angeschlossene USB-Sticks und Festplatten) oder eine Netzwerkfreigabe spezifizieren, wo die Protokoll-, Systeminformations- und Crash-Dump-Dateien gespeichert werden sollen. Diese Informationen können den Mitarbeitern des technischen Supports helfen, das entsprechende Problem zu identifizieren.

Dateifilter (Ausschluss)

Diese Option gilt nur für die Wiederherstellung von Dateien.

Diese Option definiert, welche Dateien und Ordner während eines Recovery-Prozesses übersprungen und so von der Liste der wiederherzustellenden Elemente ausgeschlossen werden.

Hinweis
Ausschließungen überschreiben eine mögliche Auswahl von wiederherzustellenden Datenelementen. Falls Sie beispielsweise festlegen, dass die Datei 'MeineDatei.tmp' wiederhergestellt werden soll und Sie aber zudem alle .tmp-Dateien ausschließen, dann wird 'MeineDatei.tmp' nicht wiederhergestellt.

Dateisicherheitseinstellungen

Diese Option gilt, wenn Sie Dateien aus Laufwerk- und Datei-Backups von NTFS-formatierten Volumes wiederherstellen.

Diese Option definiert, ob die NTFS-Zugriffsrechte für Dateien zusammen mit den Dateien wiederhergestellt werden.

Die Voreinstellung ist: **Aktiviert**.

Sie können wählen, ob die Dateien bei der Wiederherstellung ihre ursprünglichen Zugriffsrechte aus dem Backup beibehalten sollen – oder ob sie die NTFS-Berechtigungen desjenigen Ordner übernehmen sollen, in dem sie wiederhergestellt werden.

Flashback

Diese Option gilt – ausgenommen beim Mac – für die Wiederherstellung von Laufwerken und Volumes auf physischen und virtuellen Maschinen.

Diese Option funktioniert nur, wenn das Volume-Layout des gerade wiederhergestellten Laufwerks exakt mit dem des Ziellaufwerks übereinstimmt.

Wenn diese Option aktiviert ist, werden nur solche Daten wiederhergestellt, hinsichtlicher derer sich das Backup und das Ziellaufwerk unterscheiden. Dadurch kann die Wiederherstellung von physischen und virtuellen Maschinen beschleunigt werden. Der Datenvergleich erfolgt auf Blockebene.

Wenn Sie eine physische Maschine wiederherstellen, ist die Voreinstellung: **Deaktiviert**.

Bei der Wiederherstellung einer virtuellen Maschine ist die Voreinstellung: **Aktiviert**.

Wiederherstellung mit vollständigem Pfad

Diese Option gilt nur, wenn Daten aus einem Datei-Backup wiederhergestellt werden.

Wenn diese Option aktiviert wird, erhalten die Dateien am Zielspeicherort wieder ihren vollständigen (ursprünglichen) Pfad.

Die Voreinstellung ist: **Deaktiviert**.

Mount-Punkte

Diese Option gilt nur unter Windows und wenn Daten aus einem Datei-Backup wiederhergestellt werden.

Aktivieren Sie diese Option, um Dateien und Ordner wiederherzustellen, die auf gemounteten Volumes gespeichert waren und mit aktivierter Option 'Mount-Punkte' gesichert wurden.

Die Voreinstellung ist: **Deaktiviert**.

Diese Option ist nur wirksam, wenn Sie einen Ordner wiederherstellen wollen, der in der Verzeichnishierarchie höher als der Mount-Punkt liegt. Wenn Sie einen Ordner innerhalb des Mount-Punktes oder den Mount-Punkt selbst für eine Recovery-Aktion wählen, werden die gewählten Elemente unabhängig vom Wert der Option '**Mount-Punkte**' wiederhergestellt.

Hinweis
Beachten Sie, dass für den Fall, dass das Volume zum Recovery-Zeitpunkt nicht gemountet ist, die Daten direkt zu demjenigen Ordner wiederhergestellt werden, der zum Backup-Zeitpunkt der Mount-Punkt war.

Performance

Diese Option bestimmt, welche Priorität dem Recovery-Prozess innerhalb des Betriebssystems zugewiesen wird.

Die verfügbaren Einstellungen sind: **Niedrig**, **Normal**, **Hoch**.

Voreinstellung ist: **Normal**.

Die Priorität eines Prozesses, der in einem System ausgeführt wird, bestimmt, wie viele CPU-und System-Ressourcen ihm zugewiesen werden. Durch ein Herabsetzen der Recovery-Priorität werden mehr Ressourcen für andere Applikationen freigeben. Das Heraufsetzen der Recovery-Priorität kann den Wiederherstellungsprozess beschleunigen, indem z.B. CPU-Ressourcen von anderen gleichzeitig laufenden Prozessen abgezogen werden. Der Effekt ist aber abhängig von der totalen CPU-Auslastung und anderen Faktoren wie der Schreibgeschwindigkeit der Festplatte oder dem Datenverkehr im Netzwerk.

Vor-/Nach-Befehle

Diese Option ermöglicht die Definition von Befehlen, die automatisch vor oder nach der Datenwiederherstellung durchgeführt werden.

So benutzen Sie diese Vor- bzw. Nach-Befehle:

- Starten Sie den Befehl **Checkdisk**, damit logische Fehler im Dateisystem, physische Fehler oder fehlerhafte Sektoren vor Beginn oder nach Ende der Recovery-Aktion gefunden und behoben werden.

Das Programm unterstützt keine interaktiven Befehle, d.h. Befehle, die eine Reaktion des Benutzers erfordern (wie z.B. 'Pause').

Ein 'Nach-Recovery'-Befehl wird nicht ausgeführt, wenn die Wiederherstellung einen Neustart benötigt bzw. ausführt.

Befehl vor Recovery

So spezifizieren Sie einen Befehl bzw. eine Stapelverarbeitungsdatei, die vor dem Start der Wiederherstellung ausgeführt wird

1. Aktivieren Sie den Schalter **Einen Befehl vor der Wiederherstellung ausführen**.
2. Geben Sie im Feld **Befehl** ein Kommando ein oder wählen Sie eine vorbereitete Stapelverarbeitungsdatei aus dem Dateisystem aus. Das Programm unterstützt keine interaktiven Befehle, d.h. Befehle, die eine Reaktion des Benutzers erfordern (wie z.B. 'Pause').

3. Spezifizieren Sie im Eingabefeld **Arbeitsverzeichnis** einen Pfad zu einem Verzeichnis, in dem der Befehl bzw. die Stapelverarbeitungsdatei durchgeführt werden soll.
4. Tragen Sie Argumente für die Befehlsausführung in das Feld **Argumente** ein, wenn das erforderlich ist.
5. Wählen Sie in der unteren Tabelle die passenden Optionen, abhängig vom Ergebnis, das Sie erreichen wollen.
6. Klicken Sie auf **Fertig**.

Kontrollkästchen	**Auswahl**			
Wiederherstellung scheitern lassen, wenn die Befehlsausführung fehlschlägt*	Ausgewählt	Deaktiviert	Ausgewählt	Deaktiviert
Wiederherstellung erst ausführen, wenn die Befehlsausführung abgeschlossen ist	Ausgewählt	Ausgewählt	Deaktiviert	Deaktiviert
Ergebnis				
	Voreinstellung Recovery nur durchführen, nachdem der Befehl erfolgreich ausgeführt wurde. Wiederherstellung scheitern lassen, wenn die Befehlsausführung fehlschlägt.	Recovery nach Befehlsausführung fortsetzen, unabhängig vom Erfolg oder Misserfolg der Ausführung.	Nicht verfügbar	Recovery gleichzeitig mit Befehlsausführung durchführen, unabhängig vom Ergebnis der Befehlssausführung.

* Ein Befehl wird als 'fehlgeschlagen' betrachtet, wenn sein Exit-Code ungleich Null ist.

Befehl nach Recovery

So spezifizieren Sie einen Befehl bzw. eine Stapelverarbeitungsdatei, die ausgeführt wird, wenn die Wiederherstellung vollständig ist

1. Aktivieren Sie den Schalter **Einen Befehl nach der Wiederherstellung ausführen**.
2. Geben Sie im Feld **Befehl** ein Kommando ein oder wählen Sie eine vorbereitete Stapelverarbeitungsdatei aus dem Dateisystem aus.

3. Spezifizieren Sie im Eingabefeld **Arbeitsverzeichnis** einen Pfad zu einem Verzeichnis, in dem der Befehl bzw. die Stapelverarbeitungsdatei durchgeführt werden soll.
4. Tragen Sie, sofern erforderlich, in das Feld **Argumente** entsprechende Parameter für die Befehlsausführung ein.
5. Aktivieren Sie das Kontrollkästchen **Wiederherstellung scheitern lassen, wenn die Befehlsausführung fehlschlägt**, sofern eine erfolgreiche Ausführung des Befehls besonders wichtig für Sie ist. Der Befehl wird als 'fehlgeschlagen' betrachtet, wenn sein Exit-Code ungleich Null ist. Sollte die Befehlsausführung fehlschlagen, erhält der Recovery-Status den Wert '**Fehler**'.
   Wenn das Kontrollkästchen deaktiviert ist, hat das Ergebnis der Befehlsausführung keinen Einfluss darauf, ob die Recovery-Ausführung als erfolgreich oder fehlgeschlagen eingestuft wird. Sie können das Ergebnis der Befehlsausführung in der Registerkarte **Aktivitäten** überwachen.
6. Klicken Sie auf **Fertig**.

Hinweis
Ein 'Nach-Recovery'-Befehl wird nicht ausgeführt, wenn die Wiederherstellung einen Neustart benötigt bzw. ausführt.

SID ändern

Diese Option ist gültig, wenn Sie Windows 8.1/Windows Server 2012 R2 (oder früher) wiederherstellen.

Diese Option ist nicht gültig, wenn eine Wiederherstellung zu einer virtuellen Maschine (als Ziel) durchgeführt wird und dafür ein Agent für VMware, ein Agent für Hyper-V, ein Agent für Scale Computing HC3 oder ein Agent für oVirt verwendet wird.

Die Voreinstellung ist: **Deaktiviert**.

Die Software kann eine eindeutige SID (Computer Security Identifier) für das wiederhergestellte Betriebssystem erstellen. Sie benötigen diese Option nur, wenn Sie die Betriebsfähigkeit von Drittanbieter-Software sicherstellen müssen, die von der Computer-SID abhängt.

Eine Änderung der SID auf einem bereitgestellten oder wiederhergestellten System wird von Microsoft offiziell nicht unterstützt. Wenn Sie diese Option verwenden, tun Sie dies also auf eigenes Risiko hin.

VM-Energieverwaltung

Diese Optionen sind nicht gültig, wenn eine Wiederherstellung zu einer virtuellen Maschine (als Ziel) durchgeführt wird und dafür ein Agent für VMware, ein Agent für Hyper-V, ein Agent für Virtuozzo, ein Agent für Scale Computing HC3 oder ein Agent für oVirt verwendet wird.

Virtuelle Zielmaschinen bei Start der Wiederherstellung ausschalten

Die Voreinstellung ist: **Aktiviert**.

Eine vorhandene Maschine kann nicht als Wiederherstellungsziel verwendet werden, solange sie online ist. Mit dieser Option wird die Zielmaschine automatisch ausgeschaltet, sobald die Wiederherstellung startet. Möglicherweise vorhandene/aktive Benutzer werden dabei von der Maschine getrennt und nicht gespeicherte Daten gehen verloren.

Deaktivieren Sie das Kontrollkästchen für diese Option, wenn Sie die virtuelle Maschinen vor der Wiederherstellung manuell ausschalten wollen.

Virtuelle Zielmaschine nach Abschluss der Wiederherstellung einschalten

Die Voreinstellung ist: **Deaktiviert**.

Wenn eine Maschine (aus einem Backup) zu einer anderen Maschine wiederhergestellt wird, kann es passieren, dass das Replikat der vorhandenen Maschine anschließend im Netzwerk erscheint. Sie können dies vermeiden, wenn Sie die wiederhergestellte Maschine manuell einschalten, nachdem Sie die notwendigen Vorsichtsmaßnahmen getroffen haben.

Windows-Ereignisprotokoll

Diese Option gilt nur für Windows-Betriebssysteme.

Diese Option definiert, ob die Agenten für alle Recovery-Aktionen entsprechende Ereigniseinträge im Windows-Anwendungsereignisprotokoll hinterlegen sollen. Sie können die Protokolleinträge über die Windows-Ereignisanzeige einsehen, die per Eingabebefehl (eventvwr.exe) oder per Menü (**Systemsteuerung** –> **Verwaltung** –> **Ereignisanzeige**) aufgefrufen werden kann. Sie können die Ereignisse filtern, die geloggt werden.

Die Voreinstellung ist: **Deaktiviert**.

Aktionen mit Backups

Die Registerkarte 'Backup Storage'

Die Registerkarte **Backup Storage** ermöglicht den Zugriff auf alle Backups – inklusive der Backups von Offline-Maschinen, der Backups von Maschinen, die nicht mehr im Cyber Protection Service registriert sind, der Backups in Public Clouds (wie Microsoft Azure) und verwaisten Backups[1].

Backups, die über `acrocmd` erstellt wurden, werden als verwaist gekennzeichnet. Backups, die mit der Produktversion 12.5 erstellt wurden, werden ebenfalls als verwaist gekennzeichnet.

Hinweis
Bitte beachten Sie, dass verwaiste Backups ebenfalls in Rechnung gestellt werden.

[1] Ein verwaistes Backup ist ein Backup, das nicht mehr mit einem Schutzplan assoziiert ist.

Backups, die an einem freigegebenen Speicherort (wie SMB- oder NFS-Freigaben) gespeichert sind, können von allen Benutzern gesehen werden, die mindestens über Leserechte für diesen Speicherort verfügen.

Unter Windows übernehmen Backup-Dateien die Zugriffsberechtigungen von ihrem übergeordneten Ordner. Wir empfehlen daher, dass Sie die Leserechte für diesen Ordner einschränken.

Im Cloud Storage haben Benutzer jedoch immer nur Zugriff auf Ihre jeweils eigenen Backups.

Ein Administrator kann die Cloud Backups für jedes Konto einsehen, welches zu einer bestimmten Abteilung oder Firma und deren Untergruppen gehört, indem er den Cloud Storage für das entsprechende Konto auswählt. Um das Gerät auszuwählen, mit dem Sie Daten aus der Cloud abrufen wollen, klicken Sie in der Zeile **Von dieser Maschine aus durchsuchen** auf **Ändern**. In der Registerkarte **Backup Storage** werden die Backups aller Maschinen angezeigt, die jemals unter dem ausgewählten Konto registriert wurden.

Backups, die vom *Cloud* Agenten für Microsoft 365 erstellt wurden, sowie Backups von Google Workspace-Daten werden nicht im Speicherort **Cloud Storage** angezeigt, sondern in einem separaten Bereich namens **Cloud-Applikationen-Backups**.

Backup-Speicherorte, die in Backup-Plänen verwendet werden, werden automatisch in der Registerkarte **Backup Storage** aufgeführt. Wenn Sie einen benutzerdefinierten Ordner (z.B. einen USB-Stick) zur Liste der Backup-Speicherorte hinzufügen wollen, müssen Sie auf **Durchsuchen** klicken und dann den gewünschten Ordnerpfad spezifizieren.

Wenn Sie einige Backups über einen Datei-Manager (wie dem Windows Explorer) hinzugefügt oder entfernt haben, klicken Sie auf das Zahnradsymbol neben dem Speicherortsnamen und anschließend auf **Aktualisieren**.

Warnung!
Versuchen Sie nicht, die Backup-Dateien manuell zu bearbeiten, weil dies die Dateien beschädigen und damit die Backups unbrauchbar machen könnte. Wir empfehlen außerdem, dass Sie besser die Backup-Replikation verwenden, statt die Backup-Dateien manuell zu verschieben.

Ein Backup-Speicherort (mit Ausnahme des Cloud Storage) verschwindet aus der Registerkarte **Backup Storage**, wenn alle Maschinen, die je zu diesem Speicherort gesichert wurden, aus dem Cyber Protection Service gelöscht wurden. Dadurch wird sichergestellt, dass Sie für Backups, die an diesem Speicherort aufbewahrt wurden, nicht weiter bezahlen müssen. Sobald ein neues Backup zu diesem Speicherort erfolgt, wird der Speicherort mit allen darin gespeicherten Backups wieder neu hinzugefügt.

Auf der Registerkarte **Backup Storage** können Sie die Backups in der Liste nach folgenden Kriterien filtern:

- **Nur mit forensischen Daten** – es wurden nur Backups mit forensischen Daten angezeigt.

- **Nur Vor-Update-Backups, die von der Patch-Verwaltung erstellt wurden** – es werden nur Backups angezeigt, die während der Patch-Verwaltung vor Durchführung der Patch-Installation erstellt wurden.

So können Sie einen Recovery-Punkt über die Registerkarte 'Backup Storage' auswählen

1. Wählen Sie auf der Registerkarte **Backup Storage** den Speicherort aus, wo die Backups gespeichert sind.
   Die Software zeigt all diejenigen Backups an, für die Ihr Konto am ausgewählten Speicherort die Berechtigung zur Anzeige hat. Die Backups werden in Gruppen zusammengefasst. Die Gruppennamen basieren auf folgender Vorlage:
   `<Maschinenname> - <Schutzplan-Name>`
2. Wählen Sie eine Gruppe, von der die Daten wiederhergestellt werden sollen.
3. [Optional] Klicken Sie auf **Ändern** (neben dem Befehl **Von dieser Maschine aus durchsuchen**) und wählen Sie dann eine andere Maschine aus. Einige Backups können nur von bestimmten Agenten durchsucht werden. Sie müssen beispielsweise eine Maschine auswählen, auf der ein Agent für SQL läuft, um die Backups von Microsoft SQL Server-Datenbanken durchsuchen zu können.

   Wichtig
   Beachten Sie, dass die Maschine, die über **Von dieser Maschine aus durchsuchen** festgelegt wird, auch das Standardziel für die Wiederherstellung der Backups einer physischen Maschine ist. Nachdem Sie einen Recovery-Punkt ausgewählt und auf **Recovery** geklickt haben, sollten Sie die Einstellung '**Zielmaschine**' doppelt überprüfen, um sicherzustellen, dass Sie die Wiederherstellung auch wirklich zu genau dieser Maschine durchführen wollen. Wenn Sie das Recovery-Ziel ändern wollen, müssen Sie über den Befehl **Von dieser Maschine aus durchsuchen** eine andere Maschine spezifizieren.

4. Klicken Sie auf **Backups anzeigen**.
5. Wählen Sie den gewünschten Recovery-Punkt aus.

So können Sie einen Speicherort für ein Backup hinzufügen

Hinweis
Diese Aktion ist nur verfügbar, wenn Sie einen Online-Agenten haben.

Klicken Sie auf der Registerkarte **Backup Storage** auf den Befehl **Speicherort hinzufügen**.

Wählen Sie einen Speicherort aus einem der folgenden Speicherorttypen aus – und klicken Sie anschließend auf **Fertig**:

- Lokaler Ordner
- Netzwerkordner
- Secure Zone

- NFS-Ordner
- Public Cloud

Volumes aus einem Backup mounten

Indem Sie die Volumes eines Laufwerk-Backups (Images) mounten, können Sie auf diese Volumes so zugreifen, als wären es physische Laufwerke.

Wenn Sie Volumes im 'Lese/Schreib'-Modus mounten, können Sie die in diesen vorliegenden Backup-Inhalte verändern. Das bedeutet: Dateien und Ordner speichern, verschieben, erstellen oder löschen und ausführbare Programme starten (sofern diese nur aus einer Datei bestehen). Die Software erstellt in diesem Modus ein inkrementelles Backup, welches alle Änderungen enthält, die Sie am Backup-Inhalt durchführen. Beachten Sie, dass keine der nachfolgenden Backups diese Änderungen enthalten werden.

Anforderungen

- Diese Funktionalität steht nur unter Windows und bei Verwendung des Windows Datei-Explorers zur Verfügung.
- Auf der Maschine, auf der Sie das Mounten durchführen, muss der Agent für Windows installiert sein.
- Das im Backup vorliegende Dateisystem muss von der Windows-Version, die auf der Maschine läuft, unterstützt werden.
- Das Backup selbst muss entweder in einem lokalen Ordner, in einer Netzwerkfreigabe (SMB/CIFS) oder in einer Secure Zone gespeichert sein.

Anwendungsszenarien

- Daten freigeben

  Gemountete Volumes können einfach im Netzwerk freigegeben werden.
- Notlösung zur Wiederherstellung einer Datenbank

  Mounten Sie ein Volume, das eine SQL-Datenbank von einer kürzlich ausgefallenen Maschine enthält. Sie erhalten so Zugriff auf die im Backup gespeicherte Datenbank, bis die ausgefallene Maschine wiederhergestellt ist. Sie können diesen Ansatz auch dazu verwenden, um eine granulare Wiederherstellung von Microsoft SharePoint-Daten mithilfe des SharePoint Explorers durchzuführen.
- Offline Virus-Bereinigung

  Wenn eine Maschine mit einem Virus infiziert ist, können Sie ein Backup dieser Maschine als Volume mounten und dieses dann von einem Antivirus-Programm bereinigen lassen. Anschließend können Sie die Maschine aus diesem bereinigten Backup wiederherstellen. Eine Alternative zu dieser Prozedur besteht natürlich in der Wiederherstellung eines Backups, welches erst gar nicht infiziert ist, jedoch ist ein solches nicht immer verfügbar.
- Fehlerüberprüfung

Wenn die Wiederherstellung eines Volumes fehlschlägt (insbesondere bei gleichzeitiger Größenanpassung des Volumes), kann dies an einem Fehler im gespeicherten Dateisystem (des Backups) liegen. Mounten Sie in diesem Fall das Backup im 'Lese/Schreib'-Modus. Überprüfen Sie das gemountete Volume dann mit dem Befehl `chkdsk /r` auf Fehler. Nachdem die Fehler behoben wurden und das dazugehörige inkrementelle Backup erstellt wurde, können Sie das System aus diesem korrigierten Backup wiederherstellen.

So können Sie ein Volume aus einem Backup mounten

1. Verwenden Sie den Windows Datei-Explorer, um den Speicherort des Backups aufzurufen.
2. Klicken Sie doppelt auf die Backup-Datei. Die Dateinamen basieren auf folgender Vorlage:
   `<Maschinenname> - <Schutzplan-GUID>`
3. Wenn das Backup verschlüsselt ist, müssen Sie das entsprechende Kennwort eingeben. Ansonsten können Sie diesen Schritt überspringen.
   Der Windows Datei-Explorer zeigt die Recovery-Punkte an.
4. Klicken Sie doppelt auf einen gewünschten Recovery-Punkt.
   Der Windows Datei-Explorer zeigt die im Backup gespeicherten Volumes an.

   Hinweis
   Wenn Sie auf ein Volume doppelt klicken, können Sie dessen Inhalte einsehen/durchsuchen. Sie können Dateien/Ordner aus dem Backup zu einem beliebigen Ordner im Dateisystem kopieren.

5. Klicken Sie mit der rechten Maustaste auf das zu mountende Volume und wählen Sie anschließend einen der folgenden Optionen:
   a. **Mounten**

      Hinweis
      Nur das letzte Backup im Archiv (der Backup-Kette) kann im 'Lese/Schreib'-Modus gemountet werden.

   b. **Im Nur-Lesen-Modus mounten**.
6. Sollte das Backup in einer Netzwerkfreigabe gespeichert sein, müssen Sie bei Bedarf die entsprechenden Anmeldedaten angeben, um auf die Freigabe zugreifen zu können. Ansonsten können Sie diesen Schritt überspringen.
   Das ausgewählte Volume wird von der Software gemountet. Dem Volume wird dabei standardmäßig der erste freie Laufwerksbuchstabe zugewiesen.

So können Sie ein Volume wieder trennen (unmounting)

1. Gehen Sie im Windows Datei-Explorer zur obersten Ebene des Verzeichnisbaums (das Element '**Computer**' bzw. unter Windows 8.1 (und später) '**Dieser PC**').
2. Klicken Sie mit der rechten Maustaste auf das gemountete Volume.
3. Klicken Sie auf **Trennen**.

4. [Optional] Wenn das Volume im 'Lese/Schreib'-Modus gemountet wurde und dabei sein Inhalt geändert wurde, müssen Sie auswählen, ob ein inkrementelles Backup erstellt werden soll, in dem die erfolgten Änderungen gespeichert werden. Ansonsten können Sie diesen Schritt überspringen.

Das Mounten des ausgewählten Volumes wird von der Software aufgehoben und das entsprechende Laufwerk vom Dateisystem getrennt.

Backups validieren

Indem Sie ein Backup validieren, können Sie sicherstellen, dass Sie die Daten aus diesem Backup wiederherstellen können. Weitere Informationen zu dieser Aktion finden Sie im Abschnitt '"Validierung" (S. 218)'.

Hinweis
Diese Funktion ist für Kunden-Mandanten verfügbar, für die die Quota **Advanced Backup - Server** oder **Advanced Backup - NAS** als Teil des Advanced Backup-Pakets aktiviert wurde.

So können Sie ein Backup validieren

1. Wählen Sie den gesicherten Workload aus.
2. Klicken Sie auf **Recovery**.
3. Wählen Sie einen Recovery-Punkt. Beachten Sie dabei, dass Recovery-Punkte nach Speicherorten gefiltert werden.
   Falls der Workload offline ist, werden keine Recovery-Punkte angezeigt. Gehen Sie nach einer der folgenden Möglichkeiten vor:
   - Sollte sich das Backup im Cloud Storage oder einem gemeinsam genutzten Storage befinden (d.h., dass andere Agenten auf diesen zugreifen können), dann klicken Sie zuerst auf den Befehl **Maschine auswählen**. Wählen Sie anschließend einen Ziel-Workload aus, der online ist, und dann den gewünschten Recovery-Punkt.
   - Wählen Sie einen Recovery-Punkt auf der Registerkarte 'Backup Storage' aus. Weitere Informationen über die dort verfügbaren Backups finden Sie im Abschnitt '"Die Registerkarte 'Backup Storage'" (S. 577)'.
4. Klicken Sie auf das Zahnradsymbol und anschließend auf **Validieren**.
5. Wählen Sie den Agenten aus, der die Validierung durchführen soll.
6. Wählen Sie die Validierungsmethode aus.
7. Wenn das Backup verschlüsselt ist, müssen Sie das entsprechende Kennwort bereitstellen.
8. Klicken Sie auf **Start**.

Backups exportieren

Mit der Aktion 'Exportieren' wird von einem Backup eine unabhängige Kopie an einem von Ihnen spezifizierten Speicherort erstellt. Das ursprüngliche Backup bleibt dabei unverändert. Durch die

Aktion 'Exportieren' können Sie ein bestimmtes Backup aus einer Kette inkrementeller und differentieller Backups separieren, um beispielsweise dessen Wiederherstellung zu beschleunigen, um das Backup auf ein Wechselmedium speichern zu können oder andere gewünschte Aktionen mit diesem Backup besser durchführen zu können.

Hinweis
Diese Funktion ist für Kunden-Mandanten verfügbar, für die die Quota **Advanced Backup - Server** oder **Advanced Backup - NAS** als Teil des Advanced Backup-Pakets aktiviert wurde.

Das Ergebnis einer Exportieren-Aktion ist immer ein vollständiges Backup. Wenn Sie eine komplette Backup-Kette an einen anderen Speicherort replizieren und mehrfache Recovery-Punkte bewahren wollen, müssen Sie einen Backup-Replikationsplan verwenden. Weitere Informationen zu diesem Plan finden Sie im Abschnitt '"Backup-Replikation" (S. 215)'.

Der Backup-Dateiname entspricht – abgesehen von einer fortlaufenden Nummer (Sequenznummer) – dem Namen des ursprünglichen Backups. Wenn mehrere Backups aus derselben Backup-Kette zum gleichen Speicherort exportiert werden, wird an die Dateinamen aller Backups (mit Ausnahme des ersten) eine vierstellige Sequenznummer angehängt.

Das exportierte Backup übernimmt die Verschlüsselungseinstellungen und das Kennwort des ursprünglichen Backups. Wenn Sie ein verschlüsseltes Backup exportieren, müssen Sie das entsprechende Kennwort spezifizieren.

So können Sie ein Backup exportieren

1. Wählen Sie den gesicherten Workload aus.
2. Klicken Sie auf **Recovery**.
3. Wählen Sie einen Recovery-Punkt. Beachten Sie dabei, dass Recovery-Punkte nach Speicherorten gefiltert werden.
   Falls der Workload offline ist, werden keine Recovery-Punkte angezeigt. Gehen Sie nach einer der folgenden Möglichkeiten vor:
   - Sollte sich das Backup im Cloud Storage oder einem gemeinsam genutzten Storage befinden (d.h., dass andere Agenten auf diesen zugreifen können), dann klicken Sie zuerst auf den Befehl **Maschine auswählen**. Wählen Sie anschließend einen Ziel-Workload aus, der online ist, und dann den gewünschten Recovery-Punkt.
   - Wählen Sie einen Recovery-Punkt auf der Registerkarte 'Backup Storage' aus. Weitere Informationen über die dort verfügbaren Backups finden Sie im Abschnitt '"Die Registerkarte 'Backup Storage'" (S. 577)'.
4. Klicken Sie auf das Zahnradsymbol und anschließend auf **Exportieren**.
5. Wählen Sie den Agenten aus, der das Exportieren durchführen soll.
6. Wenn das Backup verschlüsselt ist, müssen Sie das entsprechende Kennwort bereitstellen. Ansonsten können Sie diesen Schritt überspringen.
7. Spezifizieren Sie das Speicherziel für den Export.
8. Klicken Sie auf **Start**.

Backups löschen

Ein Backup-Archiv enthält ein oder mehrere Backups. Sie können spezifische Backups (Recovery-Punkte) in einem Archiv oder das gesamte Archiv löschen.

Das Löschen des Backup-Archivs löscht alle Backups darin. Wenn Sie alle Backups eines Workloads löschen, wird das komplette Backup-Archiv gelöscht, in dem diese Backups enthalten sind.

Sie können Backups mit der Cyber Protect-Konsole löschen - auf der Registerkarte **Geräte** oder der Registerkarte**Backup Storage**. Außerdem können Sie Backups aus dem Cloud Storage löschen, indem Sie die Web Restore-Konsole verwenden.

Warnung!
Wenn der unveränderliche Storage deaktiviert wird, werden die entsprechenden Backup-Daten dauerhaft gelöscht und können nicht wiederhergestellt werden.

So können Sie Backups oder Backup-Archive löschen

Auf der Registerkarte Geräte

Dieses Verfahren gilt nur für Online-Workloads.

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte** –> **Alle Geräte**.
2. Wählen Sie die Workload-Backups aus, die Sie löschen möchten.
3. Klicken Sie auf **Recovery**.
4. [Wenn mehr als ein Backup-Speicherort verfügbar ist] Wählen Sie den Backup-Speicherort aus.
5. [Wenn Sie alle Backups eines Workloads löschen wollen] Klicken Sie auf **Alle löschen**.
   Das Löschen aller Backups löscht auch die Backup-Archive, die diese Backups enthalten.
6. [Wenn Sie ein bestimmtes Backup löschen wollen] Wählen Sie das Backup (den Recovery-Punkt), das Sie löschen möchten, und klicken Sie dann auf **Aktionen** > **Löschen**.
7. [Beim Löschen aller Backups] Aktivieren Sie das Kontrollkästchen und klicken Sie dann auf **Löschen**, um Ihre Entscheidung zu bestätigen.
8. [Wenn Sie ein bestimmtes Backup löschen] Klicken Sie auf **Löschen**, um Ihre Entscheidung zu bestätigen.

Auf der Registerkarte Backup Storage

Dieses Verfahren gilt für Online- und Offline-Workloads.

1. Gehen Sie in der Cyber Protect-Konsole zu **Backup Storage**.
2. Wählen Sie den Speicherort aus, aus dem Sie die Backups löschen möchten.
3. Wählen Sie das Backup-Archiv aus, aus dem Sie die Backups löschen möchten.
   Der Archivname basiert auf folgender Vorlage:

- Nicht-Cloud-zu-Cloud-Backup-Archive: <Workload-Name> - <Schutzplan-Name>
- Cloud-zu-Cloud-Backup-Archive: <Benutzername> oder <Laufwerksname> oder <Team-Name> - <Cloud Service> - <Schutzplan-Name>

4. [Wenn Sie das komplette Backup-Archiv löschen wollen] Klicken Sie auf **Löschen**.
   Das Löschen eines Backup-Archivs löscht alle Backups in diesem Archiv.
5. [Wenn Sie ein bestimmtes Backup in einem Backup-Archiv löschen wollen] Klicken Sie auf **Backups anzeigen**.
   a. Wählen Sie das Backup (den Recovery-Punkt), das Sie löschen möchten.
   b. Klicken Sie auf **Aktionen** > **Löschen**.
6. [Wenn Sie ein Backup-Archiv löschen] Aktivieren Sie das Kontrollkästchen und klicken Sie dann auf **Löschen**, um Ihre Entscheidung zu bestätigen.
7. [Wenn Sie ein bestimmtes Backup löschen] Klicken Sie auf **Löschen**, um Ihre Entscheidung zu bestätigen.

In der Web Restore-Konsole

Dieses Verfahren gilt nur für Backup-Archive im Cloud Storage.

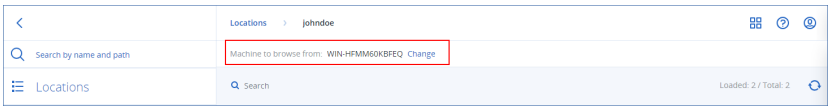
1. Gehen Sie in der Cyber Protection-Konsole zu **Geräte** –> **Alle Geräte**.
2. Wählen Sie die Workload-Backups aus, die Sie löschen möchten, und klicken Sie dann auf **Recovery**.
3. [Wenn mehrere Backup-Speicherorte verfügbar sind] Wählen Sie den Backup-Speicherort aus und klicken Sie dann auf **Weitere Wiederherstellungsmöglichkeiten**.
4. Klicken Sie auf **Dateien herunterladen**.
   Sie werden zur Web Restore-Konsole weitergeleitet.
5. Klicken Sie in der Web Restore-Konsole unter **Maschinen** auf den entsprechenden Workload-Namen.
6. Klicken Sie bei **Letzte Version** auf das Datum und dann auf **Löschen**.
   Diese Aktion ist nur auf der Backup-Archiv-Ebene verfügbar. Sie können das Archiv nicht durchsuchen und keine einzelnen Backups aus diesem löschen.
7. Klicken Sie auf **Löschen**, um Ihre Entscheidung zu bestätigen.

Backups außerhalb der Cyber Protect-Konsole löschen

Wir empfehlen, dass Sie Backups über die Cyber Protect-Konsole löschen. Wenn Sie Backups aus dem Cloud Storage über die Web Restore-Konsole löschen oder lokale Backups mit einem Dateimanager löschen, müssen Sie den Backup-Speicherort aktualisieren, um die Änderungen mit der Cyber Protect-Konsole zu synchronisieren.

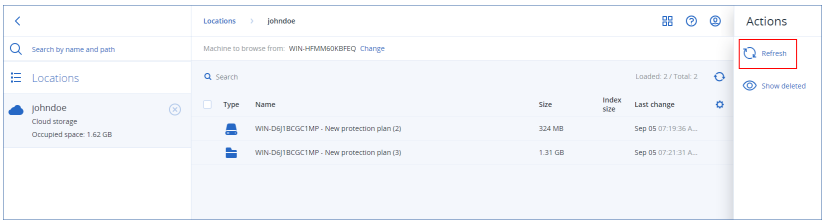
Voraussetzung

- Ein Online-Agent, der auf den Backup-Speicherort zugreifen kann, muss bei **Von dieser Maschine aus durchsuchen** in der Cyber Protect-Konsole ausgewählt werden.



So können Sie einen Backup-Speicherort aktualisieren

1. Gehen Sie in der Cyber Protect-Konsole zu **Backup Storage**.
2. Wählen Sie den Speicherort aus, wo die gelöschten Backups gespeichert waren.
3. Klicken Sie im Fensterbereich **Aktionen** auf **Aktualisieren**.



Die Erkennung von Engpässen verstehen

Mithilfe der Funktion zur Erkennung von Engpässen können Sie ermitteln, wo Sie die Performance verbessern können. Dazu wird hervorgehoben, welche Komponente in Ihrem System während eines Backup- oder Wiederherstellungsprozesses am langsamsten war.

Da es bei jedem Übertragungsvorgang *immer* zu Engpässen kommt, bedeutet dies nicht, dass diese unbedingt behoben werden müssen. Denn möglicherweise sind Ihnen die Backups bereits schnell genug und passen perfekt zu Ihren Backup-Fenstern sowie zu Ihren SLAs. Daher müssen Sie meistens gar keine Probleme beheben.

Sie können die Engpässe über die Registerkarte **Aktivitätsdetails** leicht einsehen und nachverfolgen. Gehen Sie dazu in der Cyber Protect-Konsole zu **Monitoring –> Aktivitäten** und klicken Sie auf die entsprechende Aktivität. Weitere Informationen über die Anzeige von Engpässe finden Sie in den Abschnitten '"Details zu Engpässen anzeigen" (S. 588)' und '"Für welche Workloads, Agenten und Backup-Standorte werden Engpässe angezeigt?" (S. 590)'.

Was ist ein Engpass?

Engpässe werden üblicherweise durch eine langsame Komponente in der Prozesskette verursacht. Oder anders ausgedrückt, durch eine Komponente, auf die die anderen Komponenten warten müssen.

Mithilfe der Funktion zur Erkennung von Engpässen können Sie diese langsamen Komponenten während des Backup- bzw. Recovery-Prozesses aufspüren und herausfinden, welcher der nachfolgenden Komponententypen am langsamsten ist:

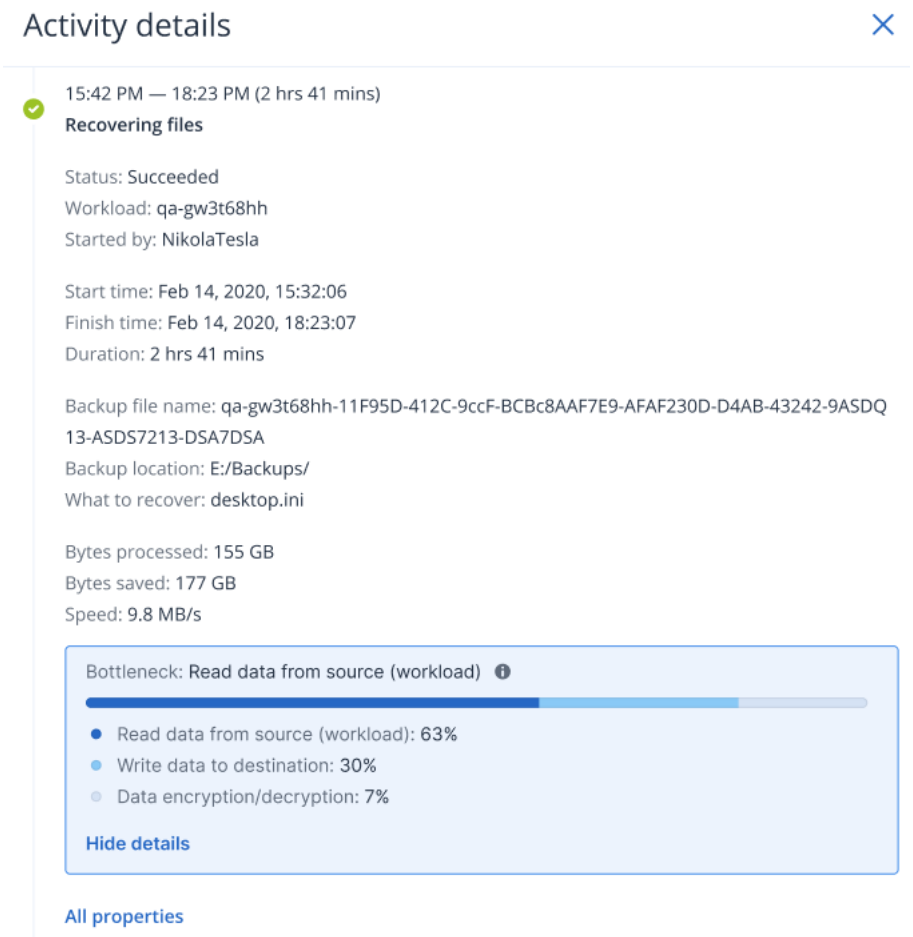
- **Quelle**: Sie können auf einen Blick feststellen, ob der Lesevorgang von der Backup- bzw. Recovery-Quelle einen Engpass darstellt.
- **Ziel**: Verstehen Sie, ob die Schreibgeschwindigkeit zum Backup- bzw. Recovery-Ziel die

Performance beeinträchtigt.

- **Agent**: Verstehen Sie, ob der Agent die Daten schnell genug verarbeitet.

Die Art des Engpasses (also ob durch die Quelle, das Ziel oder den Agenten bedingt) kann sich während der Backup- bzw. Recovery-Aktivität zu verschiedenen Zeiten ändern. Die Prozentsätze, die im Bereich **Engpass** der unteren Registerkarte **Aktivitätsdetails** angezeigt werden (z.B. **Daten aus Quelle (Workload) lesen: 63%**), stehen für den Prozentsatz der Zeit, in der diese Art von Engpass aufgetreten ist. Im vorliegenden Beispiel – mit 63% der Aktivitätszeit für die Wiederherstellung – ist der Engpass beim Lesen der Daten aufgetreten – als Geschwindigkeitsverzögerung beim Lesen der Daten aus dem Backup-Archiv durch den Agenten.

In ähnlicher Weise, für 30% der Zeit, war der Engpass eine Geschwindigkeitsverzögerung beim Schreiben der Daten zum Wiederherstellungsziel (**Daten zum Ziel schreiben: 30%**).



Hinweis
Es ist normal, Engpassstatistiken auf der Registerkarte **Aktivitätsdetails** zu sehen. Diese Statistiken sind nur für Tasks verfügbar, die länger als eine Minute dauern.

So können Sie Engpässe reduzieren

Wie zuvor schon erwähnt, hebt die Funktion zur Erkennung von Engpässen den *Lesen*- und *Schreiben*-Datenfluss zwischen den Backup-Komponenten hervor. Die Statistiken für *Lesen* beziehen sich auf den Datenfluss von der Datenquelle zum Agenten, der die Backup- bzw. Recovery-Aktion durchführt – während sich die Statistiken für *Schreiben* auf den Datenfluss zwischen dem Agenten und dem Backup-Archiv (dem Ziel) beziehen.

Wenn Sie Engpässe reduzieren und die Performance des Lesen-/Schreiben-Datenflusses verbessern wollen, sollten Sie den Kanal zwischen dem Agenten und der Datenquelle bzw. dem Backup-Archiv analysieren. Sie können beispielsweise versuchen, Ihre Laufwerke per Benchmark-Test zu bewerten, wenn der Agent einige lokale Dateien sichert.

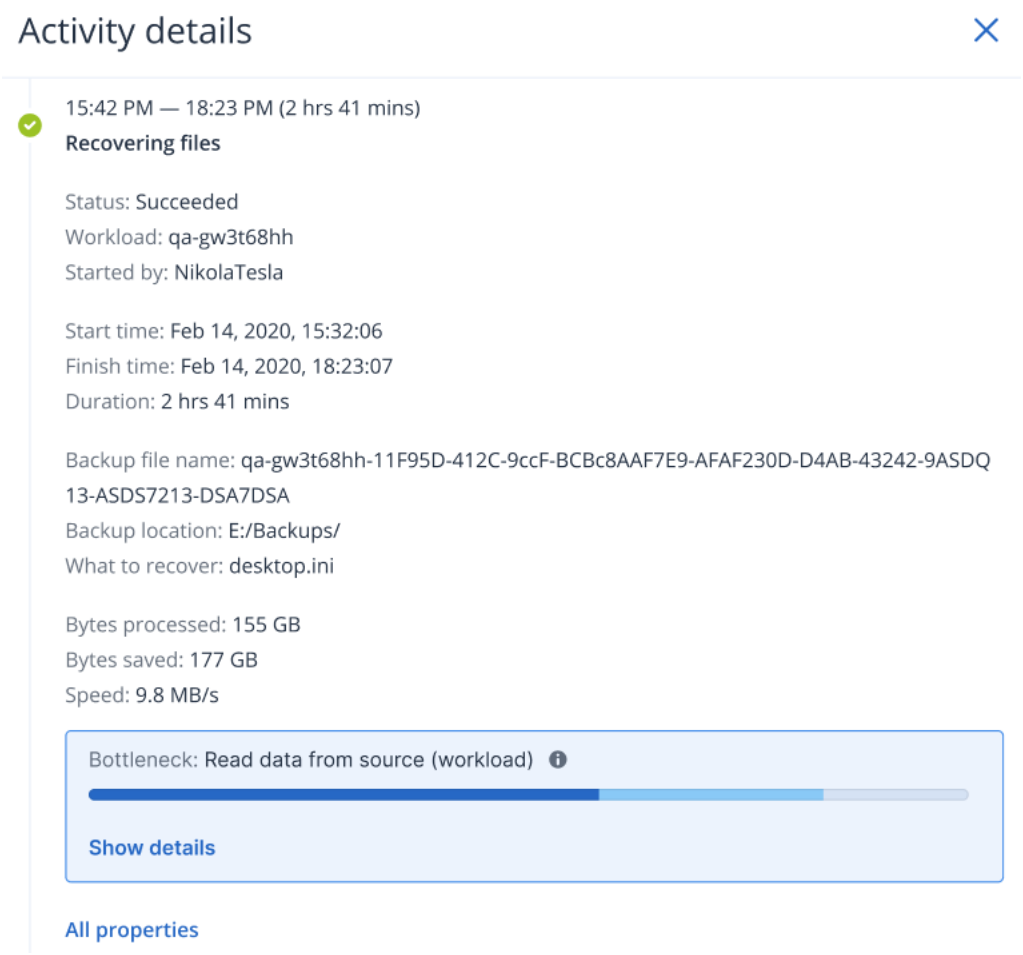
Details zu Engpässen anzeigen

Sie können sich erkannte Engpässe für jede Art von Backup-, Replikations- oder Wiederherstellungsprozess (zu jeder Art von Zielordner bzw. Speicherort) anzeigen lassen. Das gilt auch für Backups von physischen oder virtuellen Maschinen und Dateien bzw. Ordnern. Sie können sich außerdem auch die Engpässe für die Replikationen von virtuellen Maschinen und für Failback-Aktivitäten anzeigen lassen.

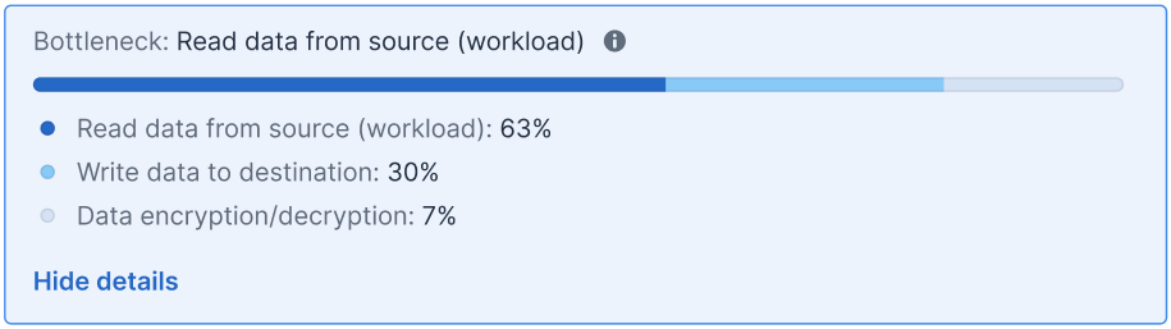
Weitere Informationen zur Definition und zu den Grundkonzepten der verschiedenen Arten von Engpässen finden Sie im Abschnitt '"Die Erkennung von Engpässen verstehen" (S. 586)'.

So können Sie die Details zu Engpässen einsehen

1. Gehen Sie in der Cyber Protect-Konsole zu **Monitoring –> Aktivitäten**.
2. Klicken Sie auf die entsprechende Aktivität.
   Der Bereich **Engpass** wird auf der Registerkarte **Aktivitätsdetails** in blauer Farbe dargestellt.



3. Klicken Sie auf **Details anzeigen**, um sich den am häufigsten aufgetretenen Engpass während der entsprechenden Backup- bzw. Recovery-Aktion anzeigen zu lassen.
   Der Bereich **Engpass** wird erweitert und zeigt eine Zusammenfassung der relevanten Engpassarten an.



   Im oberen Beispiel wurde der Engpass, der 63% der Gesamtzeit der Aktion beansprucht hat, durch die (vom Agenten durchgeführte) Aktion *Lesen* verursacht.

Hinweis
Während die entsprechende Aktivität ausgeführt wird, werden die Engpasswerte jede Minute dynamisch aktualisiert.

Für welche Workloads, Agenten und Backup-Standorte werden Engpässe angezeigt?

Die Erkennung von Engpässen ist für folgende Arten von Workloads, Agenten und Backup-Standorten verfügbar:

- Backups auf Laufwerksebene (Image-Backups), durchgeführt von:
  - Dem Agenten für Azure
  - Agent für Windows
  - Agent für Linux
  - Dem Agenten für Mac
  - Dem Agenten für VMware (sowohl virtuelle Appliance als auch Windows, einschließlich VM-Replikationen und Failbacks über Replikate (Wiederherstellungen aus Replikaten))
  - Agent für Hyper-V
  - Dem Agenten für Scale Computing
  - Agent für oVirt (KVM)
  - Dem Agenten für Virtuozzo Infrastructure Platform
  - Agent für Virtuozzo
  - Dem Agenten für VMware Cloud Director (vCD-BA)
- Backups auf Dateiebene
  - Agent für Windows
  - Agent für Linux
  - Dem Agenten für Mac
- Backups auf Applikationsebene
  - Agent für SQL
  - Agent für Exchange
  - Agent für MySQL/MariaDB
  - Agent für Oracle
  - Dem Agenten für SAP HANA
- Backup-Speicherorte
  - Acronis Cloud Storage (einschließlich Partner Hosted Storage)
  - Public Cloud Storage
  - Netzwerkfreigaben (SMB + NFS)
  - Lokale Ordner
  - Per Skript festgelegte Speicherorte
  - Acronis Secure Zone

Workloads zu Public Clouds sichern

Hinweis
Diese Funktion ist Bestandteil des Advanced Backup-Pakets, das wiederum ein Bestandteil des Cyber Protection Service ist. Wenn Sie diese Funktionalität zu einem Schutzplan hinzufügen, sollten Sie beachten, dass dafür zusätzliche Gebühren anfallen können.

Sie können Public Cloud Services wie Microsoft Azure und Amazon S3 (Simple Storage Service) als Backup-Ziele in der Cyber Protect-Konsole auswählen.

Wenn Sie Backup-Speicherorte in Public Clouds konfigurieren wollen, müssen Sie ein Firmen- oder Abteilungsadministrator sein oder Ihnen muss eine der folgenden Rollen im Cyber Protection Service zugewiesen sein: Cyber-Administrator, Administrator oder Benutzer.

Einen Backup-Speicherort in Microsoft Azure definieren

Hinweis
Wenn Sie Backup-Speicherorte auf Microsoft Azure konfigurieren möchten, müssen Sie eine der folgenden Rollen im Cyber Protection Service definiert haben: Firmenadministrator, Benutzer, Cyber-Administrator.

Wenn Sie einen Workload per Backup zu Microsoft Azure sichern wollen, müssen Sie den Microsoft Azure-Backup-Speicherort in der Cyber Protect-Konsole definieren und sich mit dem entsprechenden Microsoft Azure-Abonnement verbinden. Dies kann auf folgende Arten erfolgen:

- Wenn Sie einen Schutzplan erstellen oder bearbeiten.
- Wenn Sie Backup Storage-Speicherorte definieren und verwalten.

Wichtig
Sowohl Administratoren als auch Benutzer, die keine Administratoren sind, können Workloads zu Microsoft Azure sichern.

Benutzer, die keine Administratoren sind, können einen Zugriff auf ein Microsoft Azure-Abonnement hinzufügen (siehe Abschnitt '"Um den Zugriff auf Microsoft Azure-Abonnements zu verwalten" (S. 602)'). Sie können jedoch nur dann Schutzpläne anwenden, wenn der Backup-Speicherort mit dem Microsoft Azure-Abonnement verbunden ist, das sie selbst hinzugefügt haben, und für Workloads, die unter ihrem Namen in der Cyber Protect-Konsole registriert sind.

Administratoren können Schutzpläne anwenden, bei denen der Backup-Speicherort mit Microsoft Azure-Abonnements verbunden ist, die sie selbst hinzugefügt haben oder mit Abonnements, die von einem anderen Administrator hinzugefügt wurden, und für Workloads, die in der Cyber Protect-Konsole unter einem beliebigen Benutzer registriert sind.

So können Sie einen Backup-Speicherort in Microsoft Azure definieren

1. Führen Sie in der Cyber Protect-Konsole eine der folgenden Aktionen aus:
   - Gehen Sie, wenn Sie einen Schutzplan erstellen oder bearbeiten, zu **Geräte** und wählen Sie den entsprechenden Workload aus, den Sie per Backup zu Microsoft Azure sichern wollen. Klicken Sie im Bereich **Backup** des Schutzplans für den ausgewählten Workload auf den Link in der Zeile **Backup-Ziel**.

     Weitere Informationen über die Verwendung von Schutzplänen finden Sie im Abschnitt '"Schutzpläne und Module" (S. 231)'.
   - Wenn Sie Ihre Backup Storage-Speicherorte verwalten und Microsoft Azure als neuen Speicherort hinzufügen wollen, gehen Sie zu **Backup Storage**.

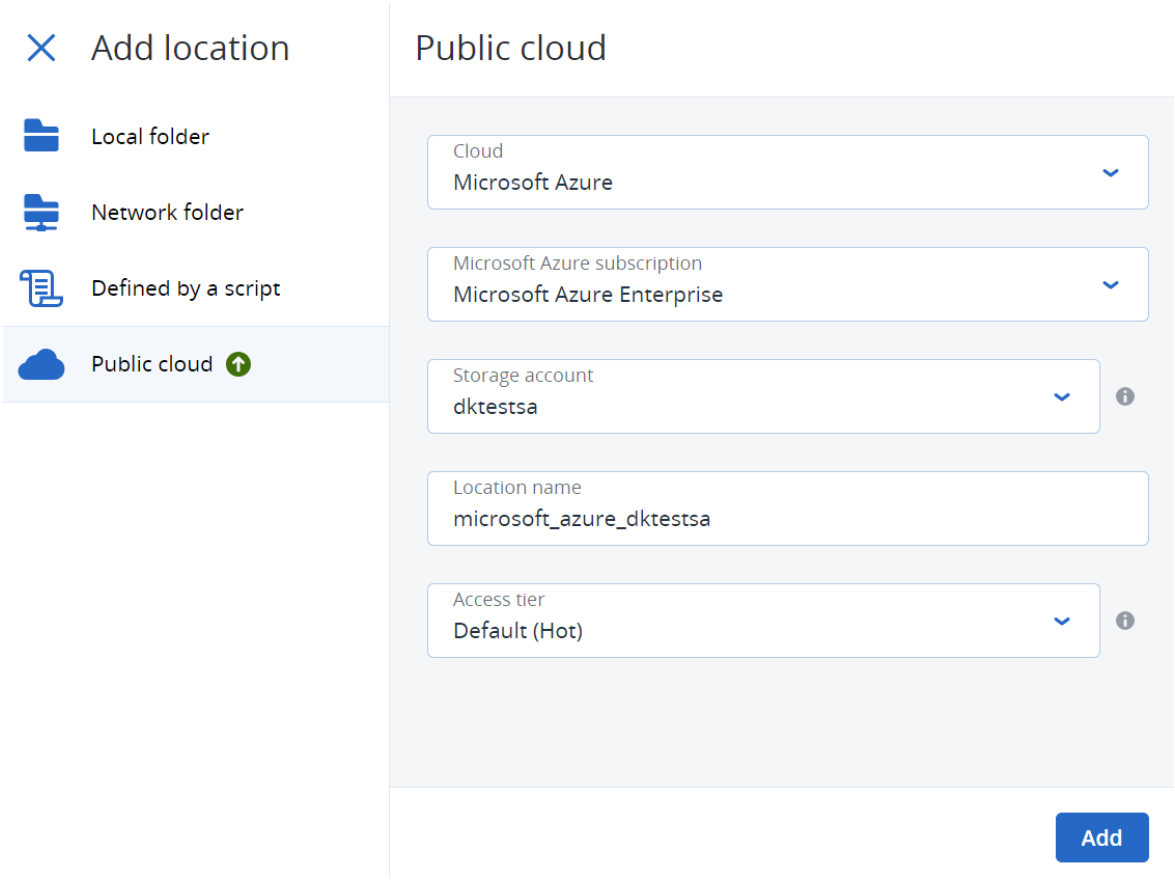
     Weitere Informationen über die Verwaltung Ihrer Backup Storage-Speicherorte finden Sie im Abschnitt '"Die Registerkarte 'Backup Storage'" (S. 577)'.
2. Klicken Sie auf **Speicherort hinzufügen**.
3. Wählen Sie aus dem Listenfeld **Public Clouds** den Eintrag **Microsoft Azure** aus.
4. Wenn das entsprechende Microsoft Azure-Abonnement bereits in der Cyber Protect-Konsole registriert ist, wählen Sie dieses aus der Liste der Abonnements aus.

   Wenn das entsprechende Abonnement nicht in der Cyber Protect-Konsole registriert ist, klicken Sie zuerst auf **Hinzufügen** und dann im angezeigten Dialog auf **Anmelden**. Sie werden zur Microsoft-Anmeldeseite weitergeleitet. Weitere Informationen darüber, wie Sie den Zugriff auf ein Microsoft Azure-Abonnement hinzufügen und definieren können, finden Sie im Abschnitt '"Den Zugriff auf ein Microsoft Azure-Abonnement hinzufügen" (S. 603)'.
5. Wählen Sie im Feld **Storage-Konto** das gewünschte Konto aus.

   Hinweis
   Derzeit werden nur Storage-Konten von Microsoft Azure mit regulären Endpunkt-Suffixen unterstützt, die `core.windows.net` enthalten. Außerdem muss es sich bei dem ausgewählten Storage-Konto um einen StorageV2-Kontotyp handeln.

   Die Felder **Speicherortname** und **Zugriffsebene** werden automatisch entsprechend dem ausgewählten Storage-Konto ausgefüllt. Der angezeigte Speicherortname lautet `microsoft_azure_[Storage-Konto]` und die ausgewählte Zugriffsebene ist **Standard (Hot)**. Beide Felder können bei Bedarf aber auch geändert werden.

   Hinweis
   Wenn Sie den Speicherortnamen ändern, geben Sie einen eindeutigen Speicherortnamen ein (der Name muss für den Kunden-Mandanten eindeutig sein). Wenn der von Ihnen hinzugefügte Name bereits im Storage-Konto vorhanden ist, wird Acronis an den Namen eine Suffix-Nummer angehängt. Wenn beispielsweise **Microsoft Azure Storage** bereits existiert, wird der Name automatisch zu **Microsoft Azure Storage_01** aktualisiert.



6. Klicken Sie auf **Hinzufügen**.

   Wenn Sie einen Schutzplan erstellen oder bearbeiten, wird der Microsoft Azure-Backup-Speicherort entsprechend in der Zeile **Backup-Ziel** festgelegt. Wenn das Backup ausgeführt wird (egal ob manuell oder nach Planung), wird es am festgelegten Speicherort gesichert.

   Wenn Sie Ihre Backup Storage-Speicherorte verwalten, können Sie die Details zum jeweiligen Speicherort bei Bedarf einsehen und aktualisieren. Der Microsoft Azure-Speicherort ist auch verfügbar, wenn Sie einen Backup-Speicherort für Ihre Workloads definieren. Weitere Informationen finden Sie im Abschnitt "Public Cloud-Backup-Speicherorte anzeigen und aktualisieren" (S. 598).

Einen Backup-Speicherort in Amazon S3 definieren

Hinweis
Wenn Sie Backup-Speicherorte auf Amazon S3 konfigurieren möchten, müssen Sie eine der folgenden Rollen im Cyber Protection Service definiert haben: Firmenadministrator, Benutzer, Cyber-Administrator.

Wenn Sie einen Workload zu Amazon S3 sichern möchten, müssen Sie den Amazon S3 Backup-Speicherort in der Cyber Protect-Konsole definieren und sich dann mit der entsprechenden Amazon S3-Verbindung verbinden. Sie können dies auf die folgenden Arten tun:

- Wenn Sie einen Schutzplan erstellen oder bearbeiten.
- Wenn Sie Backup Storage-Speicherorte definieren und verwalten.

Wichtig
Sowohl Administratoren als auch Benutzer, die keine Administratoren sind, können Workloads zu Amazon S3 sichern.

Benutzer, die keine Administratoren sind, können einen Zugriff auf eine Amazon S3-Verbindung hinzufügen (siehe Abschnitt '"Den Zugriff auf andere Public Cloud Storage Services verwalten" (S. 606)'). Sie können jedoch nur dann Schutzpläne anwenden, wenn der Backup-Speicherort mit der Amazon S3-Verbindung verbunden ist, die sie selbst hinzugefügt haben, und für Workloads, die unter ihrem Namen in der Cyber Protect-Konsole registriert sind.

Administratoren können Schutzpläne anwenden, bei denen der Backup-Speicherort mit Amazon S3-Verbindungen verbunden ist, die sie selbst hinzugefügt haben oder mit Abonnements, die von einem anderen Administrator hinzugefügt wurden, und für Workloads, die in der Cyber Protect-Konsole unter einem beliebigen Benutzer registriert sind.

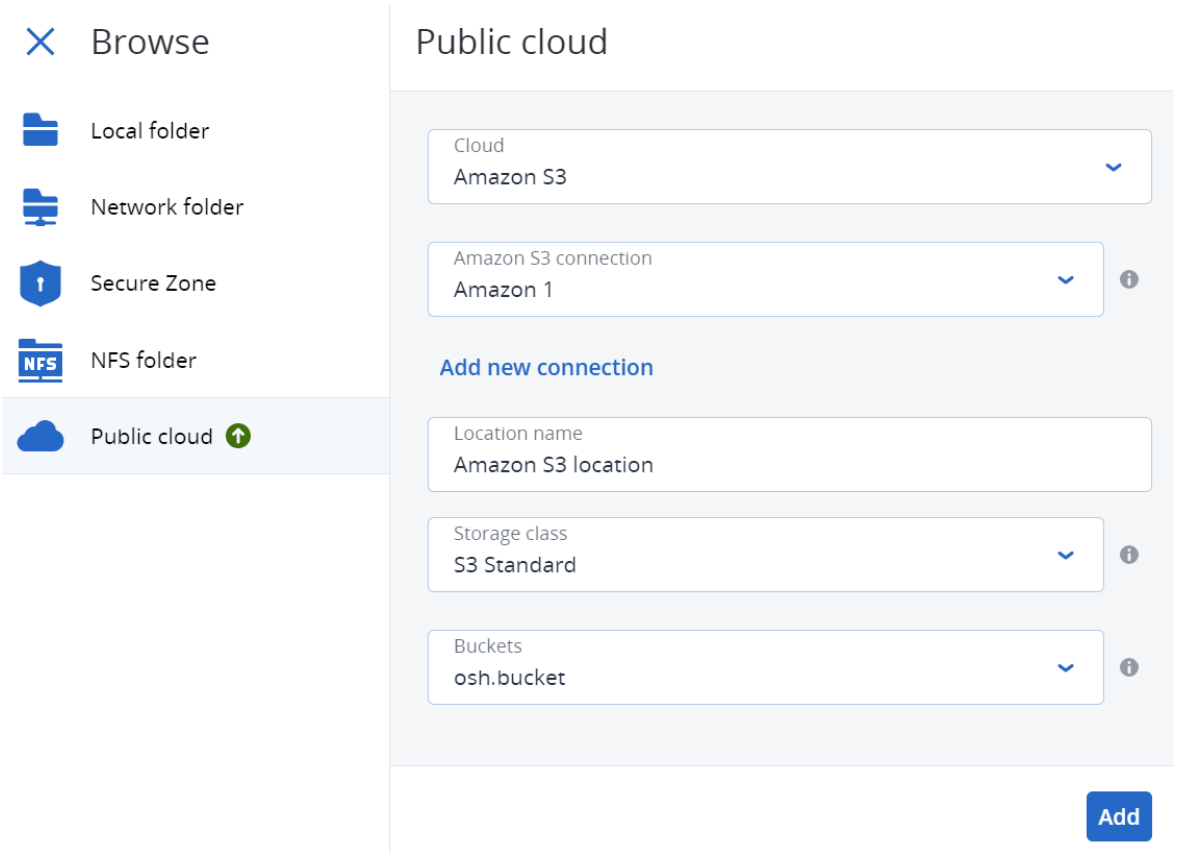
So können Sie einen Backup-Speicherort in Amazon S3 definieren

1. Führen Sie in der Cyber Protect-Konsole eine der folgenden Aktionen aus:
   - Gehen Sie, wenn Sie einen Schutzplan erstellen oder bearbeiten, zu **Geräte** und wählen Sie den Workload aus, den Sie per Backup zu Amazon S3 sichern wollen. Klicken Sie im Bereich **Backup** des Schutzplans für den ausgewählten Workload auf den Link in der Zeile **Backup-Ziel**.

     Weitere Informationen über die Verwendung von Schutzplänen finden Sie im Abschnitt '"Schutzpläne und Module" (S. 231)'.
   - Wenn Sie Ihre Backup-Speicherorte verwalten und Amazon S3 als neuen Ort hinzufügen möchten, gehen Sie zu **Backup Storage**.

     Weitere Informationen über die Verwaltung Ihrer Backup Storage-Speicherorte finden Sie im Abschnitt '"Die Registerkarte 'Backup Storage'" (S. 577)'.
2. Klicken Sie auf **Speicherort hinzufügen**.
3. Wählen Sie aus dem Listenfeld **Public Clouds** den Eintrag **Amazon S3** aus.
4. Wenn die entsprechende Amazon S3-Verbindung bereits in der Cyber Protect-Konsole registriert ist, wählen Sie diese aus der Liste aus.

   Wenn die entsprechende Verbindung noch nicht in der Cyber Protect-Konsole registriert ist, klicken Sie auf **Neue Verbindung hinzufügen**. Weitere Informationen darüber, wie den Zugriff auf eine Amazon S3-Verbindung hinzufügen und konfigurieren können, Sie unter "Zugriff auf eine Public Cloud-Verbindung hinzufügen" (S. 607). Wenn die Verbindung hinzugefügt wurde, fahren Sie mit dem nächsten Schritt fort.



5. Definieren Sie Folgendes:
   - Geben Sie im Feld **Speicherortname** die Bezeichnung des Speicherortes an.

     Hinweis
     Der Speicherortname muss eindeutig/einzigartig für den Kunden-Mandanten sein. Sollte der hinzuzufügende Name bereits in der Verbindung vorhanden sein, dann fügt Acronis dem Namen noch eine Suffixnummer hinzu. Wenn beispielsweise **Amazon S3 Storage** bereits existiert, wird der Name automatisch zu **Amazon S3 Storage 1** aktualisiert.

   - Wählen Sie im Feld **Storage-Classe** eine der folgenden unterstützten Storage-Klassen aus:
     - S3 Standard
     - Standard - Infrequent Access (S3 Standard-IA)
     - One Zone - Infrequent Access (S3 One Zone-IA)
     - S3 Intelligent Tiering
   - Wählen Sie im Feld **Bucket** den entsprechenden Amazon S3-Bucket aus.
6. Klicken Sie auf **Hinzufügen**.
   Wenn Sie einen Schutzplan erstellen oder bearbeiten, wird der Amazon S3-Backup-Speicherort entsprechend in der Zeile **Backup-Ziel** festgelegt. Wenn das Backup ausgeführt wird (egal ob manuell oder nach Planung), wird es am festgelegten Speicherort gesichert.
   Wenn Sie Ihre Backup Storage-Speicherorte verwalten, können Sie die Details zum jeweiligen Speicherort bei Bedarf einsehen und aktualisieren. Der Amazon S3-Speicherort ist auch

verfügbar, wenn Sie einen Backup-Speicherort für Ihre Workloads definieren. Weitere Informationen finden Sie im Abschnitt "Public Cloud-Backup-Speicherorte anzeigen und aktualisieren" (S. 598).

Einen Backup-Speicherort in Wasabi definieren

Hinweis
Wenn Sie Backup-Speicherorte auf Wasabi konfigurieren möchten, müssen Sie eine der folgenden Rollen im Cyber Protection Service definiert haben: Firmenadministrator, Benutzer, Cyber-Administrator.

Wenn Sie einen Workload zu Wasabi sichern möchten, müssen Sie den Wasabi-Backup-Speicherort in der Cyber Protect-Konsole definieren und sich dann mit der entsprechenden Wasabi-Verbindung verbinden. Sie können dies auf folgende Arten tun:

- Wenn Sie einen Schutzplan erstellen oder bearbeiten.
- Wenn Sie Backup Storage-Speicherorte definieren und verwalten.

Wichtig
Sowohl Administratoren als auch Benutzer, die keine Administratoren sind, können Workloads zu Wasabi sichern.

Benutzer, die keine Administratoren sind, können einen Zugriff auf eine Wasabi-Verbindung hinzufügen (siehe Abschnitt '"Den Zugriff auf andere Public Cloud Storage Services verwalten" (S. 606)'). Sie können jedoch nur dann Schutzpläne anwenden, wenn der Backup-Speicherort mit der Wasabi-Verbindung verbunden ist, die sie selbst hinzugefügt haben, und für Workloads, die unter ihrem Namen in der Cyber Protect-Konsole registriert sind.

Administratoren können Schutzpläne anwenden, bei denen der Backup-Speicherort mit Wasabi-Verbindungen verbunden ist, die sie selbst hinzugefügt haben oder mit Abonnements, die von einem anderen Administrator hinzugefügt wurden, und für Workloads, die in der Cyber Protect-Konsole unter einem beliebigen Benutzer registriert sind.

So können Sie einen Backup-Speicherort in Wasabi definieren

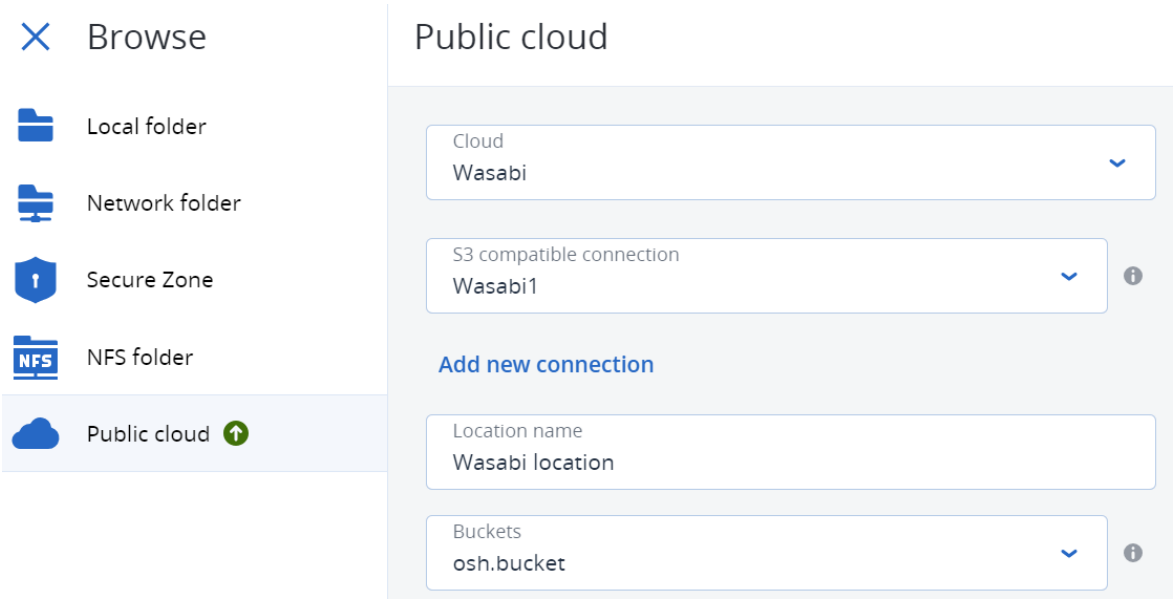
1. Führen Sie in der Cyber Protect-Konsole eine der folgenden Aktionen aus:
   - Gehen Sie, wenn Sie einen Schutzplan erstellen oder bearbeiten, zu **Geräte** und wählen Sie den Workload aus, den Sie per Backup zu Wasabi sichern wollen. Klicken Sie im Bereich **Backup** des Schutzplans für den ausgewählten Workload auf den Link in der Zeile **Backup-Ziel**.

     Weitere Informationen über die Verwendung von Schutzplänen finden Sie im Abschnitt '"Schutzpläne und Module" (S. 231)'.
   - Wenn Sie Ihre Backup-Speicherorte verwalten und Wasabi als neuen Ort hinzufügen möchten, gehen Sie zu **Backup Storage**.

Weitere Informationen über die Verwaltung Ihrer Backup Storage-Speicherorte finden Sie im Abschnitt '"Die Registerkarte 'Backup Storage'" (S. 577)'.

2. Klicken Sie auf **Speicherort hinzufügen**.
3. Wählen Sie aus dem Listenfeld **Public Clouds** den Eintrag **Wasabi** aus.
4. Wenn die entsprechende Wasabi-Verbindung bereits in der Cyber Protect-Konsole registriert ist, wählen Sie diese aus der Liste aus.

   Wenn die entsprechende Verbindung noch nicht in der Cyber Protect-Konsole registriert ist, klicken Sie auf **Neue Verbindung hinzufügen**. Weitere Informationen darüber, wie den Zugriff auf eine Wasabi-Verbindung hinzufügen und konfigurieren können, Sie unter "Zugriff auf eine Public Cloud-Verbindung hinzufügen" (S. 607). Wenn die Verbindung hinzugefügt wurde, fahren Sie mit dem nächsten Schritt fort.



5. Definieren Sie Folgendes:
   - Geben Sie im Feld **Speicherortname** die Bezeichnung des Speicherortes an.

     Hinweis
     Der Speicherortname muss eindeutig/einzigartig für den Kunden-Mandanten sein. Sollte der hinzuzufügende Name bereits in der Verbindung vorhanden sein, dann fügt Acronis dem Namen noch eine Suffixnummer hinzu. Wenn beispielsweise **Wasabi Storage** bereits existiert, wird der Name automatisch zu **Wasabi Storage 1** aktualisiert.

   - Wählen Sie im Feld **Bucket** den entsprechenden Wasabi-Bucket aus.
6. Klicken Sie auf **Hinzufügen**.

   Wenn Sie einen Schutzplan erstellen oder bearbeiten, wird der Wasabi-Backup-Speicherort entsprechend in der Zeile **Backup-Ziel** festgelegt. Wenn das Backup ausgeführt wird (egal ob manuell oder nach Planung), wird es am festgelegten Speicherort gesichert.

   Wenn Sie Ihre Backup Storage-Speicherorte verwalten, können Sie die Details zum jeweiligen Speicherort bei Bedarf einsehen und aktualisieren. Der Wasabi-Speicherort ist auch verfügbar,

wenn Sie einen Backup-Speicherort für Ihre Workloads definieren. Weitere Informationen finden Sie im Abschnitt '"Public Cloud-Backup-Speicherorte anzeigen und aktualisieren" (S. 598)'.

Public Cloud-Backup-Speicherorte anzeigen und aktualisieren

Sie können die von Ihnen definierten Backup-Speicherort für Microsoft Azure, Amazon S3 und Wasabi im Modul **Backup Storage** anzeigen und aktualisieren oder, wenn Sie einen Schutzplan erstellen oder bearbeiten.

Informationen darüber, Sie den Zugriff auf ein Microsoft Azure-Abonnement aus der Cyber Protect-Konsole wieder entfernen können, finden Sie im unter "Den Zugriff auf ein Microsoft Azure-Abonnement entfernen" (S. 605). Informationen darüber, wie Sie den Zugriff auf andere Public Cloud-Verbindungen entfernen können, finden Sie unter "Den Zugriff auf andere Public Cloud Storage Services verwalten" (S. 606).

Hinweis
Sie können einen Public Cloud-Backup-Speicherort im Modul **Backup Storage** nicht manuell aktualisieren oder löschen. Die Inhalte des Backup-Speicherorts wird automatisch nach jeder Backup- oder Recovery-Aktion aktualisiert.

So können Sie Public Cloud-Backup-Speicherorte einsehen

1. Gehen Sie in der Cyber Protect-Konsole zu **Backup Storage**.
   Eine Liste der Backup-Speicherorte wird angezeigt, mit Details zur Speicherkapazität und Anzahl der Backups, die jedem Speicherort zugewiesen wurden.
   Weitere Informationen zum Arbeiten mit den aufgeführten Backup-Speicherorten finden Sie im Abschnitt '"Die Registerkarte 'Backup Storage'" (S. 577)'.
2. Wählen Sie den gewünschten Speicherort aus.
   Es werden alle aktuellen Backups für den ausgewählten Speicherort aufgelistet.
3. (Optional) Klicken Sie auf ein Backup, um weitere Details zu diesem Backup zu erhalten.

So können Sie einen Public Cloud-Backup-Speicherort in einem Schutzplan aktualisieren

1. Gehen Sie zu dem gewünschten Schutzplan und wählen Sie den Befehl **Bearbeiten**.
2. Klicken Sie auf den Link in der Zeile **Backup-Ziel**.
3. Wählen Sie einen Speicherort aus der Liste der vorhandenen Backup-Speicherorte aus – oder klicken Sie auf **Speicherort hinzufügen**, um einen neuen Speicherort hinzuzufügen.
   Wenn das relevante Microsoft Azure-Abonnement oder die Public Cloud-Verbindung bereits in der Cyber Protect-Konsole registriert ist, wählen Sie diese(s) aus der angezeigten Liste aus.
   Wenn Sie ein neues Microsoft Azure-Abonnement hinzufügen wollen, werden Sie aufgefordert, Ihre Microsoft-Kontodetails zu authentifizieren (siehe "Den Zugriff auf ein Microsoft Azure-Abonnement hinzufügen" (S. 603)). Weitere Informationen zu den erforderlichen Berechtigungen beim Verbinden mit Microsoft Azure finden Sie im englischsprachigen Artikel Microsoft Azure connection security and audit (72684).

Zugriff auf Public Cloud-Konten verwalten

Wenn Sie Acronis Cyber Protection Services in Public Cloud-Plattformen aktivieren wollen, muss der Zugriff auf die entsprechenden Public Cloud-Konten konfiguriert werden.

Wenn Sie beispielsweise mit Microsoft Azure arbeiten, ist der Zugriff auf Ihr Microsoft Azure-Abonnement erforderlich. Sobald dieses in der Cyber Protect-Konsole hinzugefügt wurde, kann das Abonnement ausgewählt werden, wenn Sie ein direktes Backup zu Microsoft Azure konfigurieren. Auch beim Arbeiten mit Amazon S3 und Wasabi sind die entsprechenden Zugriffsschlüssel erforderlich, die mit bestimmten Backup-bezogenen Richtlinien verbunden sind.

Der Public Cloud-Zugriff wird über das **Infrastruktur**-Menü in der Cyber Protect-Konsole verwaltet.

Wichtig
Bei Backups zu einem Public Cloud Storage ist die Backup-Validierung deaktiviert, um übermäßige Kosten für ausgehenden Datenverkehr zu vermeiden. Desweiteren ist es derzeit nicht möglich, einen Backup-Speicherort in einer Public Cloud demselben oder einem anderen Kunden-Mandanten neu zuzuordnen, wenn der Speicherort zuvor entfernt wurde. Für weitere Informationen wenden Sie sich bitte an das Support-Team.

Zugriffsanforderungen, um Backups zu einem Public Cloud Storage erstellen zu können

Wenn Sie Backups direkt zu einem Public Cloud Storage durchführen wollen, gibt es einige Zugriffsanforderungen, die für jede Plattform zu berücksichtigen sind:

- Microsoft Azure
- Amazon S3
- Wasabi

Backups zu Microsoft Azure erstellen

Wenn Sie sich mit einem Microsoft Azure-Abonnement verbinden wollen, benötigen Sie mehrere Berechtigungen. Weitere Informationen dazu finden Sie im Artikel Microsoft Azure connection security and audit (72684).

Backups zu Amazon S3 erstellen

Wenn Sie Backups zu Amazon S3 sichern wollen, müssen Sie mehrere Anforderungen erfüllen, wenn Sie die entsprechenden Amazon S3-Backup-Speicherorte definieren:

- Unterstützte Storage-Klassen
- Richtlinienberechtigungen
- Zugriffsschlüssel
- Bucket-Einstellungen

Unterstützte Storage-Klassen

Folgende Amazon S3-Storage-Klassen werden derzeit unterstützt:

- S3 Standard
- Standard - Infrequent Access (S3 Standard-IA)
- One Zone - Infrequent Access (S3 One Zone-IA)
- S3 Intelligent Tiering

Richtlinienberechtigungen

Wenn Sie Backups zu Amazon S3 erstellen, muss Ihr Amazon-Konto über die Mindestberechtigungen verfügen, damit Acronis die entsprechenden Workloads zu Amazon S3 sichern kann. Das bedeutet, dass die betreffenden Benutzer Zugriff auf die AWS Management-Konsole haben sollten und dass die entsprechende Richtlinie auf die Gruppe(n), der/denen sie zugewiesen sind, angewendet worden ist.

Beispiele

Die folgende Beispielrichtlinie zeigt das Minimum an Berechtigungen für einen großen Bereich von Ressourcen an. Beachten Sie, dass * alle Ressourcen angibt.

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action":
"s3:ListAllMyBuckets", "Resource": "*" }, { "Effect": "Allow", "Action": [
"s3:GetBucketLocation", "s3:GetBucketObjectLockConfiguration" ], "Resource": "*" },
{ "Effect": "Allow", "Action": "sts:GetFederationToken", "Resource": "*" }, {
"Effect": "Allow", "Action": [ "s3:GetBucketLocation", "s3:PutObject",
"s3:GetObject", "s3:DeleteObject" ], "Resource": "*" }, { "Effect": "Allow",
"Action": [ "s3:ListBucket" ], "Resource": "*" } ] }
```

Die folgende Beispielrichtlinie zeigt das Minimum an Berechtigungen an, die auf einen bestimmten Bucket beschränkt sind. Beachten Sie, dass `[BUCKETNAME]` durch den Namen des Buckets ersetzt werden sollte.

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action":
"s3:ListAllMyBuckets", "Resource": "*" }, { "Effect": "Allow", "Action": [
"s3:GetBucketLocation", "s3:GetBucketObjectLockConfiguration" ], "Resource":
"arn:aws:s3:::[BUCKETNAME]" }, { "Effect": "Allow", "Action":
"sts:GetFederationToken", "Resource": "*" }, { "Effect": "Allow", "Action": [
"s3:GetBucketLocation", "s3:PutObject", "s3:GetObject", "s3:DeleteObject" ],
"Resource": "arn:aws:s3:::[BUCKETNAME]/*" }, { "Effect": "Allow", "Action": [
"s3:ListBucket" ], "Resource": "arn:aws:s3:::[BUCKETNAME]" } ] }
```

Zugriffsschlüssel

Zugriffsschlüssel werden von Acronis für jede Amazon S3-Verbindung benötigt und werden verwendet, wenn die Amazon S3-Verbindung definiert wird. Weitere Informationen zur Generierung von Zugriffsschlüsseln und Zugriffsschlüssel-IDs finden Sie in der Amazon S3-Dokumentation.

Bucket-Einstellungen

Wenn Sie Amazon S3-Buckets als Backup-Speicherort verwenden, stellen Sie sicher, dass der Bucket mit den Standardeinstellungen konfiguriert ist, wozu auch die Blockierung des gesamten öffentlichen Zugriffs gehört (dies ist standardmäßig mit **Ein** festgelegt). Weitere Informationen zum Arbeiten mit Buckets finden Sie in der Amazon S3-Dokumentation.

Hinweis
Acronis unterstützt derzeit keine Bucket-Versionierung und Objektsperrung in Amazon S3, auch wenn diese Funktionen für den Bucket aktiviert sind.

Backups zu Wasabi erstellen

Wenn Sie Backups zu Wasabi erstellen, gibt es eine Reihe von Anforderungen, die Sie beim Definieren der Backup-Speicherorte berücksichtigen müssen:

- Richtlinienberechtigungen
- Zugriffsschlüssel
- Bucket-Einstellungen

Richtlinienberechtigungen

Wenn Sie einen Backup-Speicherort in Wasabi definieren, sollten Sie sicherstellen, dass die entsprechenden Richtlinien auf die entsprechenden Gruppen und Benutzer in Wasabi angewendet wurden.

Beispiele

Die folgende Beispielrichtlinie zeigt das Minimum an Berechtigungen für einen großen Bereich von Ressourcen an. Beachten Sie, dass * jede Ressource angibt.

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action":
"s3:ListAllMyBuckets", "Resource": "*" }, { "Effect": "Allow", "Action":
"s3:GetBucketLocation", "Resource": "*" }, { "Effect": "Allow", "Action": [
"iam:CreateRole", "iam:AttachRolePolicy", "sts:GetCallerIdentity", "sts:AssumeRole"
], "Resource": "*" }, { "Effect": "Allow", "Action": [ "s3:PutObject",
"s3:GetObject", "s3:DeleteObject" ], "Resource": "*" }, { "Effect": "Allow",
"Action": "s3:ListBucket", "Resource": "*" } ] }
```

Die folgende Beispielrichtlinie zeigt eingeschränkte Berechtigungen mit einem begrenzten Bereich von Ressourcen an. Beachten Sie, dass `[BUCKETNAME]` durch den Namen des Buckets und `[ACCOUNTID]` durch die ID des Wasabi-Kontos ersetzt werden muss.

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action":
"s3:ListAllMyBuckets", "Resource": "*" }, { "Effect": "Allow", "Action":
"s3:GetBucketLocation", "Resource": "arn:aws:s3:::[BUCKETNAME]" }, { "Effect":
"Allow", "Action": [ "iam:CreateRole", "iam:AttachRolePolicy",
"sts:GetCallerIdentity", "sts:AssumeRole" ], "Resource": "arn:aws:iam::
[ACCOUNTID]:*" }, { "Effect": "Allow", "Action": [ "s3:PutObject", "s3:GetObject",
"s3:DeleteObject" ], "Resource": "arn:aws:s3:::[BUCKETNAME]/*" }, { "Effect":
"Allow", "Action": "s3:ListBucket", "Resource": "arn:aws:s3:::[BUCKETNAME]" } ] }
```

Zugriffsschlüssel

Zugriffsschlüssel werden von Acronis für jede Wasabi-Verbindung benötigt und werden verwendet, wenn die Wasabi-Verbindung definiert wird. Weitere Informationen zur Generierung von Zugriffsschlüsseln und Zugriffsschlüssel-IDs finden Sie in der Wasabi-Dokumentation.

Bucket-Einstellungen

Wenn Sie Wasabi-Buckets als Backup-Speicherort verwenden, sollten Sie sicherstellen, dass der Bucket mit den Standardeinstellungen konfiguriert ist. Weitere Informationen zum Arbeiten mit Buckets finden Sie in der Wasabi-Dokumentation.

Hinweis
Acronis unterstützt derzeit keine Bucket-Versionierung und Objektsperrung in Wasabi, auch wenn diese Funktionen für den Bucket aktiviert sind.

Um den Zugriff auf Microsoft Azure-Abonnements zu verwalten

Indem Sie eine Verbindung zu den gewünschten Microsoft Azure-Abonnements in der Cyber Protect-Konsole herstellen, können Sie die entsprechenden Workloads direkt zu Microsoft Azure sichern.

Sie können die Verbindung zu einem Abonnement konfigurieren, wenn Sie einen Backup-Speicherort über das **Geräte**- oder **Backup Storage**-Menü erstellen (wie im Abschnitt '"Einen Backup-Speicherort in Microsoft Azure definieren" (S. 591)' beschrieben).

Alternativ können diese Microsoft Azure-Abonnements auch in der Anzeige **Public Clouds** konfiguriert werden (wenn Sie zu **Infrastruktur –> Public Clouds** gehen). Sie können hier auch Ihre Abonnements verwalten, z.B. den Zugriff auf das Abonnement erneuern, sich die Abonnement-Eigenschaften und -Aktivitäten anzeigen lassen oder das Abonnement löschen.

Je nach der Ihnen zugewiesenen Benutzerrolle können Sie möglicherweise auch Microsoft Azure-Abonnements verwalten, die von anderen Benutzern innerhalb Ihrer Organisation hinzugefügt wurden. Wenn Sie beispielsweise Firmen- oder Abteilungsadministrator sind oder Ihnen die Rolle

Cyber-Administrator oder Administrator im Cyber Protection Service zugewiesen wurde, können Sie die Microsoft Azure-Abonnements einsehen und verwalten, die von anderen Administratoren hinzugefügt wurden, sowie die Abonnements, die von Benutzern ohne Administratorstatus hinzugefügt wurden. Benutzer, die keine Administratoren sind, können nur solche Microsoft Azure-Abonnements einsehen und darauf zugreifen, die sie der Cyber Protect-Konsole hinzugefügt haben.

Hinweis
Partner können die Microsoft Azure-Abonnements von Kunden verwalten, die unterhalb ihrer Hierarchieebene liegen. Wenn ein Partner jedoch **Alle Kunden** auswählt, wird das Menü **Infrastruktur** in der Cyber Protect-Konsole nicht angezeigt.

Wichtig
Bei einer Verbindung mit einem Microsoft Azure-Abonnement benötigt Acronis die Mindestberechtigungen, um eine Verbindung mit dem Abonnement herstellen zu können. Weitere Informationen zu den erforderlichen Berechtigungen finden Sie im Artikel Microsoft Azure connection security and audit (72684).

Den Zugriff auf ein Microsoft Azure-Abonnement hinzufügen

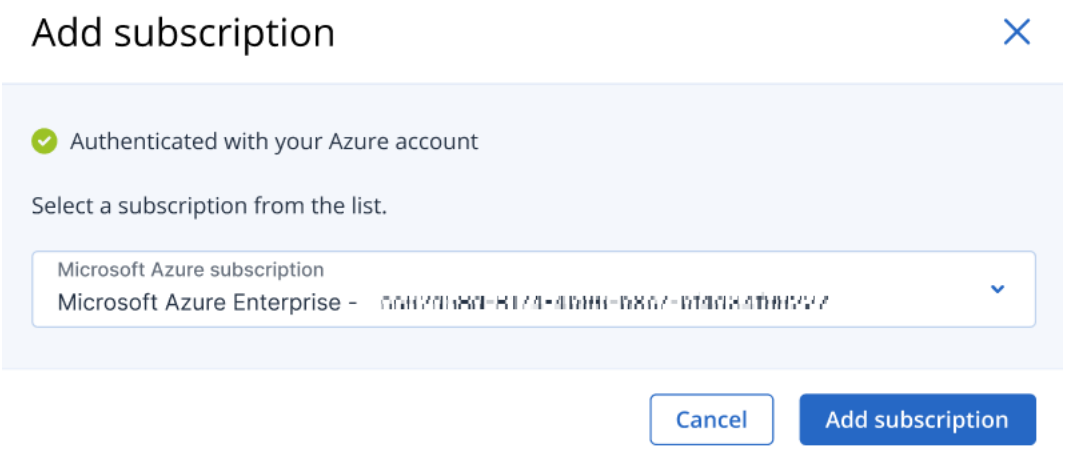
Durch Hinzufügen eines Microsoft Azure-Abonnements in der Cyber Protect-Konsole kann Acronis sicher auf Ihr Abonnement zugreifen und die entsprechenden Workloads direkt zu Microsoft Azure sichern.

So können Sie den Zugriff auf ein Microsoft Azure-Abonnement hinzufügen

1. Gehen Sie in der Cyber Protect-Konsole zu **Infrastruktur –> Public Clouds**.
2. Klicken Sie auf **Hinzufügen** und wählen Sie aus der angezeigten Liste der Optionen **Microsoft Azure** aus.
3. Klicken Sie im angezeigten Dialog auf **Anmelden**. Sie werden zur Microsoft-Anmeldeseite weitergeleitet.

   Hinweis
   Ihnen muss eine der folgenden Rollen in Microsoft Azure AD zugewiesen sein, damit Sie die Verbindung zum Abonnement abschließen können: Cloudanwendungsadministrator, Anwendungsadministrator oder Globaler Administrator. Außerdem muss Ihnen für jedes ausgewählte Abonnement die Rolle 'Besitzer' zugewiesen sein.

4. Geben Sie im Microsoft-Anmeldebildschirm Ihre Anmeldedaten ein und akzeptieren Sie die angeforderten Berechtigungen. Der Verbindungsprozess wird gestartet, was einige Minuten dauern kann.
   Weitere Informationen über den sicheren Zugriff auf Ihr Microsoft Azure und Ihr Abonnement finden Sie im Artikel 'Microsoft Azure connection security and audit (72684)'.
5. Wählen Sie nach Abschluss der Verbindung das gewünschte Abonnement aus dem Listenfeld im angezeigten Dialog aus und klicken Sie anschließend auf **Abonnement hinzufügen**.



Das Abonnement wird in die Liste der Public Clouds aufgenommen.

Informationen zur Erneuerung des jährlichen Zugriffszertifikats für das Abonnement finden Sie im Abschnitt '"Den Zugriff auf ein Microsoft Azure-Abonnement erneuern" (S. 604)'.

Informationen darüber, wie Sie den Zugriff auf das Abonnement wieder aufheben können, finden Sie im Abschnitt '"Den Zugriff auf ein Microsoft Azure-Abonnement entfernen" (S. 605)'.

Hinweis
Wenn das Microsoft Azure-Konto, bei dem Sie angemeldet sind, Zugriff auf mehrere Microsoft Azure Active Directories (ADs) hat, einschließlich solcher ADs, in die Sie als Gastbenutzer eingeladen wurden, wird nur das Standardbenutzerverzeichnis ausgewählt. Wenn Sie ein Verzeichnis verwenden wollen, in dem Sie ein Gastbenutzer sind, müssen Sie einen neuen Benutzer in diesem speziellen Microsoft Azure AD erstellen. Sie können sich dann an diesem Konto anmelden und mit dem entsprechenden Abonnement verbinden.

Den Zugriff auf ein Microsoft Azure-Abonnement erneuern

Nach der Registrierung in der Cyber Protect-Konsole wird der Zugriff auf ein Microsoft Azure-Abonnement automatisch von Acronis für ein Jahr mit einem kostenlosen und individuellen Zugriffszertifikat eingerichtet. Wenn das Zertifikat kurz vor seinem Ablaufdatum steht, können Sie es schnell und einfach erneuern.

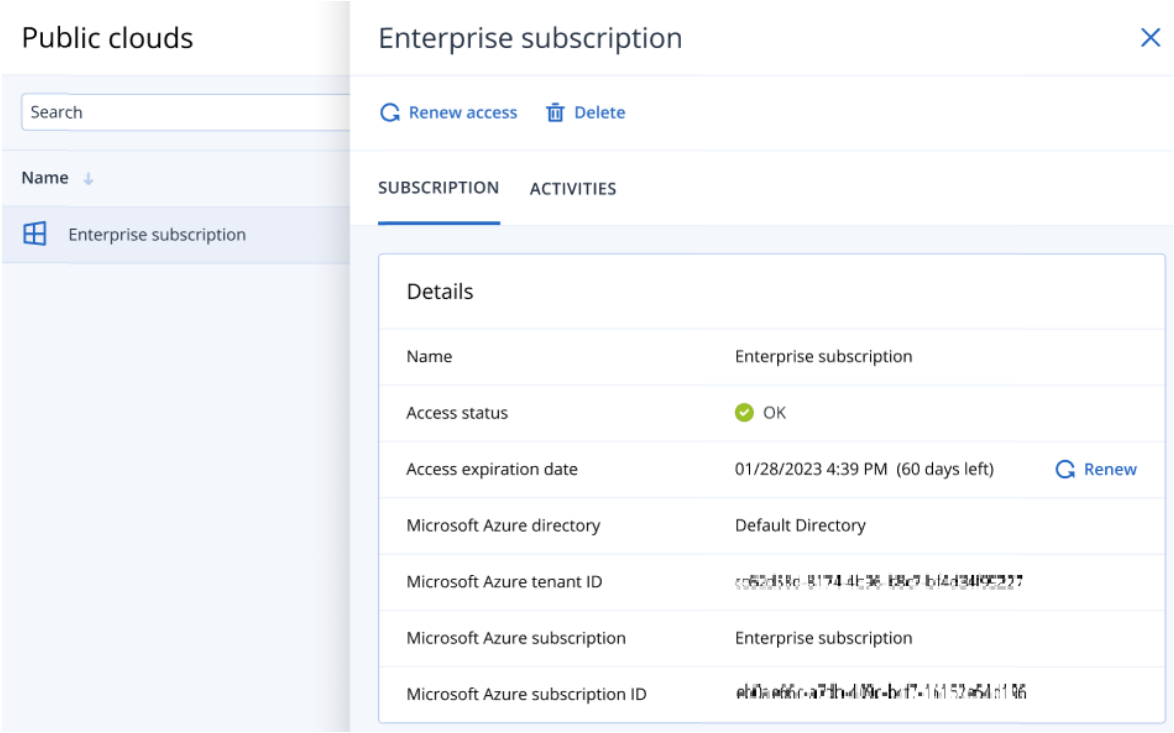
So können Sie das Zugriffszertifikat für Ihr Microsoft Azure-Abonnement erneuern

1. Gehen Sie in der Cyber Protect-Konsole zu **Infrastruktur –> Public Clouds**.
2. Wählen Sie das entsprechende Abonnement aus der angezeigten Liste aus.

   Hinweis
   In der Spalte **Zugriffsstatus** wird der aktuelle Status des Zugriffszertifikats für jedes Abonnement angezeigt, wobei dieser Status einer von zwei Zuständen sein kann: **OK** oder **Abgelaufen**.

3. Klicken Sie im rechten Fensterbereich auf **Zugriff erneuern**.

Alternativ können Sie auch auf die Registerkarte **Abonnement** klicken und dann im Feld **Zugriffsablaufdatum** auf **Erneuern** klicken.



4. Geben Sie im Microsoft-Anmeldebildschirm Ihre Anmeldedaten ein und akzeptieren Sie die angeforderten Berechtigungen. Der Verbindungsprozess wird gestartet, was einige Minuten dauern kann.

   Wenn die Authentifizierung erfolgreich war, wird der Zugriff automatisch für ein Jahr verlängert.

   Weitere Informationen zu den erforderlichen Berechtigungen finden Sie im Artikel Microsoft Azure connection security and audit (72684).

Den Zugriff auf ein Microsoft Azure-Abonnement entfernen

Sie sollten den Zugriff auf das Microsoft Azure-Abonnement entfernen, wenn Sie keine Workloads in Microsoft Azure per Backup sichern wollen.

So können Sie den Zugriff auf ein Microsoft Azure-Abonnement entfernen

Wichtig
Sie können ein Abonnement nicht entfernen, wenn es aktuell verwendet wird, um Backups zu Microsoft Azure zu erstellen.

1. Gehen Sie in der Cyber Protect-Konsole zu **Infrastruktur –> Public Clouds**.
2. Wählen Sie das entsprechende Abonnement aus der angezeigten Liste aus.
3. Klicken Sie im rechten Fensterbereich auf **Löschen**.

Hinweis
Sie können nur ein von Ihnen hinzugefügtes Abonnement entfernen. Sie können ein Abonnement auch dann entfernen, wenn Sie ein Firmen- oder Abteilungsadministrator sind oder wenn Ihnen die Rolle eines Cyber-Administrators oder Administrators im Cyber Protection Service zugewiesen wurde.

4. Klicken Sie in der angezeigten Bestätigungsmeldung auf **Entfernen**.

Den Zugriff auf andere Public Cloud Storage Services verwalten

Hinweis
Dieser Abschnitt beschreibt, wie Sie den Zugriff auf alle Public Cloud Storage Services verwalten können – mit Ausnahme von Microsoft Azure, was im Abschnitt "Um den Zugriff auf Microsoft Azure-Abonnements zu verwalten" (S. 602) beschrieben wird.

Wenn Sie sich in der Cyber Protect-Konsole mit dem entsprechenden Public Cloud-Konto verbinden, können Sie Workloads direkt zum entsprechenden Public Cloud Storage sichern.

Sie können Verbindungen zu Public Cloud Storage-Konten konfigurieren, wenn Sie einen Backup-Speicherort über das Menü **Geräte** oder **Backup Storage** erstellen. Alternativ können Sie die Public Cloud-Verbindungen auch in der Anzeige **Public Clouds** konfigurieren (gehen Sie zu **Infrastruktur > Public Clouds**). Hier können Sie Ihre Verbindung auch verwalten, also beispielsweise den Zugriff auf die Verbindung erneuern, Verbindungseigenschaften und -aktivitäten einsehen oder die Verbindung entfernen.

Je nach der Ihnen zugewiesenen Benutzerrolle können Sie möglicherweise auch Public Cloud-Verbindungen verwalten, die von anderen Benutzern innerhalb Ihrer Organisation hinzugefügt wurden. Wenn Sie beispielsweise Firmen- oder Abteilungsadministrator sind oder Ihnen die Rolle Cyber-Administrator oder Administrator im Cyber Protection Service zugewiesen wurde, können Sie die Public Cloud-Verbindungen einsehen und verwalten, die von anderen Administratoren hinzugefügt wurden, sowie solche Verbindungen, die von Benutzern ohne Administratorstatus hinzugefügt wurden. Benutzer, die keine Administratoren sind, können nur solche Public Cloud-Verbindungen einsehen und darauf zugreifen, die sie selbst in der Cyber Protect-Konsole hinzugefügt haben.

Hinweis
Partner können die Public Cloud-Verbindungen von Kunden verwalten, die unterhalb ihrer Hierarchieebene liegen. Wenn ein Partner jedoch **Alle Kunden** auswählt, wird das Menü **Infrastruktur** in der Cyber Protect-Konsole nicht angezeigt.

Wichtig
Um auf eine Public Cloud-Verbindung zugreifen zu können, benötigt Acronis einige entsprechende Berechtigungen. Weitere Informationen dazu finden Sie unter "Zugriffsanforderungen, um Backups zu einem Public Cloud Storage erstellen zu können" (S. 599).

Zugriff auf eine Public Cloud-Verbindung hinzufügen

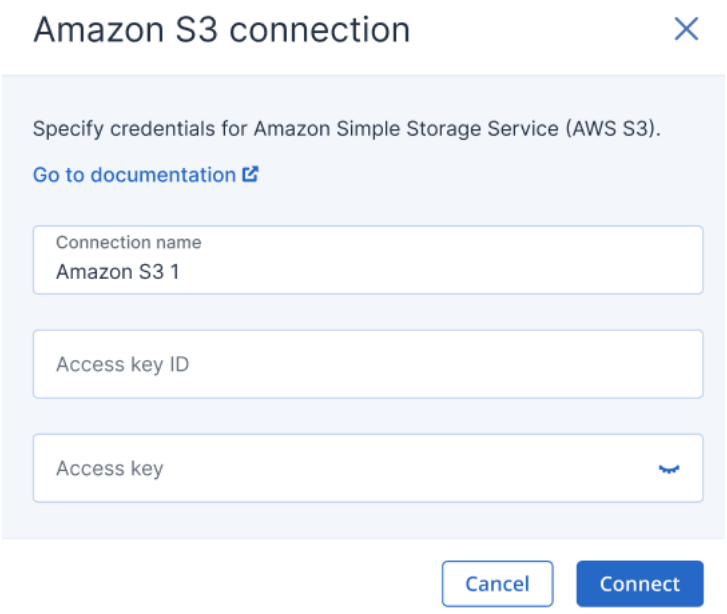
Wenn Sie eine Verbindung zu einer Public Cloud (wie Amazon S3 oder Wasabi) in der Cyber Protect-Konsole hinzugefügt haben, kann Acronis sicher auf Ihre Cloud-Ressourcen zugreifen und Workloads direkt zum entsprechenden Public Cloud Storage (als Backup-Ziel) sichern.

So können Sie einen Zugriff auf eine Public Cloud-Verbindung hinzufügen

1. Gehen Sie in der Cyber Protect-Konsole zu **Infrastruktur –> Public Clouds**.
2. Klicken Sie auf **Hinzufügen** und wählen Sie eine der folgenden Optionen:
   - **Amazon S3**

     Definieren Sie in dem angezeigten Dialogfenster folgende Elemente:
     - **Verbindungsname**: Der Name für die Amazon S3-Verbindung.
     - **Zugriffsschlüssel-ID**: Die Zugriffsschlüssel-ID des Benutzers für den Amazon S3-Service.
     - **Zugriffsschlüssel**: Der Zugriffsschlüssel des Benutzers für den Amazon S3-Service.

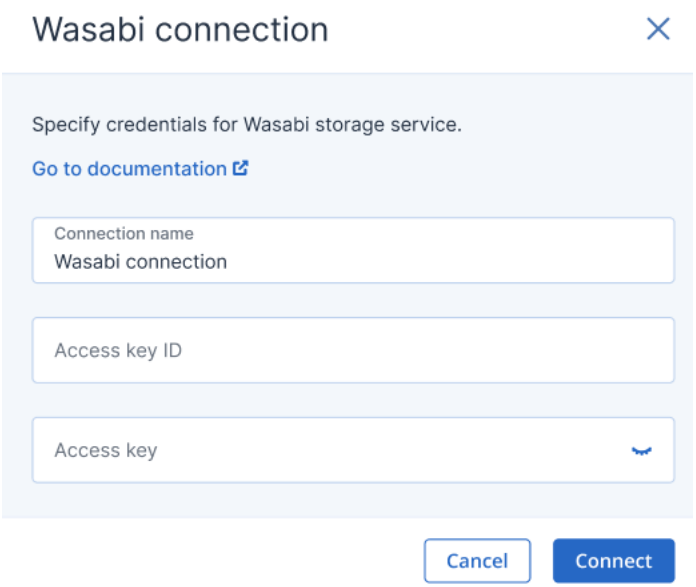
       Mit dem Zugriffsschlüssel und der Zugriffsschlüssel-ID kann Acronis auf die Storage-Klassen und Buckets für die entsprechende Verbindung zuzugreifen. Weitere Informationen zu den Zugriffsschlüsseln und Berechtigungen, die von Acronis benötigt werden, finden Sie unter "Zugriffsanforderungen, um Backups zu einem Public Cloud Storage erstellen zu können" (S. 599).



   - **Wasabi**

     Definieren Sie in dem angezeigten Dialogfenster folgende Elemente:
     - **Verbindungsname**: Der Name für die Wasabi-Verbindung.
     - **Zugriffsschlüssel-ID**: Die Zugriffsschlüssel-ID des Benutzers für den Wasabi-Service.
     - **Zugriffsschlüssel**: Der Zugriffsschlüssel des Benutzers für den Wasabi-Service.

Mit dem Zugriffsschlüssel und der Zugriffsschlüssel-ID kann Acronis auf die Storage-Klassen und Buckets für die entsprechende Verbindung zuzugreifen. Weitere Informationen zu den Zugriffsschlüsseln und Berechtigungen, die von Acronis benötigt werden, finden Sie unter "Zugriffsanforderungen, um Backups zu einem Public Cloud Storage erstellen zu können" (S. 599).



3. Klicken Sie auf **Verbinden**.

   Der Verbindungsprozess wird gestartet und kann mehrere Minuten dauern. Nach Abschluss wird die Verbindung zur Liste der Public Clouds hinzugefügt.

   Informationen zur Erneuerung des jährlichen Zugriffszertifikats für die Verbindung finden Sie im Abschnitt "Den Zugriff auf eine Public Cloud-Verbindung erneuern" (S. 608).

   Informationen darüber, wie Sie den Zugriff auf die Verbindung wieder entfernen können, finden Sie im Abschnitt "Den Zugriff auf eine Public Cloud-Verbindung entfernen" (S. 609).

Den Zugriff auf eine Public Cloud-Verbindung erneuern

Wenn eine Public Cloud-Verbindung in der Cyber Protect-Konsole registriert wurde, weist Acronis automatisch ein freies und eindeutiges Zugriffszertifikat zu, das den Zugriff auf die öffentliche Cloud-Verbindung ermöglicht. Das Zertifikat ist jeweils ein Jahr gültig. Wenn das Zertifikat sein Ablaufdatum bald erreicht, können Sie es erneuern.

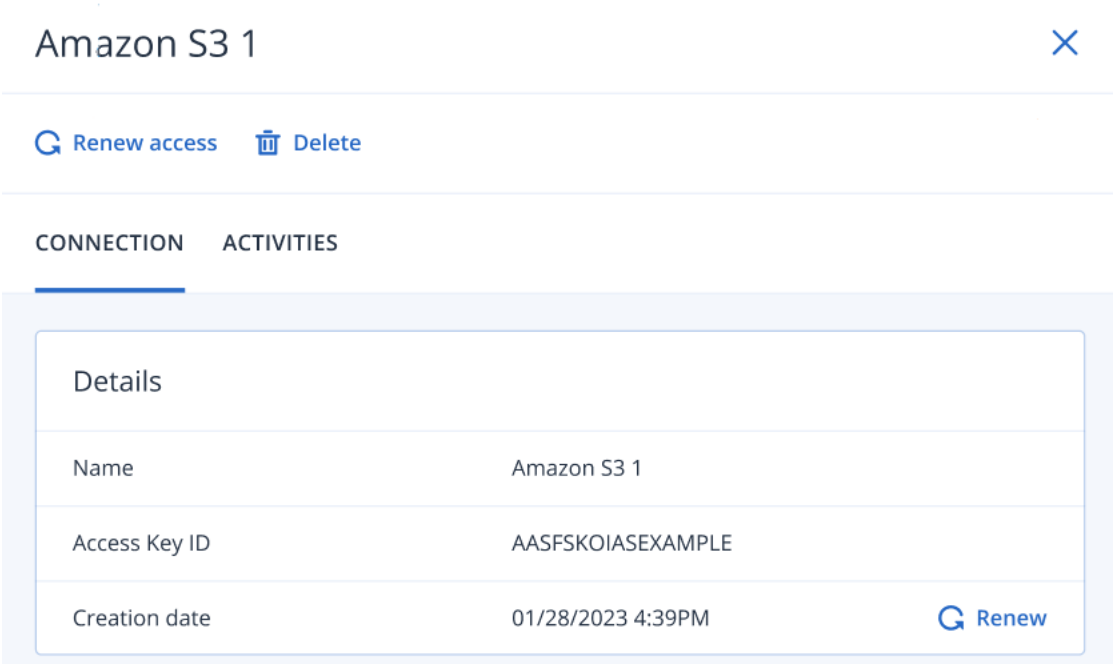
So können Sie das Zugriffszertifikat für Ihre Public Cloud-Verbindung erneuern

1. Gehen Sie in der Cyber Protect-Konsole zu **Infrastruktur –> Public Clouds**.
2. Wählen Sie die relevante Verbindung aus der Liste aus.

   Hinweis
   In der Spalte **Zugriffsstatus** wird der aktuelle Status des Zugriffszertifikats für jede Verbindung angezeigt, wobei dieser Status einer von zwei Zuständen sein kann: **OK** oder **Abgelaufen**.

3. Klicken Sie im rechten Fensterbereich auf **Zugriff erneuern**.

Alternativ können Sie auch auf die Registerkarte **Verbindung** klicken und dann im Feld **Erstellungsdatum** auf **Erneuern** klicken.



Wenn die Authentifizierung erfolgreich war, wird der Zugriff automatisch für ein Jahr verlängert.

Den Zugriff auf eine Public Cloud-Verbindung entfernen

Sie sollten den Zugriff auf eine Public Cloud-Verbindung wieder entfernen, wenn Sie keine Workloads zu der entsprechenden Public Cloud sichern.

So können Sie den Zugriff auf eine Public Cloud-Verbindung wieder löschen

Wichtig
Sie können eine Verbindung nicht entfernen, wenn diese gerade für Backups zu der entsprechenden Public Cloud verwendet wird.

1. Gehen Sie in der Cyber Protect-Konsole zu **Infrastruktur –> Public Clouds**.
2. Wählen Sie die Verbindung aus der Liste aus.
3. Klicken Sie im rechten Fensterbereich auf **Löschen**.

   Hinweis
   Sie können nur eine Verbindung entfernen, die Sie selbst hinzugefügt haben. Sie können eine Verbindung außerdem auch dann entfernen, wenn Sie ein Firmen- oder Abteilungsadministrator sind oder wenn Ihnen die Rolle eines Cyber-Administrators oder Administrators im Cyber Protection Service zugewiesen wurde.

4. Klicken Sie in der angezeigten Bestätigungsmeldung auf **Löschen**.

Microsoft-Applikationen sichern

Microsoft SQL Server und Microsoft Exchange Server sichern

Hinweis
Ein Microsoft SQL-Backup wird nur für Datenbanken unterstützt, die unter den Dateisystemen NFTS, REFS oder FAT32 laufen. ExFat wird nicht unterstützt.

Es gibt zwei Methoden, wie Sie diese Microsoft-Applikationen schützen können:

- **Datenbank-Backup**
  Hierbei handelt es sich um ein Datei-Backup der Datenbanken und der Metadaten, die mit den Datenbanken assoziiert sind. Die Datenbanken können zu einer aktiven Applikation oder als Dateien wiederhergestellt werden.
- **Applikationskonformes Backup**
  Hierbei handelt es sich um ein Laufwerk-Backup, bei dem außerdem die Metadaten der Applikationen eingesammelt werden. Diese Metadaten ermöglichen es, dass die Applikationsdaten (im Backup) durchsucht und wiederhergestellt werden können, ohne dass dafür das komplette Laufwerk/Volume wiederhergestellt werden müsste. Das Laufwerk/Volume kann natürlich auch komplett wiederhergestellt werden. Das bedeutet, dass eine einzelne Lösung und ein einzelner Schutzplan gleichermaßen die Anwendungsbereiche 'Disaster Recovery' und 'Data Protection' abdecken kann.

Bei einem Microsoft Exchange Server haben Sie die Möglichkeit, ein **Postfach-Backup** durchzuführen. Dabei handelt es sich um ein Backup von einzelnen Postfächern über das Exchange-Webdienstprotokoll. Die Postfächer oder auch einzelne Postfachelemente können zu einem aktiv laufenden Exchange Server oder zu Microsoft 365 wiederhergestellt werden. Das Postfach-Backup wird für Microsoft Exchange Server 2010 Service Pack 1 (SP1) oder höher unterstützt.

Microsoft SharePoint sichern

Eine Microsoft SharePoint-Farm besteht aus Front-End-Webservern (die die SharePoint-Dienste ausführen), Datenbankservern (die den Microsoft SQL Server ausführen) und – optional – bestimmte Applikationsserver, die die Front-End-Webserver von einigen SharePoint-Diensten entlasten. Einige Front-End- und Applikationsserver können identisch sein.

So können Sie eine komplette SharePoint-Farm schützen:

- Sichern Sie alle Datenbank-Server mit einem applikationskonformen Backup.
- Sichern Sie alle einzelnen Front-End- und Applikationsserver mit einem herkömmlichem Laufwerk-Backup.

Die Backups aller Server sollten mit derselben Planung durchgeführt werden.

Wenn Sie nur die Inhalte sichern wollen, können Sie die Inhaltsdatenbanken separat sichern.

Einen Domain-Controller sichern

Eine Maschine, auf der die Active Directory Domain Services (Active Directory-Domänendienste) laufen, kann per applikationskonformem Backup geschützt werden. Falls eine Domain mehr als zwei Domain-Controller enthält und Sie einen davon wiederherstellen, wird eine 'nicht autorisierte' Wiederherstellung durchgeführt und so ein USN-Rollback nach der Wiederherstellung vermieden.

Applikationen wiederherstellen

Die nachfolgende Tabelle gibt einen Überblick über alle Recovery-Methoden, die zur Wiederherstellung von Applikationen verfügbar sind.

	Von einem Datenbank-Backup	**Von einem applikationskonformen Backup**	**Von einem Laufwerk-Backup**
Microsoft SQL Server	Datenbanken zu einer aktiven SQL Server-Instanz Datenbanken als Dateien	Komplette Maschine Datenbanken zu einer aktiven SQL Server-Instanz Datenbanken als Dateien	Komplette Maschine
Microsoft Exchange Server	Datenbanken zu einem aktiven Exchange Server Datenbanken als Dateien Granulares Recovery zu einem aktiven Exchange Server oder zu Microsoft 365*	Komplette Maschine Datenbanken zu einem aktiven Exchange Server Datenbanken als Dateien Granulares Recovery zu einem aktiven Exchange Server oder zu Microsoft 365*	Komplette Maschine
Microsoft SharePoint-Datenbank-Server	Datenbanken zu einer aktiven SQL Server-Instanz Datenbanken als Dateien Granulares Recovery mithilfe des SharePoint Explorers	Komplette Maschine Datenbanken zu einer aktiven SQL Server-Instanz Datenbanken als Dateien Granulares Recovery mithilfe des SharePoint Explorers	Komplette Maschine
Microsoft SharePoint-Front-End-Webserver	-	-	Komplette Maschine
Active Directory-Domänendienste	-	Komplette Maschine	-

* Granulares Recovery ist auch für Postfach-Backups möglich. Die Wiederherstellung von Exchange-Datenelementen zu Microsoft 365 (und umgekehrt) wird nur unter der Bedingung unterstützt, dass der Agent für Microsoft 365 lokal installiert ist.

Voraussetzungen

Bevor Sie das applikationskonforme Backup konfigurieren, sollten Sie sicherstellen, dass die nachfolgenden Voraussetzungen bzw. Anforderungen erfüllt sind.

Verwenden Sie zum Überprüfen des VSS-Writer-Stadiums den Befehl `vssadmin list writers`.

Allgemeine Anforderungen

Für Microsoft SQL Server müssen folgende Anforderungen erfüllt sein:

- Mindestens eine Microsoft SQL Server-Instanz ist gestartet.
- Der SQL Writer für VSS ist aktiviert.

Für Microsoft Exchange Server müssen folgende Anforderungen erfüllt sein:

- Der Microsoft Exchange-Informationsspeicherdienst ist gestartet.
- Windows PowerShell ist installiert. Für Exchange 2010 (und höher) muss es mindestens Windows PowerShell-Version 2.0 sein.
- Microsoft .NET Framework ist installiert.
  Für Exchange 2007 muss es mindestens Microsoft .NET Framework-Version 2.0 sein.
  Für Exchange 2010 (und höher) muss es mindestens Microsoft .NET Framework-Version 3.5 sein.
- Der Exchange Writer für VSS ist aktiviert.

Hinweis
Der Agent für Exchange benötigt einen temporären Speicher, um arbeiten zu können. Diese temporären Dateien liegen standardmäßig im Ordner `%ProgramData%\Acronis\Temp`. Überprüfen Sie, dass der freie Speicherplatz des Volumes, auf dem der Ordner `%ProgramData%` liegt, mindestens 15% der Größe einer Exchange-Datenbank entspricht. Alternativ können Sie vor der Erstellung von Exchange-Backups den Speicherort der temporären Dateien ändern, wie es im Knowledge Base-Artikel Den Speicherort für temporäre Dateien und Ordner ändern (40040) beschrieben ist.

Auf einem Domain Controller müssen folgende Anforderungen erfüllt sein:

- Der Active Directory Writer für VSS ist aktiviert.

Zur Erstellung eines Schutzplans müssen folgende Anforderungen erfüllt sein:

- Für physische Maschinen und Maschinen mit installiertem Agenten ist die Backup-Option 'VSS (Volume Shadow Copy Service)' aktiviert.
- Für virtuelle Maschinen ist die Backup-Option 'VSS (Volume Shadow Copy Service) für virtuelle Maschinen' aktiviert.

Zusätzliche Anforderungen für applikationskonforme Backups

Überprüfen Sie bei Erstellung eines Schutzplans, dass die '**Komplette Maschine**' zum Backup ausgewählt wurde. Die Backup-Option **Sektor-für-Sektor** muss im Schutzplan deaktiviert sein, ansonsten können aus solchen Backups keine Applikationsdaten wiederhergestellt werden. Wenn der Plan im **Sektor-für-Sektor**-Modus ausgeführt wird, weil automatisch auf diesen Modus umgeschaltet wird, dann werden keine Applikationsdaten wiederherstellbar sein.

Anforderungen für virtuelle ESXi-Maschinen

Falls die Applikation auf einer virtuellen Maschine läuft, die vom Agenten für VMware gesichert wird, müssen folgende Anforderungen erfüllt sein:

- Die zu sichernde virtuelle Maschine erfüllt die Anforderungen für applikationskonsistente Backups und Wiederherstellungen, wie sie im englischsprachigen Artikel „Windows Backup Implementations“ der VMware-Dokumentation unter folgender Adresse aufgeführt sind: https://code.vmware.com/docs/1674/virtual-disk-programming-guide/doc/vddkBkupVadp.9.6.html.
- Die VMware Tools sind auf der Maschine installiert und aktuell.
- Die Benutzerkontensteuerung (UAC) ist auf der Maschine deaktiviert. Wenn Sie die Benutzerkontensteuerung (UAC) nicht ausschalten wollen, müssen Sie die Anmeldedaten des integrierten Domain-Administrators (DOMAIN\Administrator) bereitstellen, wenn Sie das Applikations-Backup aktivieren.
  Wenn Sie die Benutzerkontensteuerung (UAC) nicht ausschalten wollen, müssen Sie die Anmeldedaten des integrierten Domain-Administrators (DOMAIN\Administrator) bereitstellen, wenn Sie das Applikations-Backup aktivieren.

  Hinweis
  Verwenden Sie das integrierte Domain-Administrator-Konto, das beim Erstellen der Domain konfiguriert wurde. Später erstellte Konten werden nicht unterstützt.

Anforderungen für virtuelle Hyper-V-Maschinen

Falls die Applikation auf einer virtuellen Maschine läuft, die vom Agenten für Hyper-V gesichert wird, müssen folgende Anforderungen erfüllt sein:

- Das Gastbetriebssystem ist Windows Server 2008 oder höher.
- Für Hyper-V 2008 R2: das Gastbetriebssystem ist Windows Server 2008/2008 R2/2012.
- Die virtuelle Maschine hat keine dynamischen Laufwerke.
- Die Netzwerkverbindung besteht zwischen dem Hyper-V-Host und dem Gastbetriebssystem. Dies ist notwendig, um Remote-WMI-Abfragen innerhalb der virtuellen Maschine ausführen zu können.
- Die Benutzerkontensteuerung (UAC) ist auf der Maschine deaktiviert. Wenn Sie die Benutzerkontensteuerung (UAC) nicht ausschalten wollen, müssen Sie die Anmeldedaten des

integrierten Domain-Administrators (DOMAIN\Administrator) bereitstellen, wenn Sie das Applikations-Backup aktivieren.
Wenn Sie die Benutzerkontensteuerung (UAC) nicht ausschalten wollen, müssen Sie die Anmeldedaten des integrierten Domain-Administrators (DOMAIN\Administrator) bereitstellen, wenn Sie das Applikations-Backup aktivieren.

Hinweis
Verwenden Sie das integrierte Domain-Administrator-Konto, das beim Erstellen der Domain konfiguriert wurde. Später erstellte Konten werden nicht unterstützt.

- Die Konfiguration der virtuellen Maschine erfülllt die folgenden Kriterien:
  - Die Hyper-V-Integrationsdienste sind installiert und aktuell. Das kritische Update ist: https://support.microsoft.com/de-de/help/3063109/hyper-v-integration-components-update-for-windows-virtual-machines
  - In den Einstellungen der virtuellen Maschine ist die Option **Verwaltung** –> **Integrationsdienste** –> **Sicherung (Volumeprüfpunkt)** aktiviert.
  - Für Hyper-V 2012 und höher: die virtuelle Maschine hat keine Prüfpunkte.
  - Für Hyper-V 2012 R2 und höher: die virtuelle Maschine hat einen SCSI-Controller (überprüfen Sie **Einstellungen** –> **Hardware**).

Datenbank-Backup

Bevor Sie ein Datenbank-Backup durchführen, sollten Sie sicherstellen, dass die unter 'Voraussetzungen' aufgeführten Anforderungen erfüllt sind.

Wählen Sie die Datenbanken wie nachfolgend beschrieben aus – und spezifizieren Sie die anderen Einstellungen des Schutzplans je nach Bedarf.

SQL-Datenbanken auswählen

Das Backup einer SQL-Datenbank enthält die entsprechenden Datenbankdateien (.mdf, .ndf), Protokolldateien (.ldf) und andere zugeordnete Dateien. Die Dateien werden mithilfe des SQL-Writer-Dienstes gesichert. Der Dienst muss dann laufen, wenn der Volume Shadow Copy Service (VSS, Volumenschattenkopie-Dienst) ein Backup oder eine Wiederherstellung anfordert.

Die SQL-Transaktionsprotokolle werden nach jedem erfolgreichen Backup abgeschnitten. Die SQL-Protokollabschneidung kann in den Schutzplan-Optionen deaktiviert werden.

So können Sie SQL-Datenbanken auswählen

1. Klicken Sie auf **Geräte** –> **Microsoft SQL**.
   Die Software zeigt einen Verzeichnisbaum mit SQL Server-AlwaysOn-Verfügbarkeitsgruppen (AAG), Maschinen, die den Microsoft SQL Server ausführen, SQL Server-Instanzen und Datenbanken an.
2. Bestimmen Sie (per 'Durchsuchen') die Daten, die Sie sichern wollen.

Erweitern Sie die Verzeichnisknoten oder klicken Sie rechts neben dem Verzeichnis doppelt auf einzelne Elemente in der Liste.

3. Wählen Sie Daten aus, die Sie sichern wollen. Sie können AAGS, den SQL Server ausführende Maschinen, SQL Server-Instanzen oder bestimmte Datenbanken auswählen.
   - Wenn Sie eine AAG auswählen, werden alle in der ausgewählten AAG enthaltenen Datenbanken per Backup gesichert. Weitere Informationen über das Backup von AAGs oder einzelnen AAG-Datenbanken finden Sie im Abschnitt 'AlwaysOn-Verfügbarkeitsgruppen (AAG) sichern'.
   - Wenn Sie eine Maschine auswählen, auf welcher ein SQL Server läuft, so werden alle Datenbanken gesichert, die an allen (auf der ausgewählten Maschine laufenden) SQL Server-Instanzen angefügt sind.
   - Wenn Sie eine bestimmte SQL Server-Instanz auswählen, werden alle Datenbanken gesichert, die an diese ausgewählte Instanz angefügt sind.
   - Wenn Sie die gewünschten Datenbanken direkt auswählen, werden dagegen nur diese Datenbanken gesichert.
4. Klicken Sie auf den Befehl **Schützen**. Geben Sie bei Aufforderung die benötigten Anmeldedaten ein, um auf die SQL Server-Daten zugreifen zu können.

   Wenn Sie die Windows-Authentifizierung verwenden, muss das Konto auf der betreffenden Maschine ein Mitglied der Gruppe **Sicherungs-Operatoren** oder der Gruppe **Administratoren** sein – und auf jeder Instanz, die Sie sichern wollen, ein Mitglied der **SysAdmin**-Rolle.

   Wenn Sie die SQL Server-Authentifizierung verwenden, muss das Konto auf jeder Instanz, die Sie sichern wollen, ein Mitglied der **SysAdmin**-Rolle sein.

Exchange Server-Daten auswählen

Die nachfolgende Tabelle gibt Ihnen einen Überblick über die Microsoft Exchange Server-Daten, die Sie für ein Backup verwenden können – und die (mindestens benötigten) Benutzerrechte, die zum Sichern dieser Daten erforderlich sind.

Exchange-Version	Datenelemente	Benutzerrechte
2007	Speichergruppen	Mitglied in der Rollengruppe **Exchange-Organisationsadministratoren**
2010/2013/2016/2019	Datenbanken, Datenbankverfügbarkeitsgruppen (DAG)	Mitglied in der Rollengruppe **Serververwaltung**.

Ein Voll-Backup enthält alle ausgewählten Exchange Server-Daten.

Ein inkrementelles Backup enthält die geänderten Datenblöcke der Datenbankdateien, die Prüfpunktdateien und eine kleinere Anzahl von Protokolldateien, die neuer als der korrespondierende Datenbank-Prüfpunkt sind. Da im Backup alle Änderungen an den Datenbankdateien enthalten sind, ist es nicht notwendig, alle Transaktionsprotokoll-Datensätze seit dem letzten (vorherigen) Backup zu sichern. Es muss nur dasjenige Protokoll nach einer

Wiederherstellung zurückgespielt werden, welches neuer (jünger) als der Prüfpunkt ist. Dies ermöglicht eine schneller Wiederherstellung und gewährleistet ein erfolgreiches Datenbank-Backup auch bei aktivierter Umlaufprotokollierung.

Die Transaktionsprotokolldateien werden nach jedem erfolgreichen Backup abgeschnitten.

So können Sie Exchange-Server-Daten auswählen

1. Klicken Sie auf **Geräte** –> **Microsoft Exchange**.
   Die Software zeigt den Verzeichnisbaum der Exchange Server Datenbankverfügbarkeitsgruppen (DAG) sowie der Maschinen an, die den Microsoft Exchange Server und Exchange Server-Datenbanken ausführen. Wenn Sie den Agenten für Exchange so konfiguriert haben, wie es unter '"Postfach-Backup" (S. 623)' beschrieben ist, werden auch die Postfächer in diesem Verzeichnisbaum angezeigt.
2. Bestimmen Sie (per 'Durchsuchen') die Daten, die Sie sichern wollen.
   Erweitern Sie die Verzeichnisknoten oder klicken Sie rechts neben dem Verzeichnis doppelt auf einzelne Elemente in der Liste.
3. Wählen Sie Daten aus, die Sie sichern wollen.
   - Wenn Sie eine DAG auswählen, wird eine Kopie jeder geclusterten Datenbank gesichert. Weitere Informationen über die Sicherung von DAGs finden Sie im Abschnitt '"Datenbankverfügbarkeitsgruppen (DAG) sichern" (S. 618)'.
   - Wenn Sie eine Maschine auswählen, auf welcher ein Microsoft Exchange Server läuft, werden alle Datenbanken gesichert, die an diesen Exchange Server gemountet sind.
   - Wenn Sie die gewünschten Datenbanken direkt auswählen, werden dagegen nur diese Datenbanken gesichert.
   - Wenn Sie den Agenten für Exchange so konfiguriert haben, wie es unter '"Postfach-Backup" (S. 623)' beschrieben ist, können Sie auch Postfächer zur Sicherung auswählen.

   Wenn Ihre Auswahl mehrere Datenbanken umfasst, werden zwei auf einmal verarbeitet. Wenn das Backup der ersten Gruppe beendet ist, wird das Backup der nächsten Gruppe gestartet.
4. Geben Sie bei Aufforderung die Anmeldedaten an, die für den Datenzugriff notwendig sind.
5. Klicken Sie auf den Befehl **Schützen**.

AlwaysOn-Verfügbarkeitsgruppen (AAG) sichern

Hinweis
Diese Funktion ist über das Advanced Backup-Paket verfügbar.

SQL Server-Hochverfügbarkeitslösungen – ein Überblick

Die 'Windows Server Failover Clustering'-Funktionalität (WSFC) ermöglicht Ihnen, einen hochverfügbaren SQL Server durch Redundanz auf Instanzebene (Failover Cluster-Instanz, FCI) oder auf Datenbankebene (AlwaysOn-Verfügbarkeitsgruppe, AAG) zu konfigurieren. Sie können auch beide Methoden kombinieren.

In einer Failover Cluster-Instanz befinden sich die SQL-Datenbanken auf einem gemeinsam genutzten Storage. Auf diesen Storage kann nur vom aktiven Cluster-Knoten aus zugegriffen werden. Hat der aktive Knoten einen Fehler, dann kommt es zu einem Failover und ein anderer Knoten wird aktiv.

In einer Verfügbarkeitsgruppe liegt jedes Datenbankreplikat auf einem anderen Knoten. Ist das primäre Replikat nicht mehr verfügbar, dann wird einem zweiten Replikat, das auf einem anderen Knoten liegt, die primäre Rolle zugewiesen.

Auf diese Weise dienen die Cluster selbst bereits als eine Art von Disaster Recovery-Lösung. Es gibt jedoch Fälle, in denen die Cluster keine Data Protection bereitstellen können: Beispielsweise bei logischer Beschädigung einer Datenbank oder wenn der komplette Cluster ausgefallen ist. Cluster-Lösungen schützen außerdem nicht vor schädlichen Inhaltsänderungen, da diese üblicherweise sofort auf alle Cluster-Knoten repliziert werden.

Unterstützte Cluster-Konfigurationen

Die Backup-Software unterstützt *nur* die AlwaysOn-Verfügbarkeitsgruppen (AAG) für SQL Server 2012 oder höher. Andere Cluster-Konfigurationen wie Failover Cluster-Instanzen, Datenbankspiegelung und Protokollversand werden *nicht* unterstützt.

Wie viele Agenten sind für Backup und Recovery von Cluster-Daten erforderlich?

Um einen Cluster erfolgreich sichern und wiederherstellen zu können, muss der Agent für SQL auf jedem Knoten des WSFC-Clusters installiert sein.

Datenbanken in einer AAG per Backup sichern

1. Installieren Sie den Agenten für SQL auf jedem Knoten des WSFC-Clusters.
2. Wählen Sie die zu sichernde AAG aus wie im Abschnitt 'SQL-Datenbanken auswählen' beschrieben.

   Sie müssen die AAG selbst auswählen, um alle Datenbanken der AAG sichern zu können. Wenn Sie einen Satz von Datenbanken sichern wollen, müssen Sie diesen Datenbanksatz in allen Knoten der AAG definieren.

   Warnung!
   Der Datenbanksatz muss in allen Knoten exakt gleich sein. Wenn auch nur ein Satz unterschiedlich ist oder nicht auf allen Knoten definiert wurde, wird das Cluster-Backup nicht richtig funktionieren.
3. Konfigurieren Sie die Backup-Option 'Cluster-Backup-Modus'.

Datenbanken in einer AAG wiederherstellen

1. Wählen Sie zuerst die wiederherzustellenden Datenbanken und dann den Recovery-Punkt, von dem aus die Wiederherstellung der Datenbanken erfolgen soll.

Wenn Sie eine geclusterte Datenbank unter **Geräte** –> **Microsoft SQL** –> **Datenbanken** ausgewählt haben und anschließend auf **Recovery** klicken, zeigt die Software nur die Recovery-Punkte an, die mit den Zeitpunkten korrespondieren, wenn die ausgewählte Kopie der Datenbank gesichert wurde.

Die einfachste Möglichkeit, alle Recovery-Punkte einer geclusterten Datenbank einzusehen, besteht darin, das Backup der kompletten AAG in der Registerkarte 'Backup Storage' auszuwählen. Die Namen der AAG-Backups basieren auf folgender Vorlage: `<AAG-Name> - <Schutzplan-Name>` und haben ein spezielles Symbol.

2. Befolgen Sie zur Konfiguration der Wiederherstellung die im Abschnitt 'SQL-Datenbanken wiederherstellen' beschriebene Anleitung (beginnend mit Schritt 5).

   Die Software definiert automatisch einen Cluster-Knoten, wohin die Daten wiederhergestellt werden. Der Name des Knotens wird im Feld **Recovery zu** angezeigt. Sie können den Zielknoten manuell ändern.

Wichtig
Eine in einer AlwaysOn-Verfügbarkeitsgruppe (AAG) enthaltene Datenbank kann während einer Wiederherstellung nicht überschrieben werden, weil der Microsoft SQL Server dies verhindert. Sie müssen die Zieldatenbank daher von der AAG ausschließen, bevor Sie die Wiederherstellung durchführen. Oder Sie stellen die Datenbank einfach als 'Nicht-AGG'-Datenbank wieder her. Nach Abschluss der Wiederherstellung können Sie die ursprüngliche AAG-Konfiguration wieder aufbauen.

Datenbankverfügbarkeitsgruppen (DAG) sichern

Hinweis
Diese Funktion ist über das Advanced Backup-Paket verfügbar.

Exchange Server-Cluster – eine Übersicht

Der Leitgedanke von Exchange-Cluster ist, eine hohe Datenbankverfügbarkeit bereitzustellen – bei schneller Ausfallsicherung (Failover) und ohne Datenverlust. Üblicherweise wird dies erreicht, indem eine oder mehrere Kopien von Datenbanken oder Speichergruppen auf den Mitgliedern des Clusters (Cluster-Knoten) vorgehalten werden. Fällt der die aktive Datenbankkopie vorhaltende Cluster-Knoten oder die aktive Datenbankkopie selbst aus, dann springt der andere, die passive Kopie vorhaltende Knoten ein, übernimmt die Aktionen des fehlerhaften Knotens und ermöglicht so mit minimaler Ausfallszeit einen weiteren Zugriff auf die Exchange-Dienste. Auf diese Weise dienen die Cluster selbst bereits als eine Art von Disaster Recovery-Lösung.

Es gibt jedoch Fälle, in denen 'Failover Cluster'-Lösungen keinen Schutz für die Daten bereitstellen können: Beispielsweise bei logischer Beschädigung einer Datenbank, wenn eine bestimmte Datenbank in einem Cluster keine Kopie (Replikat) hat oder wenn der komplette Cluster ausgefallen ist. Cluster-Lösungen schützen außerdem nicht vor schädlichen Inhaltsänderungen, da diese üblicherweise sofort auf alle Cluster-Knoten repliziert werden.

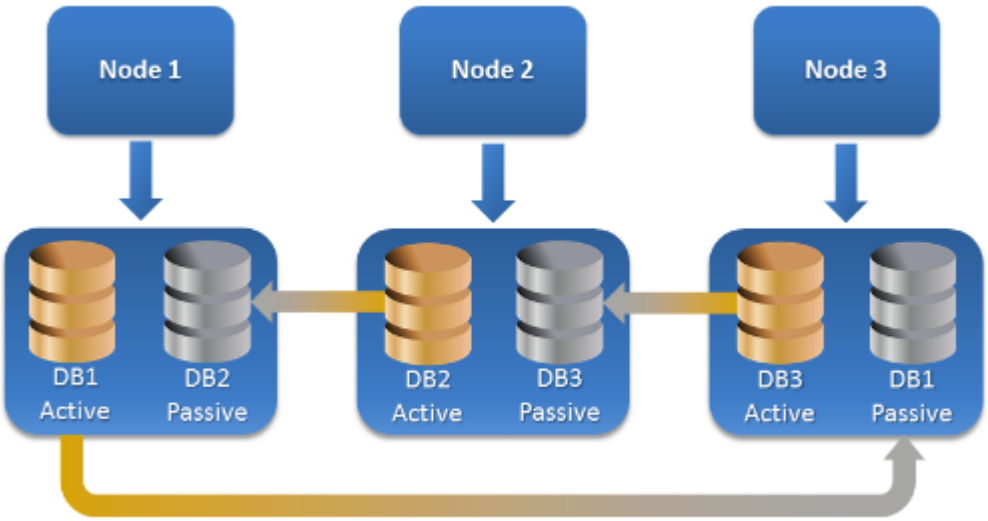
Cluster-konformes Backup

Bei einem Cluster-konformen Backup wird nur eine Kopie der geclusterten Daten gesichert. Wenn die Daten ihren Speicherort im Cluster ändern (aufgrund eines Switchovers oder Failovers), kann die Software alle Verlagerungen dieser Daten verfolgen und diese zuverlässig per Backup sichern.

Unterstützte Cluster-Konfigurationen

Cluster-konformes Backup wird *nur* für Datenbankverfügbarkeitsgruppen (DAG) in Exchange Server 2010 oder höher unterstützt. Andere Cluster-Konfigurationen – wie Einzelkopiencluster (Single Copy Cluster, SCC) und fortlaufende Cluster-Replikation (Cluster Continuous Replication, CCR) für Exchange Server 2007 – werden *nicht* unterstützt.

Eine DAG besteht aus einer Gruppe von bis zu 16 Exchange-Postfachservern. Jeder Knoten kann eine Kopie der Postfachdatenbank von jedem anderen Knoten hosten. Jeder Knoten kann passive und aktive Datenbankkopien hosten. Es können bis zu 16 Kopien von jeder Datenbank erstellt werden.



Wie viele Agenten sind für Cluster-konforme Backups und Wiederherstellungen erforderlich?

Um geclusterte Datenbanken erfolgreich sichern und wiederherstellen zu können, muss der Agent für Exchange auf jedem Knoten des Exchange-Clusters installiert sein.

Hinweis
Nachdem Sie den Agenten auf einem der Knoten installiert haben, zeigt die Cyber Protect-Konsole die DAG und deren Knoten unter **Geräte** –> **Microsoft Exchange** –> **Datenbanken** an. Um die Agenten für Exchange auf den restlichen Knoten zu installieren, müssen Sie die DAG auswählen, dann auf **Details** klicken und abschließend neben jedem Knoten auf **Agent installieren**.

Backup von Exchange-Cluster-Daten

1. Wählen Sie bei Erstellung eines Schutzplans die DAG so aus, wie es im Abschnitt '"Exchange Server-Daten auswählen" (S. 615)' beschrieben ist.
2. Konfigurieren Sie die Backup-Option '"Cluster-Backup-Modus" (S. 500)'.
3. Spezifizieren Sie bei Bedarf noch weitere Einstellungen des Schutzplans.

Wichtig
Stellen Sie bei einem Cluster-konformen Backup sicher, dass Sie die DAG selbst auswählen. Wenn Sie einzelne Knoten oder Datenbanken innerhalb der DAG auswählen, werden nur die ausgewählten Elemente gesichert und die Option **Cluster-Backup-Modus** ignoriert.

Exchange-Cluster-Daten wiederherstellen

1. Wählen Sie den Recovery-Punkt für die Datenbank aus, die Sie wiederherstellen wollen. Einen kompletten Cluster zur Wiederherstellung auszuwählen, ist jedoch nicht möglich.

   Wenn Sie die Kopie einer geclusterten Datenbank unter **Geräte** –> **Microsoft Exchange** –> **Datenbanken** –> `<Cluster-Name>` –> `<Knoten-Name>` auswählen und dann auf **Recovery** klicken, zeigt die Software nur solche Recovery-Punkte an, die mit den Zeitpunkten korrespondieren, wenn die Kopie dieser Datenbank gesichert wurde.

   Die einfachste Möglichkeit, alle Recovery-Punkte einer geclusterten Datenbank einzusehen, besteht darin, deren Backup in der Registerkarte 'Backup Storage' auszuwählen.
2. Befolgen Sie die im Abschnitt '"Exchange-Datenbanken wiederherstellen" (S. 634)' beschriebenen Aktionen (beginnend mit Schritt 5).

   Die Software definiert automatisch einen Cluster-Knoten, wohin die Daten wiederhergestellt werden. Der Name des Knotens wird im Feld **Recovery zu** angezeigt. Sie können den Zielknoten manuell ändern.

Applikationskonformes Backup

Applikationskonformes Backup auf Laufwerksebene ist für physische Maschinen, virtuelle ESXi-Maschinen und virtuelle Hyper-V-Maschinen verfügbar.

Wenn Sie eine Maschine sichern, auf der ein Microsoft SQL Server, Microsoft Exchange Server oder die Active Directory Domain Services (Active Directory-Domänendienste) ausgeführt werden, können Sie mit der Option **Applikations-Backup** einen zusätzlichen Schutz für die Daten dieser Applikationen aktivieren.

Wann ist ein applikationskonformes Backup sinnvoll?

Mit einem applikationskonformen Backup können Sie Folgendes sicherstellen:

- Die Applikationen werden in einem konsistenten Zustand gesichert und sind daher nach der Wiederherstellung der Maschine auch direkt verfügbar.
- Sie können SQL- und Exchange-Datenbanken, Exchange-Postfächer und Exchange-Postfachelemente wiederherstellen, ohne die komplette Maschine wiederherstellen zu müssen.
- Die SQL-Transaktionsprotokolle werden nach jedem erfolgreichen Backup abgeschnitten. Die SQL-Protokollabschneidung kann in den Schutzplan-Optionen deaktiviert werden. Die Exchange-Transaktionsprotokolle werden nur auf virtuellen Maschinen abgeschnitten. Sie können die Option 'VSS-Voll-Backup' aktivieren, falls Sie wollen, dass die Exchange-Transaktionsprotokolle auf einer physischen Maschine abgeschnitten werden.
- Falls eine Domain mehr als zwei Domain-Controller enthält und Sie einen davon wiederherstellen, wird eine 'nicht autorisierte' Wiederherstellung durchgeführt und so ein USN-Rollback nach der Wiederherstellung vermieden.

Was ist erforderlich, um applikationskonformes Backup verwenden zu können?

Auf einer physischen Maschine muss neben dem Agenten für Windows auch der Agent für SQL und/oder der Agent für Exchange installiert sein.

Auf einer virtuellen Maschine ist die Installation eines Agenten nicht erforderlich, weil die Maschine hier üblicherweise über den Agenten für VMware (Windows) oder den Agenten für Hyper-V gesichert wird.

Hinweis
Bei virtuellen Hyper-V- und VMware ESXi-Maschinen, auf denen der Windows Server 2022 ausgeführt wird, werden keine applikationskonformen Backups im agentenlosen Modus unterstützt (also wenn das Backup durch den Agenten für Hyper-V oder den Agenten für VMware durchgeführt wird). Wenn Sie Microsoft-Applikationen auf diesen Maschinen schützen wollen, müssen Sie den Agenten für Windows innerhalb des Gastbetriebssystems installieren.

Der Agent für VMware (Virtuelle Appliance) kann applikationskonforme Backups erstellen, aber keine Applikationsdaten aus diesen Backups wiederherstellen. Wenn Sie Applikationsdaten aus Backups wiederherstellen wollen, die von diesem Agenten erstellt wurden, benötigen Sie den Agenten für VMware (Windows), den Agenten für SQL oder den Agenten für Exchange auf einer Maschine, die auf den Speicherort zugreifen kann, wo die Backups vorliegen. Wenn Sie die Wiederherstellung von Applikationsdaten konfigurieren wollen, wählen Sie zuerst den gewünschten Recovery-Punkt auf der Registerkarte **Backup Storage** aus und dann bei **Von dieser Maschine aus durchsuchen** die entsprechende Maschine.

Weitere Anforderungen finden Sie in den Abschnitten 'Voraussetzungen' und 'Erforderliche Benutzerrechte'.

Hinweis
Applikationskonforme Backups von virtuellen Hyper-V-Maschinen können möglicherweise mit der Fehlermeldung „WMI 'ExecQuery' für die Abfrage ist fehlgeschlagen.“ oder „Es konnte kein neuer Prozess über WMI erstellt werden“ fehlschlagen, wenn die Backups auf einem Host mit hoher Auslastung durchgeführt werden, weil die Windows-Verwaltungsinstrumentation (WMI) nicht oder nur verzögert reagiert. Versuchen Sie diese Backups in einem Zeitfenster zu wiederholen, in dem der Host weniger ausgelastet ist.

Erforderliche Benutzerrechte für applikationskonforme Backups

Ein applikationskonformes Backup enthält die Metadaten von VSS-kompatiblen Applikationen, die auf dem Laufwerk vorliegen. Um auf diese Metadaten zugreifen zu können, benötigt der Agenten ein Konto mit passenden Berechtigungen, die nachfolgend aufgeführt sind. Wenn Sie ein applikationskonformes Backup aktivieren, werden Sie aufgefordert, ein solches Konto zu spezifizieren.

- Für SQL Server:
  Das Konto muss Mitglied der Gruppe **Backup-Operatoren** oder **Administratoren** auf der Maschine sein und Mitglied der Rolle **Sysadmin** auf jeder Instanz sein, die Sie per Backup sichern möchten.

  Hinweis
  Es wird nur die Windows-Authentifizierung unterstützt.

- Für Exchange Server:
  Exchange 2007: Das Konto muss auf der Maschine Mitglied in der Gruppe der **Administratoren** sein und zudem Mitglied in der Rollengruppe **Exchange-Organisationsadministratoren**.
  Exchange 2010 und höher: Das Konto muss auf der Maschine Mitglied in der Gruppe der **Administratoren** sein und zudem Mitglied in der Rollengruppe **Organisationsverwaltung**.
- Für Active Directory:
  Das Konto muss ein Domain-Administrator sein.

Zusätzliche Anforderungen für virtuelle Maschinen

Falls die Applikation auf einer virtuellen Maschine läuft, die vom Agenten für VMware oder dem Agenten für Hyper-V gesichert wird, müssen Sie sicherstellen, dass die Benutzerkontensteuerung (UAC) auf der Maschine deaktiviert ist.

Wenn Sie die Benutzerkontensteuerung (UAC) nicht ausschalten wollen, müssen Sie die Anmeldedaten des integrierten Domain-Administrators (DOMAIN\Administrator) bereitstellen, wenn Sie das Applikations-Backup aktivieren.

Hinweis
Verwenden Sie das integrierte Domain-Administrator-Konto, das beim Erstellen der Domain konfiguriert wurde. Später erstellte Konten werden nicht unterstützt.

Zusätzliche Anforderungen für Maschinen mit Windows

Um applikationskonforme Backups zu ermöglichen, müssen Sie bei allen Windows-Versionen die Richtlinien für die Benutzerkontensteuerung (UAC) deaktivieren.

Wenn Sie die Benutzerkontensteuerung (UAC) nicht ausschalten wollen, müssen Sie die Anmeldedaten des integrierten Domain-Administrators (DOMAIN\Administrator) bereitstellen, wenn Sie das Applikations-Backup aktivieren.

Hinweis
Verwenden Sie das integrierte Domain-Administrator-Konto, das beim Erstellen der Domain konfiguriert wurde. Später erstellte Konten werden nicht unterstützt.

So können Sie die UAC-Richtlinien in Windows deaktivieren

1. Suchen Sie im Registrierungs-Editor den folgenden Registrierungsschlüssel:
   `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System`
2. Ändern Sie den Wert für **EnableLUA** auf **0**.
3. Starten Sie die Maschine neu.

Postfach-Backup

Das Postfach-Backup wird für Microsoft Exchange Server 2010 Service Pack 1 (SP1) oder höher unterstützt.

Die Möglichkeit zur Sicherung von Postfächern ist dann verfügbar, wenn auf dem Management Server mindestens ein Agent für Exchange registriert ist. Die Agent muss auf einer Maschine installiert sein, die zu derselben Active Directory-Gesamtstruktur (Forest) gehört wie der Microsoft Exchange Server.

Bevor Sie Postfächer sichern können, müssen Sie den Agenten für Exchange mit der Maschine verbinden, auf welcher die Server-Rolle **Clientzugriff** (CAS) des Microsoft Exchange Servers ausgeführt wird. In Exchange 2016 oder höher ist die CAS-Rolle nicht als separate Installationsoption verfügbar. Es wird automatisch als Teil der Postfachserverrolle installiert. Auf diese Weise können Sie den Agenten mit jedem Server verbinden, auf dem die **Postfachrolle** ausgeführt wird.

Hinweis
Sie können Postfächer und Postfach-Elemente auch aus Datenbank-Backups und applikationskonformen Backups wiederherstellen. Weitere Informationen finden Sie im Abschnitt '"Exchange-Postfächer und Postfachelemente wiederherstellen" (S. 637)'. Bei Datenbank-Backups und applikationskonformen Backups können Sie keine Schutzpläne für einzelne Postfächer erstellen.

So verbinden Sie den Agenten mit der Clientzugriffsrolle

1. Klicken Sie auf **Geräte** –> **Hinzufügen**.
2. Klicken Sie auf **Microsoft Exchange Server**.
3. Klicken Sie auf **Exchange-Postfächer**.
   Wenn auf dem Management Server kein Agent für Exchange registriert ist, wird Ihnen die Software vorschlagen, dass Sie den Agenten installieren sollen. Wiederholen Sie nach der Installation diese Prozedur ab Schritt 1.
4. [Optional] Sollten auf dem Management Server mehrere Agenten für Exchange registriert sein, dann klicken Sie auf **Agent** und ändern Sie den Agenten, der das Backup durchführen soll.
5. Spezifizieren Sie bei **Clientzugriffsserver (CAS)** den vollqualifizierten Domain-Namen (FQDN) derjenigen Maschine, auf welcher die Rolle '**Clientzugriff**' des Microsoft Exchange Servers aktiviert ist.
   In Exchange 2016 oder höher werden die Clientzugriffsdienste automatisch als Teil der Postfachserverrolle installiert. Auf diese Weise können Sie jeden Server spezifizieren, auf dem die **Postfachrolle** ausgeführt wird. Wir werden diesen Server später in diesem Abschnitt einfach als „CAS“ bezeichnen.
6. Bestimmen Sie bei **Authentifizierungstyp** den Authentifizierungstyp, der für die Clientzugriffsrolle verwendet werden soll. Sie können **Kerberos** (Standard) oder **Basis** auswählen.
7. [Nur bei Basisauthentifizierung] Bestimmen Sie, welches Protokoll verwendet werden soll. Sie können **HTTPS** (Standard) oder **HTTP** auswählen.
8. [Nur bei Basisauthentifizierung mit HTTPS-Protokoll] Falls die Clientzugriffsrolle ein SSL-Zertifikat verwendet, welches von einer offiziellen Zertifizierungsstelle ausgestellt wurde, und Sie wollen, dass die Software das Zertifikat bei Verbindung mit der Clientzugriffsrolle (CAS) überprüft, dann aktivieren Sie das Kontrollkästchen **SSL-Zertifikat überprüfen**. Ansonsten können Sie diesen Schritt überspringen.
9. Geben Sie die Anmeldedaten eines Kontos ein, welches für den Zugriff auf die Clientzugriffsrolle verwendet werden soll. Die Anforderungen für dieses Konto sind im Abschnitt 'Erforderliche Benutzerrechte' aufgeführt.
10. Klicken Sie auf **Hinzufügen**.

Als Ergebnis erscheinen die Postfächer anschließend unter **Geräte** –> **Microsoft Exchange** –> **Postfächer**.

Exchange Server-Postfächer auswählen

Wählen Sie die Postfächer wie nachfolgend beschrieben aus – und spezifizieren Sie dann die anderen Einstellungen des Schutzplans nach Bedarf.

So können Sie Exchange-Postfächer auswählen

1. Klicken Sie auf **Geräte** –> **Microsoft Exchange**.
   Die Software zeigt den Verzeichnisbaum der Exchange-Datenbanken und -Postfächer.
2. Klicken Sie auf **Postfächer** und wählen Sie die Postfächer, die Sie per Backup sichern wollen.
3. Klicken Sie auf den Befehl **Schützen**.

Erforderliche Benutzerrechte

Um auf Postfächer zugreifen zu können, benötigt der Agent für Exchange ein Konto mit passenden Berechtigungen. Sie werden aufgefordert, dieses Konto zu spezifizieren, wenn Sie Aktionen mit Postfächern konfigurieren.

Die Mitgliedschaft des Kontos in der Rollengruppe **Organisationsverwaltung** ermöglicht den Zugriff auf alle Postfächer (auch solche, die in Zukunft erstellt werden).

Die mindestens erforderlichen Benutzerrechte sind:

- Das Konto muss Mitglied in den Rollengruppen **Serververwaltung** und **Empfängerverwaltung** sein.
- Das Konto muss die Verwaltungsrolle **ApplicationImpersonation** für alle Benutzer oder Benutzergruppen aktiviert haben, auf deren Postfächer der Agent zugreifen wird.
  Genauere Informationen zur Konfiguration der Verwaltungsrolle **ApplicationImpersonation** finden Sie im folgenden Microsoft Knowledge Base-Artikel: https://msdn.microsoft.com/de-de/library/office/dn722376.aspx.

SQL-Datenbanken wiederherstellen

Sie können SQL-Datenbanken aus Datenbank-Backups und applikationskonformen Backups wiederherstellen. Weitere Informationen über den Unterschied zwischen den beiden Backup-Arten finden Sie im Abschnitt '"Microsoft SQL Server und Microsoft Exchange Server sichern" (S. 610)'.

Sie können SQL-Datenbanken zur ursprünglichen Instanz, zu einer anderen Instanz auf der ursprünglichen Maschine oder zu einer Instanz auf einer nicht ursprünglichen Maschine wiederherstellen. Wenn Sie eine Wiederherstellung zu einer nicht ursprünglichen Maschine durchführen, muss der Agent für SQL auf der Zielmaschine installiert sein.

Sie können Datenbanken außerdem auch als Dateien wiederherstellen.

Wenn Sie die Windows-Authentifizierung für die SQL-Instanz verwenden, müssen Sie außerdem die Anmeldedaten für ein Konto angeben, welches auf der Maschine ein Mitglied der Gruppe **Sicherungs-Operatoren** oder der Gruppe **Administratoren** ist und zudem auf der Zielinstanz ein

Mitglied der **SysAdmin**-Rolle ist. Wenn Sie die SQL Server-Authentifizierung verwenden, müssen Sie die Anmeldedaten für ein Konto angeben, das auf der Zielinstanz ein Mitglied der **SysAdmin**-Rolle ist.

Systemdatenbanken werden wie Benutzerdatenbanken wiederhergestellt, jedoch mit einigen Unterschieden. Weitere Informationen über diese Unterschiede finden Sie im Abschnitt '"Systemdatenbanken wiederherstellen" (S. 633)'.

Während einer Wiederherstellung können Sie den Fortschritt der Aktion in der Cyber Protect-Konsole auf der Registerkarte **Monitoring** –> **Aktivitäten** überprüfen.

SQL-Datenbanken zur ursprünglichen Maschine wiederherstellen

Sie können SQL-Datenbanken zu ihrer ursprünglichen Instanz, zu einer anderen Instanz auf der ursprünglichen Maschine oder zu einer Instanz auf einer nicht ursprünglichen Zielmaschine wiederherstellen.

So können Sie SQL-Datenbanken zur ursprünglichen Maschine wiederherstellen

Von einem Datenbank-Backup

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte** –> **Microsoft SQL**.
2. Wählen Sie die SQL Server-Instanz oder klicken Sie auf den Instanznamen, um bestimmte Datenbanken auszuwählen, die Sie wiederherstellen wollen, und klicken Sie anschließend auf **Recovery**.
   Falls die Maschine offline ist, werden keine Recovery-Punkte angezeigt. Informationen über die Wiederherstellung von Daten zu einer nicht ursprünglichen Maschine finden Sie im Abschnitt '"SQL-Datenbanken zu einer nicht ursprünglichen Maschine wiederherstellen" (S. 628)'.
3. Wählen Sie einen Recovery-Punkt.
   Die Recovery-Punkte werden nach Speicherorten gefiltert.
4. Klicken Sie auf **Recovery** –> **Datenbanken zu einer Instanz**.
   Die Instanz und die Datenbanken werden standardmäßig zu ihren ursprünglichen Quellen wiederhergestellt. Sie können eine ursprüngliche Datenbank auch als neue Datenbank wiederherstellen.
5. [Wenn Sie eine Wiederherstellung zu einer nicht ursprünglichen Instanz auf derselben Maschine durchführen] Klicken Sie auf **SQL Server-Zielinstanz**, wählen Sie die gewünschte Zielinstanz aus und klicken Sie anschließend auf **Fertig**.
6. [Wenn Sie eine Datenbank als neue Datenbank wiederherstellen] Klicken Sie auf den Datenbanknamen und wählen Sie anschließend unter **Recovery zu** die Option **Neue Datenbank**.
   - Spezifizieren Sie den Namen für die neue Datenbank.
   - Spezifizieren Sie den neuen Datenbankpfad.
   - Spezifizieren Sie den Protokollpfad.

7. [Optional] [Nicht verfügbar, wenn Sie eine Datenbank als neue Datenbank wiederherstellen] Wenn Sie das Datenbankstadium nach der Wiederherstellung ändern wollen, müssen Sie auf den Datenbanknamen klicken, eines der folgenden Stadien auswählen und anschließend auf **Fertig** klicken.
   - **Einsatzbereit (Mit RECOVERY wiederherstellen)** (Standardeinstellung)
     Die Datenbank ist nach Abschluss der Wiederherstellung direkt einsatzbereit. Benutzer haben vollen Zugriff auf sie. Die Software wird für alle Transaktionen der wiederhergestellten Datenbank ein Rollback ausführen, für die kein 'Commit' ausgeführt wurde und die in den Transaktionsprotokollen gespeichert sind. Sie können keine zusätzlichen Transaktionsprotokolle von systemeigenen Microsoft SQL-Backups wiederherstellen.
   - **Nicht betriebsbereit (Mit NORECOVERY wiederherstellen)**
     Die Datenbank ist nach Abschluss der Wiederherstellung nicht betriebsbereit. Benutzer haben keinen Zugriff auf sie. Die Software behält alle nicht übernommenen Transaktionen (ohne 'Commit') der wiederhergestellten Datenbank. Sie können zusätzliche Transaktionsprotokolle von systemeigenen Microsoft SQL-Backups wiederherstellen und auf diese Weise den notwendigen Recovery-Punkt erreichen.
   - **Schreibgeschützt (Mit STANDBY wiederherstellen)**
     Benutzer haben nach Abschluss der Wiederherstellung einen Nur-Lesen-Zugriff auf die Datenbank. Die Software wird alle nicht übernommenen Transaktionen (ohne 'Commit') rückgängig machen. Die Rückgängigaktionen werden jedoch in einer temporären Standby-Datei gespeichert, sodass die Recovery-Effekte zurückgestellt werden werden können.
     Dieser Wert wird primär verwendet, um den Zeitpunkt eines SQL Server-Fehlers zu ermitteln.
8. Klicken Sie auf **Recovery starten**.

Von einem applikationskonformen Backup

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte** –> **Alle Geräte**.
2. Wählen Sie diejenige Maschine aus, in dem sich die wiederherzustellenden Daten ursprünglich befunden haben, und klicken Sie dann auf **Recovery**.
   Falls die Maschine offline ist, werden keine Recovery-Punkte angezeigt. Informationen über die Wiederherstellung von Daten zu einer nicht ursprünglichen Maschine finden Sie im Abschnitt '"SQL-Datenbanken zu einer nicht ursprünglichen Maschine wiederherstellen" (S. 628)'.
3. Wählen Sie einen Recovery-Punkt.
   Die Recovery-Punkte werden nach Speicherorten gefiltert.
4. Klicken Sie auf **Recovery** –> **SQL-Datenbanken**.
5. Wählen Sie die SQL Server-Instanz oder klicken Sie auf den Instanznamen, um bestimmte Datenbanken auszuwählen, die Sie wiederherstellen wollen, und klicken Sie anschließend auf **Recovery**.
   Die Instanz und die Datenbanken werden standardmäßig zu ihren ursprünglichen Quellen wiederhergestellt. Sie können eine ursprüngliche Datenbank auch als neue Datenbank wiederherstellen.

6. [Wenn Sie eine Wiederherstellung zu einer nicht ursprünglichen Instanz auf derselben Maschine durchführen] Klicken Sie auf **SQL Server-Zielinstanz**, wählen Sie die gewünschte Zielinstanz aus und klicken Sie anschließend auf **Fertig**.
7. [Wenn Sie eine Datenbank als neue Datenbank wiederherstellen] Klicken Sie auf den Datenbanknamen und wählen Sie anschließend unter **Recovery zu** die Option **Neue Datenbank**.
   - Spezifizieren Sie den Namen für die neue Datenbank.
   - Spezifizieren Sie den neuen Datenbankpfad.
   - Spezifizieren Sie den Protokollpfad.
8. [Optional] [Nicht verfügbar, wenn Sie eine Datenbank als neue Datenbank wiederherstellen] Wenn Sie das Datenbankstadium nach der Wiederherstellung ändern wollen, müssen Sie auf den Datenbanknamen klicken, eines der folgenden Stadien auswählen und anschließend auf **Fertig** klicken.
   - **Einsatzbereit (Mit RECOVERY wiederherstellen)** (Standardeinstellung)

     Die Datenbank ist nach Abschluss der Wiederherstellung direkt einsatzbereit. Benutzer haben vollen Zugriff auf sie. Die Software wird für alle Transaktionen der wiederhergestellten Datenbank ein Rollback ausführen, für die kein 'Commit' ausgeführt wurde und die in den Transaktionsprotokollen gespeichert sind. Sie können keine zusätzlichen Transaktionsprotokolle von systemeigenen Microsoft SQL-Backups wiederherstellen.
   - **Nicht betriebsbereit (Mit NORECOVERY wiederherstellen)**

     Die Datenbank ist nach Abschluss der Wiederherstellung nicht betriebsbereit. Benutzer haben keinen Zugriff auf sie. Die Software behält alle nicht übernommenen Transaktionen (ohne 'Commit') der wiederhergestellten Datenbank. Sie können zusätzliche Transaktionsprotokolle von systemeigenen Microsoft SQL-Backups wiederherstellen und auf diese Weise den notwendigen Recovery-Punkt erreichen.
   - **Schreibgeschützt (Mit STANDBY wiederherstellen)**

     Benutzer haben nach Abschluss der Wiederherstellung einen Nur-Lesen-Zugriff auf die Datenbank. Die Software wird alle nicht übernommenen Transaktionen (ohne 'Commit') rückgängig machen. Die Rückgängigaktionen werden jedoch in einer temporären Standby-Datei gespeichert, sodass die Recovery-Effekte zurückgestellt werden werden können.

     Dieser Wert wird primär verwendet, um den Zeitpunkt eines SQL Server-Fehlers zu ermitteln.
9. Klicken Sie auf **Recovery starten**.

SQL-Datenbanken zu einer nicht ursprünglichen Maschine wiederherstellen

Sie können sowohl applikationskonforme Backups als auch Datenbank-Backups zu SQL Server-Instanzen auf nicht ursprünglichen Zielmaschinen wiederherstellen, auf denen der Agent für SQL installiert ist. Die Backups müssen sich auf dem Cloud Storage oder auf einem freigegebenen Storage befinden, auf den die Zielmaschine Zugriff hat.

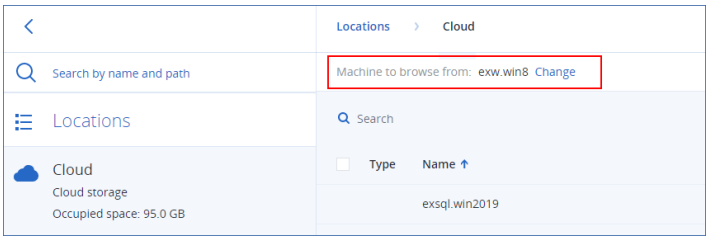
Die SQL Server-Version auf der Zielmaschine muss der Version auf der Quellmaschine entsprechen oder neuer sein.

So können Sie SQL-Datenbanken zu einer nicht ursprünglichen Maschine wiederherstellen

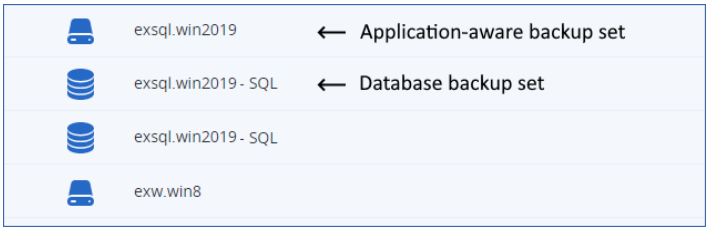
Aus dem Backup Storage

Diese Prozedur gilt für applikationskonforme Backups und Datenbank-Backups.

1. Gehen Sie in der Cyber Protect-Konsole zu **Backup Storage**.
2. Wählen Sie den Speicherort desjenigen Backups aus, aus dem Sie Daten wiederherstellen wollen.
3. Wählen Sie bei **Von dieser Maschine aus durchsuchen** die Zielmaschine aus.
   Dies ist diejenige Maschine, zu der Sie Ihre Daten wiederherstellen werden. Die Zielmaschine muss online sein.



4. Wählen Sie das gewünschte Backup-Set im Fensterbereich **Aktionen** aus und klicken Sie anschließend auf **Backups anzeigen**.
   Applikationskonforme Backup-Sätze und Datenbank-Backup-Sätze haben unterschiedliche Symbole.



5. Wählen Sie den Recovery-Punkt aus, aus dem die Daten wiederhergestellt werden sollen.
6. [Für Datenbank-Backups] Klicken Sie auf **SQL-Datenbanken wiederherstellen**.
7. [Für applikationskonforme Backups] Klicken Sie auf **Recovery** –> **SQL-Datenbanken**.
8. Wählen Sie die SQL Server-Instanz oder klicken Sie auf den Instanznamen, um bestimmte Datenbanken auszuwählen, die Sie wiederherstellen wollen, und klicken Sie anschließend auf **Recovery**.
9. [Wenn es mehr als eine SQL-Instanz auf der Zielmaschine gibt] Klicken Sie auf **SQL Server-Zielinstanz**, wählen Sie die gewünschte Zielinstanz aus und klicken Sie anschließend auf **Fertig**.
10. Klicken Sie auf den Datenbanknamen, spezifizieren Sie den neuen Datenbankpfad sowie den Protokollpfad und klicken Sie dann auf **Fertig**.
    Sie können in beiden Feldern denselben Pfad spezifizieren. Beispiel:

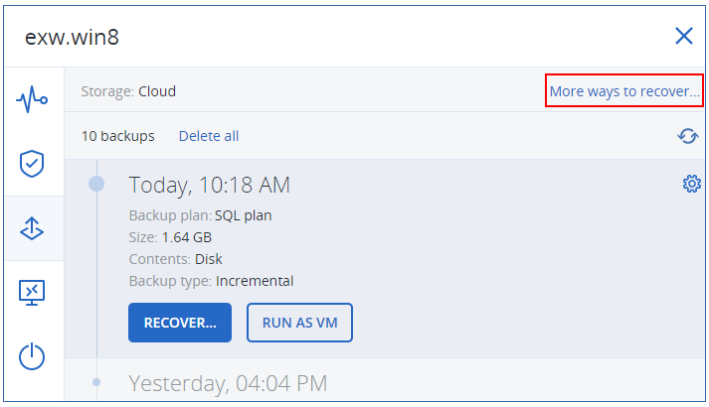
```
C:\Program Files\Microsoft SQL Server\MSSQL16.MSSQLSERVER\MSSQL\DATA\
```

11. Klicken Sie auf **Recovery starten**.

Von Geräten

Diese Prozedur gilt nur für applikationskonforme Backups.

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte** –> **Alle Geräte**.
2. Wählen Sie diejenige Maschine aus, in dem sich die wiederherzustellenden Daten ursprünglich befunden haben, und klicken Sie dann auf **Recovery**.
3. [Wenn die Quellmaschine online ist] Klicken Sie auf **Weitere Wiederherstellungsmöglichkeiten**.



4. Klicken Sie zuerst auf **Maschine auswählen**, um die Zielmaschine festzulegen, und dann auf **OK**. Dies ist diejenige Maschine, zu der Sie Ihre Daten wiederherstellen werden. Die Zielmaschine muss online sein.
5. Wählen Sie einen Recovery-Punkt.
   Die Recovery-Punkte werden nach Speicherorten gefiltert.
6. Klicken Sie auf **Recovery** –> **SQL-Datenbanken**.
7. Wählen Sie die SQL Server-Instanz oder klicken Sie auf den Instanznamen, um bestimmte Datenbanken auszuwählen, die Sie wiederherstellen wollen, und klicken Sie anschließend auf **Recovery**.
8. [Wenn es mehr als eine SQL-Instanz auf der Zielmaschine gibt] Klicken Sie auf **SQL Server-Zielinstanz**, wählen Sie die gewünschte Zielinstanz aus und klicken Sie anschließend auf **Fertig**.
9. Klicken Sie auf den Datenbanknamen, spezifizieren Sie den neuen Datenbankpfad sowie den Protokollpfad und klicken Sie dann auf **Fertig**.
   Sie können in beiden Feldern denselben Pfad spezifizieren. Beispiel:

   ```
   C:\Program Files\Microsoft SQL Server\MSSQL16.MSSQLSERVER\MSSQL\DATA\
   ```

10. Klicken Sie auf **Recovery starten**.

SQL-Datenbanken als Dateien wiederherstellen

Sie können Datenbanken als Dateien wiederherstellen. Diese Option kann nützlich sein, falls Sie Daten zur Überwachung oder weiteren Verarbeitung durch Drittthersteller-Tools extrahieren müssen. Informationen darüber, wie Sie die SQL-Datenbankdateien an eine SQL Server-Instanz anfügen können, finden Sie im Abschnitt '"SQL Server-Datenbanken anfügen" (S. 634)'.

Sie können Datenbanken als Dateien auf der ursprünglichen Maschine oder einer anderen als der ursprünglichen Zielmaschine wiederherstellen, auf denen jeweils der Agent für SQL installiert ist. Wenn Sie Daten zu Maschinen wiederherstellen wollen, die nicht die ursprünglichen sind, müssen sich die Backups auf dem Cloud Storage oder auf einem freigegebenen Storage befinden, auf den die Zielmaschine jeweils Zugriff hat.

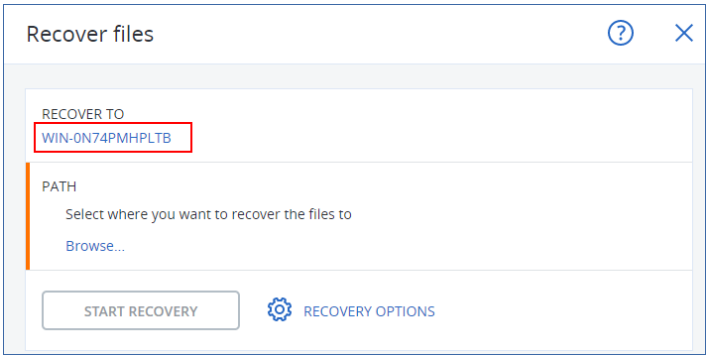
Hinweis
Wenn Sie den Agenten für VMware (Windows) verwenden, ist 'Datenbanken als Dateien wiederherstellen' die einzig verfügbare Recovery-Methode. Eine Wiederherstellung von Datenbanken über den Agenten für VMware (Virtual Appliance) ist nicht möglich.

So können Sie SQL-Datenbanken als Dateien wiederherstellen

Von einem Datenbank-Backup

Diese Prozedur gilt für Quellmaschinen, die online sind.

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte** –> **Microsoft SQL**.
2. Wählen Sie die wiederherzustellenden Datenbanken aus und klicken Sie dann auf **Recovery**.
3. Wählen Sie einen Recovery-Punkt.
   Die Recovery-Punkte werden nach Speicherorten gefiltert.
4. Klicken Sie auf **Recovery** –> **Datenbanken als Dateien**.
5. [Bei Wiederherstellung zu einer nicht ursprünglichen Maschine] Wählen Sie unter **Recovery zu** die gewünschte Zielmaschine.
   Dies ist diejenige Maschine, zu der Sie Ihre Daten wiederherstellen werden. Die Zielmaschine muss online sein.
   Wenn Sie die Auswahl ändern wollen, klicken Sie zuerst auf den Namen der Maschine, wählen Sie dann eine andere Maschine aus und klicken Sie anschließend auf **OK**.



6. Klicken Sie bei **Pfad** auf **Durchsuchen**, wählen Sie einen lokalen oder einen Netzwerk-Ordner aus, in dem Sie die Dateien speichern wollen, und klicken Sie anschließend auf **Fertig**.
7. Klicken Sie auf **Recovery starten**.

Von einem applikationskonformen Backup

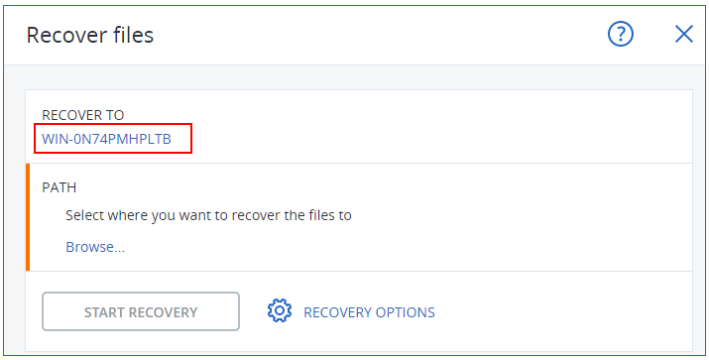
Diese Prozedur gilt für Quellmaschinen, die online sind.

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte** –> **Alle Geräte**.
2. Wählen Sie diejenige Maschine aus, in dem sich die wiederherzustellenden Daten ursprünglich befunden haben, und klicken Sie dann auf **Recovery**.
3. Wählen Sie einen Recovery-Punkt.

   Die Recovery-Punkte werden nach Speicherorten gefiltert.
4. Klicken Sie auf **Recovery** –> **SQL-Datenbanken**, wählen Sie die wiederherzustellenden Datenbanken aus, und klicken Sie anschließend auf **Als Dateien wiederherstellen**.
5. [Bei Wiederherstellung zu einer nicht ursprünglichen Maschine] Wählen Sie unter **Recovery zu** die gewünschte Zielmaschine.

   Dies ist diejenige Maschine, zu der Sie Ihre Daten wiederherstellen werden. Die Zielmaschine muss online sein.

   Wenn Sie die Auswahl ändern wollen, klicken Sie zuerst auf den Namen der Maschine, wählen Sie dann eine andere Maschine aus und klicken Sie anschließend auf **OK**.



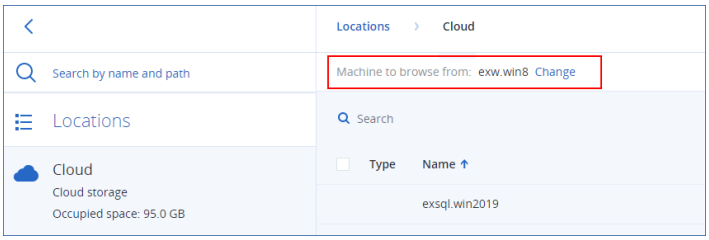
6. Klicken Sie bei **Pfad** auf **Durchsuchen**, wählen Sie einen lokalen oder einen Netzwerk-Ordner aus, in dem Sie die Dateien speichern wollen, und klicken Sie anschließend auf **Fertig**.
7. Klicken Sie auf **Recovery starten**.

Aus einem Backup auf einer Offline-Maschine

Diese Prozedur gilt für applikationskonforme Backups und Datenbank-Backups auf Quellmaschinen, die offline sind.

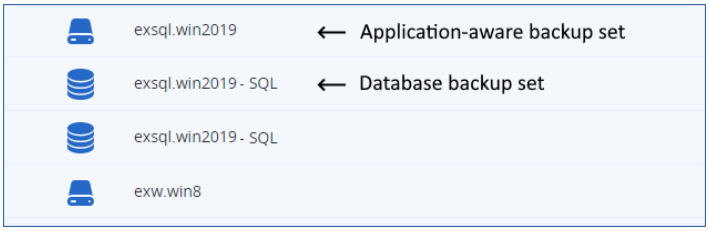
1. Gehen Sie in der Cyber Protect-Konsole zu **Backup Storage**.
2. Wählen Sie den Speicherort desjenigen Backups aus, aus dem Sie Daten wiederherstellen wollen.
3. Wählen Sie bei **Von dieser Maschine aus durchsuchen** die Zielmaschine aus.

   Dies ist diejenige Maschine, zu der Sie Ihre Daten wiederherstellen werden. Die Zielmaschine muss online sein.



4. Wählen Sie das gewünschte Backup-Set im Fensterbereich **Aktionen** aus und klicken Sie anschließend auf **Backups anzeigen**.

   Applikationskonforme Backup-Sätze und Datenbank-Backup-Sätze haben unterschiedliche Symbole.



5. Wählen Sie den Recovery-Punkt aus, aus dem die Daten wiederhergestellt werden sollen.
6. [Für Datenbank-Backups] Klicken Sie auf **SQL-Datenbanken wiederherstellen**.
7. [Für applikationskonforme Backups] Klicken Sie auf **Recovery** –> **SQL-Datenbanken**.
8. Wählen Sie die SQL Server-Instanz oder klicken Sie auf den Instanznamen, um bestimmte Datenbanken auszuwählen, die Sie wiederherstellen wollen, und klicken Sie anschließend auf **Als Dateien wiederherstellen**.
9. Klicken Sie bei **Pfad** auf **Durchsuchen**, wählen Sie einen lokalen oder einen Netzwerk-Ordner aus, in dem Sie die Dateien speichern wollen, und klicken Sie anschließend auf **Fertig**.
10. Klicken Sie auf **Recovery starten**.

Systemdatenbanken wiederherstellen

Alle Systemdatenbanken einer Instanz werden gleichzeitig wiederhergestellt. Bei der Wiederherstellung von Systemdatenbanken führt die Software einen automatischen Neustart der Zielinstanz im Einzelbenutzermodus aus. Nach Abschluss der Wiederherstellung startet die Software die Instanz neu und stellt andere Datenbanken (sofern vorhanden) wieder her.

Weitere Punkte, die bei der Wiederherstellung von Systemdatenbanken beachtet werden sollten:

- Systemdatenbanken können nur zu einer Instanz wiederhergestellt werden, die dieselbe Version wie die ursprüngliche Instanz hat.
- Systemdatenbanken können nur im Stadium 'Einsatzbereit' (ready to use) wiederhergestellt werden.

Die master-Datenbank wiederherstellen

Zu den Systemdatenbanken gehört auch die sogenannte **master**-Datenbank. Die **master**-Datenbank erfasst allgemeine Informationen über alle Datenbanken einer Instanz. Die **master**-Datenbank in einem Backup enthält daher genau die Informationen über die Datenbanken, die zum Zeitpunkt des Backups in der Instanz vorlagen. Nach der Wiederherstellung der **master**-Datenbank müssen Sie möglicherweise Folgendes tun:

- Datenbanken, die in der Instanz aufgetaucht sind, nachdem das Backup erstellt wurde, sind für die Instanz nicht sichtbar. Um diese Datenbanken zurück in die Produktion zu bringen, müssen Sie diese manuell mithilfe des Microsoft SQL Server Management Studios an die Instanz

anschließen.

- Datenbanken, die nach Erstellung des Backups gelöscht wurden, werden in der Instanz als offline angezeigt. Löschen Sie diese Datenbanken mithilfe des SQL Server Management Studios.

SQL Server-Datenbanken anfügen

Dieser Abschnitt beschreibt, wie Sie eine Datenbank im SQL Server mithilfe des SQL Server Management Studios anfügen können. Es kann immer nur eine Datenbank gleichzeitig angefügt werden.

Das Anfügen einer Datenbank erfordert eine der folgenden Berechtigungen: **Datenbank erstellen**, **Beliebige Datenbank erstellen** oder **Beliebige Datenbank ändern**. Normalerweise verfügt auf der Instanz die Rolle **SysAdmin** über diese Berechtigungen.

So fügen Sie eine Datenbank an

1. Führen Sie Microsoft SQL Server Management Studio aus.
2. Verbinden Sie sich mit der benötigten SQL Server-Instanz und erweitern Sie dann die Instanz.
3. Klicken Sie mit der rechten Maustaste auf **Datenbanken** und klicken Sie dann auf **Anfügen**.
4. Klicken Sie auf **Hinzufügen**.
5. Lokalisieren und Wählen Sie im Dialogfenster **Datenbankdateien suchen** die .mdf-Datei der Datenbank.
6. Stellen Sie im Bereich **Datenbankdetails** sicher, dass die restlichen Datenbankdateien (.ndf- und .ldf-Dateien) gefunden werden.

   Details: SQL Server-Datenbankdateien werden möglicherweise nicht automatisch gefunden, falls:

   - Sie sich nicht am Standardspeicherort befinden – oder sie nicht im selben Ordner wie die primäre Datenbankdatei (.mdf) sind. Lösung: Spezifizieren Sie den Pfad zu den benötigten Dateien manuell in der Spalte **Aktueller Dateipfad**.
   - Sie haben einen unvollständigen Satz an Dateien wiederhergestellt, der die Datenbank bildet. Lösung: Stellen Sie die fehlenden SQL Server-Datenbankdateien aus dem Backup wieder her.
7. Klicken Sie, wenn alle Dateien gefunden sind, auf **OK**.

Exchange-Datenbanken wiederherstellen

Dieser Abschnitt beschreibt die Wiederherstellung von Datenbank-Backups und applikationskonformen Backups.

Sie können Exchange Server-Daten zu einem aktiv laufenden Exchange Server wiederherstellen. Dies kann der ursprüngliche Exchange Server sein – oder ein Exchange Server mit derselben Version, der auf einer Maschine mit demselben vollqualifizierten Domain-Namen (FQDN) läuft. Der Agent für Exchange muss auf der Zielmaschine installiert sein.

Die nachfolgende Tabelle gibt Ihnen einen Überblick über die Exchange Server-Daten, die Sie für eine Wiederherstellung verwenden können – und die (mindestens benötigten) Benutzerrechte, die zur Wiederherstellung dieser Daten erforderlich sind.

Exchange-Version	Datenelemente	Benutzerrechte
2007	Speichergruppen	Mitglied in der Rollengruppe **Exchange-Organisationsadministratoren**.
2010/2013/2016/2019	Datenbanken	Mitglied in der Rollengruppe **Serververwaltung**.

Sie können die Datenbanken (Speichergruppen) alternativ auch als Dateien wiederherstellen. Die Datenbankdateien werden (zusammen mit den Transaktionsprotokolldateien) aus dem Backup in einem von Ihnen spezifizierten Ordner extrahiert. Das kann nützlich sein, falls Sie Daten für eine Überwachung oder zur weiteren Verarbeitung durch Tools von Drittherstellern extrahieren müssen – oder wenn eine Wiederherstellung aus irgendeinem Grund fehlschlägt und Sie nach einem Workaround suchen, die Datenbanken manuell zu mounten.

Falls Sie lediglich den Agenten für VMware (Windows) verwenden, ist nur eine Recovery-Methode verfügbar, nämlich Datenbanken als Dateien wiederherzustellen. Eine Wiederherstellung von Datenbanken über den Agenten für VMware (Virtual Appliance) ist nicht möglich.

Wir werden bei den unteren Prozeduren die Datenbanken und Speichergruppen einheitlich nur als 'Datenbanken' bezeichnen.

So können Sie Exchange-Datenbanken zu einem aktiv laufenden Exchange Server wiederherstellen

1. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Wenn Sie eine Wiederherstellung aus einem applikationskonformen Backup durchführen, wählen Sie unter **Geräte** diejenige Maschine aus, auf der sich die wiederherzustellenden Daten ursprünglich befunden haben.
   - Wenn Sie eine Wiederherstellung aus einem Datenbank-Backup durchführen, klicken Sie auf **Geräte** –> **Microsoft Exchange** –> **Datenbanken** – und wählen Sie dann die Datenbanken, die Sie wiederherstellen wollen.
2. Klicken Sie auf **Recovery**.
3. Wählen Sie einen Recovery-Punkt. Beachten Sie dabei, dass Recovery-Punkte nach Speicherorten gefiltert werden.

   Falls die Maschine offline ist, werden keine Recovery-Punkte angezeigt. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - [Nur bei Wiederherstellung aus einem applikationskonformen Backup] Sollte sich das Backup im Cloud Storage oder einem freigegebenen Storage befinden (d.h., dass andere Agenten auf diesen zugreifen können), dann klicken Sie zuerst auf den Befehl **Maschine auswählen**. Wählen Sie anschließend eine Maschine aus, die online ist und auf welcher der Agent für Exchange installiert ist, und dann den gewünschten Recovery-Punkt.
   - Wählen Sie einen Recovery-Punkt auf der Registerkarte 'Backup Storage'.

Die in einer der oberen Aktionen zum Durchsuchen ausgewählte Maschine wird als Zielmaschine für die Wiederherstellung der Exchange-Daten verwendet.

4. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Wenn Sie eine Wiederherstellung aus einem applikationskonformen Backup durchführen, klicken Sie auf **Recovery** –> **Exchange-Datenbanken**, wählen Sie die wiederherzustellende Datenbank aus und klicken Sie dann auf **Recovery**.
   - Wenn Sie eine Wiederherstellung aus einem Datenbank-Backup durchführen, klicken Sie auf **Recovery** –> **Datenbanken zu einem Exchange Server**.
5. Die Datenbanken werden standardmäßig zu den ursprünglichen Datenbanken wiederhergestellt. Falls die ursprüngliche Datenbank nicht existiert, wird sie automatisch neu erstellt.

   So können Sie eine Datenbank zu einer anderen Datenbank wiederherstellen:

   a. Klicken Sie auf den Datenbanknamen.

   b. Wählen Sie bei **Recovery zu** die Option **Neue Datenbank**.

   c. Spezifizieren Sie den Namen für die neue Datenbank.

   d. Spezifizieren Sie den Pfad für die neue Datenbank und den Pfad für die Protokolle. Der von Ihnen spezifizierte Ordner darf keine ursprüngliche Datenbank oder Protokolldateien enthalten.
6. Klicken Sie auf **Recovery starten**.

Der Recovery-Fortschritt wird auf der Registerkarte 'Aktivitäten' angezeigt.

So können Sie Exchange-Datenbanken als Dateien wiederherstellen

1. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Wenn Sie eine Wiederherstellung aus einem applikationskonformen Backup durchführen, wählen Sie unter **Geräte** diejenige Maschine aus, auf der sich die wiederherzustellenden Daten ursprünglich befunden haben.
   - Wenn Sie eine Wiederherstellung aus einem Datenbank-Backup durchführen, klicken Sie auf **Geräte** –> **Microsoft Exchange** –> **Datenbanken** – und wählen Sie dann die Datenbanken, die Sie wiederherstellen wollen.
2. Klicken Sie auf **Recovery**.
3. Wählen Sie einen Recovery-Punkt. Beachten Sie dabei, dass Recovery-Punkte nach Speicherorten gefiltert werden.

   Falls die Maschine offline ist, werden keine Recovery-Punkte angezeigt. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - [Nur bei Wiederherstellung aus einem applikationskonformen Backup] Sollte sich das Backup im Cloud Storage oder einem freigegebenen Storage befinden (d.h., dass andere Agenten auf diesen zugreifen können), dann klicken Sie zuerst auf den Befehl **Maschine auswählen**. Wählen Sie anschließend eine Maschine aus, die online ist und auf welcher der Agent für Exchange oder der Agent für VMware installiert ist, und dann den gewünschten Recovery-

Punkt.

- Wählen Sie einen Recovery-Punkt auf der Registerkarte 'Backup Storage'.

  Die in einer der oberen Aktionen zum Durchsuchen ausgewählte Maschine wird als Zielmaschine für die Wiederherstellung der Exchange-Daten verwendet.

4. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Wenn Sie eine Wiederherstellung aus einem applikationskonformen Backup durchführen, klicken Sie auf **Recovery** –> **Exchange-Datenbanken**, wählen Sie die wiederherzustellende Datenbank aus und klicken Sie dann auf **Als Dateien wiederherstellen**.
   - Wenn Sie eine Wiederherstellung aus einem Datenbank-Backup durchführen, klicken Sie auf **Recovery** –> **Datenbanken als Dateien**
5. Klicken Sie auf **Durchsuchen** und wählen Sie einen lokalen Ordner oder Netzwerkordner aus, in dem die Dateien gespeichert werden sollen.
6. Klicken Sie auf **Recovery starten**.

Der Recovery-Fortschritt wird auf der Registerkarte 'Aktivitäten' angezeigt.

Exchange-Server-Datenbanken mounten

Sie können die Datenbanken nach Wiederherstellung der Datenbankdateien dadurch wieder online bringen, dass Sie sie mounten. Das Mounten wird mithilfe der Exchange-Verwaltungskonsole, dem Exchange-System-Manager oder der Exchange-Verwaltungsshell durchgeführt.

Die wiederhergestellte Datenbank wird sich im Stadium 'Dirty Shutdown' befinden. Eine Datenbank, die sich im Zustand 'Dirty Shutdown' befindet, kann vom System gemountet werden, falls sie zu ihrem ursprünglichen Speicherort wiederhergestellt wurde (vorausgesetzt, die Information über die ursprüngliche Datenbank ist im Active Directory vorhanden). Wenn Sie eine Datenbank zu einem anderen Speicherort wiederherstellen (beispielsweise eine neue Datenbank oder die Wiederherstellungsdatenbank), dann kann die Datenbank solange gemountet werden, bis Sie sie mithilfe des Befehls `Eseutil /r <Enn>` in das Stadium 'Clean Shutdown' bringen. `<Enn>` gibt den Logdatei-Präfix für die Datenbank an (bzw. die Speichergruppe, welche die Datenbank enthält), auf die Sie die Transaktionsprotokolldateien anwenden müssen.

Das Konto, welches Sie zum Anfügen einer Datenbank verwenden, muss an eine Exchange-Server-Administratorrolle und an eine lokalen Administratorengruppe des Zielservers delegiert sein.

Weitere Details zum Mounten von Datenbanken finden Sie in folgenden Artikeln:

- Exchange 2010 oder höher: http://technet.microsoft.com/de-de/library/aa998871.aspx
- Exchange 2007: http://technet.microsoft.com/de-de/library/aa998871(v=EXCHG.80).aspx

Exchange-Postfächer und Postfachelemente wiederherstellen

Sie können Exchange-Postfächer und -Postfachelemente aus folgenden Backups wiederherstellen:

- Datenbank-Backups
- Applikationskonforme Backups
- Postfach-Backups

Sie können folgende Elemente wiederherstellen:

- Postfächer (ausgenommen archivierte Postfächer)
- Öffentliche Ordner

Hinweis
Nur für Datenbank-Backups verfügbar. Siehe '"Exchange Server-Daten auswählen" (S. 615)'.

- Öffentlicher Ordner-Elemente
- E-Mail-Ordner
- E-Mail-Nachrichten
- Kalendereereignisse
- Aufgaben
- Kontakte
- Journal-Einträge
- Hinweise

Sie können eine Suchfunktion verwenden, um bestimmte Elemente zu finden.

Die Postfächer oder auch einzelne Postfachelemente können zu einem aktiv laufenden Exchange Server oder zu Microsoft 365 wiederhergestellt werden.

Wiederherstellungen zu einem Exchange Server

Granulare Wiederherstellungen können zu einem Microsoft Exchange Server 2010 Service Pack 1 (SP1) oder höher durchgeführt werden. Die im Quell-Backup gespeicherten Datenbanken oder Postfächer dürfen von jeder unterstützten Exchange-Version stammen.

Granulare Wiederherstellungen können vom Agenten für Exchange oder vom Agent for VMware (Windows) durchgeführt werden. Der als Ziel verwendete Exchange Server und die Maschine, auf welcher der Agent läuft, müssen derselben Active Directory-Gesamtstruktur (Forest) angehören.

Wenn bei einer Postfach-Wiederherstellung ein vorhandenes Postfach als Ziel ausgewählt wird, werden alle dort vorliegenden Elemente, die übereinstimmende IDs haben, überschrieben.

Bei einer Wiederherstellung von Postfachelementen werden keinerlei Elemente überschrieben. Stattdessen wird der vollständige Pfad zu einem Postfachelement im Zielordner neu erstellt.

Anforderungen an Benutzerkonten

Ein von einem Backup aus wiederhergestelltes Postfach muss ein assoziiertes Benutzerkonto im Active Directory haben.

Benutzerpostfächer und deren Inhalte können nur dann wiederhergestellt werden, wenn die mit ihnen assoziierten Benutzerkonten *aktiviert* sind. Raum-, Geräte- oder freigegebene Postfächer können nur dann wiederhergestellt werden, wenn ihre assoziierten Benutzerkonten *deaktiviert* sind.

Ein Postfach, welches die oberen Bedingungen nicht erfüllt, wird während einer Wiederherstellung übersprungen.

Falls einige Postfächer übersprungen werden, die Wiederherstellung mit dem Status 'Mit Warnungen' abgeschlossen. Sollten alle Postfächer übersprungen werden, schlägt die Wiederherstellung fehl.

Wiederherstellungen zu Microsoft 365

Die Wiederherstellung von Exchange-Datenelementen zu Microsoft 365 (und umgekehrt) wird nur unter der Bedingung unterstützt, dass der Agent für Microsoft 365 lokal installiert ist.

Wiederherstellungen können aus Backups von Microsoft Exchange Server 2010 (oder höher) durchgeführt werden.

Wenn ein Postfach zu einem vorhandenen Microsoft 365-Postfach wiederhergestellt wird, bleiben dort bereits vorhandene Elemente erhalten. Die wiederhergestellten Elemente werden neben den vorhandenen gespeichert.

Wenn Sie ein einzelnes Postfach wiederherstellen, müssen Sie das Microsoft 356-Postfach auswählen, das als Ziel dienen soll. Wenn Sie mehrere Postfächer mit einer Recovery-Aktion wiederherstellen wollen, wird die Software versuchen, jedes Postfach zu dem Postfach desjenigen Benutzers wiederherzustellen, der denselben Benutzernamen hat. Wenn dieser Benutzer nicht gefunden werden kann, wird das Postfach übersprungen. Falls einige Postfächer übersprungen werden, die Wiederherstellung mit dem Status 'Mit Warnungen' abgeschlossen. Sollten alle Postfächer übersprungen werden, schlägt die Wiederherstellung fehl.

Weitere Informationen über Wiederherstellungen in Microsoft 365 finden Sie im Abschnitt '"Microsoft 365-Daten sichern" (S. 654)'.

Postfächer wiederherstellen

So können Sie Postfächer aus einem applikationskonformen Backup oder einem Datenbank-Backup wiederherstellen

1. [Nur bei Wiederherstellung eines Datenbank-Backups zu Microsoft 365] Wenn der Agent für Microsoft 365 auf der Maschine, die den Exchange Server ausführt und per Backup gesichert wurde, nicht installiert ist, gehen Sie folgendermaßen vor:
   - Falls Sie keinen Agenten für Microsoft 365 in Ihrem Unternehmen haben, dann installieren Sie den Agenten für Microsoft 365 auf der Maschine, die per Backup gesichert wurde (oder auf einer anderen Maschine mit derselben Microsoft Exchange Server-Version).
   - Falls Sie einen Agenten für Microsoft 365 in Ihrem Unternehmen haben, dann kopieren Sie Bibliotheken von der Maschine, die per Backup gesichert wurde (oder von einer anderen Maschine mit derselben Microsoft Exchange Server-Version), zu der Maschine mit dem

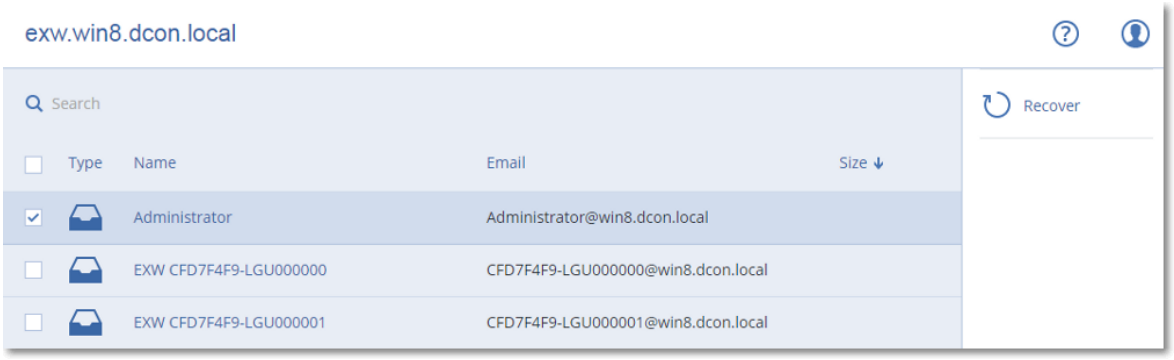
Agenten für Microsoft 365. Eine entsprechende Beschreibung dazu finden Sie im Abschnitt 'Microsoft Exchange-Bibliotheken kopieren'.

2. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Bei Wiederherstellung aus einem applikationskonformen Backup: Wählen Sie unter **Geräte** diejenige Maschine aus, auf der sich die wiederherzustellenden Daten ursprünglich befunden haben.
   - Wenn Sie eine Wiederherstellung aus einem Datenbank-Backup durchführen, klicken Sie auf **Geräte** –> **Microsoft Exchange** –> **Datenbanken** – und wählen Sie dann diejenige Datenbank aus, in der sich die wiederherzustellenden Daten ursprünglich befunden haben.
3. Klicken Sie auf **Recovery**.
4. Wählen Sie einen Recovery-Punkt. Beachten Sie dabei, dass Recovery-Punkte nach Speicherorten gefiltert werden.

   Falls die Maschine offline ist, werden keine Recovery-Punkte angezeigt. Andere Wiederherstellungsmöglichkeiten verwenden:
   - [Nur bei Wiederherstellung aus einem applikationskonformen Backup] Sollte sich das Backup im Cloud Storage oder einem freigegebenen Storage befinden (d.h., dass andere Agenten auf diesen zugreifen können), dann klicken Sie zuerst auf den Befehl **Maschine auswählen**. Wählen Sie anschließend eine Maschine aus, die online ist und auf welcher der Agent für Exchange oder der Agent für VMware installiert ist, und dann den gewünschten Recovery-Punkt.
   - Wählen Sie einen Recovery-Punkt auf der Registerkarte 'Backup Storage'.

   Die in einer der oberen Aktionen zum Durchsuchen ausgewählte Maschine wird dann die Wiederherstellung durchführen (statt der ursprünglichen Maschine, die offline ist).
5. Klicken Sie auf **Recovery** –> **Exchange-Postfächer**.
6. Wählen Sie die Postfächer aus, die Sie wiederherstellen wollen.

   Sie können die Postfächer nach einem Namen durchsuchen. Platzhalterzeichen (Wildcards) werden nicht unterstützt.



7. Klicken Sie auf **Recovery**.
8. [Nur bei Wiederherstellung zu Microsoft 365]:

a. Wählen Sie bei **Recovery zu** den Eintrag **Microsoft 365**.

b. [Wenn Sie in Schritt 6 nur ein Postfach ausgewählt haben] Spezifizieren Sie bei **Zielpostfach** das Postfach, das als Recovery-Ziel verwendet werden soll.

c. Klicken Sie auf **Recovery starten**.

Weitere Schritte dieser Prozedur sind nicht erforderlich.

Klicken Sie auf **Zielmaschine mit Microsoft Exchange Server**, wenn Sie die Zielmaschine auswählen oder ändern wollen. Mit diesem Schritt können Sie eine Maschine als Recovey-Ziel verwenden, auf der kein Agent für Exchange läuft.

Spezifizieren Sie den vollqualifizierten Domain-Namen (FQDN) einer Maschine, auf welcher die Rolle **Clientzugriff** (in Microsoft Exchange Server 2010/2013) **Postfachrolle** (in Microsoft Exchange Server 2016 oder höher) aktiviert ist. Die Maschine muss zu derselben Active Directory-Gesamtstruktur (Forest) gehören wie die Maschine, welche die Wiederherstellung durchführt.

9. Geben Sie bei Aufforderung die Anmeldedaten eines Kontos ein, welches für den Zugriff auf die Maschine verwendet werden soll. Die Anforderungen für dieses Konto sind im Abschnitt 'Erforderliche Benutzerrechte' aufgeführt.
10. [Optional] Klicken Sie auf **Datenbank zur Neuerstellung fehlender Postfächer**, wenn Sie die automatisch ausgewählte Datenbank ändern wollen.
11. Klicken Sie auf **Recovery starten**.

Der Recovery-Fortschritt wird auf der Registerkarte **Aktivitäten** angezeigt.

So können Sie ein Postfach aus einem Postfach-Backup wiederherstellen

1. Klicken Sie auf **Geräte** –> **Microsoft Exchange** –> **Postfächer**.
2. Wählen Sie das wiederherzustellende Postfach und klicken Sie dann auf **Recovery**.

   Sie können die Postfächer nach einem Namen durchsuchen. Platzhalterzeichen (Wildcards) werden nicht unterstützt.

   Falls das Postfach gelöscht wurde, wählen Sie es in der Registerkarte 'Backup Storage' aus – und klicken Sie dann auf **Backups anzeigen**.
3. Wählen Sie einen Recovery-Punkt. Beachten Sie dabei, dass Recovery-Punkte nach Speicherorten gefiltert werden.
4. Klicken Sie auf **Recovery** –> **Postfach**.
5. Führen Sie die Schritte 8-11 der oberen Prozedur durch.

Postfachelemente wiederherstellen

So können Sie Postfachelemente aus einem applikationskonformen Backup oder einem Datenbank-Backup wiederherstellen

1. [Nur bei Wiederherstellung eines Datenbank-Backups zu Microsoft 365] Wenn der Agent für Microsoft 365 auf der Maschine, die den Exchange Server ausführt und per Backup gesichert wurde, nicht installiert ist, gehen Sie folgendermaßen vor:

- Falls Sie keinen Agenten für Microsoft 365 in Ihrem Unternehmen haben, dann installieren Sie den Agenten für Microsoft 365 auf der Maschine, die per Backup gesichert wurde (oder auf einer anderen Maschine mit derselben Microsoft Exchange Server-Version).
- Falls Sie einen Agenten für Microsoft 365 in Ihrem Unternehmen haben, dann kopieren Sie Bibliotheken von der Maschine, die per Backup gesichert wurde (oder von einer anderen Maschine mit derselben Microsoft Exchange Server-Version), zu der Maschine mit dem Agenten für Microsoft 365. Eine entsprechende Beschreibung dazu finden Sie im Abschnitt 'Microsoft Exchange-Bibliotheken kopieren'.

2. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Bei Wiederherstellung aus einem applikationskonformen Backup: Wählen Sie unter **Geräte** diejenige Maschine aus, auf der sich die wiederherzustellenden Daten ursprünglich befunden haben.
   - Wenn Sie eine Wiederherstellung aus einem Datenbank-Backup durchführen, klicken Sie auf **Geräte** –> **Microsoft Exchange** –> **Datenbanken** – und wählen Sie dann diejenige Datenbank aus, in der sich die wiederherzustellenden Daten ursprünglich befunden haben.
3. Klicken Sie auf **Recovery**.
4. Wählen Sie einen Recovery-Punkt. Beachten Sie dabei, dass Recovery-Punkte nach Speicherorten gefiltert werden.

   Falls die Maschine offline ist, werden keine Recovery-Punkte angezeigt. Andere Wiederherstellungsmöglichkeiten verwenden:
   - [Nur bei Wiederherstellung aus einem applikationskonformen Backup] Sollte sich das Backup im Cloud Storage oder einem freigegebenen Storage befinden (d.h., dass andere Agenten auf diesen zugreifen können), dann klicken Sie zuerst auf den Befehl **Maschine auswählen**. Wählen Sie anschließend eine Maschine aus, die online ist und auf welcher der Agent für Exchange oder der Agent für VMware installiert ist, und dann den gewünschten Recovery-Punkt.
   - Wählen Sie einen Recovery-Punkt auf der Registerkarte 'Backup Storage'.

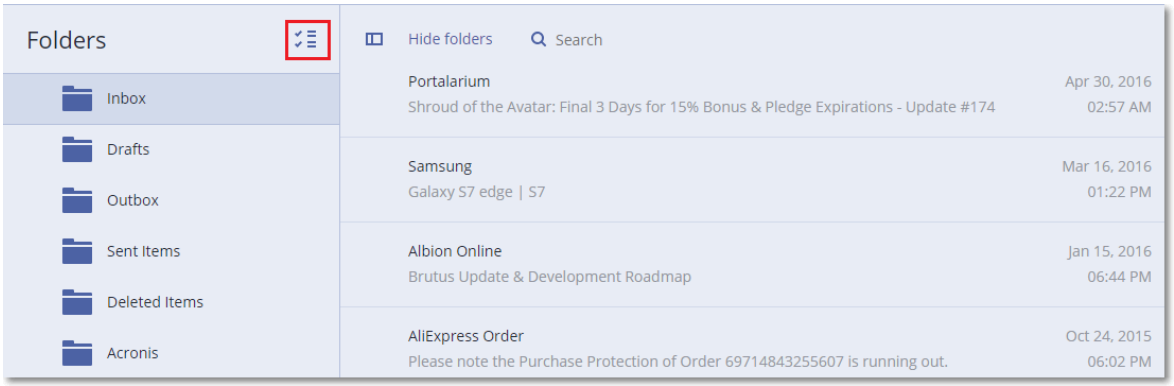
   Die in einer der oberen Aktionen zum Durchsuchen ausgewählte Maschine wird dann die Wiederherstellung durchführen (statt der ursprünglichen Maschine, die offline ist).
5. Klicken Sie auf **Recovery** –> **Exchange-Postfächer**.
6. Klicken Sie auf dasjenige Postfach, in dem sich die wiederherzustellenden Elemente ursprünglich befunden haben.
7. Wählen Sie die Elemente aus, die Sie wiederherstellen wollen.

   Folgende Suchoptionen sind verfügbar. Platzhalterzeichen (Wildcards) werden nicht unterstützt.
   - Für E-Mail-Nachrichten: Suche per Betreff, Absender, Empfänger und Datum.
   - Für Ereignisse: Suche nach Titel und Datum.
   - Für Tasks: Suche per Betreff und Datum.
   - Für Kontakte: Suche nach Namen, E-Mail-Adresse und Telefonnummer.

   Bei Auswahl einer E-Mail-Nachricht können Sie auf **Inhalt anzeigen** klicken, damit Ihnen die Nachricht (inkl. Anhänge) angezeigt wird.

Hinweis
Sie können eine angehängte Datei herunterladen, indem Sie auf ihren Namen klicken.

Wenn Sie Ordner auswählen wollen, klicken Sie auf das Symbol zum Wiederherstellen von Ordnern.



8. Klicken Sie auf **Recovery**.
9. Wenn Sie zu Microsoft 365 wiederherstellen wollen, wählen Sie bei **Recovery zu** den Eintrag **Microsoft 365**.

   Wenn Sie zu einem Exchange Server wiederherstellen wollen, übernehmen Sie bei **Recovery zu** den Standardwert **Microsoft Exchange**.

   [Nur bei Wiederherstellung zu einem Exchange Server] Klicken Sie auf **Zielmaschine mit Microsoft Exchange Server**, wenn Sie die Zielmaschine auswählen oder ändern wollen. Mit diesem Schritt können Sie eine Maschine als Recovey-Ziel verwenden, auf der kein Agent für Exchange läuft.

   Spezifizieren Sie den vollqualifizierten Domain-Namen (FQDN) einer Maschine, auf welcher die Rolle **Clientzugriff** (in Microsoft Exchange Server 2010/2013) **Postfachrolle** (in Microsoft Exchange Server 2016 oder höher) aktiviert ist. Die Maschine muss zu derselben Active Directory-Gesamtstruktur (Forest) gehören wie die Maschine, welche die Wiederherstellung durchführt.
10. Geben Sie bei Aufforderung die Anmeldedaten eines Kontos ein, welches für den Zugriff auf die Maschine verwendet werden soll. Die Anforderungen für dieses Konto sind im Abschnitt 'Erforderliche Benutzerrechte' aufgeführt.
11. Bei **Zielpostfach** können Sie das gewünschte Zielpostfach anzeigen lassen, ändern oder spezifizieren.

    Das ursprüngliche Postfach wird automatisch vorausgewählt. Wenn dieses Postfach nicht existiert oder Sie eine andere als die ursprüngliche Maschine als Ziel ausgewählt haben, müssen Sie das Zielpostfach spezifizieren.
12. [Nur bei Wiederherstellung von E-Mail-Nachrichten] Bei **Zielordner** können Sie den Zielordner im Zielpostfach einsehen oder ändern. Standardmäßig ist der Ordner **Wiederhergestellte Elemente** vorausgewählt. Aufgrund von Microsoft Exchange-Beschränkungen werden Kalendereereignisse, Aufgaben und Notizen immer zu ihrem ursprünglichen Ordner wiederhergestellt, unabhängig davon, ob ein anderer **Zielordner** spezifiziert wurde.

13. Klicken Sie auf **Recovery starten**.

Der Recovery-Fortschritt wird auf der Registerkarte **Aktivitäten** angezeigt.

So können Sie ein Postfachelement aus einem Postfach-Backup wiederherstellen

1. Klicken Sie auf **Geräte** –> **Microsoft Exchange** –> **Postfächer**.
2. Wählen Sie dasjenige Postfach aus, in dem sich die wiederherzustellenden Elemente ursprünglich befunden haben – und klicken Sie dann auf **Recovery**.

   Sie können die Postfächer nach einem Namen durchsuchen. Platzhalterzeichen (Wildcards) werden nicht unterstützt.

   Falls das Postfach gelöscht wurde, wählen Sie es in der Registerkarte 'Backup Storage' aus – und klicken Sie dann auf **Backups anzeigen**.
3. Wählen Sie einen Recovery-Punkt. Beachten Sie dabei, dass Recovery-Punkte nach Speicherorten gefiltert werden.
4. Klicken Sie auf **Recovery** –> **E-Mail-Nachrichten**.
5. Wählen Sie die Elemente aus, die Sie wiederherstellen wollen.

   Folgende Suchoptionen sind verfügbar. Platzhalterzeichen (Wildcards) werden nicht unterstützt.

   - Für E-Mail-Nachrichten: Suche per Betreff, Absender, Empfänger und Datum.
   - Für Ereignisse: Suche nach Titel und Datum.
   - Für Tasks: Suche per Betreff und Datum.
   - Für Kontakte: Suche nach Namen, E-Mail-Adresse und Telefonnummer.

   Bei Auswahl einer E-Mail-Nachricht können Sie auf **Inhalt anzeigen** klicken, damit Ihnen die Nachricht (inkl. Anhänge) angezeigt wird.

   Hinweis
   Sie können eine angehängte Datei herunterladen, indem Sie auf ihren Namen klicken.

   Wenn eine E-Mail-Nachricht ausgewählt wurde, können Sie auf **Als E-Mail senden** klicken, damit die Nachricht an eine bestimmte E-Mail-Adresse gesendet wird. Als Absender der Nachricht wird die E-Mail-Adresse Ihres Administrator-Kontos verwendet.

   Wenn Sie Ordner auswählen wollen, klicken Sie auf das Symbol 'Ordner wiederherstellen': 
6. Klicken Sie auf **Recovery**.
7. Führen Sie die Schritte 9-13 der oberen Prozedur durch.

Microsoft Exchange-Bibliotheken kopieren

Wenn Sie Exchange-Postfächer oder Postfach-Elemente zu Microsoft 365 wiederherstellen wollen, müssen Sie möglicherweise die folgenden Bibliotheken von der Maschine, die per Backup gesichert wurde (oder von einer anderen Maschine mit derselben Microsoft Exchange Server-Version), zu derjenigen Maschine kopieren, auf welcher sich der Agent für Microsoft 365 befindet.

Kopieren Sie – entsprechend der gesicherten Microsoft Exchange Server-Version – die folgenden Dateien:

Microsoft Exchange Server-Version	Bibliotheken	Standardspeicherort

Microsoft Exchange Server 2010	`ese.dll`
	`esebcli2.dll`
	`store.exe`
		`%ProgramFiles%\Microsoft\Exchange Server\V14\bin`

Microsoft Exchange Server 2013	`ese.dll`	`%ProgramFiles%\Microsoft\Exchange Server\V15\bin`
	`msvcr110.dll`	`%WINDIR%\system32`
Microsoft Exchange Server 2016, 2019	`ese.dll`	`%ProgramFiles%\Microsoft\Exchange Server\V15\bin`
	`msvcr110.dll` `msvcp110.dll`	`%WINDIR%\system32`

Die Bibliotheken sollten in diesem Ordner gespeichert werden: `%ProgramData%\Acronis\ese`. Wenn dieser Ordner noch nicht existiert, müssen Sie ihn manuell erstellen.

Die SQL Server- oder Exchange Server-Zugriffsanmeldedaten ändern

Sie können die Zugriffsanmeldedaten für einen SQL Server oder Exchange Server ändern, ohne den entsprechenden Agenten neu installieren zu müssen.

So ändern Sie die Anmeldedaten für einen SQL Server oder Exchange Server

1. Klicken Sie auf **Geräte** und anschließend auf **Microsoft SQL** oder **Microsoft Exchange**.
2. Wählen Sie die AlwaysOn-Verfügbarkeitsgruppe, Datenbankverfügbarkeitsgruppe, SQL Server-Instanz oder den Exchange Server, für die/den Sie die Anmeldedaten ändern wollen.
3. Klicken Sie auf **Anmeldedaten spezifizieren**.
4. Spezifizieren Sie die neuen Anmeldedaten und klicken Sie abschließend auf **OK**.

So ändern Sie die Anmeldedaten eines Exchange Servers bei einem Postfach-Backup

1. Klicken Sie auf **Geräte** –> **Microsoft Exchange**und erweiteren Sie dann **Postfächer**.
2. Wählen Sie den Exchange Server aus, dessen Anmeldedaten Sie ändern wollen.
3. Klicken Sie auf **Einstellungen**.
4. Spezifizieren Sie bei **Exchange-Administratorkonto** die neuen Zugriffsanmeldedaten und klicken Sie anschließend auf **Speichern**.

Mobilgeräte sichern

Mit der Cyber Protect-App können Sie die Daten Ihres Mobilgerätes in den Cloud Storage sichern – um sie von dort (bei Datenverlust oder Datenbeschädigung) wiederherstellen zu können. Beachten

Sie, dass Sie zur Backup-Erstellung in den Cloud Storage ein Konto und ein Cloud-Abonnement benötigen.

Unterstützte Mobilgeräte

Sie können die Cyber Protect-App auf einem Mobilgerät installieren, das mit einem der folgenden Betriebssysteme läuft:

- iOS 14 bis iOS 16 (iPhone, iPod, iPad)
- Android 9 bis Android 13

Was Sie per Backup sichern können

- Kontakte (Name, Telefonnummer und E-Mail-Adresse)
- Fotos (die ursprüngliche Größe und das ursprüngliche Format Ihrer Fotos bleiben erhalten)
- Videos
- Kalender
- Erinnerungen (nur bei iOS-Geräte)

Was Sie wissen sollten

- Sie können Ihre Daten nur zum Cloud Storage (als Ziel) sichern.
- Die App zeigt Ihnen bei jedem Start eine Übersicht von zwischenzeitlich erfolgten Datenänderungen an. Diese können Sie auf Wunsch dann mit einem manuellen Backup sichern.
- Standardmäßig ist die Funktionalität '**Kontinuierliches Backup**' eingeschaltet. Wenn diese Einstellung aktiviert ist, wird die Cyber Protect-App neue Daten automatisch erkennen und diese in die Cloud hochladen.
- Die Option **Nur WLAN verwenden** ist in den Einstellungen der App standardmäßig aktiviert. Wenn diese Einstellung aktiviert ist, wird die Cyber Protect-App Ihre Daten nur dann per Backup sichern, wenn eine WLAN-Verbindung verfügbar ist. Wenn die (W)LAN-Verbindung verloren ging, wird kein Backup-Prozess gestartet. Wenn die App auch die Mobilfunkdatenverbindung verwenden soll, müssen Sie diese Option deaktivieren.
- Die Akkuverbrauch-Optimierung auf Ihrem Gerät kann möglicherweise verhindern, dass die Cyber Protect-App ordnungsgemäß funktioniert. Damit die Backups planmäßig ausgeführt werden, sollten Sie die Akkuverbrauch-Optimierung für die App deaktivieren.
- Sie haben zwei Möglichkeiten, Energie zu sparen:
  - Mit der Funktionalität **Backup beim Aufladen** – die standardmäßig deaktiviert ist. Wenn diese Einstellung aktiviert ist, wird die Cyber Protect-App Ihre Daten nur dann per Backup sichern, wenn Ihr Gerät mit einer externen Stromquelle verbunden ist. Wenn das Gerät während eines kontinuierlichen Backup-Prozesses vom Ladegerät getrennt wird, wird das Backup pausiert.
  - Mit dem **Energiesparmodus** (bei iOS 'Stromsparmodus' genannt) – der standardmäßig aktiviert ist. Wenn diese Einstellung aktiviert ist, wird die Cyber Protect-App Ihre Daten nur

dann per Backup sichern, wenn Ihr Akkuladestand hoch ist. Wenn der Akkustand auf einen niedrigen Wert sinkt, wird das kontinuierliche Backup pausiert.

- Auf die gesicherten Daten können Sie anschließend von jedem Mobilgerät aus zugreifen, welches für Ihr Konto registriert ist. Dies ist hilfreich, wenn Sie Daten beispielsweise von einem alten auf ein neues Mobilgerät übertragen wollen. Bei Kontakten und Fotos ist es möglich, diese von einem Android-Gerät (Quelle) auf einem iOS-Gerät (Ziel) wiederherzustellen – und umgekehrt. Mithilfe der Cyber Protect-Konsole können Sie Fotos, Videos und Kontakte außerdem auch auf jedes andere Gerät herunterladen.
- Daten, die von Mobilgeräten gesichert wurden, welche für Ihr Konto registriert sind, sind auch nur über Ihr Konto verfügbar. Keine andere Person kann Ihre Daten einsehen oder wiederherstellen.
- In der Cyber Protect-App können Sie immer nur jeweils die letzten (neuesten) Datenversionen wiederherstellen. Wenn Sie Daten aus einer spezifischen Backup-Version wiederherstellen wollen, müssen Sie die Cyber Protect-Konsole auf einem Computer oder Tablet verwenden.
- Auf die Backups von Mobilgeräten werden keine Aufbewahrungsregeln angewendet.
- [Nur für Android-Geräte] Wenn während des Backups in dem Gerät eine SD-Karte vorhanden ist, werden auch die dort gespeicherten Daten mitgesichert. Die Daten werden auf eine SD-Karte in den Ordner **Recovered by Backup** wiederhergestellt, sofern dieser während der Wiederherstellung vorhanden ist – oder die App fragt nach einem anderen Speicherort, wohin die Daten wiederhergestellt werden sollen.

Wo Sie die Cyber Protect-App erhalten

Installieren Sie – je nachdem, was Sie für ein Mobilgerät haben – die App aus dem Apple App Store oder dem Google Play Store.

So können Sie die Sicherung Ihrer Daten starten

1. Öffnen Sie die App.
2. Melden Sie sich mit Ihrem Konto an.
3. Tippen Sie auf **Einrichten**, um Ihr Backup zu erstellen. Beachten Sie, dass diese Schaltfläche nur erscheint, wenn Sie bisher noch kein Backup Ihres Mobilgerätes haben.
4. Wählen Sie die Datenkategorien aus, die Sie sichern wollen. Standardmäßig sind alle Kategorien ausgewählt.
5. [Optionaler Schritt] Aktivieren Sie **Backup verschlüsseln**, um Ihr Backup durch Verschlüsselung zu schützen. In diesem Fall müssen Sie außerdem:
   a. Ein Verschlüsselungskennwort zweimal eingeben.

   Hinweis
   Stellen Sie sicher, dass Sie sich das Kennwort merken, weil ein vergessenes Kennwort weder

wiederhergestellt noch geändert werden kann.

b. Tippen Sie auf **Verschlüsseln**.

6. Tippen Sie auf **Backup**.
7. Erlauben Sie, dass die App auf Ihre persönlichen Daten zugreifen darf. Datenkategorien, auf die Sie den Zugriff verweigert haben, werden nicht mitgesichert.

Das Backup wird gestartet.

So können Sie Daten zu einem Mobilgerät wiederherstellen

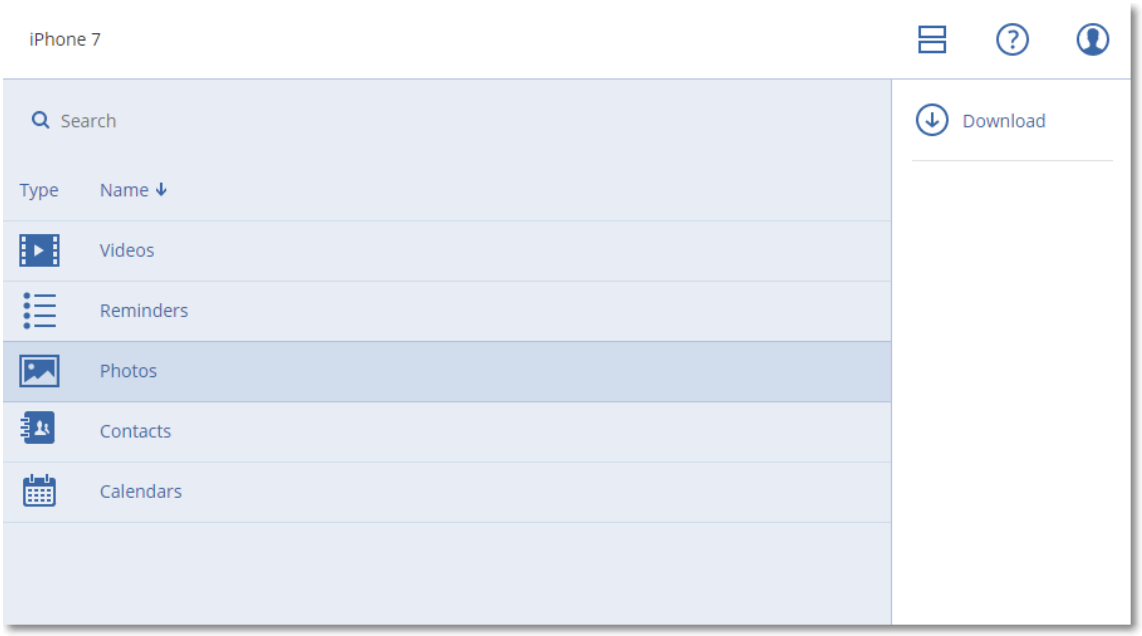
Warnung!
Um die Daten von Mobilgeräten wiederherstellen zu können, müssen Sie das Endbenutzerkonto verwenden.

1. Öffnen Sie die Cyber Protect-App.
2. Tippen Sie auf den Befehl **Durchsuchen**.
3. Tippen Sie auf den Gerätenamen.
4. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Wenn Sie alle gesicherten Daten wiederherstellen wollen, müssen Sie auf **Alle wiederherstellen** tippen. Es sind keine weiteren Aktionen erforderlich.
   - Wenn Sie eine oder mehrere Datenkategorien wiederherstellen wollen, müssen Sie auf **Auswahl** tippen und dann die Kontrollkästchen der gewünschten Datenkategorien aktivieren. Tippen Sie auf den Befehl **Recovery**. Es sind keine weiteren Aktionen erforderlich.
   - Wenn Sie eines oder mehrere Datenelemente wiederherstellen wollen, die zu einer bestimmten Datenkategorie gehören, müssen Sie auf die betreffende Datenkategorie tippen. Fahren Sie mit den nachfolgenden Schritten fort.
5. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Wenn Sie ein einzelnes Datenelement wiederherstellen wollen, müssen Sie dieses antippen.
   - Wenn Sie mehrere Datenelemente wiederherstellen wollen, müssen Sie auf **Auswahl** tippen und dann die Kontrollkästchen der gewünschten Elemente aktivieren.
6. Tippen Sie auf den Befehl **Recovery**.

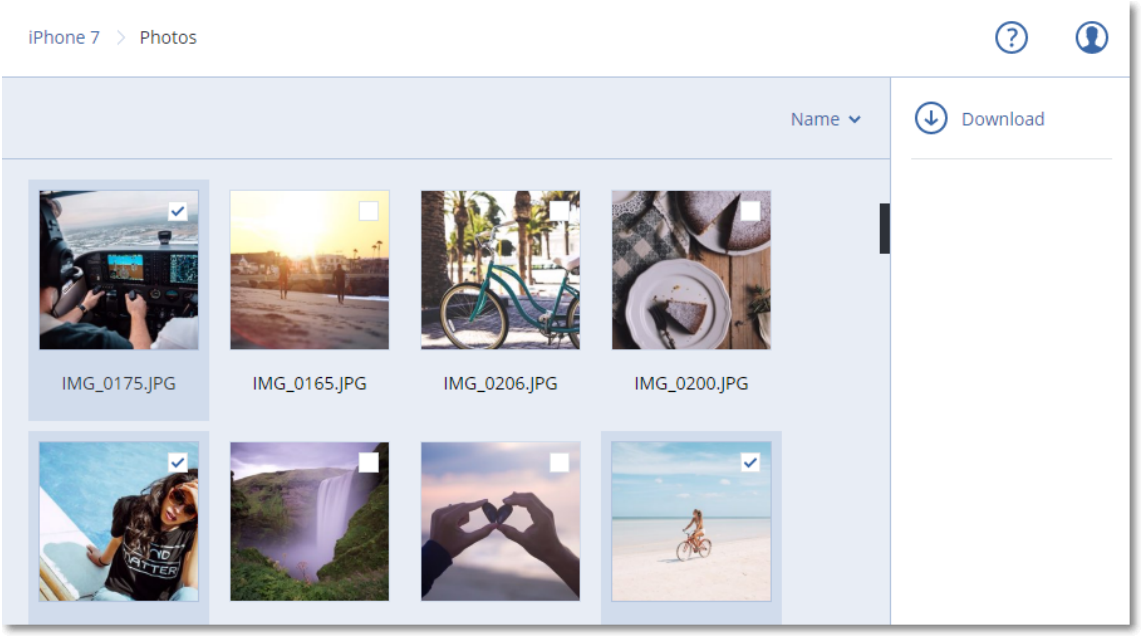
So können Sie Daten über die Cyber Protect-Konsole überprüfen

1. Öffnen Sie auf einem Computer einen Webbrowser und geben Sie die URL der Cyber Protect-Konsole ein.
2. Melden Sie sich mit Ihrem Konto an.
3. Klicken Sie bei **Alle Geräte** unter dem Namen Ihres Mobilgerätes auf den Befehl **Recovery**.
4. Gehen Sie nach einer der folgenden Möglichkeiten vor:

- Wenn Sie alle Fotos, Videos, Kontakte, Kalendereinträge oder Erinnerungen herunterladen wollen, müssen Sie die entsprechende Datenkategorie auswählen. Klicken Sie auf **Download**.



- Wenn Sie bestimmte Fotos, Videos, Kontakte, Kalendereinträge oder Erinnerungen herunterladen wollen, müssen Sie auf die entsprechende Datenkategorie klicken und dann die Kontrollkästchen der gewünschten Datenelemente aktivieren. Klicken Sie auf **Download**.



- Wenn Sie eine Vorschau von einem Foto oder einem Kontakt ansehen wollen, müssen Sie auf die entsprechende Datenkategorie klicken und dann auf das gewünschte Datenelement.

Hosted Exchange-Daten schützen

Welche Elemente können per Backup gesichert werden?

Sie können Benutzerpostfächer, freigegebene Postfächer und Gruppenpostfächer sichern. Außerdem können Sie optional auch die Archivpostfächer (**In-Situ-Archiv**) der ausgewählten Postfächer sichern.

Welche Elemente können wiederhergestellt werden?

Folgende Elemente können aus einem Postfach-Backup wiederhergestellt werden:

- Postfächer
- E-Mail-Ordner
- E-Mail-Nachrichten
- Kalenderereignisse
- Aufgaben
- Kontakte
- Journal-Einträge
- Hinweise

Sie können eine Suchfunktion verwenden, um bestimmte Elemente zu finden.

Wenn Sie Postfächer, Postfachelemente, öffentliche Ordner oder Elemente aus öffentlichen Ordnern wiederherstellen, können Sie auswählen, ob die Elemente am Zielort überschrieben werden sollen (oder nicht).

Wenn bei einer Postfach-Wiederherstellung ein vorhandenes Postfach als Ziel ausgewählt wird, werden alle dort vorliegenden Elemente, die übereinstimmende IDs haben, überschrieben.

Bei einer Wiederherstellung von Postfachelementen werden keinerlei Elemente überschrieben. Stattdessen wird der vollständige Pfad zu einem Postfachelement im Zielordner neu erstellt.

Exchange Online-Postfächer auswählen

Wählen Sie die Postfächer wie nachfolgend beschrieben aus – und spezifizieren Sie dann die anderen Einstellungen des Schutzplans nach Bedarf.

So können Sie Exchange Online-Postfächer auswählen

1. Klicken Sie auf **Geräte –> Hosted Exchange**.
2. Wenn dem Cyber Protection Service mehrere Hosted Exchange-Organisationen hinzugefügt wurden, wählen Sie diejenige Organisation aus, deren Benutzerdaten Sie sichern wollen. Ansonsten können Sie diesen Schritt überspringen.

3. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Um die Postfächer aller Benutzer und alle freigegegenen Postfächer zu sichern (einschließlich solcher Postfächer, die erst in der Zukunft angelegt werden), erweitern Sie den Knoten **Benutzer**, wählen Sie **Alle Benutzer** und klicken Sie dann auf **Gruppen-Backup**.
   - Wenn Sie einzelne Benutzerpostfächer oder freigegebene Postfächer sichern wollen, erweitern Sie den Knoten **Benutzer**, wählen Sie **Alle Benutzer**, wählen Sie die Benutzer aus, deren Postfächer Sie sichern wollen, und klicken Sie dann auf **Backup**.
   - Um alle Gruppenpostfächer zu sichern (einschließlich der Postfächer von Gruppen, die erst in der Zukunft angelegt werden), erweitern Sie den Knoten **Gruppen**, wählen Sie **Alle Gruppen** und klicken Sie dann auf **Gruppen-Backup**.
   - Wenn Sie einzelne Gruppenpostfächer sichern wollen, erweitern Sie den Knoten **Gruppen**, wählen Sie **Alle Gruppen**, wählen Sie die Gruppen aus, deren Postfächer Sie sichern wollen, und klicken Sie dann auf **Backup**.

Postfächer und Postfachelemente wiederherstellen

Postfächer wiederherstellen

1. Klicken Sie auf **Geräte –> Hosted Exchange**.
2. Wenn dem Cyber Protection Service mehrere Hosted Exchange-Organisationen hinzugefügt wurden, wählen Sie diejenige Organisation aus, deren gesicherte Daten Sie wiederherstellen wollen. Ansonsten können Sie diesen Schritt überspringen.
3. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Wenn Sie ein Benutzerpostfach wiederherstellen wollen, erweitern Sie den Knoten **Benutzer**, wählen Sie **Alle Benutzer**, wählen Sie den Benutzer aus, dessen Postfach Sie wiederherstellen wollen, und klicken Sie dann auf **Recovery**.
   - Wenn Sie ein freigegebenes Postfach wiederherstellen wollen, erweitern Sie den Knoten **Benutzer**, wählen Sie **Alle Benutzer**, wählen Sie das freigegebene Postfach aus, welches Sie wiederherstellen wollen, und klicken Sie dann auf **Recovery**.
   - Wenn Sie ein Gruppenpostfach wiederherstellen wollen, erweitern Sie den Knoten **Gruppen**, wählen Sie **Alle Gruppen**, wählen Sie die Gruppe aus, deren Postfach Sie wiederherstellen wollen, und klicken Sie dann auf **Recovery**.
   - Wenn der Benutzer, die Gruppe oder das freigegebene Postfach zuvor gelöscht wurde, können Sie das Element im Bereich **Cloud-Applikationen-Backups** in der Registerkarte 'Backup Storage' auswählen und dann auf **Backups anzeigen** klicken.

   Sie können Benutzer und Gruppen auch per Namen suchen. Platzhalterzeichen (Wildcards) werden nicht unterstützt.
4. Wählen Sie einen Recovery-Punkt.
5. Klicken Sie auf **Recovery** –> **Komplettes Postfach**.
6. Wenn dem Cyber Protection Service mehrere Hosted Exchange-Organisationen hinzugefügt werden, klicken Sie auf **Hosted Exchange-Organisation**, um die Zielorganisation einsehen,

ändern oder spezifizieren zu können.

Die ursprüngliche Organisation wird automatisch vorausgewählt. Wenn diese Organisation nicht mehr im Cyber Protection Service registriert ist, müssen Sie die Zielorganisation spezifizieren.

7. Bei**Zu Postfach wiederherstellen** können Sie das gewünschte Zielpostfach anzeigen lassen, ändern oder spezifizieren.

   Das ursprüngliche Postfach wird automatisch vorausgewählt. Wenn dieses Postfach nicht mehr existiert oder Sie eine andere als die ursprüngliche Organisation als Ziel ausgewählt haben, müssen Sie das Zielpostfach spezifizieren.
8. Klicken Sie auf **Recovery starten**.
9. Wählen Sie eine dieser Überschreiben-Optionen:
   - **Vorhandene Elemente überschreiben**
   - **Vorhandene Elemente nicht überschreiben**
10. Klicken Sie auf **Forsetzen**, um Ihre Entscheidung zu bestätigen.

Postfachelemente wiederherstellen

1. Klicken Sie auf **Geräte –> Hosted Exchange**.
2. Wenn dem Cyber Protection Service mehrere Hosted Exchange-Organisationen hinzugefügt wurden, wählen Sie diejenige Organisation aus, deren gesicherte Daten Sie wiederherstellen wollen. Ansonsten können Sie diesen Schritt überspringen.
3. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Wenn Sie Elemente aus einem Benutzerpostfach wiederherstellen wollen, erweitern Sie den Knoten **Benutzer**, wählen Sie **Alle Benutzer**, wählen Sie denjenigen Benutzer aus, in dessen Postfach sich die wiederherzustellenden Elemente ursprünglich befunden haben, und klicken Sie dann auf **Recovery**.
   - Wenn Sie Elemente aus einem freigegebenen Postfach wiederherstellen wollen, erweitern Sie den Knoten **Benutzer**, wählen Sie **Alle Benutzer**, wählen Sie dasjenige freigegebene Postfach aus, in welchem sich die wiederherzustellenden Elemente ursprünglich befunden haben, und klicken Sie dann auf **Recovery**.
   - Wenn Sie Elemente aus einem Gruppenpostfach wiederherstellen wollen, erweitern Sie den Knoten **Gruppen**, wählen Sie **Alle Gruppen**, wählen Sie diejenige Gruppe aus, in deren Postfach sich die wiederherzustellenden Elemente ursprünglich befunden haben, und klicken Sie dann auf **Recovery**.
   - Wenn der Benutzer, die Gruppe oder das freigegebene Postfach zuvor gelöscht wurde, können Sie das Element im Bereich **Cloud-Applikationen-Backups** in der Registerkarte 'Backup Storage' auswählen und dann auf **Backups anzeigen** klicken.

   Sie können Benutzer und Gruppen auch per Namen suchen. Platzhalterzeichen (Wildcards) werden nicht unterstützt.
4. Wählen Sie einen Recovery-Punkt.
5. Klicken Sie auf **Recovery** –> **E-Mail-Nachrichten**.

6. Wechseln Sie zum benötigten Ordner oder verwenden Sie die Suchfunktion, um eine Liste der erforderlichen Elemente abzurufen.

   Folgende Suchoptionen sind verfügbar. Platzhalterzeichen (Wildcards) werden nicht unterstützt.

   - Für E-Mail-Nachrichten: Suche per Betreff, Absender, Empfänger, Name des Anhangs und Datum.
   - Für Ereignisse: Suche nach Titel und Datum.
   - Für Tasks: Suche per Betreff und Datum.
   - Für Kontakte: Suche nach Namen, E-Mail-Adresse und Telefonnummer.
7. Wählen Sie die Elemente aus, die Sie wiederherstellen wollen. Wenn Sie Ordner auswählen wollen, klicken Sie auf das Symbol 'Ordner wiederherstellen'. 

   Zusätzlich haben Sie auch folgende Möglichkeiten:

   - Klicken Sie bei der Auswahl eines Elements auf **Inhalt anzeigen**, um die Inhalte (inklusive Anhänge) einsehen zu können. Klicken Sie auf den Namen einer angehängten Datei, um diese herunterzuladen.
   - Klicken Sie bei der Auswahl einer Nachricht oder eines Kalenderelements auf **Als E-Mail senden**, wenn Sie das Element an eine spezifizierte E-Mail-Adresse versenden wollen. Sie können den Absender bestimmen und einen Text schreiben, der dem weitergeleiteten Element hinzugefügt wird.
   - Nur bei einem unverschlüsselten Backup, wenn Sie die Suchfunktion verwendet und ein einzelnes Element in den Suchergebnissen ausgewählt haben: klicken Sie auf **Versionen anzeigen**, um die Version des Elements auszuwählen, die Sie wiederherstellen wollen. Sie können jede Backup-Version auswählen, auch wenn diese vor oder nach dem eigentlichen, zuvor ausgewählten Recovery-Punkt liegt.
8. Klicken Sie auf **Recovery**.
9. Wenn dem Cyber Protection Service mehrere Hosted Exchange-Organisationen hinzugefügt wurden, klicken Sie auf **Hosted Exchange-Organisation**, um die Zielorganisation einsehen, ändern oder spezifizieren zu können.

   Die ursprüngliche Organisation wird automatisch vorausgewählt. Wenn diese Organisation nicht mehr im Cyber Protection Service registriert ist, müssen Sie die Zielorganisation spezifizieren.
10. Bei**Zu Postfach wiederherstellen** können Sie das gewünschte Zielpostfach anzeigen lassen, ändern oder spezifizieren.

    Das ursprüngliche Postfach wird automatisch vorausgewählt. Wenn dieses Postfach nicht mehr existiert oder Sie eine andere als die ursprüngliche Organisation als Ziel ausgewählt haben, müssen Sie das Zielpostfach spezifizieren.
11. [Nur bei Wiederherstellung zu einem Benutzerpostfach oder freigegebenen Postfach] Bei **Pfad** können Sie den Zielordner im Zielpostfach einsehen oder ändern. Standardmäßig ist der Ordner **Wiederhergestellte Elemente** vorausgewählt.

    Gruppenpostfachelemente werden immer im Ordner **Posteingang** wiederhergestellt.
12. Klicken Sie auf **Recovery starten**.
13. Wählen Sie eine dieser Überschreiben-Optionen:

- **Vorhandene Elemente überschreiben**
- **Vorhandene Elemente nicht überschreiben**

14. Klicken Sie auf **Forsetzen**, um Ihre Entscheidung zu bestätigen.

Microsoft 365-Daten sichern

Warum sollten Sie Microsoft 365-Daten per Backup sichern?

Microsoft 365 ist zwar ein Set von Cloud-Diensten, ein regelmäßiges Backup bietet aber eine zusätzliche Schutzebene gegen Anwenderfehler und bösartige Angriffe. Sie können gelöschte Elemente auch dann noch aus einem Backup wiederherstellen, wenn die offizielle Microsoft 365-Aufbewahrungsdauer abgelaufen ist. Zusätzlich können Sie eine lokale Kopie Ihrer Exchange Online-Postfächer speichern, falls Sie dies aufgrund von gesetzlichen oder firmeninternen Vorschriften tun müssen.

Die Backup-Daten werden automatisch komprimiert und benötigen daher am Backup-Speicherort weniger Platz als am ursprünglichen Speicherort. Der Komprimierungsgrad für Cloud-zu-Cloud-Backups ist fest eingestellt und entspricht dem Komprimierungsgrad **Normal** von Nicht-Cloud-zu-Cloud-Backups. Weitere Informationen über diese Komprimierungsgrade finden Sie im Abschnitt '"Komprimierungsgrad" (S. 502)'.

Cloud Agent und lokaler Agent

Für Microsoft 365-Workloads sind zwei Agenten verfügbar:

- Der Cloud Agent

  Der Cloud Agent bietet eine erweiterte Backup-Funktionalität, die direkt über die Cyber Protect-Konsole zugänglich ist. Es ist keine Installation erforderlich. Weitere Informationen finden Sie im Abschnitt '"Den Cloud Agenten für Microsoft 365 verwenden" (S. 664)'.
- Der lokale Agent

  Der lokale Agent ermöglicht nur das Sichern von Exchange Online-Postfächern. Dieser Agent muss auf einer Windows-Maschine installiert werden, die mit dem Internet verbunden ist. Weitere Informationen finden Sie im Abschnitt '"Den lokal installierten Agenten für Office 365 verwenden" (S. 659)'.

Azure Information Protection (AIP) wird mit beiden Agenten unterstützt.

Hinweis
Für Mandanten im Compliance-Modus ist nur der lokale Agent verfügbar. Diese Mandanten können nur Microsoft 365-Postfächer sichern. Sie können nicht die erweiterte Funktionalität nutzen, die der Cloud Agent bereitstellt.

Die nachfolgende Tabelle fasst die jeweilige Funktionalität der Agenten zusammen.

	Lokaler Agent	Cloud Agent
Datenelemente, die per Backup gesichert werden können	**Exchange Online:** Benutzerpostfächer und freigegebene Postfächer (einschließlich der Postfächer von Benutzern mit einem Kiosk-Tarif und Postfächer mit aktiver Aufbewahrung für juristische Zwecke)	• **Exchange Online**: ◦ Benutzerpostfächer und freigegebene Postfächer (einschließlich der Postfächer von Benutzern mit einem Kiosk-Tarif und Postfächer mit aktiver Aufbewahrung für juristische Zwecke) ◦ Gruppenpostfächer ◦ Öffentliche Ordner • **OneDrive**: Benutzer-Dateien und -Ordner • **SharePoint Online**: ◦ Klassische Website-Sammlungen ◦ Gruppen-(Team)-Websites ◦ Kommunikations-Websites ◦ einzelne Datenelemente • **Microsoft 365-Teams**: ◦ komplette Teams ◦ Team-Kanäle ◦ Kanaldateien ◦ Team-Postfächer ◦ Dateien und E-Mail-Nachrichten in Team-Postfächern ◦ Besprechungen ◦ Team-Websites • **OneNote-Notizbüchern**: als Bestandteil von OneDrive-, SharePoint Online- und Microsoft 365 Teams-Backups
Backup von Archivpostfächern (**In-Situ-Archiv**)	Nein	Ja
Backup-Planung	Benutzerdefiniert	Bis zu sechsmal pro Tag*
Backup-Speicherorte	Cloud Storage, lokaler Ordner, Netzwerkordner	Nur Cloud Storage (einschließlich Partner Hosted Storage)

	Lokaler Agent	Cloud Agent
Automatischer Schutz für neue Microsoft 365-Benutzer, -Gruppen, -Websites und -Teams	Nein	Ja, indem Sie einen Schutzplan auf die Gruppen **Alle Benutzer**, **Alle Gruppen**, **Alle Websites** und **Alle Teams** anwenden.
Mehr als eine Microsoft 365-Organisation sichern	Nein	Ja
Granulares Recovery	Ja	Ja
Wiederherstellung zu einem anderen Benutzer innerhalb einer Organisation	Ja	Ja
Wiederherstellung zu einer anderen Organisation	Nein	Ja
Wiederherstellung zu einem lokalen Microsoft Exchange Server	Nein	Nein
Maximale Anzahl von Elementen, die ohne Performanceverlust gesichert werden können	Wenn Sie den Cloud Storage als Backup-Ziel verwenden: 5000 Postfächer pro Unternehmen Wenn andere Speicherorte als Backup-Ziel dienen: 2000 Postfächer pro Schutzplan (ohne Beschränkung der Anzahl der Postfächer pro Unternehmen)	10,000 gesicherte Elemente (Postfächer, OneDrives oder Websites) pro Unternehmen**
Maximale Anzahl von manuellen Backup-Ausführungen	Nein	10 manuelle Ausführungen in einer Stunde
Maximale Anzahl von gleichzeitigen Recovery-Aktionen	Nein	10 Aktionen, einschließlich Google Workspace-Wiederherstellungsaktionen

* Die Standardoption ist **Einmal täglich**. Mit dem Advanced Backup-Paket können Sie bis zu sechs Backups pro Tag planen. Die Backups werden in ungefähren Intervallen gestartet, die davon abhängen, wie hoch die aktuelle Auslastung des Cloud Agenten ist, der in einem Datacenter mehrere Kunden bedient. Dadurch wird gewährleistet, dass es während des Tages zu einer gleichmäßigen Auslastung kommt und alle Kunden die gleiche Service-Qualität erhalten.

Hinweis
Die Planung für den Schutz kann durch Aktionen und Einstellungen von Drittthersteller-Diensten beeinflusst werden – beispielsweise die Verfügbarkeit von Microsoft 365-Servern, den Drosselungseinstellungen auf den Microsoft-Servern und ähnlichem. Zu weiteren Informationen siehe https://docs.microsoft.com/de-de/graph/throttling.

** Wir empfohlen, dass Sie Ihre geschützten Elemente schrittweise und in dieser Reihenfolge sichern:

1. Postfächer.
2. Nachdem alle Postfächer gesichert wurden, können den OneDrives fortfahren.
3. Nachdem das OneDrive-Backup abgeschlossen wurde, können Sie mit den SharePoint Online-Websites fortfahren.

Das erste vollständige Backup kann mehrere Tage dauern, je nach Anzahl der geschützten Elemente und deren Größe.

Erforderliche Benutzerrechte

In Cyber Protection

Der lokale Agent muss unter dem Konto eines Firmenadministrators registriert sein und auf der Kunden-Mandanten-Ebene verwendet werden. Firmenadministratoren, die auf Abteilungsebene agieren, Abteilungsadministratoren und Benutzer können keine Backups oder Wiederherstellungen von Microsoft 365-Daten durchführen.

Der Cloud Agent kann sowohl auf Kunden-Mandanten- als auch auf Abteilungsebene eingesetzt werden. Weitere Informationen über diese Ebenen und ihre jeweiligen Administratoren finden Sie unter '"Microsoft 365-Organisationen verwalten, die auf verschiedenen Ebenen hinzugefügt wurden" (S. 666)'.

In Microsoft 365

Ihrem Konto muss die Rolle 'globaler Administrator' in Microsoft 365 zugewiesen sein.

Um öffentliche Microsoft 365-Ordner erkunden, sichern und wiederherstellen zu können, muss mindestens eines Ihrer Microsoft 365-Administratorkonten über ein Postfach und Lese-/Schreib-Rechte für die öffentlichen Ordner verfügen, die Sie sichern wollen.

- Der lokale Agent wird sich mit diesem Konto bei Microsoft 365 anmelden. Damit der Agent auf die Inhalte aller Postfächer zugreifen kann, wird diesem Konto die Verwaltungsrolle **ApplicationImpersonation** zugewiesen. Wenn Sie das Kennwort des Kontos ändern, müssen Sie auch das Kennwort in der Cyber Protect-Konsole aktualisieren (wie im Abschnitt '"Die Microsoft 365-Zugriffsanmeldedaten ändern" (S. 662)' beschrieben).

- Der Cloud Agent meldet sich nicht bei Microsoft 365 an. Sie müssen sich daher einmalig als globaler Administrator bei Microsoft 365 anmelden, um dem Cloud Agenten die für seine Aktion erforderlichen Berechtigungen zu gewähren.
  Folgende Berechtigungen sind in Microsoft 365 erforderlich:
  - Anmelden und Benutzerprofile lesen
  - Dateien in allen Website-Sammlungen lesen und schreiben
  - Die vollständigen Profile aller Benutzer lesen und schreiben
  - Alle Gruppen lesen und schreiben
  - Verzeichnisdaten lesen
  - Alle Kanalnachrichten lesen
  - Verwaltete Metadaten lesen und schreiben
  - Elemente und Listen in allen Website-Sammlungen lesen und schreiben
  - Volle Kontrolle über alle Website-Sammlungen haben
  - Elemente in allen Website-Sammlungen lesen und schreiben
  - Exchange-Webdienste mit vollem Zugriff auf alle Postfächer verwenden
- Der Cloud Agent speichert Ihre Kontoanmeldedaten nicht und verwendet diese beim Durchführen von Backups und Wiederherstellungen nicht. Wenn Sie die Anmeldedaten ändern oder das Konto deaktivieren bzw. löschen, hat dies keine Auswirkungen auf die Aktionen des Cloud Agenten.

Einschränkungen

- Mit dem lokalen Agenten können Sie bis zu 5000 Workloads schützen. Mit dem Cloud Agenten können Sie bis zu 50000 Workloads schützen.
- Alle Benutzer mit einem Postfach oder OneDrive werden in der Cyber Protect-Konsole angezeigt – einschließlich solcher Benutzer, die keine Microsoft 365-Lizenz haben, und Benutzer, deren Anmeldung an den Microsoft 365-Diensten blockiert wurde.
- Ein Postfach-Backup umfasst nur Order, die für Benutzer sichtbar sind. Der Ordner **Wiederherstellbare Elemente** und seine Unterordner (**Löschungen**, **Versionen**, **Säuberungen**, **Überwachungen**, **DiscoveryHolds**, **Kalenderprotokollierung**) werden nicht in ein Postfach-Backup eingeschlossen.
- Eine automatische Erstellung von Benutzern, öffentlichen Ordnern, Gruppen oder Websites während einer Wiederherstellung ist nicht möglich. Wenn Sie z.B. eine gelöschte SharePoint Online-Website wiederherstellen wollen, erstellen Sie zuerst manuell eine neue Website und spezifizieren Sie diese Website dann als Ziel für eine Wiederherstellung.
- Sie können nicht gleichzeitig Elemente von verschiedenen Recovery-Punkten wiederherstellen, auch wenn Sie solche Elemente aus den Suchergebnissen auswählen können.
- Während eines Backups bleiben alle Vertraulichkeitsbezeichnungen erhalten, die auf den Inhalt angewendet wurden. Daher werden vertrauliche Inhalte möglicherweise nicht angezeigt, wenn diese an einem anderen als dem ursprünglichen Speicherort wiederhergestellt werden und

dessen Benutzer andere Zugriffsrechte hat.

- Sie können auf denselben Workload nicht mehr als einen individuellen Backup-Plan anwenden.
- Wenn ein individueller Backup-Plan und ein Gruppen-Backup-Plan auf denselben Workload angewendet werden, haben die Einstellungen des individuellen Plans eine höhere Priorität.

Microsoft 365 Arbeitsplätze-Lizenzierungsbericht

Firmenadministratoren können einen Bericht über die geschützten Microsoft 365-Arbeitsplätze und deren Lizenzierung herunterladen. Der Bericht liegt im CSV-Format vor und enthält Informationen über den Lizenzierungsstatus eines Arbeitsplatzes sowie den Grund, warum eine Lizenz verwendet wird. Der Bericht enthält außerdem den Namen des geschützten Arbeitsplatzes, die dazugehörige E-Mail-Adresse, die Gruppe, die Microsoft 365-Organisation sowie den Namen und Typ des geschützten Workloads.

Dieser Bericht ist nur für Mandanten verfügbar, in denen eine Microsoft 365-Organisation registriert ist.

So können Sie den Lizenzierungsbericht für Microsoft 365-Arbeitsplätze herunterladen

1. Melden Sie sich als Firmenadministrator an der Cyber Protect-Konsole an.
2. Klicken Sie in der rechten oberen Ecke auf das Symbol für 'Konto'.
3. Klicken Sie auf **Microsoft 365 Arbeitsplätze-Lizenzierungsbericht**.

Protokollierung

Aktionen mit Cloud-zu-Cloud-Ressourcen (wie das Anzeigen der Inhalte von gesicherten E-Mails, das Herunterladen von Anhängen oder Dateien, das Wiederherstellen von E-Mails zu anderen als den ursprünglichen Postfächern oder das Versenden der Inhalte als E-Mail) können die Datenschutzrechte des Benutzers verletzen. Solche Aktionen werden im Management-Portal im **Monitoring** –> **Überwachungsprotokoll** protokolliert.

Den lokal installierten Agenten für Office 365 verwenden

Eine Microsoft 365-Organisation hinzufügen

So können Sie eine Microsoft 365-Organisation hinzufügen

1. Melden Sie sich als Firmenadministrator an der Cyber Protect-Konsole an.
2. Klicken Sie in der rechten oberen Ecke auf das Symbol für 'Konto' und anschließend auf die Befehle **Downloads** –> **Agent für Office 365**.
3. Laden Sie den Agenten herunter und installieren Sie ihn auf einer Windows-Maschine, die mit dem Internet verbunden ist.
4. Gehen Sie in der Konsole von Cyber Protect zu **Geräte** –> **Microsoft Office 365 (Lokaler Agent)**.

5. Geben Sie im sich öffnenden Fenster Ihre Anwendungs-ID, das Anwendungsgeheimnis und die Microsoft 365-Mandanten-ID ein. Weitere Informationen dazu, wie Sie diese finden, sind im Abschnitt '"Anwendungs-ID und Anwendungsgeheimnis abrufen" (S. 660)' aufgeführt.
6. Klicken Sie auf **OK**.

Als Ergebnis erscheinen die Datenelemente Ihrer Organisation in der Konsole von Cyber Protect auf der Registerkarte **Microsoft Office 365 (Lokaler Agent)**.

Wichtig
Innerhalb einer Organisation (Firmen-Gruppe) darf es nur einen lokal installierten Agenten für Office 365 geben.

Anwendungs-ID und Anwendungsgeheimnis abrufen

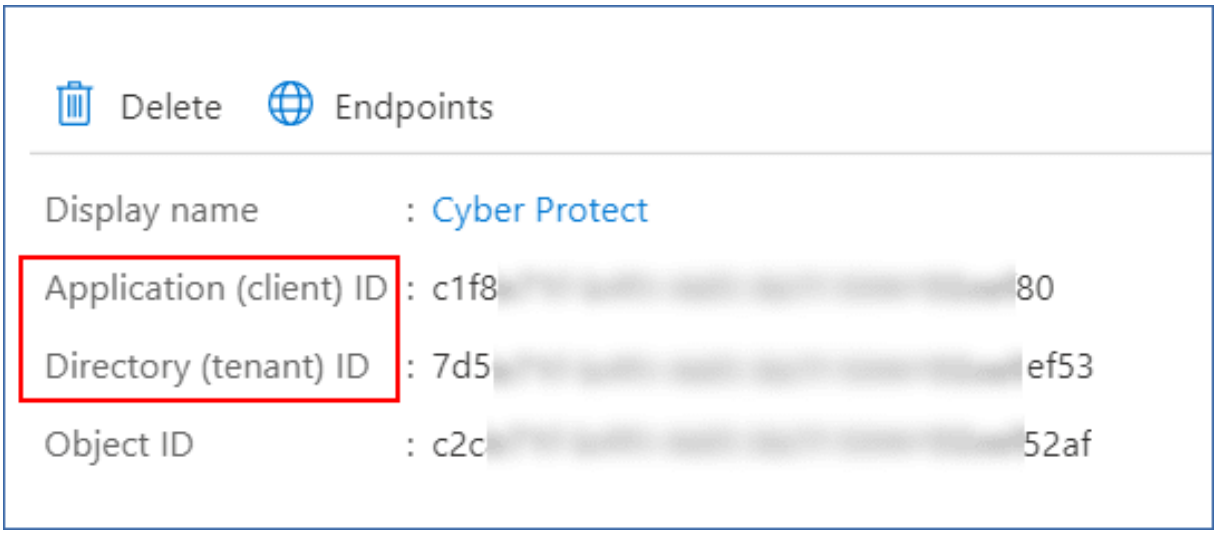
Um die moderne Authentifizierung für Microsoft 365 verwenden zu können, müssen Sie eine benutzerdefinierte Anwendung im Entra Admin Center erstellen und dieser spezifische API-Berechtigungen gewähren. Dadurch erhalten Sie die **Anwendungs-ID**, das **Anwendungsgeheimnis** und **Verzeichnis-(Mandanten)-ID**, die Sie in die Konsole von Cyber Protect eingeben müssen.

Hinweis
Stellen Sie auf der Maschine, auf der Agent für Office 365 installiert ist, sicher, dass Sie den Zugriff auf graph.microsoft.com über den Port 443 erlauben.

So können Sie eine Anwendung im Entra Admin Center erstellen

1. Melden Sie sich als Administrator im Entra Admin Center an.
2. Gehen Sie zu **Azure Active Directory** –> **App-Registrierungen** und klicken Sie dann auf **Neue Registrierung**.
3. Spezifizieren Sie einen Namen für Ihre benutzerdefinierte Anwendung – beispielsweise: Cyber Protection.
4. Wählen Sie bei **Unterstützte Kontotypen** die Option **Nur Konten in diesem Organisationsverzeichnis**.
5. Klicken Sie auf **Registrieren**.

Ihre Anwendung ist jetzt erstellt. Navigieren Sie im Entra Admin Center zur Seite **Überblick** Ihrer Anwendung und überprüfen Sie Ihre Anwendungs-(Client)-ID und Verzeichis-(Mandanten)-ID.



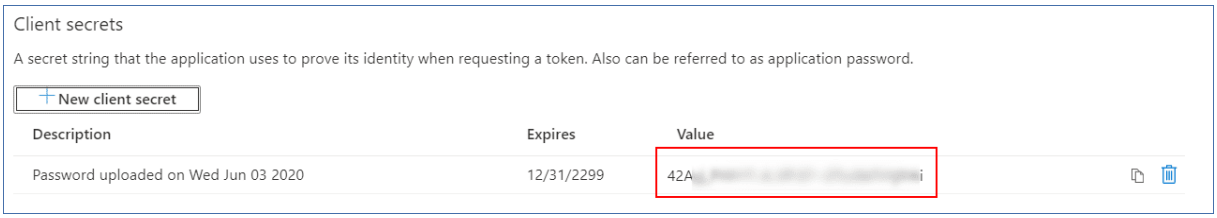
Weitere Informationen darüber, wie Sie eine Anwendung im Entra Admin Center erstellen, finden Sie in der Microsoft-Dokumentation.

So können Sie Ihrer Anwendung die erforderlichen API-Berechtigungen erteilen

1. Gehen Sie im Entra Admin Center zu den **API-Berechtigungen** der Anwendung und klicken Sie auf **Eine Berechtigung hinzufügen**.
2. Wählen Sie die Registerkarte **APIs, die mein Unternehmen verwendet** aus und suchen Sie dann nach **Office 365 Exchange Online**.
3. Klicken Sie zuerst auf **Office 365 Exchange Online** und anschließend auf **Anwendungsberechtigungen**.
4. Aktiveren Sie das Kontrollkästchen **full_access_as_app** (Vollzugriff_als_App) und klicken Sie dann auf **Berechtigungen hinzufügen**.
5. Klicken Sie bei **API-Berechtigungen** auf **Eine Berechtigung hinzufügen**.
6. Wählen Sie **Microsoft Graph**.
7. Wählen Sie **Anwendungsberechtigungen**.
8. Erweitern Sie die Registerkarte **Verzeichnis** und aktivieren Sie das Kontrollkästchen **Directory.Read.All** (Verzeichnis.Lesen.Alles). Klicken Sie auf **Berechtigungen hinzufügen**.
9. Aktivieren Sie alle Berechtigungen und klicken Sie dann auf **Administratoreinwilligung gewähren für <Name Ihrer Anwendung>**.
10. Bestätigen Sie Ihre Wahl durch Klicken auf **Ja**.

So können Sie ein Anwendungsgeheimnis erstellen

1. Gehen Sie im Entra Admin Center zum Bereich **Zertifikate & Geheimnisse** –> **Neuer geheimer Clientschlüssel** für Ihre Anwendung.
2. Wählen Sie in dem sich öffnenden Dialogfeld die Option 'Gültig bis': **Nie** – und klicken Sie dann auf **Hinzufügen**.
3. Überprüfen Sie Ihr Anwendungsgeheimnis im Feld **Wert** und stellen Sie sicher, dass Sie sich dieses merken.



Weitere Informationen über das Anwendungsgeheimnis finden Sie in der Microsoft-Dokumentation.

Die Microsoft 365-Zugriffsanmeldedaten ändern

Sie können die Zugriffsanmeldedaten für Microsoft 365 ändern, ohne den Agenten neu installieren zu müssen.

So können Sie die Anmeldedaten für Microsoft 365 ändern

1. Klicken Sie auf **Geräte** –> **Microsoft Office 365 (Lokaler Agent)**.
2. Wählen Sie die Microsoft 365-Organisation aus.
3. Klicken Sie auf **Anmeldedaten spezifizieren**.
4. Geben Sie Ihre Anwendungs-ID, das Anwendungsgeheimnis und die Microsoft 365-Mandanten-ID ein. Wie Sie diese ermitteln können, wird im Abschnitt '"Anwendungs-ID und Anwendungsgeheimnis abrufen" (S. 660)' erläutert.
5. Klicken Sie auf **OK**.

Exchange Online-Postfächer sichern

Welche Elemente können per Backup gesichert werden?

Sie können Benutzerpostfächer und freigegebene Postfächer sichern. Gruppen- und Archivpostfächer (**In-Situ-Archiv**) können nicht gesichert werden.

Welche Elemente können wiederhergestellt werden?

Folgende Elemente können aus einem Postfach-Backup wiederhergestellt werden:

- Postfächer
- E-Mail-Ordner
- E-Mail-Nachrichten
- Kalenderereignisse
- Aufgaben
- Kontakte
- Journal-Einträge
- Hinweise

Sie können eine Suchfunktion verwenden, um bestimmte Elemente zu finden.

Wenn bei einer Postfach-Wiederherstellung ein vorhandenes Postfach als Ziel ausgewählt wird, werden alle dort vorliegenden Elemente, die übereinstimmende IDs haben, überschrieben.

Bei einer Wiederherstellung von Postfachelementen werden keinerlei Elemente überschrieben. Stattdessen wird der vollständige Pfad zu einem Postfachelement im Zielordner neu erstellt.

Microsoft 365-Postfächer auswählen

Wählen Sie die Postfächer wie nachfolgend beschrieben aus – und spezifizieren Sie dann die anderen Einstellungen des Schutzplans nach Bedarf.

So können Sie Postfächer auswählen

1. Klicken Sie auf **Microsoft Office 365 (Lokaler Agent)**.
2. Wählen Sie die Postfächer aus, die Sie per Backup sichern wollen.
3. Klicken Sie auf **Backup**.

Postfächer und Postfachelemente wiederherstellen

Postfächer wiederherstellen

1. Klicken Sie auf **Microsoft Office 365 (Lokaler Agent)**.
2. Wählen Sie das wiederherzustellende Postfach und klicken Sie dann auf **Recovery**.
   Sie können die Postfächer nach einem Namen durchsuchen. Platzhalterzeichen (Wildcards) werden nicht unterstützt.
   Falls das Postfach gelöscht wurde, wählen Sie es in der Registerkarte 'Backup Storage' aus – und klicken Sie dann auf **Backups anzeigen**.
3. Wählen Sie einen Recovery-Punkt. Beachten Sie dabei, dass Recovery-Punkte nach Speicherorten gefiltert werden.
4. Klicken Sie auf **Recovery** –> **Postfach**.
5. Bei **Zielpostfach** können Sie das gewünschte Zielpostfach anzeigen lassen, ändern oder spezifizieren.
   Das ursprüngliche Postfach wird automatisch vorausgewählt. Sollte dieses Postfach nicht existieren, müssen Sie das Zielpostfach spezifizieren.
6. Klicken Sie auf **Recovery starten**.

Postfachelemente wiederherstellen

1. Klicken Sie auf **Microsoft Office 365 (Lokaler Agent)**.
2. Wählen Sie dasjenige Postfach aus, in dem sich die wiederherzustellenden Elemente ursprünglich befunden haben – und klicken Sie dann auf **Recovery**.
   Sie können die Postfächer nach einem Namen durchsuchen. Platzhalterzeichen (Wildcards) werden nicht unterstützt.

Falls das Postfach gelöscht wurde, wählen Sie es in der Registerkarte 'Backup Storage' aus – und klicken Sie dann auf **Backups anzeigen**.

3. Wählen Sie einen Recovery-Punkt. Beachten Sie dabei, dass Recovery-Punkte nach Speicherorten gefiltert werden.
4. Klicken Sie auf **Recovery** –> **E-Mail-Nachrichten**.
5. Wählen Sie die Elemente aus, die Sie wiederherstellen wollen.

   Folgende Suchoptionen sind verfügbar. Platzhalterzeichen (Wildcards) werden nicht unterstützt.

   - Für E-Mail-Nachrichten: Suche per Betreff, Absender, Empfänger, Name des Anhangs und Datum.
   - Für Ereignisse: Suche nach Titel und Datum.
   - Für Tasks: Suche per Betreff und Datum.
   - Für Kontakte: Suche nach Namen, E-Mail-Adresse und Telefonnummer.

   Bei Auswahl einer E-Mail-Nachricht können Sie auf **Inhalt anzeigen** klicken, damit Ihnen die Nachricht (inkl. Anhänge) angezeigt wird.

   Hinweis
   Sie können eine angehängte Datei herunterladen, indem Sie auf deren Namen klicken.

   Wenn eine E-Mail-Nachricht ausgewählt wurde, können Sie auf **Als E-Mail senden** klicken, damit die Nachricht an eine bestimmte E-Mail-Adresse gesendet wird. Als Absender der Nachricht wird die E-Mail-Adresse Ihres Administrator-Kontos verwendet.

   Wenn Sie Ordner auswählen wollen, klicken Sie auf das Symbol 'Ordner wiederherstellen'. 
6. Klicken Sie auf **Recovery**.
7. Bei **Zielpostfach** können Sie das gewünschte Zielpostfach anzeigen lassen, ändern oder spezifizieren.

   Das ursprüngliche Postfach wird automatisch vorausgewählt. Sollte dieses Postfach nicht existieren, müssen Sie das Zielpostfach spezifizieren.
8. Klicken Sie auf **Recovery starten**.
9. Bestätigen Sie Ihre Entscheidung.

Die Postfachelemente werden immer in einem Ordner (des Zielpostfaches) mit der Bezeichnung **Wiederhergestellte Elemente** gespeichert.

Den Cloud Agenten für Microsoft 365 verwenden

Eine Microsoft 365-Organisation hinzufügen

Ein Administrator kann ein oder mehrere Microsoft 365-Organisationen zu einem Kunden-Mandanten oder zu einer Abteilung hinzufügen.

Firmenadministratoren fügen Organisationen zu Kunden-Mandanten hinzu. Abteilungs- sowie Kunden-Administratoren, die auf Abteilungsebene agieren, fügen Organisationen zu Abteilungen hinzu.

So können Sie eine Microsoft 365-Organisation hinzufügen

1. Melden Sie sich in Abhängigkeit davon, wo Sie die Organisation hinzufügen müssen, als Firmenadministrator oder als Abteilungsadministrator an der Cyber Protect-Konsole an.
2. [Für Firmenadministratoren, die auf Abteilungsebene agieren] Navigieren Sie im Management-Portal zu der gewünschten Abteilung.
3. Klicken Sie auf **Geräte** –> **Hinzufügen** –> **Microsoft 365 Business**.
   Die Software leitet Sie zur Microsoft 365-Anmeldeseite weiter.
4. Melden Sie sich mit den Anmeldedaten des globalen Microsoft 365-Administrators an.
   Microsoft 365 zeigt eine Liste der Berechtigungen an, die erforderlich sind, um die Daten Ihres Unternehmens sichern und wiederherstellen zu können.
5. Bestätigen Sie, dass Sie dem Cyber Protection Service diese Berechtigungen gewähren wollen.

Als Ergebnis erscheint Ihre Microsoft 365-Organisation unter der Registerkarte **Geräte** in der Cyber Protect-Konsole.

Nützliche Tipps

- Der Cloud Agent führt die Synchronisierung mit Microsoft 365 alle 24 Stunden durch, beginnend mit dem Zeitpunkt, ab dem das Unternehmen dem Cyber Protection Service hinzugefügt wurde. Wenn Sie einen Benutzer, eine Gruppe oder eine Website hinzufügen oder entfernen, wird diese Änderung nicht sofort in der Cyber Protect-Konsole angezeigt. Wenn Sie die Änderung sofort synchronisieren wollen, müssen Sie die Organisation auf der Seite **Microsoft 365** auswählen und dann auf **Aktualisieren** klicken.
  Weitere Informationen darüber, wie Sie die Ressourcen einer Microsoft 365-Organisation und der Cyber Protect-Konsole synchronisieren, finden Sie im Abschnitt '"Microsoft 365-Ressourcen erkennen" (S. 667)'.
- Wenn Sie den Gruppen **Alle Benutzer**, **Alle Gruppen** oder **Alle Websites** einen Schutzplan zugewiesen haben, werden die neu hinzugefügten Elemente erst dann in das Backup aufgenommen, wenn die Synchronisierung durchgeführt wurde.
- Gemäß den Microsoft-Richtlinien bleibt ein Benutzer, eine Gruppe oder eine Website, wenn dieser/diese aus der grafischen Benutzeroberfläche von Microsoft 365 entfernt wurde, noch einige Tage lang per API verfügbar. Während dieses Zeitraums wird das entfernte Element in der Cyber Protect-Konsole als inaktiv (ausgegraut) dargestellt und nicht per Backup gesichert. Wenn das entfernte Element auch nicht mehr per API verfügbar ist, verschwinden es ganz aus der Cyber Protect-Konsole. Dessen Backups können (sofern vorhanden) unter **Backup Storage** –> **Cloud-Applikationen-Backups** gefunden werden.

Microsoft 365-Organisationen verwalten, die auf verschiedenen Ebenen hinzugefügt wurden

Firmenadministratoren haben vollen Zugriff auf die Microsoft 365 Organisationen, die auf der Ebene des Kunden-Mandanten hinzugefügt wurden.

Firmenadministratoren haben nur begrenzten Zugriff auf die Organisationen, die zu einer Abteilung hinzugefügt wurden. In diesen Organisationen, die mit dem Abteilungsnamen in Klammern angezeigt werden, können Firmenadministratoren Folgendes tun:

- Daten aus Backups wiederherstellen.
  Firmenadministratoren können Daten zu allen Organisationen im Mandanten wiederherstellen, unabhängig von der Ebene, auf der diese Organisationen hinzugefügt wurden.
- Backups und Recovery-Punkte in Backups durchsuchen.
- Backups und Recovery-Punkte in Backups löschen.
- Alarmmeldungen und Aktivitäten anzeigen.

Firmenadministratoren, die auf der Ebene des Kunden-Mandanten agieren, können folgende Aktionen NICHT durchführen:

- Microsoft 365-Organisationen zu Abteilungen hinzufügen.
- Microsoft 365-Organisationen aus Abteilungen löschen.
- Microsoft 365-Organisationen synchronisieren, die zu einer Abteilung hinzugefügt wurden.
- Schutzpläne für Datenelemente in den Microsoft 365 Organisationen, die zu einer Abteilung hinzugefügt werden, anzeigen, erstellen, bearbeiten, löschen, anwenden, ausführen oder widerrufen.

Abteilungsadministratoren und Firmenadministratoren, die auf Abteilungsebene agieren, haben vollen Zugriff auf die Organisationen, die zu einer Abteilung hinzugefügt wurden. Sie können jedoch auf keine Ressourcen des übergeordneten Kunden-Mandanten zugreifen (auch nicht auf die Schutzpläne, die in diesem erstellt werden).

Eine Microsoft 365-Organisation löschen

Das Löschen einer Microsoft 365-Organisation hat keine Auswirkungen auf die bereits bestehenden Backups der Daten dieser Organisation. Wenn Sie diese Backups nicht mehr benötigen, sollten Sie diese zuerst entfernen. Anschließend können Sie dann die Microsoft 365-Organisation löschen. Anderenfalls werden die Backups weiter Speicherplatz in der Cloud belegen, was möglicherweise kostenpflichtig ist.

Weitere Informationen zum Löschen von Backups finden Sie in Abschnitt '"So können Sie Backups oder Backup-Archive löschen" (S. 584)'.

So können Sie eine Microsoft 365-Organisation löschen

1. Melden Sie sich in Abhängigkeit davon, wo die Organisation hinzugefügt wurde, als Firmenadministrator oder als Abteilungsadministrator an der Cyber Protect-Konsole an.
2. [Für Firmenadministratoren, die auf Abteilungsebene agieren] Navigieren Sie im Management-Portal zu der gewünschten Abteilung.
3. Gehen Sie zu **Geräte** –> **Microsoft 365**.
4. Wählen Sie die Organisation aus und klicken Sie dann auf **Gruppe löschen**.

Als Ergebnis werden alle auf diese Gruppen angewendeten Backup-Pläne widerrufen.

Sie sollten jedoch zusätzlich die Zugriffsrechte der Backup Service-Applikation auf die Microsoft 365-Organisationsdaten manuell entziehen.

So können Sie die Zugriffsrechte widerrufen

1. Melden Sie sich als globaler Administrator an Microsoft 365 an.
2. Gehen Sie zu **Admin Center** –> **Azure Active Directory** –> **Unternehmensanwendungen** –> **Alle Anwendungen**.
3. Wählen Sie die Applikation **Backup Service** und blättern Sie zu dieser runter.
4. Gehen Sie zur Registerkarte **Eigenschaften** und klicken Sie dann im Aktionsbereich auf den Befehl **Löschen**.
5. Bestätigen Sie die Löschaktion.

Als Ergebnis werden der Backup Service-Applikation die Zugriffsrechte auf die Daten der Microsoft 365-Organisation entzogen.

Microsoft 365-Ressourcen erkennen

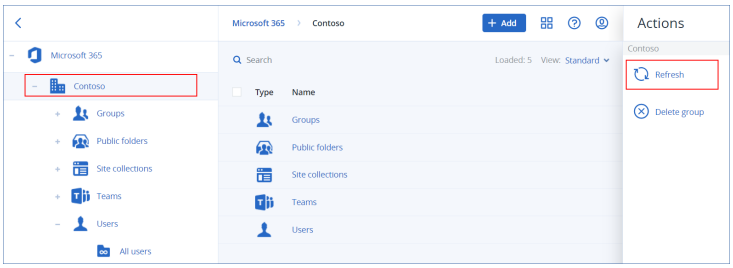
Wenn Sie dem Cyber Protection Service eine Microsoft 365-Organisation hinzufügen, werden die Ressourcen in dieser Organisation (Postfächer, OneDrive-Storages, Microsoft Teams und SharePoint-Websites) zur Cyber Protect-Konsole synchronisiert. Diese Aktion wird Erkennung (Englisch: Discovery) genannt und unter **Monitoring** –> **Aktivitäten** protokolliert.

Wenn die Erkennungsaktion abgeschlossen wurde, werden die Ressourcen der Microsoft 365-Organisation in der -Konsole auf der Registerkarte **Geräte** –> **Microsoft 365** angezeigt. Anschließend können Sie Backup-Pläne auf diese anwenden.

Eine automatische Erkennungsaktion wird einmal pro Tag ausgeführt, damit die Liste der Ressourcen in der Cyber Protect-Konsole stets auf dem neuesten Stand bleibt. Sie können diese Liste auch je nach Bedarf synchronisieren, indem Sie eine Erkennungsaktion manuell ausführen lassen.

So können Sie eine Erkennungsaktion manuell ausführen

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte** –> **Microsoft 365**.
2. Wählen Sie zuerst Ihre Microsoft 365-Organisation aus und klicken Sie anschließend im Fensterbereich **Aktionen** auf **Aktualisieren**.



Hinweis

Sie können eine Erkennungsaktion bis zu 10 Mal pro Stunde manuell ausführen. Wenn diese Anzahl erreicht ist, werden die erlaubten Ausführungen auf eine pro Stunde zurückgesetzt. Danach wird für jede Stunde eine zusätzliche Ausführung verfügbar, bis die Gesamtzahl von 10 Ausführungen pro Stunde wieder erreicht ist.

Die Häufigkeit von Microsoft 365-Backups festlegen

Microsoft 365-Backups werden standardmäßig einmal täglich ausgeführt – und es sind keine weiteren Planungsoptionen verfügbar.

Wenn das Advanced Backup-Paket in Ihrem Mandanten aktiviert ist, können Sie häufigere Backups konfigurieren. Sie können die Anzahl der Backups pro Tag festlegen, aber Sie können nicht die Startzeit der Backups konfigurieren. Die Backups werden automatisch und in ungefähren Intervallen gestartet, die wiederum davon abhängen, wie hoch die aktuelle Auslastung des Cloud Agenten ist, der in einem Datacenter mehrere Kunden bedient. Dadurch wird gewährleistet, dass es während des Tages zu einer gleichmäßigen Auslastung kommt und alle Kunden die gleiche Service-Qualität erhalten.

Folgende Optionen sind verfügbar:

Planungsoptionen	Ungefähres Intervall zwischen jedem Backup
Einmal täglich	24 Stunden
Zweimal täglich (Standard)	12 Stunden
3-mal täglich	8 Stunden
6-mal täglich	4 Stunden

Hinweis
Je nach Auslastung des Cloud Agenten und einer möglichen Drosselung auf der Seite von Microsoft 365 kann ein Backup später als geplant beginnen oder dessen Fertigstellung länger dauern. Wenn ein Backup mehr Zeit benötigt als das durchschnittliche Intervall zwischen zwei Backups lang ist, muss das nächste Backup neu geplant werden, was dazu führen kann, dass weniger Backups pro Tag erstellt werden, als es eigentlich vorgesehen ist. So kann es beispielsweise vorkommen, dass nur zwei Backups pro Tag abgeschlossen werden können, obwohl Sie sechs pro Tag eingestellt haben.

Backups von Gruppenpostfächern können nur einmal am Tag durchgeführt werden.

Exchange Online-Daten sichern

Welche Elemente können per Backup gesichert werden?

Sie können Benutzerpostfächer, freigegebene Postfächer und Gruppenpostfächer sichern. Außerdem können Sie optional auch die Online-Archivpostfächer (**In-Situ-Archiv**) der ausgewählten Postfächer sichern.

Ab Version 8.0 des Cyber Protection Service können Sie öffentliche Ordner per Backup sichern. Wenn Ihre Organisation bereits vor Veröffentlichung von Version 8.0 dem Cyber Protection Service hinzugefügt wurde, müssen Sie die Organisation erneut hinzufügen, damit Sie diese Funktionalität erhalten. Löschen Sie nicht die Organisation, sondern wiederholen Sie einfach die im Abschnitt '"Eine Microsoft 365-Organisation hinzufügen" (S. 664)' beschriebenen Schritte. Dadurch erhält der Cyber Protection Service die Berechtigung, die entsprechende API zu verwenden.

Welche Elemente können wiederhergestellt werden?

Folgende Elemente können aus einem Postfach-Backup wiederhergestellt werden:

- Postfächer
- E-Mail-Ordner
- E-Mail-Nachrichten
- Kalenderereignisse
- Aufgaben
- Kontakte
- Journal-Einträge
- Hinweise

Folgende Elemente können aus einem Öffentlicher Ordner-Backup wiederhergestellt werden:

- Unterordner
- Ihre Posts

- E-Mail-Nachrichten

Sie können eine Suchfunktion verwenden, um bestimmte Elemente zu finden.

Wenn Sie Postfächer, Postfachelemente, öffentliche Ordner oder Elemente aus öffentlichen Ordnern wiederherstellen, können Sie auswählen, ob die Elemente am Zielort überschrieben werden sollen (oder nicht).

Postfächer auswählen

Wählen Sie die Postfächer wie nachfolgend beschrieben aus – und spezifizieren Sie dann die anderen Einstellungen des Schutzplans nach Bedarf.

So können Sie Exchange Online-Postfächer auswählen

1. Klicken Sie auf **Microsoft 365**.
2. Wenn dem Cyber Protection Service mehrere Microsoft 365-Organisationen hinzugefügt wurden, wählen Sie diejenige Organisation aus, deren Benutzerdaten Sie sichern wollen. Ansonsten können Sie diesen Schritt überspringen.
3. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Um die Postfächer aller Benutzer und alle freigegegenen Postfächer zu sichern (einschließlich solcher Postfächer, die erst in der Zukunft angelegt werden), erweitern Sie den Knoten **Benutzer**, wählen Sie **Alle Benutzer** und klicken Sie dann auf **Gruppen-Backup**.
   - Wenn Sie einzelne Benutzerpostfächer oder freigegebene Postfächer sichern wollen, erweitern Sie den Knoten **Benutzer**, wählen Sie **Alle Benutzer**, wählen Sie die Benutzer aus, deren Postfächer Sie sichern wollen, und klicken Sie dann auf **Backup**.
   - Um alle Gruppenpostfächer zu sichern (einschließlich der Postfächer von Gruppen, die erst in der Zukunft angelegt werden), erweitern Sie den Knoten **Gruppen**, wählen Sie **Alle Gruppen** und klicken Sie dann auf **Gruppen-Backup**.
   - Wenn Sie einzelne Gruppenpostfächer sichern wollen, erweitern Sie den Knoten **Gruppen**, wählen Sie **Alle Gruppen**, wählen Sie die Gruppen aus, deren Postfächer Sie sichern wollen, und klicken Sie dann auf **Backup**.

     Hinweis
     Der Cloud Agent für Microsoft 365 verwendet ein Konto mit passenden Berechtigungen, um auf ein Gruppenpostfach zugreifen zu können. Um ein Gruppenpostfach sichern zu können, muss daher mindestens einer der Gruppenbesitzer ein lizenzierter Microsoft 365-Benutzer mit einem Postfach sein. Wenn die Gruppe daher 'privat' ist oder eine 'ausgeblendete Mitgliedschaft' hat, muss der Besitzer auch Mitglied der Gruppe sein.

4. Im Schutzplan-Fensterbereich:
   - Überprüfen Sie, dass das Element **Microsoft 365-Postfächer** bei **Backup-Quelle** ausgewählt ist.

     Wenn einige der individuell ausgewählten Benutzer keinen Exchange-Service in ihrem Microsoft 365-Plan enthalten haben, können Sie diese Option nicht auswählen.

Wenn einige der für ein Gruppen-Backup ausgewählten Benutzer keinen Exchange-Service in ihrem Microsoft 365-Plan enthalten haben, können Sie diese Option zwar auswählen, aber der Schutzplan wird nicht auf diese Benutzer angewendet.

- Wenn Sie keine Archivpostfächer sichern wollen, deaktivieren Sie den Schalter **Archivpostfach**.

Öffentliche Ordner auswählen

Wählen Sie die öffentlichen Ordner wie nachfolgend beschrieben aus – und spezifizieren Sie die anderen Einstellungen des Schutzplans je nach Bedarf.

Hinweis
Öffentliche Ordner verbrauchen Lizenzen aus Ihrer Backup-Quota für Microsoft 365-Arbeitsplätze.

So können Sie öffentliche Ordner von Exchange Online auswählen

1. Klicken Sie auf **Microsoft 365**.
2. Wenn dem Cyber Protection Service mehrere Microsoft 365-Organisationen hinzugefügt wurden, erweitern Sie diejenige Organisation, deren Daten Sie sichern wollen. Ansonsten können Sie diesen Schritt überspringen.
3. Erweitern Sie den Knoten **Öffentliche Ordner** und wählen Sie **Alle öffentlichen Ordner** aus.
4. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Wenn Sie alle öffentlichen Ordner sichern wollen (einschließlich öffentlicher Ordner, die erst in der Zukunft erstellt werden), klicken Sie auf **Gruppen-Backup**.
   - Wenn Sie nur bestimmte öffentliche Ordner sichern wollen, wählen Sie diejenigen öffentlichen Ordner aus, die Sie sichern wollen, und klicken Sie dann auf **Backup**.
5. Überprüfen Sie in der Schutzplan-Anzeige, dass das Element **Microsoft 365-Postfächer** bei **Backup-Quelle** ausgewählt ist.

Postfächer und Postfachelemente wiederherstellen

Postfächer wiederherstellen

1. Klicken Sie auf **Microsoft 365**.
2. Wenn dem Cyber Protection Service mehrere Microsoft 365-Organisationen hinzugefügt wurden, wählen Sie diejenige Organisation aus, deren gesicherte Daten Sie wiederherstellen wollen. Ansonsten können Sie diesen Schritt überspringen.
3. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Wenn Sie ein Benutzerpostfach wiederherstellen wollen, erweitern Sie den Knoten **Benutzer**, wählen Sie **Alle Benutzer**, wählen Sie den Benutzer aus, dessen Postfach Sie wiederherstellen wollen, und klicken Sie dann auf **Recovery**.
   - Wenn Sie ein freigegebenes Postfach wiederherstellen wollen, erweitern Sie den Knoten **Benutzer**, wählen Sie **Alle Benutzer**, wählen Sie das freigegebene Postfach aus, welches Sie wiederherstellen wollen, und klicken Sie dann auf **Recovery**.

- Wenn Sie ein Gruppenpostfach wiederherstellen wollen, erweitern Sie den Knoten **Gruppen**, wählen Sie **Alle Gruppen**, wählen Sie die Gruppe aus, deren Postfach Sie wiederherstellen wollen, und klicken Sie dann auf **Recovery**.
- Wenn der Benutzer, die Gruppe oder das freigegebene Postfach zuvor gelöscht wurde, können Sie das Element im Bereich **Cloud-Applikationen-Backups** in der Registerkarte 'Backup Storage' auswählen und dann auf **Backups anzeigen** klicken.

Sie können Benutzer und Gruppen auch per Namen suchen. Platzhalterzeichen (Wildcards) werden nicht unterstützt.

4. Wählen Sie einen Recovery-Punkt.

Hinweis
Wenn Sie nur Recovery-Punkte sehen wollen, die Postfächer enthalten, wählen Sie **Postfächer** bei **Nach Inhalt filtern**.

5. Klicken Sie auf **Recovery** –> **Komplettes Postfach**.
6. Wenn dem Cyber Protection Service mehrere Microsoft 365-Organisationen hinzugefügt werden, klicken Sie auf **Microsoft 365-Organisation**, um die Zielorganisation einsehen, ändern oder spezifizieren zu können.
   Die ursprüngliche Organisation wird automatisch vorausgewählt. Wenn diese Organisation nicht mehr im Cyber Protection Service registriert ist, müssen Sie die Zielorganisation spezifizieren.
7. Bei**Zu Postfach wiederherstellen** können Sie das gewünschte Zielpostfach anzeigen lassen, ändern oder spezifizieren.
   Das ursprüngliche Postfach wird automatisch vorausgewählt. Wenn dieses Postfach nicht mehr existiert oder Sie eine andere als die ursprüngliche Organisation als Ziel ausgewählt haben, müssen Sie das Zielpostfach spezifizieren.
   Sie können während der Wiederherstellung kein neues Zielpostfach erstellen. Um ein Postfach zu einem neuen Postfach wiederherzustellen, müssen Sie zunächst das Zielpostfach in der gewünschten Microsoft 365-Organisation erstellen und dann den Cloud Agenten die Änderung synchronisieren lassen. Der Cloud Agent synchronisiert sich automatisch alle 24 Stunden mit Microsoft 365. Um die Änderung sofort zu synchronisieren, wählen Sie in der Cyber Protect-Konsole die Organisation auf der **Microsoft 365**-Seite aus und klicken Sie dann auf **Aktualisieren**.
8. Klicken Sie auf **Recovery starten**.
9. Wählen Sie eine dieser Überschreiben-Optionen:
   - **Vorhandene Elemente überschreiben**
   - **Vorhandene Elemente nicht überschreiben**
10. Klicken Sie auf **Forsetzen**, um Ihre Entscheidung zu bestätigen.

Postfachelemente wiederherstellen

1. Klicken Sie auf **Microsoft 365**.
2. Wenn dem Cyber Protection Service mehrere Microsoft 365-Organisationen hinzugefügt wurden, wählen Sie diejenige Organisation aus, deren gesicherte Daten Sie wiederherstellen wollen. Ansonsten können Sie diesen Schritt überspringen.
3. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Wenn Sie Elemente aus einem Benutzerpostfach wiederherstellen wollen, erweitern Sie den Knoten **Benutzer**, wählen Sie **Alle Benutzer**, wählen Sie denjenigen Benutzer aus, in dessen Postfach sich die wiederherzustellenden Elemente ursprünglich befunden haben, und klicken Sie dann auf **Recovery**.
   - Wenn Sie Elemente aus einem freigegebenen Postfach wiederherstellen wollen, erweitern Sie den Knoten **Benutzer**, wählen Sie **Alle Benutzer**, wählen Sie dasjenige freigegebene Postfach aus, in welchem sich die wiederherzustellenden Elemente ursprünglich befunden haben, und klicken Sie dann auf **Recovery**.
   - Wenn Sie Elemente aus einem Gruppenpostfach wiederherstellen wollen, erweitern Sie den Knoten **Gruppen**, wählen Sie **Alle Gruppen**, wählen Sie diejenige Gruppe aus, in deren Postfach sich die wiederherzustellenden Elemente ursprünglich befunden haben, und klicken Sie dann auf **Recovery**.
   - Wenn der Benutzer, die Gruppe oder das freigegebene Postfach zuvor gelöscht wurde, können Sie das Element im Bereich **Cloud-Applikationen-Backups** in der Registerkarte 'Backup Storage' auswählen und dann auf **Backups anzeigen** klicken.

   Sie können Benutzer und Gruppen auch per Namen suchen. Platzhalterzeichen (Wildcards) werden nicht unterstützt.
4. Wählen Sie einen Recovery-Punkt.

   Hinweis
   Wenn Sie nur Recovery-Punkte sehen wollen, die Postfächer enthalten, wählen Sie **Postfächer** bei **Nach Inhalt filtern**.

5. Klicken Sie auf **Recovery** –> **E-Mail-Nachrichten**.
6. Wechseln Sie zum benötigten Ordner oder verwenden Sie die Suchfunktion, um eine Liste der erforderlichen Elemente abzurufen.

   Folgende Suchoptionen sind verfügbar. Platzhalterzeichen (Wildcards) werden nicht unterstützt.
   - Für E-Mail-Nachrichten: Suche per Betreff, Absender, Empfänger, Name des Anhangs und Datum. Sie können ein Start- oder Enddatum (beide inklusive) oder beide Daten auswählen, um innerhalb eines Zeitraums zu suchen.
   - Für Ereignisse: Suche nach Titel und Datum.
   - Für Tasks: Suche per Betreff und Datum.
   - Für Kontakte: Suche nach Namen, E-Mail-Adresse und Telefonnummer.

7. Wählen Sie die Elemente aus, die Sie wiederherstellen wollen. Wenn Sie Ordner auswählen wollen, klicken Sie auf das Symbol 'Ordner wiederherstellen'. 

   Sie können während der Wiederherstellung kein neues Zielpostfach erstellen. Um ein neues Postfach-Element in einem neuen Postfach wiederherzustellen, müssen Sie zunächst das neue Ziel-Postfach-Element in der Microsoft 365-Organisation erstellen und dann den Cloud Agenten die Änderung synchronisieren lassen. Der Cloud Agent synchronisiert sich automatisch alle 24 Stunden mit Microsoft 365. Um die Änderung sofort zu synchronisieren, wählen Sie in der Cyber Protect-Konsole die Organisation auf der **Microsoft 365**-Seite aus und klicken Sie dann auf **Aktualisieren**.

   Zusätzlich haben Sie auch folgende Möglichkeiten:

   - Wenn ein Element ausgewählt ist, klicken Sie auf **Inhalt anzeigen**, um dessen Inhalte (einschließlich Anhänge) einzusehen. Klicken Sie auf den Namen einer angehängten Datei, um diese herunterzuladen.
   - Klicken Sie bei der Auswahl einer Nachricht oder eines Kalenderelements auf **Als E-Mail senden**, wenn Sie das Element an eine spezifizierte E-Mail-Adresse versenden wollen. Sie können den Absender bestimmen und einen Text schreiben, der dem weitergeleiteten Element hinzugefügt wird.
   - Nur bei einem unverschlüsselten Backup, wenn Sie die Suchfunktion verwendet und ein einzelnes Element in den Suchergebnissen ausgewählt haben: klicken Sie auf **Versionen anzeigen**, um die Version des Elements auszuwählen, die Sie wiederherstellen wollen. Sie können jede Backup-Version auswählen, auch wenn diese vor oder nach dem eigentlichen, zuvor ausgewählten Recovery-Punkt liegt.
8. Klicken Sie auf **Recovery**.
9. Wenn dem Cyber Protection Service mehrere Microsoft 365-Organisationen hinzugefügt wurden, klicken Sie auf **Microsoft 365-Organisation**, um die Zielorganisation einsehen, ändern oder spezifizieren zu können.

   Die ursprüngliche Organisation wird automatisch vorausgewählt. Wenn diese Organisation nicht mehr im Cyber Protection Service registriert ist, müssen Sie die Zielorganisation spezifizieren.
10. Bei**Zu Postfach wiederherstellen** können Sie das gewünschte Zielpostfach anzeigen lassen, ändern oder spezifizieren.

    Das ursprüngliche Postfach wird automatisch vorausgewählt. Wenn dieses Postfach nicht mehr existiert oder Sie eine andere als die ursprüngliche Organisation als Ziel ausgewählt haben, müssen Sie das Zielpostfach spezifizieren.
11. [Nur bei Wiederherstellung zu einem Benutzerpostfach oder freigegebenen Postfach] Bei **Pfad** können Sie den Zielordner im Zielpostfach einsehen oder ändern. Standardmäßig ist der Ordner **Wiederhergestellte Elemente** vorausgewählt.

    Gruppenpostfachelemente werden immer im Ordner **Posteingang** wiederhergestellt.
12. Klicken Sie auf **Recovery starten**.
13. Wählen Sie eine dieser Überschreiben-Optionen:

- **Vorhandene Elemente überschreiben**
- **Vorhandene Elemente nicht überschreiben**

14. Klicken Sie auf **Forsetzen**, um Ihre Entscheidung zu bestätigen.

Komplette Postfächer zu PST-Dateien wiederherstellen

Hinweis
Das In-Situ-Archiv kann nicht als Teil der Wiederherstellung in PST-Dateien wiederhergestellt werden. Wie Sie das In-Situ-Archiv zusammen mit dem Postfach wiederherstellen können, erfahren Sie unter "Postfächer wiederherstellen" (S. 671).

So können ein Postfach wiederherstellen

1. Klicken Sie auf **Microsoft 365**.
2. Wenn dem Cyber Protection Service mehrere Microsoft 365-Organisationen hinzugefügt wurden, wählen Sie diejenige Organisation aus, deren gesicherte Daten Sie wiederherstellen wollen. Ansonsten können Sie diesen Schritt überspringen.
3. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Wenn Sie ein Benutzerpostfach als PST-Datendatei wiederherstellen wollen, erweitern Sie zuerst den Knoten **Benutzer**. Wählen Sie anschließend **Alle Benutzer** sowie darauf folgend das wiederherzustellende Postfach aus – und klicken Sie dann abschließend auf **Recovery**.
   - Wenn Sie ein freigegebenes Benutzerpostfach als PST-Datendatei wiederherstellen wollen, erweitern Sie zuerst den Knoten **Benutzer**. Wählen Sie anschließend **Alle Benutzer** sowie darauf folgend das wiederherzustellende Postfach aus – und klicken Sie dann abschließend auf **Recovery**.
   - Wenn Sie ein Gruppenpostfach zu einer PST-Datendatei wiederherstellen wollen, erweitern Sie zuerst den Knoten **Gruppen**. Wählen Sie anschließend **Alle Gruppen** sowie darauf folgend die Gruppe aus, deren Postfach sie wiederherstellen wollen – und klicken Sie dann abschließend auf **Recovery**.

   Sie können Benutzer und Gruppen auch per Namen suchen. Platzhalterzeichen (Wildcards) werden nicht unterstützt.

   Wenn der Benutzer, die Gruppe oder die freigegebene Outlook-Datendatei zuvor gelöscht wurde, können Sie das Element im Bereich **Cloud-Applikationen-Backups** in der Registerkarte 'Backup Storage' auswählen und dann auf **Backups anzeigen** klicken.
4. Klicken Sie auf **Recovery** –> **Als PST-Dateien**.
5. Legen Sie das Kennwort fest, um das Archiv mit den PST-Dateien zu verschlüsseln.
   Das Kennwort muss mindestens ein Zeichen enthalten.
6. Bestätigen Sie das Kennwort und klicken Sie dann auf **Fertig**.
7. Die ausgewählten Postfach-Elemente werden als PST-Datendateien wiederhergestellt und im ZIP-Format archiviert. Die maximale Größe einer einzelnen PST-Datei ist auf 2 GB begrenzt. Wenn die wiederherzustellenden Daten also 2 GB überschreiten, werden sie auf mehrere PST-Dateien aufgeteilt. Das ZIP-Archiv wird mit dem von Ihnen festgelegten Kennwort geschützt.

8. Sie werden eine E-Mail mit einem Link erhalten, der auf ein ZIP-Archiv mit den erstellten PST-Dateien verweist.
9. Der Administrator wird per E-Mail benachrichtigt, dass Sie die Recovery-Prozedur durchgeführt haben.

Hinweis
Die Wiederherstellung von Postfächern zu PST-Dateien kann zeitaufwendig sein, da dabei nicht nur Daten übertragen, sondern auch Daten mithilfe komplexer Algorithmen umgewandelt werden müssen.

So können Sie das Archiv mit den PST-Dateien herunterladen und die Wiederherstellung abschließen

1. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Folgen Sie dem Link **Dateien herunterladen**, um das Archiv aus der E-Mail herunterzuladen. Das Archiv steht 24 Stunden lang zum Download bereit. Sollte der Link abgelaufen sein, wiederholen Sie die Recovery-Prozedur.
   - So können Sie das Archiv über die Cyber Protect-Konsole herunterladen:
     a. Gehen Sie zu **Backup Storage** –> **PST-Dateien**.
     b. Wählen Sie das letzte hervorgehobene Archiv aus.
     c. Klicken Sie im rechten Fensterbereich auf **Download**.

   Das Archiv wird in das Standard-Download-Verzeichnis auf Ihrem Computer heruntergeladen.
2. Extrahieren Sie die PST-Dateien aus dem Archiv unter Verwendung des Kennworts, das Sie zur Verschlüsselung des Archivs festgelegt haben.
3. Öffnen Sie die PST-Dateien mit Microsoft Outlook.
   Die resultierenden PST-Dateien könnten viel kleiner sein als das ursprüngliche Postfach. Das ist normal.

   Wichtig
   Sie dürfen diese Dateien nicht über den **Import- und Export-Assistenten** in Microsoft Outlook importieren.
   Öffnen Sie die Dateien, indem Sie doppelt auf diese klicken oder indem Sie mit der rechten Maustaste auf die Dateien klicken und dann im Kontextmenü die Befehle **Öffnen mit...** –> **Microsoft Outlook** wählen.

Postfach-Elemente zu PST-Dateien wiederherstellen

Hinweis
Das In-Situ-Archiv kann nicht als Teil der Wiederherstellung in PST-Dateien wiederhergestellt werden. Wie Sie das In-Situ-Archiv zusammen mit dem Postfach wiederherstellen können, erfahren Sie unter "Postfächer wiederherstellen" (S. 671).

So können Sie Postfach-Elemente wiederherstellen

1. Klicken Sie auf **Microsoft 365**.
2. Wenn dem Cyber Protection Service mehrere Microsoft 365-Organisationen hinzugefügt wurden, wählen Sie diejenige Organisation aus, deren gesicherte Daten Sie wiederherstellen wollen. Ansonsten können Sie diesen Schritt überspringen.
3. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Wenn Sie Elemente aus einem Benutzerpostfach wiederherstellen wollen, erweitern Sie den Knoten **Benutzer**, wählen Sie **Alle Benutzer**, wählen Sie denjenigen Benutzer aus, in dessen Postfach sich die wiederherzustellenden Elemente ursprünglich befunden haben, und klicken Sie dann auf **Recovery**.
   - Wenn Sie Elemente aus einem freigegebenen Postfach wiederherstellen wollen, erweitern Sie den Knoten **Benutzer**, wählen Sie **Alle Benutzer**, wählen Sie dasjenige freigegebene Postfach aus, in welchem sich die wiederherzustellenden Elemente ursprünglich befunden haben, und klicken Sie dann auf **Recovery**.
   - Wenn Sie Elemente aus einem Gruppenpostfach wiederherstellen wollen, erweitern Sie den Knoten **Gruppen**, wählen Sie **Alle Gruppen**, wählen Sie diejenige Gruppe aus, in deren Postfach sich die wiederherzustellenden Elemente ursprünglich befunden haben, und klicken Sie dann auf **Recovery**.
   - Wenn der Benutzer, die Gruppe oder das freigegebene Postfach zuvor gelöscht wurde, können Sie das Element im Bereich **Cloud-Applikationen-Backups** in der Registerkarte 'Backup Storage' auswählen und dann auf **Backups anzeigen** klicken.

   Sie können Benutzer und Gruppen auch per Namen suchen. Platzhalterzeichen (Wildcards) werden nicht unterstützt.
4. Klicken Sie auf **Recovery** –> **E-Mail-Nachrichten**.
5. Wechseln Sie zum benötigten Ordner oder verwenden Sie die Suchfunktion, um eine Liste der erforderlichen Elemente abzurufen.

   Folgende Suchoptionen sind verfügbar. Platzhalterzeichen (Wildcards) werden nicht unterstützt.
   - Für E-Mail-Nachrichten: Suche per Betreff, Absender, Empfänger, Name des Anhangs und Datum.
   - Für Ereignisse: Suche nach Titel und Datum.
   - Für Tasks: Suche per Betreff und Datum.
   - Für Kontakte: Suche nach Namen, E-Mail-Adresse und Telefonnummer.
6. Wählen Sie die Elemente aus, die Sie wiederherstellen wollen. Wenn Sie Ordner auswählen wollen, klicken Sie auf das Symbol 'Ordner wiederherstellen'. 

   Zusätzlich haben Sie auch folgende Möglichkeiten:
   - Klicken Sie bei der Auswahl eines Elements auf **Inhalt anzeigen**, um die Inhalte (inklusive Anhänge) einsehen zu können. Klicken Sie auf den Namen einer angehängten Datei, um diese herunterzuladen.
   - Klicken Sie bei der Auswahl einer Nachricht oder eines Kalenderelements auf **Als E-Mail senden**, wenn Sie das Element an eine spezifizierte E-Mail-Adresse versenden wollen. Sie

können den Absender bestimmen und einen Text schreiben, der dem weitergeleiteten Element hinzugefügt wird.

- Nur bei einem unverschlüsselten Backup, wenn Sie die Suchfunktion verwendet und ein einzelnes Element in den Suchergebnissen ausgewählt haben: klicken Sie auf **Versionen anzeigen**, um die Version des Elements auszuwählen, die Sie wiederherstellen wollen. Sie können jede Backup-Version auswählen, auch wenn diese vor oder nach dem eigentlichen, zuvor ausgewählten Recovery-Punkt liegt.

7. Klicken Sie auf **Als PST-Dateien wiederherstellen**.
8. Legen Sie das Kennwort fest, um das Archiv mit den PST-Dateien zu verschlüsseln.
   Das Kennwort muss mindestens ein Zeichen enthalten.
9. Bestätigen Sie das Kennwort und klicken Sie dann auf **FERTIG**.

Die ausgewählten Postfach-Elemente werden als PST-Datendateien wiederhergestellt und im ZIP-Format archiviert. Die maximale Größe einer einzelnen PST-Datei ist auf 2 GB begrenzt. Wenn die wiederherzustellenden Daten also 2 GB überschreiten, werden sie auf mehrere PST-Dateien aufgeteilt. Das ZIP-Archiv wird mit dem von Ihnen festgelegten Kennwort geschützt.

Sie werden eine E-Mail mit einem Link erhalten, der auf ein ZIP-Archiv mit den erstellten PST-Dateien verweist.

Der Administrator wird per E-Mail benachrichtigt, dass Sie die Recovery-Prozedur durchgeführt haben.

So können Sie das Archiv mit den PST-Dateien herunterladen und die Wiederherstellung abschließen

1. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Folgen Sie dem Link **Dateien herunterladen**, um das Archiv aus der E-Mail herunterzuladen. Das Archiv steht 24 Stunden lang zum Download bereit. Sollte der Link abgelaufen sein, wiederholen Sie die Recovery-Prozedur.
   - So können Sie das Archiv über die Cyber Protect-Konsole herunterladen:
     a. Gehen Sie zu **Backup Storage** –> **PST-Dateien**.
     b. Wählen Sie das letzte hervorgehobene Archiv aus.
     c. Klicken Sie im rechten Fensterbereich auf **Download**.

   Das Archiv wird in das Standard-Download-Verzeichnis auf Ihrem Computer heruntergeladen.
2. Extrahieren Sie die PST-Dateien aus dem Archiv unter Verwendung des Kennworts, das Sie zur Verschlüsselung des Archivs festgelegt haben.
3. Öffnen Sie die PST-Dateien mit Microsoft Outlook.
   Die resultierenden PST-Dateien könnten viel kleiner sein als das ursprüngliche Postfach. Das ist normal.

Wichtig
Sie dürfen diese Dateien nicht über den **Import- und Export-Assistenten** in Microsoft Outlook importieren.
Öffnen Sie die Dateien, indem Sie doppelt auf diese klicken oder indem Sie mit der rechten Maustaste auf die Dateien klicken und dann im Kontextmenü die Befehle **Öffnen mit...** –> **Microsoft Outlook** wählen.

Öffentliche Ordner und Ordnerelemente wiederherstellen

Um einen öffentlichen Ordner oder einzelne Elemente eines öffentlichen Ordners wiederherzustellen, muss mindestens ein Administrator der Microsoft 365-Zielorganisation über die Berechtigung **Besitzer** für den als Recovery-Ziel dienenden öffentlichen Ordner verfügen. Wenn die Wiederherstellung aufgrund eines verweigerten Zugriffs fehlschlägt, müssen Sie dem Zielordner (über dessen Eigenschaften) diese Berechtigung zuweisen, die Zielorganisation in der Cyber Protect-Konsole erneut auswählen, auf **Aktualisieren** klicken und dann die Wiederherstellung wiederholen.

So können Sie einen öffentlichen Ordner oder dessen Ordnerelemente wiederherstellen

1. Klicken Sie auf **Microsoft 365**.
2. Wenn dem Cyber Protection Service mehrere Microsoft 365-Organisationen hinzugefügt wurden, erweitern Sie diejenige Organisation, deren Backup-Daten Sie wiederherstellen wollen. Ansonsten können Sie diesen Schritt überspringen.
3. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Erweiteren Sie den Knoten **Öffentliche Ordner**, wählen Sie **Alle öffentlichen Ordner** aus, wählen Sie denjenigen öffentlichen Ordern aus, in welchem sich die wiederherzustellenden Elemente ursprünglich befunden haben, und klicken Sie dann auf **Recovery**.
   - Wenn der öffentliche Ordner zuvor gelöscht wurde, können Sie diese im Bereich **Cloud-Applikationen-Backups** der Registerkarte 'Backup Storage' auswählen und dann auf **Backups anzeigen** klicken.

   Sie können die öffentlichen Ordner nach einem Namen durchsuchen. Platzhalterzeichen (Wildcards) werden nicht unterstützt.
4. Wählen Sie einen Recovery-Punkt.
5. Klicken Sie auf **Daten wiederherstellen**.
6. Wechseln Sie zum benötigten Ordner oder verwenden Sie die Suchfunktion, um eine Liste der erforderlichen Elemente abzurufen.
   Sie können E-Mail-Nachrichten und Postings nach Betreff, Absender, Empfänger oder Datum durchsuchen. Platzhalterzeichen (Wildcards) werden nicht unterstützt.
7. Wählen Sie die Elemente aus, die Sie wiederherstellen wollen. Wenn Sie Ordner auswählen wollen, klicken Sie auf das Symbol 'Ordner wiederherstellen'. 
   Zusätzlich haben Sie auch folgende Möglichkeiten:

- Klicken Sie bei der Auswahl einer E-Mail-Nachricht oder eines Postings auf **Inhalt anzeigen**, um die Inhalte (inklusive Anhänge) einsehen zu können. Klicken Sie auf den Namen einer angehängten Datei, um diese herunterzuladen.
- Wenn Sie eine E-Mail-Nachricht oder ein Posting ausgewählt haben, können Sie auch auf **Als E-Mail senden** klicken, um das Element an bestimmte E-Mail-Adressen zu versenden. Sie können den Absender bestimmen und einen Text schreiben, der dem weitergeleiteten Element hinzugefügt wird.
- Nur bei einem unverschlüsselten Backup, wenn Sie die Suchfunktion verwendet und ein einzelnes Element in den Suchergebnissen ausgewählt haben: klicken Sie auf **Versionen anzeigen**, um die Version des Elements auszuwählen, die Sie wiederherstellen wollen. Sie können jede Backup-Version auswählen, auch wenn diese vor oder nach dem eigentlichen, zuvor ausgewählten Recovery-Punkt liegt.

8. Klicken Sie auf **Recovery**.
9. Wenn dem Cyber Protection Service mehrere Microsoft 365-Organisationen hinzugefügt wurden, klicken Sie auf **Microsoft 365-Organisation**, um die Zielorganisation einsehen, ändern oder spezifizieren zu können.
   Die ursprüngliche Organisation wird automatisch vorausgewählt. Wenn diese Organisation nicht mehr im Cyber Protection Service registriert ist, müssen Sie die Zielorganisation spezifizieren.
10. Bei **Zu öffentlichem Ordner wiederherstellen** können Sie den gewünschten öffentlichen Zielordner anzeigen lassen, ändern oder spezifizieren.
    Standardmäßig ist der ursprüngliche Ordner vorausgewählt. Wenn dieser Ordner nicht mehr existiert oder Sie eine andere als die ursprüngliche Organisation als Ziel ausgewählt haben, müssen Sie den Zielordner spezifizieren.
    Sie können während der Wiederherstellung keinen neuen öffentlichen Ordner erstellen. Um einen öffentlichen Ordner zu einem neuen wiederherzustellen, müssen Sie zuerst den als Ziel dienenden öffentlichen Ordner in der gewünschten Microsoft 365-Organisation erstellen und dann den Cloud Agenten die Änderung synchronisieren lassen. Der Cloud Agent synchronisiert sich automatisch alle 24 Stunden mit Microsoft 365. Um die Änderung sofort zu synchronisieren, wählen Sie in der Cyber Protect-Konsole die Organisation auf der **Microsoft 365**-Seite aus und klicken Sie dann auf **Aktualisieren**.
11. Bei **Pfad** können Sie den als Ziel dienenden Unterordner im öffentlichen Ordner einsehen oder ändern. Der ursprüngliche Pfad wird standardmäßig neu erstellt.
12. Klicken Sie auf **Recovery starten**.
13. Wählen Sie eine dieser Überschreiben-Optionen:

Option	Beschreibung
Vorhandene Elemente überschreiben	Alle vorhandenen Dateien am Zielspeicherort werden überschrieben.
Vorhandene	Wenn am Zielspeicherort bereits eine Datei mit dem gleichen Namen

Option	Beschreibung
Elemente nicht überschreiben	vorhanden ist, wird diese nicht überschrieben und die Quelldatei wird nicht am Zielspeicherort gespeichert.

14. Klicken Sie auf **Forsetzen**, um Ihre Entscheidung zu bestätigen.

OneDrive-Dateien sichern

Welche Elemente können per Backup gesichert werden?

Sie können ein komplettes OneDrive sichern – oder auch nur einzelne Dateien und Ordner.

Eine separate Option im Backup-Plan ermöglicht die Sicherung von OneNote-Notizbüchern.

Dateien werden inklusive ihrer Freigabe-Berechtigungen gesichert. Erweiterte Berechtigungsstufen (**Entwerfen**, **Vollzugriff**, **Mitwirken**) werden nicht mitgesichert.

Einige Dateien können sensible Informationen enthalten und der Zugriff auf diese kann durch eine Regel zur Verhinderung von Datenverlust (Data Loss Prevention, DLP) in Microsoft 365 blockiert sein. Diese Dateien werden nicht gesichert und es werden auch keine dementsprechenden Warnungen angezeigt, nachdem die Backup-Aktion abgeschlossen wurde.

Einschränkungen

Das Sichern von OneDrive-Inhalten per Backup wird für freigegebene Postfächer nicht unterstützt. Wenn Sie diese Inhalte sichern wollen, müssen Sie das freigegebene Postfach zu einem regulären Benutzerkonto konvertieren und sicherstellen, dass OneDrive für dieses Konto aktiviert ist.

Welche Elemente können wiederhergestellt werden?

Sie können ein komplettes OneDrive wiederherstellen oder beliebige einzelne Dateien/Ordner, die gesichert wurden.

Sie können eine Suchfunktion verwenden, um bestimmte Elemente zu finden.

Sie können wählen, ob die Dateien bei der Wiederherstellung ihre ursprünglichen Freigabe-Berechtigungen aus dem Backup beibehalten sollen – oder ob sie die Berechtigungen desjenigen Ordner übernehmen sollen, in dem sie wiederhergestellt werden.

Freigabelinks für Dateien und Ordner werden nicht wiederhergestellt.

OneDrive-Dateien auswählen

Wählen Sie die Dateien wie nachfolgend beschrieben aus – und spezifizieren Sie dann die anderen Einstellungen des Schutzplans nach Bedarf.

So können Sie OneDrive-Dateien auswählen

1. Klicken Sie auf **Microsoft 365**.
2. Wenn dem Cyber Protection Service mehrere Microsoft 365-Organisationen hinzugefügt wurden, wählen Sie diejenige Organisation aus, deren Benutzerdaten Sie sichern wollen. Ansonsten können Sie diesen Schritt überspringen.
3. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Um die Dateien aller Benutzer zu sichern (einschließlich solcher Benutzer, die erst in der Zukunft angelegt werden), erweitern Sie den Knoten **Benutzer**, wählen Sie **Alle Benutzer** und klicken Sie dann auf **Gruppen-Backup**.
   - Wenn Sie die Dateien einzelner Benutzer sichern wollen, erweitern Sie den Knoten **Benutzer**, wählen Sie **Alle Benutzer**, wählen Sie die Benutzer aus, deren Dateien Sie sichern wollen, und klicken Sie dann auf **Backup**.
4. Im Schutzplan-Fensterbereich:
   - Überprüfen Sie, dass das Element **OneDrive** bei **Backup-Quelle** ausgewählt ist.

     Wenn einige der individuell ausgewählten Benutzer keinen OneDrive-Service in ihrem Microsoft 365-Plan enthalten haben, können Sie diese Option nicht auswählen.

     Wenn einige der für ein Gruppen-Backup ausgewählten Benutzer keinen OneDrive-Service in ihrem Microsoft 365-Plan enthalten haben, können Sie diese Option zwar auswählen, aber der Schutzplan wird nicht auf diese Benutzer angewendet.
   - Wählen Sie bei **Elemente für das Backup** eine der folgenden Möglichkeiten:
     - Übernehmen Sie die Voreinstellung **[Alle]** (alle Dateien).
     - Spezifizieren Sie die zu sichernden Dateien und Ordner an, indem Sie deren Namen oder Pfade hinzufügen.

       Sie können Platzhalterzeichen (*, ** und ?) verwenden. Ausführlichere Informationen über die Verwendung von Pfaden und Platzhalterzeichen finden Sie im Abschnitt 'Dateifilter'.
     - Spezifizieren Sie Dateien und Ordner für das Backup, indem Sie diese per 'Durchsuchen' auswählen.

       Der Link **Durchsuchen** ist nur verfügbar, wenn ein Schutzplan für einen einzelnen Benutzer erstellt wird.
   - [Optional] Klicken Sie bei **Elemente für das Backup** auf **Ausschlusskriterien anzeigen**, um zu spezifizieren, ob und welche Dateien und Ordner während des Backup-Prozesses übersprungen werden sollen.

     Dateiausschlusskritieren überschreiben eine vorherige Dateiauswahl, d.h., wenn Sie in beiden Feldern dieselbe Datei spezifizieren, wird diese Datei beim anschließenden Backup übersprungen.
   - [Optional] Wenn Sie die OneNote-Notizbücher sichern wollen, aktivieren Sie den Schalter **OneNote einschließen**.

OneDrive und OneDrive-Dateien wiederherstellen

Ein komplettes OneDrive wiederherstellen

1. Klicken Sie auf **Microsoft 365**.
2. Wenn dem Cyber Protection Service mehrere Microsoft 365-Organisationen hinzugefügt wurden, wählen Sie diejenige Organisation aus, deren gesicherte Daten Sie wiederherstellen wollen. Ansonsten können Sie diesen Schritt überspringen.
3. Erweitern Sie den Knoten **Benutzer**, wählen Sie die Option **Alle Benutzer**, wählen Sie den Benutzer, dessen OneDrive Sie wiederherstellen wollen, und klicken Sie dann auf **Recovery**.

   Wenn der Benutzer zuvor gelöscht wurde, können Sie diesen im Bereich **Cloud-Applikationen-Backups** der Registerkarte 'Backup Storage' auswählen und dann auf **Backups anzeigen** klicken.

   Sie können Benutzer auch per Namen suchen. Platzhalterzeichen (Wildcards) werden nicht unterstützt.
4. Wählen Sie einen Recovery-Punkt.

   Hinweis
   Wenn Sie nur Recovery-Punkte sehen wollen, die OneDrive-Dateien enthalten, wählen Sie **OneDrive** bei **Nach Inhalt filtern**.
5. Klicken Sie auf **Recovery** –> **Kompletter OneDrive-Ordner**.
6. Wenn dem Cyber Protection Service mehrere Microsoft 365-Organisationen hinzugefügt wurden, klicken Sie auf **Microsoft 365-Organisation**, um die Zielorganisation einsehen, ändern oder spezifizieren zu können.

   Die ursprüngliche Organisation wird automatisch vorausgewählt. Wenn diese Organisation nicht mehr im Cyber Protection Service registriert ist, müssen Sie die Zielorganisation spezifizieren.

   Sie können während der Wiederherstellung kein neues OneDrive-Ziel erstellen. Um alle OneDrive-Daten zu einem neuen OneDrive wiederherzustellen, müssen Sie zuerst das als Ziel dienende OneDrive in der Microsoft 365-Organisation erstellen und dann den Cloud Agenten die Änderung dorthin synchronisieren lassen. Der Cloud Agent synchronisiert sich automatisch alle 24 Stunden mit Microsoft 365. Um die Änderung sofort zu synchronisieren, wählen Sie in der Cyber Protect-Konsole die Organisation auf der **Microsoft 365**-Seite aus und klicken Sie dann auf **Aktualisieren**.
7. Bei **Zu Laufwerk wiederherstellen** können Sie den gewünschten Zielbenutzer anzeigen lassen, ändern oder spezifizieren.

   Der ursprüngliche Benutzer wird automatisch vorausgewählt. Wenn dieser Benutzer nicht mehr existiert oder Sie eine andere als die ursprüngliche Organisation als Ziel ausgewählt haben, müssen Sie den Zielbenutzer spezifizieren.
8. Bestimmen Sie, ob Sie auch die Freigabe-Berechtigungen der Dateien mit wiederherstellen wollen.

9. Klicken Sie auf **Recovery starten**.
10. Wählen Sie eine dieser Überschreiben-Optionen:

Option	Beschreibung
Vorhandene Datei überschreiben, wenn diese älter ist	Wenn es am Zielort bereits eine Datei mit dem gleichen Namen gibt, die jedoch älter als die Quelldatei ist, wird die Quelldatei am Zielort gespeichert und dabei die ältere Version ersetzt.
Vorhandene Dateien überschreiben	Alle bereits vorhandenen Dateien am Zielort werden überschrieben, unabhängig von ihrem letzten Änderungsdatum.
Vorhandene Dateien nicht überschreiben	Wenn es am Zielort bereits eine Datei mit dem gleichen Namen gibt, werden keine Änderungen an dieser vorgenommen und die Quelldatei wird nicht am Zielort gespeichert.

Hinweis
Wenn Sie OneNote-Notizbücher wiederherstellen, führen sowohl die Option **Vorhandene Datei überschreiben, wenn diese älter ist** als auch **Vorhandene Dateien überschreiben** dazu, dass vorhandene OneNote-Notizbücher überschrieben werden.

11. Klicken Sie auf **Forsetzen**, um Ihre Entscheidung zu bestätigen.

OneDrive-Dateien wiederherstellen

1. Klicken Sie auf **Microsoft 365**.
2. Wenn dem Cyber Protection Service mehrere Microsoft 365-Organisationen hinzugefügt wurden, wählen Sie diejenige Organisation aus, deren gesicherte Daten Sie wiederherstellen wollen. Ansonsten können Sie diesen Schritt überspringen.
3. Erweitern Sie den Knoten **Benutzer**, wählen Sie die Option **Alle Benutzer**, wählen Sie den Benutzer, dessen OneDrive-Dateien Sie wiederherstellen wollen, und klicken Sie dann auf **Recovery**.
   Wenn der Benutzer zuvor gelöscht wurde, können Sie diesen im Bereich **Cloud-Applikationen-Backups** der Registerkarte 'Backup Storage' auswählen und dann auf **Backups anzeigen** klicken.
   Sie können Benutzer auch per Namen suchen. Platzhalterzeichen (Wildcards) werden nicht unterstützt.
4. Wählen Sie einen Recovery-Punkt.

Hinweis
Wenn Sie nur Recovery-Punkte sehen wollen, die OneDrive-Dateien enthalten, wählen Sie **OneDrive** bei **Nach Inhalt filtern**.

5. Klicken Sie auf **Recovery** –> **Dateien/Ordner**.
6. Wechseln Sie zum benötigten Ordner oder verwenden Sie die Suchfunktion, um eine Liste der erforderlichen Dateien und Ordner abzurufen.

7. Wählen Sie die Dateien, die Sie wiederherstellen wollen.

   Wenn das Backup unverschlüsselt ist und Sie eine einzelne Datei ausgewählt haben, können Sie auf **Versionen anzeigen** klicken, um eine bestimmte Dateiversion auszuwählen, die Sie wiederherstellen wollen. Sie können jede Backup-Version auswählen, auch wenn diese vor oder nach dem eigentlichen, zuvor ausgewählten Recovery-Punkt liegt.
8. Wenn Sie eine Datei herunterladen wollen, müssen Sie diese auswählen, auf **Download** klicken, den Zielspeicherort für die Datei bestimmen und schließlich auf **Speichern** klicken. Ansonsten können Sie diesen Schritt überspringen.
9. Klicken Sie auf **Recovery**.
10. Wenn dem Cyber Protection Service mehrere Microsoft 365-Organisationen hinzugefügt wurden, klicken Sie auf **Microsoft 365-Organisation**, um die Zielorganisation einsehen, ändern oder spezifizieren zu können.

    Die ursprüngliche Organisation wird automatisch vorausgewählt. Wenn diese Organisation nicht mehr im Cyber Protection Service registriert ist, müssen Sie die Zielorganisation spezifizieren.

    Sie können während der Wiederherstellung kein neues OneDrive erstellen. Um eine Datei zu einem neuen OneDrive wiederherzustellen, müssen Sie zuerst das als Ziel dienende OneDrive in der gewünschten Microsoft 365-Organisation erstellen und dann den Cloud Agenten die Änderung synchronisieren lassen. Der Cloud Agent synchronisiert sich automatisch alle 24 Stunden mit Microsoft 365. Um die Änderung sofort zu synchronisieren, wählen Sie in der Cyber Protect-Konsole die Organisation auf der **Microsoft 365**-Seite aus und klicken Sie dann auf **Aktualisieren**.
11. Bei **Zu Laufwerk wiederherstellen** können Sie den gewünschten Zielbenutzer anzeigen lassen, ändern oder spezifizieren.

    Der ursprüngliche Benutzer wird automatisch vorausgewählt. Wenn dieser Benutzer nicht mehr existiert oder Sie eine andere als die ursprüngliche Organisation als Ziel ausgewählt haben, müssen Sie den Zielbenutzer spezifizieren.
12. Bei **Pfad** können Sie den Zielordner im OneDrive des Zielbenutzers einsehen oder ändern. Standardmäßig ist der ursprüngliche Speicherort vorausgewählt.
13. Bestimmen Sie, ob Sie auch die Freigabe-Berechtigungen der Dateien mit wiederherstellen wollen.
14. Klicken Sie auf **Recovery starten**.
15. Wählen Sie eine der folgenden Optionen zum Überschreiben:

Option	Beschreibung
Vorhandene Datei überschreiben, wenn diese älter ist	Wenn es am Zielort bereits eine Datei mit dem gleichen Namen gibt, die jedoch älter als die Quelldatei ist, wird die Quelldatei am Zielort gespeichert und dabei die ältere Version ersetzt.
Vorhandene Dateien überschreiben	Alle bereits vorhandenen Dateien am Zielort werden überschrieben, unabhängig von ihrem letzten Änderungsdatum.
Vorhandene Dateien	Wenn es am Zielort bereits eine Datei mit dem gleichen Namen gibt, werden

Option	Beschreibung
nicht überschreiben	keine Änderungen an dieser vorgenommen und die Quelldatei wird nicht am Zielort gespeichert.

Hinweis
Wenn Sie OneNote-Notizbücher wiederherstellen, führen sowohl die Option **Vorhandene Datei überschreiben, wenn diese älter ist** als auch **Vorhandene Dateien überschreiben** dazu, dass vorhandene OneNote-Notizbücher überschrieben werden.

16. Klicken Sie auf **Forsetzen**, um Ihre Entscheidung zu bestätigen.

SharePoint Online-Websites sichern

Welche Elemente können per Backup gesichert werden?

Sie können klassische SharePoint Website-Sammlungen, Gruppen-Websites (moderne Team-Websites) und Kommunikations-Websites sichern. Sie können außerdem einzelne Unterwebsites, Listen und Bibliotheken für ein Backup auswählen.

Eine separate Option im Backup-Plan ermöglicht die Sicherung von OneNote-Notizbüchern.

Folgende Elemente werden bei einem Backup *übersprungen*:

- Die Website-Einstellungen für **Aussehen und Verhalten** (mit Ausnahme von **Titel, Beschreibung und Logo**).
- Seitenkommentare und Seitenkommentar-Einstellungen (Kommentare **An**/**Aus**).
- Die Website-Einstellungen **Websitefeatures**.
- Webpartseiten und Webparts, die in Wiki-Seiten eingebettet sind (aufgrund von Beschränkungen der SharePoint Online API).
- Ausgecheckte Dateien – Dateien, die zur Bearbeitung manuell ausgecheckt wurden, sowie alle Dateien, die in Bibliotheken erstellt oder hochgeladen wurden und für die die Option **Auschecken erfordern** aktiviert wurde. Wenn Sie diese Dateien per Backup sichern wollen, müssen Sie diese zuerst einchecken.
- Externe Daten und verwaltete Metadatentypen von Spalten.
- Die Standard-Website-Sammlung 'domain-my.sharepoint.com'. Dies ist eine Sammlung, in der sich alle OneDrive-Dateien der Benutzer der Organisation/desUnternehmens befinden.
- Der Inhalt des Papierkorbs.

Einschränkungen

- Titel und Beschreibungen von Webseiten/Unterwebsites/Listen/Spalten werden während eines Backups abgeschnitten, wenn der Titel/Beschreibungsumfang größer als 10000 Byte ist.

- Sie können keine 'Vorherige Dateiversionen' (auch 'Vorgängerversionen' genannt) per Backup sichern, die in SharePoint Online erstellt wurden. Es werden jeweils nur die letzten (jüngsten) Dateiversionen gesichert.
- Das permanente Dokumentarchiv (Preservation Hold Library) kann nicht gesichert werden.
- Sie können keine Websites sichern, die mit der Business Productivity Online Suite (BPOS), dem Vorgänger von Microsoft 365, erstellt wurden.
- Sie können keine Einstellungen von Websites sichern, die den verwalteten Pfad '`/portals`' verwenden (Beispiel: `https://<Mandant>.sharepoint.com/portals/...`).
- Die IRM-Einstellungen (Information Rights Management) einer Liste oder einer Bibliothek können nur dann wiederhergestellt werden, wenn IRM in der Microsoft 365-Zielorganisation aktiviert ist.

Welche Elemente können wiederhergestellt werden?

Folgende Elemente können aus einem Website-Backup wiederhergestellt werden:

- Die komplette Website
- Unterwebsites
- Listen
- Listenelemente
- Dokumentbibliotheken
- Dokumente
- Listenelement-Anhänge
- Website-Seiten und Wiki-Seiten

Sie können eine Suchfunktion verwenden, um bestimmte Elemente zu finden.

Elemente können zur ursprünglichen oder einer nicht-ursprünglichen Website wiederhergestellt werden. Der Pfad zu einem wiederhergestellten Element ist derselbe wie der ursprüngliche Pfad. Wenn der Pfad nicht existiert, wird er automatisch erstellt.

Sie können wählen, ob die Elemente bei der Wiederherstellung ihre ursprünglichen Freigabe-Berechtigungen aus dem Backup beibehalten sollen – oder ob sie die Berechtigungen des übergeordneten Ojekts übernehmen sollen, in dem sie wiederhergestellt werden.

Welche Elemente können nicht wiederhergestellt werden?

- Unterwebsites, die auf dem Template **Visio-Prozessrepository** beruhen.
- Listen der folgenden Typen: **Umfrageliste**, **Aufgabenliste**, **Bildbibliothek**, **Links**, **Kalender**, **Diskussionsrunde**, **Externe** und **Interne Tabelle**.
- Listen, für die mehrere Inhaltstypen aktiviert wurden.

SharePoint Online-Daten auswählen

Wählen Sie die Daten wie nachfolgend beschrieben aus – und spezifizieren Sie die anderen Einstellungen des Schutzplans je nach Bedarf.

So können Sie SharePoint Online-Daten auswählen

1. Klicken Sie auf **Microsoft 365**.
2. Wenn dem Cyber Protection Service mehrere Microsoft 365-Organisationen hinzugefügt wurden, wählen Sie diejenige Organisation aus, deren Benutzerdaten Sie sichern wollen. Ansonsten können Sie diesen Schritt überspringen.
3. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Um alle klassichen SharePoint-Websites in der Organisation zu sichern, einschließlich solcher Websites, die erst in der Zukunft angelegt werden, müssen Sie den Knoten **Website-Sammlung** erweitern, dann **Alle Website-Sammlungen** auswählen und anschließend auf **Gruppen-Backup** klicken.
   - Wenn Sie einzelne klassische Websites sichern wollen, erweitern Sie den Knoten **Website-Sammlung**, wählen Sie **Alle Website-Sammlungen**, wählen Sie die Website aus, die Sie sichern wollen, und klicken Sie dann auf **Backup**.
   - Um alle Gruppen-Websites (moderne Team-Websites) zu sichern, einschließlich der Websites, die erst in der Zukunft erstellt werden, müssen Sie den Knoten **Gruppen** erweitern, dann **Alle Gruppen** auswählen und anschließend dann auf **Gruppen-Backup** klicken.
   - Wenn Sie einzelne Gruppen-Websites (moderne Team-Websites) sichern wollen, erweitern Sie den Knoten **Gruppen**, wählen Sie **Alle Gruppen**, wählen Sie die Gruppen aus, deren Websites Sie sichern wollen, und klicken Sie dann auf **Backup**.
4. Im Schutzplan-Fensterbereich:
   - Überprüfen Sie, dass das Element **SharePoint-Websites** bei **Backup-Quelle** ausgewählt ist.
   - Wählen Sie bei **Elemente für das Backup** eine der folgenden Möglichkeiten:
     - Übernehmen Sie die Voreinstellung **[Alle]** (alle Elemente der ausgewählten Websites).
     - Spezifizieren Sie die zu sichernden Unterwebsites, Listen und Bibliotheken, indem Sie deren Namen oder Pfade hinzufügen.

       Wenn Sie eine Unterwebsite oder eine Toplevel-Website-Liste/Bibliothek sichern wollen, spezifizieren Sie deren Anzeigenamen im folgenden Format: `/anzeigename/**`

       Wenn Sie eine Unterwebsite-Liste/Bibliothek sichern wollen, spezifizieren Sie deren Anzeigenamen im folgenden Format: `/unterwebsite anzeigename/liste anzeigename/**`

       Die Anzeigenamen der Unterwebsites, Listen und Bibliotheken werden auf der Seite **Website-Inhalte** einer SharePoint-Website oder -Unterwebsite angezeigt.
     - Spezifizieren Sie Unterwebsites für das Backup, indem Sie diese per 'Durchsuchen' auswählen.

       Der Link **Durchsuchen** ist nur verfügbar, wenn ein Schutzplan für eine einzelne Website erstellt wird.

- [Optional] Klicken Sie bei **Elemente für das Backup** auf **Ausschlusskriterien anzeigen**, um zu spezifizieren, ob und welche Unterwebsites, Listen und Bibliotheken während des Backup-Prozesses übersprungen werden sollen.

  Elementausschlusskritieren überschreiben eine vorherige Elementauswahl, d.h., wenn Sie in beiden Feldern dieselbe Unterwebsite spezifizieren, wird diese Unterwebsite beim anschließenden Backup übersprungen.
- [Optional] Wenn Sie die OneNote-Notizbücher sichern wollen, aktivieren Sie den Schalter **OneNote einschließen**.

SharePoint Online-Daten wiederherstellen

1. Klicken Sie auf **Microsoft 365**.
2. Wenn dem Cyber Protection Service mehrere Microsoft 365-Organisationen hinzugefügt wurden, wählen Sie diejenige Organisation aus, deren gesicherte Daten Sie wiederherstellen wollen. Ansonsten können Sie diesen Schritt überspringen.
3. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Wenn Sie Daten aus einem Gruppen-Website (moderne Team-Website) wiederherstellen wollen, erweitern Sie den Knoten **Gruppen**, wählen Sie **Alle Gruppen**, wählen Sie diejenige Gruppe aus, deren Website die wiederherzustellenden Elemente ursprünglich enthalten hat, und klicken Sie dann auf **Recovery**.
   - Wenn Sie Daten aus einem klassischen Website wiederherstellen wollen, erweitern Sie den Knoten **Website-Sammlungen**, wählen Sie **Alle Website-Sammlungen**, wählen Sie diejenige Website aus, in der sich die wiederherzustellenden Elemente ursprünglich befunden haben, und klicken Sie dann auf **Recovery**.
   - Wenn die Website zuvor gelöscht wurde, können Sie diese im Bereich **Cloud-Applikationen-Backups** der Registerkarte 'Backup Storage' auswählen und dann auf **Backups anzeigen** klicken.

   Sie können Gruppen und Websites auch per Namen suchen. Platzhalterzeichen (Wildcards) werden nicht unterstützt.
4. Wählen Sie einen Recovery-Punkt.

   Hinweis
   Wenn Sie nur Recovery-Punkte sehen wollen, die SharePoint-Websites enthalten, wählen Sie **SharePoint-Websites** bei **Nach Inhalt filtern**.

5. Klicken Sie auf **SharePoint-Dateien wiederherstellen**.
6. Wechseln Sie zum benötigten Ordner oder verwenden Sie die Suchfunktion, um eine Liste der erforderlichen Datenelemente abzurufen.
7. Wählen Sie die Elemente aus, die Sie wiederherstellen wollen.

   Wenn das Backup unverschlüsselt ist, Sie die Suchfunktion verwendet und dann eine einzelne Datei in den Suchergebnissen ausgewählt haben, können Sie auf **Versionen anzeigen** klicken, um eine bestimmte Elementversion auszuwählen, die Sie wiederherstellen wollen. Sie können

jede Backup-Version auswählen, auch wenn diese vor oder nach dem eigentlichen, zuvor ausgewählten Recovery-Punkt liegt.

8. [Optional] Wenn Sie ein Element herunterladen wollen, müssen Sie dieses zuerst auswählen, dann auf **Download** klicken, den Zielspeicherort für das Element bestimmen und schließlich auf **Speichern** klicken.
9. Klicken Sie auf **Recovery**.
10. Wenn dem Cyber Protection Service mehrere Microsoft 365-Organisationen hinzugefügt wurden, klicken Sie auf **Microsoft 365-Organisation**, um die Zielorganisation einsehen, ändern oder spezifizieren zu können.

    Die ursprüngliche Organisation wird automatisch vorausgewählt. Wenn diese Organisation nicht mehr im Cyber Protection Service registriert ist, müssen Sie die Zielorganisation spezifizieren.
11. Bei **Zu Website wiederherstellen** können Sie die gewünschte Ziel-Website anzeigen lassen, ändern oder spezifizieren.

    Sie können während der Wiederherstellung keine neue SharePoint-Website erstellen. Um eine SharePoint-Website zu einer neuen wiederherzustellen, müssen Sie zuerst die als Ziel dienende Website in der gewünschten Microsoft 365-Organisation erstellen und dann den Cloud Agenten die Änderung synchronisieren lassen. Der Cloud Agent synchronisiert sich automatisch alle 24 Stunden mit Microsoft 365. Um die Änderung sofort zu synchronisieren, wählen Sie in der Cyber Protect-Konsole die Organisation auf der **Microsoft 365**-Seite aus und klicken Sie dann auf **Aktualisieren**.
12. Bestimmen Sie, ob Sie auch die Freigabe-Berechtigungen der wiederhergestellten Elemente mit wiederherstellen wollen.
13. Klicken Sie auf **Recovery starten**.
14. Wählen Sie eine dieser Überschreiben-Optionen:

Option	Beschreibung
Vorhandene Datei überschreiben, wenn diese älter ist	Wenn es am Zielort bereits eine Datei mit dem gleichen Namen gibt, die jedoch älter als die Quelldatei ist, wird die Quelldatei am Zielort gespeichert und dabei die ältere Version ersetzt.
Vorhandene Dateien überschreiben	Alle bereits vorhandenen Dateien am Zielort werden überschrieben, unabhängig von ihrem letzten Änderungsdatum.
Vorhandene Dateien nicht überschreiben	Wenn es am Zielort bereits eine Datei mit dem gleichen Namen gibt, werden keine Änderungen an dieser vorgenommen und die Quelldatei wird nicht am Zielort gespeichert.

Hinweis
Wenn Sie OneNote-Notizbücher wiederherstellen, führen sowohl die Option **Vorhandene Datei überschreiben, wenn diese älter ist** als auch **Vorhandene Dateien überschreiben** dazu, dass vorhandene OneNote-Notizbücher überschrieben werden.

15. Klicken Sie auf **Forsetzen**, um Ihre Entscheidung zu bestätigen.

Microsoft 365-Teams schützen

Welche Elemente können per Backup gesichert werden?

Sie können komplette Teams per Backup sichern. Dazu gehören der Team-Name, die Liste der Team-Mitglieder, die Team-Kanäle und ihre Inhalte, das Postfach und die Besprechungen des Teams sowie die Team-Website.

Eine separate Option im Backup-Plan ermöglicht die Sicherung von OneNote-Notizbüchern.

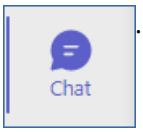
Welche Elemente können wiederhergestellt werden?

- Das komplette Team
- Die Team-Kanäle
- Die Kanaldateien
- Das Team-Postfach
- Der E-Mail-Ordner im Team-Postfach
- Die E-Mail-Nachrichten im Team-Postfach
- Die Besprechungen
- Die Team-Website

Sie können keine Unterhaltungen in Team-Kanälen wiederherstellen, aber Sie können diese als html-Datei herunterladen.

Einschränkungen

Folgende Elemente werden nicht gesichert:

- Die Einstellungen des allgemeinen Kanals (Moderationseinstellungen) – aufgrund von Beschränkungen der Microsoft Teams-Beta-API.
- Die Einstellungen der benutzerdefinierten Kanäle (Moderationseinstellungen) – aufgrund von Beschränkungen der Microsoft Teams-Beta-API.
- Besprechungsnotizen.
- Nachrichten im Chat-Bereich 

. Dieser Bereich enthält private Einzelchats und Gruppenchats.
- Aufkleber und Lobs.

Backup und Recovery werden für folgende Kanal-Registerkarten unterstützt:

- Word
- Excel

- PowerPoint
- PDF
- Dokumentbibliothek

Teams auswählen

Wählen Sie Teams wie nachfolgend beschrieben aus – und spezifizieren Sie dann die anderen Einstellungen des Schutzplans nach Bedarf.

So können Sie Teams auswählen

1. Klicken Sie auf **Microsoft 365**.
2. Wenn dem Cyber Protection Service mehrere Microsoft 365-Organisationen hinzugefügt wurden, wählen Sie diejenige Organisation aus, deren Teams Sie sichern wollen. Ansonsten können Sie diesen Schritt überspringen.
3. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Um alle Teams in der Organisation zu sichern (einschließlich solcher Teams, die erst in der Zukunft angelegt werden), erweitern Sie den Knoten**Teams**, wählen Sie**Alle Teams** und klicken Sie dann auf**Gruppen-Backup**.
   - Wenn Sie einzelne Teams sichern wollen, erweitern Sie den Knoten**Teams**, wählen Sie**Alle Teams**, wählen Sie die zu sichernden Teams aus und klicken Sie dann auf**Backup**.

   Sie können Teams auch per Namen suchen. Platzhalterzeichen (Wildcards) werden nicht unterstützt.
4. Im Schutzplan-Fensterbereich:
   - Überprüfen Sie, dass das Element **Microsoft Teams** bei **Backup-Quelle** ausgewählt wurde.
   - [Optional] Legen Sie bei **Aufbewahrungsdauer** die Bereinigungsoptionen fest.
   - [Optional] Wenn Sie Ihr Backup verschlüsseln wollen, aktivieren Sie den Schalter **Verschlüsselung**, legen Sie dann Ihr Kennwort fest und wählen Sie anschließend den Verschlüsselungsalgorithmus.
   - [Optional] Wenn Sie die OneNote-Notizbücher sichern wollen, aktivieren Sie den Schalter **OneNote einschließen**.

Ein komplettes Team wiederherstellen

1. Klicken Sie auf **Microsoft 365**.
2. Wenn dem Cyber Protection Service mehrere Microsoft 365-Organisationen hinzugefügt wurden, wählen Sie diejenige Organisation aus, deren gesicherte Teams Sie wiederherstellen wollen. Ansonsten können Sie diesen Schritt überspringen.
3. Erweitern Sie den Knoten **Teams**, wählen Sie die Option **Alle Teams**, wählen Sie das wiederherzustellende Team aus und klicken Sie dann auf **Recovery**.

   Sie können Teams auch per Namen suchen. Platzhalterzeichen (Wildcards) werden nicht unterstützt.
4. Wählen Sie einen Recovery-Punkt.

5. Klicken Sie auf**Recovery**–>**Komplettes Team**.

   Wenn dem Cyber Protection Service mehrere Microsoft 365-Organisationen hinzugefügt wurden, klicken Sie auf **Microsoft 365-Organisation**, um die Zielorganisation einsehen, ändern oder spezifizieren zu können.

   Die ursprüngliche Organisation wird automatisch vorausgewählt. Wenn diese Organisation nicht mehr im Cyber Protection Service registriert ist, müssen Sie die Zielorganisation spezifizieren.
6. Bei **Zu Team wiederherstellen** können Sie sich das Zielteam anzeigen lassen oder ein anderes auswählen.

   Das ursprüngliche Team wird automatisch vorausgewählt. Wenn dieses Team nicht mehr existiert (z.B. weil es gelöscht wurde) oder Sie eine Organisation ausgewählt haben, die das ursprüngliche Team nicht enthält, müssen Sie ein Zielteam aus dem Listenfeld auswählen.

   Sie können ein Team nur in einem bestehenden Team wiederherstellen. Sie können keine Teams bei Wiederherstellungsaktionen erstellen.
7. Klicken Sie auf **Recovery starten**.
8. Wählen Sie eine dieser Überschreiben-Optionen:
   - **Vorhandene Inhalte überschreiben, wenn diese älter sind**
   - **Vorhandene Inhalte überschreiben**
   - **Vorhandene Inhalte nicht überschreiben**

   Hinweis
   Wenn Sie OneNote-Notizbücher wiederherstellen, führen sowohl die Option **Vorhandene Inhalte überschreiben, wenn diese älter sind** als auch **Vorhandene Inhalte überschreiben** dazu, dass vorhandene OneNote-Notizbücher überschrieben werden.
9. Klicken Sie auf **Forsetzen**, um Ihre Entscheidung zu bestätigen.

Wenn Sie einen Kanal in der grafischen Oberfläche von Microsoft Teams löschen, wird dieser nicht sofort aus dem System entfernt. Wenn Sie also das komplette Team wiederherstellen, kann der Name dieses Kanals nicht verwendet werden. Daher wird dem Namen ein Postfix hinzugefügt.

Unterhaltungen werden in Form einer einzelnen html-Datei in der Registerkarte **Dateien** des Kanals wiederhergestellt. Sie können diese Datei in einem Ordner finden, der nach folgendem Muster benannt ist: `<Team-Name>_<Kanal-Name>_unterhaltungen_backup_<Datum der Wiederherstellung>T<Uhrzeit der Wiederherstellung>Z`.

Hinweis
Nachdem Sie ein Team oder Team-Kanäle wiederhergestellt haben, gehen Sie zu Microsoft Teams, wählen Sie die wiederhergestellten Kanäle aus und klicken Sie dann auf deren Registerkarte **Dateien**. Anderenfalls werden die nachfolgenden Backups dieser Kanäle die Inhalte dieser Registerkarte nicht enthalten – aufgrund von Beschränkungen der Microsoft Teams-Beta-API.

Team-Kanäle oder Dateien in Team-Kanälen wiederherstellen

So können Sie Team-Kanäle wiederherstellen

1. Klicken Sie auf **Microsoft 365**.
2. Wenn dem Cyber Protection Service mehrere Microsoft 365-Organisationen hinzugefügt wurden, wählen Sie diejenige Organisation aus, deren gesicherte Teams Sie wiederherstellen wollen. Ansonsten können Sie diesen Schritt überspringen.
3. Erweitern Sie den Knoten**Teams**, wählen Sie die Option **All Teams**, wählen Sie das Team aus, dessen Kanäle Sie wiederherstellen wollen, und klicken Sie dann auf **Recovery**.
4. Wählen Sie einen Recovery-Punkt.
5. Klicken Sie auf **Recovery** –> **Kanäle**.
6. Wählen Sie die wiederherzustellenden Kanäle aus und klicken Sie dann auf **Recovery**. Wenn Sie einen Kanal im Hauptbereich auswählen wollen, aktivieren Sie das Kontrollkästchen vor dessen Namen.

   Folgende Suchoptionen sind verfügbar:
   - Für **Unterhaltungen**: Absender, Betreff, Inhalt, Sprache, Name der Anlage, Datum oder Datumsbereich.
   - Für **Dateien**: Dateiname oder Ordnername, Dateityp, Größe, Datum oder Datumsbereich der letzten Änderung.

   Hinweis
   Sie können die Dateien auch lokal herunterladen, anstatt sie wiederherzustellen.
7. Wenn dem Cyber Protection Service mehrere Microsoft 365-Organisationen hinzugefügt wurden, klicken Sie auf **Microsoft 365-Organisation**, um die Zielorganisation einsehen, ändern oder spezifizieren zu können.

   Die ursprüngliche Organisation wird automatisch vorausgewählt. Wenn diese Organisation nicht mehr im Cyber Protection Service registriert ist, müssen Sie die Zielorganisation spezifizieren.
8. Bei **Zu Team wiederherstellen** können Sie das gewünschten Zielteam anzeigen lassen, ändern oder spezifizieren.

   Das ursprüngliche Team wird automatisch vorausgewählt. Wenn dieses Team nicht mehr existiert oder Sie eine andere als die ursprüngliche Organisation als Ziel ausgewählt haben, müssen Sie das Zielteam spezifizieren.
9. Bei **Zu Kanal wiederherstellen** können Sie den gewünschte Zielkanal anzeigen lassen, ändern oder spezifizieren.
10. Klicken Sie auf **Recovery starten**.
11. Wählen Sie eine dieser Überschreiben-Optionen:
    - **Vorhandene Inhalte überschreiben, wenn diese älter sind**
    - **Vorhandene Inhalte überschreiben**
    - **Vorhandene Inhalte nicht überschreiben**

Hinweis
Wenn Sie OneNote-Notizbücher wiederherstellen, führen sowohl die Option **Vorhandene Inhalte überschreiben, wenn diese älter sind** als auch **Vorhandene Inhalte überschreiben** dazu, dass vorhandene OneNote-Notizbücher überschrieben werden.

12. Klicken Sie auf **Forsetzen**, um Ihre Entscheidung zu bestätigen.

Unterhaltungen werden in Form einer einzelnen html-Datei in der Registerkarte **Dateien** des Kanals wiederhergestellt. Sie können diese Datei in einem Ordner finden, der nach folgendem Muster benannt ist: `<Team-Name>_<Kanal-Name>_unterhaltungen_backup_<Datum der Wiederherstellung>T<Uhrzeit der Wiederherstellung>Z`.

Hinweis
Nachdem Sie ein Team oder Team-Kanäle wiederhergestellt haben, gehen Sie zu Microsoft Teams, wählen Sie die wiederhergestellten Kanäle aus und klicken Sie dann auf deren Registerkarte **Dateien**. Anderenfalls werden die nachfolgenden Backups dieser Kanäle die Inhalte dieser Registerkarte nicht enthalten – aufgrund von Beschränkungen der Microsoft Teams-Beta-API.

So können Sie Dateien in einem Team-Kanal wiederherstellen

1. Klicken Sie auf **Microsoft 365**.
2. Wenn dem Cyber Protection Service mehrere Microsoft 365-Organisationen hinzugefügt wurden, wählen Sie diejenige Organisation aus, deren gesicherte Teams Sie wiederherstellen wollen. Ansonsten können Sie diesen Schritt überspringen.
3. Erweitern Sie den Knoten**Teams**, wählen Sie die Option **All Teams**, wählen Sie das Team aus, dessen Kanäle Sie wiederherstellen wollen, und klicken Sie dann auf **Recovery**.
4. Wählen Sie einen Recovery-Punkt.
5. Klicken Sie auf **Recovery** –> **Kanäle**.
6. Wählen Sie den gewünschten Kanal aus und öffnen Sie dann den Ordner **Dateien** .
   Wechseln Sie zum benötigten Elementen oder verwenden Sie die Suchfunktion, um eine Liste der gewünschten Elemente abzurufen. Folgende Suchoptionen sind verfügbar: Dateiname oder Ordnername, Dateityp, Größe, Datum oder Datumsbereich der letzten Änderung.
7. [Optional] Wenn Sie ein Element herunterladen wollen, müssen Sie dieses zuerst auswählen, dann auf **Download** klicken, den Zielspeicherort für das Element bestimmen und schließlich auf **Speichern** klicken.
8. Wählen Sie die wiederherzustellenden Elemente aus und klicken Sie dann auf **Recovery**.
9. Wenn dem Cyber Protection Service mehrere Microsoft 365-Organisationen hinzugefügt wurden, klicken Sie auf 'Microsoft 365-Organisation', um die Zielorganisation einsehen, ändern oder spezifizieren zu können.
   Die ursprüngliche Organisation wird automatisch vorausgewählt. Wenn diese Organisation nicht mehr im Cyber Protection Service registriert ist, müssen Sie die Zielorganisation spezifizieren.

10. Bei **Zu Team wiederherstellen** können Sie das gewünschten Zielteam anzeigen lassen, ändern oder spezifizieren.
    Das ursprüngliche Team wird automatisch vorausgewählt. Wenn dieses Team nicht mehr existiert oder Sie eine andere als die ursprüngliche Organisation als Ziel ausgewählt haben, müssen Sie das Zielteam spezifizieren.
11. Bei **Zu Kanal wiederherstellen** können Sie den gewünschte Zielkanal anzeigen lassen, ändern oder spezifizieren.
12. Bestimmen Sie, ob Sie auch die Freigabe-Berechtigungen der wiederhergestellten Elemente mit wiederherstellen wollen.
13. Klicken Sie auf **Recovery starten**.
14. Wählen Sie eine dieser Überschreiben-Optionen:
    - **Vorhandene Inhalte überschreiben, wenn diese älter sind**
    - **Vorhandene Inhalte überschreiben**
    - **Vorhandene Inhalte nicht überschreiben**

    Hinweis
    Wenn Sie OneNote-Notizbücher wiederherstellen, führen sowohl die Option **Vorhandene Inhalte überschreiben, wenn diese älter sind** als auch **Vorhandene Inhalte überschreiben** dazu, dass vorhandene OneNote-Notizbücher überschrieben werden.
15. Klicken Sie auf **Forsetzen**, um Ihre Entscheidung zu bestätigen.

Sie können keine einzelnen Unterhaltungen wiederherstellen. Sie können im Hauptbereich nur den Ordner **Unterhaltung** durchsuchen oder dessen Inhalte in Form einer einzelnen html-Datei herunterladen. Klicken Sie dafür auf das Symbol 'Ordner wiederherstellen'  , wählen Sie den gewünschten Ordner **Unterhaltungen** und klicken Sie dann auf **Download**.

Sie können die Nachrichten im Ordner **Unterhaltung** nach folgenden Parametern durchsuchen:

- Absender
- Inhalt
- Name des Anhangs
- Datum

Ein Team-Postfach wiederherstellen

1. Klicken Sie auf **Microsoft 365**.
2. Wenn dem Cyber Protection Service mehrere Microsoft 365-Organisationen hinzugefügt wurden, wählen Sie diejenige Organisation aus, deren gesicherte Teams Sie wiederherstellen wollen. Ansonsten können Sie diesen Schritt überspringen.
3. Erweitern Sie den Knoten **Teams**, wählen Sie die Option **Alle Teams**, wählen Sie das Team aus, dessen Postfach Sie wiederherstellen wollen, und klicken Sie dann auf **Recovery**.

Sie können Teams auch per Namen suchen. Platzhalterzeichen (Wildcards) werden nicht unterstützt.

4. Wählen Sie einen Recovery-Punkt.
5. Klicken Sie auf **Recovery** –> **E-Mail-Nachrichten**.
6. Klicken Sie auf das Symbol 'Ordner wiederherstellen'  , wählen Sie den Postfach-Stammordner und klicken Sie dann auf **Recovery**.

   Hinweis
   Sie können auch einzelne Ordner aus dem ausgewählten Postfach wiederherstellen.

7. Klicken Sie auf **Recovery**.
8. Wenn dem Cyber Protection Service mehrere Microsoft 365-Organisationen hinzugefügt wurden, klicken Sie auf **Microsoft 365-Organisation**, um die Zielorganisation einsehen, ändern oder spezifizieren zu können.
   Die ursprüngliche Organisation wird automatisch vorausgewählt. Wenn diese Organisation nicht mehr im Cyber Protection Service registriert ist, müssen Sie die Zielorganisation spezifizieren.
9. Bei**Zu Postfach wiederherstellen** können Sie das gewünschte Zielpostfach anzeigen lassen, ändern oder spezifizieren.
   Das ursprüngliche Postfach wird automatisch vorausgewählt. Wenn dieses Postfach nicht mehr existiert oder Sie eine andere als die ursprüngliche Organisation als Ziel ausgewählt haben, müssen Sie das Zielpostfach spezifizieren.
10. Klicken Sie auf **Recovery starten**.
11. Wählen Sie eine dieser Überschreiben-Optionen:
    - **Vorhandene Elemente überschreiben**
    - **Vorhandene Elemente nicht überschreiben**
12. Klicken Sie auf **Forsetzen**, um Ihre Entscheidung zu bestätigen.

Team-Postfach-Elemente zu PST-Dateien wiederherstellen

So können Sie Team-Postfach-Elemente wiederherstellen

1. Klicken Sie auf **Microsoft 365**.
2. Wenn dem Cyber Protection Service mehrere Microsoft 365-Organisationen hinzugefügt wurden, wählen Sie diejenige Organisation aus, deren gesicherte Daten Sie wiederherstellen wollen. Ansonsten können Sie diesen Schritt überspringen.
3. Sie können Benutzer und Gruppen auch per Namen suchen. Platzhalterzeichen (Wildcards) werden nicht unterstützt.
4. Erweitern Sie den Knoten **Teams**, wählen Sie die Option **Alle Teams**, wählen Sie ein Team aus, in dessen Postfach sich die wiederherzustellenden Elemente ursprünglich befunden haben – und klicken Sie dann auf **Recovery**.
5. Klicken Sie auf **Recovery** –> **E-Mail-Nachrichten**.

6. Wechseln Sie zum benötigten Ordner oder verwenden Sie die Suchfunktion, um eine Liste der erforderlichen Elemente abzurufen.
   Folgende Suchoptionen sind verfügbar. Platzhalterzeichen (Wildcards) werden nicht unterstützt.
   - Für E-Mail-Nachrichten: Suche per Betreff, Absender, Empfänger, Name des Anhangs und Datum.
   - Für Ereignisse: Suche nach Titel und Datum.
   - Für Tasks: Suche per Betreff und Datum.
   - Für Kontakte: Suche nach Namen, E-Mail-Adresse und Telefonnummer.
7. Wählen Sie die Elemente aus, die Sie wiederherstellen wollen. Wenn Sie Ordner auswählen wollen, klicken Sie auf das Symbol 'Ordner wiederherstellen'. 
   Zusätzlich haben Sie auch folgende Möglichkeiten:
   - Klicken Sie bei der Auswahl eines Elements auf **Inhalt anzeigen**, um die Inhalte (inklusive Anhänge) einsehen zu können. Klicken Sie auf den Namen einer angehängten Datei, um diese herunterzuladen.
   - Klicken Sie bei der Auswahl einer Nachricht oder eines Kalenderelements auf **Als E-Mail senden**, wenn Sie das Element an eine spezifizierte E-Mail-Adresse versenden wollen. Sie können den Absender bestimmen und einen Text schreiben, der dem weitergeleiteten Element hinzugefügt wird.
   - Wenn das Backup nicht verschlüsselt ist, Sie die Suche verwendet und ein einzelnes Element aus dem Suchergebnis ausgewählt haben: klicken Sie auf **Versionen anzeigen**, wenn Sie sich die Version des Elements anzeigen lassen wollen. Sie können jede Backup-Version auswählen, auch wenn diese vor oder nach dem eigentlichen, zuvor ausgewählten Recovery-Punkt liegt.
8. Klicken Sie auf **Als PST-Dateien wiederherstellen**.
9. Legen Sie das Kennwort fest, um das Archiv mit den PST-Dateien zu verschlüsseln.
   Das Kennwort muss mindestens ein Zeichen enthalten.
10. Bestätigen Sie das Kennwort und klicken Sie dann auf **FERTIG**.

Die ausgewählten Postfach-Elemente werden als PST-Datendateien wiederhergestellt und im ZIP-Format archiviert. Die maximale Größe einer einzelnen PST-Datei ist auf 2 GB begrenzt. Wenn die wiederherzustellenden Daten also 2 GB überschreiten, werden sie auf mehrere PST-Dateien aufgeteilt. Das ZIP-Archiv wird mit dem von Ihnen festgelegten Kennwort geschützt.

Sie werden eine E-Mail mit einem Link erhalten, der auf ein ZIP-Archiv mit den erstellten PST-Dateien verweist.

Der Administrator wird per E-Mail benachrichtigt, dass Sie die Recovery-Prozedur durchgeführt haben.

So können Sie das Archiv mit den PST-Dateien herunterladen und die Wiederherstellung abschließen

1. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Folgen Sie dem Link **Dateien herunterladen**, um das Archiv aus der E-Mail herunterzuladen. Das Archiv steht 24 Stunden lang zum Download bereit. Sollte der Link abgelaufen sein,

wiederholen Sie die Recovery-Prozedur.

- So können Sie das Archiv über die Cyber Protect-Konsole herunterladen:
  a. Gehen Sie zu **Backup Storage** –> **PST-Dateien**.
  b. Wählen Sie das letzte hervorgehobene Archiv aus.
  c. Klicken Sie im rechten Fensterbereich auf **Download**.

  Das Archiv wird in das Standard-Download-Verzeichnis auf Ihrem Computer heruntergeladen.

2. Extrahieren Sie die PST-Dateien aus dem Archiv unter Verwendung des Kennworts, das Sie zur Verschlüsselung des Archivs festgelegt haben.
3. Öffnen oder importieren Sie die PST-Dateien in Microsoft Outlook. Informationen darüber, wie das geht, finden Sie in der Microsoft-Dokumentation.

E-Mail-Nachrichten und Besprechungen wiederherstellen

1. Klicken Sie auf **Microsoft 365**.
2. Wenn dem Cyber Protection Service mehrere Microsoft 365-Organisationen hinzugefügt wurden, wählen Sie diejenige Organisation aus, deren gesicherte Teams Sie wiederherstellen wollen. Ansonsten können Sie diesen Schritt überspringen.
3. Erweitern Sie den Knoten **Teams**, wählen Sie die Option **Alle Teams**, wählen Sie das Team aus, dessen E-Mail-Nachrichten und Besprechungen Sie wiederherstellen wollen, und klicken Sie dann auf **Recovery**.

   Sie können Teams auch per Namen suchen. Platzhalterzeichen (Wildcards) werden nicht unterstützt.
4. Wählen Sie einen Recovery-Punkt.
5. Klicken Sie auf **Recovery** –> **E-Mail-Nachrichten**.
6. Wechseln Sie zum benötigten Element oder verwenden Sie die Suchfunktion, um eine Liste der gewünschten Elemente abzurufen.

   Folgende Suchoptionen sind verfügbar:
   - Für E-Mail-Nachrichten: Suche per Betreff, Absender, Empfänger und Datum.
   - Für Besprechungen: nach Ereignisname und Datum suchen.
7. Wählen Sie die wiederherzustellenden Elemente aus und klicken Sie dann auf **Recovery**.

   Hinweis
   Sie können die Besprechungen im Ordner **Kalender** finden.

   Zusätzlich haben Sie auch folgende Möglichkeiten:
   - Klicken Sie bei der Auswahl eines Elements auf **Inhalt anzeigen**, um die Inhalte (inklusive Anhänge) einsehen zu können. Klicken Sie auf den Namen einer angehängten Datei, um diese herunterzuladen.
   - Wenn Sie eine E-Mail-Nachricht oder Besprechung ausgewählt haben, können Sie auch auf**Als E-Mail senden** klicken, um das Element an bestimmte E-Mail-Adressen zu versenden. Sie

können den Absender bestimmen und einen Text schreiben, der dem weitergeleiteten Element hinzugefügt wird.

8. Wenn dem Cyber Protection Service mehrere Microsoft 365-Organisationen hinzugefügt wurden, klicken Sie auf **Microsoft 365-Organisation**, um die Zielorganisation einsehen, ändern oder spezifizieren zu können.

   Die ursprüngliche Organisation wird automatisch vorausgewählt. Wenn diese Organisation nicht mehr im Cyber Protection Service registriert ist, müssen Sie die Zielorganisation spezifizieren.
9. Bei**Zu Postfach wiederherstellen** können Sie das gewünschte Zielpostfach anzeigen lassen, ändern oder spezifizieren.

   Das ursprüngliche Postfach wird automatisch vorausgewählt. Wenn dieses Postfach nicht mehr existiert oder Sie eine andere als die ursprüngliche Organisation als Ziel ausgewählt haben, müssen Sie das Zielpostfach spezifizieren.
10. Klicken Sie auf **Recovery starten**.
11. Wählen Sie eine dieser Überschreiben-Optionen:
    - **Vorhandene Elemente überschreiben**
    - **Vorhandene Elemente nicht überschreiben**
12. Klicken Sie auf **Forsetzen**, um Ihre Entscheidung zu bestätigen.

Eine Team-Website oder bestimmte Elemente einer Website wiederherstellen

1. Klicken Sie auf **Microsoft 365**.
2. Wenn dem Cyber Protection Service mehrere Microsoft 365-Organisationen hinzugefügt wurden, wählen Sie diejenige Organisation aus, deren gesicherte Teams Sie wiederherstellen wollen. Ansonsten können Sie diesen Schritt überspringen.
3. Erweitern Sie den Knoten **Teams**, wählen Sie die Option **Alle Teams**, wählen Sie das Team aus, dessen Website Sie wiederherstellen wollen, und klicken Sie dann auf **Recovery**.

   Sie können Teams auch per Namen suchen. Platzhalterzeichen (Wildcards) werden nicht unterstützt.
4. Wählen Sie einen Recovery-Punkt.
5. Klicken Sie auf**Recovery**–>**Team-Website**.
6. Wechseln Sie zum benötigten Element oder verwenden Sie die Suchfunktion, um eine Liste der gewünschten Elemente abzurufen.
7. [Optional] Wenn Sie ein Element herunterladen wollen, müssen Sie dieses zuerst auswählen, dann auf **Download** klicken, den Zielspeicherort für das Element bestimmen und schließlich auf **Speichern** klicken.
8. Wählen Sie die wiederherzustellenden Elemente aus und klicken Sie dann auf **Recovery**.
9. Wenn dem Cyber Protection Service mehrere Microsoft 365-Organisationen hinzugefügt wurden, klicken Sie auf **Microsoft 365-Organisation**, um die Zielorganisation einsehen, ändern oder spezifizieren zu können.

Die ursprüngliche Organisation und das ursprüngliche Team werden automatisch vorausgewählt. Wenn diese Organisation nicht mehr im Cyber Protection Service registriert ist, müssen Sie die Zielorganisation spezifizieren.

10. Bei **Zu Team wiederherstellen** können Sie das gewünschten Zielteam anzeigen lassen, ändern oder spezifizieren.

    Das ursprüngliche Team wird automatisch vorausgewählt. Wenn dieses Team nicht mehr existiert oder Sie eine andere als die ursprüngliche Organisation als Ziel ausgewählt haben, müssen Sie die Ziel-Website spezifizieren.
11. Bestimmen Sie, ob Sie auch die Freigabe-Berechtigungen der wiederhergestellten Elemente mit wiederherstellen wollen.
12. Klicken Sie auf **Recovery starten**.
13. Wählen Sie eine dieser Überschreiben-Optionen:
    - **Vorhandene Inhalte überschreiben, wenn diese älter sind**
    - **Vorhandene Inhalte überschreiben**
    - **Vorhandene Inhalte nicht überschreiben**

    Hinweis
    Wenn Sie OneNote-Notizbücher wiederherstellen, führen sowohl die Option **Vorhandene Inhalte überschreiben, wenn diese älter sind** als auch **Vorhandene Inhalte überschreiben** dazu, dass vorhandene OneNote-Notizbücher überschrieben werden.
14. Klicken Sie auf **Forsetzen**, um Ihre Entscheidung zu bestätigen.

OneNote-Notizbücher schützen

OneNote-Notizbücher werden standardmäßig in die Backups von OneDrive-Dateien, Microsoft Teams und SharePoint-Websites aufgenommen.

Wenn Sie OneNote-Notizbücher von diesen Backups ausschließen wollen, müssen Sie den Schalter **OneNote einschließen** im entsprechenden Backup-Plan deaktivieren.

Gesicherte OneNote-Notizbücher wiederherstellen

Wie Sie ein gesichertes OneNote-Notizbuch wiederherstellen können, erfahren Sie unter dem entsprechenden Thema:

- Für OneDrive-Backups – siehe den Abschnitt '"Ein komplettes OneDrive wiederherstellen" (S. 683)' oder '"OneDrive-Dateien wiederherstellen" (S. 684)'.
- Für Teams-Backups – siehe die Abschnitte '"Ein komplettes Team wiederherstellen" (S. 692)', '"Team-Kanäle oder Dateien in Team-Kanälen wiederherstellen" (S. 693)' oder '"Eine Team-Website oder bestimmte Elemente einer Website wiederherstellen" (S. 700)'.
- Für SharePoint-Website-Backups – siehe Abschnitt '"SharePoint Online-Daten wiederherstellen" (S. 689)'.

Unterstützte Versionen

- OneNote (OneNote 2016 und höher)
- OneNote für Windows 10

Einschränkungen und bekannte Probleme

- OneNote-Notizbücher, die in OneDrive oder SharePoint gespeichert werden, sind auf 2 GB begrenzt. Sie können keine größeren OneNote-Notizbücher auf OneDrive- oder SharePoint-Zielen wiederherstellen.
- OneNote-Notizbücher mit Abschnittsgruppen werden nicht unterstützt.
- In gesicherten OneNote-Notizbüchern, die Abschnitte mit nicht standardmäßigen Namen enthalten, wird der erste Abschnitt mit dem Standardnamen angezeigt (wie `Neuer Abschnitt` oder `Unbenannter Abschnitt`). Dies kann die Reihenfolge der Abschnitte in Notizbüchern mit mehreren Abschnitten beeinflussen.
- Wenn Sie OneNote-Notizbücher wiederherstellen, führen sowohl die Option **Vorhandene Inhalte überschreiben, wenn diese älter sind** als auch **Vorhandene Inhalte überschreiben** dazu, dass vorhandene OneNote-Notizbücher überschrieben werden.
- Wenn Sie ein komplettes Team, eine Team-Website oder den Ordner `Websiteobjekte` (Englisch: Site Assets) einer Team-Website wiederherstellen wollen und Sie entweder die Option **Vorhandene Inhalte überschreiben, wenn diese älter sind** oder die Option **Vorhandene Inhalte überschreiben** ausgewählt haben, wird das OneNote-Standardnotizbuch des betreffenden Teams nicht überschrieben. The recovery Die Wiederherstellung wird mit der Warnung *Die Eigenschaften der Datei '/sites/<Team-Name>/Websiteobjekte/<OneNote-Notizbuch-Name>' konnten nicht aktualisiert werden.* abgeschlossen.

Microsoft 365-Kollaborations-Apps-Arbeitsplätze schützen

Sie können das Advanced Email Security-Paket verwenden, das einen Echtzeitschutz für Ihre Microsoft 365-, Google Workspace- oder Open-Xchange-Postfächer bietet:

- Antimalware und Antispam
- Scannen von URLs in E-Mails
- DMARC-Analyse
- Antiphishing
- Impersonation Protection
- Scannen von Anhängen
- Content Disarm & Reconstruction (CDR)
- Vertrauensgraph

Sie können auch die Option Microsoft 365-Kollaborations-Apps-Arbeitsplätze aktivieren, die es ermöglicht, Microsoft 365-Cloud-Kollaborationsapplikationen vor inhaltsbasierten

Sicherheitsbedrohungen zu schützen. Diese Applikationen umfassen u.a. OneDrive, SharePoint und Teams.

Die Advanced Email Security-Erweiterung kann pro Workload oder pro Gigabyte aktiviert werden und hat Auswirkungen auf Ihr Lizenzierungsmodell.

So können Sie das Advanced Email Security-Onboarding über die Cyber Protect Cloud-Konsole aufrufen

1. Klicken Sie auf **Geräte** –> **Microsoft 365**.
2. Klicken Sie auf den **Benutzer**-Knoten und dann oben rechts auf den Link **Zu Email Security gehen**.

Im Datenblatt für Advanced Email Security können Sie mehr über die Advanced Email Security-Funktionalität erfahren.

Anweisungen zur Konfiguration finden Sie unter Advanced Email Security mit Perception Point.

Google Workspace-Daten sichern

Hinweis
Diese Funktion ist im Compliance-Modus nicht für Mandanten verfügbar. Weitere Informationen dazu finden Sie im Abschnitt "Compliance-Modus" (S. 1194).

Was bedeutet die Sicherung von Google Workspace?

- Cloud-zu-Cloud-basiertes Backup & Recovery von Google Workspace-Benutzerdaten (Gmail-Postfächer, Kalender, Kontakte, Google Drives) und Google Workspace Shared Drives.
- Granulares Recovery von E-Mails, Dateien, Kontakten und anderen Datenelementen.
- Unterstützung für mehrere Google Workspace-Organisationen und organisationsübergreifende Wiederherstellungen.
- Optionale Beglaubigung (Notarization) von gesicherten Dateien mithilfe der Blockchain-Datenbank von Ethereum. Wenn die Beglaubigungsfunktion aktiviert ist, können Sie überprüfen und belegen, ob und dass Ihre gesicherten Dateien seit Erstellung des dazugehörigen Backups authentisch und unverändert geblieben sind.
- Optionale Volltextsuche. Wenn diese Funktion aktiviert wird, können Sie E-Mail-Nachrichten nach ihren Inhalten durchsuchen.
- Pro Unternehmen können bis zu 5000 Elemente (Postfächer, Google Drives und Shared Drives) ohne Performanceverlust gesichert werden.
- Die Backup-Daten werden automatisch komprimiert und benötigen daher am Backup-Speicherort weniger Platz als am ursprünglichen Speicherort. Der Komprimierungsgrad für Cloud-zu-Cloud-Backups ist fest eingestellt und entspricht dem Komprimierungsgrad **Normal** von Nicht-Cloud-zu-Cloud-Backups. Weitere Informationen über diese Komprimierungsgrade finden Sie im Abschnitt '"Komprimierungsgrad" (S. 502)'.

Erforderliche Benutzerrechte

In Cyber Protection

Sie müssen in Cyber Protection ein Firmenadministrator sein, der auf einer Kunden-Mandanten-Ebene agiert. Firmenadministratoren, die auf Abteilungsebene agieren, Abteilungsadministratoren und Benutzer können keine Backups oder Wiederherstellungen von Google Workspace-Daten durchführen.

In Google Workspace

Wenn Sie Ihre Google-Workspace-Organisation zum Cyber Protection Service hinzufügen wollen, müssen Sie als Super Admin mit aktiviertem API-Zugriff angemeldet sein (**Sicherheit** –> **API-Referenz** –> **API-Zugriff aktivieren** in der Google Admin-Konsole).

Das Super Admin-Kennwort wird nirgendwo gespeichert und wird weder für Backups noch Wiederherstellungen verwendet. Wenn Sie dieses Kennwort in Google Workspace ändern, hat dies keinen Einfluss auf die Cyber Protection Service-Operationen.

Wenn der Super Admin, der die Google Workspace-Organisation hinzugefügt hat, aus Google Workspace gelöscht wird oder eine Admin-Rolle mit weniger Rechten erhält, werden die Backups mit einer Fehlermeldung wie 'Zugriff verweigert' fehlschlagen. Wiederholen Sie in diesem Fall die im Abschnitt '"Eine Google Workspace-Organisation hinzufügen" (S. 705)' beschriebene Prozedur und spezifizieren Sie die gültigen Anmeldedaten für den Super Admin. Damit dies nicht passiert, empfehlen wir, dass Sie einen dedizierten Super Admin-Benutzer für Backup- und Wiederherstellungszwecke anlegen.

Über die Backup-Planung

Da der Cloud Agent mehrere Kunden bedient, bestimmt der Agent die Startzeit für jeden Schutzplan selbst, um eine gleichmäßige Auslastung über den Tag und die gleiche Service-Qualität für alle Kunden zu gewährleisten.

Jeder Schutzplan wird täglich zur gleichen Tageszeit ausgeführt.

Die Standardoption ist **Einmal täglich**. Mit dem Advanced Backup-Paket können Sie bis zu sechs Backups pro Tag planen. Die Backups werden in ungefähren Intervallen gestartet, die davon abhängen, wie hoch die aktuelle Auslastung des Cloud Agenten ist, der in einem Datacenter mehrere Kunden bedient. Dadurch wird gewährleistet, dass es während des Tages zu einer gleichmäßigen Auslastung kommt und alle Kunden die gleiche Service-Qualität erhalten.

Einschränkungen

- Die Konsole zeigt nur Benutzer an, die eine zugewiesene Google Workspace-Lizenz sowie ein entsprechendes Postfach oder Google Drive haben.

- Dokumente in den nativen Google-Formaten werden als generische Office-Dokumente gesichert und daher in der Cyber Protect-Konsole mit einer anderen Erweiterung angezeigt (beispielsweise .docx oder .pptx). Die Dokumente werden bei einer Wiederherstellung wieder in ihr ursprüngliches Format zurückkonvertiert.
- Nicht mehr als 10 manuelle Backup-Ausführungen in einer Stunde.
- Nicht mehr als 10 gleichzeitige Recovery-Aktionen (diese Anzahl beinhaltet sowohl Microsoft 365- als auch Google Workspace-Wiederherstellungen).
- Sie können nicht gleichzeitig Elemente von verschiedenen Recovery-Punkten wiederherstellen, auch wenn Sie solche Elemente aus den Suchergebnissen auswählen können.
- Die Backups von gelöschten Google Workspace-Benutzerkonten werden nicht automatisch aus dem Cloud Storage gelöscht. Diese Backups werden nach dem von ihnen genutzten Speicherplatz berechnet.
- Sie können auf denselben Workload nicht mehr als einen individuellen Backup-Plan anwenden.
- Wenn ein individueller Backup-Plan und ein Gruppen-Backup-Plan auf denselben Workload angewendet werden, haben die Einstellungen des individuellen Plans eine höhere Priorität.

Protokollierung

Aktionen mit Cloud-zu-Cloud-Ressourcen (wie das Anzeigen der Inhalte von gesicherten E-Mails, das Herunterladen von Anhängen oder Dateien, das Wiederherstellen von E-Mails zu anderen als den ursprünglichen Postfächern oder das Versenden der Inhalte als E-Mail) können die Datenschutzrechte des Benutzers verletzen. Solche Aktionen werden im Management-Portal im **Monitoring** –> **Überwachungsprotokoll** protokolliert.

Eine Google Workspace-Organisation hinzufügen

Um eine Google Workspace-Organisationzum Cyber Protection Service hinzufügen zu können, benötigen Sie ein persönliches Google Cloud-Projekt. Weitere Informationen darüber, wie Sie ein solches Projekt erstellen und konfigurieren können, finden Sie im Abschnitt '"Ein persönliches Google Cloud-Projekt erstellen" (S. 706)'.

So können Sie eine Google Workspace-Organisation hinzufügen, indem Sie ein dediziertes persönliches Google Cloud-Projekt verwenden

1. Melden Sie sich als Firmenadministrator an der Cyber Protect-Konsole an.
2. Klicken Sie auf **Geräte** –> **Hinzufügen** –> **Google Workspace**.
3. Geben Sie die E-Mail-Adresse eines Super-Administrators für Ihr Google Workspace-Konto ein. Für diese Prozedur ist es unerheblich, ob die Zwei-Schritt-Verifizierung für das Super-Administrator E-Mail-Konto aktiviert ist.
4. Suchen Sie nach der JSON-Datei, die den privaten Schlüssel des Service-Kontos enthält, welches Sie in Ihrem Google Cloud-Projekt erstellt haben.
   Sie können den Dateiinhalt auch über die Zwischenablage als Text einfügen.

5. Klicken Sie auf **Bestätigen**.

   Als Ergebnis erscheint Ihre Google Workspace-Organisation unter der Registerkarte **Geräte** in der Cyber Protect-Konsole.

Nützliche Tipps

- Nach dem Hinzufügen einer Google-Workspace-Organisation werden die Benutzerdaten und Shared Drives in der primären Domäne und in allen sekundären Domänen (sofern vorhanden) per Backup gesichert. Die gesicherten Ressourcen werden in einer Liste angezeigt und nicht nach ihrer Domain gruppiert.
- Der Cloud Agent führt die Synchronisierung mit Google Workspace alle 24 Stunden durch, beginnend mit dem Zeitpunkt, ab dem das Unternehmen dem Cyber Protection Service hinzugefügt wurde. Wenn Sie einen Benutzer oder ein Shared Drive hinzufügen oder entfernen, wird diese Änderung nicht sofort in der Cyber Protect-Konsole angezeigt. Wenn Sie die Änderung sofort synchronisieren wollen, müssen Sie die Organisation auf der Seite **Google Workspace** auswählen und dann auf **Aktualisieren** klicken.

  Weitere Informationen darüber, wie Sie die Ressourcen einer Google Workspace-Organisation und der Cyber Protect-Konsole synchronisieren, finden Sie im Abschnitt '"Google Workspace-Ressourcen erkennen" (S. 710)'.
- Wenn Sie den Gruppen **Alle Benutzer** oder **Alle Shared Drives** einen Schutzplan zugewiesen haben, werden die neu hinzugefügten Elemente erst dann in das Backup aufgenommen, wenn die Synchronisierung durchgeführt wurde.
- Gemäß den Google-Richtlinien bleibt ein Benutzer oder ein Shared Drive, wenn dieser/dieses aus der grafischen Benutzeroberfläche von Google Workspace entfernt wurde, noch einige Tage lang per API verfügbar. Während dieses Zeitraums wird das entfernte Element in der Cyber Protect-Konsole als inaktiv (ausgegraut) dargestellt und nicht per Backup gesichert. Wenn das entfernte Element auch nicht mehr per API verfügbar ist, verschwinden es ganz aus der Cyber Protect-Konsole. Dessen Backups können (sofern vorhanden) unter **Backup Storage** –> **Cloud-Applikationen-Backups** gefunden werden.

Ein persönliches Google Cloud-Projekt erstellen

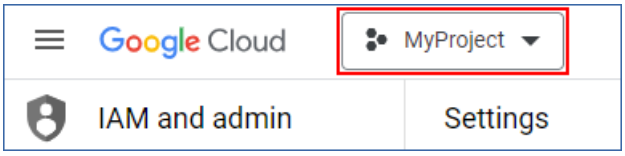
Wenn Sie Ihre Google Workspace-Organisation zum Cyber Protection Service hinzufügen wollen, indem Sie ein dediziertes Google Cloud-Projekt verwenden, müssen Sie folgendermaßen vorgehen:

1. Erstellen Sie ein neues Google Cloud-Projekt.
2. Aktivieren Sie die erforderlichen APIs für dieses Projekt.
3. Konfigurieren Sie die Anmeldedaten für dieses Projekt:
   a. Konfigurieren Sie die Anzeige für die OAuth-Zustimmung.
   b. Erstellen und konfigurieren Sie das Dienstkonto für den Cyber Protection Service.
4. Gewähren Sie dem neuen Projekt Zugriff auf Ihr Google Workspace-Konto.

Hinweis
Dieses Thema enthält eine Beschreibung der Benutzeroberfläche von Drittanbietern, die ohne vorherige Ankündigung geändert werden kann.

So können Sie ein neues Google Cloud-Projekt erstellen

1. Melden Sie sich an der Google Cloud Platform (console.cloud.google.com) als Super-Administrator an.
2. Klicken Sie in der Google Cloud Platform-Konsole in der linken oberen Ecke auf den Projektpicker.



3. Wählen Sie in dem sich öffnenden Fenster eine Organisation aus und klicken Sie dann auf **Neues Projekt**.

4. Spezifizieren Sie einen Namen für Ihr neues Projekt.
5. Klicken Sie auf **Erstellen**.

Daraufhin wird Ihr neues Google Cloud-Projekt erstellt.

So können Sie die erforderlichen APIs für dieses Projekt aktivieren

1. Wählen Sie in der Google Cloud Platform-Konsole Ihr neues Projekt aus.
2. Wählen Sie im Navigationsmenü die Elemente **APIs und Dienste** –> **Aktivierte APIs und Dienste** aus.
3. Deaktivieren Sie einzeln nacheinander alle APIs, die in diesem Projekt standardmäßig aktiviert sind:
   a. Scrollen Sie auf der Seite **Aktivierte APIs und Dienste** nach unten und klicken Sie dann auf den Namen einer aktivierten API.
   Die Seite **API/Dienst-Details** wird geöffnet.
   b. Klicken Sie auf **API deaktivieren** und bestätigen Sie Ihre Entscheidung, indem Sie auf **Deaktivieren** klicken.
   c. [Bei Aufforderung] Bestätigen Sie Ihre Auswahl, indem Sie auf **Bestätigen** klicken.
   d. Gehen Sie zurück zu **APIs und Dienste** –> **Aktivierte APIs und Dienste** und deaktivieren Sie die nächste API.
4. Wählen Sie im Navigationsmenü die Elemente **APIs und Dienste** –> **Bibliothek** aus.
5. Aktivieren Sie in der API-Bibliothek einzeln nacheinander die folgenden APIs:
   - Admin SDK API
   - Gmail API

- Google Calendar API
- Google Drive API
- Google People API

Verwenden Sie die Suchleiste, um die gewünschten APIs zu finden. Wenn Sie eine API aktivieren wollen, müssen Sie zuerst auf ihren Namen klicken und dann auf **Aktivieren**. Um nach der nächsten API suchen zu können, gehen Sie zurück zur API-Bibliothek, indem Sie im Navigationsmenü die Elemente **APIs und Dienste** –> **Bibliothek** auswählen.

So können Sie die Anzeige für die OAuth-Zustimmung konfigurieren

1. Wählen Sie im Google Cloud Platform-Navigationsmenü die Elemente **APIs und Dienste** –> **OAuth-Zustimmungsbildschirm** aus.
2. Wählen Sie im geöffneten Fenster für Nutzertyp **Intern** aus und klicken Sie dann auf **Erstellen**.
3. Spezifizieren Sie im Feld **Anwendungsname** einen Namen für Ihre Applikation.
4. Geben Sie im Feld **Nutzersupport-E-Mail** die E-Mail-Adresse des Super-Administrators ein.
5. Geben Sie im Feld **Kontaktdaten des Entwicklers** die E-Mail-Adresse des Super-Administrators ein.
6. Lassen Sie alle anderen Felder leer und klicken Sie dann auf **Speichern und fortfahren**.
7. Klicken Sie in der Seite **Bereiche** ohne irgendetwas zu ändern auf **Speichern und fortfahren**.
8. Überprüfen Sie auf der Seite **Zusammenfassung** Ihre Einstellungen und klicken Sie dann auf **Zurück zum Dashboard**.

So können Sie das Dienstkonto für den Cyber Protection Service erstellen und konfigurieren

1. Wählen Sie im Google Cloud Platform-Navigationsmenü die Elemente **IAM & Admin** –> **Dienstkonten** aus.
2. Klicken Sie auf **Dienstkonto erstellen**.
3. Spezifizieren Sie einen Namen für das Dienstkonto.
4. [Optional] Spezifizieren Sie eine Beschreibung für das Dienstkonto.
5. Klicken Sie auf **Erstellen und weiter**.
6. Nehmen Sie in den Schritten **Diesem Dienstkonto Zugriff auf das Projekt erteilen** und **Nutzern Zugriff auf dieses Dienstkonto erteilen** keine Änderungen vor.
7. Klicken Sie auf **Fertig**.
   Die Seite **Dienstkonten** wird geöffnet.
8. Wählen Sie auf der Seite **Dienstkonten** das neue Dienstkonto aus und klicken Sie dann unter **Aktionen** auf **Schlüssel verwalten**.
9. Klicken Sie bei **Schlüssel** auf **Schlüssel hinzufügen** –> **Neuen Schlüssel erstellen** und wählen Sie dann **JSON** als Schlüsseltyp aus.
10. Klicken Sie auf **Erstellen**.

Daraufhin wird automatisch eine JSON-Datei mit dem privaten Schlüssel des Dienstkontos auf Ihre Maschine heruntergeladen. Bewahren Sie diese Datei sicher auf, denn diese wird benötigt, um Ihre Google Workspace-Organisation dem Cyber Protection Service hinzufügen zu können.

So können Sie dem neuen Projekt Zugriff auf Ihr Google Workspace-Konto gewähren

1. Wählen Sie im Google Cloud Platform-Navigationsmenü die Elemente **IAM & Admin** –> **Dienstkonten** aus.
2. Suchen Sie in der Liste das von Ihnen erstellte Dienstkonto und kopieren Sie die Client-ID, die in der Spalte **OAuth 2.0-Client-ID** angezeigt wird.
3. Melden Sie sich an der Google-Admin-Konsole (admin.google.com) als Super-Administrator an.
4. Wählen Sie im Navigationsmenü die Elemente **Sicherheit** –> **Zugriff und Datensteuerung** –> **API-Steuerung**.
5. Scrollen Sie auf der Seite **API-Steuerung** nach unten und klicken Sie dann unter **Domänenweite Delegierung** auf **Domänenweite Delegierung verwalten**.
   Daraufhin wird die Seite **Domänenweite Delegierung** geöffnet.
6. Klicken Sie auf der Seite **Domänenweite Delegierung** auf **Neu hinzufügen**.
   Das Fenster **Neue Client-ID hinzufügen** wird geöffnet.
7. Geben Sie im Feld **Client-ID** die Client-ID Ihres Dienstkonto-Clients ein.
8. Kopieren Sie in das Feld **OAuth-Bereiche** die folgende kommaseparierte Bereichsliste und fügen Sie diese ein:

   ```
   https://mail.google.com,https://www.googleapis.com/auth/contacts,https://www.googleapis.com/auth/calendar,https://www.googleapis.com/auth/admin.directory.user.readonly,https://www.googleapis.com/auth/admin.directory.domain.readonly,https://www.googleapis.com/auth/drive,https://www.googleapis.com/auth/gmail.modify
   ```

   Alternativ können Sie die Bereiche auch einzeln pro Zeile hinzufügen:
   - https://mail.google.com
   - https://www.googleapis.com/auth/contacts
   - https://www.googleapis.com/auth/calendar
   - https://www.googleapis.com/auth/admin.directory.user.readonly
   - https://www.googleapis.com/auth/admin.directory.domain.readonly
   - https://www.googleapis.com/auth/drive
   - https://www.googleapis.com/auth/gmail.modify
9. Klicken Sie auf **Autorisieren**.

Als Ergebnis kann Ihr neues Google Cloud-Projekt auf die Daten in Ihrem Google Workspace-Konto zugreifen. Um die Daten sichern zu können, müssen Sie dieses Projekt mit dem Cyber Protection Service verknüpfen. Weitere Informationen über die entsprechende Durchführung finden Sie im Abschnitt '"So können Sie eine Google Workspace-Organisation hinzufügen, indem Sie ein dediziertes persönliches Google Cloud-Projekt verwenden" (S. 705)'.

Wenn Sie den Zugriff Ihres Google Cloud-Projekts auf Ihr Google Workspace-Konto (und damit auch den Zugriff auf den Cyber Protection Service) widerrufen müssen, löschen Sie den API-Client, den Ihr Projekt verwendet.

So können Sie den Zugriff auf Ihr Google Workspace-Konto widerrufen

1. Melden Sie sich an der Google-Admin-Konsole (admin.google.com) als Super-Administrator an.
2. Wählen Sie im Navigationsmenü die Elemente **Sicherheit** –> **Zugriff und Datensteuerung** –> **API-Steuerung**.
3. Scrollen Sie auf der Seite **API-Steuerung** nach unten und klicken Sie dann unter **Domänenweite Delegierung** auf **Domänenweite Delegierung verwalten**.
   Daraufhin wird die Seite **Domänenweite Delegierung** geöffnet.
4. Wählen Sie auf der Seite **Domänenweite Delegierung** den API-Client aus, den Ihr Projekt verwendet, und klicken Sie dann auf **Löschen**.
   Infolgedessen wird Ihr Google Cloud-Projekt und der Cyber Protection Service nicht mehr auf Ihr Google Workspace-Konto zugreifen und die darin enthaltenen Daten sichern können.

Google Workspace-Ressourcen erkennen

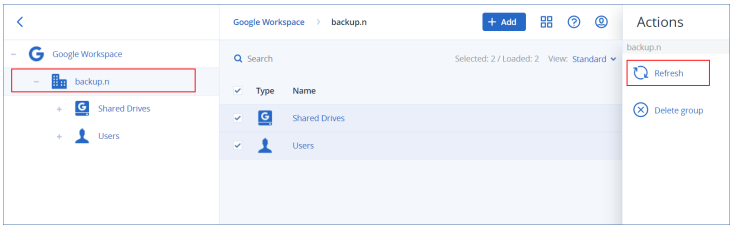
Wenn Sie dem Cyber Protection Service eine Google Workspace-Organisation hinzufügen, werden die Ressourcen in dieser Organisation (wie etwa Postfächer und Google Drives) zur Cyber Protect-Konsole synchronisiert. Diese Aktion wird Erkennung (Englisch: Discovery) genannt und unter **Monitoring** –> **Aktivitäten** protokolliert.

Wenn die Erkennungsaktion abgeschlossen wurde, werden die Ressourcen der Google Workspace-Organisation in der -Konsole auf der Registerkarte **Geräte** –> **Google Workspace** angezeigt. Anschließend können Sie Backup-Pläne auf diese anwenden.

Eine automatische Erkennungsaktion wird einmal pro Tag ausgeführt, damit die Liste der Ressourcen in der Cyber Protect-Konsole stets auf dem neuesten Stand bleibt. Sie können diese Liste auch je nach Bedarf synchronisieren, indem Sie eine Erkennungsaktion manuell ausführen lassen.

So können Sie eine Erkennungsaktion manuell ausführen

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte** –> **Google Workspace**.
2. Wählen Sie zuerst Ihre Google Workspace-Organisation aus und klicken Sie anschließend im Fensterbereich **Aktionen** auf **Aktualisieren**.



Hinweis
Sie können eine Erkennungsaktion bis zu 10 Mal pro Stunde manuell ausführen. Wenn diese Anzahl erreicht ist, werden die erlaubten Ausführungen auf eine pro Stunde zurückgesetzt. Danach wird für jede Stunde eine zusätzliche Ausführung verfügbar, bis die Gesamtzahl von 10 Ausführungen pro Stunde wieder erreicht ist.

Die Häufigkeit von Google Workspace-Backups festlegen

Google Workspace-Backups werden standardmäßig einmal täglich ausgeführt – und es sind keine weiteren Planungsoptionen verfügbar.

Wenn das Advanced Backup-Paket in Ihrem Mandanten aktiviert ist, können Sie häufigere Backups konfigurieren. Sie können die Anzahl der Backups pro Tag festlegen, aber Sie können nicht die Startzeit der Backups konfigurieren. Die Backups werden automatisch und in ungefähren Intervallen gestartet, die wiederum davon abhängen, wie hoch die aktuelle Auslastung des Cloud Agenten ist, der in einem Datacenter mehrere Kunden bedient. Dadurch wird gewährleistet, dass es während des Tages zu einer gleichmäßigen Auslastung kommt und alle Kunden die gleiche Service-Qualität erhalten.

Folgende Optionen sind verfügbar:

Planungsoptionen	Ungefähres Intervall zwischen jedem Backup
Einmal täglich	24 Stunden
Zweimal täglich (Standard)	12 Stunden
3-mal täglich	8 Stunden
6-mal täglich	4 Stunden

Hinweis
Je nach Auslastung des Cloud Agenten und einer möglichen Drosselung auf der Seite von Google Workspace kann ein Backup später als geplant beginnen oder dessen Fertigstellung länger dauern. Wenn ein Backup mehr Zeit benötigt als das durchschnittliche Intervall zwischen zwei Backups lang ist, muss das nächste Backup neu geplant werden, was dazu führen kann, dass weniger Backups pro Tag erstellt werden, als es eigentlich vorgesehen ist. So kann es beispielsweise vorkommen, dass nur zwei Backups pro Tag abgeschlossen werden können, obwohl Sie sechs pro Tag eingestellt haben.

Gmail-Daten sichern

Welche Elemente können per Backup gesichert werden?

Sie können die Postfächer von Gmail-Benutzern per Backup sichern. Ein Postfach-Backup beinhaltet auch die Daten von Kalendern und Kontakten. Optional können Sie auch die freigegebenen

Kalender sichern.

Folgende Elemente werden bei einem Backup *übersprungen*:

- Die Kalender **Geburtstage**, **Erinnerungen** und **Tasks**.
- Ordner, die an Kalenderereignisse angehängt sind
- Der Ordner **Verzeichnis** in den Kontakten.

Folgende Kalenderelemente werden aufgrund von Beschränkungen der Google Calender API *übersprungen*:

- Terminvereinbarungen (Appointment Slots)
- Das Konferenzfeld eines Ereignisses
- Die Kalendereinstellung **Ganztätige Ereignisbenachrichtigungen**
- Die Kalendereinstellung **Automatisch Einladungen hinzufügen** (in Kalendern für Räume oder Gemeinschafsbereiche)

Folgende Kontaktelemente werden aufgrund von Beschränkungen der Google People API *übersprungen*:

- Der Ordner **Weitere Kontakte**
- Die externen Profile eines Kontaktes (**Verzeichnis-Profil**, **Google-Profil**)
- Das Kontaktfeld **Speichern unter**

Welche Elemente können wiederhergestellt werden?

Folgende Elemente können aus einem Postfach-Backup wiederhergestellt werden:

- Postfächer
- E-Mail-Ordner (nach der Terminologie von Google 'Labels' genannt. **Labels** werden in der Backup-Software als Ordner dargestellt, um die Konsistenz mit anderen Datendarstellungen zu gewährleisten.)
- E-Mail-Nachrichten
- Kalenderereignisse
- Kontakte

Sie können eine Suchfunktion verwenden, um bestimmte Elemente in einem Backup zu finden.

Wenn Sie Postfächer oder Postfachelemente wiederherstellen, können Sie auswählen, ob die Elemente am Zielort überschrieben werden sollen (oder nicht).

Einschränkungen

- Kontaktfotos können nicht wiederhergestellt werden
- Das Kalenderelement **Außer Haus** wird aufgrund von Beschränkungen der Google Calender API als reguläres Kalenderereignis wiederhergestellt.

Gmail-Postfächer auswählen

Wählen Sie die Postfächer wie nachfolgend beschrieben aus – und spezifizieren Sie dann die anderen Einstellungen des Schutzplans nach Bedarf.

So können Sie Gmail-Postfächer auswählen

1. Klicken Sie auf **Google Workspace**.
2. Wenn dem Cyber Protection Service mehrere Google Workspace-Organisationen hinzugefügt wurden, wählen Sie diejenige Organisation aus, deren Benutzerdaten Sie sichern wollen. Ansonsten können Sie diesen Schritt überspringen.
3. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Um die Postfächer aller Benutzer zu sichern (einschließlich solcher Postfächer, die erst in der Zukunft erstellt werden), erweitern Sie den Knoten **Benutzer**, wählen Sie **Alle Benutzer** und klicken Sie dann auf **Gruppen-Backup**.
   - Wenn Sie einzelne Benutzerpostfächer sichern wollen, erweitern Sie den Knoten **Benutzer**, wählen Sie **Alle Benutzer**, wählen Sie die Benutzer aus, deren Postfächer Sie sichern wollen, und klicken Sie dann auf **Backup**.
4. Im Schutzplan-Fensterbereich:
   - Überprüfen Sie, dass das Element **Gmail** bei **Backup-Quelle** ausgewählt ist.
   - Wenn Sie Kalender sichern möchten, die für die ausgewählten Benutzer freigegeben wurden, aktivieren Sie den Schalter **Freigegebene Kalender einbeziehen**.
   - Entscheiden Sie, ob Sie die gesicherten E-Mail-Nachrichten per Volltextsuche durchsuchen wollen. Sie finden diese Option, wenn Sie zuerst auf das Zahnradsymbol klicken – und dann auf **Backup-Optionen** –> **Volltextsuche**.

Postfächer und Postfachelemente wiederherstellen

Postfächer wiederherstellen

1. Klicken Sie auf **Google Workspace**.
2. Wenn dem Cyber Protection Service mehrere Google Workspace-Organisationen hinzugefügt wurden, wählen Sie diejenige Organisation aus, deren Backup-Daten Sie wiederherstellen möchten. Ansonsten können Sie diesen Schritt überspringen.
3. Erweitern Sie den Knoten **Benutzer**, wählen Sie die Option **Alle Benutzer**, wählen Sie den Benutzer, dessen Postfach Sie wiederherstellen wollen, und klicken Sie dann auf **Recovery**.

   Wenn der Benutzer zuvor gelöscht wurde, können Sie diesen im Bereich **Cloud-Applikationen-Backups** der Registerkarte 'Backup Storage' auswählen und dann auf **Backups anzeigen** klicken.

   Sie können Benutzer und Gruppen auch per Namen suchen. Platzhalterzeichen (Wildcards) werden nicht unterstützt.
4. Wählen Sie einen Recovery-Punkt.

Hinweis
Wenn Sie nur Recovery-Punkte sehen wollen, die Postfächer enthalten, wählen Sie **Gmail** bei **Nach Inhalt filtern**.

5. Klicken Sie auf **Recovery** –> **Komplettes Postfach**.
6. Wenn dem Cyber Protection Service mehrere Google Workspace-Organisationen hinzugefügt werden, klicken Sie auf **Google Workspace-Organisation**, um die Zielorganisation einsehen, ändern oder spezifizieren zu können.
   Die ursprüngliche Organisation wird automatisch vorausgewählt. Wenn diese Organisation nicht mehr im Cyber Protection Service registriert ist, müssen Sie eine neue Zielorganisation aus den verfügbaren registrierten Organisationen auswählen.
7. Bei**Zu Postfach wiederherstellen** können Sie das gewünschte Zielpostfach anzeigen lassen, ändern oder spezifizieren.
   Das ursprüngliche Postfach wird automatisch vorausgewählt. Wenn dieses Postfach nicht mehr existiert oder Sie eine andere als die ursprüngliche Organisation als Ziel ausgewählt haben, müssen Sie das Zielpostfach spezifizieren.
   Sie können während der Wiederherstellung kein neues Zielpostfach erstellen. Wenn Sie ein Postfach zu einem neuen wiederherstellen wollen, müssen Sie zunächst das Zielpostfach in der gewünschten Google Workspace-Organisation erstellen und dann den Cloud Agenten die Änderung synchronisieren lassen. Der Cloud Agent führt alle 24 Stunden eine automatische Synchronisierung mit Google Workspace durch. Wenn Sie die Änderung sofort synchronisieren wollen, müssen Sie in der Cyber Protect-Konsole die Organisation auf der Seite **Google Workspace** auswählen und dann auf **Aktualisieren** klicken.
8. Klicken Sie auf **Recovery starten**.
9. Wählen Sie eine dieser Überschreiben-Optionen:
   - **Vorhandene Elemente überschreiben**
   - **Vorhandene Elemente nicht überschreiben**
10. Klicken Sie auf **Forsetzen**, um Ihre Entscheidung zu bestätigen.

Postfachelemente wiederherstellen

1. Klicken Sie auf **Google Workspace**.
2. Wenn dem Cyber Protection Service mehrere Google Workspace-Organisationen hinzugefügt wurden, wählen Sie diejenige Organisation aus, deren Backup-Daten Sie wiederherstellen möchten. Ansonsten können Sie diesen Schritt überspringen.
3. Erweitern Sie den Knoten **Benutzer**, wählen Sie die Option **Alle Benutzer**, wählen Sie denjenigen Benutzer aus, in dessen Postfach sich die wiederherzustellenden Elemente ursprünglich befunden haben, und klicken Sie dann auf **Recovery**.

Wenn der Benutzer zuvor gelöscht wurde, können Sie diesen im Bereich **Cloud-Applikationen-Backups** der Registerkarte 'Backup Storage' auswählen und dann auf **Backups anzeigen** klicken.

Sie können Benutzer und Gruppen auch per Namen suchen. Platzhalterzeichen (Wildcards) werden nicht unterstützt.

4. Wählen Sie einen Recovery-Punkt.

Hinweis
Wenn Sie nur Recovery-Punkte sehen wollen, die Postfächer enthalten, wählen Sie **Gmail** bei **Nach Inhalt filtern**.

5. Klicken Sie auf **Recovery** –> **E-Mail-Nachrichten**.
6. Wählen Sie den gewünschten Ordner aus. Wenn das Backup unverschlüsselt ist, können Sie die Suchfunktion verwenden, um eine Liste der gewünschten Datenelemente abzurufen.

   Folgende Suchoptionen sind verfügbar. Platzhalterzeichen (Wildcards) werden nicht unterstützt.

   - Für E-Mail-Nachrichten: Suche per Betreff, Absender, Empfänger, Datum, Name eines Anhangs und Nachrichteninhalt.

     Wenn Sie nach Datum suchen, können Sie ein Start- oder Enddatum (beide inklusive) oder beide Daten auswählen, um innerhalb eines bestimmten Zeitraums zu suchen.

     Wenn Sie nach dem Namen des Anhangs oder im Nachrichteninhalt suchen wollen, erhalten Sie nur dann Ergebnisse, wenn die Option **Volltextsuche** während des Backups aktiviert wurde. Sie können die Sprache des Nachrichtenfragments spezifizieren, das als zusätzlicher Parameter durchsucht werden soll.
   - Für Ereignisse: Suche nach Titel und Datum.
   - Für Kontakte: Suche nach Namen, E-Mail-Adresse und Telefonnummer.
7. Wählen Sie die Elemente aus, die Sie wiederherstellen wollen. Wenn Sie Ordner auswählen wollen, klicken Sie auf das Symbol 'Ordner wiederherstellen'. 

   Zusätzlich haben Sie auch folgende Möglichkeiten:

   - Klicken Sie bei der Auswahl eines Elements auf **Inhalt anzeigen**, um die Inhalte (inklusive Anhänge) einsehen zu können. Klicken Sie auf den Namen einer angehängten Datei, um diese herunterzuladen.
   - Nur bei einem unverschlüsselten Backup, wenn Sie die Suchfunktion verwendet und ein einzelnes Element in den Suchergebnissen ausgewählt haben: klicken Sie auf **Versionen anzeigen**, um die Version des Elements auszuwählen, die Sie wiederherstellen wollen. Sie können jede Backup-Version auswählen, auch wenn diese vor oder nach dem eigentlichen, zuvor ausgewählten Recovery-Punkt liegt.
8. Klicken Sie auf **Recovery**.
9. Wenn dem Cyber Protection Service mehrere Google Workspace-Organisationen hinzugefügt wurden, klicken Sie auf **Google Workspace-Organisation**, um die Zielorganisation einsehen, ändern oder spezifizieren zu können.

Die ursprüngliche Organisation wird automatisch vorausgewählt. Wenn diese Organisation nicht mehr im Cyber Protection Service registriert ist, müssen Sie eine neue Zielorganisation aus den verfügbaren registrierten Organisationen auswählen.

10. Bei**Zu Postfach wiederherstellen** können Sie das gewünschte Zielpostfach anzeigen lassen, ändern oder spezifizieren.

    Das ursprüngliche Postfach wird automatisch vorausgewählt. Wenn dieses Postfach nicht mehr existiert oder Sie eine andere als die ursprüngliche Organisation als Ziel ausgewählt haben, müssen Sie das Zielpostfach spezifizieren.
11. Bei **Pfad** können Sie den Zielordner im Zielpostfach einsehen oder ändern. Standardmäßig ist der ursprüngliche Ordner vorausgewählt.
12. Klicken Sie auf **Recovery starten**.
13. Wählen Sie eine dieser Überschreiben-Optionen:
    - **Vorhandene Elemente überschreiben**
    - **Vorhandene Elemente nicht überschreiben**
14. Klicken Sie auf **Forsetzen**, um Ihre Entscheidung zu bestätigen.

Google Drive-Dateien sichern

Welche Elemente können per Backup gesichert werden?

Sie können ein komplettes Google Drive sichern – oder auch nur einzelne Dateien und Ordner. Dateien werden inklusive ihrer Freigabe-Berechtigungen gesichert.

Wichtig
Folgende Elemente werden nicht gesichert:

- Der Ordner **Für mich freigegeben**
- Der Ordner **Computer** (vom Backup & Sync-Client erstellt)

Einschränkungen

Von den Google-spezifischen Dateiformaten werden Google Docs, Google Sheets sowie Google Slides für Backups und Wiederherstellungen vollständig unterstützt. Andere Google-spezifische Formate werden möglicherweise nicht vollständig oder gar nicht unterstützt – so werden etwa Google Drawings-Dateien als `.svg`-Dateien wiederhergestellt, Google Sites-Dateien als `.txt`-Dateien und Google Jamboard-Dateien als `.pdf`-Dateien, während Google My Maps-Dateien bei einem Backup übersprungen werden.

Hinweis
Dateiformate, die nicht Google-spezifisch sind – wie `.txt`, `.docx`, `.pptx`, `.pdf`, `.jpg`, `.png`, `.zip` – werden bei Backups und Wiederherstellungen vollständig unterstützt.

Welche Elemente können wiederhergestellt werden?

Sie können ein komplettes Google Drive wiederherstellen oder beliebige einzelne Dateien/Ordner, die gesichert wurden.

Sie können wählen, ob die Dateien bei der Wiederherstellung ihre ursprünglichen Freigabe-Berechtigungen aus dem Backup beibehalten sollen – oder ob sie die Berechtigungen desjenigen Ordner übernehmen sollen, in dem sie wiederhergestellt werden.

Einschränkungen

- Kommentare in Dateien werden nicht wiederhergestellt.
- Freigabelinks für Dateien und Ordner werden nicht wiederhergestellt.
- Die **Eigentümer-Einstellungen** für freigegebene Dateien (**Bearbeiter dürfen weder die Zugriffsberechtigung ändern noch neue Personen hinzufügen** und **Optionen zum Herunterladen, Drucken und Kopieren für Kommentatoren und Betrachter deaktivieren**) können während einer Wiederherstellung nicht geändert werden.
- Die Eigentümerschaft für eine freigegebene Datei kann während einer Wiederherstellung nicht geändert werden, wenn die Option **Bearbeiter dürfen weder die Zugriffsberechtigung ändern noch neue Personen hinzufügen** für diesen Ordner aktiviert ist. Diese Einstellung verhindert, dass die Google Drive API die Ordnerberechtigungen auflistet. Die Eigentümerschaft von Dateien in dem Ordner wird korrekt wiederhergestellt.

Google Drive-Dateien auswählen

Wählen Sie die Dateien wie nachfolgend beschrieben aus – und spezifizieren Sie dann die anderen Einstellungen des Schutzplans nach Bedarf.

So können Sie Google Drive-Dateien auswählen

1. Klicken Sie auf **Google Workspace**.
2. Wenn dem Cyber Protection Service mehrere Google Workspace-Organisationen hinzugefügt wurden, wählen Sie diejenige Organisation aus, deren Benutzerdaten Sie sichern wollen. Ansonsten können Sie diesen Schritt überspringen.
3. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Um die Dateien aller Benutzer zu sichern (einschließlich solcher Benutzer, die erst in der Zukunft angelegt werden), erweitern Sie den Knoten **Benutzer**, wählen Sie **Alle Benutzer** und klicken Sie dann auf **Gruppen-Backup**.
   - Wenn Sie die Dateien einzelner Benutzer sichern wollen, erweitern Sie den Knoten **Benutzer**, wählen Sie **Alle Benutzer**, wählen Sie die Benutzer aus, deren Dateien Sie sichern wollen, und klicken Sie dann auf **Backup**.
4. Im Schutzplan-Fensterbereich:
   - Überprüfen Sie, dass das Element **Google Drive** bei **Backup-Quelle** ausgewählt wurde.
   - Wählen Sie bei **Elemente für das Backup** eine der folgenden Möglichkeiten:

- Übernehmen Sie die Voreinstellung **[Alle]** (alle Dateien).
- Spezifizieren Sie die zu sichernden Dateien und Ordner an, indem Sie deren Namen oder Pfade hinzufügen.

  Sie können Platzhalterzeichen (*, ** und ?) verwenden. Ausführlichere Informationen über die Verwendung von Pfaden und Platzhalterzeichen finden Sie im Abschnitt 'Dateifilter'.
- Spezifizieren Sie Dateien und Ordner für das Backup, indem Sie diese per 'Durchsuchen' auswählen.

  Der Link **Durchsuchen** ist nur verfügbar, wenn ein Schutzplan für einen einzelnen Benutzer erstellt wird.

- [Optional] Klicken Sie bei **Elemente für das Backup** auf **Ausschlusskriterien anzeigen**, um zu spezifizieren, ob und welche Dateien und Ordner während des Backup-Prozesses übersprungen werden sollen.

  Dateiausschlusskritieren überschreiben eine vorherige Dateiauswahl, d.h., wenn Sie in beiden Feldern dieselbe Datei spezifizieren, wird diese Datei beim anschließenden Backup übersprungen.
- Wenn Sie für alle zu sichernden Dateien die Beglaubigungsfunktion aktivieren wollen, aktivieren Sie den Schalter **Beglaubigung (Notarization)**. Weitere Informationen zu diesem Thema finden Sie im Abschnitt 'Beglaubigung (Notarization)'.

Google Drive und Google Drive-Dateien wiederherstellen

Ein komplettes Google Drive wiederherstellen

1. Klicken Sie auf **Google Workspace**.
2. Wenn dem Cyber Protection Service mehrere Google Workspace-Organisationen hinzugefügt wurden, wählen Sie diejenige Organisation aus, deren Backup-Daten Sie wiederherstellen möchten. Ansonsten können Sie diesen Schritt überspringen.
3. Erweitern Sie den Knoten **Benutzer**, wählen Sie die Option **Alle Benutzer**, wählen Sie den Benutzer, dessen Google Drive Sie wiederherstellen wollen, und klicken Sie dann auf **Recovery**.

   Wenn der Benutzer zuvor gelöscht wurde, können Sie diesen im Bereich **Cloud-Applikationen-Backups** der Registerkarte 'Backup Storage' auswählen und dann auf **Backups anzeigen** klicken.

   Sie können Benutzer auch per Namen suchen. Platzhalterzeichen (Wildcards) werden nicht unterstützt.
4. Wählen Sie einen Recovery-Punkt.

   Hinweis
   Wenn Sie nur Recovery-Punkte sehen wollen, die Google Drive-Dateien enthalten, wählen Sie **Google Drive** bei **Nach Inhalt filtern**.

5. Klicken Sie auf **Recovery** –> **Komplettes Laufwerk**.

6. Wenn dem Cyber Protection Service mehrere Google Workspace-Organisationen hinzugefügt wurden, klicken Sie auf **Google Workspace-Organisation**, um die Zielorganisation einsehen, ändern oder spezifizieren zu können.

   Die ursprüngliche Organisation wird automatisch vorausgewählt. Wenn diese Organisation nicht mehr im Cyber Protection Service registriert ist, müssen Sie eine neue Zielorganisation aus den verfügbaren registrierten Organisationen auswählen.
7. Bei **Zu Laufwerk wiederherstellen** können Sie den gewünschten Zielbenutzer oder das Ziel-Shared Drive anzeigen lassen, ändern oder spezifizieren.

   Der ursprüngliche Benutzer wird automatisch vorausgewählt. Wenn dieser Benutzer nicht mehr existiert oder Sie eine andere als die ursprüngliche Organisation als Ziel ausgewählt haben, müssen Sie den Zielbenutzer oder das Ziel-Shared Drive spezifizieren.

   Wenn das Backup freigegebene Dateien enthält, werden die Dateien im Stammverzeichnis des Ziellaufwerks (Ziel-Team Drive) wiederhergestellt.
8. Bestimmen Sie, ob Sie auch die Freigabe-Berechtigungen der Dateien mit wiederherstellen wollen.
9. Klicken Sie auf **Recovery starten**.
10. Wählen Sie eine dieser Überschreiben-Optionen:

Option	Beschreibung
Vorhandene Datei überschreiben, wenn diese älter ist	Wenn es am Zielort bereits eine Datei mit dem gleichen Namen gibt, die jedoch älter als die Quelldatei ist, wird die Quelldatei am Zielort gespeichert und dabei die ältere Version ersetzt.
Vorhandene Dateien überschreiben	Alle bereits vorhandenen Dateien am Zielort werden überschrieben, unabhängig von ihrem letzten Änderungsdatum.
Vorhandene Dateien nicht überschreiben	Wenn es am Zielort bereits eine Datei mit dem gleichen Namen gibt, werden keine Änderungen an dieser vorgenommen und die Quelldatei wird nicht am Zielort gespeichert.

11. Klicken Sie auf **Forsetzen**, um Ihre Entscheidung zu bestätigen.

Google Drive-Dateien wiederherstellen

1. Klicken Sie auf **Google Workspace**.
2. Wenn dem Cyber Protection Service mehrere Google Workspace-Organisationen hinzugefügt wurden, wählen Sie diejenige Organisation aus, deren Backup-Daten Sie wiederherstellen möchten. Ansonsten können Sie diesen Schritt überspringen.
3. Erweitern Sie den Knoten **Benutzer**, wählen Sie die Option **Alle Benutzer**, wählen Sie den Benutzer, dessen Google Drive-Dateien Sie wiederherstellen wollen, und klicken Sie dann auf **Recovery**.

   Wenn der Benutzer zuvor gelöscht wurde, können Sie diesen im Bereich **Cloud-Applikationen-Backups** der Registerkarte 'Backup Storage' auswählen und dann auf **Backups anzeigen** klicken.

Sie können Benutzer auch per Namen suchen. Platzhalterzeichen (Wildcards) werden nicht unterstützt.

4. Wählen Sie einen Recovery-Punkt.

   Hinweis
   Wenn Sie nur Recovery-Punkte sehen wollen, die Google Drive-Dateien enthalten, wählen Sie **Google Drive** bei **Nach Inhalt filtern**.

5. Klicken Sie auf **Recovery** –> **Dateien/Ordner**.
6. Wechseln Sie zum benötigten Ordner oder verwenden Sie die Suchfunktion, um eine Liste der erforderlichen Dateien und Ordner abzurufen.
7. Wählen Sie die Dateien, die Sie wiederherstellen wollen.

   Wenn das Backup unverschlüsselt ist und Sie eine einzelne Datei ausgewählt haben, können Sie auf **Versionen anzeigen** klicken, um eine bestimmte Dateiversion auszuwählen, die Sie wiederherstellen wollen. Sie können jede Backup-Version auswählen, auch wenn diese vor oder nach dem eigentlichen, zuvor ausgewählten Recovery-Punkt liegt.
8. Wenn Sie eine Datei herunterladen wollen, müssen Sie diese auswählen, auf **Download** klicken, den Zielspeicherort für die Datei bestimmen und schließlich auf **Speichern** klicken. Ansonsten können Sie diesen Schritt überspringen.
9. Klicken Sie auf **Recovery**.
10. Wenn dem Cyber Protection Service mehrere Google Workspace-Organisationen hinzugefügt wurden, klicken Sie auf **Google Workspace-Organisation**, um die Zielorganisation einsehen, ändern oder spezifizieren zu können.

    Die ursprüngliche Organisation wird automatisch vorausgewählt. Wenn diese Organisation nicht mehr im Cyber Protection Service registriert ist, müssen Sie eine neue Zielorganisation aus den verfügbaren registrierten Organisationen auswählen.
11. Bei **Zu Laufwerk wiederherstellen** können Sie den gewünschten Zielbenutzer oder das Ziel-Shared Drive anzeigen lassen, ändern oder spezifizieren.

    Der ursprüngliche Benutzer wird automatisch vorausgewählt. Wenn dieser Benutzer nicht mehr existiert oder Sie eine andere als die ursprüngliche Organisation als Ziel ausgewählt haben, müssen Sie den Zielbenutzer oder das Ziel-Shared Drive spezifizieren.
12. Bei **Pfad** können Sie den Zielordner im Google Drive des Zielbenutzers oder im Ziel-Shared Drive einsehen oder ändern. Standardmäßig ist der ursprüngliche Speicherort vorausgewählt.
13. Bestimmen Sie, ob Sie auch die Freigabe-Berechtigungen der Dateien mit wiederherstellen wollen.
14. Klicken Sie auf **Recovery starten**.
15. Wählen Sie eine der folgenden Optionen zum Überschreiben:

Option	Beschreibung
Vorhandene Datei überschreiben, wenn	Wenn es am Zielort bereits eine Datei mit dem gleichen Namen gibt, die jedoch älter als die Quelldatei ist, wird die Quelldatei am Zielort gespeichert

Option	Beschreibung
diese älter ist	und dabei die ältere Version ersetzt.
Vorhandene Dateien überschreiben	Alle bereits vorhandenen Dateien am Zielort werden überschrieben, unabhängig von ihrem letzten Änderungsdatum.
Vorhandene Dateien nicht überschreiben	Wenn es am Zielort bereits eine Datei mit dem gleichen Namen gibt, werden keine Änderungen an dieser vorgenommen und die Quelldatei wird nicht am Zielort gespeichert.

16. Klicken Sie auf **Forsetzen**, um Ihre Entscheidung zu bestätigen.

Shared Drive-Dateien sichern

Welche Elemente können per Backup gesichert werden?

Sie können ein komplettes Shared Drive per Backup sichern – oder auch nur einzelne Dateien und Ordner. Dateien werden inklusive ihrer Freigabe-Berechtigungen gesichert.

Wichtig
Der Ordner **Für mich freigegeben** wird nicht per Backup gesichert.

Einschränkungen

- Ein Shared Drive ohne Mitglieder kann aufgrund von Beschränkungen der Google Drive API nicht gesichert werden.
- Von den Google-spezifischen Dateiformaten werden Google Docs, Google Sheets sowie Google Slides für Backups und Wiederherstellungen vollständig unterstützt. Andere Google-spezifische Formate werden möglicherweise nicht vollständig oder gar nicht unterstützt – so werden etwa Google Drawings-Dateien als `.svg`-Dateien wiederhergestellt, Google Sites-Dateien als `.txt`-Dateien und Google Jamboard-Dateien als `.pdf`-Dateien, während Google My Maps-Dateien bei einem Backup übersprungen werden.

  Hinweis
  Dateiformate, die nicht Google-spezifisch sind – wie `.txt`, `.docx`, `.pptx`, `.pdf`, `.jpg`, `.png`, `.zip` – werden bei Backups und Wiederherstellungen vollständig unterstützt.

Welche Elemente können wiederhergestellt werden?

Sie können ein komplettes Shared Drive wiederherstellen oder beliebige einzelne Dateien/Ordner, die gesichert wurden.

Sie können wählen, ob die Dateien bei der Wiederherstellung ihre ursprünglichen Freigabe-Berechtigungen aus dem Backup beibehalten sollen – oder ob sie die Berechtigungen desjenigen Ordner übernehmen sollen, in dem sie wiederhergestellt werden.

Folgende Elemente werden nicht wiederhergestellt:

- Freigabe-Berechtigungen für eine Datei, die für einen Benutzer außerhalb der Organisation freigegeben wurde, werden nicht wiederhergestellt, wenn im als Ziel verwendeten Shared Drive der Dateizugriff für Personen außerhalb der Organisation deaktiviert ist.
- Freigabe-Berechtigungen für eine Datei, die für einen Benutzer freigegeben wurde, der kein Mitglied des als Ziel verwendeten Shared Drive ist, werden nicht wiederhergestellt, wenn die Option **Freigabe für Nichtmitglieder** im als Ziel verwendeten Shared Drive deaktiviert ist.

Einschränkungen

- Kommentare in Dateien werden nicht wiederhergestellt.
- Freigabelinks für Dateien und Ordner werden nicht wiederhergestellt.

Shared Drive-Dateien auswählen

Wählen Sie die Dateien wie nachfolgend beschrieben aus – und spezifizieren Sie dann die anderen Einstellungen des Schutzplans nach Bedarf.

So können Sie Shared Drive-Dateien auswählen

1. Klicken Sie auf **Google Workspace**.
2. Wenn dem Cyber Protection Service mehrere Google Workspace-Organisationen hinzugefügt wurden, wählen Sie diejenige Organisation aus, deren Benutzerdaten Sie sichern wollen. Ansonsten können Sie diesen Schritt überspringen.
3. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Um die Dateien aller Shared Drives zu sichern (einschließlich solcher Shared Drives, die erst in der Zukunft erstellt werden), erweitern Sie den Knoten **Shared Drives**, wählen Sie **Alle Shared Drives** und klicken Sie dann auf **Gruppen-Backup**.
   - Wenn Sie die Dateien einzelner Shared Drives sichern wollen, erweitern Sie den Knoten **Shared Drives**, wählen Sie **Alle Shared Drives**, wählen Sie diejenigen Shared Drives aus, die Sie sichern wollen, und klicken Sie dann auf **Backup**.
4. Im Schutzplan-Fensterbereich:
   - Wählen Sie bei **Elemente für das Backup** eine der folgenden Möglichkeiten:
     - Übernehmen Sie die Voreinstellung **[Alle]** (alle Dateien).
     - Spezifizieren Sie die zu sichernden Dateien und Ordner an, indem Sie deren Namen oder Pfade hinzufügen.

       Sie können Platzhalterzeichen (*, ** und ?) verwenden. Ausführlichere Informationen über die Verwendung von Pfaden und Platzhalterzeichen finden Sie im Abschnitt 'Dateifilter'.
     - Spezifizieren Sie Dateien und Ordner für das Backup, indem Sie diese per 'Durchsuchen' auswählen.

       Der Link **Durchsuchen** ist nur verfügbar, wenn ein Schutzplan für ein einzelnes Shared Drive erstellt wird.
   - [Optional] Klicken Sie bei **Elemente für das Backup** auf **Ausschlusskriterien anzeigen**, um zu spezifizieren, ob und welche Dateien und Ordner während des Backup-Prozesses

übersprungen werden sollen.

Dateiausschlusskritieren überschreiben eine vorherige Dateiauswahl, d.h., wenn Sie in beiden Feldern dieselbe Datei spezifizieren, wird diese Datei beim anschließenden Backup übersprungen.

- Wenn Sie für alle zu sichernden Dateien die Beglaubigungsfunktion aktivieren wollen, aktivieren Sie den Schalter **Beglaubigung (Notarization)**. Weitere Informationen zu diesem Thema finden Sie im Abschnitt 'Beglaubigung (Notarization)'.

Ein Shared Drive und Shared Drive-Dateien wiederherstellen

Ein komplettes Shared Drive wiederherstellen

1. Klicken Sie auf **Google Workspace**.
2. Wenn dem Cyber Protection Service mehrere Google Workspace-Organisationen hinzugefügt wurden, wählen Sie diejenige Organisation aus, deren Backup-Daten Sie wiederherstellen möchten. Ansonsten können Sie diesen Schritt überspringen.
3. Erweitern Sie den Knoten **Shared Drives**, wählen Sie die Option **Alle Shared Drives**, wählen Sie das wiederherzustellende Shared Drive aus und klicken Sie dann auf **Recovery**.

   Wenn das Shared Drive zuvor gelöscht wurde, können Sie diese im Bereich **Cloud-Applikationen-Backups** der Registerkarte 'Backup Storage' auswählen und dann auf **Backups anzeigen** klicken.

   Sie können die Shared Drives nach einem Namen durchsuchen. Platzhalterzeichen (Wildcards) werden nicht unterstützt.
4. Wählen Sie einen Recovery-Punkt.
5. Klicken Sie auf **Recovery** –> **Komplettes Shared Drive**.
6. Wenn dem Cyber Protection Service mehrere Google Workspace-Organisationen hinzugefügt wurden, klicken Sie auf **Google Workspace-Organisation**, um die Zielorganisation einsehen, ändern oder spezifizieren zu können.

   Die ursprüngliche Organisation wird automatisch vorausgewählt. Wenn diese Organisation nicht mehr im Cyber Protection Service registriert ist, müssen Sie eine neue Zielorganisation aus den verfügbaren registrierten Organisationen auswählen.
7. Bei **Zu Laufwerk wiederherstellen** können Sie den gewünschten Zielbenutzer oder das Ziel-Shared Drive anzeigen lassen, ändern oder spezifizieren. Wenn Sie einen Benutzer angeben, werden die Daten zu dem Google Drive dieses Benutzers wiederhergestellt.

   Standardmäßig ist das ursprüngliche Shared Drive vorausgewählt. Wenn dieses Shared Drive nicht mehr existiert oder Sie eine andere als die ursprüngliche Organisation als Ziel ausgewählt haben, müssen Sie den Zielbenutzer oder das Ziel-Shared Drive spezifizieren.
8. Bestimmen Sie, ob Sie auch die Freigabe-Berechtigungen der Dateien mit wiederherstellen wollen.
9. Klicken Sie auf **Recovery starten**.

10. Wählen Sie eine dieser Überschreiben-Optionen:

Option	Beschreibung
Vorhandene Datei überschreiben, wenn diese älter ist	Wenn es am Zielort bereits eine Datei mit dem gleichen Namen gibt, die jedoch älter als die Quelldatei ist, wird die Quelldatei am Zielort gespeichert und dabei die ältere Version ersetzt.
Vorhandene Dateien überschreiben	Alle bereits vorhandenen Dateien am Zielort werden überschrieben, unabhängig von ihrem letzten Änderungsdatum.
Vorhandene Dateien nicht überschreiben	Wenn es am Zielort bereits eine Datei mit dem gleichen Namen gibt, werden keine Änderungen an dieser vorgenommen und die Quelldatei wird nicht am Zielort gespeichert.

11. Klicken Sie auf **Forsetzen**, um Ihre Entscheidung zu bestätigen.

Shared Drive-Dateien wiederherstellen

1. Klicken Sie auf **Google Workspace**.
2. Wenn dem Cyber Protection Service mehrere Google Workspace-Organisationen hinzugefügt wurden, wählen Sie diejenige Organisation aus, deren Backup-Daten Sie wiederherstellen möchten. Ansonsten können Sie diesen Schritt überspringen.
3. Erweitern Sie den Knoten **Shared Drives**, wählen Sie die Option **Alle Shared Drives**, wählen Sie dasjenige Shared Drive aus, in dem sich die wiederherzustellenden Dateien ursprünglich befunden haben, und klicken Sie dann auf **Recovery**.

   Wenn das Shared Drive zuvor gelöscht wurde, können Sie diese im Bereich **Cloud-Applikationen-Backups** der Registerkarte 'Backup Storage' auswählen und dann auf **Backups anzeigen** klicken.

   Sie können die Shared Drives nach einem Namen durchsuchen. Platzhalterzeichen (Wildcards) werden nicht unterstützt.
4. Wählen Sie einen Recovery-Punkt.
5. Klicken Sie auf **Recovery** –> **Dateien/Ordner**.
6. Wechseln Sie zum benötigten Ordner oder verwenden Sie die Suchfunktion, um eine Liste der erforderlichen Dateien und Ordner abzurufen.
7. Wählen Sie die Dateien, die Sie wiederherstellen wollen.

   Wenn das Backup unverschlüsselt ist und Sie eine einzelne Datei ausgewählt haben, können Sie auf **Versionen anzeigen** klicken, um eine bestimmte Dateiversion auszuwählen, die Sie wiederherstellen wollen. Sie können jede Backup-Version auswählen, auch wenn diese vor oder nach dem eigentlichen, zuvor ausgewählten Recovery-Punkt liegt.
8. Wenn Sie eine Datei herunterladen wollen, müssen Sie diese auswählen, auf **Download** klicken, den Zielspeicherort für die Datei bestimmen und schließlich auf **Speichern** klicken. Ansonsten können Sie diesen Schritt überspringen.
9. Klicken Sie auf **Recovery**.

10. Wenn dem Cyber Protection Service mehrere Google Workspace-Organisationen hinzugefügt wurden, klicken Sie auf **Google Workspace-Organisation**, um die Zielorganisation einsehen, ändern oder spezifizieren zu können.

    Die ursprüngliche Organisation wird automatisch vorausgewählt. Wenn diese Organisation nicht mehr im Cyber Protection Service registriert ist, müssen Sie eine neue Zielorganisation aus den verfügbaren registrierten Organisationen auswählen.
11. Bei **Zu Laufwerk wiederherstellen** können Sie den gewünschten Zielbenutzer oder das Ziel-Shared Drive anzeigen lassen, ändern oder spezifizieren. Wenn Sie einen Benutzer angeben, werden die Daten zu dem Google Drive dieses Benutzers wiederhergestellt.

    Standardmäßig ist das ursprüngliche Shared Drive vorausgewählt. Wenn dieses Shared Drive nicht mehr existiert oder Sie eine andere als die ursprüngliche Organisation als Ziel ausgewählt haben, müssen Sie den Zielbenutzer oder das Ziel-Shared Drive spezifizieren.
12. Bei **Pfad** können Sie den Zielordner im Google Drive des Zielbenutzers oder im Ziel-Shared Drive einsehen oder ändern. Standardmäßig ist der ursprüngliche Speicherort vorausgewählt.
13. Bestimmen Sie, ob Sie auch die Freigabe-Berechtigungen der Dateien mit wiederherstellen wollen.
14. Klicken Sie auf **Recovery starten**.
15. Wählen Sie eine der folgenden Optionen zum Überschreiben:

Option	Beschreibung
Vorhandene Datei überschreiben, wenn diese älter ist	Wenn es am Zielort bereits eine Datei mit dem gleichen Namen gibt, die jedoch älter als die Quelldatei ist, wird die Quelldatei am Zielort gespeichert und dabei die ältere Version ersetzt.
Vorhandene Dateien überschreiben	Alle bereits vorhandenen Dateien am Zielort werden überschrieben, unabhängig von ihrem letzten Änderungsdatum.
Vorhandene Dateien nicht überschreiben	Wenn es am Zielort bereits eine Datei mit dem gleichen Namen gibt, werden keine Änderungen an dieser vorgenommen und die Quelldatei wird nicht am Zielort gespeichert.

16. Klicken Sie auf **Forsetzen**, um Ihre Entscheidung zu bestätigen.

Beglaubigung (Notarization)

Mit der Beglaubigungsfunktion können Sie überprüfen und belegen, ob und dass Ihre gesicherten Dateien seit dem Backup authentisch und unverändert geblieben sind. Wir empfehlen die Nutzung dieser Funktion, wenn Sie wichtige Dateien (wie rechtlich relevante Dokumente) sichern, deren Authentizität Sie später einmal überprüfen wollen/müssen.

Die Beglaubigungsfunktion ist nur für Backups von Google Drive-Dateien und Google Workspace Shared Drive-Dateien verfügbar.

So können Sie die Beglaubigungsfunktion verwenden

Wenn Sie die Beglaubigungsfunktion für alle zum Backup ausgewählten Dateien aktivieren wollen, müssen Sie beim Erstellen des entsprechenden Schutzplans den Schalter **Beglaubigung (Notarization)** einschalten.

Wenn Sie eine Wiederherstellung konfigurieren, werden die beglaubigten Dateien durch ein spezielles Symbol gekennzeichnet. Das bedeutet, dass Sie die Authentizität dieser Dateien überprüfen können.

Und so funktioniert es

Der Agent berechnet während eines Backups die Hash-Werte der gesicherten Dateien, erstellt einen Hash-Baum (basierend auf der Ordnerstruktur), speichert diesen Hash-Baum mit im Backup und sendet dann das Stammverzeichnis (Root) des Hash-Baums an den Notary Service. Der Notary Service speichert das Wurzelverzeichnis des Hash-Baums in der Blockchain-Datenbank von Ethereum. Damit wird sichergestellt, dass dieser Wert nicht mehr geändert werden kann.

Wenn die Authentizität einer Datei überprüft werden soll, berechnet der Agent den Hash-Wert der Datei und vergleicht diesen dann mit dem Hash-Wert, der im Hash-Baum innerhalb des Backups gespeichert ist. Sollten diese Hash-Werte nicht übereinstimmen, wird die Datei als 'nicht authentisch' eingestuft. Im anderen Fall ist die Authentizität der Datei durch den Hash-Baum verbürgt.

Um zu verifizieren, dass der Hash-Baum selbst nicht kompromittiert wurde, sendet der Agent den Wert des Hash-Baum-Wurzelverzeichnisses an den Notary Service. Der Notary Service vergleicht diesen Wert mit dem, der in der Blockchain-Datenbank gespeichert ist. Wenn die Hash-Werte übereinstimmen, ist die ausgewählte Datei garantiert authentisch. Falls nicht, zeigt die Software über eine Nachricht an, dass die Datei nicht authentisch ist.

Die Authentizität von Dateien mit dem Notary Service überprüfen

Falls die Beglaubigungsfunktion (Notarization) während eines Backups aktiviert wurde, können Sie später bei Bedarf die Authentizität einer gesicherten Datei überprüfen.

So können Sie die Authentizität von Dateien überprüfen

1. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Wenn Sie die Authentizität einer Google Drive-Datei überprüfen wollen, müssen Sie die Datei wie in Schritt 1-7 des Abschnitts 'Google Drive-Dateien wiederherstellen' beschrieben auswählen.
   - Wenn Sie die Authentizität einer Google Workspace Shared Drive-Datei überprüfen wollen, müssen Sie die Datei wie in Schritt 1-7 des Abschnitts 'Shared Drive-Dateien wiederherstellen' beschrieben auswählen.

2. Überprüfen Sie, dass die ausgewählte Datei mit dem folgenden Symbol gekennzeichet ist:  . Das bedeutet, dass die Datei 'beglaubigt' (notarized) ist.
3. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Klicken Sie auf **Verifizieren**.
     Die Software überprüft die Authentizität der Datei und zeigt das Ergebnis an.
   - Klicken Sie auf **Zertifikat abrufen**.
     Ein Zertifikat, das die Dateibeglaubigung bestätigt, wird in einem Webbrowser-Fenster geöffnet. In dem Fenster werden außerdem Anweisungen angezeigt, wie Sie die Dateiauthentizität manuell überprüfen können.

In Cloud-zu-Cloud-Backups suchen

Bei der Wiederherstellung von Daten können Sie auch, statt das ganze Backup-Archiv durchsuchen zu müssen, gezielt nach bestimmten gesicherten Elementen suchen.

Bei nicht verschlüsselten Backups ist die Suchfunktion immer verfügbar. Es wird nur die erweiterte (indexbasierte) Suche unterstützt.

Die indexbasierte Suche ist schneller und bietet zusätzliche Optionen – wie etwa Dateiversionen von gesicherten Elementen anzuzeigen, nach Namen von Dateianhängen in E-Mails zu suchen oder eine Volltextsuche in Gmail-Backups durchzuführen.

Die erweiterte (indexbasierte) Suche kann auch für verschlüsselte Backups aktiviert werden. Wenn Sie die erweiterte Suche nicht aktivieren, ist nur die Basissuche für Backups von Microsoft 365-Postfächern verfügbar. Für alle anderen Workloads ist keine Suche verfügbar.

In der nachfolgenden Tabelle werden die verfügbaren Optionen für verschlüsselte Backups zusammengefasst.

Workloadtyp	Recovery-Quelle	Die erweiterte Suche ist deaktiviert	Die erweiterte Suche ist aktiviert
Microsoft 365-Workloads			
Postfach	E-Mail-Nachrichten	Die Basissuche (nicht indexbasiert) ist verfügbar	Die erweiterte Suche (indexbasiert) ist verfügbar
OneDrive	Dateien/Ordner	Die Suche ist nicht verfügbar	Die erweiterte Suche (indexbasiert) ist verfügbar
SharePoint-Website	SharePoint-Dateien	Die Suche ist nicht verfügbar	Die erweiterte Suche (indexbasiert) ist verfügbar
Teams	Kanäle	Die Suche ist nicht verfügbar	Die erweiterte Suche (indexbasiert) ist verfügbar
	E-Mail-Nachrichten	Die Basissuche (nicht indexbasiert) ist verfügbar	Die erweiterte Suche (indexbasiert) ist verfügbar

Workloadtyp	Recovery-Quelle	Die erweiterte Suche ist deaktiviert	Die erweiterte Suche ist aktiviert
	Die Team-Website	Die Suche ist nicht verfügbar	Die erweiterte Suche (indexbasiert) ist verfügbar
Google Workspace-Workloads			
Postfach	E-Mail-Nachrichten	Die Suche ist nicht verfügbar	Die erweiterte Suche (indexbasiert) ist verfügbar
Google Drive	Dateien/Ordner	Die Suche ist nicht verfügbar	Die erweiterte Suche (indexbasiert) ist verfügbar
Shared Drives	Dateien/Ordner	Die Suche ist nicht verfügbar	Die erweiterte Suche (indexbasiert) ist verfügbar

Volltextsuche

Die Volltextsuche steht nur für Gmail-Backups zur Verfügung. Sie ist standardmäßig aktiviert. Mit ihr können Sie im eigentlichen Textkörper (Haupttext) der per Backup gesicherten E-Mails suchen. Wenn diese Option deaktiviert ist, können Sie nur nach Betreff, Absender, Empfänger und Datum suchen.

Der Index für eine Volltextsuche benötigt 10–30% des vom Gmail-Backup belegten Speicherplatzes. Ein Index ohne Volltextsuchdaten ist deutlich kleiner. Wenn Sie Speicherplatz sparen wollen, können Sie die Volltextsuche deaktivieren und den Teil des Indexes löschen, der die Volltextsuchdaten enthält.

Suchindizes

Suchindizes ermöglichen erweiterte Suchfähigkeiten in Cloud-zu-Cloud-Backup-Archiven.

Die Archive werden nach jeder Backup-Aktion automatisch indiziert. Der Indizierungsprozess hat keinen Einfluss auf die Backup-Performance, da die Indizierung und das Backup von unterschiedlichen Software-Komponenten durchgeführt werden.

Die Möglichkeit zur Anzeige von Suchergebnissen ist erst dann verfügbar, wenn die Indizierungsaktion abgeschlossen wurde. Das kann bis zu 24 Stunden dauern. Eine Indizierung des ersten Backups, bei dem es sich um ein Voll-Backup handelt, dauert in der Regel länger als die Indizierung der nachfolgenden inkrementellen Backups.

Alle Indizes enthalten Metadaten, die die wichtigste Such-Möglichkeiten, nämlich das Suchen nach Betreff, Absender, Empfänger oder Datum, unterstützen. Die Indizes für Gmail-Backups enthalten zusätzliche Daten, wenn die Volltextsuche aktiviert wurde.

Die Größe eines Suchindexes überprüfen

Suchindizes werden mit der Zeit immer größer. Die Indizes für Backup-Archive, in denen die Volltextsuche aktiviert ist, können bis zu 30 Prozent der Archivgröße beanspruchen.

So können Sie die Größe eines Suchindexes überprüfen

1. Melden Sie sich als Administrator an der Cyber Protect-Konsole an.
2. Klicken Sie in der Registerkarte **Backup Storage** den **Cloud-Applikationen-Backup**.
3. Überprüfen Sie den Wert in der Spalte **Indexgröße**.

Indizes aktualisieren, neu aufbauen oder löschen

Um Probleme bei der Suche in Cloud-zu-Cloud Backups zu beheben, kann es notwendig sein, die Suchindizes zu aktualisieren, neu zu erstellen oder zu löschen.

Hinweis
Wir empfehlen Ihnen, das Support-Team zu kontaktieren, bevor Sie einen Index aktualisieren, neu erstellen oder löschen.

So können Sie einen Index aktualisieren, neu aufbauen oder löschen

1. Melden Sie sich als Administrator an der Cyber Protect-Konsole an.
2. Klicken Sie in der Registerkarte **Backup Storage** den **Cloud-Applikationen-Backup**.
   Wählen Sie das Archiv, dessen Index Sie aktualisieren, neu aufbauen oder löschen wollen.
   Die Verfügbarkeit dieser Aktionen hängt folgendermaßen von der Administrator-Ebene und -Rolle ab:

Kontoebene	Rolle	Kann den Index aktualisieren	Kann den Index neu aufbauen	Kann den Index löschen
Partner-Mandant	Firmenadministrator	+	+	+
	Cyber Protection-Administrator	+	-	-
	Schutz-Administrator	+	-	-
	Nur-Lesen-Schutz-Administrator	-	-	-
Kunden-Mandant	Firmenadministrator	+	-	-
	Schutz-Administrator	+	-	-
	Nur-Lesen-Schutz-Administrator	-	-	-

Kontoebene	Rolle	Kann den Index aktualisieren	Kann den Index neu aufbauen	Kann den Index löschen
Abteilung	Abteilungsadministrator	+	-	-
	Schutz-Administrator	+	-	-
	Nur-Lesen-Schutz-Administrator	-	-	-

3. Wählen Sie im Fensterbereich **Aktionen** diejenige Aktion aus, die Sie durchführen wollen:
   - **Index aktualisieren** – die Recovery-Punkte im Archiv werden überprüft und die fehlenden Indizes werden hinzugefügt.
   - **Index neu aufbauen** – die Indizes für alle Recovery-Punkte im Archiv werden gelöscht und anschließend werden die Indizes neu erstellt.
   - **Index löschen** – die Indizes für alle Recovery-Punkte im Archiv werden gelöscht.
4. [Für verschlüsselte Archive] Spezifizieren Sie das Verschlüsselungskennwort und klicken Sie anschließend auf **OK**.
5. Wählen Sie den Aktionsbereich und klicken Sie dann auf **OK**.
   Je nach Archiv und gewählter Aktion sind eine oder mehrere der folgenden Optionen verfügbar:
   - **Nur Metadaten**
   - **Nur Inhalte**
   - **Metadaten- und Inhaltssuche**

Die erweiterte Suche für verschlüsselte Backups aktivieren

Wenn Sie einen Backup-Plan für ein verschlüsseltes Cloud-zu-Cloud-Backup erstellen, können Sie die erweiterte (indexbasierte) Suche aktivieren.

Wenn Sie die erweiterte Suche nicht aktivieren, ist nur die Basissuche für Backups von Microsoft 365-Postfächern verfügbar. Für alle anderen Workloads ist keine Suche verfügbar. Weitere Informationen über die verfügbaren Optionen finden Sie im Abschnitt '"In Cloud-zu-Cloud-Backups suchen" (S. 727)'.

Hinweis
Diese Funktionalität steht nur in ausgewählten Datacentern zur Verfügung und ist möglicherweise nicht für alle Kunden zugänglich.

So können Sie die erweiterte Suche für verschlüsselte Backups aktivieren

1. Aktivieren Sie beim Erstellen eines Backup-Plans den Schalter **Verschlüsselung**.
2. Spezifizieren und bestätigen Sie das Verschlüsselungskennwort.
3. Aktivieren Sie das Kontrollkästchen **Erweitertes Suchen in verschlüsselten Backups**

erlauben.

4. Klicken Sie auf **Fertig**.

Hinweis
Sie können die Verschlüsselung nicht deaktivieren oder das Verschlüsselungskennwort nachträglich ändern. Wenn Sie ein nicht verschlüsseltes Backup erstellen oder das Verschlüsselungskennwort ändern wollen, müssen Sie einen neuen Backup-Plan erstellen.

Die erweiterte Suche in bestehenden Plänen aktivieren oder deaktivieren

Sie können einen bestehenden Plan für verschlüsselte Backups bearbeiten, um die erweiterte (indexbasierte) Suche zu aktivieren oder zu deaktivieren.

Wenn Sie die erweiterte Suche nicht aktivieren, ist nur die Basissuche für Backups von Microsoft 365-Postfächern verfügbar. Für alle anderen Workloads ist keine Suche verfügbar. Weitere Informationen über die verfügbaren Optionen finden Sie im Abschnitt '"In Cloud-zu-Cloud-Backups suchen" (S. 727)'.

Bei nicht verschlüsselten Backups ist die erweiterte Suchfunktion immer verfügbar. Diese Option kann nicht deaktiviert werden.

So können Sie die erweiterte Suche für verschlüsselte Backups aktivieren oder deaktivieren

1. Klicken Sie beim Bearbeiten eines Backup-Plans, in dem die Verschlüsselung aktiviert ist, auf das Zahnrad-Symbol in der rechten oberen Ecke.
2. Schalten Sie auf der Registerkarte **Suchoptionen** den Schalter nach Bedarf entsprechend um.
3. Klicken Sie auf **Fertig**.
4. Klicken Sie auf **Einstellungen speichern**.

Hinweis
Wenn Sie die erweiterte Suche wieder aktivieren, werden alle von diesem Backup-Plan erstellten Archive erneut indiziert. Das ist eine zeitaufwendige Aktion.

Die Volltextsuche für Gmail-Backups deaktivieren

Die Volltextsuche steht nur für Gmail-Backups zur Verfügung. Sie ist standardmäßig aktiviert. Mit ihr können Sie im eigentlichen Textkörper (Haupttext) der per Backup gesicherten E-Mails suchen. Wenn diese Option deaktiviert ist, können Sie nur nach Betreff, Absender, Empfänger und Datum suchen.

Es kann beispielsweise sinnvoll sein, die Volltextsuche zu deaktivieren, wenn Sie die Größe des Suchindexes gering halten wollen.

So können Sie die Volltextsuche deaktivieren

1. Klicken Sie beim Erstellen oder Bearbeiten eines Backup-Plans auf das Zahnrad-Symbol in der rechten oberen Ecke.
2. Deaktivieren Sie auf der Registerkarte **Volltextsuche** den entsprechenden Schalter.
3. Klicken Sie auf **Fertig**.
4. [Beim Erstellen eines Plans] Klicken Sie auf **Anwenden**.
5. [Beim Bearbeiten eines Plans] Klicken Sie auf **Einstellungen speichern**.

Hinweis
Wenn Sie die Volltextsuche wieder aktivieren, werden alle von diesem Backup-Plan erstellten Archive erneut indiziert. Das ist eine zeitaufwendige Aktion.

Oracle Database sichern

Hinweis
Diese Funktion ist über das Advanced Backup-Paket verfügbar.

Die Sicherung von Oracle Database wird in einem separaten Dokument erläutert, welches hier verfügbar ist: https://dl.managed-protection.com/u/pdf/OracleBackup_whitepaper_en-US.pdf

SAP HANA sichern

Hinweis
Diese Funktion ist über das Advanced Backup-Paket verfügbar.

Die Sicherung von SAP HANA wird in einem separaten Dokument erläutert, welches hier verfügbar ist: https://dl.managed-protection.com/u/pdf/SAP_HANA_backup_whitepaper_en-US.pdf

MySQL- und MariaDB-Daten schützen

Sie können MySQL- oder MariaDB-Daten mit einem applikationskonformen Backup schützen. Das Backup sammelt Applikations-Metadaten und ermöglicht granulare Wiederherstellungen auf Instanz-, Datenbank- oder Tabellenebene.

Hinweis
Applikationskonforme Backups von MySQL- oder MariaDB-Daten sind über das Advanced Backup-Paket verfügbar.

Wenn Sie eine physische oder virtuelle Maschine, auf der MySQL- oder MariaDB-Instanzen laufen, mit einem applikationskonformen Backup schützen wollen, muss der Agent für MySQL/MariaDB auf dieser Maschine installiert sein. Der Agent für MySQL/MariaDB kommt im Bundle mit dem Agenten für Linux (64 Bit) und kann daher nur auf Linux-Betriebssystemen mit 64 Bit installiert werden. Siehe Abschnitt '"Unterstützte Betriebssysteme und Umgebungen" (S. 25)'.

So können Sie die Installationsdatei des Agenten für Linux (64 Bit) herunterladen

1. Melden Sie sich an der Cyber Protect-Konsole an.
2. Klicken Sie auf das Symbol 'Konto' in der oberen rechten Ecke und wählen Sie dann **Downloads**.
3. Klicken Sie auf **Agent für Linux (64 Bit)**.

Die Installationsdatei wird auf Ihrer Maschine heruntergeladen. Gehen Sie zur Installation des Agenten vor, wie im Abschnitt '"Protection Agenten in Linux installieren" (S. 84)' oder '"Unbeaufsichtigte Installation oder Deinstallation unter Linux" (S. 113)' erläutert. Stellen Sie sicher, dass Sie den Agenten für MySQL/MariaDB auswählen, der eine optionale Komponente ist.

Um Datenbanken und Tabellen zu einer Live-Instanz wiederherstellen zu können, benötigt der Agent für MySQL/MariaDB einen temporären Storage für seine Operationen. Standardmäßig wird dafür das Verzeichnis `/tmp` verwendet. Sie können dieses Verzeichnis ändern, indem Sie die Umgebungsvariable `ACRONIS_MYSQL_RESTORE_DIR` festlegen.

Einschränkungen

- Es werden keine MySQL- oder MariaDB-Cluster unterstützt.
- Es werden keine MySQL- oder MariaDB-Instanzen unterstützt, die in Docker-Containern ausgeführt werden.
- Es werden keine MySQL- oder MariaDB-Instanzen unterstützt, die auf Betriebssystemen laufen, die das BTRFS-Dateisystem verwenden.
- Systemdatenbanken (`sys`, `mysql`, `information-schema` und `performance_schema`) sowie Datenbanken, die keine Tabellen enthalten, können nicht zu Live-Instanzen wiederhergestellt werden. Diese Datenbanken können jedoch als Dateien wiederhergestellt werden, wenn die komplette Instanz wiederhergestellt wird.
- Wiederherstellungen werden nur zu Zielinstanzen unterstützt, die dieselbe Version (oder eine höhere) wie die ursprünglich gesicherte Instanz haben, wobei es folgende Einschränkungen gibt:
  - Es werden keine Wiederherstellungen von MySQL 5.x-Instanzen zu MySQL 8.x-Instanzen unterstützt.
  - Wiederherstellungen zu einer höheren Version von MySQL 5.x (einschließlich der Nebenversionen) werden nur in der Form unterstützt, dass die komplette Instanz als Dateien wiederhergestellt wird. Bevor Sie Wiederherstellungsversuche unternehmen, sollten Sie sich in der offiziellen MySQL-Upgrade-Anleitung für die jeweilige Zielversion informieren – zum Beispiel in der MySQL 5.7-Upgrade-Anleitung.
- Es werden keine Wiederherstellungen aus Backups unterstützt, die in der Secure Zone gespeichert sind.
- Datenbanken und Tabellen können nicht durch den Agent für MySQL/MariaDB wiederhergestellt werden, wenn dieser auf einer Maschine läuft, auf der AppArmor installiert ist. Sie können immer noch eine Instanz als Dateien oder die komplette Maschine wiederherstellen.

- Es werden keine Wiederherstellungen zu Zieldatenbanken unterstützt, die mit symbolischen Links konfiguriert sind. Sie können die gesicherten Datenbanken als neue Datenbanken wiederherstellen, indem Sie deren Namen ändern.

Bekannte Probleme und Sachverhalte

Wenn Sie bei der Datenwiederherstellung von kennwortgeschützten Samba-Freigaben auf Probleme stoßen, sollten Sie sich von der Cyber Protect-Konsole abmelden und anschließend wieder anmelden. Wählen Sie den gewünschten Recovery-Punkt aus und klicken Sie dann auf **MySQL/MariaDB-Datenbanken**. Klicken Sie nicht auf **Komplette Maschine** oder **Dateien/Ordner**.

Ein applikationskonformes Backup konfigurieren

Voraussetzungen

- Auf der ausgewählten Maschine muss mindestens eine MySQL- oder MariaDB-Instanz laufen.
- Auf der Maschine, auf der die MySQL- oder MariaDB-Instanz ausgeführt wird, muss der Protection Agent unter dem Benutzer 'root' gestartet werden.
- Ein applikationskonformes Backup ist nur dann verfügbar, wenn im Schutzplan die **komplette Maschine** als Backup-Quelle ausgewählt wird.
- Die Backup-Option **Sektor-für-Sektor** muss im Schutzplan deaktiviert sein. Anderenfalls können keine Applikationsdaten wiederhergestellt werden.

So können Sie ein applikationskonformes Backup konfigurieren

1. Wählen Sie in der Cyber Protect-Konsole eine oder mehrere Maschinen aus, auf denen die MySQL- oder MariaDB-Instanzen laufen.
   Sie können eine oder mehrere Instanzen auf jeder Maschine haben.
2. Erstellen Sie einen Schutzplan, in dem das Backup-Modul aktiviert ist.
3. Wählen Sie bei **Backup-Quelle** die Option **Komplette Maschine**.
4. Klicken Sie auf **Applikations-Backup** und aktivieren Sie den Schalter neben dem Element **MySQL/MariaDB Server**.
5. Bestimmen Sie, wie Sie die MySQL- oder MariaDB-Instanzen spezifizieren wollen:
   - **Für alle Workloads**
     Verwenden Sie diese Option, wenn Sie Instanzen mit identischen Konfigurationen auf mehreren Servern betreiben. Für alle Instanzen werden die gleichen Verbindungsparameter und Anmeldedaten verwendet.
   - **Für bestimmte Workloads**
     Verwenden Sie diese Option, um die Verbindungsparameter und Anmeldedaten für jede Instanz zu spezifizieren.
6. Klicken Sie auf **Instanz hinzufügen**, um die Verbindungsparameter und Anmeldedaten zu konfigurieren.

a. Wählen Sie den Verbindungstyp aus und spezifizieren Sie dann Folgendes:
   - [Für TCP-Socket] IP-Adresse und Port.
   - [Für Unix-Socket] Socket-Pfad.

b. Spezifizieren Sie die Anmeldedaten eines Benutzerkontos, welches über folgende Berechtigungen für die Instanz verfügt:
   - `FLUSH_TABLES` oder `RELOAD` für alle Datenbanken und Tabellen (`*.*`)
   - `SELECT` für die `information_schema.tables`

c. Klicken Sie auf **OK**.

7. Klicken Sie auf **Fertig**.

Daten aus einem applikationskonformen Backup wiederherstellen

Sie können aus einem applikationskonformen Backup MySQL- oder MariaDB-Instanzen, Datenbanken und Tabellen wiederherstellen. Sie können außerdem den kompletten Server wiederherstellen, auf dem die Instanzen ausgeführt werden, oder Dateien und Ordner von diesem Server.

In der nachfolgenden Tabelle sind alle Recovery-Optionen zusammengefasst.

Recovery-Quelle	Wiederherstellen als	Recovery zu
MySQL Server MariaDB Server	Komplette Maschine	Maschine*, auf der der Agent für Linux installiert ist
MySQL Server MariaDB Server	Dateien oder Ordner	Maschine*, auf der der Agent für Linux installiert ist
Instanz	Dateien	Maschine*, auf der der Agent für MySQL/MariaDB installiert ist
Datenbank	Die gleiche Datenbank Neue Datenbank	Maschine*, auf der der Agent für MySQL/MariaDB installiert ist • Ursprüngliche Instanz • Eine andere Instanz • Ursprüngliche Datenbank • Neue Datenbank
Tabelle	Die gleiche Tabelle Neue Tabelle	Maschine*, auf der der Agent für MySQL/MariaDB installiert ist • Ursprüngliche Instanz • Eine andere Instanz • Ursprüngliche Datenbank

Recovery-Quelle	Wiederherstellen als	Recovery zu
		• Ursprüngliche Tabelle • Neue Tabelle

* Eine virtuelle Maschine, in der ein Agent installiert ist, wird aus Backup-Sicht wie eine physische Maschine behandelt.

Den kompletten Server wiederherstellen

Informationen zur Wiederherstellung eines kompletten Servers, auf dem MySQL- oder MariaDB-Instanzen ausgeführt werden, finden Sie in Abschnitt '"Recovery einer Maschine" (S. 545)'.

Instanzen wiederherstellen

Sie können aus einem applikationskonformen Backup MySQL- oder MariaDB-Instanzen als Dateien wiederherstellen.

So können Sie eine Instanz wiederherstellen

1. Wählen Sie in der Cyber Protect-Konsole diejenige Maschine aus, auf der sich die wiederherzustellenden Daten ursprünglich befunden haben.
2. Klicken Sie auf **Recovery**.
3. Wählen Sie einen Recovery-Punkt. Beachten Sie dabei, dass Recovery-Punkte nach Speicherorten gefiltert werden.
   Falls die Maschine offline ist, werden keine Recovery-Punkte angezeigt. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Sollte sich das Backup im Cloud Storage oder einem gemeinsam genutzten Storage befinden (d.h., dass andere Agenten auf diesen zugreifen können), dann klicken Sie zuerst auf den Befehl **Maschine auswählen**. Wählen Sie anschließend eine Maschine aus, die online ist und auf welcher der Agent für MySQL/MariaDB installiert ist, und dann den gewünschten Recovery-Punkt.
   - Wählen Sie einen Recovery-Punkt auf der Registerkarte **Backup Storage** aus.

   Die in einer der oberen Aktionen zum Durchsuchen ausgewählte Maschine wird als Zielmaschine für die Wiederherstellung verwendet.
4. Klicken Sie auf **Recovery** –> **MySQL/MariaDB-Datenbank**.
5. Wählen Sie die wiederherzustellende Instanz aus und klicken Sie dann auf **Als Dateien wiederherstellen**.
6. Wählen Sie bei **Pfad** das Verzeichnis, in dem die Dateien wiederhergestellt werden sollen.
7. Klicken Sie auf **Recovery starten**.

Datenbanken wiederherstellen

Sie können aus einem applikationskonformen Backup Datenbanken zu MySQL- oder MariaDB-Live-Instanzen wiederherstellen.

1. Wählen Sie in der Cyber Protect-Konsole diejenige Maschine aus, auf der sich die wiederherzustellenden Daten ursprünglich befunden haben.
2. Klicken Sie auf **Recovery**.
3. Wählen Sie einen Recovery-Punkt. Beachten Sie dabei, dass Recovery-Punkte nach Speicherorten gefiltert werden.

   Falls die Maschine offline ist, werden keine Recovery-Punkte angezeigt. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:

   - Sollte sich das Backup im Cloud Storage oder einem gemeinsam genutzten Storage befinden (d.h., dass andere Agenten auf diesen zugreifen können), dann klicken Sie zuerst auf den Befehl **Maschine auswählen**. Wählen Sie anschließend eine Maschine aus, die online ist und auf welcher der Agent für MySQL/MariaDB installiert ist, und dann den gewünschten Recovery-Punkt.
   - Wählen Sie einen Recovery-Punkt auf der Registerkarte **Backup Storage** aus.

   Die in einer der oberen Aktionen zum Durchsuchen ausgewählte Maschine wird als Zielmaschine für die Wiederherstellung verwendet.
4. Klicken Sie auf **Recovery** –> **MySQL/MariaDB-Datenbank**.
5. Klicken Sie auf den Namen der gewünschten Instanz, um sich deren Datenbanken anzeigen zu lassen.
6. Wählen Sie eine oder mehrere Datenbanken, welche Sie wiederherstellen wollen.
7. Klicken Sie auf **Recovery**.
8. Klicken Sie auf **MySQL- / MariaDB-Zielinstanz**, um die Verbindungsparameter und Anmeldedaten für die Zielinstanz zu spezifizieren.
   - Überprüfen Sie die Instanz, auf der Sie die Daten wiederherstellen wollen. Standardmäßig ist die ursprüngliche Instanz ausgewählt.
   - Spezifizieren Sie die Anmeldedaten eines Benutzerkontos, das auf die Zielinstanz zugreifen kann. Diesem Benutzerkonto müssen folgende Berechtigungen für alle Datenbanken und Tabellen zugewiesen sein (`*.*`):
     - `INSERT`
     - `CREATE`
     - `DROP`
     - `LOCK_TABLES`
     - `ALTER`
     - `SELECT`
   - Klicken Sie auf **OK**.

9. Überprüfen Sie die Zieldatenbank.

   Standardmäßig ist die ursprüngliche Datenbank vorausgewählt.

   Wenn Sie eine Datenbank als neue Datenbank wiederherstellen wollen, klicken Sie auf den Namen der Zieldatenbank und ändern Sie diesen. Diese Aktion ist nur verfügbar, wenn Sie eine einzelne Datenbank wiederherstellen.
10. Wählen Sie bei **Vorhandene Datenbanken überschreiben** den Überschreibmodus.

    Überschreiben ist standardmäßig aktiviert, sodass die gesicherte Datenbank die Zieldatenbank mit demselben Namen ersetzen wird.

    Wenn das Überschreiben deaktiviert ist, wird die gesicherte Datenbank während der Wiederherstellungsaktion übersprungen und die Zieldatenbank, die denselben Namen hat, nicht ersetzt.
11. Klicken Sie auf **Recovery starten**.

Tabellen wiederherstellen

Sie können aus einem applikationskonformen Backup Tabellen zu MySQL- oder MariaDB-Live-Instanzen wiederherstellen.

1. Wählen Sie in der Cyber Protect-Konsole diejenige Maschine aus, auf der sich die wiederherzustellenden Daten ursprünglich befunden haben.
2. Klicken Sie auf **Recovery**.
3. Wählen Sie einen Recovery-Punkt. Beachten Sie dabei, dass Recovery-Punkte nach Speicherorten gefiltert werden.

   Falls die Maschine offline ist, werden keine Recovery-Punkte angezeigt. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:

   - Sollte sich das Backup im Cloud Storage oder einem gemeinsam genutzten Storage befinden (d.h., dass andere Agenten auf diesen zugreifen können), dann klicken Sie zuerst auf den Befehl **Maschine auswählen**. Wählen Sie anschließend eine Maschine aus, die online ist und auf welcher der Agent für MySQL/MariaDB installiert ist, und dann den gewünschten Recovery-Punkt.
   - Wählen Sie einen Recovery-Punkt auf der Registerkarte **Backup Storage** aus.

   Die in einer der oberen Aktionen zum Durchsuchen ausgewählte Maschine wird als Zielmaschine für die Wiederherstellung verwendet.
4. Klicken Sie auf **Recovery** –> **MySQL/MariaDB-Datenbank**.
5. Klicken Sie auf den Namen der gewünschten Instanz, um sich deren Datenbanken anzeigen zu lassen.
6. Klicken Sie auf den Namen der gewünschten Datenbank, um sich deren Tabellen anzeigen zu lassen.
7. Wählen Sie eine oder mehrere Tabellen, welche Sie wiederherstellen wollen.
8. Klicken Sie auf **Recovery**.

9. Klicken Sie auf **MySQL- / MariaDB-Zielinstanz**, um die Verbindungsparameter und Anmeldedaten für die Zielinstanz zu spezifizieren.
   - Überprüfen Sie die Instanz, auf der Sie die Daten wiederherstellen wollen. Standardmäßig ist die ursprüngliche Instanz ausgewählt.
   - Spezifizieren Sie die Anmeldedaten eines Benutzerkontos, das auf die Zielinstanz zugreifen kann. Diesem Benutzerkonto müssen folgende Berechtigungen für alle Datenbanken und Tabellen zugewiesen sein (`*.*`):
     - `INSERT`
     - `CREATE`
     - `DROP`
     - `LOCK_TABLES`
     - `ALTER`
     - `SELECT`
   - Klicken Sie auf **OK**.
10. Überprüfen Sie die Zieltabelle.
    Die ursprüngliche Tabelle ist standardmäßig ausgewählt.
    Wenn Sie eine Tabelle als neue Datenbank wiederherstellen wollen, klicken Sie auf den Namen der Zieltabelle und ändern Sie diesen. Diese Aktion ist nur verfügbar, wenn Sie eine einzelne Tabelle wiederherstellen.
11. Wählen Sie bei **Vorhandene Tabellen überschreiben** den Überschreibmodus.
    Überschreiben ist standardmäßig aktiviert, sodass die gesicherte Tabelle die Zieltabelle mit demselben Namen ersetzen wird.
    Wenn das Überschreiben deaktiviert ist, wird die gesicherte Tabelle während der Wiederherstellungsaktion übersprungen und die Zieltabelle, die denselben Namen hat, nicht ersetzt.
12. Klicken Sie auf **Recovery starten**.

Gespeicherte Routinen wiederherstellen

Wenn Sie eine komplette MySQL-Instanz wiederherstellen, werden die gespeicherten Routinen automatisch wiederhergestellt.

Wenn Sie eine einzelne Datenbank in einer nicht ursprünglichen Instanz wiederherstellen oder sie als neue Datenbank wiederherstellen wollen, werden die gespeicherten Routinen nicht automatisch wiederhergestellt. Sie können diese manuell wiederherstellen, indem Sie sie in eine SQL-Datei exportieren und dann der wiederhergestellten Datenbank hinzufügen.

So können Sie die gespeicherten Routinen exportieren und diese zu einer wiederhergestellten Datenbank hinzufügen

1. Öffnen Sie auf der Maschine mit der ursprünglichen MySQL-Instanz das Terminal.
2. Führen Sie folgenden Befehl aus, um die gespeicherten Routinen zu exportieren.

3.
```
mysqldump -p [source_database_name] --routines --no-create-info --no-data >
[exported_db_routines.sql]
```
4. Öffnen Sie auf der Maschine, auf der die Datenbank wiederhergestellt wird, den MySQL-Befehlszeilen-Client.
5. Führen Sie folgende Befehle aus, um die Routinen der wiederhergestellten Datenbank hinzuzufügen.

```
mysql>  use [recovered_database_name];
```

```
mysql>  source [path_to_exported_db_routines.sql];
```

Websites und Webhosting-Server sichern

Websites sichern

Eine Website kann als Folge eines unberechtigten Zugriffs oder eines Malware-Angriffs beschädigt werden. Erstellen Sie ein Backup Ihrer Website, wenn Sie diese (nach bzw. aufgrund einer Beschädigung) leicht auf einen fehlerfreien Zustand zurücksetzen wollen.

Was benötige ich, um eine Website sichern zu können?

Sie müssen auf die Website über das SFTP- oder SSH-Protokoll zugreifen können. Es ist nicht notwendig, einen Agenten zu installieren. Sie müssen Ihre Website einfach nur so hinzufügen, wie es später in diesem Abschnitt beschrieben ist.

Welche Elemente können per Backup gesichert werden?

Sie können folgende Elemente sichern:

- **Dateien mit Website-Inhalten**
  Alle Dateien, die über das Konto verfügbar sind, welches Sie für die SFTP- oder SSH-Verbindung spezifiziert haben.
- **Verknüpfte Datenbanken (sofern vorhanden), auf MySQL-Servern gehostet.**
  Alle Datenbanken, die über das von Ihnen spezifizierten MySQL-Konto verfügbar sind.

Wenn Ihre Website Datenbanken verwendet, sollten Sie die Dateien und Datenbanken gemeinsam per Backup sichern, damit Sie diese in einem konsistenten Zustand wiederherstellen können.

Einschränkungen

- Der einzig verfügbare Speicherort für ein Website-Backup ist der Cloud Storage.
- Es ist möglich, mehrere Schutzpläne auf eine Website anzuwenden, aber nur einer davon kann per Planung ausgeführt werden. Die anderen Pläne müssen manuell gestartet werden.

- Die einzig verfügbare Backup-Option 'Backup-Dateiname'.
- Die Website-Schutzpläne werden nicht auf der Registerkarte **Verwaltung** –> **Schutzpläne** angezeigt.

Eine Website per Backup sichern

So können Sie eine Website hinzufügen

1. Klicken Sie auf **Geräte** –> **Hinzufügen**.
2. Klicken Sie auf **Website**.
3. Konfigurieren Sie die folgenden Zugriffseinstellungen für die Website:
   - Geben Sie bei **Website-Name** eine (von Ihnen erstellte) Bezeichnung für Ihre Website ein. Dieser Name wird in der Cyber Protect-Konsole angezeigt.
   - Spezifizieren Sie bei **Host** den Namen und die IP-Adresse des Hosts, die für den Zugriff auf die Website per SFTP oder SSH verwendet werden sollen. Beispielsweise `mein.server.com` oder `10.250.100.100`
   - Spezifizieren Sie bei **Port** die Port-Nummer.
   - Spezifizieren Sie bei **Benutzername** und **Kennwort** die Anmeldedaten des Kontos, welches für den Zugriff auf die Website per SFTP oder SSH verwendet werden soll.

     Wichtig
     Es werden nur die Dateien per Backup gesichert, die über das spezifizierte Konto verfügbar sind.

     Statt eines Kennworts können Sie auch Ihren privaten SSH-Schlüssel spezifizieren. Aktivieren Sie dafür das Kontrollkästchen **Privaten SSH-Schlüssel statt Kennwort verwenden** und spezifizieren Sie dann den entsprechenden Schlüssel.
4. Klicken Sie auf **Weiter**.
5. Wenn Ihre Website MySQL-Datenbanken verwendet, konfigurieren Sie die Zugriffseinstellungen für diese Datenbanken. Anderenfalls können Sie auf **Überspringen** klicken.
   a. Wählen Sie bei **Verbindungstyp**, wie auf die Datenbanken aus der Cloud zugegriffen werden soll:
      - **Per SSH vom Host** – Es wird über den Host auf die Datenbanken zugegriffen, der in Schritt 3 spezifiziert wurde.
      - **Direkte Verbindung** – Es wird direkt auf die Datenbanken zugegriffen. Wählen Sie diese Einstellung nur, wenn die Datenbanken auch über das Internet verfügbar sind.

   b. Spezifizieren Sie bei **Host** den Namen oder die IP-Adresse des Hosts, auf dem der entsprechende MySQL-Server ausgeführt wird.
   c. Spezifizieren Sie bei **Port** die Port-Nummer für die TCP/IP-Verbindung zum Server. Die Standardportnummer ist 3306.
   d. Spezifizieren Sie bei **Benutzername** und **Kennwort** die Anmeldedaten für das MySQL-Konto.

Wichtig
Es werden nur die Datenbanken per Backup gesichert, die über das spezifizierte Konto verfügbar sind.

e. Klicken Sie auf **Erstellen**.

Die Website erscheint in der Cyber Protect-Konsole unter **Geräte** –> **Websites**.

So können Sie die Verbindungseinstellungen ändern

1. Wählen Sie die Website unter **Geräte** –> **Websites** aus.
2. Klicken Sie auf **Details**.
3. Klicken Sie auf das Stiftsymbol neben der Website oder neben den Datenbank-Verbindungseinstellungen.
4. Nehmen Sie alle notwendigen Änderungen vor und klicken Sie dann auf **Speichern**.

So können Sie einen Schutzplan für Websites erstellen

1. Wählen Sie eine oder mehrere Websites unter **Geräte** –> **Websites** aus.
2. Klicken Sie auf den Befehl **Schützen**.
3. [Optional] Aktivieren Sie das Backup von Datenbanken.
   Wenn mehrere Websites ausgewählt wurden, ist das Backup von Datenbanken standardmäßig deaktiviert.
4. [Optional] Ändern Sie die Aufbewahrungsregeln.
5. [Optional] Aktivieren Sie die Verschlüsselung von Backups.
6. [Optional] Klicken Sie auf das Zahnradsymbol, wenn Sie die **Backup-Dateiname** bearbeiten wollen. Dies ist in zwei Fällen sinnvoll:
   - Wenn Sie diese Website früher schon einmal gesichert haben und die vorhandene Sequenz der Backups fortsetzen wollen.
   - Wenn Sie den benutzerdefinierten Namen in der Registerkarte **Backup Storage** einsehen wollen.
7. Klicken Sie auf **Anwenden**.

Sie können Schutzpläne für Websites auf die gleiche Weise wie für Maschinen bearbeiten, widerrufen und löschen. Diese Aktionen sind im Abschnitt 'Aktionen mit Schutzplänen' beschrieben.

Eine Website wiederherstellen

So können Sie eine Website wiederherstellen

1. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Wählen Sie bei **Geräte** –> **Websites** diejenige Website aus, die Sie wiederherstellen wollen, und klicken Sie dann auf **Recovery**.

Sie können die gewünschte Website auch per Namen suchen. Platzhalterzeichen (Wildcards) werden nicht unterstützt.

- Wenn die Website zuvor gelöscht wurde, können Sie diese im Bereich **Cloud-Applikationen-Backups** der Registerkarte 'Backup Storage' auswählen und dann auf **Backups anzeigen** klicken.

  Wenn Sie eine gelöschte Website wiederherstellen wollen, müssen Sie die Ziel-Website als Gerät hinzufügen.

2. Wählen Sie den gewünschten Recovery-Punkt aus.
3. Klicken Sie auf **Recovery** und bestimmen Sie, welche Elemente Sie wiederherstellen wollen: **Komplette Website**, **Datenbanken** (sofern vorhanden) oder **Dateien/Ordner**.

   Um sicherzustellen, dass Ihre Website anschließend in einem konsistenten Zustand ist, sollten Sie sowohl die Dateien als auch Datenbanken wiederherstellen (in beliebiger Reihenfolgen).
4. Befolgen Sie in Abhängigkeit von Ihrer Wahl eine der nachfolgend beschriebenen Prozeduren.

So können Sie die komplette Website widerherstellen

1. Bei **Zur Website wiederherstellen** können Sie die Ziel-Website einsehen oder ändern.

   Standardmäßig ist die ursprüngliche Website vorausgewählt. Sollte diese nicht existieren, müssen Sie die Ziel-Website auswählen.
2. Bestimmen Sie, ob Sie auch die Freigabe-Berechtigungen der wiederhergestellten Elemente mit wiederherstellen wollen.
3. Klicken Sie auf **Recovery starten** und bestätigen Sie dann die Aktion.

So können Sie die Datenbanken wiederherstellen

1. Wählen Sie Datenbanken, die Sie wiederherstellen wollen.
2. Wenn Sie eine Datenbank als Datei herunterladen wollen, müssen Sie auf **Download** klicken, dann den Zielspeicherort für die Datei bestimmen und schließlich auf **Speichern** klicken. Ansonsten können Sie diesen Schritt überspringen.
3. Klicken Sie auf **Recovery**.
4. Bei **Zur Website wiederherstellen** können Sie die Ziel-Website einsehen oder ändern.

   Standardmäßig ist die ursprüngliche Website vorausgewählt. Sollte diese nicht existieren, müssen Sie die Ziel-Website auswählen.
5. Klicken Sie auf **Recovery starten** und bestätigen Sie dann die Aktion.

So können Sie die Website-Dateien/-Ordner wiederherstellen

1. Wählen Sie die Dateien/Ordner, die Sie wiederherstellen wollen.
2. Wenn Sie eine Datei speichern wollen, müssen Sie auf **Download** klicken, dann den Speicherort für die Datei bestimmen und schließlich auf **Speichern** klicken. Ansonsten können Sie diesen Schritt überspringen.
3. Klicken Sie auf **Recovery**.
4. Bei **Zur Website wiederherstellen** können Sie die Ziel-Website einsehen oder ändern.

Standardmäßig ist die ursprüngliche Website vorausgewählt. Sollte diese nicht existieren, müssen Sie die Ziel-Website auswählen.

5. Bestimmen Sie, ob Sie auch die Freigabe-Berechtigungen der wiederhergestellten Elemente mit wiederherstellen wollen.
6. Klicken Sie auf **Recovery starten** und bestätigen Sie dann die Aktion.

Webhosting-Server sichern

Sie können Linux-basierte Webhosting-Server schützen, auf denen Plesk, cPanel-, DirectAdmin-, VirtualMin- oder ISPManager-Control-Panels laufen. Server, auf denen Webhosting-Control-Panels anderer Anbieter laufen, werden wie reguläre Workloads geschützt.

Quotas

Server, auf denen Plesk-, cPanel-, DirectAdmin-, VirtualMin- oder ISPManager-Control-Panels laufen, gelten als Webhosting-Server. Jeder per Backup gesicherte Webhosting-Server wird auf die Quota **Webhosting-Server** angerechnet. Wenn dieses Quota deaktiviert ist oder die Überschreitungsgrenze für diese Quota erreicht ist, wird ein Quota wie nachfolgend beschrieben zugewiesen oder die Backups werden fehlschlagen:

- Bei einem physischen Server wird die Quota **Server** verwendet. Wenn diese Quota deaktiviert ist oder die Überschreitungsgrenze für diese Quota erreicht ist, wird das Backup fehlschlagen.
- Bei einem virtuellen Server wird die Quota **Virtuelle Maschinen** verwendet. Wenn diese Quota deaktiviert ist oder die Überschreitungsgrenze für diese Quota erreicht ist, wird das Backup fehlschlagen.

Integrationen für DirectAdmin, cPanel und Plesk

Webhosting-Administratoren, die DirectAdmin, Plesk oder cPanel verwenden, können diese Control Panels in den Cyber Protection Service integrieren, um mehrere leistungsstarke Fähigkeiten zu erhalten. Wie etwa:

- Komplette Webhosting-Server per Backup auf Laufwerksebene in den Cloud Storage sichern
- Den kompletten Server (einschließlich aller Websites und Konten) wiederherstellen
- Websites granular wiederherstellen und Konten, Websites, einzelne Dateien, Postfächer oder Datenbanken herunterladen
- Resellern und Kunden ermöglichen, ihre eigenen Daten eigenständig (per Self-Service) wiederherstellen zu können

Um die Integration durchführen zu können, müssen Sie eine Erweiterung für den Cyber Protection Service verwenden. Detaillierte Informationen dazu finden Sie in den entsprechenden Integrationsanleitungen:

- Integrationsanleitung für DirectAdmin
- Integrationsanleitung für WHM & cPanel

Spezielle Aktionen mit virtuellen Maschinen

Eine virtuelle Maschine aus einem Backup heraus ausführen (Instant Restore)

Sie können eine virtuelle Maschine aus einem Laufwerk-Backup heraus ausführen, welches ein Betriebssystem enthält. Mit dieser Aktion, die auch 'sofortige Wiederherstellung' oder 'Instant Restore' genannt wird, können Sie einen virtuellen Server innerhalb von Sekunden hochfahren. Die virtuellen Laufwerke werden direkt aus dem Backup heraus emuliert und belegen daher keinen Speicherplatz im Datenspeicher (Storage). Zusätzlicher Speicherplatz wird lediglich benötigt, um Änderungen, die an den virtuellen Laufwerken durchgeführt werden, zu speichern.

Wir empfehlen, dass Sie diese temporäre virtuelle Maschine bis zu drei Tage lang in Betrieb lassen. Danach können Sie sie vollständig entfernen oder in eine reguläre virtuelle Maschine konvertieren (durch 'Finalisieren'), ohne dass es dabei zu einer Ausfallzeit kommt.

Solange die temporäre virtuelle Maschine vorhanden ist bzw. verwendet wird, können keine Aufbewahrungsregeln auf das Backup angewendet werden, welches die Maschine als Grundlage verwendet. Backups der ursprünglichen Maschine können weiterhin ungestört ausgeführt werden.

Anwendungsbeispiele

- **Disaster Recovery**
  Bringen Sie die Kopie einer ausgefallenen Maschine in kürzester Zeit online.
- **Ein Backup testen**
  Führen Sie eine Maschine von einem Backup aus und überprüfen Sie, ob das Gastbetriebssystem und Applikationen korrekt funktionieren.
- **Auf Applikationsdaten zugreifen**
  Verwenden Sie, während eine Maschine ausgeführt wird, die integrierten Verwaltungswerkzeuge der Applikation und extrahieren Sie erforderliche Daten.

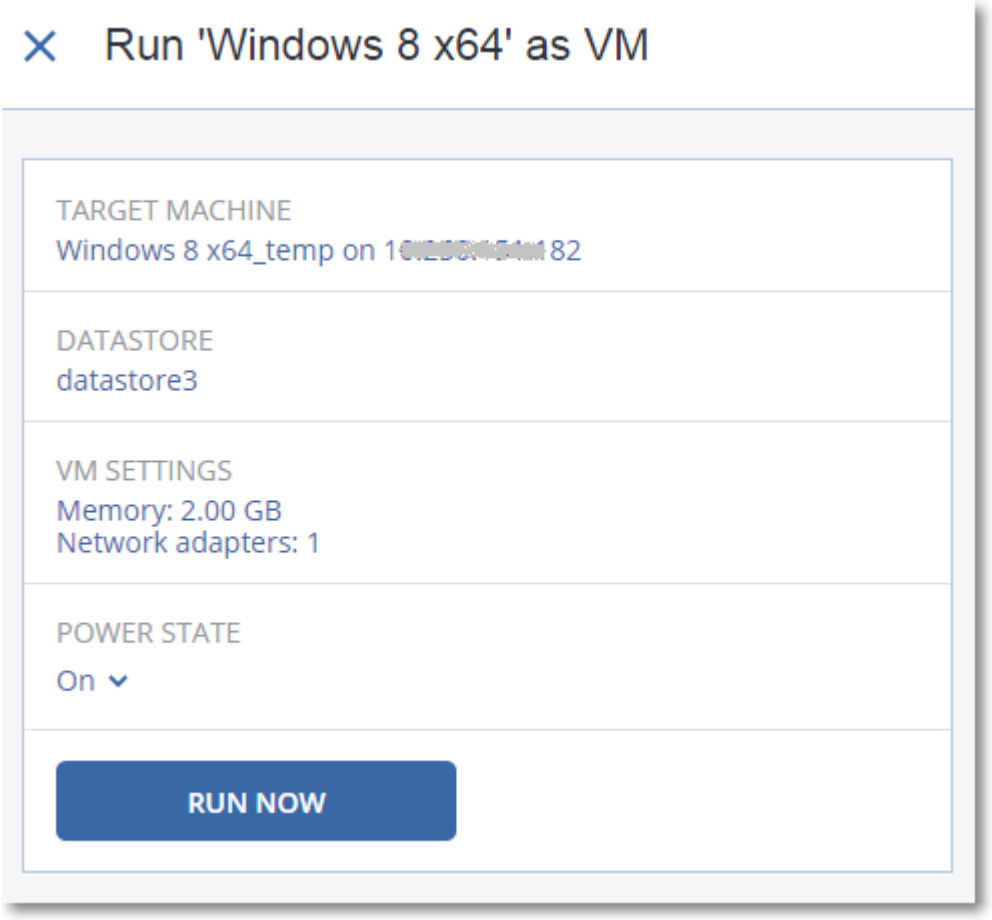
Voraussetzungen

- Mindestens ein Agent für VMware oder Agent für Hyper-V muss für den Cyber Protection Service registriert sein.
- Das Backup kann in einem Netzwerkordner oder einem lokalen Ordner auf derjenigen Maschine gespeichert werden, auf welcher der Agent für VMware oder Agent für Hyper-V installiert ist. Wenn Sie einen Netzwerkordner verwenden, muss dieser von der entsprechenden Maschine aus verfügbar sein. Eine virtuelle Maschine kann auch direkt von einem Backup heraus ausgeführt werden, welches im Cloud Storage gespeichert ist. Dies ist jedoch langsamer, weil für diese Aktion intensive wahlfreie Lesezugriffe auf das Backup notwendig sind.

- Das Backup muss eine komplette Maschine enthalten oder doch zumindest alle Volumes, die zur Ausführung des Betriebssystems notwendig sind.
- Es können sowohl die Backups von physischen wie auch virtuellen Maschinen verwendet werden. Die Backups von Virtuozzo-*Containern* können nicht verwendet werden.
- Backups, die logische Linux-Volumes (LVMs) enthalten, müssen mit dem Agenten für VMware oder Agenten für Hyper-V erstellt werden. Die virtuelle Maschine muss denselben Typ wie die Originalmaschine (ESXi oder Hyper-V) haben.

Eine Maschine ausführen

1. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Wählen Sie eine zu sichernde Maschine, klicken Sie auf **Recovery** und wählen Sie dann einen Recovery-Punkt.
   - Wählen Sie einen Recovery-Punkt auf der Registerkarte 'Backup Storage'.
2. Klicken Sie auf **Als VM ausführen**.
   Die Software wählt den Host und die anderen benötigten Parameter automatisch aus.



3. [Optional] Klicken Sie auf **Zielmaschine** und ändern Sie den Typ der virtuellen Maschine (ESXi oder Hyper-V), den Host oder den Namen der virtuellen Maschine.
4. [Optional] Klicken Sie auf **Datenspeicher** für ESXi oder **Pfad** für Hyper-V – und bestimmten Sie dann den Datenspeicher für die neue virtuelle Maschine.

Während die Maschine ausgeführt wird, werden die (möglichen) Änderungen gesammelt, die an den virtuellen Laufwerken erfolgen. Stellen Sie sicher, dass der ausgewählte Datenspeicher genügend freien Speicherplatz hat. Wenn Sie diese Änderungen dadurch bewahren wollen, dass Sie die virtuelle Maschine zu einer 'dauerhaften' Maschine machen, müssen Sie einen Datenspeicher wählen, der für den Produktionsbetrieb der Maschine geeignet ist.

5. [Optional] Klicken Sie auf **VM-Einstellungen**, um die Größe des Arbeitsspeichers und die Netzwerkverbindungen der virtuellen Maschine zu ändern.
6. [Optional] Bestimmen Sie den Betriebszustand der VM (**An**/**Aus**).
7. Klicken Sie auf **Jetzt ausführen**.

Als Ergebnis dieser Aktion wird die Maschine in der Weboberfläche mit einem dieser Symbole angezeigt:  oder 

. Von solchen virtuellen Maschinen kann kein Backup erstellt werden.

Hinweis
Sie können die Aktion 'Als virtuelle Maschine ausführen' (Instant Restore) mit Backups in Microsoft Azure durchführen. Diese Aktion führt jedoch zu einem erheblichen ausgehenden Datenverkehr, der auf die Abrechnung Ihres Microsoft Azure-Abonnements aufgeschlagen wird. Der typische ausgehende Datenverkehr für eine Windows-Maschine, die aus einem Microsoft Azure-Backup ausgeführt wird, beträgt etwa 5 GB (vom Einschalten der virtuellen Maschine bis zur Anmeldung).

Eine Maschine löschen

Wir raten davon ab, eine temporäre virtuelle Maschine direkt in vSphere/Hyper-V zu löschen. Denn dies kann zu Fehlern in der Weboberfläche führen. Außerdem kann das Backup, von dem die Maschine ausgeführt wurde, für eine gewisse Zeit gesperrt bleiben (es kann nicht von Aufbewahrungsregeln gelöscht werden).

So löschen Sie eine virtuelle Maschine, die aus einem Backup heraus ausgeführt wird.

1. Wählen Sie auf der Registerkarte **Alle Geräte** eine Maschine aus, die aus einem Backup heraus ausgeführt wird.
2. Klicken Sie auf **Löschen**.

Die Maschine wird von der Weboberfläche entfernt. Sie wird außerdem auch aus der vSphere- oder Hyper-V-Bestandsliste (Inventory) und dem Datenspeicher (Storage) entfernt. Alle Änderungen an den Daten der Maschine, die während ihrer Ausführungen erfolgten, gehen verloren.

Eine Maschine finalisieren

Wenn eine virtuelle Maschine aus einem Backup heraus ausgeführt wird, werden auch die Inhalte der virtuellen Laufwerke direkt aus dem Backup entnommen. Sollte daher während der Ausführung die Verbindung zum Backup-Speicherort oder dem Protection Agenten verloren gehen, geht auch der Zugriff auf die Maschine verloren und kann die Maschine beschädigt werden.

Sie können diese Maschine in eine 'dauerhafte' Maschine umwandeln. Das bedeutet, dass alle virtuellen Laufwerke der Maschine zusammen mit allen Änderungen, die während ihrer Ausführung aufgetreten sind, zu dem Datenspeicher wiederhergestellt werden, in dem diese Änderungen gespeichert werden. Dieser Prozess wird 'Finalisieren' genannt.

Das Finalisieren erfolgt, ohne dass es zu einem Ausfall der Maschine kommt. Die virtuelle Maschine wird also während des Finalisierens *nicht* ausgeschaltet.

Der Speicherort der finalen virtuellen Laufwerke ist in den Parameter der Aktion **Als VM ausführen** definiert (**Datenspeicher** für ESXi oder **Pfad** für Hyper-V). Stellen Sie vor Beginn der Finalisierung sicher, dass der freie Speicherplatz, die Freigabefunktionen und die Performance dieses Datenspeichers geeignet sind, um die Maschine unter Produktionsbedingungen auszuführen.

Hinweis
Für die Hyper-V-Version, die in Windows Server 2008/2008 R2 läuft, und den Microsoft Hyper-V Server 2008/2008 R2 wird keine Finalisierung nicht unterstützt, da in diesen Hyper-V-Versionen die erforderliche API fehlt.

So können Sie eine virtuelle Maschine finalisieren, die aus einem Backup ausgeführt wird

1. Wählen Sie auf der Registerkarte **Alle Geräte** eine Maschine aus, die aus einem Backup heraus ausgeführt wird.
2. Klicken Sie auf **Finalisieren**.
3. [Optional] Spezifizieren Sie einen neuen Namen für die Maschine.
4. [Optional] Den Laufwerk-Provisioning-Modus ändern. Standardeinstellung ist **Thin**.
5. Klicken Sie auf **Finalisieren**.

Der Name der Maschine wird sofort geändert. Der Recovery-Fortschritt wird auf der Registerkarte **Aktivitäten** angezeigt. Sobald die Wiederherstellung fertiggstellt wurde, wird das Symbol der Maschine zu dem für eine reguläre virtuelle Maschine geändert.

Das sollten Sie über die Finalisierung wissen

Finalisierung vs. normale Wiederherstellung

Der Finalisierungsprozess ist aus folgenden Gründen langsamer als eine normale Wiederherstellung:

- Während einer Finalisierung greift der Agent per Zufallszugriff auf unterschiedliche Teile des Backups zu. Wenn eine komplette Maschine wiederhergestellt wird, liest der Agent die Daten nacheinander aus dem Backup aus.
- Wenn die virtuelle Maschine während der Finalisierung ausgeführt wird, liest der Agent die Daten aus dem Backup häufiger aus, um beide Prozesse gleichzeitig aufrechtzuerhalten. Während einer normalen Wiederherstellung wird die virtuelle Maschine gestoppt.

Die Finalisierung von Maschinen, die aus Cloud Backups ausgeführt werden

Die Finalisierungsgeschwindigkeit hängt – aufgrund des intensiven Zugriffs auf die Backup-Daten – stark von der Verbindungsbandbreite zwischen dem Backup-Speicherort und dem Agenten ab. Die Finalisierung von Backups, die in der Cloud liegen, ist langsamer als von lokalen Backups. Wenn die Internetverbindung sehr langsam oder sogar instabil ist, kann die Finalisierung einer Maschine, die aus einem Cloud-Backup ausgeführt wird, fehlschlagen. Falls Sie die Wahl haben, empfehlen wir Ihnen daher, virtuelle Maschinen möglichst aus lokalen Backups auszuführen, wenn Sie eine Finalisierung planen.

Hinweis
Die Geschwindigkeit der Finalisierung hängt davon ab, ob der Agent mit einem VMware ESXi-Host oder vCenter verbunden ist (wie in Schritt 3 des Abschnitts '"Die virtuelle Appliance konfigurieren" (S. 148)' beschrieben). Eine Verbindung zu einem VMware vCenter kann die Finalisierungsaktion aufgrund der Besonderheiten der VMware-APIs verlangsamen. Wenn Sie die Finalisierungsaktion beschleunigen wollen, sollten Sie einen separaten Agenten für VMware zur Durchführung der Aktion **Als VM ausführen** mit anschließender Finalisierung verwenden, wobei dieser Agent statt mit einem vCenter mit einem ESXi-Host verbunden wird.

Mit VMware vSphere arbeiten

Dieser Abschnitt beschreibt Aktionen, die spezifisch für VMware vSphere-Umgebungen sind.

Replikation von virtuellen Maschinen

Die Möglichkeit zur Replikation ist nur für virtuelle VMware ESXi-Maschinen verfügbar.

Unter Replikation wird (hier) ein Prozess verstanden, bei dem von einer virtuellen Maschine zuerst eine exakte Kopie (Replikat) erstellt wird – und dieses Replikat dann mit der ursprünglichen Maschine fortlaufend synchronisiert wird. Wenn Sie eine wichtige virtuelle Maschine replizieren, haben Sie immer eine Kopie dieser Maschine in einem startbereiten Zustand verfügbar.

Eine Replikation kann entweder manuell oder auf Basis einer (von Ihnen spezifizierten) Planung gestartet werden. Die erste Replikation ist vollständig, was bedeutet, dass die komplette Maschine kopiert wird. Alle nachfolgenden Replikationen erfolgen dann inkrementell und werden mithilfe von 'CBT (Changed Block Tracking)' durchgeführt (außer diese Option wird extra deaktiviert).

Replikation vs. Backup

Anders als bei geplanten Backups wird bei einem Replikat immer nur der letzte (jüngste) Zustand der virtuellen Maschine aufbewahrt. Ein Replikat belegt Platz im Datenspeicher, während für Backups ein kostengünstigerer Storage verwendet werden kann.

Das Aktivieren eines Replikats geht jedoch deutlich schneller als eine klassische Wiederherstellung aus einem Backup – und ist auch schneller als die Ausführung einer virtuellen Maschine aus einem

Backup. Ein eingeschaltetes Replikat arbeitet schneller als eine VM, die aus einem Backup ausgeführt wird, und es muss kein Agent für VMware geladen werden.

Anwendungsbeispiele

- **Sie replizieren virtuelle Maschinen zu einem Remote-Standort.**
  Die Replikation ermöglicht Ihnen, teilweise oder vollständige Datacenter-Ausfälle zu überstehen, indem Sie die virtuellen Maschinen von einem primären zu einem sekundären Standort klonen. Als sekundärer Standort wird üblicherweise eine entfernt gelegene Einrichtung verwendet, die normalerweise nicht von denselben Störereignissen (Katastrophen in der Umgebung, Infrastrukturprobleme etc.) wie der primäre Standort betroffen wird/werden kann.
- **Sie replizieren virtuelle Maschinen innerhalb eines Standortes (von einem Host/Datenspeicher zu einem anderen).**
  Eine solche Onsite-Replikation kann zur Gewährleistung einer hohen Verfügbarkeit und für Disaster Recovery-Szenarien verwendet werden.

Das können Sie mit einem Replikat tun

- **Ein Replikat testen**
  Das Replikat wird für den Test eingeschaltet. Verwenden Sie den vSphere Client oder andere Tools, um die korrekte Funktion des Replikats zu überprüfen. Die Replikation wird angehalten, solange der Test läuft.
- **Failover auf ein Replikat**
  Bei einem Failover wird der Workload der ursprünglichen virtuellen Maschine auf ihr Replikat verschoben. Die Replikation wird angehalten, solange die Failover-Aktion läuft.
- **Das Replikat sichern**
  Backup und Replikation erfordern beide einen Zugriff auf virtuelle Laufwerke, wodurch wiederum der Host, auf dem die virtuelle Maschine läuft, in seiner Performance beeinflusst wird. Wenn Sie von einer virtuellen Maschine sowohl Backups als auch ein Replikat haben wollen, der Produktions-Host dadurch aber nicht zusätzlich belastet werden soll, dann replizieren Sie die Maschine zu einem anderen Host. Dieses Replikat können Sie anschließend per Backup sichern.

Einschränkungen

- Folgende Arten von virtuellen Maschinen können nicht repliziert werden:
  - Fehlertolerante Maschinen, die auf ESXi 5.5 (und niedriger) laufen.
  - Maschine, die aus Backups ausgeführt werden.
  - Die Replikate von virtuellen Maschinen.
- Einige Hardwareänderungen, wie z.B. das Hinzufügen einer Netzwerkkarte (NIC) zum ESXi-Host oder das Entfernen einer NIC aus dem Host, führen zu einer Änderung der internen IDs des Hosts. Diese Änderung wirkt sich auf die VM-Replikationspläne aus. Nach einer solchen Änderung müssen Sie die VM-Replikationspläne, in denen der ESXi-Host als Quelle oder Ziel ausgewählt ist, neu erstellen. Anderenfalls werden die VM-Replikationspläne fehlschlagen.

Einen Replikationsplan erstellen

Ein Replikationsplan muss für jede Maschine individuell erstellt werden. Es ist nicht möglich, einen vorhandenen Plan auf andere Maschinen anzuwenden.

So erstellen Sie einen Replikationsplan

1. Wählen Sie eine virtuelle Maschine aus, die repliziert werden soll.
2. Klicken Sie auf **Replikation**.
   Die Software zeigt eine Vorlage für den neuen Replikationsplan an.
3. [Optional] Wenn Sie den Namen des Replikationsplans ändern wollen, klicken Sie auf den vorgegebenen Standardnamen.
4. Klicken Sie auf **Zielmaschine** – und gehen Sie dann folgendermaßen vor:
   a. Bestimmen Sie, ob ein neues Replikat erstellt werden oder ein bereits vorhandenes Replikat der Maschine verwendet werden soll.
   b. Wählen Sie den ESXi-Host und spezifizieren Sie einen Namen für das neue Replikat – oder wählen Sie eine bereits vorhandenes Replikat aus.
      Der Standardname für ein neues Replikat ist **[Name der ursprünglichen Maschine]_ replica**.
   c. Klicken Sie auf **OK**.
5. [Nur bei Replikation zu einer neuen Maschine] Klicken Sie auf **Datenspeicher** und bestimmten Sie dann den Datenspeicher für die neue virtuelle Maschine.
6. [Optional] Klicken Sie auf **Planung**, wenn Sie die Planung für die Replikation ändern wollen.
   Die Replikation erfolgt standardmäßig einmal am Tag – und zwar von Montag bis Freitag. Sie können den genauen Zeitpunkt festlegen, an dem die Replikation ausgeführt werden soll.
   Wenn Sie die Replikationshäufigkeit ändern wollen, bewegen Sie einfach den entsprechenden grafischen Schieber – und spezifizieren Sie dann die gewünschte Planung.
   Sie außerdem noch Folgendes tun:
   - Sie können einen Datumsbereich für die Planung festlegen, zu dem die entsprechende Operation ausgeführt werden soll. Aktivieren Sie das Kontrollkästchen **Den Plan in einem Datumsbereich ausführen** und spezifizieren Sie anschließend den gewünschten Datumsbereich.
   - Sie können die Planung deaktivieren. In diesem Fall kann die Replikation manuell gestartet werden.
7. [Optional] Klicken Sie auf das Zahnradsymbol, wenn Sie die Replikationsoptionen anpassen wollen.
8. Klicken Sie auf **Anwenden**.
9. [Optional] Wenn Sie den Plan manuell ausführen wollen, klicken im Fensterbereich für die Planung auf **Jetzt ausführen**.

Wenn ein Replikationsplan ausgeführt wird, erscheint das virtuelle Maschinen-Replikat in der Liste '**Alle Geräte**' und wird mit diesem Symbol gekennzeichnet: 

Ein Replikat testen

So bereiten Sie ein Replikat für einen Test vor

1. Wählen Sie ein Replikat aus, das getestet werden soll.
2. Klicken Sie auf **Replikat testen**.
3. Klicken Sie auf **Test starten**.
4. Bestimmen Sie, ob das eingeschaltete Replikat mit dem Netzwerk verbunden werden soll. Die Standardvorgabe ist, dass das Replikat nicht mit dem Netzwerk verbunden wird.
5. [Optional] Falls Sie das Replikat mit dem Netzwerk verbinden wollen, müssen Sie das Kontrollkästchen **Ursprüngliche virtuelle Maschine stoppen** aktivieren, damit die ursprüngliche Maschine angehalten wird, bevor das Replikat eingeschaltet wird.
6. Klicken Sie auf **Start**.

So stoppen Sie den Test eines Replikats

1. Wählen Sie das Replikat aus, welches gerade getestet wird.
2. Klicken Sie auf **Replikat testen**.
3. Klicken Sie auf **Test stoppen**.
4. Bestätigen Sie Ihre Entscheidung.

Ein Failover auf ein Replikat durchführen

So führen Sie einen Failover von einer Maschine auf ein Replikat durch

1. Wählen Sie ein Replikat aus, auf welches der Failover erfolgen soll.
2. Klicken Sie auf **Replikat-Aktionen**.
3. Klicken Sie auf **Failover**.
4. Bestimmen Sie, ob das eingeschaltete Replikat mit dem Netzwerk verbunden werden soll. Als Standardvorgabe wird das Replikat mit demselben Netzwerk wie die ursprüngliche Maschine verbunden.
5. [Optional] Falls Sie das Replikat mit dem Netzwerk verbinden wollen, müssen Sie das Kontrollkästchen **Ursprüngliche virtuelle Maschine stoppen** deaktivieren, wenn die ursprüngliche Maschine online bleiben soll.
6. Klicken Sie auf **Start**.

Während sich das Replikat im Failover-Stadium befindet, können Sie eine der folgenden Aktionen wählen:

- **Failover stoppen**

  Stoppen Sie das Failover, wenn die ursprüngliche Maschine repariert wurde. Das Replikat wird ausgeschaltet. Die Replikation wird fortgesetzt.
- **Permanentes Failover auf das Replikat durchführen**

  Diese sofortige Aktion entfernt die 'Replikat'-Kennzeichnung von der virtuellen Maschine, sodass diese nicht mehr als Replikationsziel verwendet werden kann. Wenn Sie die Replikation wieder aufnehmen wollen, bearbeiten Sie den Replikationsplan, um diese Maschine als Quelle auszuwählen.
- **Failback**

  Führen Sie einen Failback aus, falls Sie einen Failover zu einer Site gemacht haben, die nicht für den Dauerbetrieb gedacht ist. Das Replikat wird zu der ursprünglichen oder einer neuen virtuellen Maschine wiederhergestellt. Sobald die Wiederherstellung zu der ursprünglichen Maschine abgeschlossen ist, wird diese eingechaltet und die Replikation fortgesetzt. Wenn Sie die Wiederherstellung zu einer neuen Maschine durchgeführt haben, bearbeiten Sie den Replikationsplan, um diese Maschine als Quelle auszuwählen.

Failover wird gestoppt

So stoppen Sie einen Failover-Vorgang

1. Wählen Sie ein Replikat, das sich im Failover-Stadium befindet.
2. Klicken Sie auf **Replikat-Aktionen**.
3. Klicken Sie auf **Failover stoppen**.
4. Bestätigen Sie Ihre Entscheidung.

Einen permanenten Failover durchführen

So können Sie einen permanenten Failover durchführen

1. Wählen Sie ein Replikat, das sich im Failover-Stadium befindet.
2. Klicken Sie auf **Replikat-Aktionen**.
3. Klicken Sie auf **Permanentes Failover**.
4. [Optional] Ändern Sie den Namen der virtuellen Maschine.
5. [Optional] Aktivieren Sie das Kontrollkästchen **Ursprüngliche virtuelle Maschine stoppen**.
6. Klicken Sie auf **Start**.

Ein Failback durchführen

So führen Sie einen Failback von einem Replikat durch

1. Wählen Sie ein Replikat, das sich im Failover-Stadium befindet.
2. Klicken Sie auf **Replikat-Aktionen**.
3. Klicken Sie auf **Failback vom Replikat**.

Die Software wählt automatisch die ursprüngliche Maschine als Zielmaschine aus.

4. [Optional] Klicken Sie auf **Zielmaschine** – und gehen Sie dann folgendermaßen vor:
   a. Bestimmen Sie, ob der Failback zu einer neuen oder einer bereits vorhandenen Maschine durchgeführt werden soll:
   b. Wählen Sie den ESXi-Host und spezifizieren Sie einen Namen für die neue Maschine – oder wählen Sie eine bereits vorhandene Maschine aus.
   c. Klicken Sie auf **OK**.
5. [Optional] Wenn Sie eine neue Maschine als Failback-Ziel verwenden, können Sie außerdem noch Folgendes tun:
   - Klicken Sie auf **Datenspeicher**, um den Datenspeicher für die virtuelle Maschine festzulegen.
   - Klicken Sie auf **VM-Einstellungen**, um die Größe des Arbeitsspeichers, die Anzahl der Prozessoren und die Netzwerkverbindungen für die virtuelle Maschine zu ändern.
6. [Optional] Klicken Sie auf **Recovery-Optionen**, wenn Sie die Failback-Optionen ändern wollen.
7. Klicken Sie auf **Recovery starten**.
8. Bestätigen Sie Ihre Entscheidung.

Replikationsoptionen

Wenn Sie die Replikationsoptionen ändern wollen, klicken Sie auf das Zahnradsymbol neben dem Namen des Replikationsplans und dann auf das Element **Replikationsoptionen**.

Changed Block Tracking (CBT)

Diese Option entspricht im Wesentlichen der Backup-Option 'CBT (Changed Block Tracking)'.

Laufwerk-Provisioning

Diese Option definiert den Laufwerk-Provisioning-Modus für das Replikat.

Die Voreinstellung ist: **Thin Provisioning**.

Folgende Werte sind verfügbar: **Thin Provisioning**, **Thick Provisioning**, **Ursprüngliche Einstellung behalten**.

Fehlerbehandlung

Diese Option entspricht im Wesentlichen der Backup-Option 'Fehlerbehandlung'.

Vor-/Nach-Befehle

Diese Option entspricht im Wesentlichen der Backup-Option 'Vor-/Nach-Befehle'.

VSS (Volume Shadow Copy Service) für virtuelle Maschinen

Diese Option entspricht im Wesentlichen der Backup-Option 'VSS (Volume Shadow Copy Service) für virtuelle Maschinen'.

Failback-Optionen

Wenn Sie die Failback-Optionen ändern wollen, klicken Sie während der Failbackup-Konfiguration auf **Recovery-Optionen**.

Fehlerbehandlung

Diese Option entspricht im Wesentlichen der Recovery-Option 'Fehlerbehandlung'.

Performance

Diese Option entspricht im Wesentlichen der Recovery-Option 'Performance'.

Vor-/Nach-Befehle

Diese Option entspricht im Wesentlichen der Recovery-Option 'Vor-/Nach-Befehle'.

VM-Energieverwaltung

Diese Option entspricht im Wesentlichen der Recovery-Option 'VM-Energieverwaltung'.

Seeding eines anfänglichen Replikats

Um die Replikation zu einem Remote-Standort zu beschleunigen und Netzwerkbandbreite einzusparen, können Sie ein Replikat-Seeding durchführen.

Wichtig
Um ein Replikat-Seeding durchführen zu können, muss der Agent für VMware (Virtuelle Appliance) auf dem ESXi-Zielhost ausgeführt werden.

So führen Sie das Seeding eines anfänglichen Replikats durch

1. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Wenn die ursprüngliche Maschine ausgeschaltet werden kann, tun Sie dies – und springen sie dann zu Schritt 4.
   - Wenn die ursprüngliche virtuelle Maschine nicht ausgeschaltet werden kann, fahren Sie mit dem nächsten Schritt fort.
2. Erstellen Sie einen Replikationsplan.

   Wählen Sie beim Erstellen des Plans bei **Zielmaschine** die Option **Neues Replikat** sowie den ESXi, der die ursprüngliche Maschine hostet.
3. Führen Sie den Plan einmal aus.

   Auf dem ursprünglichen ESXi wird ein Replikat erstellt.
4. Exportieren Sie die Dateien der virtuellen Maschine (oder des Replikats) auf ein externes Festplattenlaufwerk.
   a. Verbinden Sie das externe Laufwerk mit der Maschine, auf welcher der vSphere Client ausgeführt wird.

b. Verbinden Sie den vSphere Client mit dem ursprünglichen vCenter/ESXi.

c. Wählen Sie das neu erstellte Replikat in der Bestandsliste (Inventory) aus.

d. Klicken Sie auf **Datei** –> **Exportieren** –> **OVF-Vorlage exportieren**.

e. Spezifizieren Sie im **Verzeichnis** den entsprechenden Ordner auf dem externen Laufwerk.

f. Klicken Sie auf **OK**.

5. Senden Sie das Festplattenlaufwerk zum Remote-Standort.

6. Importieren Sie das Replikat in den ESXi-Zielhost.

a. Verbinden Sie das externe Laufwerk mit der Maschine, auf welcher der vSphere Client ausgeführt wird.

b. Verbinden Sie den vSphere Client mit dem Ziel-vCenter/-ESXi.

c. Klicken Sie auf **Datei** –> **OVF-Vorlage bereitstellen**.

d. Spezifizieren Sie bei **Von einer Datei oder URL bereitstellen** die Vorlage, die Sie in Schritt 4 exportiert haben.

e. Schließen Sie die Import-Prozedur ab.

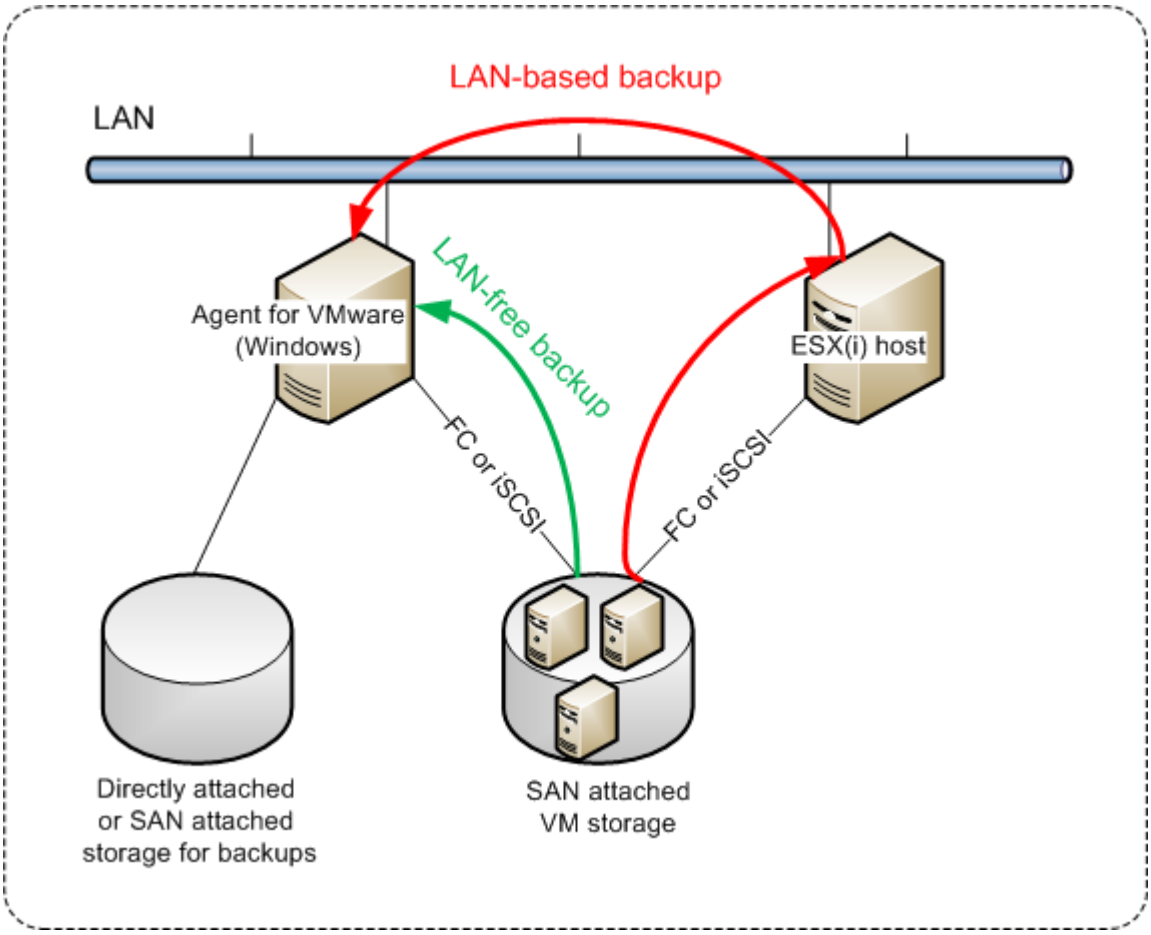
7. Bearbeiten Sie den Replikationsplan, den Sie in Schritt 2 erstellt haben. Wählen Sie bei **Zielmaschine** die Option **Vorhandenes Replikat** und wählen Sie dann das importierte Replikat aus.

Die Software wird daraufhin die Aktualisierung des Replikats fortsetzen. Alle Replikationen werden inkrementell sein.

Agent für VMware – LAN-freies Backup

Sollte Ihr ESXi einen per SAN angeschlossenen Storage verwenden, dann installieren Sie den Agenten auf einer Maschine, die an dasselbe SAN angeschlossen ist. Der Agent führt das Backup der virtuellen Maschinen dann direkt vom Storage aus, statt über den ESXi-Host und das LAN. Diese Fähigkeit wird auch als 'LAN-freies Backup' bezeichnet.

Das nachfolgende Diagramm illustriert LAN-basierte und LAN-freie Backups. Ein LAN-freier Zugriff auf virtuelle Maschinen ist verfügbar, falls Sie ein per Fibre Channel (FC) oder iSCSI angebundenes Storage Area Network haben. Um die Übertragung von Backup-Daten via LAN komplett ausschließen zu können, müssen Sie die Backups auf einem lokalen Laufwerk der Maschine des Agenten oder auf einem per SAN angebundenen Storage speichern.



So ermöglichen Sie dem Agenten, auf einen Datenspeicher direkt zuzugreifen

1. Installieren Sie den Agenten für VMware auf einer Windows-Maschine, die Netzwerkzugriff auf den vCenter Server hat.
2. Verbinden Sie die LUN (Logical Unit Number), die den Datenspeicher für die Maschine hostet. Beachten Sie dabei:
   - Verwenden Sie dasselbe Protokoll (z.B. iSCSI oder FC), das auch zur Datenspeicher-Verbindung mit dem ESXi verwendet wird.
   - Die LUN *darf nicht* initialisiert werden und muss als 'Offline'-Laufwerk in der **Datenträgerverwaltung** erscheinen. Falls Windows die LUN initialisiert, kann sie beschädigt und damit unlesbar für VMware vSphere werden.

Als Ergebnis wird der Agent den SAN-Transportmodus nutzen, um auf die virtuelle Laufwerke zuzugreifen. Das bedeutet, es werden nur die blanken ('raw') LUN-Sektoren über iSCSI/FC gelesen, ohne dass das VMFS-Dateisystem erkannt wird (welches von Windows nicht unterstützt wird).

Einschränkungen

- In vSphere 6.0 (und höher) kann der Agent den SAN-Transportmodus nicht verwenden, wenn sich einige der VM-Laufwerke auf einem „VMware Virtual Volume“ (VVol) befinden und einige nicht. Die Backups solcher virtuellen Maschinen werden daher fehlschlagen.

- Verschlüsselte virtuelle Maschinen, die mit VMware vSphere 6.5 eingeführt wurden, werden via LAN gesichert – und zwar auch dann, wenn Sie den SAN-Transportmodus für den Agenten konfiguriert haben. Der Agent wird stattdessen auf den NBD-Transportmodus zurückgreifen, weil VMware den SAN-Transportmodus beim Backup verschlüsselter virtueller Laufwerke nicht unterstützt.

Beispiel

Falls Sie ein iSCSI-SAN verwenden, konfigurieren Sie den iSCSI-Initiator auf einer unter Windows laufenden Maschine, auf welcher der Agent für VMware installiert ist.

So konfigurieren Sie die SAN-Richtlinie

1. Melden Sie sich als Administrator an, öffnen Sie die Eingabeaufforderung, geben Sie den Befehl `diskpart` ein und drücken Sie dann auf die **Eingabetaste**.
2. Geben Sie `san` und drücken Sie dann die **Eingabetaste**. Überprüfen Sie, dass **SAN-Richtlinie: Offline – Alle** angezeigt wird.
3. Falls ein anderer Wert für die SAN-Richtlinie eingestellt ist:
   a. Geben Sie `san policy=offlineall` ein.
   b. Drücken Sie die **Eingabetaste**.
   c. Führen Sie Schritt 2. aus, um zu überprüfen, dass die Einstellung korrekt angewendet wurde.
   d. Starten Sie die Maschine neu.

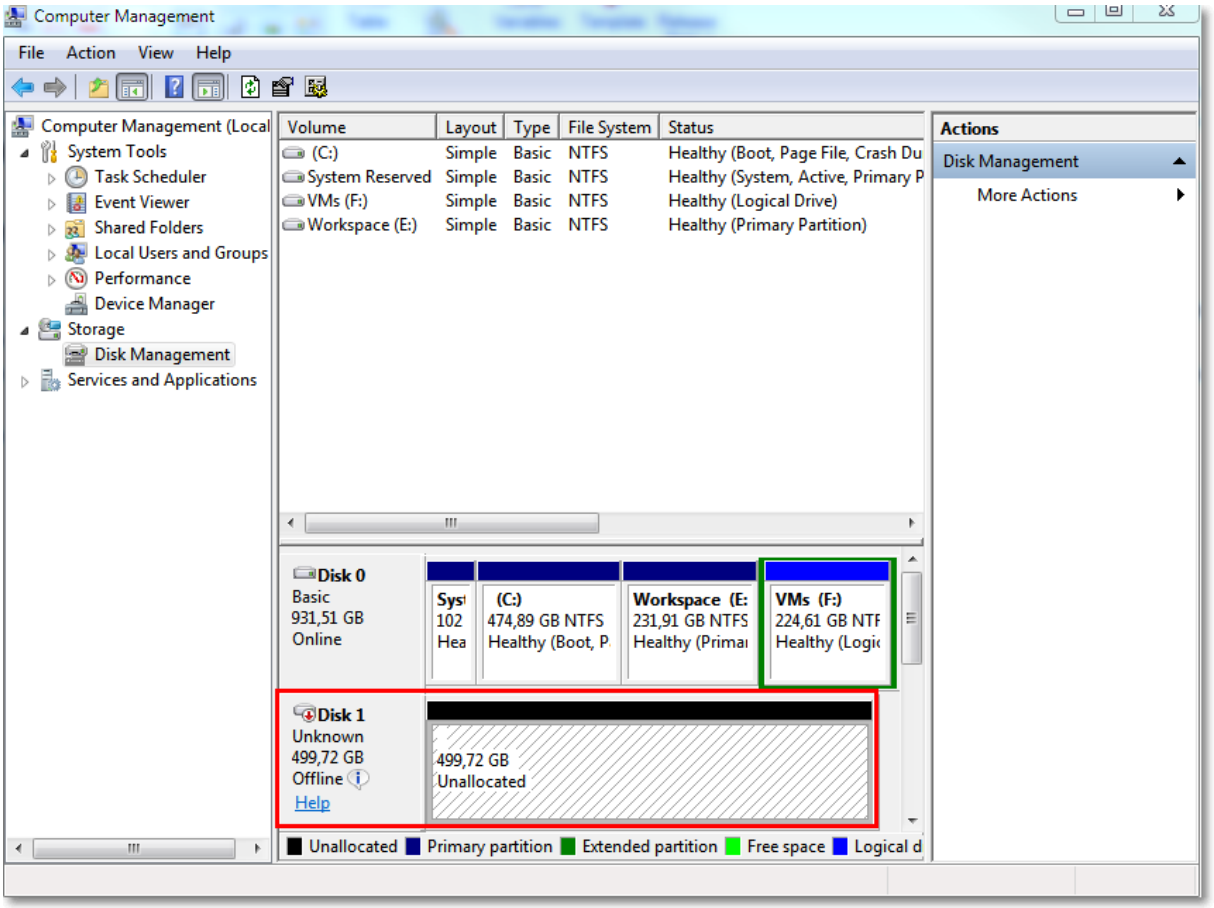
So konfigurieren Sie einen iSCSI-Initiator

1. Gehen Sie zu **Systemsteuerung** –> **Verwaltung** –> **iSCSI-Initiator**.

   Hinweis
   Wenn Sie das Systemsteuerungsmodul **Verwaltung** nicht finden können, müssen Sie evtl. die Ansicht der **Systemsteuerung** von **Start** oder **Kategorie** auf eine andere Ansicht umstellen – oder die Suchfunktion verwenden.

2. Wenn Sie den Microsoft iSCSI-Initiator das erste Mal aufrufen, müssen Sie bestätigen, dass Sie den Microsoft iSCSI-Initiator-Dienst starten wollen.
3. Geben Sie in der Registerkarte **Ziele** den vollqualifizierten Domain-Namen (FQDN) oder die IP-Adresse des SAN-Zielgerätes ein und klicken Sie dann auf **Schnell verbinden**.
4. Wählen Sie die LUN aus, die den Datenspeicher hostet, und klicken Sie dann auf **Verbinden**.
   Sollte die LUN nicht angezeigt werden, dann überprüfen Sie, dass die Zonenzuweisung auf dem iSCSI-Ziel der Maschine, die den Agenten ausführt, ermöglicht, auf die LUN zuzugreifen. Die Maschine muss in die Liste der erlaubten iSCSI-Initiatoren auf diesem Ziel aufgenommen sein.
5. Klicken Sie auf **OK**.

Die betriebsbereite SAN-LUN sollte in der **Datenträgerverwaltung** so wie im unterem Screenshot angezeigt werden.



Einen lokal angeschlossenen Storage verwenden

Sie können an einen Agenten für VMware (Virtuelle Appliance) ein zusätzliches Laufwerk anschließen, sodass der Agent seine Backups zu diesem lokal angeschlossenen Storage durchführen kann. Mit diesem Ansatz wird Netzwerkverkehr zwischen dem Agenten und dem Backup-Speicherort vermieden.

Eine virtuelle Appliance, die auf demselben Host oder Cluster mit den gesicherten virtuellen Maschinen ausgeführt wird, hat direkten Zugriff auf den/die Datenspeicher, wo sich die Maschinen befinden. Das bedeutet, dass die Appliance die gesicherten Laufwerke per HotAdd-Transport anschließen kann und der Backup-Verkehr daher von einem lokalen Laufwerk zu einem anderen weitergeleitet wird. Wenn der Datenspeicher als **Festplatte/LUN** (statt per **NFS**) verbunden ist, wird das Backup komplett 'LAN-frei' sein. Bei einem NFS-Datenspeicher kommt es dagegen zum Netzwerkverkehr zwischen dem Datenspeicher und dem Host.

Die Verwendung eines lokal angeschlossenen Storages setzt voraus, dass der Agent immer dieselben Maschinen sichert. Sie müssen, falls mehrere Agenten innerhalb der vSphere arbeiten – und einer oder mehrere davon lokal angeschlossene Storages verwenden – jeden Agenten manuell an alle Maschinen binden, die er sichern soll. Falls die Maschinen stattdessen vom Management Server zwischen den Agenten verteilt werden, können die Backups einer Maschine über mehrere Storages zerstreut werden.

Sie können den Storage zu einem bereits arbeitenden Agenten hinzufügen oder wenn Sie den Agenten über eine OVF-Vorlage bereitstellen.

So können Sie einen Storage an einen bereits arbeitenden Agenten anschließen

1. Klicken Sie in der VMware vSphere-Bestandsliste (Inventory) mit der rechten Maustaste auf den Agenten für VMware (Virtuelle Appliance).
2. Fügen Sie das Laufwerk hinzu, indem Sie die Einstellungen der virtuellen Maschine bearbeiten. Die Laufwerksgröße muss mindestens 10 GB betragen.

   Warnung!
   Seien Sie vorsichtig, wenn Sie ein bereits existierendes Laufwerk hinzufügen. Sobald der Storage erstellt wird, gehen alle zuvor auf dem Laufwerk enthaltenen Daten verloren.

3. Gehen Sie zur Konsole der virtuellen Appliance. Der Link **Storage erstellen** ist im unteren Bereich der Anzeige verfügbar. Wenn nicht, klicken Sie auf **Aktualisieren**.
4. Klicken Sie auf den Link **Storage erstellen**, wählen Sie das Laufwerk und spezifizieren Sie eine Bezeichnung für dieses. Die Länge der Bezeichnung ist aufgrund von Dateisystembeschränkungen auf 16 Zeichen limitiert.

So können Sie einen lokal angeschlossen Storage als Backup-Ziel auswählen

- Wählen Sie beim Erstellen eines Schutzplans unter **Backup-Ziel** die Option **Lokale Ordner** – Sie dann den mit dem lokal angeschlossenen Storage korrespondierenden Laufwerksbuchstaben an, beispielsweise **D:**.

Hinweis
Ein Locally Attached Storage (LAS) ist für relativ kleine Umgebungen mit einem einzigen Agenten (Virtuelle Appliance) konzipiert. Wir haben Locally Attached Storage-Geräte mit einer Größe von bis zu 5 TB getestet. Sie können auf eigenes Risiko größere Laufwerke anschließen, aber solche Konfigurationen werden nicht offiziell unterstützt. Für mehr als 5 TB an Backup-Daten empfehlen wir Ihnen, andere Storage-Typen zu verwenden. Sie können zum Beispiel ein virtuelles VMware-Laufwerk erstellen und an eine beliebige virtuelle Maschine anhängen sowie darauf eine Netzwerkfreigabe erstellen, die dann als Backup-Ziel anstelle eines LAS verwendet wird.

Virtuelle Maschinen anbinden

Dieser Abschnitt gibt Ihnen einen Überblick darüber, wie der Cyber Protection Service die Aktionen mehrerer Agenten innerhalb des VMware vCenters organisiert.

Der untere Verteilungsalgorithmus gilt für die virtuellen Appliances und die unter Windows installierten Agenten.

Verteilungsalgorithmus

Die virtuellen Maschinen werden automatisch gleichmäßig zwischen den Agenten für VMware verteilt. Mit 'gleichmäßig' ist gemeint, dass jeder Agent eine gleiche Anzahl von Maschinen verwaltet. Die Menge an Speicherplatz, die eine virtuelle Maschine belegt, wird nicht gezählt.

Wenn Sie jedoch einen Agenten für eine Maschine auswählen, versucht die Software die Gesamt-Performance des Systems zu optimieren. Das bedeutet, dass die Software den Speicherort des Agenten und der virtuellen Maschine berücksichtigt. Ein Agent, der auf demselben Host vorliegt, wird bevorzugt. Falls es keinen Agenten auf demselben Host gibt, wird ein Agent aus demselben Cluster bevorzugt.

Sobald eine virtuelle Maschine einem Agenten zugewiesen wurde, werden alle Backups dieser Maschine an diesen Agenten delegiert.

Neuverteilung

Wenn eine aufgebaute Verteilung nicht (mehr) funktioniert, weil es bei der Auslastung zwischen den Agenten zu einem Ungleichgewicht von über 20% gekommen ist, erfolgt eine automatische Neuverteilung. Dazu kann es kommen, wenn eine Maschine oder ein Agent hinzugefügt oder entfernt wird – oder eine Maschine zu einem anderen Host bzw. Cluster migriert – oder wenn Sie eine Maschine manuell an einen Agenten anbinden. Wenn das passiert, teilt der Cyber Protection Service die Maschinen unter Verwendung desselben Algorithmus neu auf.

Beispielsweise, wenn Sie erkennen, dass Sie mehr Agenten zur Unterstützung des Durchsatzes benötigen, und eine virtuelle Appliance auf einen Cluster bereitstellen. Der Cyber Protection Service wird die geeignetsten Maschinen dem neuen Agenten zuweisen. Die Last der alten Agenten wird reduziert.

Wenn Sie einen Agenten aus dem Cyber Protection Service entfernen, dann werden die diesem Agenten zugewiesenen Maschinen unter den verbliebenen Agenten verteilt. Diese passiert jedoch nicht, wenn ein Agent beschädigt wird oder manuell aus vSphere gelöscht wird. Eine Neuverteilung wird in diesem Fall nur dann gestartet, wenn Sie einen solchen Agenten über die Weboberfläche entfernen.

Die Verteilungsergebnisse einsehen

Sie können das Ergebnis der automatischen Verteilung einsehen:

- für jede virtuelle Maschine in der Spalte **Agent** im Bereich **Alle Geräte**
- im Abschnitt **Zugewiesene virtuelle Maschinen** des Fensterbereichs **Details**, wenn ein Agent im Bereich **Einstellungen** –> **Agenten** ausgewählt wurde

Manuelle Anbindung

Durch die Option 'Anbindung des Agenten für VMware' können Sie eine virtuelle Maschine von diesem Verteilungsprozess ausschließen, indem Sie einen Agenten spezifizieren, der die Backups dieser Maschine immer durchführen muss. Die Gesamtbalance bleibt erhalten, aber diese spezielle Maschine kann nur dann zu einem anderen Agenten weitergereicht werden, wenn der der ursprüngliche Agent entfernt wurde.

So können Sie eine Maschine an einen Agenten binden

1. Wählen Sie die Maschine aus.
2. Klicken Sie auf **Details**.
   Die Software zeigt im Bereich **Zugewiesener Agent** den Agenten an, der die ausgewählte Maschine derzeit verwaltet.
3. Klicken Sie auf **Ändern**.
4. Wählen Sie **Manuell**.
5. Bestimmen Sie den Agenten, den Sie an die Maschine anbinden wollen.
6. Klicken Sie auf **Speichern**.

So können Sie eine Maschine von einem Agenten trennen

1. Wählen Sie die Maschine aus.
2. Klicken Sie auf **Details**.
   Die Software zeigt im Bereich **Zugewiesener Agent** den Agenten an, der die ausgewählte Maschine derzeit verwaltet.
3. Klicken Sie auf **Ändern**.
4. Wählen Sie **Automatisch**.
5. Klicken Sie auf **Speichern**.

Die automatische Zuweisung für einen Agenten deaktivieren

Sie können die automatische Zuweisung für einen Agenten für VMware deaktivieren und ihn so vom Verteilungsprozess ausschließen, indem Sie eine Liste der Maschinen spezifizieren, die dieser Agent sichern muss. Die Gesamtbalance zwischen den anderen Agenten bleibt erhalten.

Die Automatische Zuweisung für einen Agenten kann nicht deaktiviert werden, wenn es keine anderen/weiteren registrierten Agenten gibt oder wenn die automatische Zuweisung für alle anderen Agenten deaktiviert ist.

So können Sie die automatische Zuweisung für einen Agenten deaktivieren

1. Klicken Sie auf **Einstellungen** –> **Agenten**.
2. Wählen Sie den Agenten für VMware aus, für den Sie die automatische Zuweisung deaktivieren wollen.
3. Klicken Sie auf **Details**.
4. Deaktivieren Sie den Schalter für **Automatische Zuweisung**.

Anwendungsbeispiele

- Die manuelle Anbindung kann nützlich sein, falls Sie eine bestimmte (sehr große) Maschine durch den Agenten für VMware (Windows) über eine 'Fibre Channel'-Verbindung sichern wollen, während das Backup anderer Maschinen durch virtuelle Appliances erfolgt.

- Es ist außerdem notwendig, VMs an einen Agenten zu binden, wenn der Agent einen lokal angeschlossenen Storage hat.
- Durch Deaktivierung der automatischen Zuweisung können Sie sicherstellen, dass eine bestimmte Maschine auf vorhersehbare Weise nach einer von Ihnen spezifizierten Planung gesichert wird. Ein Agent, der nur eine einzige VM sichern muss, ist nicht mit dem Backup anderer VMs beschäftigt, wenn der geplante Backup-Zeitpunkt kommt.
- Die Deaktivierung der automatischen Zuweisung ist nützlich, wenn Sie mehrere ESXi-Hosts haben, die an geografisch unterschiedlichen Orten stehen. Wenn Sie die automatische Zuweisung deaktivieren und dann die VMs auf jedem Host an einen Agenten auf demselben Host binden, können Sie sicherstellen, dass der Agent niemals irgendwelche Maschinen sichert, die auf einem entfernten ESXi-Host liegen, und so zudem Netzwerkdatenverkehr einsparen.

Pre-Freeze- und Post-Thaw-Skripte automatisch ausführen

Mit VMware Tools können Sie benutzerdefinierte Pre-Freeze- und Post-Thaw-Skripte automatisch auf virtuellen Maschinen ausführen, die Sie im agentenlosen Modus sichern. So können Sie z.B. benutzerdefinierte Stilllegungsskripte (Quiescing-Skripte) ausführen und applikationskonsistente Backups für virtuelle Maschinen erstellen, auf denen Applikationen laufen, die nicht VSS-kompatibel sind.

Voraussetzungen

Die Pre-Freeze- und Post-Thaw-Skripte müssen sich in einem bestimmten Speicherort auf der virtuellen Maschine befinden.

- Bei virtuellen Windows-Maschinen hängt der Speicherort dieses Ordners von der ESXi-Version des Hosts ab.

  Bei virtuellen Maschinen, die auf einem ESXi 6.5-Host laufen, lautet dieser Ordner beispielsweise: `C:\Programme\VMware\VMware Tools\backupScripts.d\`. Sie müssen den Ordner `backupScritps.d` manuell erstellen. Sie sollten keine anderen Dateitypen in diesem Ordner speichern, weil dies die VMware Tools instabil machen könnte.

  Weitere Informationen zum Speicherort der Pre-Freeze- und Post-Thaw-Skripts für andere ESXi-Versionen finden Sie in der VMware-Dokumentation.
- Bei virtuellen Linux-Maschinen sollten Sie Ihre Skripte in das Verzeichnis `/usr/sbin/pre-freeze-script` bzw. `/usr/sbin/post-thaw-script` kopieren. Die Skripte in `/usr/sbin/pre-freeze-script` werden ausgeführt, wenn Sie einen Snapshot erstellen – während die in `/usr/sbin/post-thaw-script` ausgeführt werden, wenn der Snapshot finalisiert wird. Die Skripte müssen vom VMware Tools-Benutzer ausführbar sein.

So können Sie Pre-Freeze- und Post-Thaw-Skripte automatisch ausführen

1. Stellen Sie sicher, dass die VMware Tools auf der virtuellen Maschine installiert sind.
2. Speichern Sie auf der virtuellen Maschine Ihre benutzerdefinierten Skripte in dem gewünschten Ordner.

3. Aktivieren Sie im Schutzplan für diese Maschine die Option **VSS (Volume Shadow Copy Service) für virtuelle Maschinen**.
   Dadurch wird ein VMware-Snapshot erstellt, bei dem die Option **Gast-Dateisystem stilllegen** (Quiesce guest file system) aktiviert ist, was wiederum die Pre-Freeze- und Post-Thaw-Skripte innerhalb der virtuellen Maschine auslöst.

Auf virtuellen Maschinen, auf denen VSS-konforme Applikationen (wie Microsoft SQL Server oder Microsoft Exchange) laufen, müssen Sie keine benutzerdefinierten Ruheskripte ausführen. Wenn Sie für solche Maschinen ein applikationskonsistentes Backup erstellen wollen, müssen Sie im Schutzplan die Option **VSS (Volume Shadow Copy Service) für virtuelle Maschinen** aktivieren.

Unterstützung für die Migration von virtuellen Maschinen

Dieser Abschnitt enthält Informationen über die Migration von virtuellen Maschinen innerhalb einer vSphere-Umgebung – einschließlich der Migration zwischen ESXi Hosts, die Teil eines vSphere Clusters sind.

vMotion ermöglicht es, das Stadium und die Konfiguration einer virtuellen Maschine zu einem anderen Host zu verschieben, während die Laufwerke der Maschine am selben Speicherort auf einem gemeinsam genutzten Storage (Shared Storage) verbleiben. Storage vMotion ermöglicht es, die Laufwerke einer virtuellen Maschine von einem Datenspeicher zu einem anderen zu verschieben.

- Für virtuelle Maschinen, auf denen der Agent für VMware (Virtuelle Appliance) läuft, wird keine Migration mit vMotion (einschließlich Storage vMotion) unterstützt, sodass diese automatisch deaktiviert ist. Diese virtuelle Maschine wird in der vSphere-Cluster-Konfiguration in die Liste **VM-Außerkraftsetzungen** aufgenommen.
- Wenn ein Backup einer virtuellen Maschine gestartet wird, wird die Migration mit vMotion (einschließlich Storage vMotion) automatisch deaktiviert. Diese virtuelle Maschine wird in der vSphere-Cluster-Konfiguration temporär in die Liste **VM-Außerkraftsetzungen** aufgenommen. Nachdem das Backup abgeschlossen wurde, werden die Einstellungen für **VM-Außerkraftsetzungen** automatisch auf ihr vorheriges Stadium zurückgesetzt.
- Ein Backup für eine virtuelle Maschine kann nicht gestartet werden, wenn diese gerade mit vMotion (einschließlich Storage vMotion) migriert wird. Das Backup dieser Maschine wird jedoch gestartet, sobald deren Migration abgeschlossen wurde.

Virtualisierungsumgebungen verwalten

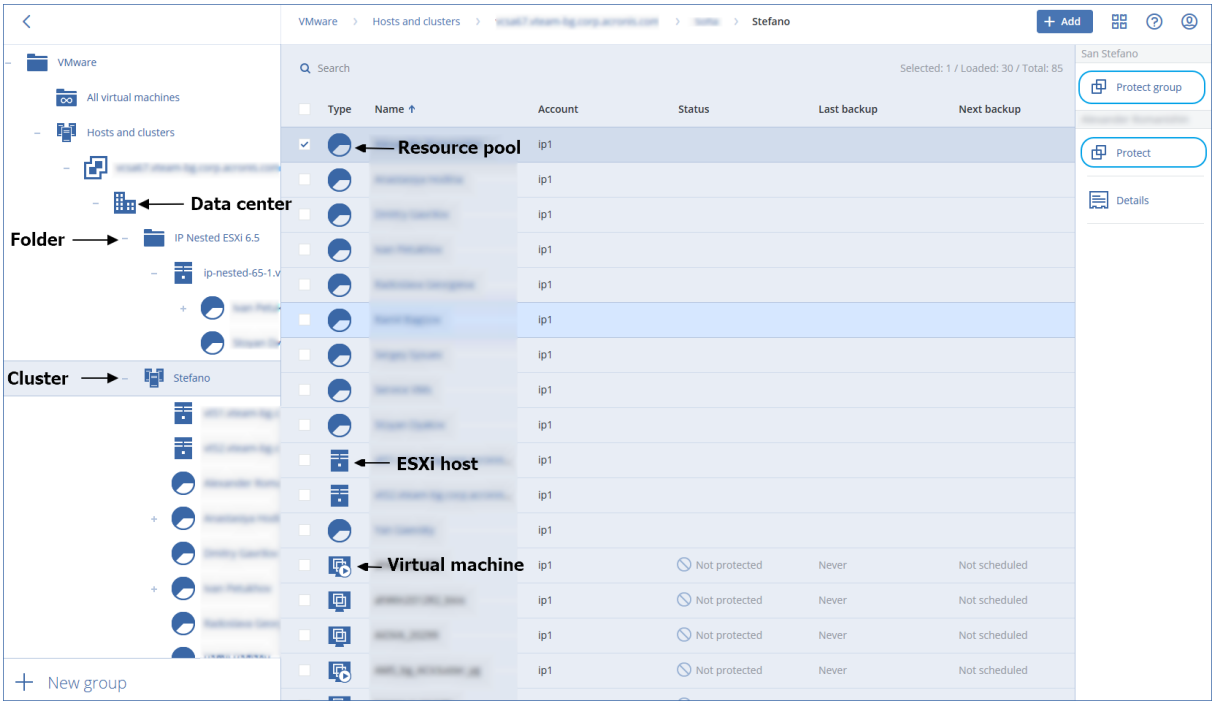
Sie können vSphere-, Hyper-V- und Virtuozzo-Umgebungen in ihrer nativen Darstellung anzeigen lassen. Sobald der entsprechende Agent installiert und registriert ist, werden die Registerkarten **VMware**, **Hyper-V** oder **Virtuozzo** unter **Geräte** angezeigt.

Sie können in der Registerkarte **VMware** die folgenden vSphere-Infrastrukturobjekte per Backup sichern:

- Datacenter
- Ordner
- Cluster
- ESXi-Host
- Ressourcenpool

Jedes dieser Infrastrukturobjekte funktioniert als Gruppenobjekt für virtuelle Maschinen. Wenn Sie einen Schutzplan auf irgendeines dieser Gruppenobjekte anwenden, werden alle Maschinen, die in diesem enthalten sind, per Backup gesichert. Sie können entweder die ausgewählte Maschinengruppe sichern, indem Sie auf **Schützen** klicken – oder die übergeordnete Maschinengruppe, zu der die ausgewählte Gruppe gehört, indem Sie auf **Gruppe schützen** klicken.

Beispiel: Sie haben erst den Cluster 'Stefano' ausgewählt und dann den darin befindlichen Ressourcenpool. Wenn Sie auf **Schützen** klicken, werden alle virtuellen Maschinen per Backup gesichert, die zu dem ausgewählten Ressourcenpool gehören. Wenn Sie auf **Gruppe schützen** klicken, werden alle virtuellen Maschinen per Backup gesichert, die sich im Cluster 'Stefano' befinden.



Über die Registerkarte **VMware** können Sie die Zugriffsanmeldedaten für einen vCenter Server oder eigenständigen ESXi-Host ändern, ohne den Agenten neu installieren zu müssen.

So ändern Sie die Zugriffsanmeldedaten für einen vCenter Server oder eigenständigen ESXi-Host

1. Klicken Sie bei **Geräte** auf **VMware**.
2. Klicken Sie auf **Hosts und Cluster**.

3. Wählen Sie in der '**Hosts und Cluster**'-Liste (rechts neben dem '**Hosts und Cluster**'-Verzeichnisbaum) denjenigen vCenter Server oder eigenständigen ESXi-Host aus, der bei der Installation des Agenten für VMware spezifiziert wurde.
4. Klicken Sie auf **Details**.
5. Klicken Sie unter **Anmeldedaten** auf den Benutzernamen.
6. Spezifizieren Sie die neuen Anmeldedaten und klicken Sie abschließend auf **OK**.

Den Backup-Status im vSphere Client einsehen

Sie können den Backup-Status und den letzte Backup-Zeitpunkt einer virtuellen Maschine im vSphere Client einsehen.

Diese Informationen erscheinen in der Übersicht der virtuellen Maschine (**Übersicht** –> **Benutzerdefinierte Attribute**/**Anmerkungen**/**Hinweise**, in Abhängigkeit vom Client-Typ und der vSphere-Version). Sie können außerdem die Spalten **Letztes Backup** und **Backup-Status** auf der Registerkarte **Virtuelle Maschinen** für jedes Datacenter, jeden Host, Ordner, Ressourcenpool oder gesamten vCenter Server aktivieren.

Um diese Attribute bereitzustellen, muss der Agent für VMware neben den in Abschnitt 'Agent für VMware – notwendige Berechtigungen' beschriebenen Berechtigungen noch über folgende Berechtigungen verfügen:

- **Global** –> **Benutzerdefinierte Attribute verwalten**
- **Global** –> **Benutzerdefinierte Attribute festlegen**

Agent für VMware – notwendige Berechtigungen

Um Aktionen mit vCenter-Objekten (wie z.B. virtuelle Maschinen, ESXi-Hosts, Cluster, vCenter und mehr) durchführen zu können, muss sich der Agent für VMware auf dem vCenter- oder ESXi-Host mithilfe der von einem Benutzer bereitgestellten vSphere-Anmeldedaten authentifizieren. Das vSphere-Konto, welches vom Agenten für VMware zur Verbindung mit vSphere verwendet wird, muss auf allen Ebenen der vSphere-Infrastruktur (beginnend mit der vCenter-Ebene) über die erforderlichen Berechtigungen verfügen.

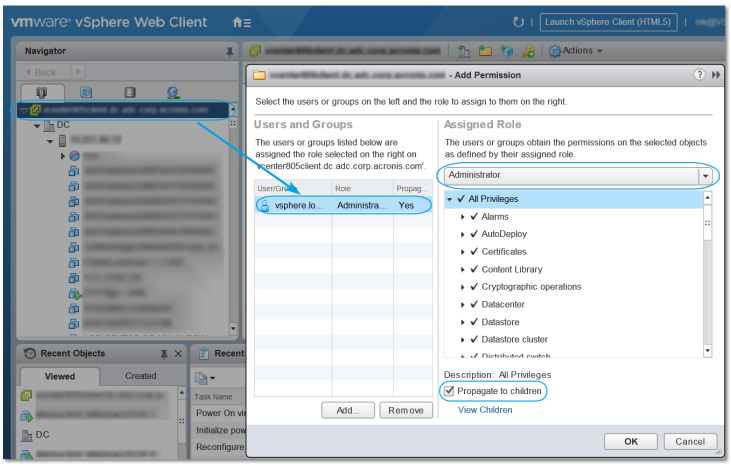
Spezifizieren Sie das vSphere-Konto mit den benötigten Berechtigungen, wenn Sie den Agenten für VMware installieren oder konfigurieren. Informationen darüber, wie Sie das Konto auch zu einem späteren Zeitpunkt noch ändern können, finden Sie im Abschnitt '"Virtualisierungsumgebungen verwalten" (S. 764)'.

So können Sie einem vSphere-Benutzer auf der vCenter-Ebene die Berechtigungen zuweisen

1. Melden Sie sich am vSphere Web Client an
2. Klicken Sie mit der rechten Maustaste auf vCenter und wählen Sie **Berechtigung hinzufügen**.
3. Sie müssen einen neuen Benutzer mit der erforderlichen Rolle (die Rolle muss alle erforderlichen

Berechtigungen aus der unteren Tabelle enthalten) auswählen oder hinzufügen.

4. Aktivieren Sie die Option **An untergeordnete Objekte weitergeben**.



Objekt	Recht	Aktion			
		Backup einer VM	Recovery zu einer neuen VM	Recovery zu einer existierenden VM	VM von Backup ausführen
Kryptografische Operationen (ab vSphere 6.5)	**Laufwerk hinzufügen**	+*			
	Direktzugriff	+*			
Datenspeicher	**Speicher zuweisen**		+	+	+
	Datenspeicher durchsuchen				+
	Datenspeicher konfigurieren	+	+	+	+
	Dateivorgänge auf niedriger Ebene				+
Global	**Lizenzen**	+	+	+	+
	Methoden deaktivieren	+	+	+	
	Methoden aktivieren	+	+	+	
	Benutzerdefinierte Attribute verwalten	+	+	+	
	Benutzerdefinierte Attribute festlegen	+	+	+	
Host –>	**Konfiguration für**				+

Konfiguration	**Speicherpartition**				
Host > **Lokale Operationen**	**VM erstellen**				+
	VM löschen				+
	Virtuelle Maschine rekonfigurieren				+
Netzwerk	**Netzwerk zuweisen**		+	+	+
Ressource	**Virtuelle Maschine zu Ressourcenpool zuweisen**		+	+	+
Virtuelle Maschine –> **Konfiguration**	**Vorhandenes Laufwerk hinzufügen**	+	+		+
	Neues Laufwerk hinzufügen		+	+	+
	Gerät hinzufügen oder entfernen		+		+
	Erweitert	+	+	+	
	CPU-Anzahl ändern		+		
	Festplattenänderungsverfolgung	+		+	
	Festplatten-Lease	+		+	
	Arbeitsspeicher		+		
	Laufwerk entfernen	+	+	+	+
	Umbenennen		+		
	Anmerkung festlegen				+
	Einstellungen		+	+	+
Virtuelle Maschine –> **Gastbetriebssystem**	**Programmausführung im Gastbetriebssystem**	+**			
	Gastvorgangsabfragen	+**			
	Änderungen des Gastbetriebssystems	+**			
Virtuelle Maschine –>	**Ticket zur Steuerung durch Gast abrufen** (in vSphere 4.1				+

Interaktion	und 5.0)				
	CD-Medien konfigurieren		+	+	
	Gastbetriebssystem-Verwaltung über VIX API (in vSphere 5.1 und höher)				+
	Ausschalten			+	+
	Einschalten		+	+	+
Virtuelle Maschine –> **Inventarisierung**	**Aus vorhandener erstellen**		+	+	+
	Neu erstellen		+	+	+
	Registrieren				+
	Entfernen		+	+	+
	Registrierung aufheben				+
Virtuelle Maschine –> **Provisioning**	**Laufwerkszugriff erlauben**		+	+	+
	Lesezugriff auf Laufwerk erlauben	+		+	
	Download virtueller Maschine zulassen	+	+	+	+
Virtuelle Maschine –> **Status** **Virtuelle Maschine** –> **Snapshot-Verwaltung** (vSphere 6.5 und höher)	**Snapshot erstellen**	+		+	+
	Snapshot entfernen	+		+	+
vApp	**Virtuelle Maschine hinzufügen**				+

* Diese Berechtigung ist nur zum Backup von verschlüsselten Maschinen erforderlich.

** Diese Berechtigung ist nur für applikationskonforme Backups erforderlich.

Backup von geclusterten Hyper-V-Maschinen

In einem Hyper-V-Cluster können virtuelle Maschinen zwischen den Cluster-Knoten migrieren. Folgen Sie diesen Anweisungen, um ein korrektes Backup von geclusterten Hyper-V-Maschinen einzurichten:

1. Eine Maschine muss für Backups verfügbar sein, egal zu welchem Knoten sie migriert wird. Um zu gewährleisten, dass der Agent für Hyper-V auf jedem Knoten auf eine Maschine zugreifen kann, muss der Agenten-Dienst (Agent Service) unter einem Domain-Benutzerkonto ausgeführt werden, welches auf jedem der Cluster-Knoten über administrative Berechtigungen verfügt.
   Wir empfehlen, dass Sie ein solches Konto für den Agenten-Dienst während der Installation des Agenten für Hyper-V spezifizieren.
2. Installieren Sie den Agenten für Hyper-V auf jedem Knoten des Clusters.
3. Registrieren Sie alle Agenten im Cyber Protection Service.

Hochverfügbarkeit einer wiederhergestellten Maschine

Wenn Sie Laufwerke aus einem Backup zu einer *existierenden* virtuellen Hyper-V-Maschine wiederherstellen, wird die Eigenschaft 'Hochverfügbarkeit' der Maschine nicht verändert.

Wenn Sie gesicherte Laufwerke zu einer *neuen* virtuellen Hyper-V-Maschine wiederherstellen, wird die resultierende Maschine nicht hochverfügbar sein. Sie wird als Reserve-Maschine (Spare Machine) betrachtet und ist normalerweise ausgeschaltet. Falls Sie die Maschine in einer Produktionsumgebung einsetzen müssen, können Sie deren Hochverfügbarkeit über das **Failovercluster-Verwaltungs-**-Snap-in konfigurieren.

Die Gesamtzahl der gleichzeitig gesicherten virtuellen Maschinen begrenzen

In der Backup-Option **Planung** können Sie die maximale Anzahl der virtuellen Maschinen festlegen, die gleichzeitig pro Planung gesichert werden.

Wenn ein Agent mehrere Pläne gleichzeitig ausführt, addiert sich die Anzahl der Maschinen, die gleichzeitig gesichert werden. Dies kann die Backup-Performance beeinträchtigen und den Host sowie den Storage für virtuelle Maschinen überlasten. Sie können diese Probleme vermeiden, wenn Sie eine entsprechende Beschränkung auf der Ebene des Agenten konfigurieren.

So können Sie die Anzahl der gleichzeitigen Backups auf Agenten-Ebene beschränken

Agent für VMware (Windows)

1. Erstellen Sie auf der Maschine mit dem Agenten ein neues Text-Dokument und öffnen Sie dieses in einem Text-Editor.
2. Kopieren Sie die nachfolgenden Zeilen und fügen Sie diese dann in die Datei ein.

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_
MACHINE\SOFTWARE\Acronis\MMS\Configuration\ManagedMachine\SimultaneousBackupsLimits]
"MaxNumberOfSimultaneousBackups"=dword:00000001
```

3. Ersetzen Sie `00000001` mit dem Hexadezimalwert der Begrenzung, die Sie festlegen wollen. Beispiele: `00000001` ist 1 und `0000000A` ist 10.
4. Speichern Sie das Dokument als Datei mit dem Namen '**limit.reg**'.
5. Führen Sie die Datei 'als Administrator' aus.
6. Bestätigen Sie, dass Sie die Änderung der Windows Registry wirklich ausführen wollen.
7. Starten Sie den Agenten neu.
   a. Klicken Sie im **Start**-Menü auf **Ausführen**.
   b. Geben Sie **cmd** ein und klicken Sie anschließend auf **OK**.
   c. Führen Sie in der Kommandozeile die nachfolgenden Befehle aus:

```
net stop mms
net start mms
```

Agent für Hyper-V

1. Erstellen Sie auf der Maschine mit dem Agenten ein neues Text-Dokument und öffnen Sie dieses in einem Text-Editor.
2. Kopieren Sie die nachfolgenden Zeilen und fügen Sie diese dann in die Datei ein.

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_
MACHINE\SOFTWARE\Acronis\MMS\Configuration\ManagedMachine\SimultaneousBackupsLimits]
"MaxNumberOfSimultaneousBackups"=dword:00000001
```

3. Ersetzen Sie `00000001` mit dem Hexadezimalwert der Begrenzung, die Sie festlegen wollen. Beispiele: `00000001` ist 1 und `0000000A` ist 10.
4. Speichern Sie das Dokument als Datei mit dem Namen '**limit.reg**'.
5. Führen Sie die Datei 'als Administrator' aus.
6. Bestätigen Sie, dass Sie die Änderung der Windows Registry wirklich ausführen wollen.
7. Starten Sie den Agenten neu.
   a. Klicken Sie im **Start**-Menü auf **Ausführen**.
   b. Geben Sie **cmd** ein und klicken Sie anschließend auf **OK**.
   c. Führen Sie in der Kommandozeile die nachfolgenden Befehle aus:

```
net stop mms
net start mms
```

Virtuelle Appliances

Diese Prozedur gilt für den Agenten für VMware (Virtuelle Appliance), den Agenten für Scale Computing, den Agenten für Virtuozzo Hybrid Infrastructure und den Agenten für oVirt.

1. Drücken Sie in der Konsole der virtuellen Appliance die Tastenkombination STRG+UMSCHALT+F2, um die Befehlszeilenschnittstelle zu öffnen.
2. Öffnen Sie die Datei `/etc/Acronis/MMS.config` in einem Text-Editor.
3. Suchen Sie den folgenden Abschnitt:

   ```
   <key name="SimultaneousBackupsLimits">
       <value name="MaxNumberOfSimultaneousBackups" type="Tdword">"10"</value>
   </key>
   ```

4. Ersetzen Sie die Zahl `10` durch die maximale Anzahl der gleichzeitigen Backups, die Sie festlegen wollen.
5. Speichern Sie die Datei.
6. Starten Sie den Agenten mit dem Befehlen `reboot` neu.

Migration von Maschinen

Sie können eine Maschine migrieren, wenn Sie ihr Backup zu einer anderen (also nicht der ursprünglichen) Maschine wiederherstellen.

Die nachfolgende Tabelle fasst alle verfügbaren Migrationsoptionen zusammen.

Maschinentyp im Backup	Verfügbare Recovery-Ziele							
	Physische Maschine	Virtuelle ESXi-Maschine	Virtuelle Hyper-V-Maschine	Virtuozzo		Virtuelle Virtuozzo Hybrid Infrastructure-Maschine	Virtuelle Scale Computing HC3-Maschine	Virtuelle RHV/oVirt-Maschine
				Virtuelle Maschine	Container			
Physische Maschine	+	+	+	-	-	+	+*	+
Virtuelle VMware ESXi-Maschine	+	+	+	-	-	+	+*	+
Virtuelle Hyper-V-Maschine	+	+	+	-	-	+	+*	+

Virtuelle Virtuozzo-Maschine	+	+	+	+	-	+	+*	+
Virtuozzo-Container	-	-	-	-	+	-	-	-
Virtuelle Virtuozzo Hybrid Infrastructure-Maschine	+	+	+	-	-	+	+*	+
Virtuelle Scale Computing HC3-Maschine	+	+	+	-	-	+	+	+
Virtuelle Red Hat Virtualization/oVirt-Maschine	+	+	+	-	-	+	+*	+

*Wenn auf der Quellmaschine die Secure Boot-Funktionalität aktiviert ist, kann die wiederhergestellte VM nicht starten, außer Sie deaktivieren die Secure Boot-Option nach der Wiederherstellung in der VM-Konsole.

Hinweis
Sie können keine virtuellen Maschinen mit macOS zu einem Hyper-V-Host wiederherstellen, weil macOS von Hyper-V nicht unterstützt wird. Sie können virtuelle Maschinen mit macOS zu einem VMware-Host wiederherstellen, wenn dieser auf Mac-Hardware installiert ist.

Weitere Informationen darüber, wie Sie die Migrationsaktionen durchführen können, finden Sie in den folgenden Abschnitten:

- Für Migrationen vom Typ 'physisch zu virtuell' (P2V) siehe Abschnitt '"Physische Maschinen als virtuelle Maschinen wiederherstellen" (S. 548)'.
- Für Migrationen vom Typ 'virtuell zu virtuell' (V2V) siehe Abschnitt '"Eine virtuelle Maschine wiederherstellenSie können virtuelle Maschinen aus deren Backups wiederherstellen.Bei Mandanten, die sich im Compliance-Modus befinden, können Sie keine Backups in der Cyber Protect-Konsole wiederherstellen. Weitere Informationen darüber, wie Sie solche Backups wiederherstellen können, finden Sie in Abschnitt "Backups für Mandanten im Compliance-Modus wiederherstellen" (S. 1).VoraussetzungenEine virtuelle Maschine, die als Recovery-Ziel dient, muss während der Wiederherstellung gestoppt werden. Standardmäßig stoppt die Software die

Maschine ohne weitere Nachfrage. Wenn die Wiederherstellung abgeschlossen wurde, müssen Sie die Maschine manuell wieder starten. Sie können dieses vorgegebene Verhalten mithilfe der Recovery-Option für die VM-Energieverwaltung ändern (klicken Sie dafür auf Recovery-Optionen –> VM-Energieverwaltung).VorgehensweiseGehen Sie nach einer der nachfolgenden Möglichkeiten vor:Wählen Sie eine zu sichernde Maschine, klicken Sie auf Recovery und wählen Sie dann einen Recovery-Punkt.Wählen Sie einen Recovery-Punkt auf der Registerkarte 'Backup Storage'.Klicken Sie auf Recovery –> Komplette Maschine.Wenn Sie die Wiederherstellung zu einer physischen Maschine durchführen wollen, wählen Sie bei Recovery zu das Element Physische Maschine. Ansonsten können Sie diesen Schritt überspringen.Eine Wiederherstellung auf einer physischen Maschine ist nur dann möglich, wenn die Laufwerkskonfiguration im Backup exakt mit der Laufwerkskonfiguration der Zielmaschine übereinstimmt.Falls dies zutrifft, fahren Sie mit Schritt 4 im Abschnitt 'Physische Maschine' fort. Falls dies nicht zutrifft, empfehlen wir Ihnen, eine V2P-Migration mithilfe eines Boot-Mediums durchzuführen.[Optional] Die Software wählt standardmäßig automatisch die ursprüngliche Maschine als Zielmaschine aus. Wenn Sie die Wiederherstellung auf eine andere virtuelle Maschine durchführen wollen, müssen Sie auf Zielmaschine klicken und dann Folgendes tun:Wählen Sie den Hypervisor (VMware ESXi, Hyper-V, Virtuozzo, Virtuozzo Hybrid Infrastructure, Scale Computing HC3 oder oVirt).Nur virtuelle Virtuozzo-Maschinen können zu Virtuozzo wiederhergestellt werden. Weiter Informationen zu V2V-Migrationen finden Sie im Abschnitt 'Migration von Maschinen'.Bestimmen Sie, ob eine neue oder eine vorhandene Maschine als Recovery-Ziel verwendet werden soll.Wählen Sie den Host und spezifizieren Sie einen Namen für die neue Maschine – oder wählen Sie eine bereits vorhandene Zielmaschine aus.Klicken Sie auf OK.Richten Sie die zusätzlichen Recovery-Optionen ein, die Sie benötigen.[Nicht für Virtuozzo Hybrid Infrastructure und Scale Computing HC3 verfügbar] Wenn Sie das Speicherziel für die virtuelle Maschine auswählen wollen, klicken Sie auf Datenspeicher für ESXi, Pfad für Hyper-V bzw. Virtuozzo oder Storage-Domain für Red Hat Virtualization (oVirt) – und bestimmten Sie dann den Datenspeicher (Storage) für die virtuelle Maschine.Klicken Sie auf Laufwerkszuordnung, um den Datenspeicher (Storage), die Schnittstelle und den Provisioning-Modus für jedes virtuelle Laufwerk einzusehen. Sie können diese Einstellungen ändern, außer Sie stellen einen Virtuozzo-Container oder eine virtuelle Maschine für Virtuozzo Hybrid Infrastructure wieder her.Für Virtuozzo Hybrid Infrastructure können Sie nur die Storage-Richtlinie für die Ziellaufwerke auswählen. Wählen Sie dafür das gewünschte Ziellaufwerk aus und klicken Sie dann auf Ändern. Klicken Sie in dem sich öffnenden Blatt auf das Zahnradsymbol, wählen Sie die Storage-Richtlinie aus und klicken Sie dann Fertig.Der Zuordnungsbereich ermöglicht Ihnen außerdem, bestimmte Laufwerke für die Wiederherstellung auszuwählen.[Für VMware ESXi, Hyper-V und Virtuozzo verfügbar] Klicken Sie auf VM-Einstellungen, um die Größe des Arbeitsspeichers, die Anzahl der Prozessoren und die Netzwerkverbindungen für die virtuelle Maschine zu ändern.[Für Virtuozzo Hybrid Infrastructure] Wählen Sie Variante, um die Speichergröße sowie die Anzahl der Prozessoren der virtuellen Maschine zu ändern.[Nur für Windows-Maschinen verfügbar, auf denen ein Protection Agent installiert ist] Aktivieren Sie den Schalter Safe Recovery, um sicherzustellen, dass die wiederhergestellten Daten frei von Malware sind. Weitere Informationen darüber, wie Safe Recovery funktioniert, finden Sie im Abschnitt '"Safe Recovery" (S. 1)'.Klicken Sie auf Recovery starten.Wenn Sie eine vorhandene virtuelle Maschine als Recovery-Ziel verwenden, müssen Sie

noch bestätigen, dass deren Laufwerke überschrieben werden.Der Recovery-Fortschritt wird auf der Registerkarte Aktivitäten angezeigt." (S. 1)'.

- Für Migrationen vom Typ 'virtuell zu physisch' (V2P) siehe die Abschnitte '"Eine virtuelle Maschine wiederherstellenSie können virtuelle Maschinen aus deren Backups wiederherstellen.Bei Mandanten, die sich im Compliance-Modus befinden, können Sie keine Backups in der Cyber Protect-Konsole wiederherstellen. Weitere Informationen darüber, wie Sie solche Backups wiederherstellen können, finden Sie in Abschnitt "Backups für Mandanten im Compliance-Modus wiederherstellen" (S. 1).VoraussetzungenEine virtuelle Maschine, die als Recovery-Ziel dient, muss während der Wiederherstellung gestoppt werden. Standardmäßig stoppt die Software die Maschine ohne weitere Nachfrage. Wenn die Wiederherstellung abgeschlossen wurde, müssen Sie die Maschine manuell wieder starten. Sie können dieses vorgegebene Verhalten mithilfe der Recovery-Option für die VM-Energieverwaltung ändern (klicken Sie dafür auf Recovery-Optionen –> VM-Energieverwaltung).VorgehensweiseGehen Sie nach einer der nachfolgenden Möglichkeiten vor:Wählen Sie eine zu sichernde Maschine, klicken Sie auf Recovery und wählen Sie dann einen Recovery-Punkt.Wählen Sie einen Recovery-Punkt auf der Registerkarte 'Backup Storage'.Klicken Sie auf Recovery –> Komplette Maschine.Wenn Sie die Wiederherstellung zu einer physischen Maschine durchführen wollen, wählen Sie bei Recovery zu das Element Physische Maschine. Ansonsten können Sie diesen Schritt überspringen.Eine Wiederherstellung auf einer physischen Maschine ist nur dann möglich, wenn die Laufwerkskonfiguration im Backup exakt mit der Laufwerkskonfiguration der Zielmaschine übereinstimmt.Falls dies zutrifft, fahren Sie mit Schritt 4 im Abschnitt 'Physische Maschine' fort. Falls dies nicht zutrifft, empfehlen wir Ihnen, eine V2P-Migration mithilfe eines Boot-Mediums durchzuführen.[Optional] Die Software wählt standardmäßig automatisch die ursprüngliche Maschine als Zielmaschine aus. Wenn Sie die Wiederherstellung auf eine andere virtuelle Maschine durchführen wollen, müssen Sie auf Zielmaschine klicken und dann Folgendes tun:Wählen Sie den Hypervisor (VMware ESXi, Hyper-V, Virtuozzo, Virtuozzo Hybrid Infrastructure, Scale Computing HC3 oder oVirt).Nur virtuelle Virtuozzo-Maschinen können zu Virtuozzo wiederhergestellt werden. Weiter Informationen zu V2V-Migrationen finden Sie im Abschnitt 'Migration von Maschinen'.Bestimmen Sie, ob eine neue oder eine vorhandene Maschine als Recovery-Ziel verwendet werden soll.Wählen Sie den Host und spezifizieren Sie einen Namen für die neue Maschine – oder wählen Sie eine bereits vorhandene Zielmaschine aus.Klicken Sie auf OK.Richten Sie die zusätzlichen Recovery-Optionen ein, die Sie benötigen.[Nicht für Virtuozzo Hybrid Infrastructure und Scale Computing HC3 verfügbar] Wenn Sie das Speicherziel für die virtuelle Maschine auswählen wollen, klicken Sie auf Datenspeicher für ESXi, Pfad für Hyper-V bzw. Virtuozzo oder Storage-Domain für Red Hat Virtualization (oVirt) – und bestimmten Sie dann den Datenspeicher (Storage) für die virtuelle Maschine.Klicken Sie auf Laufwerkszuordnung, um den Datenspeicher (Storage), die Schnittstelle und den Provisioning-Modus für jedes virtuelle Laufwerk einzusehen. Sie können diese Einstellungen ändern, außer Sie stellen einen Virtuozzo-Container oder eine virtuelle Maschine für Virtuozzo Hybrid Infrastructure wieder her.Für Virtuozzo Hybrid Infrastructure können Sie nur die Storage-Richtlinie für die Ziellaufwerke auswählen. Wählen Sie dafür das gewünschte Ziellaufwerk aus und klicken Sie dann auf Ändern. Klicken Sie in dem sich öffnenden Blatt auf das Zahnradsymbol, wählen Sie die Storage-Richtlinie aus und klicken Sie dann Fertig.Der Zuordnungsbereich ermöglicht Ihnen außerdem, bestimmte Laufwerke für die Wiederherstellung

auszuwählen.[Für VMware ESXi, Hyper-V und Virtuozzo verfügbar] Klicken Sie auf VM-Einstellungen, um die Größe des Arbeitsspeichers, die Anzahl der Prozessoren und die Netzwerkverbindungen für die virtuelle Maschine zu ändern.[Für Virtuozzo Hybrid Infrastructure] Wählen Sie Variante, um die Speichergröße sowie die Anzahl der Prozessoren der virtuellen Maschine zu ändern.[Nur für Windows-Maschinen verfügbar, auf denen ein Protection Agent installiert ist] Aktivieren Sie den Schalter Safe Recovery, um sicherzustellen, dass die wiederhergestellten Daten frei von Malware sind. Weitere Informationen darüber, wie Safe Recovery funktioniert, finden Sie im Abschnitt '"Safe Recovery" (S. 1)'.Klicken Sie auf Recovery starten.Wenn Sie eine vorhandene virtuelle Maschine als Recovery-Ziel verwenden, müssen Sie noch bestätigen, dass deren Laufwerke überschrieben werden.Der Recovery-Fortschritt wird auf der Registerkarte Aktivitäten angezeigt." (S. 1)' und '"Laufwerke mithilfe eines Boot-Mediums wiederherstellen" (S. 554)'

Migration über ein Boot-Medium

Alternativ zur Maschinen-Migration, die Sie über die Cyber Protect-Konsole durchführen, können Sie eine Maschine auch mithilfe eines Boot-Mediums wiederherstellen.

Wir empfehlen, dass Sie für folgende Szenarien ein Boot-Medium verwenden:

- Um eine Migration durchzuführen, die nicht standardmäßig unterstützt wird.
  Verwenden Sie beispielsweise ein Boot-Medium, um eine physische Maschine oder eine virtuelle Maschine, die keine Virtuozzo-Maschine ist, als virtuelle Virtuozzo-Maschine auf einem Virtuozzo-Host wiederherzustellen.
- Um eine Linux-Maschine zu migrieren, die logische Volumes (LVM) enthält.
  Verwenden Sie den Agenten für Linux oder ein Boot-Medium, um das entsprechende Backup zu erstellen – und verwenden Sie dann ein Boot-Medium, um das Backup wiederherzustellen.
- Um Treiber für bestimmte Hardware bereitzustellen, die für die Bootfähigkeit des Systems notwendig sind.
  Erstellen Sie ein Boot-Medium, das die erforderlichen Treiber verwenden kann. Weitere Informationen finden Sie im Abschnitt '"Bootable Media Builder" (S. 779)'.

Virtuelle Microsoft Azure- und Amazon EC2-Maschinen

Um eine virtuelle Microsoft Azure- oder Amazon EC2-Maschine sichern zu können, müssen Sie einen Protection Agenten auf der entsprechenden Maschine installieren. Backup- und Recovery-Aktionen werden hier genauso wie bei physischen Maschinen durchgeführt. Davon unabhängig wird die Maschine jedoch als virtuelle Maschine gezählt, wenn Sie Quotas für eine bestimmte Anzahl von Maschinen festlegen.

Der Unterschied zu einer physischen Maschine ist, dass virtuelle Microsoft Azure- und Amazon EC2-Maschinen nicht mit einem Boot-Medium gebootet werden können. Wenn Sie bei einer Wiederherstellung eine neue virtuelle Microsoft Azure- und Amazon EC2-Maschine als Ziel verwenden wollen, gehen Sie wie nachfolgend beschrieben vor.

Hinweis
Die folgende Recovery-Prozedur gilt nur für Backups von Maschinen, die alle notwendigen Treiber enthalten, um nativ in Microsoft Azure zu laufen (Backups, die von einer Azure-VM, einer lokalen Hyper-V-Maschine oder einem Windows Server 2016 und höher erstellt wurden). Für Plattform-übergreifende Wiederherstellungen können Sie sich in diesem Knowledge Base-Artikel informieren.

So können Sie eine Maschine als virtuelle Microsoft Azure- oder Amazon EC2-Maschine wiederherstellen

1. Erstellen Sie in Microsoft Azure oder Amazon EC2 eine neue virtuelle Maschine von einem Image/Template. Die neue Maschine muss dieselbe Laufwerkskonfiguration wie die Maschine haben, die Sie wiederherstellen wollen.
2. Installieren Sie den Agenten für Windows oder den Agenten für Linux auf der neuen Maschine.
3. Stellen Sie die Maschine aus dem Backup nach der Anleitung im Abschnitt 'Physische Maschine' wieder her. Wählen Sie die neue Maschine als Zielmaschine aus, wenn Sie die Wiederherstellung konfigurieren.

Ein Boot-Medium zur Wiederherstellung von Betriebssystemen erstellen

Ein Boot-Medium ist ein physisches Medium (CD, DVD, USB-Stick oder ein vergleichbares Wechselmedium), mit dem Sie den Protection Agenten in einer Linux-basierten Umgebung oder einer WinPE-/WinRE-basierten Umgebung (Windows Preinstallation Environment/Windows Recovery Environment) auszuführen können, damit er auch ohne die Hilfe eines bereits vorhandenen Betriebssystems laufen kann. Der Haupteinsatzzweck eines solchen Boot-Mediums besteht in der Möglichkeit, eine Maschine wiederherstellen zu können, die nicht mehr selbst starten (booten) kann.

Hinweis
Das Boot-Medium unterstützt keine Hybrid-Laufwerke.

Ein benutzerdefiniertes oder ein vorgefertigtes Boot-Medium?

Sie können mit dem Bootable Media Builder Ihre eigenen benutzerdefinierten Boot-Medien (Linux- oder WinPE-basiert) für Windows-, Linux- oder macOS-Computer erstellen. Bei Linux- und WinPE-/WinRE-basierten benutzerdefinierten Boot-Medien können Sie zusätzliche Einstellungen konfigurieren – wie etwa eine automatische Registrierung sowie Netzwerk- oder Proxy-Server-Einstellungen. Außerdem können Sie bei den WinPE-/WinRE-basierten benutzerdefinierten Boot-Medien auch noch zusätzliche Treiber hinzufügen.

Sie können alternativ auch ein vorgefertigtes Boot-Medium herunterladen (nur auf Linux-basiert). Sie können das vorgefertigtes Boot-Medium für Wiederherstellungsaktionen verwenden und um die Universal Restore-Funktionalität zu nutzen.

Linux-basiertes oder WinPE-/WinRE-basiertes Boot-Medium?

Linux-basiert

Ein Linux-basiertes Boot-Medium enthält einen Protection Agenten, der auf einem Linux-Kernel beruht. Der Agent kann auf jeder PC-kompatiblen Hardware booten und dort Aktionen ausführen, einschließlich auf fabrikneuer Hardware und Maschinen mit einem beschädigten oder nicht unterstützten Dateisystem.

WinPE-/WinRE-basiert

Ein WinPE-basierte Boot-Medium enthält ein funktionsreduziertes Windows-System, welches WinPE (für Windows Preinstallation Environment) genannt wird, sowie ein Cyber Protection-Plug-in für dieses WinPE-Medium. Bei diesem Plug-in handelt es sich um eine speziell angepasste Variante des Protection Agenten, damit dieser unter WinPE laufen kann. Ein WinRE-basiertes Boot-Medium verwendet die Windows-Wiederherstellungsumgebung (Windows Recovery Environment) und erfordert keine Installation von irgendwelchen zusätzlichen Windows-Paketen.

WinPE hat sich gerade bei großen IT-Umgebungen mit unterschiedlicher Hardware als sehr praktische bootfähige Lösung erwiesen.

Vorteile:

- Die Verwendung von Cyber Protection für ein WinPE-Medium bietet mehr Funktionalität als die Verwendung Linux-basierter Boot-Medien. Wenn Sie Ihre PC-kompatible Hardware mit einem WinPE-Medium booten, können Sie nicht nur den Protection Agenten ausführen, sondern auch spezielle WinPE-Befehle, Skripte und andere Plug-ins, die Sie in das WinPE-Medium eingebunden haben.
- Boot-Medien auf PE-Basis helfen, Linux-bezogene Probleme zu umgehen, z.B. fehlende Unterstützung für RAID-Controller oder gewisse RAID-Level. Auf WinPE 2.x (und höher) basierende Medien ermöglichen es, benötigte Gerätetreiber dynamisch zu laden.

Beschränkungen:

- Boot-Medien, die auf WinPE vor Version 4.0 basieren, können keine Maschinen booten, die UEFI (Unified Extensible Firmware Interface) verwenden.

Ein physisches Boot-Medium erstellen

Wir empfehlen dringend, dass Sie ein Boot-Medium erstellen und dieses testen, sobald Sie das erste Mal ein Backup auf Laufwerksebene erstellt haben. Es hat sich außerdem bewährt, nach jedem größeren Update des Protection Agenten auch ein neues Medium zu erstellen.

Zur Wiederherstellung von Windows oder Linux können Sie dasselbe Medium verwenden. Um macOS wiederherstellen zu können, müssen Sie ein separates Medium auf einer Maschine erstellen, die unter macOS läuft.

So können Sie ein physisches Boot-Medium unter Windows oder Linux erstellen

1. Erstellen Sie ein benutzerdefiniertes Boot-Medium als ISO-Datei oder laden Sie die vorgefertigte ISO-Datei herunter.

   Informationen zur Erstellung einer benutzerdefinierten ISO-Datei finden Sie im Abschnitt '"Bootable Media Builder" (S. 779)'.

   Wählen Sie zum Herunterladen der vorgefertigten ISO-Datei in der Cyber Protect-Konsole eine Maschine aus – und klicken Sie dann auf **Wiederherstellen** –> **Weitere Wiederherstellungsmöglichkeiten...** > **Laden Sie das ISO-Image herunter**.
2. [Optional] Generieren Sie in der Cyber Protect-Konsole ein Registrierungstoken. Der Registrierungstoken wird automatisch angezeigt, wenn Sie eine vorgefertigte ISO-Datei herunterladen.

   Mithilfe dieses Tokens kann das Boot-Medium auf den Cloud Storage zugreifen, ohne dass Sie zur Eingabe von Anmeldendaten (Benutzername, Kennwort) aufgefordert werden.
3. Sie können ein physisches Boot-Medium auf eine der folgenden Arten erstellen:
   - Brennen Sie die ISO-Datei auf eine CD/DVD.
   - Erstellen Sie einen bootfähigen USB-Stick mit der ISO-Datei. Um einen USB-Stick grundsätzlich bootfähig zu machen, können Sie eines (von vielen) kostenlos im Internet verfügbaren Freeware-Tools verwenden.

     Verwenden Sie beispielsweise `ISO to USB` oder `RUFUS`, falls Sie eine UEFI-Maschine booten wollen – oder `Win32DiskImager`, wenn Sie eine BIOS-Maschine haben. Unter Linux können Sie das Utility `dd` verwenden.

   Bei virtuellen Maschinen können Sie die ISO-Datei als virtuelles CD-/DVD-Laufwerk an die Maschine anschließen, die Sie wiederherstellen wollen.

So können Sie ein physisches Boot-Medium unter macOS erstellen

1. Klicken Sie auf einer Maschine, auf welcher der Agent für Mac installiert ist, im Menü **Applikationen** auf den Eintrag **Rescue Media Builder**.
2. Die Software zeigt Ihnen die angeschlossenen Wechsellaufwerke/Wechselmedien an. Wählen Sie dasjenige aus, welches Sie bootfähig machen wollen.

   Warnung!
   Alle Daten auf dem Laufwerk werden gelöscht.
3. Klicken Sie auf **Erstellen**.
4. Warten Sie, bis die Software das Boot-Medium erstellt hat.

Bootable Media Builder

Der Bootable Media Builder ist ein spezielles Werkzeug zur Erstellung eines Boot-Mediums. Er wird als optionale Komponente auf derjenigen Maschine installiert, auf welcher der Protection Agent installiert ist.

Warum sollten Sie den Bootable Media Builder verwenden?

Das vorgefertigte Boot-Medium, das in der Cyber Protect-Konsole zum Download bereitgestellt wird, basiert auf einem Linux-Kernel. Anders als Windows PE ist es hier nicht möglich, eigene benutzerdefinierte Treiber in das Medium mit zu integrieren.

Mit dem Bootable Media Builder können Sie benutzerdefinierte Images von Linux- und WinPE-basierten Boot-Medien erstellen.

32 Bit oder 64 Bit?

Der Bootable Media Builder kann Boot-Medien mit 32-Bit- und 64-Bit-Komponenten erstellen. Um eine Maschinen zu booten, die ein modernes UEFI (Unified Extensible Firmware Interface) verwendet, benötigen Sie normalerweise ein 64-Bit-Boot-Medium.

Linux-basiertes Boot-Medium

So können Sie ein Boot-Medium erstellen, das auf Linux basiert

1. Starten Sie den **Bootable Media Builder**.
2. Wählen Sie bei **Typ des Boot-Mediums** die Option **Standard (Linux-basiertes Medium)**.
3. Bestimmen Sie, wie die Volumes und Netzwerkressourcen angezeigt werden sollen:
   - Bei einem Boot-Medium mit Linux-typischer Volume-Darstellung werden die Volumes beispielsweise als hda1 und sdb2 angezeigt. Das Medium versucht, MD-Geräte und logische Volumes (vom LVM verwaltet) vor Start einer Wiederherstellung zu rekonstruieren.
   - Bei einem Boot-Medium mit Windows-typischer Volumes-Darstellung werden die Volumes durch Laufwerksbuchstaben repräsentiert – beispielsweise Laufwerk 'C:' und 'D:'. Das Medium ermöglicht auch Zugriffe auf dynamische Volumes (LDM verwaltet).
4. [Optional] Sie können Parameter für den Linux-Kernel spezifizieren. Wenn Sie mehrere Parameter eingeben wollen, trennen Sie diese per Leerzeichen.

   Geben Sie beispielsweise Folgendes ein, wenn Sie beim Starten des Mediums einen bestimmten Anzeigemodus für eine bootfähigen Agenten auswählen wollen: **vga=ask**. Weitere Informationen über die verfügbaren Parameter finden Sie im Abschnitt '"Kernel-Parameter" (S. 781)'.
5. [Optional] Wählen Sie die Sprache für das Boot-Medium aus.
6. [Optional] Bestimmen Sie den Boot-Modus (BIOS oder UEFI), den Windows nach der Wiederherstellung verwenden wird.
7. Bestimmen Sie die Komponente, die auf dem Medium gespeichert werden soll – der Cyber Protection Bootable Agent
8. [Optional] Spezifizieren Sie das Timeout-Intervall für das Boot-Menü. Wenn diese Einstellung nicht konfiguriert wird, wartet der Loader des Boot-Mediums darauf, dass Sie auswählen, ob das Betriebssystem (sofern vorhanden) oder eine entsprechende Komponente gestartet werden soll.

9. [Optional] Wenn Sie die Aktionen des bootfähigen Agenten automatisieren wollen, aktivieren Sie das Kontrollkästchen **Folgendes Skript verwenden**. Wählen Sie dann eines der Skripte aus und spezifizieren Sie die Skript-Parameter. Weitere Informationen über die Skripte finden Sie im Abschnitt '"Skripte in Boot-Medien" (S. 783)'.
10. [Optional] Bestimmen Sie, wie das Boot-Medium beim Booten im Cyber Protection Service registriert werden soll. Weitere Informationen über die Registrierungseinstellungen finden Sie im Abschnitt '"Das Boot-Medium registrieren" (S. 793)'.
11. Spezifizieren Sie die Netzwerkeinstellungen für die Netzwerkadapter der gebooteten Maschine oder übernehmen Sie die automatische DHCP-Konfiguration.
12. [Optional] Falls in Ihrem Netzwerk ein Proxy-Server aktiv ist, spezifizieren Sie dessen Host-Namen/IP-Adresse und Port.
13. Bestimmen Sie den Dateityp des erstellten Boot-Mediums:
    - ISO-Image
    - ZIP-Datei
14. Spezifizieren Sie einen Dateinamen für die Datei des Boot-Mediums.
15. Überprüfen Sie Ihre Einstellungen im Fenster 'Zusammenfassung' und klicken Sie dann auf **Forsetzen**.

Kernel-Parameter

Sie können einen oder mehrere Parameter für den Linux-Kernel spezifizieren, die beim Start des Boot-Mediums automatisch angewendet werden. Diese Parameter werden in der Regel dann eingesetzt, wenn beim Arbeiten mit dem Boot-Medium Probleme auftreten. Normalerweise brauchen Sie in dieses Feld nichts einzutragen.

Sie können diese Parameter auch dann spezifizieren, wenn Sie die Taste 'F11' drücken, während Sie sich im Boot-Menü befinden.

Parameter

Trennen Sie mehrere Parameter mit Leerzeichen.

- **acpi=off**
  Deaktiviert ACPI (Advanced Configuration and Power Interface). Dieser Parameter kann hilfreich sein, wenn bei einer bestimmten Hardware-Konfiguration Probleme auftauchen.
- **noapic**
  Deaktiviert APIC (Advanced Programmable Interrupt Controller). Dieser Parameter kann hilfreich sein, wenn bei einer bestimmten Hardware-Konfiguration Probleme auftauchen.
- **vga=ask**
  Erfragt den Grafikkartenmodus, der in der grafischen Benutzeroberfläche eines Boot-Mediums verwendet werden soll. Ist kein **vga**-Parameter angegeben, wird der Videomodus automatisch erkannt.
- **vga=** *mode_number*

Spezifiziert den Grafikkartenmodus, der in der grafischen Benutzeroberfläche des Boot-Mediums verwendet werden soll. Die Modus-Nummer wird unter *mode_number* im Hexadezimalformat angegeben, z.B.: **vga=0x318**

Die Bildschirmauflösung und die Anzahl der Farben für eine Modus-Nummer können sich von Maschine zu Maschine unterscheiden. Wir empfehlen, dass Sie zuerst den Parameter **vga=ask** zu verwenden, um einen Wert für *mode_number* festzulegen.

- **quiet**

  Deaktiviert die Anzeige von Pop-up-Meldungen während der Linux-Kernel geladen wird und startet danach die Management Konsole.

  Dieser Parameter wird implizit spezifiziert, wenn das Boot-Medium erstellt wird. Sie können diesen Parameter jedoch wieder entfernen, solange Sie sich im Boot-Menü befinden.

  Wenn dieser Parameter entfernt wird, werden alle Meldungen beim Start angezeigt – gefolgt von einer Eingabeaufforderung. Geben Sie bei der Eingabeaufforderung folgenden Befehl ein, um die Management Konsole zu starten: **/bin/product**
- **nousb**

  Deaktiviert, dass das USB-Subsystem geladen wird.
- **nousb2**

  Deaktiviert die USB 2.0-Unterstützung. USB 1.1-Geräte arbeiten, auch wenn dieser Parameter gesetzt ist. Mit dem Parameter können Sie manche USB-Laufwerke im USB 1.1-Modus verwenden, wenn sie im USB 2.0-Modus nicht arbeiten.
- **nodma**

  Deaktiviert den Speicherdirektzugriff (DMA) für alle IDE-Festplatten. Verhindert auf mancher Hardware ein Einfrieren des Kernels.
- **nofw**

  Deaktiviert die Unterstützung für die FireWire (IEEE1394)-Schnittstelle.
- **nopcmcia**

  Deaktiviert die Erkennung von PCMCIA-Hardware.
- **nomouse**

  Deaktiviert die Maus-Unterstützung.
- *module_name* **=off**

  Deaktiviert das Modul, dessen Name in *module_name* angeben ist. Um beispielsweise die Nutzung des SATA-Moduls zu deaktivieren, geben Sie folgenden Wert an: **sata_sis=off**
- **pci=bios**

  Erzwingt die Verwendung des PCI-BIOS statt direkt auf die Hardware-Geräte zuzugreifen. Dieser Parameter kann hilfreich sein, z.B. wenn die Maschine eine nicht standardgemäße PCI Host-Bridge hat.
- **pci=nobios**

  Deaktiviert die Verwendung des PCI BIOS und erlaubt nur direkte Hardware-Zugriffsmethoden. Dieser Parameter kann z.B. hilfreich sein, wenn das Boot-Medium nicht startet und dies wahrscheinlich durch das BIOS verursacht wird.
- **pci=biosirq**

Verwendet PCI BIOS-Aufrufe, um die Interrupt Routing-Tabelle zu erhalten. Dieser Parameter kann hilfreich sein, wenn es dem Kernel nicht gelingt, Unterbrechungsanforderungen (IRQs) zuzuordnen oder den sekundären PCI-Bus auf dem Mainboard zu finden.

Auf einigen Maschinen funktionieren diese Aufrufe möglicherweise nicht richtig. Es kann unter Umständen aber der einzige Weg sein, die Interrupt Routing-Tabelle anzuzeigen.

- **LAYOUTS=en-US, de-DE, fr-FR, ...**

  Spezifiziert das Tastaturlayout, das in der grafischen Benutzeroberfläche des Boot-Mediums verwendet werden soll.

  Ohne diesen Parameter können nur zwei Layouts verwendet werden: Englisch (USA) und dasjenige Layout, welches der Sprache entspricht, die im Boot-Menü des Mediums ausgewählt wurde.

  Sie können jedes der folgenden Layouts verwenden:

  Belgisch **be-BE**

  Tschechisch: **cz-CZ**

  Englisch: **en-GB**

  Englisch (USA): **en-US**

  Französisch: **fr-FR**

  Französisch (Schweiz): **fr-CH**

  Deutsch: **de-DE**

  Deutsch (Schweiz): **de-CH**

  Italienisch: **it-IT**

  Polnisch: **pl-PL**

  Portugiesisch: **pt-PT**

  Portugiesisch (Brasilien): **pt-BR**

  Russisch: **ru-RU**

  Serbisch (Kyrillische Zeichen): **sr-CR**

  Serbisch (Lateinische Zeichen): **sr-LT**

  Spanisch: **es-ES**

  Wenn Sie unter einem Boot-Medium arbeiten, können Sie mit der Tastenkombination Strg+Umschalt durch die verfügbaren Layouts wechseln.

Skripte in Boot-Medien

Wenn Sie möchten, dass ein Boot-Medium eine vordefinierte Folge von Aktionen ausführt, können Sie beim Erstellen des Mediums mit dem Bootable Media Builder ein Skript definieren. Dadurch wird das spezifizierte Skript jedes Mal ausgeführt, wenn eine Maschine mit dem Medium gebootet wird – und die Benutzeroberfläche wird nicht angezeigt.

Sie können eines der vordefinierten Skripte auswählen oder ein benutzerdefiniertes Skript auf Grundlage der Skript-Konventionen erstellen.

Vordefinierte Skripte

Der Bootable Media Builder stellt folgende vordefinierte Skripte bereit:

- Recovery aus dem Cloud Storage (**entire_pc_cloud**)
- Recovery von einer Netzwerkfreigabe (**entire_pc_share**)

Die Skripte befinden sich in folgenden Speicherorten auf derjenigen Maschine, auf welcher der Bootable Media Builder installiert ist:

- Unter Windows: %**ProgramData%\Acronis\MediaBuilder\scripts**
- Unter Linux: **/var/lib/Acronis/MediaBuilder/scripts/**

Aus dem Cloud Storage wiederherstellen

Spezifizieren Sie im Bootable Media Builder folgende Skript-Parameter:

1. Der Backup-Dateiname.
2. [Optional] Ein Kennwort, welches das Skript verwendet, um auf verschlüsselte Backups zuzugreifen.

Recovery von einer Netzwerkfreigabe

Spezifizieren Sie im Bootable Media Builder folgende Skript-Parameter:

- Der Pfad zur Netzwerkfreigabe.
- Die Anmeldedaten (Benutzername, Kennwort) für die Netzwerkfreigabe.
- Der Backup-Dateiname. So können Sie den Namen einer Backup-Datei herausfinden:
  a. Gehen Sie in der Cyber Protect-Konsole zu **Backup Storage** –> **Speicherorte**.
  b. Wählen Sie die Netzwerkfreigabe aus (klicken Sie auf **Speicherort hinzufügen**, wenn die Freigabe noch nicht aufgeführt ist).
  c. Wählen Sie das Backup.
  d. Klicken Sie auf **Details**. Der Dateiname wird unter **Backup-Dateiname** angezeigt.
- [Optional] Ein Kennwort, welches das Skript verwendet, um auf verschlüsselte Backups zuzugreifen.

Benutzerdefinierte Skripts

Wichtig
Um benutzerdefinierte Skripte erstellen zu können, müssen Sie sich mit der Befehlssprache Bash und JSON (JavaScript Object Notation) auskennen. Falls Sie mit Bash nicht vertraut sind, ist 'http://www.tldp.org/LDP/abs/html' eine gute Adresse für den Einstieg. Die Spezifikationen für JSON finden Sie unter der Adresse 'http://www.json.org'.

Die Dateien eines Skripts

Ihr Skript muss sich auf der Maschine, auf welcher der Bootable Media Builder installiert ist, in folgenden Verzeichnissen befinden:

- Unter Windows: %**ProgramData%\Acronis\MediaBuilder\scripts**
- Unter Linux: **/var/lib/Acronis/MediaBuilder/scripts/**

Ein Skript muss aus mindestens drei Dateien bestehen:

- **<Skriptdatei>.sh** – eine Datei mit Ihrem Bash-Skript. Verwenden Sie beim Erstellen des Skripts nur einen begrenzten Satz von Shell-Befehlen, wie er unter der Adresse 'https://busybox.net/downloads/BusyBox.html' aufgeführt ist. Es können außerdem noch folgende Befehle verwendet werden:
  - `acrocmd` – das Befehlszeilenwerkzeug für Backup und Recovery
  - `product` – der Befehl, mit dem die Benutzeroberfläche des Boot-Mediums gestartet wird

  Diese Datei und alle weiteren Dateien, die das Skript einschließt (beispielsweise durch Verwendung des Befehls 'dot'), müssen im Unterordner **bin** gespeichert sein. Spezifizieren Sie die Pfade der weiteren Dateien im Skript in folgender Form: **/ConfigurationFiles/bin/<irgendeine_Datei>**.
- **autostart** – eine Datei zum Starten von **<Skriptdatei>.sh**. Die Dateiinhalte müssen folgendermaßen aussehen:

```
#!/bin/sh
. /ConfigurationFiles/bin/variables.sh
. /ConfigurationFiles/bin/<Skriptdatei>.sh
. /ConfigurationFiles/bin/post_actions.sh
```

- **autostart.json** – eine JSON-Datei mit folgenden Inhalten:
  - Der/die im Bootable Media Builder anzuzeigende Skript-Name/-Beschreibung.
  - Die Namen der Skript-Variablen, die über den Bootable Media Builder konfiguriert werden sollen.
  - Die Parameter der Steuerlemente, die im Bootable Media Builder für jede Variable angezeigt werden.

Die Struktur von 'autostart.json'

Top-Level-Objekt

Paar		Erforderlich	Beschreibung
Name	Wertetyp		

`displayName`	String	Ja	Der im Bootable Media Builder anzuzeigende Skriptname.
`description`	String	Nein	Die im Bootable Media Builder anzuzeigende Skriptbeschreibung.
`timeout`	Zahl	Nein	Eine Zeitverzögerung (in Sekunden) für das Boot-Menü, bevor das Skript gestartet wird. Falls das Paar nicht spezifiziert ist, gilt eine Zeitverzögerung von 10 Sekunden.
`variables`	Objekt	Nein	Jede Variable für **<Skriptdatei>.sh**, die Sie über den Bootable Media Builder konfigurieren wollen. Der Wert sollte ein Satz der folgenden Paare sein: der String-Identifier einer Variable und das Objekt der Variablen (vergl. untere Tabelle).

Variablenobjekt

Paar		Erforderlich	Beschreibung
Name	**Wertetyp**		
`displayName`	String	Ja	Der in **<Skriptdatei>.sh** verwendete Variablenname.
`type`	String	Ja	Der Typ eines Steuerelements, welches im Bootable Media Builder angezeigt wird. Dieses Steuerelement wird verwendet, um den Variablenwert zu konfigurieren. Eine Auflistung aller unterstützten Typen finden Sie in der unteren Tabelle.
`description`	String	Ja	Die Steuerelementbezeichnung, die im Bootable Media Builder über dem Steuerungselement angezeigt wird.
`default`	eine Zeichenfolge (String), falls `type` Folgendes ist: `string`, `multiString`, `password` oder `enum` eine Zahl, falls `type` Folgendes	Nein	Der Standardwert für das Steuerelement. Falls das Paar nicht spezifiziert ist, wird der Standardwert ein leerer String oder eine Null sein (abhängig vom Steuerelementtyp). Der Standardwert für ein Kontrollkästchen kann `0` (deaktivierter/abgewählter Zustand) oder `1` sein (aktivierter/ausgewählter Zustand).

	ist: `number`, `spinner` oder `checkbox`		
`order`	Zahl (nicht negativ)	Ja	Die Reihenfolge der Steuerelemente im Bootable Media Builder. Je höher der Wert ist, umso tiefer wird das Steuerelement relativ zu anderen in **autostart.json** definierten Steuerelementen platziert. Der Anfangswert muss `0` sein.
`min` (nur für `spinner`)	Zahl	Nein	Der kleinste Wert für das Drehsteuerelement in einem Drehfeld. Falls das Paar nicht spezifiziert ist, wird der Wert auf `0` gesetzt.
`max` (nur für `spinner`)	Zahl	Nein	Der größte Wert für das Drehsteuerelement in einem Drehfeld. Falls das Paar nicht spezifiziert ist, wird der Wert auf `100` gesetzt.
`step` (nur für `spinner`)	Zahl	Nein	Der Schrittwert (Inkrement) für das Drehsteuerelement in einem Drehfeld. Falls das Paar nicht spezifiziert ist, wird der Wert auf `1` gesetzt.
`items` (nur für `enum`)	Array von Strings	Ja	Eine Folge von Werten für ein Listenfeld (Drop-down-Liste).
`required` (für `string`, `multiString`, `password` und `enum`)	Zahl	Nein	Spezifiziert, ob der Steuerelementwert leer sein darf (`0`) oder nicht (`1`). Falls das Paar nicht spezifiziert ist, kann der Steuerelementwert leer sein.

Steuerelementtyp

Name	Beschreibung
`String`	Ein einzeiliges, nicht weiter beschränktes Textfeld, welches zur Eingabe oder Bearbeitung kurzer Zeichenfolgen (Strings) verwendet wird.
`multiString`	Ein mehrzeiliges, nicht weiter beschränktes Textfeld, welches zur Eingabe oder Bearbeitung längerer Zeichenfolgen (Strings) verwendet wird.
`password`	Ein einzeiliges, nicht weiter beschränktes Textfeld, welches zur sicheren Eingabe von Kennwörtern verwendet wird.
`Zahl`	Ein einzeiliges, nur Zahlen zulassendes Textfeld, welches zur Eingabe oder Bearbeitung von Nummern verwendet wird.

spinner	Ein einzeiliges, nur Zahlen zulassendes Textfeld, welches zur Eingabe oder Bearbeitung von Nummern mit einem Drehsteuerelement verwendet wird. Wird auch Drehfeld genannt.
enum	Ein Standardlistenfeld (Drop-Down-Liste), mit einem festen Satz von vordefinierten Werten.
checkbox	Ein Kontrollkästchen mit zwei Zuständen – deaktiviert (abgewählt) oder aktiviert (ausgewählt).

Die untere **autostart.json**-Beispielsdatei enthält alle verwendbaren Typen von Steuerelementen, die zur Konfiguration von Variablen für die Datei **<script_file>.sh** verwendet werden können.

```
{
        "displayName": "Name des Autostart-Skripts",
        "description": "Dies ist eine Beschreibung für das Autostart-Skript.",
        "variables": {
                "var_string": {
                        "displayName": "VAR_STRING",
                        "type": "string", "order": 1,
                        "description": "Dies ist ein 'string'-Kontrollfeld:", "default": "Hallo
Welt!"
                },
                "var_multistring": {
                        "displayName": "VAR_MULTISTRING",
                        "type": "multiString", "order": 2,
                        "description": "Dies ist ein 'multiString'-Kontrollfeld:",
                        "default": "Lorem ipsum dolor sit amet,\nconsectetur adipiscing elit."
                },
                "var_number": {
                        "displayName": "VAR_NUMBER",
                        "type": "number", "order": 3,
                        "description": "Dies ist ein 'number'-Kontrollfeld:", "default": 10
                },
                "var_spinner": {
                        "displayName": "VAR_SPINNER",
```

```
                "type": "spinner", "order": 4,
                "description": "Dies ist ein 'spinner'-Kontrollfeld:",
                "min": 1, "max": 10, "step": 1, "default": 5
        },
        "var_enum": {
                "displayName": "VAR_ENUM",
                "type": "enum", "order": 5,
                "description": "Dies ist ein 'enum'-Kontrollfeld:",
                "items": ["first", "second", "third"], "default": "second"
        },
        "var_password": {
                "displayName": "VAR_PASSWORD",
                "type": "password", "order": 6,
                "description": "Dies ist ein 'password'-Kontrollfeld:", "default":
"qwe"
        },
        "var_checkbox": {
                "displayName": "VAR_CHECKBOX",
                "type": "checkbox", "order": 7,
                "description": "Die ist ein 'checkbox'-Kontrollfeld", "default": 1
        }
    }
}
```

WinPE- und WinRE-basierte Boot-Medien

Sie können WinRE-Images ohne zusätzliche Vorbereitung erstellen – oder die WinPE-Images nach der Installation des Windows Automated Installation Kits (AIK) oder des Windows Assessment and Deployment Kits (ADK) erstellen.

WinRE-Images

Die Erstellung von WinRE-Images wird für folgende Betriebssysteme unterstützt:

- Windows 7 (64 Bit)
- Windows 8 (32 Bit und 64 Bit)
- Windows 8.1 (32 Bit und 64 Bit)
- Windows 10 (32 Bit und 64 Bit)
- Windows 11 (64 Bit)
- Windows Server 2012 (64 Bit)
- Windows Server 2016 (64 Bit)
- Windows Server 2019 (64 Bit)
- Windows Server 2022 (64 Bit)

WinPE-Images

Nach der Installation des Windows Automated Installation Kits (AIK) oder Windows Assessment and Deployment Kits (ADK) unterstützt der Bootable Media Builder solche WinPE-Distributionen, die auf einem der folgenden Kernel basieren:

- Windows Vista (PE 2.0)
- Windows Vista SP1 und Windows Server 2008 (PE 2.1).
- Windows 7 (PE 3.0), mit oder ohne das 'Supplement for Windows 7 SP1' (PE 3.1)
- Windows 8 (PE 4.0)
- Windows 8.1 (PE 5.0)
- Windows 10 (PE 10.0.1xxx)
- Windows 11 (PE 10.0.2xxx)

Bootable Media Builder unterstützt sowohl 32-Bit- wie auch 64-Bit-WinPE-Distributionen. Die 32-Bit-WinPE-Distributionen funktionieren auch auf 64-Bit-Hardware. Sie benötigen jedoch 64-Distributionen, um von einer Maschine booten zu können, die UEFI (Unified Extensible Firmware Interface) verwendet.

Hinweis
PE-Images, die auf WinPE 4 (und höher) basieren, benötigen zum Arbeiten ca. 1 GB RAM.

WinPE- oder WinRE-Boot-Medien erstellen

Der Bootable Media Builder ermöglicht zwei Methoden, um Cyber Protection in WinPE und WinRE einzubinden:

- Eine komplett neue ISO-Datei mit dem Cyber Protection-Plugin erstellen
- Das Cyber Protection-Plug-in einer WIM-Datei zur späteren Verwendung hinzufügen (manuelle ISO-Erstellung, dem Image noch andere Tools hinzufügen usw.).

So können Sie ein WinPE- oder WinRE-Boot-Medien erstellen

1. Führen Sie auf der Maschine, auf der der Protection Agent installiert ist, den Bootable Media Builder aus.
2. Wählen Sie bei **Typ des Boot-Mediums** entweder **Windows PE** oder **Windows PE (64 Bit)** aus. Sie benötigen ein 64-Bit-Medium, um eine Maschine booten zu können, die UEFI (Unified Extensible Firmware Interface) verwendet.
3. Wählen Sie den Subtyp des Boot-Mediums aus: **WinRE** oder **WinPE**.

   Zum Erstellen eines WinRE-Boot-Mediums müssen keine zusätzlichen Pakete installiert werden.

   Wenn Sie ein 64-Bit-WinPE-Medium erstellen wollen, müssen Sie das Windows Automated Installation Kit (AIK) oder das Windows Assessment and Deployment Kit (ADK) herunterladen.

   Wenn Sie ein 32-Bit-WinPE-Medium erstellen wollen, müssen Sie nicht nur das AIK oder ADK herunterladen, sondern zusätzlich noch Folgendes tun:

   a. Klicken Sie auf **Plug-in für WinPE (32 Bit) herunterladen**.

   b. Speichern Sie das Plug-in im Ordner **%PROGRAM_ FILES%\BackupClient\BootableComponents\WinPE32**.
4. [Optional] Wählen Sie die Sprache für das Boot-Medium aus.
5. [Optional] Bestimmen Sie den Boot-Modus (BIOS oder UEFI), den Windows nach der Wiederherstellung verwenden wird.
6. Spezifizieren Sie die Netzwerkeinstellungen für die Netzwerkadapter der gebooteten Maschine oder übernehmen Sie die automatische DHCP-Konfiguration.
7. [Optional] Bestimmen Sie, wie das Boot-Medium beim Booten im Cyber Protection Service registriert werden soll. Weitere Informationen über die Registrierungseinstellungen finden Sie im Abschnitt '"Das Boot-Medium registrieren" (S. 793)'.
8. [Optional] Spezifizieren Sie die Windows-Treiber, die dem Boot-Medium hinzugefügt werden sollen.

   Wenn Sie eine Maschine mit Windows PE oder Windows RE booten, ermöglichen Ihnen diese Treiber, auch auf spezielle Geräte zugreifen zu können, wo das Backup gespeichert ist. Verwenden Sie 32-Bit-Treiber, sofern Sie eine 32-Bit-Distribution von WinPE oder WinRE verwenden – oder 64-Bit-Treiber, sofern Sie eine entsprechende 64-Bit-Distribution einsetzen.

   So können Sie Treiber hinzufügen:

   - Klicken Sie auf **Hinzufügen** und spezifizieren Sie dann den Pfad zu der benötigten . inf-Datei (beispielsweise für einen SCSI-, RAID- oder SATA-Controller, eine Netzwerkkarte, ein Bandlaufwerk oder ein anderes Gerät).
   - Wiederholen Sie dieses Prozedur für jeden Treiber, den Sie in das resultierende WinPE- oder WinRE-Medium aufnehmen wollen.
9. Bestimmen Sie den Dateityp des erstellten Boot-Mediums:
   - ISO-Image
   - WIM-Image
10. Spezifizieren Sie den vollständigen Pfad (einschließlich Dateiname) für das resultierende Image.
11. Überprüfen Sie Ihre Einstellungen im Fenster 'Zusammenfassung' und klicken Sie dann auf **Forsetzen**.

So können Sie ein PE-Image (ISO-Datei) von der resultierenden WIM-Datei erstellen

- Überschreiben Sie die vorgegebene Datei 'boot.wim' (im Windows PE-Ordner) mit der neu erstellten .wim-Datei. Geben Sie (für das obere Beispiel) Folgendes ein:

```
copy c:\RecoveryWIMMedia.wim c:\winpe_x86\ISO\sources\boot.wim
```

- Verwenden Sie das Tool **Oscdimg**. Geben Sie (für das obere Beispiel) Folgendes ein:

```
oscdimg -n -bc:\winpe_x86\etfsboot.com c:\winpe_x86\ISO c:\winpe_x86\winpe_x86.iso
```

Warnung!
(Sie sollten dieses Beispiel nicht kopieren und einfügen. Geben Sie den Befehl stattdessen manuell ein, weil er sonst nicht funktioniert.)

Vorbereitung: WinPE 2.x und 3.x

Um PE 2.x oder 3.x-Images erstellen oder modifizieren zu können, installieren Sie den Bootable Media Builder auf einer Maschine, auf der das Windows Automated Installation Kit (AIK) installiert ist.

So können Sie eine Maschine vorbereiten

1. Laden Sie die AIK-Image-Datei von der Microsoft-Website wie folgt herunter:
   - Für Windows Vista (PE 2.0): https://www.microsoft.com/de-de/download/details.aspx?id=10333
   - Für Windows Vista SP1 und Windows Server 2008 (PE 2.1): https://www.microsoft.com/de-de/download/details.aspx?id=9085
   - Für Windows 7 (PE 3.0): https://www.microsoft.com/de-de/download/details.aspx?id=5753
     Für Windows 7 SP1 (PE 3.1) benötigen Sie außerdem das AIK-Supplement, das unter https://www.microsoft.com/en-us/download/details.aspx?id=5188 verfügbar ist.
2. Brennen Sie die Image-Datei auf eine DVD-Disk oder erstellen Sie damit einen bootfähigen USB-Stick.
3. Installieren Sie Folgendes aus der Image-Datei:
   - Microsoft .NET Framework (NETFXx86 oder NETFXx64, abhängig von Ihrer Hardware)
   - MSXML (Microsoft XML-Parser)
   - Windows AIK
4. Installieren Sie Bootable Media Builder auf der gleichen Maschine.

Vorbereitung: WinPE 4.0 (und höher)

Um Images von PE 4 (oder höher) erstellen oder ändern zu können, installieren Sie den Bootable Media Builder auf einer Maschine, auf der das Windows Assessment and Deployment Kit (ADK) installiert ist.

So können Sie eine Maschine vorbereiten

1. Laden Sie das ADK-Setup-Programm von der Microsoft-Website herunter.
   Folgende Windows-Versionen werden unterstützt:
   - Windows 11 (PE 10.0.2xxx)
   - Windows 10 (PE 10.0.1xxx)
   - Windows 8.1 (PE 5.0)
   - Windows 8 (PE 4.0)
2. Installieren Sie das Assessment and Deployment Kit.
3. Installieren Sie den Bootable Media Builder.

Das Boot-Medium registrieren

Die Registrierung des Boot-Mediums im Cyber Protection Service ermöglicht Ihnen, auf den Cloud Storage für Ihre Backups zuzugreifen. Sie können die Registrierung beim Erstellen des Boot-Mediums vorkonfigurieren. Wenn die Registrierung nicht vorkonfiguriert wurde, können Sie das Medium registrieren, nachdem Sie eine Maschine damit gebootet haben.

So können Sie die Registrierung im Cyber Protection Service vorkonfigurieren

1. Gehen Sie im Bootable Media Builder zum Punkt **Boot-Medium-Registrierung**.
2. Spezifizieren Sie bei **Service-URL** die Adresse des Cyber Protection Service.
3. [Optional] Spezifizieren Sie bei **Anzeigename** einen Namen für die gebootete Maschine.
4. Wenn Sie die automatische Registrierung im Cyber Protection Service festlegen wollen, müssen Sie das Kontrollkästchen **Das Boot-Medium automatisch registrieren** aktivieren und dann die Stufe der automatischen Registrierung auswählen:
   - **Beim Booten nach dem Registrierungstoken fragen**
     Das Token muss jedes Mal bereitgestellt werden, wenn eine Maschine mit diesem Boot-Medium gestartet wird.
   - **Das folgende Token verwenden**
     Die Maschine wird automatisch registriert, wenn sie mit diesem Boot-Medium gestartet wird.

So können Sie das Boot-Medium registrieren, nachdem Sie eine Maschine damit gebootet haben

1. Booten Sie die Maschine mithilfe eines Boot-Mediums.
2. Klicken Sie im Startfenster auf **Medium registrieren**.
3. Spezifizieren Sie bei **Server** die Adresse des Cyber Protection Service.
4. Geben Sie bei **Registrierungstoken** das Registrierungstoken ein.
5. Klicken Sie auf **Registrieren**.

Netzwerkeinstellungen

Sie erhalten während der Erstellung eines Boot-Mediums die Möglichkeit, die Netzwerkverbindungen vorzukonfigurieren, die vom bootfähigen Agenten verwendet werden.

Folgende Parameter können vorkonfiguriert werden:

- IP-Adresse
- Subnetzmaske
- Gateway
- DNS-Server
- WINS-Server

Wenn der bootfähige Agent auf einer Maschine gestartet wurde, wird die Konfiguration auf die Netzwerkkarte (NIC) der Maschine angewendet. Wenn keine Einstellungen vorkonfiguriert wurden, wird der Agent die DHCP-Autokonfiguration verwenden.

Sie können die Netzwerkeinstellungen auch manuell konfigurieren, wenn der bootfähige Agent auf der Maschine ausgeführt wird.

Mehrere Netzwerkverbindungen vorkonfigurieren

Sie können die TCP/IP-Einstellungen für bis zu zehn Netzwerkkarten (NICs) vorkonfigurieren. Um sicherzustellen, dass jede NIC die passenden Einstellungen bekommt, sollten Sie das Medium auf dem Server erstellen, für den das Medium konfiguriert wird. Wenn Sie im Assistentenfenster eine vorhandene NIC auswählen, werden deren Einstellungen ausgewählt und auf dem Medium gespeichert. Die MAC-Adresse jeder existierenden NIC wird ebenso auf dem Medium gespeichert.

Sie können die Einstellungen (mit Ausnahme der MAC-Adresse) ändern oder die Einstellungen für eine nicht existierende NIC konfigurieren.

Wenn der bootfähige Agent auf dem Server gestartet wurde, fragt er die Liste der verfügbaren NICs ab. Diese Liste ist nach den Steckplätzen sortiert, die von den NICs belegt werden. Dabei steht der Steckplatz, der dem Prozessor am nächsten liegt, an erster Stelle.

Der bootfähige Agent teilt jeder bekannten NIC die passenden Einstellungen zu, wobei die NICs anhand ihrer MAC-Adressen identifiziert werden. Nachdem die NICs mit bekannten MAC-Adressen konfiguriert wurden, bekommen die verbliebenen NICs (beginnend mit der untersten in der Liste) die Einstellungen zugewiesen, die Sie für unbekannte NICs vorkonfiguriert haben.

Sie können das Boot-Medium für jede beliebige Maschine konfigurieren – und nicht nur für die Maschine, auf der das Medium erstellt wurde. Um dies durchzuführen, konfigurieren Sie die NICs entsprechend ihrer Steckplatzreihenfolge in der betreffenden Maschine. NIC1 besetzt den zum Prozessor am nächsten liegenden Steckplatz, NIC2 wiederum den folgenden und so weiter. Wenn der bootfähige Agent auf dieser Maschine startet, wird er die NICs mit bekannten MAC-Adressen nicht finden und daher die NICs in der von Ihnen bestimmten Reihenfolge konfigurieren.

Beispiel

Der bootfähige Agent kann einen der Netzwerkadapter zur Kommunikation mit der Management-Konsole innerhalb des Produktionsnetzwerks nutzen. Für diese Verbindung kann eine automatische Konfiguration durchgeführt werden. Größere Datenmengen für eine Wiederherstellung können

über die zweite NIC übertragen werden, die in das dafür bestimmte Backup-Netzwerk mithilfe statischer TCP/IP-Einstellungen eingebunden ist.

Eine Verbindung mit einer Maschine aufbauen, die per Boot-Medium gestartet wurde

Lokale Verbindung

Um direkt auf einer Maschine arbeiten zu können, die mit einem Boot-Medium gestartet wurde, müssen Sie im Startfenster auf **Diese Maschine lokal verwalten** klicken.

Wenn eine Maschine mithilfe eines Boot-Medium gestartet wurde, erscheint ein Konsolenfenster mit den IP-Adressen, die per DHCP oder als manuell vorkonfigurierte Werte zugewiesen wurden.

Netzwerkeinstellungen konfigurieren

Klicken Sie zum Ändern der Netzwerkeinstellungen für eine aktuelle Sitzung im Startfenster auf **Netzwerk konfigurieren**. Das dann angezeigte Fenster **Netzwerkeinstellungen** ermöglicht Ihnen, die Netzwerkeinstellungen für jede Netzwerkkarte (NIC) auf der Maschine zu konfigurieren.

Die Änderungen, die während einer Sitzung vorgenommen werden, gehen nach dem Neustart der Maschine verloren.

VLANs hinzufügen

Sie können im Fenster **Netzwerkeinstellungen** VLANs (Virtual Local Area Networks, virtuelle lokale Netzwerke) hinzufügen. Verwenden Sie diese Funktionalität, falls Sie auf einen Backup-Speicherort zugreifen müssen, der sich in einem spezifischen VLAN befindet.

VLANs werden hauptsächlich dazu verwendet, um lokale Netzwerke (LANs) in logische Teilnetze zu segmentieren. Eine Netzwerkkarte (NIC), die mit einem *Zugriffs*-Port des Switches verbunden ist, kann immer auf das in der Port-Konfiguration spezifizierte VLAN zugreifen. Eine Netzwerkkarte (NIC), die mit einem *Trunk*-Port des Switches verbunden ist, kann nur dann auf die in der Port-Konfiguration erlaubten VLANs zugreifen, wenn Sie die VLANs in den Netzwerkeinstellungen spezifizieren.

So ermöglichen Sie den Zugriff auf ein VLAN über einen Trunk-Port

1. Klicken Sie auf **VLAN hinzufügen**.
2. Wählen Sie die Netzwerkkarte aus, die Zugriff auf dasjenige lokale Netzwerk bereitstellt, welches das benötigte VLAN enthält.
3. Spezifizieren Sie den VLAN-Bezeichner (Identifier).

Nachdem Sie auf **OK** geklickt haben, erscheint in der Liste der Netzwerkkarten ein neuer Eintrag.

Sollten Sie ein VLAN entfernen wollen, dann klicken Sie auf den erforderlichen VLAN-Eintrag – und anschließend auf **VLAN entfernen**.

Lokale Aktionen mit einem Boot-Medium

Die Aktionen, die Sie mit einem Boot-Medium durchführen können, sind den Wiederherstellungsaktionen sehr ähnlich, die Sie unter dem regulären Betriebssystem durchführen können. Die Unterschiede sind wie folgt:

1. Bei einem Boot-Medium mit Windows-typischer Darstellung hat ein Volume denselben Laufwerksbuchstaben wie unter Windows selbst. Volumes, die unter Windows keine Laufwerksbuchstaben haben (wie etwa das Volume System-reserviert) bekommen freie Laufwerksbuchstaben in der Reihenfolge ihres Vorkommens auf den Laufwerken zugewiesen.
   Sollte das Boot-Medium kein Windows auf der Maschine erkennen können oder mehrere Windows-Versionen erkennen, dann wird allen Volumes (einschließlich solchen ohne Laufwerksbuchstaben) in der Reihenfolge ihres Vorkommens auf den Laufwerken ein Buchstabe zugewiesen. Daher können die Laufwerksbuchstaben dann von denen unter Windows vorliegenden abweichen. So könnte beispielsweise die Zuordnung des Laufwerks D: unter dem Boot-Medium dem Laufwerk E: entsprechen, welches Windows verwendet.

   Hinweis
   Es empfiehlt sich, den Volumes eindeutige Namen zuzuweisen.

2. Ein Boot-Medium mit Linux-typische Darstellung zeigt lokale Laufwerke und Volumes als 'unmounted' an (sda1, sda2...).
3. Tasks können nicht per Planung gestartet werden. Wenn Sie eine Aktion wiederholen wollen, müssen Sie diese ganz neu konfigurieren.
4. Der Speicherzeitraum für Ereignisse (Logs) ist auf die aktuelle Sitzung beschränkt. Sie können die gesamte Ereignisliste oder gefilterte Logs in eine Datei speichern.

Einen Anzeigemodus einstellen

Wenn Sie eine Maschine mit einem Linux-basierten Boot-Medium starten, wird der Anzeigemodus basierend auf der vorliegenden Hardware-Konfiguration (Monitor- und Grafikkarten-Spezifikationen) automatisch erkannt. Sollte der Anzeigemodus nicht korrekt erkannt werden, gehen Sie folgendermaßen vor:

1. Drücken Sie im Boot-Menü auf F11.
2. Geben Sie in der Befehlszeile **vga=ask** ein und fahren Sie dann mit dem Bootvorgang fort.
3. Wählen Sie aus der Liste der verfügbaren Anzeigemodi den passenden durch Eingabe der entsprechenden Nummer aus (z.B. **318**) und drücken Sie dann die **Eingabetaste**.

Falls Sie diese Prozedur nicht jedes Mal ausführen wollen, wenn Sie eine bestimmte Hardware-Konfiguration mit einem Boot-Medium starten, erstellen Sie das Medium mit der entsprechenden Modus-Nummer (in unserem Beispiel: **vga=0x318**) neu, die im Feld **Kernel-Parameter** spezifiziert wird.

Wiederherstellung mit einem Boot-Medium bei einem lokalen System

1. Booten Sie Ihre Maschine mithilfe eines Boot-Mediums.
2. Klicken Sie auf **Diese Maschine lokal verwalten**.
3. Klicken Sie auf **Recovery**.
4. Klicken Sie bei **Recovery-Quelle** auf **Daten wählen**.
5. Wählen Sie die Backup-Datei, die Sie wiederherstellen wollen.
6. Wählen Sie im unteren linken Fensterbereich die wiederherzustellenden Laufwerke/Volumes oder Dateien/Ordner aus und klicken Sie dann auf **OK**.
7. Konfigurieren Sie die Regeln zum Überschreiben.
8. Konfigurieren Sie Ausschlüsse für die Wiederherstellung.
9. Konfigurieren Sie die Recovery-Optionen.
10. Überprüfen Sie, ob Ihre Einstellungen richtig sind, und klicken Sie dann auf **OK**.

Remote-Aktionen mit einem Boot-Medium

Hinweis
Diese Funktion ist über das Advanced Backup-Paket verfügbar.

Um das Boot-Medium in der Cyber Protect-Konsole sehen zu können, müssen Sie es zuerst registrieren (wie im Abschnitt '"Das Boot-Medium registrieren" (S. 793)' beschrieben).

Wenn Sie das Medium in der Cyber Protect-Konsole registriert haben, wird es auf der Registerkarte **Geräte** –> **Boot-Medium** angezeigt. Ein Boot-Medium verschwindet wieder aus dieser Registerkarte, wenn es mehr als 30 Tage lang offline war.

Sie können die Boot-Medien remote über die Cyber Protect-Konsole verwalten. Sie können beispielsweise Daten wiederherstellen. die Maschine (die mit dem Medium gebootet wurde) neu starten oder herunterfahren oder sich Informationen, Aktivitäten und Alarmmeldungen zu dem Medium anzeigen lassen.

Wichtig
Sie können das Boot-Medium jedoch nicht remote auf der Registerkarte **Einstellungen** –> **Agenten** in der Cyber Protect-Konsole aktualisieren.

Wenn Sie das Boot-Medium aktualisieren wollen, müssen Sie ein neues Medium erstellen (wie im Abschnitt '"Bootable Media Builder" (S. 779)' beschrieben). Alternativ können Sie das gebrauchsfertige Medium herunterladen, indem Sie in der -Konsole auf folgende Befehlssequenz klicken: Kontosymbol –>**Downloads** –> **Boot-Medium**.

So können Sie Dateien oder Ordner mit einem Boot-Medium aus der Ferne wiederherstellen

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte** –> **Boot-Medium**.
1. Wählen Sie das Medium aus, das Sie für die Datenwiederherstellung verwenden wollen.
2. Klicken Sie auf **Recovery**.
3. Wählen Sie zuerst den Speicherort und dann das gewünschte Backup aus. Beachten Sie dabei, dass die Backups nach Speicherorten gefiltert werden.
4. Wählen Sie den Recovery-Punkt aus und klicken Sie dann auf **Dateien/Ordner wiederherstellen**.
5. Wechseln Sie zum benötigten Ordner oder verwenden Sie die Suchleiste, um eine Liste der gewünschten Dateien und Ordner abzurufen.

   Die Suche ist sprachunabhängig.

   Sie können ein oder mehrere Platzhalterzeichen (* und ?) verwenden. Ausführlichere Informationen über die Verwendung von Platzhalterzeichen finden Sie im Abschnitt '"Dateifilter (Ausschlüsse/Einschlüsse)" (S. 504)'.
6. Wählen Sie die wiederherzustellenden Dateien aus und klicken Sie dann auf **Recovery**.
7. Wählen Sie bei **Pfad** das gewünschte Ziel für die Wiederherstellung.
8. [Optional] Wenn Sie erweiterte Konfigurationsmöglichkeiten für die Wiederherstellung benötigen, klicken Sie auf **Recovery-Optionen**. Weitere Informationen dazu finden Sie im Abschnitt '"Recovery-Optionen" (S. 568)'.
9. Klicken Sie auf **Recovery starten**.
10. Wählen Sie eine der folgenden Optionen zum Überschreiben:
    - **Vorhandene Dateien überschreiben**
    - **Vorhandene Datei überschreiben, wenn diese älter ist**
    - **Vorhandene Dateien nicht überschreiben**

    Bestimmen Sie, ob ein automatischer Neustart der Maschine erfolgen soll.
11. Klicken Sie auf **Fortsetzen**, um die Wiederherstellung zu starten. Der Recovery-Fortschritt wird auf der Registerkarte **Aktivitäten** angezeigt.

So können Sie Laufwerke, Volumes oder komplette Maschinen mit einem Boot-Medium aus der Ferne wiederherstellen

1. Gehen Sie auf der Registerkarte **Geräte** zur Gruppe **Boot-Medium** und wählen Sie dann das Medium aus, das Sie für die Datenwiederherstellung verwenden wollen.
2. Klicken Sie auf **Recovery**.
3. Wählen Sie zuerst den Speicherort und dann das gewünschte Backup aus. Beachten Sie dabei, dass die Backups nach Speicherorten gefiltert werden.
4. Wählen Sie den Recovery-Punkt aus und klicken Sie dann auf **Recovery** –> **Komplette Maschine**.

   Bei Bedarf können Sie die Zuordnung der Zielmaschinen bzw. ihrer Volumes konfigurieren, wie im Abschnitt '"Physische Maschinen wiederherstellenDieser Abschnitt erläutert, wie Sie physische Maschinen mithilfe der Weboberfläche wiederherstellen können.Für die

Wiederherstellung folgender Systeme müssen Sie ein Boot-Medium (statt der Weboberfläche) verwenden:Eine Maschine, die unter macOS läuftEine Maschine von einem Mandanten im Compliance-ModusEin beliebiges Betriebssystem, das auf fabrikneuer Hardware (Bare Metal Recovery) oder zu einer Offline-Maschine wiederhergestellt werden sollDie Struktur logischer Volumes (Volumes, die mit dem Logical Volume Manager unter Linux erstellt wurden). Das Medium ermöglicht Ihnen, die logische Volume-Struktur automatisch neu erstellen zu lassen.Sie können keine Laufwerk-Backups von Intel-basierten Macs auf Macs wiederherstellen, die einen Apple Silicon-Prozessor verwenden (oder umgekehrt). Sie können jedoch einzelne Dateien und Ordner wiederherstellen.Recovery mit NeustartDie Wiederherstellung eines Betriebssystems und die Wiederherstellung von Volumes, die per BitLocker verschlüsselt wurden, erfordert einen Neustart. Sie können wählen, ob die Maschine automatisch neu gestartet werden soll – oder ob Ihr der Status Benutzereingriff erforderlich zugewiesen werden soll. Das wiederhergestellte System geht automatisch online.Verschlüsselte Volumes, die per Backup gesichert wurden, werden als unverschlüsselte Volumes wiederhergestellt.Die Wiederherstellung von Volumes, die bei der Sicherung per BitLocker verschlüsselt waren, setzt voraus, dass sich auf derselben Maschine ein unverschlüsseltes Volume befindet. Dieses Volume muss außerdem über mindestens 1 GB freien Speicherplatz verfügen. Wenn eine dieser beiden Bedingungen nicht erfüllt ist, wird die Wiederherstellung fehlschlagen.Für die Wiederherstellung eines verschlüsselten System-Volumes sind keine weiteren Maßnahmen erforderlich. Wenn Sie ein verschlüsseltes Nicht-System-Volume wiederherstellen wollen, müssen Sie es zunächst sperren. Beispielsweise, indem Sie eine Datei öffnen, die sich auf diesem Volume befindet. Anderenfalls wird die Wiederherstellung ohne einen Neustart fortgesetzt, wodurch es passieren kann, dass das wiederhergestellte Volume von Windows nicht erkannt wird.Falls die Wiederherstellung fehlschlägt und Ihre Maschine mit der Fehlermeldung Datei kann nicht von der Partition abgerufen werden neu startet, sollten Sie versuchen, die Secure Boot-Funktion zu deaktivieren. Weitere Informationen dazu finden Sie im Abschnitt Deaktivieren des sicheren Starts („Disabling Secure Boot“) in der Microsoft-Dokumentation.So können Sie eine physische Maschine wiederherstellenWählen Sie die Maschine aus, die per Backup gesichert wurde.Klicken Sie auf Recovery.Wählen Sie einen Recovery-Punkt. Beachten Sie dabei, dass Recovery-Punkte nach Speicherorten gefiltert werden.Falls die Maschine offline ist, werden keine Recovery-Punkte angezeigt. Gehen Sie nach einer der folgenden Möglichkeiten vor:Sollte sich das Backup im Cloud Storage oder einem freigegebenen Storage befinden (d.h., dass andere Agenten auf diesen zugreifen können), dann klicken Sie zuerst auf den Befehl Maschine auswählen. Wählen Sie anschließend eine Zielmaschine, die online ist, und dann den gewünschten Recovery-Punkt.Wählen Sie einen Recovery-Punkt auf der Registerkarte 'Backup Storage'.Stellen Sie die Maschine so wieder her, wie es im Abschnitt 'Laufwerke mithilfe eines Boot-Mediums wiederherstellen' beschrieben ist.Klicken Sie auf Recovery –> Komplette Maschine.Die Software weist die Laufwerke im Backup automatisch den Laufwerken der Zielmaschine zu.Wenn Sie eine andere physische Maschine als Recovery-Ziel verwenden wollen, klicken Sie auf Zielmaschine und wählen Sie dann eine Zielmaschine aus, die online ist.Falls die Zuordnung erfolglos war oder falls Sie mit dem Zuordnungsergebnis unzufrieden sind, können Sie auf Volume-Zuordnung klicken, um die Laufwerke manuell zuzuordnen.Der Zuordnungsbereich ermöglicht Ihnen außerdem, bestimmte Laufwerke oder Volumes für die Wiederherstellung auszuwählen. Mit

dem Link Wechseln zu... (in der oberen rechten Ecke) können Sie zwischen Wiederherstellung von Laufwerken und Volumes wechseln.[Nur für Windows-Maschinen verfügbar, auf denen ein Protection Agent installiert ist] Aktivieren Sie den Schalter Safe Recovery, um sicherzustellen, dass die wiederhergestellten Daten frei von Malware sind. Weitere Informationen darüber, wie Safe Recovery funktioniert, finden Sie im Abschnitt '"Safe Recovery" (S. 1)'.Klicken Sie auf Recovery starten.Bestätigen Sie, dass die Daten auf den Laufwerken durch die Datenversionen überschrieben werden sollen, die im Backup vorliegen. Bestimmen Sie, ob ein automatischer Neustart der Maschine erfolgen soll.Der Recovery-Fortschritt wird auf der Registerkarte Aktivitäten angezeigt." (S. 1)' beschrieben.

5. Wenn Sie erweiterte Konfigurationsmöglichkeiten für die Wiederherstellung benötigen, klicken Sie auf **Recovery-Optionen**. Weitere Informationen dazu finden Sie im Abschnitt '"Recovery-Optionen" (S. 568)'.
6. Klicken Sie auf **Recovery starten**.
7. Bestätigen Sie, dass die Daten auf den Laufwerken durch die Datenversionen überschrieben werden sollen, die im Backup vorliegen. Bestimmen Sie, ob ein automatischer Neustart der Maschine erfolgen soll.
8. Der Recovery-Fortschritt wird auf der Registerkarte **Aktivitäten** angezeigt.

So können Sie die gebootete Maschine aus der Ferne neu starten

1. Gehen Sie auf der Registerkarte **Geräte** zur Gruppe **Boot-Medium** und wählen Sie dann das Medium aus, das Sie für die Datenwiederherstellung verwenden wollen.
2. Klicken Sie auf **Neustart**.
3. Bestätigen Sie, dass Sie die Maschine, die mit dem Medium gebootet wurde, neu starten wollen.

So können Sie die gebootete Maschine aus der Ferne herunterfahren

1. Gehen Sie auf der Registerkarte **Geräte** zur Gruppe **Boot-Medium** und wählen Sie dann das Medium aus, das Sie für die Datenwiederherstellung verwenden wollen.
2. Klicken Sie auf **Herunterfahren**.
3. Bestätigen Sie, dass Sie die Maschine, die mit dem Medium gebootet wurde, herunterfahren wollen.

So können Sie sich Informationen über das Boot-Medium anzeigen lassen

1. Gehen Sie auf der Registerkarte **Geräte** zur Gruppe **Boot-Medium** und wählen Sie dann das Medium aus, das Sie für die Datenwiederherstellung verwenden wollen.
2. Klicken Sie auf **Details**, **Aktivitäten** oder **Alarmmeldungen**, um die entsprechenden Informationen einzusehen.

So können Sie ein Boot-Medium aus der Ferne löschen

1. Gehen Sie auf der Registerkarte **Geräte** zur Gruppe **Boot-Medium** und wählen Sie dann das Medium aus, das Sie für die Datenwiederherstellung verwenden wollen.

2. Klicken Sie auf **Löschen**, um das Boot-Medium aus der Cyber Protect-Konsole zu entfernen.
3. Bestätigen Sie, dass Sie das Boot-Medium löschen wollen.

Startup Recovery Manager

Startup Recovery Manager ist eine bootfähige Komponente, die auf der Festplatte gespeichert ist. Mit Startup Recovery Manager können Sie das bootfähige Notfallwerkzeug starten, ohne ein eigenständiges Boot-Medium verwenden zu müssen.

Wenn es zu einem Ausfall der Maschine kommt, starten Sie diese neu, warten Sie auf die Aufforderung **Druecken Sie F11 zum Ausfuehren des Acronis Startup Recovery Manager**, drücken Sie dann F11 oder wählen Sie die Option Startup Recovery Manager aus dem Boot-Menü aus (wenn Sie den GRUB-Bootloader verwenden). Daraufhin wird Startup Recovery Manager gestartet und Sie können eine Wiederherstellung durchführen.

Einschränkungen

- [Nicht anwendbar auf GRUB, das im Master Boot Record installiert ist] Wenn Startup Recovery Manager aktiviert wird, überschreibt dessen Boot-Code den MBR (Master Boot Record). Daher müssen Sie möglicherweise vorhandene Bootloader von Drittanbietern anschließend neu aktivieren.
- [Für GRUB nicht zutreffend] Bevor Sie Startup Recovery Manager unter Linux aktivieren, empfehlen wir Ihnen, den Bootloader in den Boot Record der Root-Partition oder in den Boot Record der /boot-Partitionen zu installieren, anstatt ihn in den MBR zu installieren. Anderenfalls müssen Sie den Bootloader nach der Aktivierung manuell neu konfigurieren.

Startup Recovery Manager aktivieren

Um die Boot-Zeit-Aufforderung zu aktivieren **Drücken Sie F11 für Acronis Startup Recovery Manager** (oder fügen Sie das Element **Startup Recovery Manager** dem GRUB-Menü hinzu). Sie müssen Startup Recovery Manager aktivieren.

Hinweis
Die Aktivierung von Startup Recovery Manager auf einer Maschine mit nicht verschlüsseltem Systemvolumen erfordert mindestens 100 MB freien Speicherplatz auf dieser Maschine. Eine Wiederherstellung mit Neustart erfordert zusätzliche 100 MB.

Um Startup Recovery Manager auf einer Maschine aktivieren zu können, die ein BitLocker-verschlüsseltes Laufwerk hat, muss diese Maschine mindestens ein nicht verschlüsseltes Laufwerk haben, auf dem mindestens 500 MB freier Speicherplatz vorhanden sind. Die Wiederherstellung mit Neustart erfordert zusätzliche 500 MB freien Speicherplatz.

Backup-Aktionen, die One-Click-Recovery-Backups erstellen, werden fehlschlagen, wenn Startup Recovery Manager nicht aktiviert ist.

So können Sie Startup Recovery Manager aktivieren

Auf einem Windows- oder Linux-Rechner mit einem Agenten

1. Wählen Sie in der Cyber Protect-Konsole die Maschine aus, auf der Sie Startup Recovery Manager aktivieren möchten.
2. Klicken Sie auf **Details**.
3. Aktivieren Sie den **Startup Recovery Manager** Schalter.

Auf einer Maschine ohne Agenten

1. Starten Sie die Maschine mit einem Boot-Medium.
2. Klicken Sie in der grafischen Benutzeroberfläche des Boot-Mediums auf **Tools** > **Aktivieren Startup Recovery Manager**.
3. Wählen Sie **Aktivieren**.
4. Klicken Sie auf **OK**.
5. Überprüfen Sie auf der Registerkarte **Details** die Zeile **Ergebnis**, um zu bestätigen, dass die Aktivierung erfolgreich war. Klicken Sie dann auf **Schließen**.

Startup Recovery Manager deaktivieren

Mit der Deaktivierung wird auch die Boot-Meldung **Drucken Sie F11 zum Ausfuehren des AcronisStartup Recovery Manager** (oder der entsprechende Menü-Eintrag **Startup Recovery Manager** aus GRUB) entfernt.

Wenn Startup Recovery Manager nicht aktiviert ist, können Sie eine Maschine, die nicht mehr starten kann, immer noch mit einem eigenständigen Boot-Medium wiederherstellen.

Hinweis
Backup-Aktionen, die One-Click-Recovery-Backups erstellen, werden fehlschlagen, wenn Startup Recovery Manager nicht aktiviert ist.

So können Sie Startup Recovery Manager deaktivieren

Auf einem Windows- oder Linux-Rechner mit einem Agenten

1. Wählen Sie in der Cyber Protect-Konsole die Maschine aus, auf der Sie Startup Recovery Manager deaktivieren möchten.
2. Klicken Sie auf **Details**.
3. Deaktivieren Sie den Schalter für **Startup Recovery Manager**.

Auf einer Maschine ohne Agenten

1. Starten Sie die Maschine mit einem Boot-Medium.
2. Klicken Sie in der grafischen Benutzeroberfläche des Boot-Mediums auf auf **Extras** > **Deaktivieren Startup Recovery Manager**.
3. Wählen Sie **Deaktivieren**.
4. Klicken Sie auf **OK**.

5. Überprüfen Sie auf der Registerkarte **Details** Sie die Zeile **Ergebnis**, um zu bestätigen, dass die Deaktivierung erfolgreich war. Klicken Sie anschließend auf **Schließen**.

Disaster Recovery implementieren

Hinweis
- Diese Funktionalität unterstützt keine Microsoft Azure-Backup-Speicherorte.

Über Cyber Disaster Recovery Cloud

Cyber Disaster Recovery Cloud (DR) – ein Bestandteil von Cyber Protection, der eine DRaaS-Funktionalität (Disaster Recovery as a Service) bereitstellt. Cyber Disaster Recovery Cloud bietet Ihnen eine schnelle und stabile Lösung, um exakte Kopien Ihrer Maschinen auf einer Cloud-Site zu starten und so Workloads von beschädigten Maschinen zu Recovery-Servern in der Cloud umschalten zu können, falls es zu einem Desaster kommt (egal ob von von Menschen verursacht oder natürlichen Ursprungs).

Sie können die Disaster Recovery-Funktionalität auf folgende Arten einrichten und konfigurieren:

- Erstellen Sie einen Schutzplan, der das Disaster Recovery-Modul enthält, und wenden Sie den Plan auf Ihre Geräte an. Dadurch wird automatisch eine Standard-Disaster-Recovery-Infrastruktur eingerichtet. Siehe auch den Abschnitt 'Einen Disaster Recovery-Schutzplan erstellen'.
- Richten Sie die Disaster Recovery Cloud-Infrastruktur manuell ein, wenn Sie jeden Schritt kontrollieren wollen. Siehe '"Recovery-Server einrichten" (S. 854)'.

Die Kernfunktionalität

Hinweis
In Abhängigkeit davon, welches Lizenzierungsmodell angewendet wird, kann für einige Funktionen eine zusätzliche Lizenzierung erforderlich sein.

- Verwalten Sie den Cyber Disaster Recovery Cloud Service über eine einzelne, zentrale Konsole
- Erweitern Sie bis zu 23 lokale Netzwerke über einen sicheren VPN-Tunnel in die Cloud
- Bauen Sie eine Verbindung zur Cloud-Site auf, ohne dass eine VPN-Appliance[1]-Bereitstellung notwendig ist ('Nur Cloud'-Modus)
- Bauen Sie eine Point-to-Site-Verbindung zur Ihrem lokalen Standort und zur Cloud-Site auf
- Schützen Sie Ihre Maschinen, indem Sie Recovery-Server in der Cloud verwenden
- Schützen Sie Applikationen und Appliances, indem Sie primäre Servern in der Cloud verwenden
- Führen Sie automatische Disaster Recovery-Aktionen für verschlüsselte Backups durch
- Führen Sie einen Test-Failover in einem isolierten Netzwerk aus
- Verwenden Sie Runbooks, um die Produktionsumgebung in die Cloud zu übertragen

[1] [Disaster Recovery] Eine spezielle virtuelle Maschine, die eine Verbindung (über einen sicheren VPN-Tunnel) zwischen dem lokalen Netzwerk und der Cloud-Site ermöglicht. Die VPN-Appliance wird am lokalen Standort bereitgestellt.

Software-Anforderungen

Unterstützte Betriebssysteme

Der Schutz mit einem Recovery-Server wurde mit folgenden Betriebssystemen getestet:

- CentOS 6.6, 7.x, 8.x
- Debian 9.x, 10.x, 11.x
- Red Hat Enterprise Linux 6.6, 7.x, 8.x
- Ubuntu 16.04, 18.04, 20.x, 21.x
- Oracle Linux 7.3 and 7.9 with Unbreakable Enterprise Kernel
- Windows Server 2008 R2
- Windows Server 2012/2012 R2
- Windows Server 2016 – alle Installationsoptionen, mit Ausnahme des Nano Servers
- Windows Server 2019 – alle Installationsoptionen, mit Ausnahme des Nano Servers
- Windows Server 2022 – alle Installationsoptionen, mit Ausnahme des Nano Servers

Eine korrekte Funktion der Software mit anderen Windows-Betriebssystemen und Linux-Distributionen ist möglich, wird jedoch nicht garantiert.

Hinweis
Der Schutz mit einem Recovery-Server wurde für Microsoft Azure-VMs mit den nachfolgenden Betriebssystemen getestet.

- Windows Server 2008 R2
- Windows Server 2012/2012 R2
- Windows Server 2016 – alle Installationsoptionen, mit Ausnahme des Nano Servers
- Windows Server 2019 – alle Installationsoptionen, mit Ausnahme des Nano Servers
- Windows Server 2022 – alle Installationsoptionen, mit Ausnahme des Nano Servers
- Ubuntu Server 20.04 LTS - Gen2 (Canonical). Weitere Informationen über den Zugriff auf die Recovery-Server-Konsole finden Sie unter https://kb.acronis.com/content/71616.

Unterstützte Virtualisierungsplattformen

Der Schutz von virtuellen Maschinen mit einem Recovery-Server wurde mit folgenden Virtualisierungsplattformen getestet:

- VMware ESXi 5.1, 5.5, 6.0, 6.5, 6.7, 7.0
- Windows Server 2008 R2 mit Hyper-V
- Windows Server 2012/2012 R2 mit Hyper-V

- Windows Server 2016 mit Hyper-V – alle Installationsoptionen, mit Ausnahme des Nano Servers
- Windows Server 2019 mit Hyper-V – alle Installationsoptionen, mit Ausnahme des Nano Servers
- Windows Server 2022 mit Hyper-V – alle Installationsoptionen, mit Ausnahme des Nano Servers
- Microsoft Hyper-V Server 2012/2012 R2
- Microsoft Hyper-V Server 2016
- Kernel-based Virtual Machines (KVM) – nur vollständig virtualisierte Gäste (HVM). Paravirtualisierte Gäste (PV) werden nicht unterstützt.
- Red Hat Enterprise Virtualization (RHEV) 3.6
- Red Hat Virtualization (RHV) 4.0
- Citrix XenServer: 6.5, 7.0, 7.1, 7.2

Die VPN-Appliance wurde mit folgenden Virtualisierungsplattformen getestet:

- VMware ESXi 5.1, 5.5, 6.0, 6.5, 6.7
- Windows Server 2008 R2 mit Hyper-V
- Windows Server 2012/2012 R2 mit Hyper-V
- Windows Server 2016 mit Hyper-V – alle Installationsoptionen, mit Ausnahme des Nano Servers
- Windows Server 2019 mit Hyper-V – alle Installationsoptionen, mit Ausnahme des Nano Servers
- Windows Server 2022 mit Hyper-V – alle Installationsoptionen, mit Ausnahme des Nano Servers
- Microsoft Hyper-V Server 2012/2012 R2
- Microsoft Hyper-V Server 2016

Eine korrekte Funktion der Software mit anderen Virtualisierungsplattformen und Versionen ist möglich, wird jedoch nicht garantiert.

Einschränkungen

Folgende Plattformen und Konfigurationen werden in Cyber Disaster Recovery Cloud nicht unterstützt:

1. Nicht unterstützte Plattformen:
   - Agenten für Virtuozzo
   - macOS
   - Windows-Desktop-Betriebssysteme werden aufgrund von Microsoft-Produktbedingungen nicht unterstützt.
   - Windows Server Azure Edition
     Die Azure Edition ist eine besondere Version des Windows Servers, die speziell dafür entwickelt wurde, entweder als virtuelle Maschine (VM) in Azure IaaS oder als VM auf einem Azure Stack HCI-Cluster zu laufen. Im Gegensatz zur Standard Edition und der Datacenter Edition ist die Azure Edition nicht für den Betrieb auf farbrikneuer physischer Hardware (Bare-

Metal-Hardware), Windows Client Hyper-V, Windows Server Hyper-V, Drittanbieter-Hypervisoren oder in Drittanbieter-Clouds lizenziert.

2. Nicht unterstützte Konfigurationen:

   Microsoft Windows

   - Dynamische Laufwerke werden nicht unterstützt
   - Windows-Desktop-Betriebssysteme werden (aufgrund von Microsoft-Produktbedingungen) nicht unterstützt
   - Der Active Directory Service mit FRS-Replikation wird nicht unterstützt
   - Wechselmedien ohne GPT- oder MBR-Formatierung (auch „Superfloppy“ genannt) werden nicht unterstützt

   Linux

   - Dateisysteme ohne Partitionstabelle
   - Linux-Workloads, die mit einem Agenten von einem Gastbetriebssystem aus gesichert werden und über Volumes mit folgenden erweiterten LVM-Konfigurationen (Logical Volume Manager) verfügen: Stripeset-Volumes, gespiegelte Volumes sowie Volumes mit RAID 0, RAID 4, RAID 5, RAID 6 oder RAID 10.

   Hinweis
   Workloads, die mehrere Betriebssysteme installiert haben, werden nicht unterstützt.

3. Nicht unterstützte Backup-Typen:
   - Recovery-Punkte aus einer kontinuierlichen Datensicherung (CDP) sind nicht kompatibel.

     Wichtig
     Wenn Sie einen Recovery-Server aus einem Backup mit einem CDP-Recovery-Punkt erstellt haben, werden Sie während des Failbacks – oder wenn Sie ein Backup eines Recovery-Servers erstellen – die im CDP-Recovery-Punkt enthaltenen Daten verlieren.

   - Forensik-Backups können nicht verwendet werden, um Recovery-Server zu erstellen.

Ein Recovery-Server hat eine Netzwerkschnittstelle. Wenn die ursprüngliche mehrere Netzwerkschnittstellen hat, wird nur eine davon emuliert.

Cloud-Server werden nicht verschlüsselt.

Cyber Disaster Recovery Cloud-Testversion

Sie können eine Testversion von Acronis Cyber Disaster Recovery Cloud für einen Zeitraum von 30 Tagen verwenden. In diesem Fall unterliegt die Disaster Recovery-Funktionalität für die Partner-Mandanten folgende Einschränkungen:

- Kein Zugriff auf das öffentliche Internet für primäre Server und Recovery-Server. Sie können den Servern keine öffentlichen IP-Adressen zuweisen.
- Multi-Site-IPsec-VPN ist nicht verfügbar.

Einschränkungen bei der Verwendung des Geo-redundant Cloud Storage

Der Geo-redundant Cloud Storage stellt Ihnen einen zweiten Speicherort für Ihre Backup-Daten zur Verfügung. Der sekundäre Speicherort befindet sich in einer Region, die geografisch vom primären Speicherort entfernt liegt. Durch die geografische Trennung der Regionen wird sichergestellt, dass eine der beiden Regionen jeweils nicht in Mitleidenschaft gezogen wird, wenn der jeweils andere Standort von einem Desaster (wie einer Naturkatastrophe) heimgesucht wird und die entsprechenden Backup-Daten nicht wiederhergestellt werden können. Dank dieser Maßnahme kann der Geschäftsbetrieb dennoch weitergeführt werden.

Wichtig
Der Disaster Recovery Service wird nicht unterstützt, wenn der Backup Storage vom primären Standort zum georedundanten sekundären Standort umgestellt wird.

Disaster Recovery-Kompatibilität mit Verschlüsselungsprogrammen

Die Disaster Recovery-Funktionalität ist mit folgenden laufwerksbasierten Verschlüsselungsprogrammen kompatibel:

- Microsoft BitLocker Drive Encryption
- McAfee Endpoint Encryption
- PGP Whole Disk Encryption

Hinweis
- Bei Laufwerken mit einer Verschlüsselung auf Festplattenebene empfehlen wir Ihnen, dass Sie den Protection Agent im Gastbetriebssystem des Workloads installieren und agentenbasierte Backups durchführen.
- Für agentenlose Backups von verschlüsselten Workloads werden keine Failover- und Failback-Aktionen unterstützt.

Weitere Informationen über die Kompatibilität von Cyber Protection mit anderen Verschlüsselungsprogrammen Sie im Abschnitt '"Kompatibilität mit Verschlüsselungssoftware" (S. 44)'.

Berechnungspunkte

Bei Disaster Recovery werden Berechnungspunkte für primäre Server und Recovery-Server bei Test-Failovers und Produktions-Failovers verwendet. Berechnungspunkte spiegeln diejenigen Compute-

Ressourcen wider, die für die Ausführung der Server (virtuelle Maschinen) in der Cloud eingesetzt werden.

Der Verbrauch von Berechnungspunkten bei Disaster Recovery-Prozessen hängt von den Parametern des Servers und der Dauer des Zeitraums ab, während dessen sich der Server im Failover-Stadium befindet. Je leistungsfähiger der Server und je länger dieser Zeitraum ist, desto mehr Berechnungspunkte werden verbraucht. Und je mehr Berechnungspunkte verbraucht werden, desto höher ist der Preis, der Ihnen berechnet wird.

Alle Server, die in der Acronis Cloud laufen, werden nach Compute-Punkten berechnet, abhängig von ihrer konfigurierten Ausführung, unabhängig von ihrem Zustand (eingeschaltet oder ausgeschaltet).

Wiederherstellungsserver im Standby-Zustand verbrauchen keine Rechenpunkte und es werden keine Gebühren für Rechenpunkte berechnet.

In der untenstehenden Tabelle sehen Sie ein Beispiel für acht Server in der Cloud mit verschiedenen Ausführungen und die entsprechenden Rechenpunkte, die sie pro Stunde verbrauchen werden. Sie können die Ausführungen der Server im **Details** Tab ändern.

Typ	CPU	RAM	Berechnungspunkte
V1	1 vCPU	2 GB	1
V2	1 vCPU	4 GB	2
V3	2 vCPU	8 GB	4
V4	4 vCPU	16 GB	8
V5	8 vCPU	32 GB	16
V6	16 vCPU	64 GB	32
V7	16 vCPU	128 GB	64
V8	16 vCPU	256 GB	128

Anhand der Informationen in der Tabelle können Sie leicht einschätzen, wie viele Berechnungspunkte ein Server (eine virtuelle Maschine) verbrauchen wird.

Wenn Sie beispielsweise eine virtuelle Maschine mit 4 vCPU* und 16 GB RAM sowie eine virtuelle Maschine mit 2 vCPU und 8 GB RAM per Disaster Recovery schützen wollen, wird die erste virtuelle Maschine 8 Berechnungspunkte pro Stunde verbrauchen und die zweite virtuelle Maschine 4 Berechnungspunkte pro Stunde. Wenn sich beide virtuellen Maschinen im Failover-Stadium befinden, ergibt sich ein Gesamtverbrauch von 12 Berechnungspunkten pro Stunde – oder 288 Berechnungspunkten für den gesamten Tag (12 Berechnungspunkte x 24 Stunden = 288 Berechnungspunkte).

*Eine vCPU bezieht sich auf einen physischen Zentralprozessor (CPU), der einer virtuellen Maschine zugewiesen wurde, und zudem eine zeitabhängige Einheit ist.

Hinweis
Wenn das Limit für die Quota der **Berechnungspunkte** überschritten wird, werden alle primären und Recovery-Server heruntergefahren. Es wird nicht möglich sein, diese Server zu nutzen, bis der nächste Abrechnungszeitraum beginnt oder bis Sie die Quota erhöhen. Der Standardabrechnungszeitraum ist ein voller Kalendermonat.

Die Disaster Recovery-Funktionalität einrichten

Hinweis
In Abhängigkeit davon, welches Lizenzierungsmodell angewendet wird, kann für einige Funktionen eine zusätzliche Lizenzierung erforderlich sein.

So können Sie die Disaster Recovery-Funktionalität einrichten

1. Konfigurieren Sie den Verbindungstyp mit der Cloud-Site:
   - Point-to-Site-Verbindung
   - Site-to-Site-OpenVPN-Verbindung
   - Multi-Site-IPsec-VPN-Verbindung
   - 'Nur Cloud'-Modus
2. Erstellen Sie einen Schutzplan mit aktiviertem Backup-Modul und wählen Sie die komplette Maschine oder die System- sowie Boot-Volumes als Backup-Quelle aus. Für die Erstellung eines Recovery-Servers ist mindestens ein Schutzplan erforderlich.
3. Wenden Sie den Schutzplan auf die zu schützenden lokalen Server an.
4. Erstellen Sie die Recovery-Server für jeden Ihrer lokalen Server, den Sie schützen wollen.
5. Führen Sie einen Test-Failover aus, um zu überprüfen, wie dieser funktioniert.
6. [Optional] Erstellen Sie die primären Server zur Replikation von Applikationen.

Als Ergebnis haben Sie die Disaster Recovery-Funktionalität eingerichtet, um Ihre lokalen Server vor Desastern zu schützen.

Sollte es zu einem Desaster kommen, können Sie Ihren Workload per Failover auf die Recovery-Server in der Cloud auslagern. Es muss mindestens ein Recovery-Punkt erstellt worden sein, bevor ein Failover-Prozess zu einem Recovery-Server durchgeführt werden kann. Wenn Ihr lokaler Standort dann nach dem Desaster wiederhergestellt wurde , können Sie den Workload per Failback wieder zurück aus der Cloud zu Ihrem lokalen Standort umschalten. Weitere Informationen über den Failback-Prozess finden Sie in den Abschnitten '"Voraussetzungen" (S. 870)' und '"Voraussetzungen" (S. 875)'.

Einen Disaster Recovery-Schutzplan erstellen

Erstellen Sie einen Schutzplan, der das Disaster Recovery-Modul enthält, und wenden Sie den Plan auf Ihre Geräte an.

Wenn ein neuer Schutzplan erstellt wird, ist das Disaster Recovery-Modul standardmäßig deaktiviert. Wenn Sie die Disaster Recovery-Funktionalität aktivieren und den Plan auf Ihre Geräte anwenden, wird die Cloud-Netzwerkinfrastruktur erstellt – einschließlich eines *Recovery-Servers* für jedes geschütztes Gerät. Ein solcher *Recovery-Server* ist eine virtuelle Maschine in der Cloud, bei der es sich um eine Kopie des ausgewählten Gerätes handelt. Für jedes der ausgewählten Geräte wird ein Recovery-Server mit Standardeinstellungen im Standby-Stadium erstellt (die virtuelle Maschine wird also nicht ausgeführt). Die Größe des Recovery-Servers wird automatisch in Abhängigkeit von der CPU und dem Arbeitsspeicher des geschützten Gerätes festgelegt. Die Standard-Cloud-Netzwerk-Infrastruktur wird ebenfalls automatisch erstellt: das VPN-Gateway und die Netzwerke auf der Cloud-Site, mit denen die Recovery-Server verbunden sind.

Wenn Sie das Disaster Recovery-Modul eines Schutzplanes widerrufen, löschen oder ausschalten, werden die Recovery-Server und Cloud-Netzwerke nicht automatisch gelöscht. Sie können die Disaster Recovery-Infrastruktur bei Bedarf aber manuell entfernen.

Hinweis

- Nachdem Sie die Disaster Recovery-Funktionalität konfiguriert haben, können Sie einen Test- oder Produktions-Failover von jedem Recovery-Punkt aus durchführen, der zu einem Zeitpunkt generiert wurde, nachdem der Recovery-Server für das entsprechende Gerät erstellt wurde. Recovery-Punkte, die generiert wurden, bevor das Gerät per Disaster Recovery geschützt wurde (z.B. bevor der Recovery-Server erstellt wurde), können nicht für ein Failover verwendet werden.
- Ein Disaster Recovery-Schutzplan kann nicht aktiviert werden, wenn die IP-Adresse eines Geräts nicht ermittelt werden kann. Beispielsweise, wenn virtuelle Maschinen agentenlos gesichert werden und ihnen keine IP-Adresse zugewiesen wurde.
- Wenn Sie einen Schutzplan anwenden, werden die gleichen Netzwerke und IP-Adressen in der Cloud-Site zugewiesen. Die IPsec-VPN-Konnektivität setzt voraus, dass sich die Netzwerksegmente der Cloud und der lokalen Standorte nicht überlappen. Wenn eine Multi-Site-IPsec-VPN-Konnektivität konfiguriert wurde und Sie später einen Schutzplan auf ein oder mehrere Geräte anwenden wollen, müssen Sie zusätzlich die Cloud-Netzwerke aktualisieren und die IP-Adressen der Cloud Server neu zuweisen. Weitere Informationen finden Sie im Abschnitt '"IP-Adressen neu zuweisen" (S. 844)'.

So können Sie einen Disaster Recovery-Schutzplan erstellen

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte** –> **Alle Geräte**.
2. Wählen Sie die Maschinen aus, die Sie sichern wollen.
3. Klicken Sie zuerst auf **Schützen** und dann auf **Plan erstellen**.
   Daraufhin werden die Standardeinstellungen des Schutzplans geöffnet.

4. Konfigurieren Sie die Backup-Optionen.

   Wenn Sie die Disaster Recovery-Funktionalität verwenden wollen, muss der Plan die komplette Maschine in den Cloud Storage sichern – oder zumindest diejenigen Laufwerke, die zum Booten und zur Bereitstellung notwendiger Services erforderlich sind.
5. Aktivieren Sie das Disaster Recovery-Modul, indem Sie auf den Schalter neben dem Namen des Moduls klicken.
6. Klicken Sie auf **Erstellen**.

   Der Plan wird erstellt und auf die ausgewählten Maschinen angewendet.

Was ist als nächstes zu tun?

- Sie können die Standardkonfiguration des Recovery-Servers bearbeiten. Weitere Informationen finden Sie im Abschnitt '"Recovery-Server einrichten" (S. 854)'.
- Sie können die Standardnetzwerkkonfiguration bearbeiten. Weitere Informationen finden Sie im Abschnitt '"Verbindungen einrichten" (S. 814)'.
- Sie können mehr über die Standardparameter für die Recovery-Server und die Cloud-Netzwerkinfrastruktur erfahren. Weitere Informationen dazu finden Sie in den Abschnitten '"Die Standardparameter für Recovery-Server bearbeiten" (S. 812)' und '"Cloud-Netzwerk-Infrastruktur" (S. 814)'.

Die Standardparameter für Recovery-Server bearbeiten

Wenn Sie einen Disaster Recovery-Schutzplan erstellen und anwenden, wird ein Recovery-Server mit Standardparametern konfiguriert. Sie können diese Standardparameter auch später noch bearbeiten.

Hinweis
Ein Recovery-Server wird nur dann neu erstellt, wenn er noch nicht vorhanden ist. Bereits vorhandene Recovery-Server werden weder verändert noch neu erstellt.

So können Sie die Standardparameter für Recovery-Server bearbeiten

1. Gehen Sie zu **Geräte** –> **Alle Geräte**.
2. Wählen Sie ein Gerät aus und klicken Sie auf **Disaster Recovery**.
3. Bearbeiten Sie die Standardparameter für Recovery-Server.
   Die Recovery-Server-Parameter werden in der nachfolgenden Tabelle beschrieben.

Recovery-Server Parameter	Standard Wert	Beschreibung
CPU und RAM	auto	Die Anzahl der virtuellen CPUs und die Menge an Arbeitsspeicher (RAM) für den Recovery-Server. Die Standardeinstellungen werden automatisch auf der Grundlage der

		ursprünglichen Geräte-CPU- und RAM-Konfiguration festgelegt.
Cloud-Netzwerk	auto	Das Cloud-Netzwerk, mit dem der Server verbunden sein wird. Weitere Informationen zur Konfiguration von Cloud-Netzwerken finden Sie im Abschnitt Cloud-Netzwerkinfrastruktur.
IP-Adresse im Produktionsnetzwerk	auto	Die IP-Adresse, die der Server im Produktionsnetzwerk haben wird. Standardmäßig ist die IP-Adresse der ursprünglichen Maschine vorgegeben.
Test-IP-Adresse	deaktiviert	Die Test-IP-Adresse gibt Ihnen die Möglichkeit, einen Failover in einem isolierten Testnetzwerk zu testen und sich während eines Test-Failovers per RDP oder SSH mit dem Recovery-Server zu verbinden. Im Test-Failover-Modus wird das VPN-Gateway mithilfe des NAT-Protokolls die Test-IP-Adresse gegen die Produktions-IP-Adresse ersetzen. Wenn keine Test-IP-Adresse spezifiziert wird, ist die Konsole die einzige Möglichkeit, während eines Test-Failovers auf den Server zuzugreifen.
Internetzugriff	aktiviert	Ermöglichen Sie dem Recovery-Server, sich während eines Failovers (im Realbetrieb oder im Testmodus) mit dem Internet zu verbinden. Standardmäßig wird der TCP-Port 25 für ausgehende Verbindungen verweigert.
Öffentliche IP-Adresse verwenden	deaktiviert	Wenn der Recovery-Server über eine öffentliche IP-Adresse verfügt, ist er während eines Failovers (auch im Testmodus) aus dem Internet verfügbar. Wenn Sie keine öffentliche IP-Adresse verwenden, ist der Server nur innerhalb Ihres Produktionsnetzwerks verfügbar. Um eine öffentliche IP-Adresse verwenden zu können, müssen Sie den Zugriff auf das Internet ermöglichen. Die öffentliche IP-Adresse wird angezeigt, nachdem Sie die Konfiguration abgeschlossen haben. Standardmäßig ist der TCP-Port 443 für eingehende Verbindungen geöffnet.
RPO-Grenzwert	deaktiviert	Der RPO-Grenzwert definiert also das

festlegen		maximal erlaubte Zeitintervall, das zwischen dem letzten Recovery-Punkt und dem aktuellen Zeitpunkt (an dem es zu einem Desaster kommen kann) zulässig ist. Der Wert kann zwischen 15–60 Minuten, 1–24 Stunden oder 1–14 Tagen eingestellt werden.

Cloud-Netzwerk-Infrastruktur

Die Cloud-Netzwerkinfrastruktur besteht aus dem VPN-Gateway auf der Cloud-Site und den Cloud-Netzwerken, mit denen die Recovery-Server verbunden sind.

Hinweis
Bei der Anwendung eines Disaster Recovery-Schutzplans wird nur dann eine Disaster-Recovery-Cloud-Netzwerkinfrastruktur erstellt, wenn diese noch nicht vorhanden ist. Bereits vorhandene Cloud-Netzwerke werden weder verändert noch neu erstellt.

Das System überprüft die IP-Adressen der Geräte und erstellt dann automatisch geeignete Cloud-Netzwerke, wenn es noch keine Cloud-Netzwerke gibt, zu denen eine IP-Adresse passen würden. Wenn bei Ihnen bereits Cloud Netzwerke vorhanden sind, zu denen die IP-Adressen der Recovery-Server passen, werden die vorhandenen Cloud-Netzwerke weder geändert noch neu erstellt.

- Wenn noch keine Cloud-Netzwerke vorhanden sind oder Sie die Disaster Recovery-Konfiguration zum ersten Mal einrichten, werden die Cloud-Netzwerke mit den maximalen IP-Bereichen erstellt, die von der IANA für den privaten Gebrauch empfohlen werden (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16) – basierend auf dem IP-Adressbereich Ihrer Geräte. Sie können Ihr Netzwerk eingrenzen, indem Sie die Netzwerkmaske bearbeiten.
- Wenn Sie Geräte in mehreren lokalen Netzwerken haben, wird das Netzwerk auf der Cloud-Site zu einer Obermenge der lokalen Netzwerke. Sie können die Netzwerke im Bereich **Verbindung** auch rekonfigurieren. Siehe '"Netzwerke verwalten" (S. 836)'.
- Wenn Sie eine Site-to-Site-OpenVPN-Verbindung einrichten müssen, laden Sie die VPN-Appliance herunter und richten Sie diese ein. Siehe '"Eine Site-to-Site-OpenVPN-Verbindung konfigurieren" (S. 827)'. Stellen Sie sicher, dass die Bereiche Ihrer Cloud-Netzwerke zu den Bereichen Ihres lokalen Netzwerks passen, das mit der VPN-Appliance verbunden ist.
- Wenn Sie die Standard-Netzwerkkonfiguration ändern wollen, müssen Sie im Disaster Recovery-Modul des Schutzplans auf den Link **Zu 'Verbindung' gehen** klicken oder zu **Disaster Recovery** –> **Verbindung** gehen.

Verbindungen einrichten

In diesem Abschnitt werden die erforderlichen Netzwerkkonzepte erläutert, um Ihnen die Funktionsprinzipien von Cyber Disaster Recovery Cloud zu verdeutlichen. Dabei werden Sie lernen, wie Sie – abhängig von Ihren Anforderungen – verschiedene Arten von Verbindungen zur Cloud-Site

konfigurieren können. Und abschließend erfahren Sie, wie Sie Ihre Netzwerke in der Cloud sowie die Einstellungen der VPN-Appliance und des VPN-Gateways verwalten können.

Netzwerkkonzepte

Hinweis
In Abhängigkeit davon, welches Lizenzierungsmodell angewendet wird, kann für einige Funktionen eine zusätzliche Lizenzierung erforderlich sein.

Mit Cyber Disaster Recovery Cloud können Sie folgende Verbindungstypen zur Cloud-Site definieren:

- **'Nur Cloud'-Modus**

  Diese Verbindungstyp erfordert keine Bereitstellung der VPN-Appliance am lokalen Standort.

  Die lokalen und Cloud-Netzwerke sind unabhängige Netzwerke. Diese Verbindungstyp bedingt entweder, dass alle geschützten Server des lokalen Standorts per Failover in die Cloud umgeschaltet werden – oder einen partiellen Failover von unabhängigen Servern, die nicht mit dem lokalen Standort kommunizieren müssen.

  Die Cloud Server in der Cloud-Site sind über die Point-to-Site-VPN-Verbindung und über öffentliche IP-Adressen (sofern zugewiesen) zugänglich.
- **Site-to-Site-OpenVPN-Verbindung**

  Diese Verbindungstyp erfordert eine Bereitstellung der VPN-Appliance am lokalen Standort.

  Mit der Site-to-Site-OpenVPN-Verbindung können Sie Ihre Netzwerke in die Cloud erweitern und die IP-Adressen beibehalten.

  Ihr lokaler Standort ist über einen sicheren VPN-Tunnel mit der Cloud-Site verbunden. Diese Verbindungstyp ist geeignet, wenn Sie stark voneinander abhängige Server am lokalen Standort vorliegen haben (wie z.B. ein Webserver und ein Datenbankserver). Bei einem partiellen Failover, wenn beispielsweise einer dieser Server auf der Cloud-Site neu erstellt wird, während der andere am lokalen Standort verbleibt, können diese dennoch weiter über einen VPN-Tunnel miteinander kommunizieren.

  Die Cloud Server in der Cloud-Site sind über das lokale Netzwerk, über die Point-to-Site-VPN-Verbindung und über öffentliche IP-Adressen (sofern zugewiesen) zugänglich.
- **Multi-Site-IPsec-VPN-Verbindung**

  Dieser Verbindungstyp erfordert ein lokales VPN-Gerät, welches den Standard IPsec IKE v2 unterstützt.

  Wenn Sie mit der Konfiguration der Multi-Site-IPsec-VPN-Verbindung beginnen, wird Cyber Disaster Recovery Cloud automatisch ein Cloud-VPN-Gateway mit einer öffentlichen IP-Adresse erstellen.

  Mit einer Multi-Site-IPsec-VPN-Konnektivität werden Ihre lokalen Standorte über einen sicheren IPsec-VPN-Tunnel mit der Cloud-Site verbunden.

Dieser Verbindungstyp eignet sich für Disaster Recovery-Szenarien, wenn Sie einen oder mehrere lokale Standorte haben, die geschäftskritische Workloads oder stark voneinander abhängige Services hosten.

Bei einem partiellen Failover von einem der Server wird dieser auf der Cloud-Site neu erstellt, während die anderen am lokalen Standort verbleiben. Dabei können die Server weiterhin über einen IPsec-VPN-Tunnel miteinander kommunizieren.

Bei einem partiellen Failover von einem der lokalen Standorte bleiben die übrigen lokalen Standorte weiterhin funktionsfähig und können weiterhin über einen IPsec-VPN-Tunnel miteinander kommunizieren.

- **Point-to-Site-VPN-Remote-Zugriff**

  Ein sicherer Point-to-Site-Remote-VPN-Zugriff auf Ihre Cloud-Site und die Workloads am lokalen Standort von außen über Ihr Endpunkgerät.

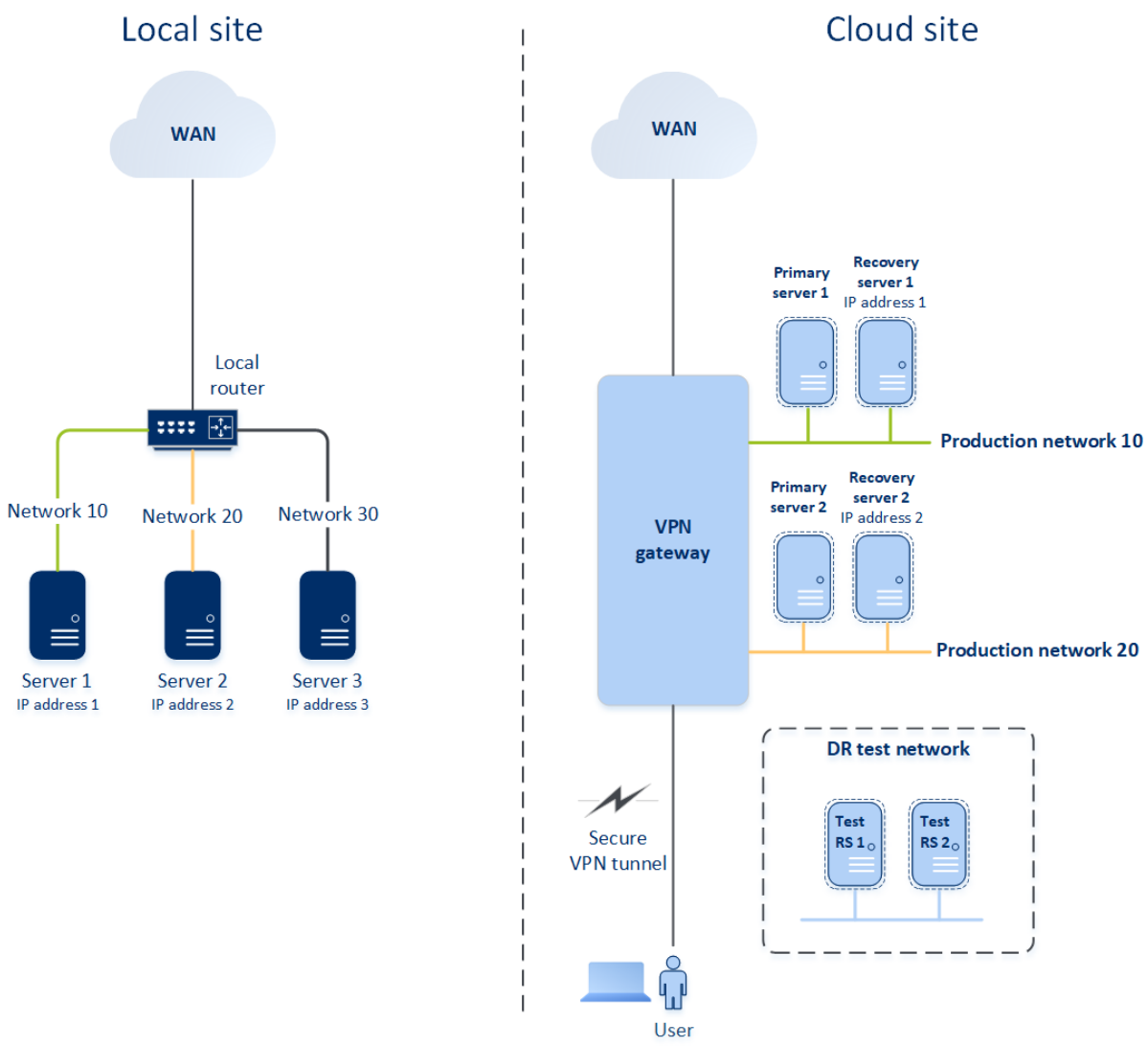
  Für den Zugriff auf einen lokalen Standort erfordert dieser Verbindungstyp eine Bereitstellung der VPN-Appliance am lokalen Standort.

'Nur Cloud'-Modus

Der 'Nur Cloud'-Modus erfordert keine Bereitstellung der VPN-Appliance am lokalen Standort. Er setzt voraus, dass Sie über zwei unabhängige Netzwerke verfügen: eines am lokalen Standort und ein anderes in der Cloud-Site. Das Routing erfolgt mit dem Router in der Cloud-Site.

So funktioniert Routing

Wenn der 'Nur Cloud'-Modus aktiviert ist, wird das Routing mit dem Router auf der Cloud-Site durchgeführt, sodass die Server aus verschiedenen Cloud-Netzwerken miteinander kommunizieren können.



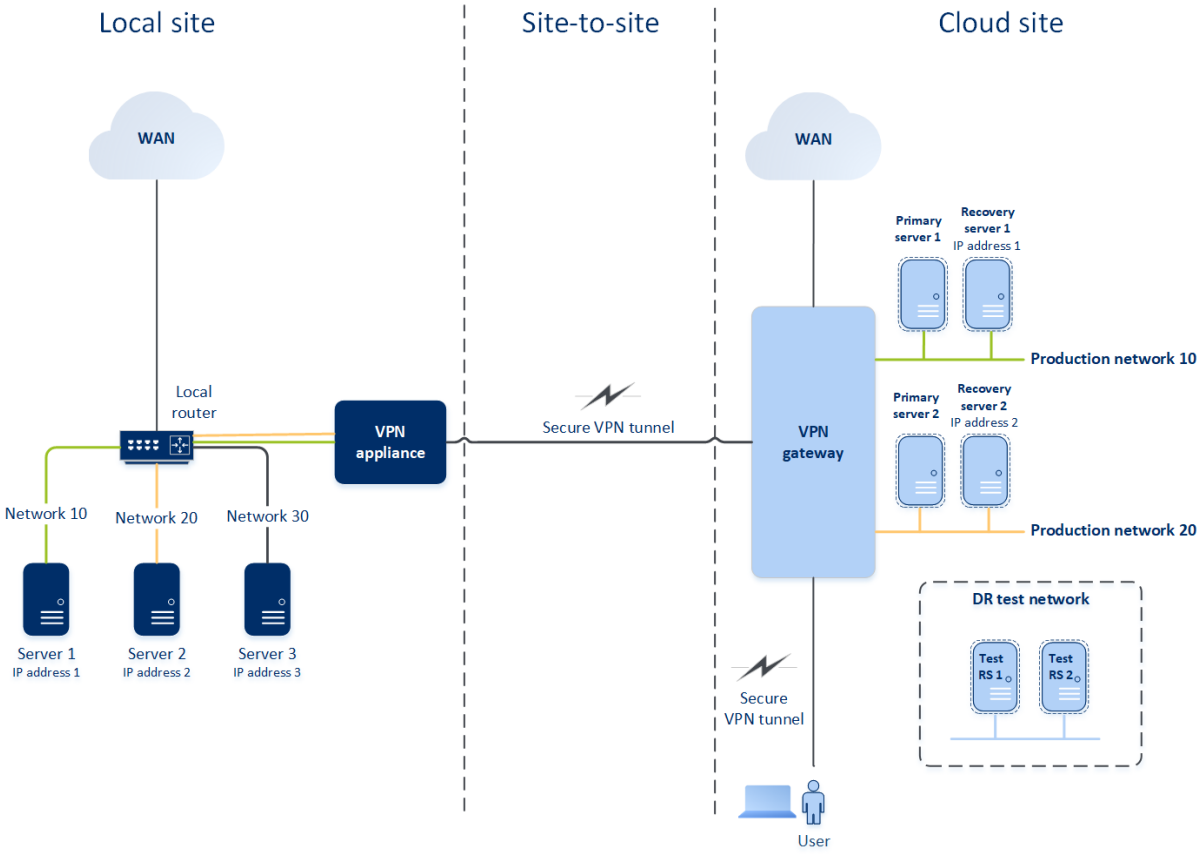
Site-to-Site-OpenVPN-Verbindung

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Um zu verstehen, wie die Vernetzung in Cyber Disaster Recovery Cloud funktioniert, werden wir einen Anwendungsfall betrachten, bei dem Sie drei Netzwerke mit jeweils einer Maschine am lokalen Standort verwenden. Sie werden für zwei Netzwerke – Netzwerk 10 und Netzwerk 20 genannt – einen Schutz vor Desastern konfigurieren.

In der nachfolgenden Abbildung sehen Sie den lokalen Standort, wo Ihre Maschinen gehostet werden, sowie die Cloud-Site, wo die Cloud Server gestartet werden, falls es zu einem Desaster kommt.

Die Cyber Disaster Recovery Cloud-Lösung ermöglicht es Ihnen, alle Workloads von beschädigten Maschinen, die sich an Ihrem lokalen Standort befinden, per Failover zu Cloud Servern in der Cloud umzuschalten. Sie können bis zu 23 Netzwerke mit Cyber Disaster Recovery Cloud schützen.



Um eine Site-to-Site-OpenVPN-Kommunikation zwischen dem lokalen Standort und der Cloud-Site aufzubauen, werden eine **VPN-Appliance** und ein **VPN-Gateway** verwendet. Wenn Sie mit der Konfiguration der Site-to-Site-OpenVPN-Verbindung in der Cyber Protect-Konsole beginnen, wird das VPN-Gateway automatisch in der Cloud-Site bereitgestellt. Anschließend müssen Sie die VPN-Appliance an Ihrem lokalen Standort bereitstellen, die zu schützenden Netzwerke hinzufügen und die Appliance in der Cloud registrieren. Cyber Disaster Recovery Cloud erstellt dann ein Replikat Ihres lokalen Netzwerks in der Cloud. Es wird ein sicherer VPN-Tunnel zwischen der VPN-Appliance und dem VPN-Gateway aufgebaut. Dadurch wird die Erweiterung Ihres lokalen Netzwerks in die Cloud bereitgestellt. Die Produktionsnetzwerke in der Cloud werden mit Ihren lokalen Netzwerken verknüpft. Die lokalen Server und Cloud Server können über den VPN-Tunnel so kommunizieren, als würden sie sich alle im selben Ethernet-Segment befinden. Das Routing erfolgt mit Ihrem lokalen Router.

Für jede zu schützende Quellmaschine müssen Sie einen Recovery-Server in der Cloud-Site erstellen. Dieser verbleibt solange im **Standby**-Stadium, bis es zu einem Failover-Ereignis kommt. Wenn es zu einem Desaster kommt und Sie einen Failover-Prozess starten (im **Produktionsmodus**), wird der Recovery-Server, der eine exakte Kopie Ihrer geschützten Maschine darstellt, in der Cloud ausgeführt. Ihm kann die gleiche IP-Adresse zugewiesen werden, die die Quellmaschine hat, und er

kann im selben Ethernet-Segment ausgeführt werden. Ihre Clients können wie gewohnt weiter mit dem Server arbeiten, ohne irgendwelche der im Hintergrund erfolgten Änderungen zu bemerken.

Sie können einen Failover-Prozess auch im **Testmodus** starten. Das bedeutet, dass die Quellmaschine weiter arbeitet und gleichzeitig der entsprechende Recovery-Server mit der gleichen IP-Adresse in der Cloud gestartet wird. Um IP-Adresskonflikte zu vermeiden, wird in der Cloud ein spezielles virtuelles Netzwerk erstellt – **Testnetzwerk** genannt. Das Testnetzwerk ist isoliert, um zu verhindern, dass die IP-Adresse der Quellmaschine im selben Ethernet-Segment doppelt vorkommt. Um auf den Recovery-Server im Test-Failover-Modus zugreifen zu können, müssen Sie dem Recovery-Server bei dessen Erstellung eine **Test-IP-Adresse** zuweisen. Weitere Parameter, die Sie für den Recovery-Server spezifizieren können, werden in entsprechenden Abschnitten weiter unten betrachtet.

So funktioniert Routing

Bei einer Site-to-Site-Verbindung wird das Routing zwischen den Cloud-Netzwerken mit Ihrem lokalen Router durchgeführt. Der VPN-Server führt kein Routing zwischen den Cloud-Servern durch, die sich in verschiedenen Cloud-Netzwerken befinden. Wenn ein Cloud-Server aus einem Netzwerk mit einem Server aus einem anderen Cloud-Netzwerk kommunizieren möchte, geht der Datenverkehr durch den VPN-Tunnel zum lokalen Router am lokalen Standort. Anschließend wird der Datenverkehr vom lokalen Router in ein anderes Netzwerk weitergeleitet und geht durch den Tunnel zurück zum Zielserver auf der Cloud-Site.

VPN-Gateway

Die Hauptkomponente, die die Kommunikation zwischen dem lokalen Standort und der Cloud-Site ermöglicht, ist das **VPN-Gateway**. Dabei handelt sich um eine virtuelle Maschine in der Cloud, auf welcher eine spezielle Software installiert und das Netzwerk in spezieller Weise konfiguriert ist. Das VPN-Gateway hat folgende Funktionen:

- Es verbindet die Ethernet-Segmente Ihres lokalen Netzwerks und des Produktionsnetzwerks in der Cloud im L2-Modus.
- Es stellt iptables- und ebtables-Regeln bereit.
- Es fungiert als Standardrouter und NAT für die Maschinen in den Test- und Produktionsnetzwerken.
- Es fungiert als DHCP-Server. Alle Maschinen in den Produktions- und Testnetzwerken erhalten ihre Netzwerkkonfiguration (IP-Adressen, DNS-Einstellungen) per DHCP. Ein Cloud-Server erhält jedes Mal die gleiche IP-Adresse vom DHCP-Server. Wenn Sie die benutzerdefinierte DNS-Konfiguration einrichten müssen, sollten Sie sich an Ihr Support-Team wenden.
- Es fungiert als DNS-Cache.

Netzwerkkonfiguration des VPN-Gateways

Das VPN-Gateway hat mehrere Netzwerkschnittstellen:

- Eine externe Schnittstelle, die mit dem Internet verbunden ist
- Produktionsschnittstellen, die mit den Produktionsnetzwerken verbunden sind
- Eine Testschnittstelle, die mit dem Testnetzwerk verbunden ist

Darüber hinaus werden zwei virtuelle Schnittstellen für Point-to-Site- und Site-to-Site-Verbindungen hinzugefügt.

Wenn das VPN-Gateway bereitgestellt und initialisiert wird, werden die Brücken erstellt: eine für die externe Schnittstelle und eine für die Client- und Produktionsschnittstellen. Obwohl die Client-Produktionsbrücke und die Testschnittstelle die gleichen IP-Adressen verwenden, kann das VPN-Gateway die Datenpakete mithilfe einer bestimmten Technik korrekt weiterleiten.

VPN-Appliance

Die **VPN-Appliance** ist eine virtuelle Maschine am lokalen Standort, auf der Linux und eine spezielle Software installiert ist und die über eine spezielle Netzwerkkonfiguration verfügt. Sie ermöglicht die Kommunikation zwischen dem lokalen Standort und der Cloud-Site.

Recovery-Server

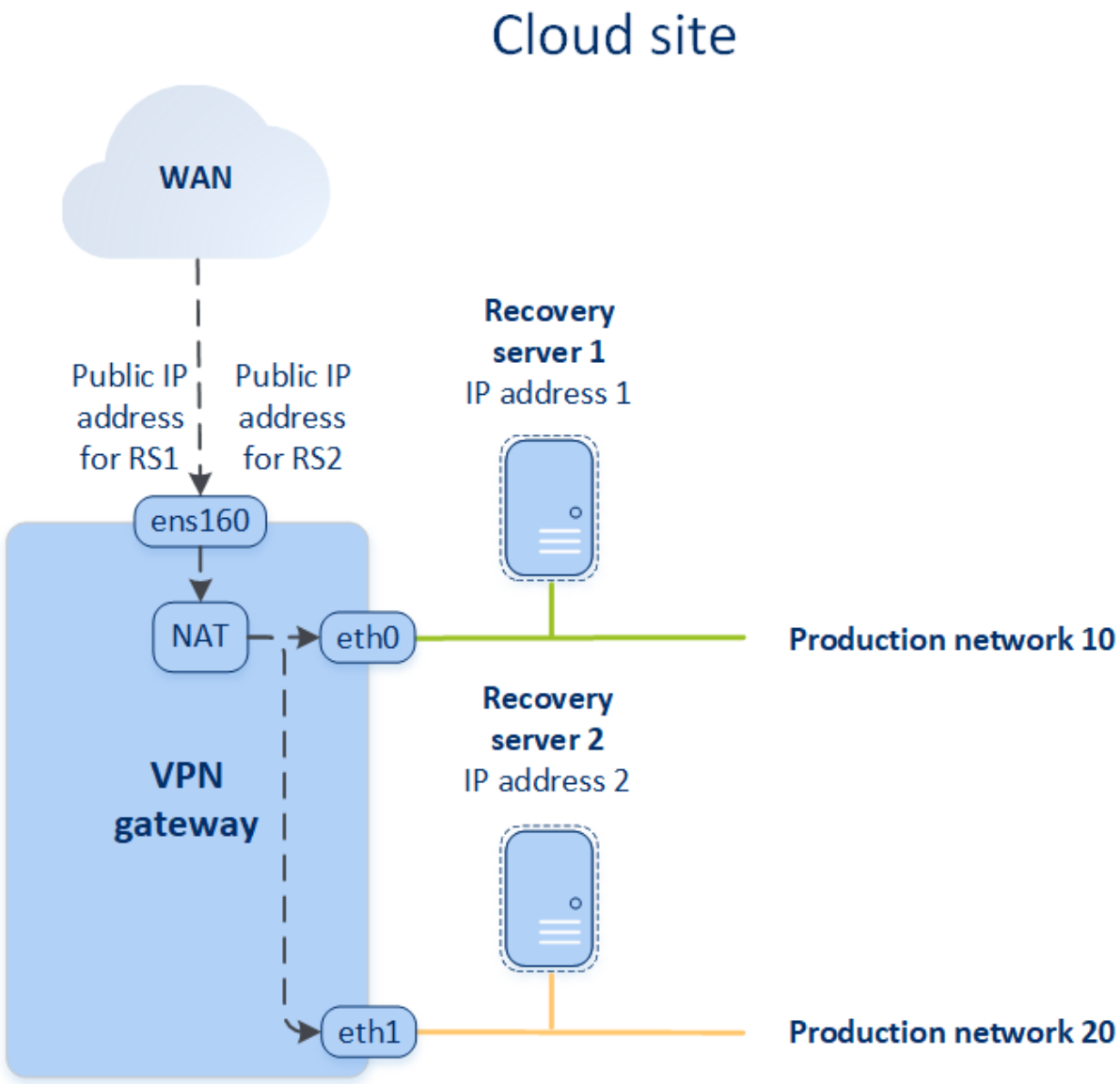
Ein **Recovery-Server** – ist das VM-Replikat einer ursprünglichen Maschine, das auf den (in der Cloud gespeicherten) Backups eines geschützten Servers basiert. Recovery-Server werden verwendet, um bei einem Desaster die Workloads der ursprünglichen Server in die Cloud umschalten zu können.

Wenn Sie einen Recovery-Server erstellen, müssen Sie folgende Netzwerkparameter spezifizieren:

- **Cloud-Netzwerk** (erforderlich): das Cloud-Netzwerk, mit dem der Recovery-Server verbunden wird.
- **IP-Adresse im Produktionsnetzwerk** (erforderlich): die IP-Adresse, mit der die virtuelle Maschine des Recovery-Servers gestartet wird. Diese Adresse wird in den Produktions- und Testnetzwerken verwendet. Die virtuelle Maschine wird vor dem Starten so konfiguriert, dass sie ihre IP-Adresse per DHCP erhält.
- **Test-IP-Adresse** (optional): eine IP-Adresse, um beim Test-Failover vom Client-Produktionsnetzwerk aus auf den Recovery-Server zugreifen zu können. Dadurch wird verhindert, dass die Produktions-IP-Adresse innerhalb desselben Netzwerks doppelt verwendet wird. Diese IP-Adresse unterscheidet sich von der IP-Adresse im Produktionsnetzwerk. Die Server am lokalen Standort können den Recovery-Server während des Test-Failovers über die Test-IP-Adresse erreichen, während in umgekehrter Richtung jedoch kein Zugriff nicht möglich ist. Der Recovery-Server im Testnetzwerk kann auf das Internet zugreifen, wenn bei der Erstellung des Recovery-Servers die Option **Internetzugriff** ausgewählt wurde.
- **Öffentliche IP-Adresse** (optional): eine IP-Adresse, um aus dem Internet auf den Recovery-Server zugreifen zu können. Wenn ein Server keine öffentliche IP-Adresse hat, ist er nur aus dem lokalen Netzwerk erreichbar.
- **Internetzugriff** (optional): diese Option ermöglicht dem Recovery-Server, auf das Internet zuzugreifen (gilt bei Produktions- und Test-Failovers).

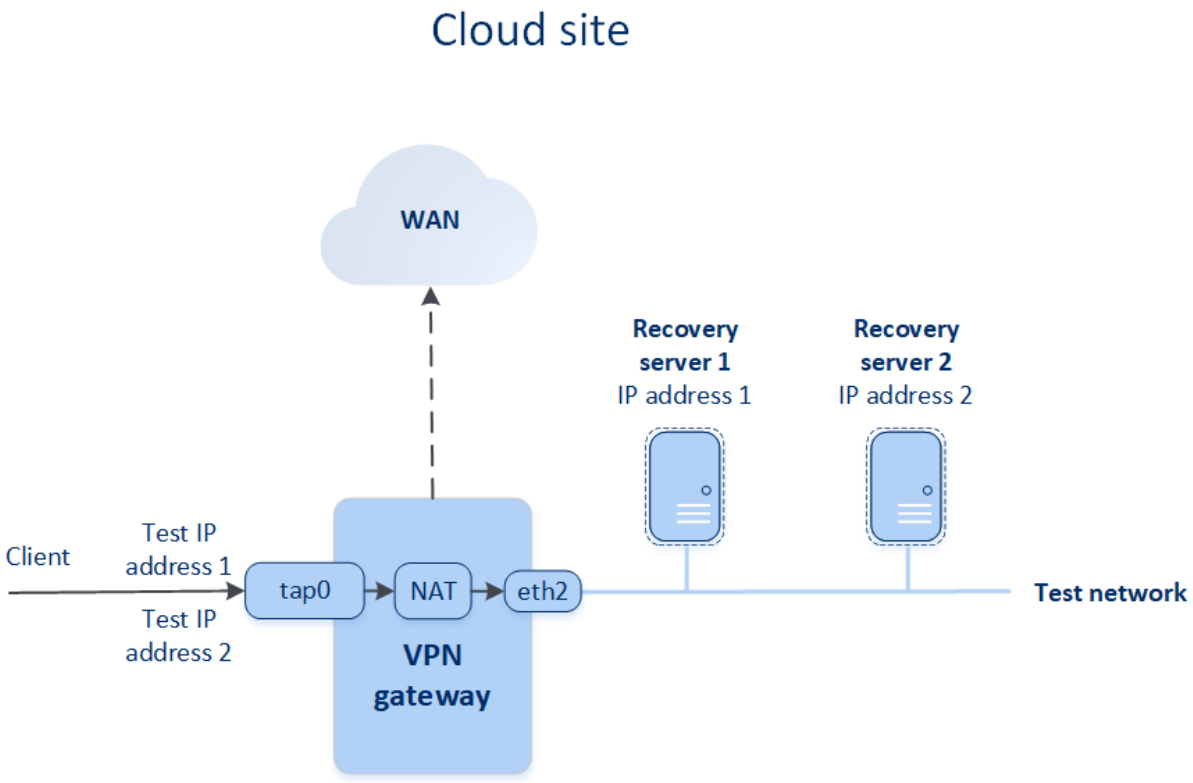
Öffentliche und Test-IP-Adresse

Wenn Sie einem Recovery-Server bei dessen Erstellung eine öffentliche IP-Adresse zuweisen, kann auf den Server über diese IP-Adresse aus dem Internet zugriffen werden. Wenn ein Datenpaket aus dem Internet mit der öffentlichen Ziel-IP-Adresse ankommt, wird das VPN-Gateway das Datenpaket per NAT der jeweiligen Produktions-IP-Adresse zuordnen und es dann an den entsprechenden Recovery-Server weitersenden.



Wenn Sie einem Recovery-Server bei dessen Erstellung eine Test-IP-Adresse zuweisen, kann auf den Server innerhalb des Testnetzwerks über diese IP-Adresse zugriffen werden. Wenn Sie den Test-Failover durchführen, wird die ursprüngliche Maschine weiter ausgeführt – während der Recovery-Server mit der gleichen IP-Adresse im Testnetzwerk in der Cloud gestartet wird. Es kommt jedoch zu keinem IP-Adresskonflikt, weil das Testnetzwerk isoliert ist. Die Recovery-Server im Testnetzwerk

sind über ihre Test-IP-Adressen erreichbar, die per NAT den Produktions-IP-Adressen zugeordnet werden.



Weitere Informationen zu Site-to-Site-OpenVPN finden Sie unter '"Site-to-Site-OpenVPN – Zusätzliche Informationen" (S. 203)'.

Primäre Server

Ein **primärer Server** ist eine virtuelle Maschine, die (im Vergleich zu einem Recovery-Server) keine verknüpfte Maschine am lokalen Standort hat. Primäre Server werden zum Schutz einer Applikation durch Replikation oder zur Ausführung verschiedener Hilfsdienste (z.B. als Webserver) verwendet.

Ein primärer Server wird üblicherweise verwendet, um Echtzeit-Datenreplikationen zwischen Servern durchzuführen, die wichtige Applikationen ausführen. Sie richten die Replikation selbst ein, indem Sie die internen Tools der jeweiligen Applikation verwenden. Beispielsweise kann eine Active Directory- oder SQL-Replikation zwischen lokalen Servern und dem primären Server konfiguriert werden.

Alternativ kann ein primärer Server auch in eine AlwaysOn-Verfügbarkeitsgruppe (AAG) oder Datenbankverfügbarkeitsgruppen (DAG) aufgenommen werden.

Beide Methoden erfordern weitreichende Kenntnisse der jeweiligen Applikation und Administratorrechte. Ein primärer Server verbraucht fortlaufend Computing-Ressourcen (Berechnungspunkte) und benötigt Speicherplatz im schnellen Disaster Recovery Storage. Zudem sind gewisse Wartungsaktivitäten auf Ihrer Seite erforderlich: Überwachung der Replikation, Installation von Software-Updates und Durchführung von Backups. Die Vorteile sind minimale RPOs

und RTOs bei minimaler Belastung der Produktionsumgebung (im Vergleich zum Backup kompletter Server in der Cloud).

Primäre Server werden immer nur im Produktionsnetzwerk gestartet. Sie verfügen über folgende Netzwerkparameter:

- **Cloud-Netzwerk** (erforderlich): das Cloud-Netzwerk, mit dem ein primärer Server verbunden wird.
- **IP-Adresse im Produktionsnetzwerk** (erforderlich): die IP-Adresse, die der primäre Server im Produktionsnetzwerk haben wird. Als Standardeinstellung wird die erste freie IP-Adresse aus Ihrem Produktionsnetzwerk verwendet.
- **Öffentliche IP-Adresse** (optional): eine IP-Adresse, um aus dem Internet auf einen primären Server zugreifen zu können. Wenn ein Server keine öffentliche IP-Adresse hat, ist er nur aus dem lokalen Netzwerk und nicht über das Internet erreichbar.
- **Internetzugriff** (optional): diese Option ermöglicht es einem primären Server, auf das Internet zuzugreifen.

Multi-Site-IPsec-VPN-Verbindung

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Sie können die Multi-Site-IPsec-VPN-Konnektivität verwenden, um einen einzelnen oder mehrere lokale Standorte über eine sichere L3-IPsec-VPN-Verbindung mit der Cyber Disaster Recovery Cloud zu verbinden.

Dieser Verbindungstyp ist für Disaster Recovery-Szenarien nützlich, wenn Sie einen der folgenden Anwendungsfälle haben:

- Sie haben einen lokalen Standort, der geschäftskritische Workloads hostet.
- Sie haben mehrere lokale Standorte, die geschäftskritische Workloads hosten (z.B. Büros an verschiedenen Standorten).
- Sie verwenden Stand- bzw. Speicherorte, die auf Software von Drittanbietern basieren, oder Stand- bzw. Speicherorte von Managed Service Providern – und sind mit diesen über einen IPsec-VPN-Tunnel verbunden.

Um eine Multi-Site-IPsec-VPN-Kommunikation zwischen den lokalen Standorten und der Cloud-Site aufzubauen, wird ein **VPN-Gateway** verwendet. Wenn Sie mit der Konfiguration der Multi-Site-IPsec-VPN-Verbindung in der Cyber Protect-Konsole beginnen, wird das VPN-Gateway automatisch in der Cloud-Site bereitgestellt. Sie sollten die Cloud-Netzwerksegmente konfigurieren und dabei sicherstellen, dass sich diese nicht mit den lokalen Netzwerksegmenten überlappen. Ein sicherer VPN-Tunnel wird zwischen den lokalen Standorten und der Cloud-Site aufgebaut. Die lokalen Server und Cloud Server können über den VPN-Tunnel so kommunizieren, als würden sie sich alle im selben Ethernet-Segment befinden.

Für jede zu schützende Quellmaschine müssen Sie einen Recovery-Server in der Cloud-Site erstellen. Dieser verbleibt solange im **Standby**-Stadium, bis es zu einem Failover-Ereignis kommt. Wenn es zu einem Desaster kommt und Sie einen Failover-Prozess starten (im **Produktionsmodus**), wird der Recovery-Server, der eine exakte Kopie Ihrer geschützten Maschine darstellt, in der Cloud ausgeführt. Ihre Clients können wie gewohnt weiter mit dem Server arbeiten, ohne irgendwelche der im Hintergrund erfolgten Änderungen zu bemerken.

Sie können einen Failover-Prozess auch im **Testmodus** starten. Das bedeutet, dass die Quellmaschine weiterhin arbeitet und gleichzeitig der entsprechende Recovery-Server in der Cloud in einem speziellen virtuellen Netzwerk gestartet wird, welches in der Cloud erstellt wird – ein **Testnetzwerk**. Das Testnetzwerk ist isoliert, um die Duplizierung von IP-Adressen in den anderen Cloud-Netzwerksegmenten zu verhindern.

VPN-Gateway

Die Hauptkomponente, die die Kommunikation zwischen den lokalen Standorten und der Cloud-Site ermöglicht, ist das **VPN-Gateway**. Dabei handelt sich um eine virtuelle Maschine in der Cloud, auf welcher eine spezielle Software installiert und das Netzwerk in spezieller Weise konfiguriert ist. Das VPN-Gateway stellt folgende Funktionen bereit:

- Es verbindet die Ethernet-Segmente Ihres lokalen Netzwerks und des Produktionsnetzwerks in der Cloud im L3-IPsec-Modus.
- Es fungiert als Standardrouter und NAT für die Maschinen in den Test- und Produktionsnetzwerken.
- Es fungiert als DHCP-Server. Alle Maschinen in den Produktions- und Testnetzwerken erhalten ihre Netzwerkkonfiguration (IP-Adressen, DNS-Einstellungen) per DHCP. Ein Cloud-Server erhält jedes Mal die gleiche IP-Adresse vom DHCP-Server.

  Wenn Sie es bevorzugen, können Sie auch eine benutzerdefinierte DNS-Konfiguration einrichten. Weitere Informationen finden Sie im Abschnitt '"Benutzerdefinierte DNS-Server konfigurieren" (S. 845)'.
- Es fungiert als DNS-Cache.

So funktioniert Routing

Das Routing zwischen den Cloud-Netzwerken wird mit dem Router auf der Cloud-Site durchgeführt, sodass die Server aus verschiedenen Cloud-Netzwerken miteinander kommunizieren können.

Point-to-Site-VPN-Remote-Zugriff

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

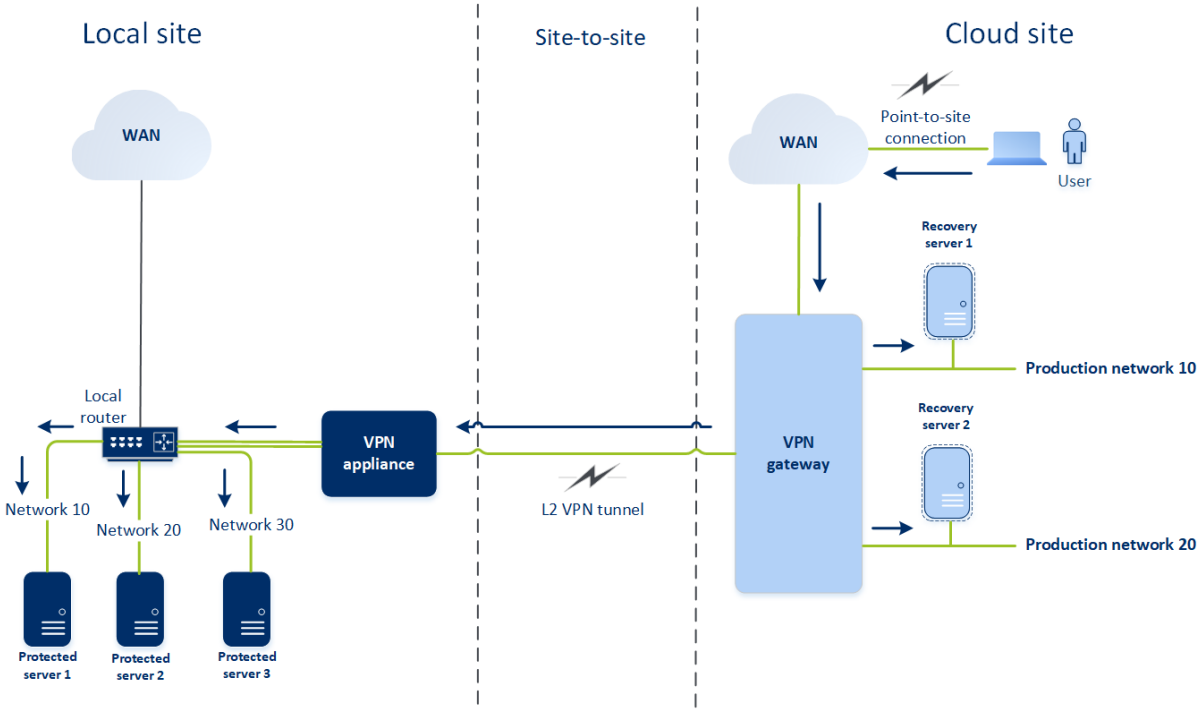
Die Point-to-Site-Verbindung ist eine sichere, von außen kommende Verbindung von einem Ihrer Endgeräte (z.B. einem Desktop-Computer oder Laptop) über ein VPN zu einem lokalen Standort und

einer Cloud-Site. Sie ist verfügbar, nachdem Sie eine Site-to-Site-OpenVPN-Verbindung zur Cyber Disaster Recovery Cloud-Site aufgebaut haben. Diese Art der Verbindung ist in folgenden Fällen nützlich:

- In vielen Unternehmen sind die Unternehmensdienste und Webressourcen nur über das Unternehmensnetzwerk verfügbar. Sie können die Point-to-Site-Verbindung verwenden, um sich sicher mit dem lokalen Standort zu verbinden.
- Bei einem Desaster, wenn Workloads in die Cloud-Site umgeschaltet werden und Ihr lokales Netzwerk ausgefallen ist, benötigen Sie möglicherweise direkten Zugriff auf Ihre Cloud Server. Die ist über die Point-to-Site-Verbindung zur Cloud-Site möglich.

Für die Point-to-Site-Verbindung zum lokalen Standort müssen Sie die VPN-Appliance am lokalen Standort installieren, dann die Site-to-Site-Verbindung konfigurieren und anschließend die Point-to-Site-Verbindung zum lokalen Standort. Auf diese Weise haben Ihre Remote-Mitarbeiter über ein Layer-2-VPN (L2-VPN) Zugriff auf das Unternehmensnetzwerk.

Das unten stehende Schema zeigt den lokalen Standort, die Cloud-Site und die Kommunikationen zwischen den Servern (grün markiert). Der L2-VPN-Tunnel verbindet Ihren lokalen Standort und die Cloud-Site. Wenn ein Benutzer eine Point-to-Site-Verbindung aufbaut, erfolgen die Kommunikationen mit dem lokalen Standort über die Cloud-Site.



Eine Point-to-Site-Konfiguration verwendet Zertifikate zur Authentifizierung gegenüber dem VPN-Client. Und zudem werden auch noch Anmeldedaten für die Authentifizierung verwendet. Beachten Sie folgende Hinweise zu Point-to-Site-Verbindungen mit dem lokalen Standort:

- Die Benutzer sollten Ihre Cyber Protect Cloud-Anmeldedaten verwenden, um sich im VPN-Client zu authentifizieren. Sie müssen entweder die Rolle 'Firmenadministrator' oder 'Cyber Protection' haben.

- Wenn Sie die OpenVPN-Konfiguration neu generieren, müssen Sie die aktualisierte Konfiguration allen Benutzern zur Verfügung stellen, die die Point-to-Site-Verbindung zur Cloud-Site verwenden.

Automatisches Löschen einer ungenutzten Kundenumgebung auf der Cloud-Site

Der Disaster Recovery Service überwacht die Nutzung der Kundenumgebungen, die für Disaster Recovery-Zwecke erstellt wurden, und löscht diese automatisch, wenn sie nicht verwendet werden.

Folgende Kriterien werden verwendet, um zu definieren, ob ein Kunden-Mandant aktiv ist:

- Es gibt aktuell mindestens einen Cloud Server – oder es gab einen (oder mehrere) Cloud Server in den letzten sieben Tagen.

  ODER

- Die Option **VPN-Zugriff auf den lokalen Standort** aktiviert und entweder ist der Site-to-Site-OpenVPN-Tunnel aufgebaut oder von der VPN-Appliance werden Daten für die letzten 7 Tage gemeldet.

Alle übrigen Mandanten werden als inaktive Mandanten betrachtet. Für solche Mandanten führt das System folgende Aktionen aus:

- Das VPN-Gateway wird gelöscht und alle Cloud-Ressourcen, die zu dem Mandanten gehören.
- Die Registrierung der VPN-Appliance wird aufgehoben.

Die inaktiven Mandanten werden auf ihr Stadium zurückversetzt, bevor die Verbindung konfiguriert wurde.

Grundsätzliche Verbindungskonfiguration

In diesem Abschnitt werden verschiedene Szenarien für die Verbindungskonfiguration beschrieben.

Den 'Nur Cloud'-Modus konfigurieren

So können Sie eine Verbindung im 'Nur Cloud'-Modus konfigurieren

1. Gehen Sie in der Cyber Protect-Konsole zu **Disaster Recovery** –> **Verbindung**.
2. Wählen Sie **Nur Cloud** und klicken Sie dann auf **Konfigurieren**.
   Als Ergebnis wird das VPN-Gateway und Cloud-Netzwerk mit der definierten Adresse und Netzwerkmaske auf der Cloud-Site bereitgestellt.

Informationen zur Verwaltung Ihrer Netzwerke in der Cloud und zur Konfiguration der VPN-Gateway-Einstellungen finden Sie im Abschnitt 'Cloud-Netzwerke verwalten'.

Eine Site-to-Site-OpenVPN-Verbindung konfigurieren

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Anforderungen für die VPN-Appliance

Systemanforderungen

- 1 CPUs
- 1 GB RAM
- 8 GB Festplattenspeicherplatz

Ports

- TCP 443 (ausgehend) – für VPN-Verbindungen
- TCP 80 (ausgehend) – für automatische Updates der Appliance

Stellen Sie sicher, dass Ihre Firewalls und anderen Komponenten des Netzwerk-Sicherheitssystems Verbindungen zu allen IP-Adressen über diese Ports zulassen.

Eine Site-to-Site-OpenVPN-Verbindung konfigurieren

Die VPN-Appliance erweitert Ihr lokales Netzwerk (LAN) über einen sicheren VPN-Tunnel in die Cloud. Eine solche Verbindung wird oft auch als Site-to-Site-Verbindung (S2S) bezeichnet. Sie können die nachfolgende Prozedur befolgen oder sich das Video-Tutorial ansehen.

So können Sie eine Verbindung über die VPN-Appliance konfigurieren

1. Gehen Sie in der Cyber Protect-Konsole zu **Disaster Recovery** –> **Verbindung**.
2. Wählen Sie **Site-to-Site-OpenVPN-Verbindung** aus und klicken Sie dann auf **Konfigurieren**.
   Das System beginnt damit, das VPN-Gateway in der Cloud bereitzustellen. Dies wird einige Zeit benötigen. Währenddessen können Sie zum nächsten Schritt weitergehen.

   Hinweis
   Das VPN-Gateway wird kostenlos bereitgestellt. Er wird gelöscht, wenn die Disaster Recovery-Funktionalität nicht verwendet wird (d.h., wenn sieben Tage lang kein primärer oder Recovery-Server in der Cloud vorhanden ist).

3. Klicken Sie im Block **VPN-Appliance** auf den Befehl **Herunterladen und bereitstellen**. Laden Sie je nach der von Ihnen verwendeten Virtualisierungsplattform die entsprechende VPN-Appliance für VMware vSphere oder Microsoft Hyper-V herunter.
4. Stellen Sie die Appliance bereit und verbinden Sie diese mit den Produktionsnetzwerken.

Überprüfen Sie in vSphere, dass für alle virtuellen Switche, die die VPN-Appliance mit den Produktionsnetzwerken verbinden, die Optionen **Promiscuous-Modus** und **Gefälschte Übertragungen** aktiviert sind und auf **Akzeptieren** eingestellt ist. Sie können im vSphere Client mit folgender Befehlssequenz auf diese Einstellungen zugreifen: Host auswählen –> **Übersicht** –> **Netzwerk** –> den Switch auswählen –> **Einstellungen bearbeiten...** > **Sicherheit**.

Erstellen Sie in Hyper-V eine virtuelle Maschine der **Generation 1** mit 1,024 MB Arbeitsspeicher. Wir empfehlen außerdem, dass Sie für diese Maschine die Option **Dynamischer Arbeitsspeicher** aktivieren. Gehen Sie, sobald die Maschine erstellt wurde, zu **Einstellungen** –> **Hardware** –> **Netzwerkkarte** –> **Erweiterte Features** – und aktivieren Sie dort das Kontrollkästchen **Spoofing von MAC-Adressen aktivieren**.

5. Schalten Sie die Appliance ein.
6. Öffnen Sie die Appliance-Konsole und melden Sie sich mit der Benutzernamen-/Kennwort-Kombination 'admin/admin' an.
7. [Optional] Ändern Sie das Kennwort.
8. [Optional] Ändern Sie bei Bedarf die Netzwerkeinstellungen. Definieren Sie, welche Schnittstelle als WAN-Schnittstelle für die Internetverbindung verwendet werden soll.
9. Registrieren Sie die Appliance im Cyber Protection Service, indem Sie die Anmeldedaten des Firmenadministrators verwenden.

   Diese Anmeldedaten werden nur einmal verwendet, um das Zertifikat abzurufen. Die Datacenter-URL ist vordefiniert.

   Hinweis
   Wenn für Ihr Konto eine Zwei-Faktor-Authentifizierung konfiguriert ist, werden Sie auch aufgefordert, den TOTP-Code einzugeben. Wenn die Zwei-Faktor-Authentifizierung aktiviert, aber für Ihr Konto nicht konfiguriert ist, können Sie die VPN-Appliance nicht registrieren. Zuerst müssen Sie zur Anmeldeseite der Cyber Protect-Konsole gehen und die Konfiguration der Zwei-Faktor-Authentifizierung für Ihr Konto abschließen. Weitere Informationen zur Zwei-Faktor-Authentifizierung finden Sie in der Management-Portal-Administrator-Anleitung.

Wenn die Konfiguration abgeschlossen wurde, zeigt die Appliance als Status '**Online**' an. Die Appliance verbindet sich mit dem VPN-Gateway und beginnt, Informationen über die Netzwerke von allen aktiven Schnittstellen an den Cyber Disaster Recovery Cloud Service zu melden. Die Cyber Protect-Konsole zeigt die Schnittstellen basierend auf den Informationen der VPN-Appliance an.

Multi-Site-IPsec-VPN konfigurieren

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Sie können eine Multi-Site-IPsec-VPN-Verbindung auf die folgenden zwei Arten konfigurieren:

- über die Registerkarte **Disaster Recovery** –> **Verbindung**.
- indem Sie einen Schutzplan auf ein oder mehrere Geräte anwenden und dann manuell von der automatisch erstellten Site-to-Site-OpenVPN-Verbindung zu einer Multi-Site-IPsec-VPN-Verbindung wechseln, anschließend die Multi-Site-IPsec-VPN-Einstellungen konfigurieren und abschließend die IP-Adressen neu zuweisen.

So können Sie eine Multi-Site-IPsec-VPN-Verbindung über die Registerkarte Verbindung konfigurieren

1. Gehen Sie in der Cyber Protect-Konsole zu **Disaster Recovery** –> **Verbindung**.
2. Klicken Sie im Bereich **Multi-Site-VPN-Verbindung** auf den Befehl **Konfigurieren**.
   Ein VPN-Gateway wird in der Cloud-Site bereitgestellt.
3. Konfigurieren Sie die Multi-Site-IPsec-VPN-Einstellungen.

So können Sie eine Multi-Site-IPsec-VPN-Verbindung über einen Schutzplan konfigurieren

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte**.
2. Wenden Sie einen Schutzplan auf ein oder mehrere Geräte aus der Liste an.
   Der Recovery-Server und die Cloud-Infrastruktur-Einstellungen werden automatisch für die Site-to-Site-OpenVPN-Verbindung konfiguriert.
3. Gehen Sie zu **Disaster Recovery** –> **Verbindung**.
4. Klicken Sie auf **Eigenschaften anzeigen**.
5. Klicken Sie auf **Zu Multi-Site-IPsec-VPN wechseln**.
6. Konfigurieren Sie die Multi-Site-IPsec-VPN-Einstellungen.
7. Weisen Sie die IP-Adressen des Cloud-Netzwerks und der Cloud Server neu zu.

Die Multi-Site-IPsec-VPN-Einstellungen konfigurieren

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Wenn Sie eine Multi-Site-IPsec-VPN-Verbindung konfiguriert haben, müssen Sie anschließend die Einstellungen für die Cloud-Site und die lokalen Standorte auf der Registerkarte **Disaster Recovery** –> **Verbindung** konfigurieren.

Voraussetzungen

- Die Multi-Site-IPsec-VPN-Konnektivität ist konfiguriert. Weitere Informationen zur Konfiguration der Multi-Site-IPsec-VPN-Konnektivität finden Sie im Abschnitt '"Multi-Site-IPsec-VPN konfigurieren" (S. 828)'.
- Jedes lokale IPsec-VPN-Gateway hat eine öffentliche IP-Adresse.

- Ihr Cloud-Netzwerk hat genügend IP-Adressen für die Cloud Server, die Kopien Ihrer geschützten Maschinen sind (im Produktionsnetzwerk), und für die Recovery-Server (mit einer oder zwei IP-Adressen, je nach Ihren Anforderungen).
- [Wenn Sie eine Firewall zwischen den lokalen Standorten und der Cloud-Site verwenden] Die folgenden IP-Protokolle und UDP-Ports sind an den lokalen Standorten zugelassen: IP-Protokoll ID 50 (ESP), UDP-Port 500 (IKE) und UDP-Port 4500.
- Die NAT-T-Konfiguration am lokalen Standort ist deaktiviert.

So können Sie eine Multi-Site-IPsec-VPN-Verbindung konfigurieren

1. Fügen Sie ein oder mehrere Netzwerke zur Cloud-Site hinzu.
   a. Klicken Sie auf **Netzwerk hinzufügen**.

   Hinweis
   Wenn Sie ein Cloud-Netzwerk hinzufügen, wird automatisch ein entsprechendes Testnetzwerk mit der gleichen Netzwerkadresse und Maske hinzugefügt, um Test-Failover durchführen zu können. Die Cloud Server im Testnetzwerk haben die gleichen IP-Adressen wie die im Cloud-Produktionsnetzwerk. Wenn Sie während eines Test-Failover vom Produktionsnetzwerk aus auf einen Cloud Server zugreifen müssen, sollten Sie beim Erstellen eines Recovery-Servers diesem eine zweite Test-IP-Adresse zuweisen.

   b. Geben Sie im Feld **Netzwerkadresse** die IP-Adresse des Netzwerks ein.
   c. Geben Sie im Feld **Netzwerkmaske** die Maske des Netzwerkes ein.
   d. Klicken Sie auf **Hinzufügen**.
2. Konfigurieren Sie die Einstellungen für jeden lokalen Standort, den Sie mit der Cloud-Site verbinden wollen, gemäß den Empfehlungen für lokale Standorte. Weitere Informationen zu diesen Empfehlungen finden Sie in Abschnitt '"Allgemeine Empfehlungen für lokale Standorte" (S. 831)'.
   a. Klicken Sie auf **Verbindung hinzufügen**.
   b. Geben Sie einen Namen für das lokale VPN-Gateway ein.
   c. Geben Sie die öffentliche IP-Adresse des lokalen VPN-Gateways ein.
   d. [Optional] Geben Sie eine Beschreibung für das lokale VPN-Gateway ein.
   e. Klicken Sie auf **Weiter**.
   f. Geben Sie im Feld **Vorinstallierter Schlüssel (PSK)** den „Pre-Shared Key“ ein – oder klicken Sie auf **Einen neuen vorinstallierten Schlüssel (PSK) generieren**, um einen automatisch generierten Wert zu verwenden.

   Hinweis
   Sie müssen den gleichen vorinstallierten Schlüssel (Pre-Shared Key, PSK) für das lokale und das Cloud-VPN-Gateway verwenden.

g. Klicken Sie auf **IPsec/IKE-Sicherheitseinstellungen**, um die Einstellungen zu konfigurieren. Weitere Informationen zu den Einstellungen, die Sie konfigurieren können, finden Sie im Abschnitt '"IPsec/IKE-Sicherheitseinstellungen" (S. 832)'.

Hinweis
Sie können die Standardeinstellungen verwenden, die automatisch ausgefüllt werden, oder eigene Werte verwenden. Es werden nur Verbindungen mit dem IKEv2-Protokoll unterstützt. Die vorgegebene **Aktion bei Start** bei Aufbau der VPN-Verbindung ist **Hinzufügen** (bedeutet: Ihr lokales VPN-Gateway initiiert die Verbindung). Sie können den Wert aber auch auf **Start** (bedeutet: das Cloud-VPN-Gateway initiiert die Verbindung) oder **Route** (geeignet für Firewalls, die die Route-Option unterstützen) ändern.

h. Konfigurieren Sie die **Netzwerkrichtlinien**.
Die Netzwerkrichtlinien spezifizieren diejenigen Netzwerke, mit denen sich das IPsec-VPN verbindet. Geben Sie die IP-Adresse und Maske des Netzwerks im CIDR-Format ein. Die lokalen und Cloud-Netzwerksegmente sollten sich nicht überlappen.

i. Klicken Sie auf **Speichern**.

Allgemeine Empfehlungen für lokale Standorte

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Wenn Sie die lokalen Standorte für Ihre Multi-Site-IPsec-VPN-Konnektivität konfigurieren, sollten Sie folgende Empfehlungen beachten:

- Legen Sie für jede IKE-Phase mindestens einen der Werte fest, die in der Cloud-Site für folgende Parameter konfiguriert sind: Verschlüsselungsalgorithmus, Hash-Algorithmus und Diffie-Hellman-Gruppennummern.
- Aktivieren Sie 'Perfect Forward Secrecy' (PFS, perfekte vorwärts gerichtete Geheimhaltung) mit mindestens einem der Werte für Diffie-Hellman-Gruppennummern, der in der Cloud-Site für die IKE-Phase 2 konfiguriert ist.
- Konfigurieren Sie für die IKE-Phase 1 und IKE-Phase 2 denselben **Lebensdauer**-Wert wie in der Cloud-Site.
- Konfigurationen mit NAT-Traversal (NAT-T) werden nicht unterstützt. Deaktivieren Sie die NAT-T-Konfiguration am lokalen Standort. Anderenfalls kann die zusätzliche UDP-Kapselung nicht ausgehandelt werden.
- Die Konfiguration von **Aktion bei Start** definiert, welche Seite die Verbindung initiiert. Der Standardwert **Hinzufügen** bedeutet, dass der lokale Standort die Verbindung einleitet und die Cloud-Site auf die Initiierung der Verbindung wartet. Ändern Sie den Wert auf **Start**, wenn die Cloud-Site die Verbindung initiieren soll – oder auf **Route**, wenn Sie wollen, dass beide Seiten die Verbindung initiieren können (geeignet für Firewalls, die die Route-Option unterstützen).

Weitere Informationen und Konfigurationsbeispiele für verschiedene Lösungen finden Sie unter:

- Diese Serie von Knowledge Base-Artikeln
- Dieses Video-Beispiel

IPsec/IKE-Sicherheitseinstellungen

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Die folgende Tabelle gibt weitere Informationen über die IPsec-/IKE-Sicherheitsparameter.

Parameter	Beschreibung
Verschlüsselungsalgorithmus	Der Verschlüsselungsalgorithmus, durch den sichergestellt wird, dass die Daten während der Übertragung nicht einsehbar sind. Standardmäßig sind alle Algorithmen ausgewählt. Sie müssen mindestens einen der ausgewählten Algorithmen auf Ihrem lokalen Gateway-Gerät für jede IKE-Phase konfigurieren.
Hash-Algorithmus	Der Hash-Algorithmus, der verwendet wird, um die Integrität und Authentizität der Daten überprüfen zu können. Standardmäßig sind alle Algorithmen ausgewählt. Sie müssen mindestens einen der ausgewählten Algorithmen auf Ihrem lokalen Gateway-Gerät für jede IKE-Phase konfigurieren.
Diffie-Hellman-Gruppennummern	Die Diffie-Hellman-Gruppennummern definieren die Stärke des Schlüssels, der beim IKE-Prozess (Internet Key Exchange, Internetschlüsselaustausch) verwendet wird. Höhere Gruppennummern sind sicherer, erfordern jedoch mehr Zeit für die Berechnung des Schlüssels. Standardmäßig sind alle Gruppen ausgewählt. Sie müssen mindestens eine der ausgewählten Gruppen auf Ihrem lokalen Gateway-Gerät für jede IKE-Phase konfigurieren.
Lebensdauer (Sekunden)	Der Wert 'Lebensdauer' bestimmt die Zeitspanne einer Verbindungsinstanz mit einem Satz von Verschlüsselungs-/Authentifizierungsschlüsseln für Benutzerpakete, von der erfolgreichen Aushandlung bis zum Ablaufzeitpunkt. Bereich für Phase 1: 900-28800 Sekunden

Parameter	Beschreibung
	(Vorgabe: 28800). Bereich für Phase 2: 900-3600 Sekunden (Vorgabe: 3600). Die Lebensdauer für Phase 2 muss kleiner sein als die Lebensdauer für Phase 1. Die Verbindung wird, bevor sie abläuft, über den Schlüsselkanal neu ausgehandelt. Vergleiche den Abschnitt '**Grenzzeit bis zur Schlüsselerneuerung**'. Wenn sich die lokale und die Remote-Seite nicht über die Lebensdauer einig sind, kommt es auf der Seite mit der längeren Lebensdauer zu einem Wust von überflüssigen Verbindungen. Siehe außerdem die Abschnitte '**Grenzzeit bis zur Schlüsselerneuerung** und '**Schlüsselerneuerungsvarianz**'.
Grenzzeit bis zur Schlüsselerneuerung (Sekunden)	Die Grenzzeit (Englisch: Rekey Margin Time) bevor die Verbindung oder der Schlüsselkanal abläuft, während der die lokale Seite der VPN-Verbindung versucht, einen Ersatzschlüssel auszuhandeln. Die Schlüsselerneuerungszeit (Englisch: Rekey Time) wird zufällig variiert und zwar nach dem Wert für die **Schlüsselerneuerungsvarianz**. Ist nur lokal relevant. Die Remote-Seite (Gegenstelle) muss dem nicht zustimmen. Bereich: 900-3600 Sekunden. Der Standardwert ist 3600.
Replay-Fenstergröße (Paket)	Die IPsec-Replay-Fenstergröße (Replay = Wiedereinspielung von übertragenen Daten) für diese Verbindung. Der Standardwert -1 verwendet den Wert, der mit 'charon.replay_window' in der Datei 'strongswan.conf' konfiguriert wurde. Werte größer als 32 werden nur unterstützt, wenn das Netlink-Backend verwendet wird. Ein Wert von 0 deaktiviert den IPsec-Replay-Schutz.
Schlüsselerneuerungsvarianz (%)	Der maximale Prozentsatz, um den die Werte für 'marginbytes', 'marginpackets' und 'margintime' zufällig erhöht werden, um die Schlüsselerneuerungsintervalle zufällig zu variieren (wichtig für Hosts mit vielen gleichzeitigen Verbindungen).

Parameter	Beschreibung
	Diese Wert für die Schlüsselerneuerungsvarianz (Englisch: Rekey Fuzz) kann 100% überschreiten. Der Wert von 'marginTYPE' darf nach der zufälligen Erhöhung 'lifeTYPE' nicht überschreiten, wobei 'TYPE' für Bytes, Pakete oder Zeit steht. Ein Wert von 0% deaktiviert die Zufallsverteilung. Ist nur lokal relevant. Die Remote-Seite (Gegenstelle) muss dem nicht zustimmen.
DPD-Timeout (Sekunden)	Die Zeit, nach der ein DPD-Zeitüberschreitung (Dead Peer Detection) auftritt. Sie können einen Wert von 30 oder höher spezifizieren. Der Standardwert ist 30.
Aktion bei DPD-Timeout	Die Aktion, die ausgeführt werden soll, wenn eine DPD-Zeitüberschreitung (Dead Peer Detection) auftritt. **Neustart** – Die Sitzung wird neu gestartet, wenn es zu einer DPD-Zeitüberschreitung kommt. **Löschen** – Die Sitzung wird gelöscht, wenn es zu einer DPD-Zeitüberschreitung kommt. **Ohne** – Keine Aktion durchführen, wenn es zu einer DPD-Zeitüberschreitung kommt
Aktion bei Start	Bestimmt, welche Seite die Verbindung initiiert und den Tunnel für die VPN-Verbindung aufbaut. **Hinzufügen** – Ihr lokales VPN-Gateway initiiert die Verbindung. **Start** – das Cloud-VPN-Gateway initiiert die Verbindung. **Route** – eignet sich für VPN-Gateways, die die Route-Option unterstützen. Der Tunnel ist nur dann aktiv, wenn ein Datenverkehr vom lokalen VPN-Gateway oder vom Cloud VPN-Gateway initiiert wird.

Empfehlungen für die Verfügbarkeit der Active Directory-Domänendienste

Wenn sich Ihre geschützten Workloads an einem Domain Controller authentifizieren müssen, empfehlen wir, dass Sie eine Active Directory Domain Controller (AD DC)-Instanz auf der Disaster Recovery-Site haben.

Active Directory Domain Controller für L2-OpenVPN-Konnektivität

Mit der L2-OpenVPN-Konnektivität bleiben die IP-Adressen der geschützten Workloads bei einem Test- oder Produktions-Failover in der Cloud-Site erhalten. Daher hat der AD DC während eines Test- oder Produktions-Failovers die gleiche IP-Adresse wie am lokalen Standort.

Mit einer benutzerdefinierten DNS-Konfiguration können Sie Ihren eigenen benutzerdefinierten DNS-Server für alle Cloud Server festlegen. Weitere Informationen finden Sie im Abschnitt '"Benutzerdefinierte DNS-Server konfigurieren" (S. 845)'.

Active Directory Domain Controller für L3-IPsec-VPN-Konnektivität

Mit der L3-IPsec-VPN-Konnektivität bleiben die IP-Adressen der geschützten Workloads nicht in der Cloud-Site erhalten. Daher empfehlen wir, dass Sie eine zusätzliche dedizierte AD DC-Instanz als primären Server in der Cloud-Site haben, bevor Sie einen Produktions-Failover durchführen.

Die Empfehlungen für eine dedizierte AD DC-Instanz, die als primärer Server in der Cloud-Site konfiguriert wird, sehen folgendermaßen aus:

- Schalten Sie die Windows-Firewall aus.
- Verknüpfen Sie den primären Server mit dem Active Directory-Dienst.
- Stellen Sie sicher, dass der primäre Server auf das Internet zugreifen kann.
- Fügen Sie die Active Directory-Funktion hinzu.

Mit einer benutzerdefinierten DNS-Konfiguration können Sie Ihren eigenen benutzerdefinierten DNS-Server für alle Cloud Server festlegen. Weitere Informationen finden Sie im Abschnitt '"Benutzerdefinierte DNS-Server konfigurieren" (S. 845)'.

Einen Point-to-Site-VPN-Remote-Zugriff konfigurieren

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Wenn Sie eine Remote-Verbindung zu Ihrem lokalen Standort aufbauen müssen, können Sie die Point-to-Site-Verbindung zum lokalen Standort konfigurieren. Sie können die nachfolgende Prozedur befolgen oder sich das Video-Tutorial ansehen.

Voraussetzungen

- Es wurde eine Site-to-Site-OpenVPN-Konnektivität konfiguriert.
- Die VPN-Appliance wurde am lokalen Standort installiert.

So können Sie eine Point-to-Site-Verbindung zum lokalen Standort konfigurieren

1. Gehen Sie in der Cyber Protect-Konsole zu **Disaster Recovery** –> **Verbindung**.
2. Klicken Sie auf **Eigenschaften anzeigen**.
3. Aktivieren Sie die Option **VPN-Zugriff auf den lokalen Standort**.
4. Stellen Sie sicher, dass Ihr Benutzer, der die Point-to-Site-Verbindung zum lokalen Standort aufbauen muss, Folgendes hat:
   - ein Benutzerkonto in Cyber Protect Cloud. Diese Anmeldedaten werden für die Authentifizierung im VPN-Client verwendet. Ansonsten müssen Sie ein Benutzerkonto in Cyber Protect Cloud erstellen.
   - eine Benutzerrolle 'Firmenadministrator' oder 'Cyber Protection'.
5. Den OpenVPN-Client konfigurieren:
   a. Sie können den OpenVPN-Client v2.4.0 oder höher von dieser Adresse herunterladen: https://openvpn.net/community-downloads/.
   b. Installieren Sie den OpenVPN-Client auf derjenigen Maschine, von der aus Sie sich mit dem lokalen Standort verbinden wollen.
   c. Klicken Sie auf **Konfiguration für OpenVPN herunterladen**. Die Konfigurationsdatei ist auf Benutzer in Ihrer Organisation anwendbar, die die Benutzerrolle 'Firmenadministrator' oder 'Cyber Protection' haben.
   d. Importieren Sie die heruntergeladene Konfiguration in die OpenVPN-Einstellungen.
   e. Melden Sie mit Ihren Benutzeranmeldedaten von Cyber Protect Cloud am OpenVPN-Client an (siehe Schritt 4 weiter oben).
   f. [Optional] Wenn für Ihre Organisation eine Zwei-Faktor-Authentifizierung aktiviert ist, müssen Sie den einmaligen TOTP-Code (Einmalkennwort) bereitstellen.

Wichtig
Wenn Sie die Zwei-Faktor-Authentifizierung für Ihr Konto aktiviert haben, müssen Sie die Konfigurationsdatei neu generieren und für Ihre vorhandenen OpenVPN-Clients erneuern. Die Benutzer müssen sich erneut an Cyber Protect Cloud anmelden, um die Zwei-Faktor-Authentifizierung für ihre Konten einzurichten.

Anschließend kann sich Ihr Benutzer mit Maschinen am lokalen Standort verbinden.

Netzwerkverwaltung

In diesem Abschnitt werden verschiedene Szenarien für die Netzwerkverwaltung beschrieben.

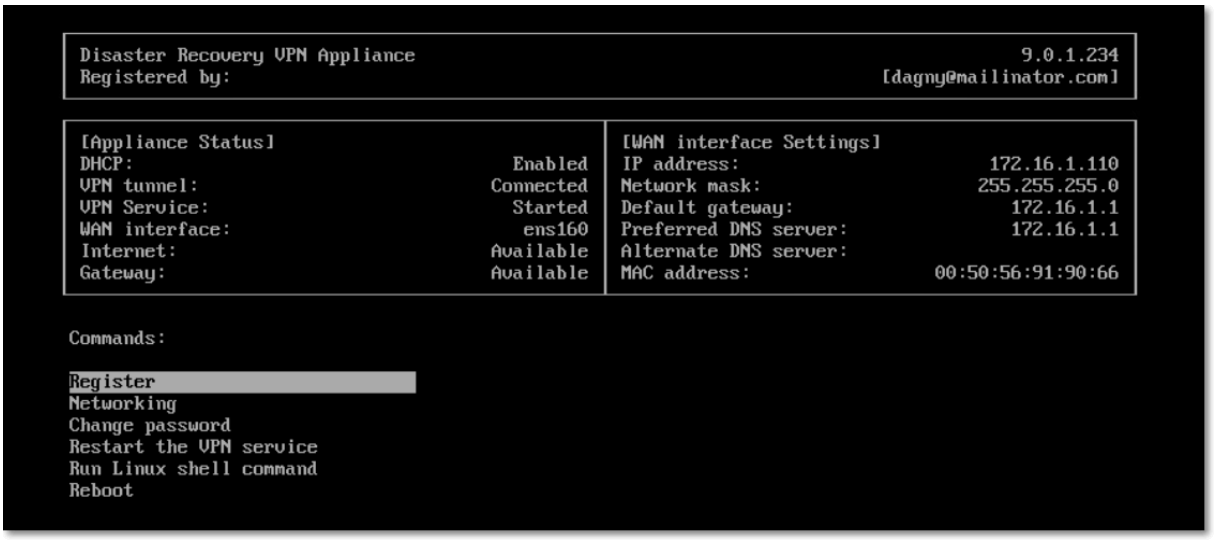
Netzwerke verwalten

Hinweis
In Abhängigkeit davon, welches Lizenzierungsmodell angewendet wird, kann für einige Funktionen eine zusätzliche Lizenzierung erforderlich sein.

Site-to-Site-OpenVPN-Verbindung

So können Sie ein Netzwerk am lokalen Standort hinzufügen und dieses in die Cloud erweitern

1. Richten Sie auf der VPN-Appliance eine neue Netzwerkschnittstelle mit dem lokalen Netzwerk ein, welches Sie in die Cloud erweitern wollen.
2. Melden Sie sich an der Konsole der VPN-Appliance an.
3. Konfigurieren Sie im Bereich **Netzwerk** die Netzwerkeinstellungen für die neue Schnittstelle.



Die Appliance beginnt, Informationen über die Netzwerke von allen aktiven Schnittstellen an Cyber Disaster Recovery Cloud zu melden. Die Cyber Protect-Konsole zeigt die Schnittstellen basierend auf den Informationen der VPN-Appliance an.

So können Sie ein Netzwerk, das in die Cloud erweitert ist, löschen

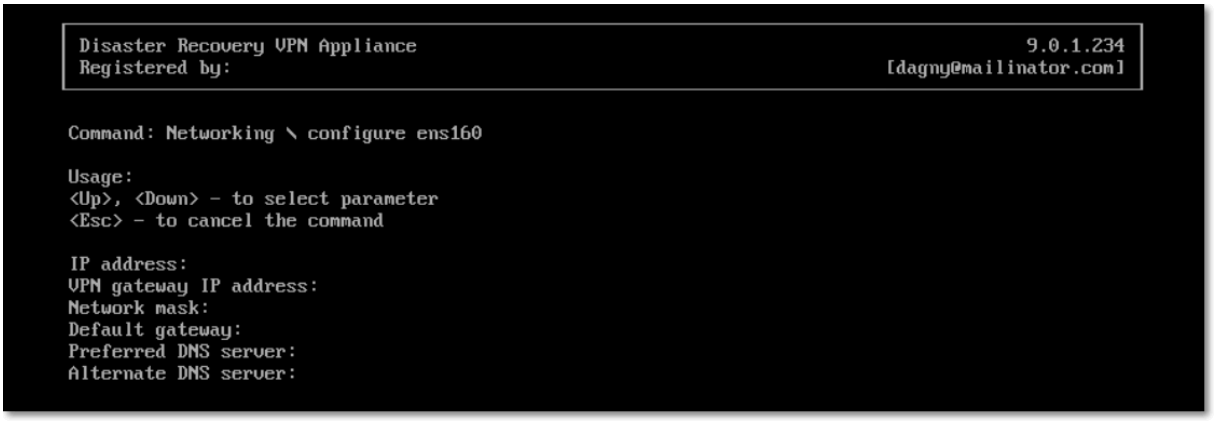
1. Melden Sie sich an der Konsole der VPN-Appliance an.
2. Wählen Sie im Bereich **Netzwerk** die Schnittstelle, die Sie löschen wollen, und klicken Sie dann auf **Netzwerkeinstellungen bereinigen**.
3. Bestätigen Sie die Aktion.

Als Ergebnis wird die lokale Netzwerkerweiterung in die Cloud über einen sicheren VPN-Tunnel gestoppt. Dieses Netzwerk wird als unabhängiges Cloud-Segment arbeiten. Wenn diese Schnittstelle verwendet wird, um den Datenverkehr von der/zur Cloud-Site durchzuleiten, werden alle Ihre Netzwerkverbindungen von der/zur Cloud-Site getrennt.

So können Sie die Netzwerkparameter ändern

1. Melden Sie sich an der Konsole der VPN-Appliance an.
2. Wählen Sie im Bereich **Netzwerk** die Schnittstelle, die Sie bearbeiten wollen.
3. Klicken Sie auf **Netzwerkeinstellungen bearbeiten**.
4. Wählen Sie eine der zwei möglichen Optionen:

- Bei einer automatischen Netzwerkkonfiguration per DHCP: klicken Sie auf **DHCP verwenden**. Bestätigen Sie die Aktion.
- Bei einer manuellen Netzwerkkonfiguration: klicken Sie auf **Statische IP-Adresse festlegen**. Folgende Einstellungen können bearbeitet werden:
  - **IP-Adresse**: die IP-Adresse der Schnittstelle im lokalen Netzwerk.
  - **IP-Adresse des VPN-Gateway**: die spezielle IP-Adresse, die für das Cloud-Segment des Netzwerks reserviert ist, damit der Cyber Disaster Recovery Cloud Service ordnungsgemäß funktionieren kann.
  - **Netzwerk-Maske**: die Netzwerk-Maske des lokalen Netzwerks.
  - **Standard-Gateway**: das Standard-Gateway am lokalen Standort.
  - **Bevorzugter DNS-Server**: der primäre DNS-Server am lokalen Standort.
  - **Alternativer DNS-Server**: der sekundäre DNS-Server am lokalen Standort.



- Nehmen Sie die erforderlichen Änderungen vor und bestätigen Sie diese durch Drücken der Eingabetaste.

'Nur Cloud'-Modus

Sie können bis zu 23 Netzwerke in der Cloud haben.

So können Sie ein neues Cloud-Netzwerk hinzufügen

1. Gehen Sie zu **Disaster Recovery** –> **Verbindung**.
2. Klicken Sie bei **Cloud-Site** auf **Cloud-Netzwerk hinzufügen**.
3. Definieren Sie die Parameter des Cloud-Netzwerks: die Netzwerkadresse und Netzwerkmaske. Wenn Sie dies abgeschlossen haben, klicken Sie auf **Fertig**.

Anschließend wird das zusätzliche Cloud-Netzwerk mit der definierten Adresse und Netzwerkmaske auf der Cloud-Site bereitgestellt.

So können Sie ein Cloud-Netzwerk löschen

Hinweis
Sie können ein Cloud-Netzwerk nicht löschen, solange sich noch wenigstens ein Cloud Server darin befindet. Löschen Sie dann zuerst den Cloud Server und anschließend das Netzwerk.

1. Gehen Sie zu **Disaster Recovery** –> **Verbindung**.
2. Klicken Sie bei **Cloud-Site** auf die Netzwerkadresse, die Sie löschen wollen.
3. Klicken Sie auf **Löschen** und bestätigen Sie die Aktion.

So können Sie die Cloud-Netzwerkparameter ändern

1. Gehen Sie zu **Disaster Recovery** –> **Verbindung**.
2. Klicken Sie bei **Cloud-Site** auf die Netzwerkadresse, die Sie bearbeiten wollen.
3. Klicken Sie auf **Bearbeiten**.
4. Definieren Sie die Netzwerkadresse und Netzwerkmaske und klicken Sie dann auf **Fertig**.

Rekonfiguration der IP-Adresse

Für eine optimale Disaster Recovery-Performance müssen die IP-Adressen, die den lokalen und Cloud-Servern zugewiesen werden, konsistent sein. Wenn Inkonsistenzen oder Unstimmigkeiten bei den IP-Adressen vorliegen, sehen Sie ein Ausrufezeichen neben dem entsprechenden Netzwerk bei **Disaster Recovery** –> **Verbindung**.

Nachfolgend sind einige gängige Gründe für Inkonsistenzen mit IP-Adressen aufgeführt:

1. Ein Recovery-Server wurde von einem Netzwerk in ein anderes migriert oder die Netzwerkmaske des Cloud-Netzwerks wurde geändert. Infolgedessen haben Cloud-Server die IP-Adressen aus Netzwerken, mit denen sie nicht verbunden sind.
2. Der Verbindungstyp wurde von einer 'Ohne Site-to-Site'-Verbindung zu einer Site-to-Site-Verbindung umgestellt. Dadurch wird ein lokaler Server in ein anderes Netzwerk platziert als das, welches für den Recovery-Server in der Cloud-Site erstellt wurde.
3. Der Verbindungstyp wurde von Site-to-Site-OpenVPN zu Multi-Site-IPsec-VPN umgestellt – oder von Multi-Site-IPsec-VPN zu Site-to-Site-OpenVPN. Weitere Informationen zu diesem Szenario finden Sie in den Abschnitten 'Verbindungen wechseln' und 'IP-Adressen neu zuweisen'.
4. Bearbeiten der folgenden Netzwerkparameter auf der VPN-Appliance-Site:
   - Hinzufügen einer Schnittstelle über die Netzwerkeinstellungen
   - Manuelles Bearbeiten der Netzwerkmaske über die Schnittstelleneinstellungen
   - Bearbeiten der Netzwerkmaske über DHCP
   - Manuelles Bearbeiten der Netzwerkadresse und Netzwerkmaske über die Schnittstelleneinstellungen
   - Bearbeiten der Netzwerkmaske und Netzwerkadresse über DHCP

Als Ergebnis dieser aufgeführten Aktionen kann das Netzwerk in der Cloud-Site eine Teilmenge oder Obermenge des lokalen Netzwerks werden – oder die VPN-Appliance-Schnittstelle kann die gleichen Netzwerkeinstellungen für verschiedene Schnittstellen melden.

So können Sie das Problem mit den Netzwerkeinstellungen lösen

1. Klicken Sie auf das Netzwerk, dessen IP-Adresse rekonfiguriert werden muss.
   Sie sehen eine Liste der Server in dem ausgewählten Netzwerk, deren Status und IP-Adressen. Server, deren Netzwerkeinstellungen inkonsistent sind, sind mit einem Ausrufezeichen gekennzeichnet.
2. Wenn Sie die Netzwerkeinstellungen eines Servers ändern wollen, müssen Sie auf **Zu Server gehen** klicken. Wenn Sie die Netzwerkeinstellungen für alle Server gemeinsam ändern wollen, müssen Sie im Benachrichtigungsblock auf **Ändern** klicken.
3. Ändern Sie die IP-Adressen nach Bedarf, indem Sie diese in den Feldern **Neue IP** und **Neue Test-IP** definieren.
4. Wenn Sie dies abgeschlossen haben, klicken Sie auf **Bestätigen**.

Server zu einem geeigneten Netzwerk verschieben

Wenn Sie einen Disaster Recovery-Schutzplan erstellen und diesen auf ausgewählte Geräte anwenden, überprüft das System die entsprechenden IP-Adressen der Geräte und erstellt dann automatisch Cloud-Netzwerke, wenn es noch keine Cloud-Netzwerke gibt, zu denen die IP-Adresse passen würden. Standardmäßig sind die Cloud-Netze mit den maximalen Bereichen konfiguriert, die von der IANA für den privaten Gebrauch empfohlen werden (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16). Sie können Ihr Netzwerk eingrenzen, indem Sie die Netzwerkmaske bearbeiten.

Falls sich die ausgewählten Geräte in mehreren lokalen Netzwerken befinden, kann das Netzwerk auf der Cloud-Site zu einer Obermenge der lokalen Netzwerke werden. Gehen Sie in diesem Fall folgendermaßen vor, um die Cloud-Netzwerke zu rekonfigurieren:

1. Klicken Sie zuerst auf das Cloud-Netzwerk, das eine Rekonfiguration der Netzwerkgröße erfordert, und klicken Sie dann auf **Bearbeiten**.
2. Rekonfigurieren Sie die Netzwerkgröße mit den passenden Einstellungen.
3. Erstellen Sie bei Bedarf weitere Netzwerke.
4. Klicken Sie neben der Anzahl der Geräte, die mit dem Netzwerk verbunden sind, auf das Benachrichtigungssymbol.
5. Klicken Sie auf **Zu einem geeigneten Netzwerk verschieben**.
6. Wählen Sie die Server aus, die Sie in die geeigneten Netzwerke verschieben wollen, und klicken Sie dann auf **Verschieben**.

Die Einstellungen der VPN-Appliance verwalten

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

In der Cyber Protect-Konsole (**Disaster Recovery** –> **Verbindung**) können Sie:

- Die Protokolldateien herunterladen.
- Die Registrierung der Appliance aufheben (wenn Sie die Einstellungen der VPN-Appliance zurücksetzen oder zum 'Nur Cloud'-Modus wechseln müssen).

Wenn Sie auf diese Einstellungen zugreifen wollen, klicken Sie im Block **VPN-Appliance** auf das **i**-Symbol.

In der VPN-Appliance-Konsole können Sie:

- Das Kennwort für die Appliance ändern.
- Die Netzwerkeinstellungen einsehen/ändern und definieren, welche Schnittstelle als WAN-Schnittstelle für die Internetverbindung verwendet werden soll.
- Das Registrierungskonto registrieren/ändern (durch Wiederholung der Registrierung).
- Den VPN-Dienst neu starten.
- Die VPN-Appliance neu booten.
- Einen Linux-Shell-Befehl ausführen (nur für fortgeschrittene Fehlerbehebungsfälle).

Das VPN-Gateway neu installieren

Wenn es ein nicht behebbares Problem mit dem VPN-Gateway gibt, wollen Sie das VPN-Gateway möglicherweise neu installieren. Zu den möglichen Problemen, die dabei auftauchen können, gehören:

- Das VPN-Gateway befindet sich im Status **Fehler**.
- Das VPN-Gateway befindet sich für längere Zeit im Status **Ausstehend**.
- Der Status des VPN-Gateways bleibt für längere Zeit unbestimmt.

Der Prozess zur Neuinstallation des VPN-Gateways umfasst folgende automatische Aktionen: die vorhandene virtuelle Maschine des VPN-Gateways vollständig löschen, eine neue virtuelle Maschine aus der Vorlage installieren sowie die Einstellungen des vorherigen VPN-Gateways auf die neue virtuelle Maschine anwenden.

Voraussetzungen:

Einer der Verbindungstypen zur Cloud-Site muss festgelegt sein.

So können Sie das VPN-Gateway neu installieren

1. Gehen Sie in der Cyber Protect-Konsole zu **Disaster Recovery** –> **Verbindung**.
2. Klicken Sie auf das Zahnradsymbol des VPN-Gateways und wählen Sie den Befehl **VPN-Gateway neu installieren**.
3. Geben Sie im Dialog **VPN-Gateway neu installieren** Ihre Anmeldedaten ein.
4. Klicken Sie auf **Neu installieren**.

Die Site-to-Site-Verbindung (de)aktivieren

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

In folgenden Fällen können Sie die Site-zu-Site-Verbindung aktivieren:

- Wenn die Cloud Server in der Cloud-Site mit den Servern am lokalen Standort kommunizieren müssen.
- Nach einem Failover in die Cloud wurde die lokale Infrastruktur wiederhergestellt – und Sie wollen Ihre Server per Failback wieder zum lokalen Standort zurücksetzen.

So können Sie die Site-to-Site-Verbindung aktivieren

1. Gehen Sie zu **Disaster Recovery** –> **Verbindung**.
2. Klicken Sie auf **Eigenschaften anzeigen** und aktivieren Sie die Option **Site-to-Site-Verbindung**.

Infolgedessen wird die Site-to-Site-VPN-Verbindung zwischen dem lokalen Standort und der Cloud-Site aktiviert. Der Cyber Disaster Recovery Cloud Service ruft die Netzwerkeinstellungen von der VPN-Appliance ab und erweitert die lokalen Netzwerke in die Cloud-Site.

Wenn Ihre Cloud Server in der Cloud-Site nicht mit den Servern am lokalen Standort kommunizieren müssen, können Sie die Site-to-Site Verbindung deaktivieren.

So können Sie die Site-to-Site-Verbindung deaktivieren

1. Gehen Sie zu **Disaster Recovery** –> **Verbindung**.
2. Klicken Sie zuer auf **Eigenschaften anzeigen** und deaktivieren Sie dann die Option **Site-to-Site-Verbindung**.

Als Ergebnis wird die Verbindung vom lokalen Standort zur Cloud-Site getrennt.

Den Site-to-Site-Verbindungstyp wechseln

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Sie können einfach von einer Site-to-Site-OpenVPN- zu einer Multi-Site-IPsec-VPN-Verbindung wechseln – oder von einer Multi-Site-IPsec-VPN- zu einer Site-to-Site-OpenVPN-Verbindung.

Wenn Sie den Verbindungstyp wechseln, werden gerade aktive VPN-Verbindungen gelöscht, aber die Cloud Server und Netzwerkkonfigurationen bleiben erhalten. Sie müssen jedoch noch die IP-Adressen der Cloud-Netzwerke und Cloud Server neu zuweisen.

Die folgende Tabelle vergleicht die grundlegenden Eigenschaften der Site-to-Site-OpenVPN- und der Multi-Site-IPsec-VPN-Verbindung.

	Site-to-Site-OpenVPN	Multi-Site-IPsec-VPN
Unterstützung für lokalen Standort	Einzel	Einzel, Mehrere
VPN-Gateway-Modus	L2 Open VPN	L3 IPsec VPN
Netzwerksegmente	Erweitert das lokale Netzwerk in das Cloud-Netzwerk	Lokale und Cloud-Netzwerksegmente sollten sich nicht überlappen
Unterstützt Point-to-Site-Zugriffe auf den lokalen Standort	Ja	Nein
Unterstützt Point-to-Site-Zugriffe auf die Cloud-Site	Ja	Ja
Erfordert ein Angebotselement 'Öffentliche IP'	Nein	Ja

So können Sie von einer Site-to-Site-OpenVPN- zu einer Multi-Site-IPsec-VPN-Verbindung wechseln

1. Gehen Sie in der Cyber Protect-Konsole zu **Disaster Recovery** –> **Verbindung**.
2. Klicken Sie auf **Eigenschaften anzeigen**.
3. Klicken Sie auf **Zu Multi-Site-IPsec-VPN wechseln**.
4. Klicken Sie auf **Rekonfigurieren**.
5. Weisen Sie die IP-Adressen des Cloud-Netzwerks und der Cloud Server neu zu.
6. Konfigurieren Sie die Multi-Site-IPsec-Verbindungseinstellungen.

So können Sie von einer Multi-Site-IPsec-VPN- zu einer Site-to-Site-OpenVPN-Verbindung wechseln

1. Gehen Sie in der Cyber Protect-Konsole zu **Disaster Recovery** –> **Verbindung**.
2. Klicken Sie auf **Eigenschaften anzeigen**.
3. Klicken Sie auf **Zu Site-to-Site-OpenVPN wechseln**.
4. Klicken Sie auf **Rekonfigurieren**.
5. Weisen Sie die IP-Adressen des Cloud-Netzwerks und der Cloud Server neu zu.
6. Konfigurieren Sie die Site-to-Site-Verbindungseinstellungen.

IP-Adressen neu zuweisen

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Sie müssen die IP-Adressen der Cloud-Netzwerke und der Cloud Server neu zuweisen, um die Konfiguration in folgenden Fällen abschließen zu können:

- Nachdem Sie von einer Site-to-Site-OpenVPN- zu einer Multi-Site-IPsec-VPN-Konnektivität umgestellt haben – oder umgekehrt.
- Nachdem Sie einen Schutzplan angewendet haben (wenn die Multi-Site-IPsec-VPN-Konnektivität konfiguriert wurde).

So können Sie die IP-Adresse eines Cloud-Netzwerks neu zuweisen

1. Klicken Sie in der Registerkarte **Verbindung** auf die IP-Adresse des Cloud-Netzwerks.
2. Klicken Sie im sich öffnenden Dialogfenster **Netzwerk** auf den Befehl **Bearbeiten**.
3. Geben Sie die neue Netzwerkadresse und Netzwerkmaske ein.
4. Klicken Sie auf **Fertig**.

Nachdem Sie die IP-Adresse eines Cloud-Netzwerks neu zugewiesen haben, müssen Sie auch die Cloud Server neu zuweisen, die zu dem neu zugewiesenen Cloud-Netzwerk gehören.

So können Sie die IP-Adresse eines Servers neu zuweisen

1. Klicken Sie in der Registerkarte **Verbindung** auf die IP-Adresse des Servers im Cloud-Netzwerk.
2. Klicken Sie im sich öffnenden Dialogfenster **Server** auf den Befehl **IP-Adresse ändern**.
3. Geben Sie im sich öffnenden Dialogfenster **IP-Adresse ändern** die neue IP-Adresse des Servers ein – oder verwenden Sie die automatisch generierte IP-Adresse, die zum neu zugewiesenen Cloud-Netzwerk gehört.

   Hinweis
   Cyber Disaster Recovery Cloud weist allen Cloud Servern, die vor der Neuzuweisung der Netzwerk-IP-Adresse zum Cloud-Netzwerk gehörten, automatisch IP-Adressen aus dem Cloud-Netzwerk zu. Sie können die vorgeschlagenen IP-Adressen verwenden, um die IP-Adressen aller Cloud Server gemeinsam neu zuzuweisen.

4. Klicken Sie auf **Bestätigen**.

Benutzerdefinierte DNS-Server konfigurieren

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Wenn Sie eine Verbindung (Konnektivität) konfigurieren, erstellt Cyber Disaster Recovery Cloud Ihre Cloud-Netzwerkinfrastruktur. Der Cloud-DHCP-Server weist den Recovery-Servern und den primären Servern automatisch Standard-DNS-Server zu. Sie können diese Standardeinstellungen aber jederzeit ändern und eigene DNS-Server konfigurieren. Die neuen DNS-Einstellungen werden bei der nächsten Anfrage an den DHCP-Server angewendet.

Voraussetzungen:

Einer der Verbindungstypen zur Cloud-Site muss festgelegt sein.

So können Sie einen benutzerdefinierten DNS-Server konfigurieren

1. Gehen Sie in der Cyber Protect-Konsole zu **Disaster Recovery** –> **Verbindung**.
2. Klicken Sie auf **Eigenschaften anzeigen**.
3. Klicken Sie auf **Standard (von der Cloud-Site bereitgestellt)**.
4. Wählen Sie **Benutzerdefinierte Server**.
5. Geben Sie die IP-Adresse des DNS-Servers ein.
6. [Optional] Wenn Sie einen weiteren DNS-Server hinzufügen wollen, klicken Sie auf **Hinzufügen** und geben Sie dann die IP-Adresse dieses DNS-Servers ein.

   Hinweis
   Wenn Sie die benutzerdefinierten DNS-Server hinzugefügt haben, können Sie auch noch die Standard-DNS-Server hinzufügen. Dadurch wird Cyber Disaster Recovery Cloud auf die Standard-DNS-Server zurückgreifen können, wenn die benutzerdefinierten DNS-Server einmal nicht verfügbar sein sollten.

7. Klicken Sie auf **Fertig**.

Benutzerdefinierte DNS-Server löschen

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Sie können DNS-Server aus der benutzerdefinierten DNS-Liste löschen.

Voraussetzungen:

Benutzerdefinierte DNS-Server sind konfiguriert.

So können Sie einen benutzerdefinierten DNS-Server löschen

1. Gehen Sie in der Cyber Protect-Konsole zu **Disaster Recovery** –> **Verbindung**.
2. Klicken Sie auf **Eigenschaften anzeigen**.
3. Klicken Sie auf **Benutzerdefinierte Server**.
4. Klicken Sie neben dem DNS-Server auf das Symbol 'Löschen'.

   Hinweis
   Die Löschaktion ist deaktiviert, wenn nur ein benutzerdefinierter DNS-Server verfügbar ist. Wenn Sie alle benutzerdefinierten DNS-Server löschen wollen, müssen Sie **Standard (von der Cloud-Site bereitgestellt)** auswählen.

5. Klicken Sie auf **Fertig**.

Lokales Routing konfigurieren

Neben Ihren lokalen Netzwerken, die über die VPN-Appliance in die Cloud erweitert sind, haben Sie möglicherweise noch andere lokale Netzwerke, die nicht in der VPN-Appliance registriert sind, aber deren Server dennoch mit den Cloud Servern kommunizieren müssen. Um eine Verbindung zwischen solchen lokalen Servern und den Cloud Servern herzustellen, müssen Sie die Einstellungen für das lokale Routing konfigurieren.

So können Sie ein lokales Routing konfigurieren

1. Gehen Sie zu **Disaster Recovery** –> **Verbindung**.
2. Klicken Sie auf **Eigenschaften anzeigen** und anschließend auf **Lokales Routing**.
3. Spezifizieren Sie die lokalen Netzwerke in der CIDR-Notation.
4. Klicken Sie auf **Speichern**.

Als Ergebnis können die Server aus den spezifizierten lokalen Netzwerken mit den Cloud Servern kommunizieren.

DHCP-Traffic über L2-VPN zulassen

Wenn Geräte an Ihrem lokalen Standort ihre IP-Adresse von einem DHCP-Server beziehen, können Sie diesen DHCP-Server per Disaster Recovery schützen, indem Sie ihn per Failover in die Cloud verlagern und dann den DHCP-Datenverkehr über ein L2-VPN laufen lassen. Auf diese Weise wird Ihr DHCP-Server in der Cloud ausgeführt, von wo er aber weiterhin Ihren lokalen Geräten deren IP-Adressen zuweisen kann.

Voraussetzungen:

Es muss ein Site-to-Site-L2-VPN-Verbindungstyp zur Cloud-Site festgelegt werden.

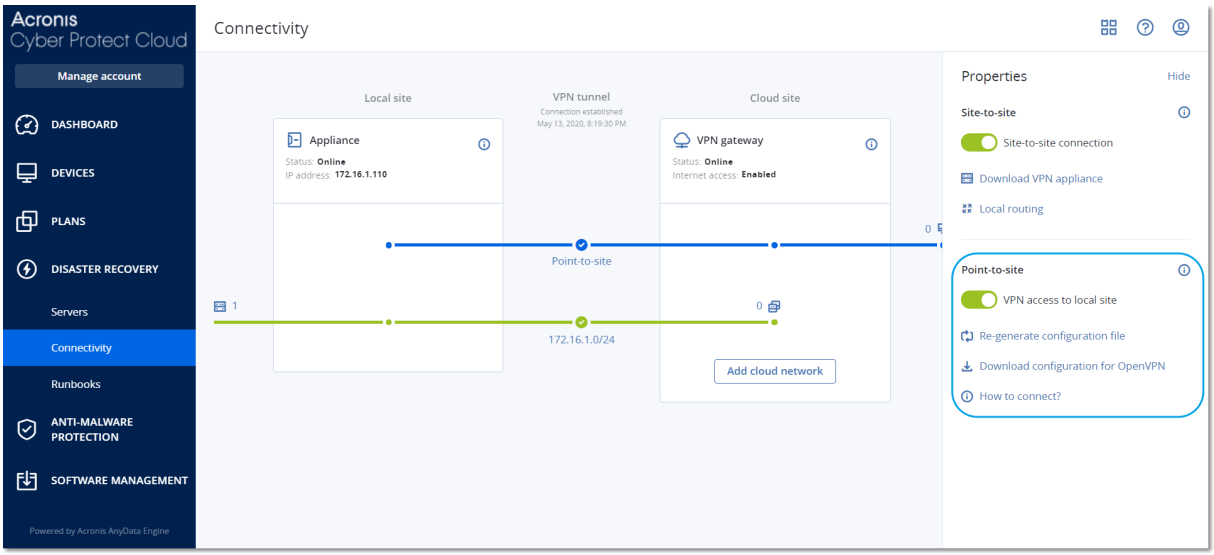
So können Sie den DHCP-Traffic über die L2-VPN-Verbindung zulassen

1. Gehen Sie zu Registerkarte **Disaster Recovery** –> **Verbindung**.
2. Klicken Sie auf **Eigenschaften anzeigen**.
3. Aktivieren Sie den Schalter **DHCP-Traffic über L2-VPN zulassen**.

Einstellungen der Point-to-Site-Verbindung verwalten

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Gehen Sie in der Cyber Protect-Konsole zu **Disaster Recovery** –> **Verbindung** und klicken Sie dann in der rechten oberen Ecke auf **Eigenschaften anzeigen**.



VPN-Zugriff auf den lokalen Standort

Diese Option wird verwendet, um den VPN-Zugriff auf den lokalen Standort zu verwalten. Die Option ist standardmäßig aktiviert. Wenn sie deaktiviert ist, wird kein Point-to-Site-Zugriff auf den lokalen Standort erlaubt.

Konfiguration für OpenVPN herunterladen

Mit diesem Befehl wird die Konfigurationsdatei für den OpenVPN-Client heruntergeladen. Diese Datei ist erforderlich, um eine Point-to-Site-Verbindung zur Cloud-Site aufzubauen.

Konfigurationsdatei neu generieren

Sie können die Konfigurationsdatei für den OpenVPN-Client neu generieren.

Dies ist in folgenden Fällen erforderlich:

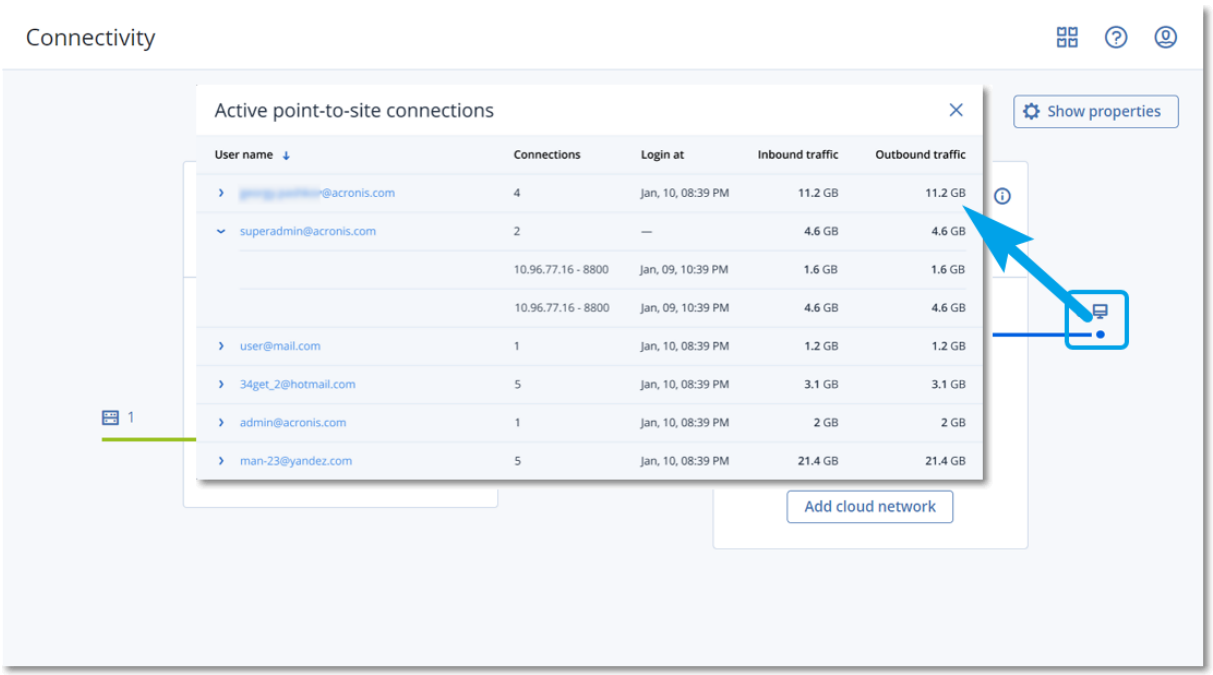
- Wenn Sie annehmen, dass die Konfigurationsdatei kompromittiert sein könnte.
- Wenn die Zwei-Faktor-Authentifizierung für Ihr Konto aktiviert wurde.

Sobald die Konfigurationsdatei aktualisiert wurde, ist keine Verbindung mehr über die alte Konfigurationsdatei möglich. Stellen Sie sicher, dass die neue Datei an alle Benutzer verteilt wird, die die Point-to-Site-Verbindung verwenden dürfen.

Aktive Point-to-Site-Verbindungen

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Sie können alle aktiven Point-to-Site-Verbindungen im Bereich **Disaster Recovery** –> **Verbindung** einsehen. Klicken Sie in der blauen **Point-to-Site**-Linie auf das Maschinen-Symbole und Ihnen werden ausführliche Informationen über die aktiven Point-to-Site-Verbindungen (nach Benutzernamen gruppiert) angezeigt.



Mit Protokollen arbeiten

Die Disaster Recovery-Funktionalität sammelt Protokolle für die VPN-Appliance und das VPN-Gateway. Die Protokolle werden als .txt-Dateien gespeichert, die dann in einem .zip-Archiv komprimiert werden. Sie können das Archiv herunterladen, anschließend extrahieren und die Informationen zur Fehlerbehebung oder zum Monitoring verwenden.

Die folgende Liste beschreibt die Protokolldateien, die Teil des .zip-Archivs sind, und die darin enthaltenen Informationen.

`dnsmasq.config.txt` – Die Datei enthält Informationen über die Konfiguration des Dienstes, der DNS- und DHCP-Adressen bereitstellt.

`dnsmsq.leases.txt` – Die Datei enthält Informationen über die aktuellen DHCP-Adressleases.

`dnsmasq_log.txt` – Die Datei enthält Protokolle des dnsmasq-Dienstes.

`ebtables.txt` – Die Datei enthält Informationen über die Firewall-Tabellen.

`free.txt` – Die Datei enthält Informationen über den freien Arbeitsspeicher.

`ip.txt` – Die Datei enthält die Protokolle über die Konfiguration der Netzwerkschnittstellen, einschließlich ihrer Namen, die bei der Konfiguration der **Netzwerkpakete erfassen**-Einstellungen verwendet werden können.

`NetworkManager_log.txt` – Die Datei enthält Protokolle vom NetworkManager-Dienst.

`NetworkManager_status.txt` – Die Datei enthält Informationen über den Status des NetworkManager-Dienstes.

`openvpn@p2s_log.txt` – Die Datei enthält Protokolle vom OpenVPN-Dienst.

`openvpn@p2s_status.txt` – Die Datei enthält Informationen über den Status der VPN-Tunnel.

`ps.txt` – Die Datei enthält Informationen über die Prozesse, die gerade auf dem VPN-Gateway oder der VPN-Appliance ausgeführt werden.

`resolf.conf.txt` – Die Datei enthält Informationen über die Konfiguration der DNS-Server.

`routes.txt` – Die Datei enthält Informationen über die Netzwerk-Routen.

`uname.txt` – Die Datei enthält Informationen über die aktuelle Kernel-Version des Betriebssystems.

`uptime.txt` – Die Datei enthält Informationen über den Zeitraum, in dem das Betriebssystem nicht neu gestartet worden ist.

`vpnserver_log.txt` – Die Datei enthält Protokolle vom VPN-Dienst.

`vpnserver_status.txt` – Die Datei enthält Informationen über den Status des VPN-Servers.

Weitere Informationen zu den Protokolldateien, die für die IPsec-VPN-Konnektivität spezifisch sind, finden Sie im Abschnitt '"Multi-Site-IPSec-VPN-Protokolldateien" (S. 854)'.

Die Protokolle der VPN-Appliance herunterladen

Sie können das Archiv, das die Protokolle der VPN-Appliance enthält, herunterladen, dann extrahieren und die Informationen zur Fehlerbehebung oder zum Monitoring verwenden.

So können Sie die Protokolle der VPN-Appliance herunterladen

1. Klicken Sie auf der Seite **Verbindung** auf das Zahnradsymbol neben der VPN-Appliance.
2. Klicken Sie auf **Protokoll herunterladen**.
3. [Optional] Wählen Sie **Netzwerkpakete erfassen** und konfigurieren Sie die Einstellungen. Weitere Informationen finden Sie im Abschnitt '"Netzwerkpakete erfassen" (S. 850)'.

4. Klicken Sie auf **Fertig**.
5. Wenn das .zip-Archiv zum Herunterladen bereit ist, klicken Sie auf **Protokoll herunterladen** und speichern Sie es lokal.

Die Protokolle des VPN-Gateways herunterladen

Sie können das Archiv, das die Protokolle des VPN-Gateways enthält, herunterladen, dann extrahieren und die Informationen zur Fehlerbehebung oder zum Monitoring verwenden.

So können Sie die Protokolle des VPN-Gateways herunterladen

1. Klicken Sie auf der Seite **Verbindung** auf das Zahnradsymbol neben dem VPN-Gateway.
2. Klicken Sie auf **Protokoll herunterladen**.
3. [Optional] Wählen Sie **Netzwerkpakete erfassen** und konfigurieren Sie dann die Einstellungen. Weitere Informationen finden Sie im Abschnitt '"Netzwerkpakete erfassen" (S. 850)'.
4. Klicken Sie auf **Fertig**.
5. Wenn das .zip-Archiv zum Herunterladen bereit ist, klicken Sie auf **Protokoll herunterladen** und speichern Sie es lokal.

Netzwerkpakete erfassen

Wenn Sie die Kommunikation zwischen dem lokalen Produktionsstandort und einem primären Server oder Recovery-Server analysieren bzw. zwischen diesen auftretende Probleme beheben wollen, können Sie Netzwerkpakete auf dem VPN-Gateway oder der VPN-Appliance sammeln lassen.

Nachdem 32000 Netzwerkpakete gesammelt wurden oder das Zeitlimit erreicht wurde, wird die Netzwerkpaket-Erfassung beendet und die Ergebnisse werden in eine .libpcap-Datei geschrieben, die in das .zip-Archiv der Protokolle aufgenommen wird.

n der nachfolgenden Tabelle finden Sie weitere Informationen zu den **Netzwerkpakete erfassen**-Einstellungen, die Sie konfigurieren können.

Einstellung	Beschreibung
Netzwerkschnittstellenname	Die Netzwerkschnittstelle, über die Netzwerkpakete erfasst werden sollen. Wenn Sie Netzwerkpakete auf allen Netzwerkschnittstellen erfassen wollen, wählen Sie die Option **Alle**.
Zeitlimit (in Sekunden)	as Zeitlimit für die Erfassung von Netzwerkpaketen. Der Höchstwert, den Sie festlegen können, ist 1800.
Filterung	Ein zusätzlicher Filter, der auf die erfassten Netzwerkpakete angewendet wird. Sie können eine Zeichenfolge eingeben, die Protokolle, Ports, Richtungen sowie deren Kombinationen enthält,

Einstellung	Beschreibung
	durch Leerzeichen getrennt – beispielsweise: "and", "or", "not", " (", ") ", "src", "dst", "net", "host", "port", "ip", "tcp", "udp", "icmp", "arp", "esp". Wenn Sie Klammern verwenden wollen, müssen Sie diese mit Leerzeichen umschließen. Sie können außerdem IP-Adressen und Netzwerkadressen eingeben. Beispielsweise: "icmp or arp" und "port 67 or 68". Weitere Informationen über die Werte, die Sie eingeben können, finden Sie in der Linux-Hilfe für tcpdump.

Probleme mit der IPsec-VPN-Konfiguration beheben

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Wenn Sie die IPsec-VPN-Verbindung konfigurieren oder verwenden, kann es gelegentlich auch zu Problemen kommen.

Wenn Sie auf Probleme stoßen, können Sie die IPsec-Protokolldateien auswerten und im Abschnitt 'IPsec-VPN-Konfigurationsprobleme beheben' nach möglichen Lösungen für gängige Probleme suchen.

IPsec-VPN-Konfigurationsprobleme beheben

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Die nachfolgende Tabelle beschreibt häufig auftretende IPsec-VPN-Konfigurationsprobleme und erläutert, wie Sie diese beheben können.

Problem	Mögliche Lösung
Ich sehe folgende Fehlermeldung: **IKE-Phase-1-Aushandlungsfehler. Überprüfen Sie die IPsec-IKE-Einstellungen auf den Cloud- und den lokalen Sites.**	Klicken Sie zuerst auf **Wiederholen** und überprüfen Sie, ob eine spezifischere Fehlermeldung erscheint. Eine solche spezifischere Fehlermeldung kann z.B. Angaben zu einer Algorithmus-Diskrepanz oder einem falschen vorinstallierten Schlüssel (PSK) enthalten.

Problem	Mögliche Lösung
	Hinweis Aus Sicherheitsgründen gelten für IPsec-VPN-Verbindungen folgende Einschränkungen: • IKEv1 wird in RFC8247 als nicht mehr zeitgemäß bezeichnet und aufgrund von Sicherheitsrisiken daher nicht mehr unterstützt. Es werden nur Verbindungen mit dem IKEv2-Protokoll unterstützt. • Folgende Verschlüsselungsalgorithmen gelten mittlerweile als unsicher und werden daher nicht mehr unterstützt: DES und 3DES. • Folgende Hash-Algorithmen gelten mittlerweile als unsicher und werden daher nicht mehr unterstützt: SHA1 und MD5. • Die Diffie-Hellman-Gruppennummer 2 gilt als unsicher und wird daher nicht unterstützt.
Die Verbindung zwischen meinem lokalen Standort und der Cloud-Site bleibt im Status **Verbindungsaufbau** hängen.	Überprüfen Sie: • Falls der UDP-Port 500 offen ist (wenn Sie eine Firewall verwenden). • Die Konnektivität zwischen dem lokalen Standort und der Cloud-Site. • Falls die IP-Adresse des lokalen Standorts korrekt ist.
Die Verbindung zwischen meinem lokalen Standort und der Cloud-Site bleibt im Status **Auf eine Verbindung warten** hängen.	Dieser Status wird angezeigt, wenn die **Aktion bei Start** für die Cloud-Site mit **Hinzufügen** festgelegt wurde, was bedeutet, dass die Cloud-Site darauf wartet, dass der lokale Standort die Verbindung initiiert. Die Verbindung vom lokalen Standort aus initiieren.
Die Verbindung zwischen meinem lokalen Standort und der Cloud-Site bleibt im Status **Auf Datenverkehr warten** hängen.	Dieser Zustand wird angezeigt, wenn die **Aktion bei Start** für die Cloud-Site mit **Route** festgelegt wurde. Gehen Sie wie folgt vor, wenn Sie eine Verbindung vom lokalen Standort aus erwarten: • Versuchen Sie vom lokalen Standort aus die virtuelle Maschine in der Cloud-Site anzupingen. Dies ist ein Standardverhalten, das bei einigen Geräten (z.B. Cisco ASA) zum Aufbau eines VPN-Tunnels notwendig ist. (Route-Modus)

Problem	Mögliche Lösung
	• Stellen Sie sicher, dass der lokale Standort einen VPN-Tunnel eingerichtet hat, indem Sie die **Aktion bei Start** für den lokalen Standort mit **Start** festlegen.
Die Verbindung zwischen meinem lokalen Standort und der Cloud-Site ist hergestellt, aber ich kann sehen, dass eine oder mehrere Netzwerkrichtlinien nicht funktionieren.	Dieses Problem kann folgende Ursachen haben: • Die Netzwerkzuordnung in der IPsec-Cloud-Site unterscheidet sich von der Netzwerkzuordnung am lokalen Standort. Stellen Sie sicher, dass die Netzwerk-Zuordnungen und die Abfolge der Netzwerk-Richtlinien am lokalen Standort und in der Cloud-Site genau übereinstimmen. • Dieses Stadium ist korrekt, wenn die **Aktion bei Start** des lokalen Standorts und/oder der Cloud-Site auf **Route** eingestellt ist (z.B. auf Cisco ASA-Geräten) und derzeit kein Datenverkehr stattfindet. Sie können einen Ping-Test durchführen, um sicherzustellen, dass der Tunnel korrekt aufgebaut wurde. Wenn der Ping-Test nicht funktioniert, prüfen Sie die Netzwerkzuordnung am lokalen Standort und in der Cloud-Site.
Ich möchte eine bestimmte IPsec-Verbindung neu starten.	So können Sie eine bestimmte IPsec-Verbindung neu starten: 1. Klicken Sie in der Anzeige **Disaster Recovery** –> **Verbindung** auf die gewünschte IPsec-Verbindung. 2. Klicken Sie auf **Verbindung deaktivieren**. 3. Klicken Sie erneut auf die IPsec-Verbindung. 4. Klicken Sie auf **Verbindung aktivieren**.

Die IPsec-VPN-Protokolldateien herunterladen

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Sie können zusätzliche Informationen über die IPsec-Konnektivität in den Protokolldateien auf dem VPN-Server finden. Die Protokolldateien befinden sich komprimiert in einem .zip-Archiv, welches Sie herunterladen und entpacken können.

Voraussetzungen

Die Multi-Site-IPsec-VPN-Konnektivität ist konfiguriert.

So können Sie das .zip-Archiv mit den Protokolldateien herunterladen

1. Gehen Sie in der Cyber Protect-Konsole zu **Disaster Recovery** –> **Verbindung**.
2. Klicken Sie neben dem VPN-Gateway der Cloud-Site auf das Zahnradsymbol.
3. Klicken Sie auf **Protokoll herunterladen**.
4. Klicken Sie auf **Fertig**.
5. Wenn das .zip-Archiv zum Herunterladen bereit ist, klicken Sie auf **Protokoll herunterladen** und speichern Sie es lokal.

Multi-Site-IPSec-VPN-Protokolldateien

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Die folgende Liste beschreibt die IPsec-VPN-Protokolldateien, die Teil des .zip-Archivs sind, und die darin enthaltenen Informationen.

- `ip.txt` – Diese Datei enthält die Protokolle über die Konfiguration der Netzwerkschnittstellen. Sie müssen zwei IP-Adressen sehen: eine öffentliche IP-Adresse und eine lokale IP-Adresse. Wenn Sie diese IP-Adressen nicht im Protokoll sehen, liegt ein Problem vor. Kontaktieren Sie dann den Support.

  Hinweis
  Die Netzwerkmaske für die öffentliche IP-Adresse muss 32 sein.

- `swanctl-list-loaded-config.txt` – Diese Datei enthält Informationen über alle IPsec-Standorte (Sites).
  Wenn Sie in der Datei keinen Standort sehen, wurde die IPsec-Konfiguration nicht angewendet. Versuchen Sie, die Konfiguration zu aktualisieren und zu speichern – oder wenden Sie sich an den Support.
- `swanctl-list-active-sas.txt` – Diese Datei enthält Verbindungen und Richtlinien, die sich im Status 'aktiv' oder 'Verbindungsaufbau' befinden.

Recovery-Server einrichten

Dieser Abschnitt beschreibt die Konzepte von Failover und Failback, die Erstellung eines Recovery-Servers und die entsprechenden Disaster Recovery-Aktionen.

Einen Recovery-Server erstellen

Wenn Sie einen Recovery-Server erstellen wollen, der eine Kopie Ihres Workloads ist, gehen Sie wie nachfolgend beschrieben vor. Sie können sich außerdem das Video-Tutorial ansehen, in dem der Prozess demonstriert wird.

Wichtig
Wenn Sie einen Failover durchführen, können Sie nur Recovery-Punkte auswählen, die erst nach dem Erstellen des Recovery-Servers erstellt wurden.

Voraussetzungen

- Sie müssen einer ursprünglichen Maschine, die Sie sichern wollen, einen Schutzplan zuweisen. Dieser Plan muss die komplette Maschine in den Cloud Storage sichern – oder nur diejenigen Laufwerke, die zum Booten und zur Bereitstellung notwendiger Dienste erforderlich sind.
- Einer der Verbindungstypen zur Cloud-Site muss festgelegt sein.

So können Sie einen Recovery-Server erstellen

1. Wählen Sie in der Registerkarte **Alle Geräte** diejenige Maschine aus, den Sie schützen wollen.
2. Klicken Sie zuerst auf **Disaster Recovery** und dann auf **Recovery-Server erstellen**.
3. Bestimmen Sie die Anzahl der virtuellen CPU-Kerne und die Größe des Arbeitsspeichers.

   Hinweis
   Sie können die Berechnungspunkte für jede Option sehen. Die Anzahl der Berechnungspunkte spiegelt wieder, wie viel die Ausführung des Recovery-Servers pro Stunde kostet. Weitere Informationen finden Sie im Abschnitt '"Berechnungspunkte" (S. 808)'.

4. Spezifizieren Sie das Cloud-Netzwerk, mit dem der Server verbunden werden soll.
5. Wählen Sie die **DHCP**-Option.

DHCP-Option	Beschreibung
Von der Cloud-Site bereitgestellt	Standardeinstellung. Die IP-Adresse des Servers wird von einem automatisch konfigurierten DHCP-Server in der Cloud bereitgestellt.
Benutzerdefiniert	Die IP-Adresse des Servers wird von Ihrem eigenen DHCP-Server in der Cloud bereitgestellt.

6. [Optional] Spezifizieren Sie die **MAC-Adresse**.
   Die MAC-Adresse ist eine eindeutige Kennung, die dem Netzwerkadapter des Servers zugewiesen wird. Wenn Sie benutzerdefiniertes DHCP verwenden, können Sie es so konfigurieren, dass einer bestimmten MAC-Adresse immer eine bestimmte IP-Adresse zugewiesen wird. Auf diese Weise können Sie sicherstellen, dass der Recovery-Server immer die gleiche IP-Adresse erhält. Dadurch können Sie Applikationen ausführen, die Lizenzen haben, die wiederum auf die MAC-Adresse registriert sind.

7. Spezifizieren Sie die IP-Adresse, die der Server im Produktionsnetzwerk haben wird. Standardmäßig ist die IP-Adresse der ursprünglichen Maschine vorgegeben.

   Hinweis
   Falls Sie einen DHCP-Server verwenden, fügen Sie dessen IP-Adresse zu der Server-Ausschlussliste hinzu, um IP-Adressen-Konflikte zu vermeiden.
   Wenn Sie einen benutzerdefinierten DHCP-Server verwenden, müssen Sie unter **IP-Adresse im Produktionsnetzwerk** dieselbe IP-Adresse spezifizieren, die im DHCP-Server konfiguriert ist. Ansonsten wird der Test-Failover nicht richtig funktionieren und der Server wird nicht über eine öffentliche IP-Adresse erreichbar sein.

8. [Optional] Aktivieren Sie das Kontrollkästchen **Test-IP-Adresse** und spezifizieren Sie dann die IP-Adresse.
   Dies gibt Ihnen die Möglichkeit, einen Failover im isolierten Testnetzwerk zu testen und sich während eines Test-Failovers per RDP oder SSH mit dem Recovery-Server zu verbinden. Im Test-Failover-Modus wird das VPN-Gateway mithilfe des NAT-Protokolls die Test-IP-Adresse gegen die Produktions-IP-Adresse ersetzen.
   Wenn Sie das Kontrollkästchen deaktiviert lassen, können Sie sich während eines Test-Failovers nur über die Konsole mit dem Server verbinden.

   Hinweis
   Falls Sie einen DHCP-Server verwenden, fügen Sie dessen IP-Adresse zu der Server-Ausschlussliste hinzu, um IP-Adressen-Konflikte zu vermeiden.

   Sie können eine der vorgeschlagenen IP-Adressen verwenden oder eine andere eingeben.
9. [Optional] Aktivieren Sie das Kontrollkästchen **Internetzugriff**.
   Dies ermöglicht es dem Recovery-Server, sich während eines Failovers (auch im Testmodus) mit dem Internet zu verbinden. Standardmäßig ist der TCP-Port 25 für ausgehende Verbindungen zu öffentlichen IP-Adressen geöffnet.
10. [Optional] Legen Sie einen **RPO-Grenzwert** fest.
    Der RPO-Grenzwert definiert also das maximale Zeitintervall, das zwischen dem letzten (für einen Failover verwendbaren) Recovery-Punkt und dem aktuellen Zeitpunkt (an dem es zu einem Desaster kommen kann) zulässig ist. Der Wert kann zwischen 15–60 Minuten, 1–24 Stunden oder 1–14 Tagen eingestellt werden.
11. [Optional] Aktivieren Sie das Kontrollkästchen **Öffentliche IP-Adresse verwenden**.
    Wenn der Recovery-Server über eine öffentliche IP-Adresse verfügt, ist er während eines Failovers (auch im Testmodus) aus dem Internet verfügbar. Wenn Sie das Kontrollkästchen deaktiviert lassen, wird der Server nur in Ihrem Produktionsnetzwerk verfügbar sein.
    Die Option **Öffentliche IP-Adresse verwenden** erfordert, dass die Option **Internetzugriff** ebenfalls aktiviert ist.
    Die öffentliche IP-Adresse wird angezeigt, nachdem Sie die Konfiguration abgeschlossen haben. Standardmäßig ist der TCP-Port 443 für eingehende Verbindungen zu öffentlichen IP-Adressen geöffnet.

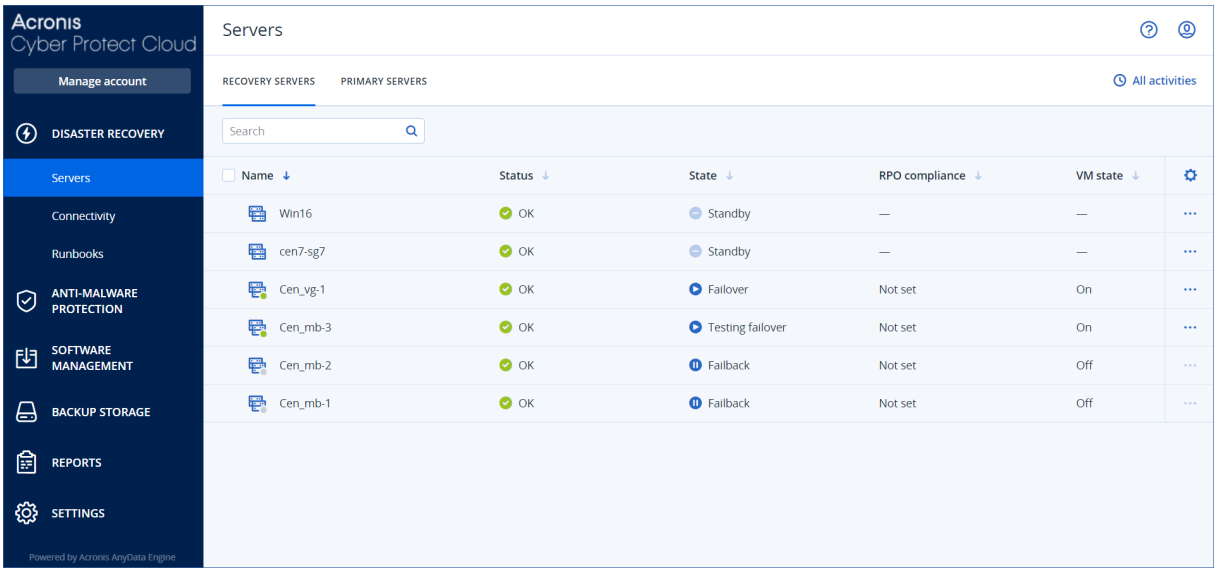
Hinweis
Wenn Sie das Kontrollkästchen **Öffentliche IP-Adresse verwenden** deaktivieren oder den Recovery-Server löschen, wird dessen öffentliche IP-Adresse nicht reserviert.

12. [Optional] [Wenn die Backups für die ausgewählte Maschine verschlüsselt sind, indem die Verschlüsselung als Maschineneigenschaft verwendet wird] Spezifizieren Sie das Kennwort, das automatisch verwendet wird, wenn eine virtuelle Maschine für den Recovery-Server aus dem verschlüsselten Backup erstellt wird.
    a. Klicken Sie zuerst auf **Spezifizieren**, geben Sie dann das Kennwort für das verschlüsselte Backup ein und definieren Sie dann einen Namen für die Anmeldedaten.
    Standardmäßig wird Ihnen das neueste Backup in der Liste angezeigt.
    b. [Optional] Wenn Sie alle Backups sehen wollen, müssen Sie auf **Alle Backups anzeigen** klicken.
    c. Klicken Sie auf **Fertig**.

Hinweis
Obwohl das von Ihnen spezifizierte Kennwort in einem sicheren Anmeldedatenspeicher hinterlegt wird, kann es dennoch sein, dass das Speichern von Kennwörtern gegen Ihre Compliance-Auflagen verstößt.

13. [Optional] Ändern Sie den Namen des Recovery-Servers.
14. [Optional] Geben Sie eine Beschreibung für den Recovery-Server ein.
15. [Optional] Klicken Sie auf die Registerkarte **Cloud-Firewall-Regeln**, um die Standard-Firewall-Regeln zu bearbeiten. Weitere Informationen finden Sie im Abschnitt '"Firewall-Regeln für Cloud Server einrichten" (S. 885)'.
16. Klicken Sie auf **Erstellen**.

Der Recovery-Server wird in der Cyber Protect-Konsole in der Registerkarte **Disaster Recovery** –> **Server** –> **Recovery-Server** angezeigt. Sie können dessen Einstellungen einsehen, wenn Sie die ursprüngliche Maschine auswählen und dann auf **Disaster Recovery** klicken.



Wie ein Failover funktioniert

Produktions-Failover

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Wenn ein Recovery-Server erstellt wird, verbleibt er zunächst im **Standby**-Stadium. Die entsprechende virtuelle Maschine existiert erst, wenn Sie den Failover starten. Bevor Sie einen Failover-Prozess starten, müssen Sie mindestens ein Disk-Image-Backup (mit bootfähigem Volume) von der ursprünglichen Maschine erstellen.

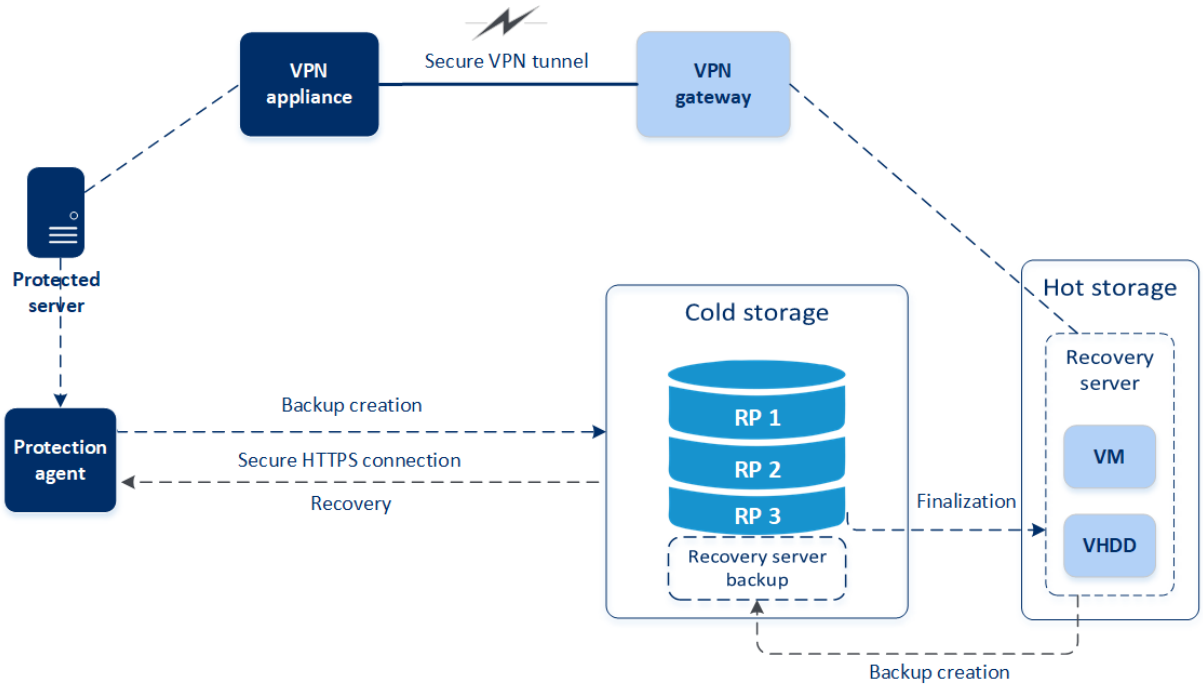
Wenn Sie den Failover-Prozess starten, wählen Sie den Recovery-Punkt (das Backup) der ursprünglichen Maschine, aus der dann eine virtuelle Maschine mit vordefinierten Parametern erstellt wird. Eine Failover-Aktion basiert auf der Funktion „VM von Backup ausführen“. Der Recovery-Server erhält das Übergangsstadium **Finalisierung**. Dieser Prozess beinhaltet die Übertragung der virtuellen Laufwerke des Servers aus dem Backup Storage („Cold Storage“) zum Disaster Recovery Storage („Hot Storage“).

Hinweis
Der Server bleibt während der **Finalisierung** verfügbar und betriebsbereit. Die Performance ist gegenüber dem Normalzustand jedoch herabgesetzt. Sie können die Server-Konsole öffnen, indem Sie auf den Link **Konsole ist bereit** klicken. Der Link ist in der Spalte **VM-Stadium** auf der Anzeige **Disaster Recovery** –> **Server** sowie in der Ansicht **Details** des Servers verfügbar.

Wenn die **Finalisierung** abgeschlossen ist, erreicht der Server wieder eine normale Performance. Das Server-Stadium wird auf **Failover** geändert. Der Workload wird nun von der ursprünglichen Maschine zum Recovery-Server in der Cloud-Site umgeschaltet (übertragen).

Wenn auf dem Recovery-Server ein Protection Agent ist, wird der Agenten-Dienst gestoppt, um Störungen (wie Backup-Starts oder das Senden veralteter Statusmeldungen an die Backup-Komponente) zu vermeiden.

Die untere Abbildung verdeutlicht die Failover- und Failback-Prozesse.



Failover testen

Bei einem **Test-Failover** wird die virtuelle Maschine nicht finalisiert. Das bedeutet, dass der Agent die Inhalte der virtuellen Laufwerke direkt aus dem Backup auslesen kann, also die verschiedenen Bereiche des Backups per wahlfreien Zugriff verfügbar sind und dass dessen Performance unter Umständen langsamer als normal ist. Weitere Informationen über den Failover-Prozess finden Sie im Abschnitt '"Einen Test-Failover durchführen" (S. 859)'.

Automatisierter Test-Failover

Wenn der automatisierte Failover-Test konfiguriert ist, wird er einmal im Monat durchgeführt, ohne dass ein manuelles Eingreifen erforderlich ist. Weitere Informationen dazu finden Sie in den Abschnitten '"Automatisierter Test-Failover" (S. 862)' und '"Automatisierte Test-Failover konfigurieren" (S. 863)'.

Einen Test-Failover durchführen

Einen Test-Failover durchzuführen bedeutet, einen Recovery-Server in einem Test-VLAN zu starten, welches von Ihrem Produktionsnetzwerk isoliert ist. Sie können mehrere Recovery-Server gleichzeitig testen und deren Interaktion überprüfen. Innerhalb des Testnetzwerks kommunizieren die Server über ihre Produktions-IP-Adressen. Die Server können jedoch keine TCP- oder UDP-Verbindungen zu den Workloads in Ihrem lokalen Netzwerk (LAN) aufbauen.

Bei einem Test-Failover wird die virtuelle Maschine (der Recovery-Server) nicht finalisiert. Der Agent liest die Inhalte der virtuellen Laufwerke direkt aus dem Backup aus und hat dabei wahlfreien Zugriff auf die verschiedenen Bereiche des Backups. Dies kann dazu führen, dass die Performance des Recovery-Servers im Test-Failover-Stadium langsamer ist als seine normale Performance.

Obwohl die Durchführung eines Test-Failovers optional ist, empfehlen wir Ihnen, einen solchen doch so häufig durchzuführen, wie Sie es unter Berücksichtigung der Faktoren Kosten und Sicherheit passend finden. Bewährt hat sich die Erstellung eines sogenannten Runbooks. Das ist eine Zusammenstellung von Anweisungen, die beschreibt, wie die Produktionsumgebung in die Cloud übertragen wird.

Wichtig
Sie müssen bereits im Vorfeld einen Recovery-Server erstellen, um Ihre Geräte vor einem möglicherweise auftretenden Desaster schützen zu können.

Sie können einen Failover nur aus Recovery-Punkten durchführen, die erstellt wurden, nachdem der Recovery-Server des Gerätes erstellt wurde.

Es muss mindestens ein Recovery-Punkt erstellt worden sein, bevor ein Failover-Prozess zu einem Recovery-Server durchgeführt werden kann. Die maximale Anzahl der unterstützten Recovery-Punkte beträgt 100.

So können Sie einen Test-Failover durchführen

1. Wählen Sie die ursprüngliche Maschine oder den Recovery-Server aus, für die/den Sie den Test durchführen wollen.
2. Klicken Sie auf **Disaster Recovery**.
   Die Beschreibung des Recovery-Servers wird angezeigt.
3. Klicken Sie auf **Failover**.
4. Wählen Sie **Failover testen** als Art des durchzuführenden Failovers aus.
5. Wählen Sie den gewünschten Recovery-Punkt (das Backup) und klicken Sie dann auf **Start**.
6. Wenn das von Ihnen ausgewählte Backup verschlüsselt ist, wobei die Verschlüsselung über die Maschineneigenschaften festgelegt ist:
   a. Geben Sie das Verschlüsselungskennwort für den Backup-Satz ein.

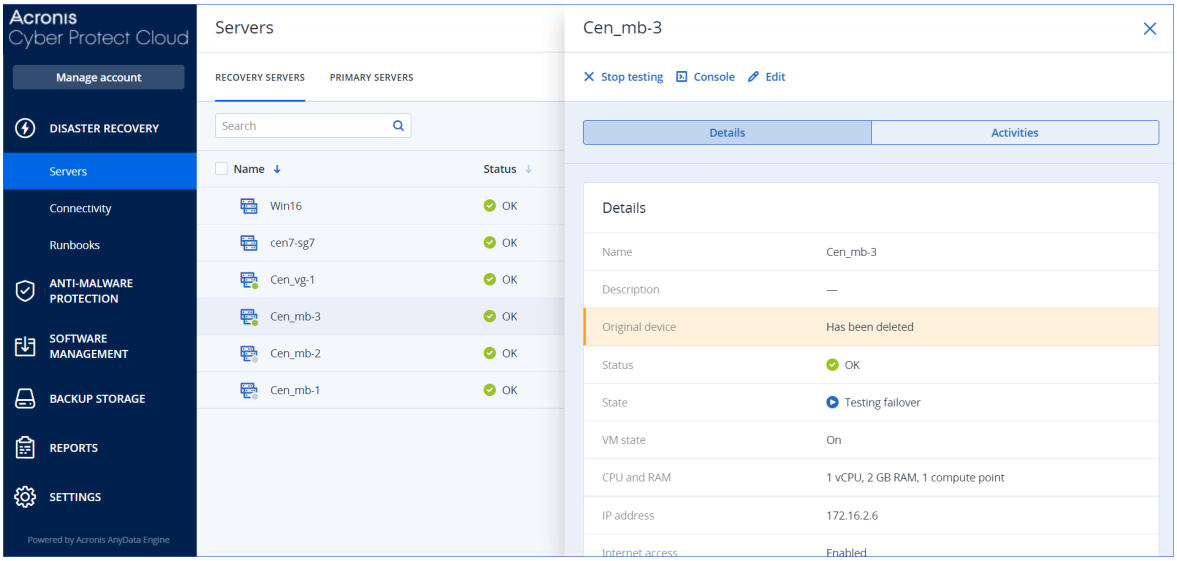
      Hinweis
      Das Kennwort wird nur temporär gespeichert und nur für die aktuelle Test-Failover-Aktion verwendet. Das Kennwort wird automatisch aus dem Anmeldedatenspeicher gelöscht, wenn der Test-Failover-Prozess gestoppt wird oder abgeschlossen wurde.

   b. [Optional] Wenn Sie das Kennwort für den Backup-Satz speichern und für nachfolgende Failover-Aktionen verwenden wollen, müssen Sie das Kontrollkästchen **Das Kennwort in einem sicheren Anmeldedatenspeicher speichern...** aktivieren und dann im Feld **Anmeldedatenname** einen Namen für die Anmeldedaten eingeben.

Wichtig
Das Kennwort wird in einem sicheren Anmeldedatenspeicher hinterlegt und bei späteren Failover-Aktionen automatisch angewendet. Es kann jedoch sein, dass das Speichern von Kennwörtern im Konflikt mit Ihren Compliance-Verpflichtungen steht.

c. Klicken Sie auf **Fertig**.

Wenn der Recovery-Server gestartet ist, ändert sich dessen Stadium auf '**Failover wird getestet**'.



7. Testen Sie den Recovery-Server mit einer der nachfolgenden Methoden:
   - Wählen Sie bei **Disaster Recovery** –> **Server** den gewünschten Recovery-Server aus und klicken Sie dann auf **Konsole**.
   - Verbinden Sie sich per RDP oder SSH mit dem Recovery-Server und verwenden Sie dabei die Test-IP-Adresse, die Sie bei der Erstellung des Recovery-Servers spezifiziert haben. Testen Sie die Verbindung sowohl innerhalb als auch außerhalb des Produktionsnetzwerks (wie im Abschnitt 'Point-to-Site-Verbindung' beschrieben).
   - Führen Sie ein Skript im Recovery-Server aus.

     Dieses Skript kann beispielsweise den Anmeldebildschirm überprüfen, ob Applikationen gestartet wurden, ob eine Internetverbindung besteht oder ob sich andere Maschinen mit dem Recovery-Server verbinden können.
   - Wenn der Recovery-Server auf das Internet zugreifen kann und eine öffentliche IP-Adresse hat, können Sie auch TeamViewer verwenden.
8. Klicken Sie nach Abschluss der Installation auf **Test stoppen**.

   Der Recovery-Server wird gestoppt. Alle Änderungen am Recovery-Server, die während des Test-Failovers erfolgten, gehen verloren.

Hinweis
Die Aktionen **Server starten** und **Server stoppen** sind für Test-Failover-Aktionen nicht anwendbar, egal ob in Runbooks oder beim manuellen Starten eines Test-Failovers. Wenn Sie versuchen, eine solche Aktion auszuführen, wird diese mit folgender Fehlermeldung fehlschlagen: Fehlgeschlagen: Die Aktion ist auf das aktuelle Server-Stadium nicht anwendbar.

Automatisierter Test-Failover

Mit einem automatisierten Test-Failover kann der Recovery-Server einmal im Monat automatisch getestet werden, ohne dass manuelle Eingriffe erforderlich sind.

Der automatisierte Test-Failover-Prozess besteht aus folgenden Abschnitten:

1. Es wird eine virtuelle Maschine aus dem jüngsten Recovery-Punkt erstellt
2. Es wird ein Screenshot von der virtuellen Maschine aufgenommen
3. Es wird analysiert, ob das Betriebssystem der virtuellen Maschine erfolgreich startet
4. Sie werden über den Status des Failover-Tests benachrichtigt

Hinweis
Automatisierte Test-Failover verbrauchen Berechnungspunkte.

Sie können die automatisierten Test-Failover in den Einstellungen des Recovery-Servers konfigurieren. Weitere Informationen finden Sie im Abschnitt '"Automatisierte Test-Failover konfigurieren" (S. 863)'.

Beachten Sie, dass es in sehr seltenen Fällen vorkommen kann, dass ein automatisierter Test-Failover übersprungen und nicht zum geplanten Zeitpunkt durchgeführt wird. Weil ein Produktions-Failover eine höhere Priorität als ein automatisierter Test-Failover hat, werden die Hardware-Ressourcen (CPU und RAM), die dem automatisierten Test-Failover zugeordnet wurden, möglicherweise vorübergehend eingeschränkt, um sicherzustellen, dass für einen gleichzeitig stattfindenden Produktions-Failover genügend Ressourcen vorhanden sind.

Wenn ein automatisierter Test-Failover aus irgendeinem Grund übersprungen wird, wird eine entsprechende Alarmmeldung ausgelöst.

Hinweis
Der automatisierte Failover-Test wird fehlschlagen, wenn die Backups der ursprünglichen Maschine verschlüsselt sind (wobei die Verschlüsselung als Maschinen-Eigenschaft festgelegt wurde) und das Verschlüsselungskennwort beim Erstellen des Recovery-Servers nicht spezifiziert wurde. Weitere Informationen über das Spezifizieren des Verschlüsselungskennworts finden Sie im Abschnitt '"Einen Recovery-Server erstellen" (S. 855)'.

Automatisierte Test-Failover konfigurieren

Durch die Konfiguration eines automatisierten Test-Failovers können Sie Ihren Recovery-Server jeden Monat automatisiert testen lassen, ohne dabei manuell eingreifen zu müssen.

So können Sie einen automatisierten Test-Failover konfigurieren

1. Gehen Sie in der Konsole zu **Disaster Recovery** –> **Server** –> **Recovery-Server** und wählen Sie den gewünschten Recovery-Server aus.
2. Klicken Sie auf **Bearbeiten**.
3. Wählen Sie im Bereich **Automatisierter Test-Failover** im Feld **Planung** die Option **Monatlich**.
4. [Optional] Ändern Sie bei **Screenshot-Zeitlimit** den Standardwert für den maximalen Zeitraum (in Minuten), in dem das System versuchen soll, einen automatisierten Test-Failover durchzuführen.
5. [Optional] Wenn Sie den Wert für das **Screenshot-Zeitlimit** als Standard speichern und automatisch eintragen lassen wollen, wenn Sie einen automatisierten Test-Failover für andere Recovery-Server aktivieren, wählen Sie **Als Standard-Zeitlimit speichern**.
6. Klicken Sie auf **Speichern**.

Den Status des automatisierten Test-Failovers einsehen

Sie können sich die Details eines abgeschlossenen automatisierten Test-Failovers anzeigen lassen, z.B. den Status, die Startzeit, die Endzeit, die Dauer sowie einen Screenshot der virtuellen Maschine.

So können Sie sich den automatisierten Test-Failover-Status eines Recovery-Servers anzeigen lassen

1. Gehen Sie in der Konsole zu **Disaster Recovery** –> **Server** –> **Recovery-Server** und wählen Sie den gewünschten Recovery-Server aus.
2. Überprüfen Sie im Bereich **Automatisierter Test-Failover** die angezeigten Details des letzten automatisierten Test-Failovers.
3. [Optional] Klicken Sie auf **Screenshot anzeigen**, um sich den Screenshot der virtuellen Maschine anzusehen.

Automatisierte Test-Failover deaktivieren

Sie können einen automatisierten Test-Failover deaktivieren, wenn Sie Ressourcen einsparen wollen oder für einen bestimmten Recovery-Server keinen automatisierten Test-Failover durchführen müssen.

So können Sie einen automatisierten Test-Failover deaktivieren

1. Gehen Sie in der Konsole zu **Disaster Recovery** –> **Server** –> **Recovery-Server** und wählen Sie den gewünschten Recovery-Server aus.
2. Klicken Sie auf **Bearbeiten**.

3. Wählen Sie im Bereich **Automatisierter Test-Failover** im Feld **Planung** die Option **Nie**.
4. Klicken Sie auf **Speichern**.

Einen Failover durchführen

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Ein Failover ist ein Prozess, bei dem ein Workload von Ihren lokalen Systemen (on-premise) in die Cloud verschoben wird. Der Begriff wird außerdem auch für das Stadium verwendet, wenn der Workload in der Cloud bleibt.

Wenn Sie einen Failover-Prozess starten, wird der Recovery-Server im Produktionsnetzwerk gestartet. Um Störungen und unerwünschte Problemen zu vermeiden, sollten Sie sicherstellen, dass der ursprüngliche Workload nicht mehr online ist und nicht per VPN zugänglich ist.

Um zu vermeiden, dass Backups, die in dasselbe Cloud-Archiv durchgeführt werden, gestört werden, sollten Sie den Schutzplan vom Workload, der sich gerade im **Failover**-Stadium befindet, manuell widerrufen. Weitere Informationen über das Widerrufen von Plänen finden Sie im Abschnitt Einen Schutzplan widerrufen.

Wichtig
Sie müssen bereits im Vorfeld einen Recovery-Server erstellen, um Ihre Geräte vor einem möglicherweise auftretenden Desaster schützen zu können.

Sie können einen Failover nur aus Recovery-Punkten durchführen, die erstellt wurden, nachdem der Recovery-Server des Gerätes erstellt wurde.

Es muss mindestens ein Recovery-Punkt erstellt worden sein, bevor ein Failover-Prozess zu einem Recovery-Server durchgeführt werden kann. Die maximale Anzahl der unterstützten Recovery-Punkte beträgt 100.

Sie können die nachfolgenden Anleitungen befolgen oder sich das Video-Tutorial ansehen.

So können Sie einen Failover durchführen

1. Überprüfen Sie, dass die ursprüngliche Maschine nicht mehr im Netzwerk verfügbar ist.
2. Gehen Sie in der Cyber Protect-Konsole zu **Disaster Recovery** –> **Server** –> **Recovery-Server** und wählen Sie den gewünschten Recovery-Server aus.
3. Klicken Sie auf **Failover**.
4. Wählen Sie **Produktions-Failover** als Art des durchzuführenden Failovers aus.
5. Wählen Sie den gewünschten Recovery-Punkt (das Backup) und klicken Sie dann auf **Start**.
6. [Wenn das von Ihnen ausgewählte Backup verschlüsselt ist, wobei die Verschlüsselung über die Maschineneigenschaften festgelegt ist]

a. Geben Sie das Verschlüsselungskennwort für den Backup-Satz ein.

Hinweis
Das Kennwort wird nur temporär gespeichert und nur für die aktuelle Failover-Aktion verwendet. Das Kennwort wird automatisch aus dem Anmeldedatenspeicher gelöscht, nachdem die Failover-Aktion abgeschlossen wurde und der Server in das Stadium **Standby** zurückgesetzt wurde.

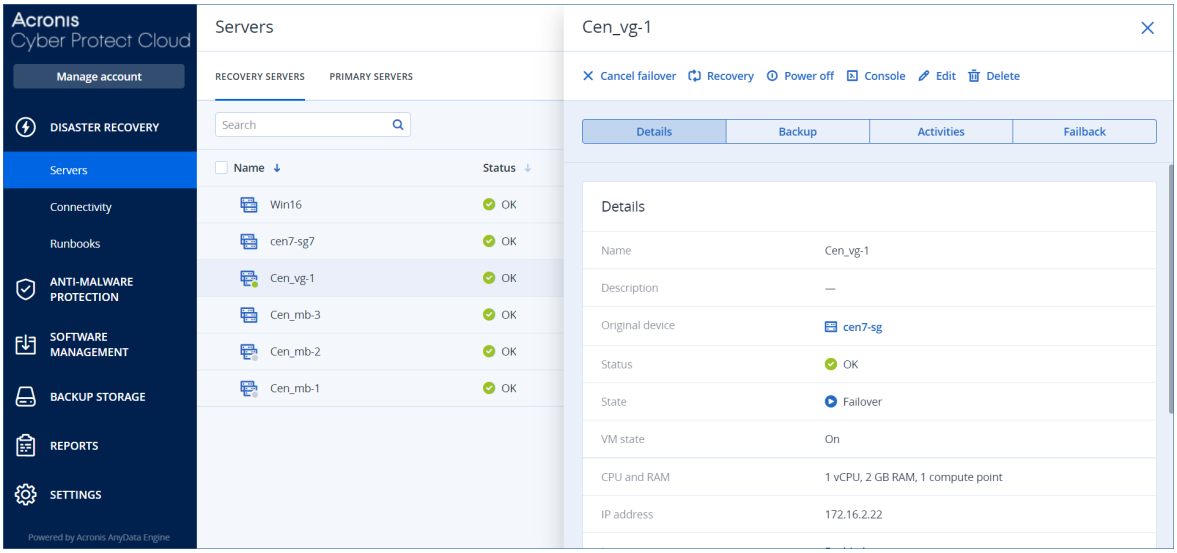
b. [Optional] Wenn Sie das Kennwort für den Backup-Satz speichern und für nachfolgende Failover-Aktionen verwenden wollen, müssen Sie das Kontrollkästchen **Das Kennwort in einem sicheren Anmeldedatenspeicher speichern...** aktivieren und dann im Feld **Anmeldedatenname** einen Namen für die Anmeldedaten eingeben.

Wichtig
Das Kennwort wird in einem sicheren Anmeldedatenspeicher hinterlegt und bei späteren Failover-Aktionen automatisch angewendet. Es kann jedoch sein, dass das Speichern von Kennwörtern im Konflikt mit Ihren Compliance-Verpflichtungen steht.

c. Klicken Sie auf **Fertig**.

Wenn der Recovery-Server gestartet ist, ändert sich dessen Stadium auf **Finalisierung** und nach einer gewissen Zeit auf **Failover.**

Wichtig
Es ist wichtig zu verstehen, dass der Server sowohl im Stadium **Finalisierung** also auch **Failover** verfügbar ist. Im Stadium **Finalisierung** können Sie auf die Server-Konsole zugreifen, indem Sie auf den Link **Konsole ist bereit** klicken. Der Link ist in der Spalte **VM-Stadium** auf der Anzeige **Disaster Recovery** –> **Server** sowie in der Ansicht **Details** des Servers verfügbar. Weitere Informationen finden Sie unter '"Wie ein Failover funktioniert" (S. 858)'.



7. Überprüfen Sie, dass der Recovery-Server gestartet ist, indem Sie sich dessen Konsole anzeigen lassen. Klicken Sie auf **Disaster Recovery** –> **Server**, wählen Sie den Recovery-Server aus und klicken Sie dann auf **Konsole**.
8. Stellen Sie sicher, dass der Recovery-Server über die Produktions-IP-Adresse verfügbar ist, die Sie bei Erstellung des Recovery-Servers spezifiziert haben.

Sobald der Recovery-Server finalisiert ist, wird automatisch ein neuer Schutzplan erstellt und dem Recovery-Server zugewiesen. Bis auf einige Einschränkungen basiert dieser Schutzplan auf demjenigen Schutzplan, der zu Erstellung des Recovery-Servers verwendet wurde. Sie können in diesem Plan nur die Planung und Aufbewahrungsregeln ändern. Weitere Informationen dazu finden Sie im Abschnitt 'Backup der Cloud-Server'.

Wenn Sie den Failover-Prozess abbrechen wollen, müssen Sie den Recovery-Server auswählen und dann auf **Failover abbrechen** klicken. Alle Änderungen, die ab dem Zeitpunkt des Failover beginnen, mit Ausnahme der Backups des Recovery-Servers, werden verloren gehen. Der Recovery-Server wird in das Stadium **Standby** zurückkehren.

Wenn Sie einen Failback-Prozess durchführen wollen, müssen Sie zuerst den Recovery-Server auswählen und dann auf **Failback** klicken.

So können Sie einen Failover von Servern mit einem lokalem DNS durchführen

Wenn Sie die Maschinennamen am lokalen Standort über DNS-Server auflösen, können die Recovery-Server, die den Maschinen entsprechen, die auf die DNS-Server zurückgreifen, nach einem Failover nicht mehr kommunizieren, da in der Cloud andere DNS-Server verwendet werden. Standardmäßig werden die DNS-Server der Cloud-Site für neu erstellte Cloud Server verwendet. Wenn Sie benutzerdefinierte DNS-Einstellungen anwenden müssen, sollten Sie das Support-Team kontaktieren.

So können Sie einen Failover für einen DHCP-Server durchführen

In Ihrer lokalen Infrastruktur kann sich der DHCP-Server auf einem Windows- oder Linux-Host befinden. Wenn ein solcher Host per Failover in die Cloud-Site umgeschaltet wird, kommt es zu einem DHCP-Server-Duplizierungsproblem, weil das VPN-Gateway in der Cloud ebenfalls die DHCP-Rolle übernimmt. Führen Sie einen der folgenden Schritte aus, um dieses Problem zu beheben:

- Wenn nur der DHCP-Host per Failover in die Cloud umgeschaltet wurde, während sich die restlichen lokalen Server weiterhin am lokalen Standort befinden, müssen Sie sich beim DHCP-Host in der Cloud anmelden und den dort laufenden DHCP-Server ausschalten. Somit gibt es keine Konflikte mehr und nur das VPN-Gateway wird als DHCP-Server fungieren.
- Wenn Ihre Cloud Server bereits ihre IP-Adressen vom DHCP-Host erhalten haben, müssen Sie sich beim DHCP-Host in der Cloud anmelden und den dort laufenden DHCP-Server ausschalten. Sie müssen sich auch bei den Cloud Servern anmelden und die DHCP-IP-Vergabe erneuern, damit neue IP-Adressen vom richtigen (auf dem VPN-Gateway gehosteten) DHCP-Server zugewiesen werden.

Hinweis
Diese Anweisungen sind nicht gültig, wenn Ihr Cloud-DHCP-Server mit der Option **Benutzerdefiniertes DHCP** konfiguriert wurde – und einige der primären oder Recovery-Server ihre IP-Adresse von diesem DHCP-Server beziehen.

Wie ein Failback funktioniert

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Ein Failback ist ein Prozess, bei dem ein Workload aus der Cloud zurück zu einer physischen oder virtuellen Maschine am lokalen Standort des entsprechenden Unternehmens/Kunden verschoben wird. Sie können einen Failback-Prozess auf einen Recovery-Server im **Failover**-Stadium anwenden – und den entsprechenden Server dann an Ihrem lokalen Standort weiter verwenden.

Sie können einen automatisierten Failback zu einer virtuellen oder physischen Zielmaschine durchführen, die sich an Ihrem lokalen Standort befindet. Während des Failback-Prozesses können Sie die Backup-Daten zu Ihrem lokalen Standort übertragen, während die virtuelle Maschine weiter in der Cloud ausgeführt wird. Mit dieser Technologie können Sie eine sehr kurze Ausfallzeit erreichen, die in der Cyber Protect-Konsole auch entsprechend prognostiziert und angezeigt wird. Sie können diese Informationen einsehen und verwenden, um Ihre Aktivitäten zu planen – und (falls nötig) Ihre Kunden vor einer anstehenden Ausfallzeit zu warnen.

Die Failback-Prozesse zu virtuellen Zielmaschinen und physischen Zielmaschinen unterscheiden sich leicht. Weitere Informationen zu den verschiedenen Phasen eines Failback-Prozesses finden Sie in den Abschnitten '"Failback zu einer virtuellen Zielmaschine" (S. 868)' und '"Failback zu einer physischen Zielmaschine" (S. 873)'.

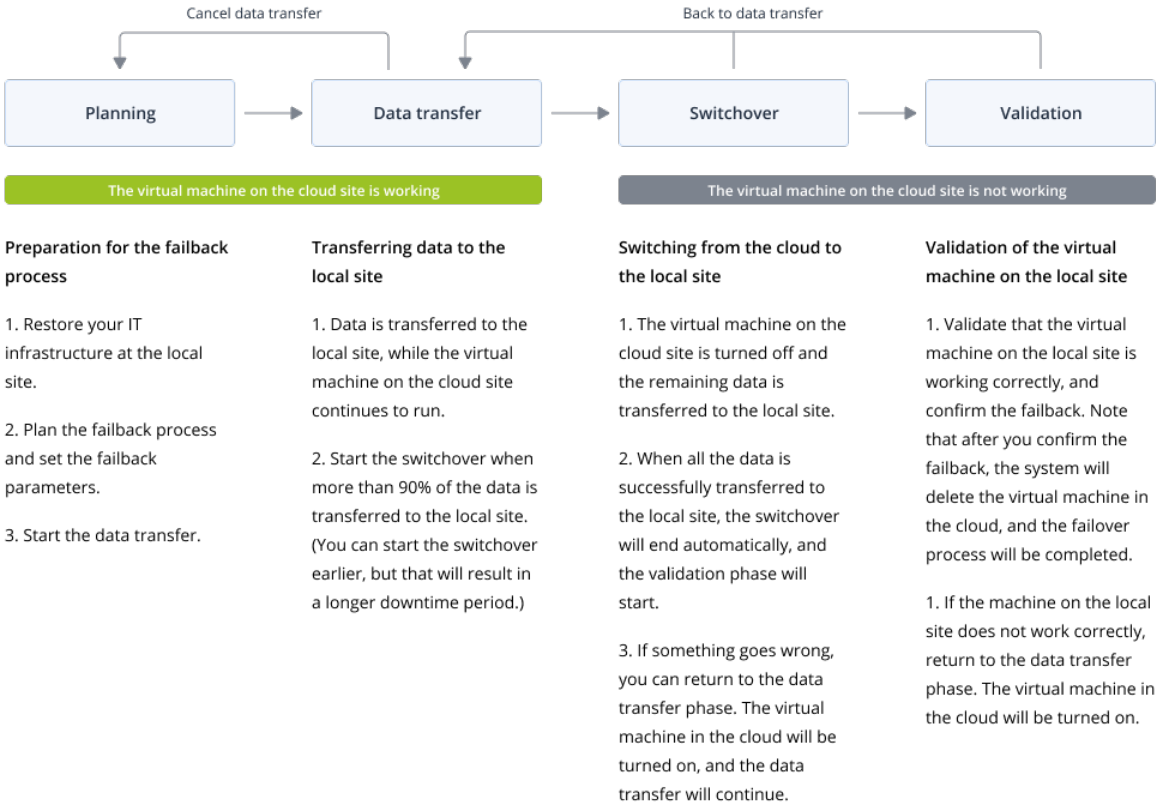
Wenn Sie die automatisierte Failback-Prozedur aus bestimmten Gründen nicht verwenden können, können Sie auch einen manuellen Failback-Prozess durchführen. Weitere Informationen finden Sie im Abschnitt '"Manueller Failback-Prozess" (S. 877)'.

Hinweis
Runbook-Aktionen unterstützen Failbacks nur im manuellen Modus. Das heißt, wenn Sie den Failback-Prozess durch die Ausführung eines Runbooks starten, in dem ein **Server-Failback ausführen**-Schritt enthalten ist, erfordert die Prozedur eine manuelle Interaktion: Sie müssen die Maschine zuerst manuell wiederherstellen und dann den Failback-Prozess über die Registerkarte **Disaster Recovery** –> **Server** bestätigen oder abbrechen.

Failback zu einer virtuellen Zielmaschine

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Der Failback-Prozess zu einer virtuellen Maschine umfasst vier Phasen:



1. **Planung**. In dieser Phase stellen Sie die IT-Infrastruktur (z.B. die Hosts und Netzwerkkonfigurationen) an Ihrem lokalen Standort wieder her, konfigurieren Sie die Failback-Parameter und planen Sie, wann die Datenübertragung beginnen soll.

   Hinweis
   Um die Gesamtzeit für den Failback-Prozess möglichst kurz zu halten, empfehlen wir, dass Sie die Datenübertragungsphase direkt nach der Einrichtung Ihrer lokalen Server starten und während dieser Datenübertragungsphase dann mit der Konfiguration des Netzwerks und der restlichen lokalen Infrastruktur fortfahren.

2. **Datenübertragung**. In dieser Phase werden die Daten von der Cloud-Site zum lokalen Standort übertragen, während die virtuelle Maschine in der Cloud weiter ausgeführt wird. Sie können die nächste Phase (die Switchover-Phase) jederzeit während der Datenübertragungsphase starten.

Dabei sollten Sie jedoch folgende Zusammenhänge beachten.

Je länger Sie in der Datenübertragungsphase verbleiben,

- desto länger wird die virtuelle Maschine in der Cloud weiter ausgeführt.
- desto mehr Daten werden zu Ihrem lokalen Standort übertragen.
- desto höher werden die Kosten sein, die Sie zahlen müssen (Sie werden mehr Berechnungspunkte verbrauchen).
- desto kürzer wird die Ausfallzeit sein, die Sie während der Switchover-Phase erleben werden.

Wenn Sie die Ausfallzeit minimieren wollen, starten Sie die Switchover-Phase, nachdem mehr als 90% der Daten an den lokalen Standort übertragen wurden.

Wenn Sie eine längere Ausfallzeit in Kauf nehmen können und nicht mehr Berechnungspunkte für den Betrieb der virtuellen Maschine in der Cloud ausgeben wollen, können Sie die Switchover-Phase früher starten.

Wenn Sie den Failback-Prozess während der Datenübertragungsphase abbrechen, werden die bisher zum lokalen Standort übertragenen Daten nicht gelöscht. Bevor Sie einen neuen Failback-Prozess starten, sollten Sie die übertragenen Daten manuell löschen, um mögliche Probleme zu vermeiden. Der nachfolgenden Datenübertragungsprozess wird ganz neu gestartet.

3. **Switchover**. In dieser Phase wird die virtuelle Maschine in der Cloud ausgeschaltet und die verbleibenden Daten (einschließlich des letzten Backup-Inkrements) werden zum lokalen Standort übertragen. Wenn auf den Recovery-Server kein Backup-Plan angewendet wurde, wird automatisch während der Switchover-Phase ein Backup durchgeführt, was jedoch den Prozess verlangsamt.

   Sie können die geschätzte Zeit bis zur Fertigstellung (entspricht der Ausfallzeit) für diese Phase in der Cyber Protect-Konsole einsehen Wenn alle Daten zum lokalen Standort übertragen wurden (es gehen keine Daten verloren und die virtuelle Maschine am lokalen Standort ist eine exakte Kopie der virtuellen Maschine in der Cloud), ist die Switchover-Phase abgeschlossen. Die virtuelle Maschine am lokalen Standort wird wiederhergestellt und die Validierungsphase beginnt automatisch.
4. **Validierung**.Während dieser Phase ist die virtuelle Maschine am lokalen Standort bereits verfügbar und automatisch gestartet. Sie können überprüfen, ob die virtuelle Maschine korrekt funktioniert – und können Folgendes tun:
   - Falls alles wie erwartet funktioniert, bestätigen Sie das Failback. Nach der Failback-Bestätigung wird die virtuelle Maschine in der Cloud gelöscht und der Recovery-Server in das Stadium Standby **Standby** zurückversetzt. Damit ist der Failback-Prozess beendet.
   - Wenn etwas nicht stimmt, können Sie den Switchover-Prozess abbrechen und zur Datenübertragungsphase zurückkehren.

Einen Failback zu einer virtuellen Maschine durchführen

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Sie können einen Failback zu einer virtuellen Zielmaschine durchführen, die sich an Ihrem lokalen Standort befindet.

Voraussetzungen

- Der Agent, den Sie zur Durchführung des Failbacks verwenden wollen, ist online und wird aktuell für keine andere Failback-Aktion verwendet.
- Ihre Internetverbindung ist stabil.
- Es gibt mindestens ein vollständiges Backup der virtuellen Maschine in der Cloud.

So können Sie einen Failback zu einer virtuellen Maschine durchführen

1. Gehen Sie in der Cyber Protect-Konsole zu **Disaster Recovery** –> **Server**.
2. Wählen Sie den Recovery-Server aus, der sich im **Failover**-Stadium befindet.
3. Klicken Sie auf die Registerkarte **Failback**.
4. Wählen Sie im Bereich **Failback-Parameter** den Eintrag **Virtuelle Maschine** als **Ziel** aus und konfigurieren Sie dann die Parameter.
   Beachten Sie, dass standardmäßig einige der **Failback-Parameter** automatisch mit vorgeschlagenen Werten ausgefüllt werden. Sie können diese Werte aber ändern.
   Die nachfolgende Tabelle gibt Ihnen weitere Informationen über die **Failback-Parameter**.

Parameter	Beschreibung
Backup-Größe	Die Datenmenge, die während des Failback-Prozesses zu Ihrem lokalen Standort übertragen wird. Nach dem der Start des Failback-Prozesses zu einer virtuellen Zielmaschine nimmt die **Backup-Größe** während der Datenübertragungsphase zu, weil die virtuelle Maschine in der Cloud weiter ausgeführt wird und dabei neue Daten generiert. Wenn Sie die geschätzte Ausfallzeit während des Failback-Prozesses zu einer virtuellen Zielmaschine berechnen wollen, nehmen Sie 10% des Wertes für die **Backup-Größe** (da wir empfehlen, die Switchover-Phase zu starten, nachdem 90% der Daten zum lokalen Standort übertragen wurden) und teilen Sie diesen Wert dann durch Ihre Internet-Geschwindigkeit. **Hinweis** Der Wert für die Internet-Geschwindigkeit wird kleiner, wenn Sie mehrere Failback-Prozesse gleichzeitig durchführen.
Ziel	Die Art des Workloads an Ihrem lokalen Standort, zu dem Sie den Cloud Server wiederherstellen wollen: **Virtuelle Maschine** oder **Physische Maschine**.
Speicherort der Zielmaschine	Failback-Speicherort: ein VMware ESXi- oder ein Microsoft Hyper-V-Host.

Parameter	Beschreibung
	Sie können aus allen Hosts wählen, die einen Agent haben, welcher wiederum im Cyber Protection Service registriert ist.
Agent	Der Agent, der die Failback-Aktion durchführen wird. Sie können einen (1) Agenten verwenden, um eine (1) Failback-Aktion gleichzeitig durchzuführen. Sie können einen Agenten auswählen, der online ist und aktuell für keinen anderen Failback-Prozess verwendet wird. Außerdem muss die Agenten-Version die Failback-Funktionalität unterstützen sowie über die Berechtigung verfügen, um auf das Backup zugreifen zu können. Beachten Sie, dass Sie mehrere Agenten auf VMware ESXi-Hosts installieren können und mit jedem von diesen einen separaten Failback-Prozess starten können. Diese Failback-Prozesse können auch gleichzeitig ausgeführt werden.
Einstellungen der Zielmachine	Einstellungen der virtuellen Maschine: • **Virtuelle Prozessoren**. Bestimmen Sie die Anzahl der virtuellen Prozessoren (CPUs). • **Arbeitsspeicher**. Bestimmen Sie, wie viel Arbeitsspeicher die virtuelle Maschine erhalten soll. • **Abteilungen**. Wählen Sie die Abteilungen für den Arbeitsspeicher. • [Optional] **Netzwerkadapter**. Wenn Sie einen Netzwerkadapter hinzufügen wollen, klicken Sie zuerst auf **Hinzufügen** und wählen Sie dann ein Netzwerk im Feld **Netzwerk** aus. Klicken Sie auf **Fertig**, wenn Sie die Änderungen abgeschlossen haben.
Pfad	(Für Microsoft Hyper-V-Hosts) Ordner auf dem Host, wo Ihre Maschine gespeichert werden soll. Sorgen Sie dafür, dass auf dem Host genügend freier Speicherplatz für die Maschine vorhanden ist.
Datenspeicher	(Für VMware ESXi-Hosts) Datenspeicher auf dem Host, wo Ihre Maschine gespeichert werden soll. Sorgen Sie dafür, dass auf dem Host genügend freier Speicherplatz für die Maschine vorhanden ist.
Provisioning-Modus	Zuordnungsmethode für das virtuelle Laufwerk. Für Microsoft Hyper-V-Hosts: • **Dynamisch erweiterbar** (Standardwert). • **Feste Größe**. Für Microsoft Hyper-V-Hosts: • **Thin** (Standardwert). • **Thick**.
Name der	Name der Zielmaschine. Standardmäßig ist der Name der Zielmaschine

Parameter	Beschreibung
Zielmaschine	identisch mit dem Namen des Recovery-Servers. Der Name der Zielmaschine muss für den gewählten **Speicherort der Zielmaschine** eindeutig (einmalig) sein.

5. Klicken Sie zuerst auf **Datenübertragung starten** und klicken Sie dann im Bestätigungsfenster auf **Start**.

Hinweis
Wenn es kein Backup der virtuellen Maschine in der Cloud gibt, führt das System automatisch ein Backup durch, bevor die Datenübertragungsphase beginnt.

Die **Datenübertragungs**phase wird gestartet. In der Konsole werden folgende Informationen angezeigt:

Feld	Beschreibung
Fortschritt	Dieser Parameter zeigt an, wie viele Daten bereits zum lokalen Standort übertragen wurden und wie viele Daten insgesamt noch übertragen werden müssen. Die Gesamtmenge der Daten setzt sich folgendermaßen zusammen: Die Daten des letzten Backups, bevor die Datenübertragungsphase gestartet wurde, sowie die Backups von neu generierten Daten (also Backup-Inkremente), während die virtuelle Maschine in der Datenübertragungsphase weiter ausgeführt wird. Aus diesem Grund werden beide Werte des Parameters **Fortschritt** mit der Zeit größer.
Schätzung der Ausfallzeit	Dieser Parameter gibt an, wie lange die virtuelle Maschine in der Cloud nicht verfügbar sein wird, wenn Sie die Switchover-Phase zum jetzigen Zeitpunkt starten. Dieser Wert wird aus den Werten des Parameters **Fortschritt** berechnet – und wird mit der Zeit kleiner.

6. Klicken Sie zuerst auf **Switchover** und dann im Bestätigungsfenster erneut auf **Switchover**.
Die Switchover-Phase wird gestartet. In der Konsole werden folgende Informationen angezeigt:

Feld	Beschreibung
Fortschritt	Dieser Parameter zeigt an, wie die Wiederherstellung der Maschine am lokalen Standort fortschreitet.
Geschätzte Zeit bis zur Fertigstellung	Dieser Parameter gibt an, wann die Switchover-Phase ungefähr abgeschlossen sein wird und wann Sie die Maschine am lokalen Standort starten können.

Hinweis
Wenn kein Backup-Plan auf die virtuelle Maschine in der Cloud angewendet wurde, wird automatisch während der Switchover-Phase ein Backup durchgeführt, was jedoch zu einer längeren Ausfallzeit führt.

7. Nachdem die **Switchover**-Phase abgeschlossen und die virtuelle Maschine an Ihrem lokalen Standort automatisch gestartet wurde, sollten Sie überprüfen, ob diese wie erwartet funktioniert.
8. Klicken Sie zuerst auf **Failback bestätigen** und dann im Bestätigungsfenster auf **Bestätigen**, um den Prozess abzuschließen.
   Die virtuelle Maschine wird daraufhin in der Cloud gelöscht und der Recovery-Server in das Stadium Standby **Standby** zurückversetzt.

Hinweis
Das Anwenden eines Schutzplans auf den wiederhergestellten Server ist kein Bestandteil des Failback-Prozesses. Nach Abschluss des Failback-Prozesses können Sie aber einen Schutzplan auf den wiederhergestellten Server anwenden, damit dieser wieder geschützt ist. Sie können den gleichen Schutzplan anwenden, der auf den ursprünglichen Server angewendet wurde – oder einen neuen Schutzplan, bei dem das **Disaster Recovery**-Modul aktiviert ist.

Failback zu einer physischen Zielmaschine

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Der automatische Failback-Prozess zu einer physischen Maschine umfasst folgende Phasen:

1. **Planung**. In dieser Phase stellen Sie die IT-Infrastruktur (z.B. die Hosts und Netzwerkkonfigurationen) an Ihrem lokalen Standort wieder her, konfigurieren Sie die Failback-Parameter und planen Sie, wann die Datenübertragung beginnen soll.
2. **Datenübertragung**. In dieser Phase werden die Daten von der Cloud-Site zum lokalen Standort übertragen, während die virtuelle Maschine in der Cloud weiter ausgeführt wird. Sie können die nächste Phase (die Switchover-Phase) jederzeit während der Datenübertragungsphase starten. Dabei sollten Sie jedoch folgende Zusammenhänge beachten.
   Je länger Sie in der Datenübertragungsphase verbleiben,
   - desto länger wird die virtuelle Maschine in der Cloud weiter ausgeführt.
   - desto mehr Daten werden zu Ihrem lokalen Standort übertragen.
   - desto höher werden die Kosten sein, die Sie zahlen müssen (Sie werden mehr Berechnungspunkte verbrauchen).
   - desto kürzer wird die Ausfallzeit sein, die Sie während der Switchover-Phase erleben werden.

Wenn Sie die Ausfallzeit minimieren wollen, starten Sie die Switchover-Phase, nachdem mehr als 90% der Daten an den lokalen Standort übertragen wurden.

Wenn Sie eine längere Ausfallzeit in Kauf nehmen können und nicht mehr Berechnungspunkte für den Betrieb der virtuellen Maschine in der Cloud ausgeben wollen, können Sie die Switchover-Phase früher starten.

Hinweis

Der Datenübertragungsprozess verwendet eine Flashback-Technologie. Diese Technologie vergleicht die Daten, die auf der Zielmaschine vorhanden sind, mit den Daten der virtuellen Maschine in der Cloud. Wenn bereits ein Teil der Daten auf der Maschine vorhanden ist, werden diese nicht erneut übertragen. Durch diese Technologie wird die Datenübertragungsphase beschleunigt.

Aus diesem Grund empfehlen wir Ihnen, dass Sie den Server an Ihrem lokalen Standort zu der ursprünglichen Maschine wiederherstellen.

3. **Switchover**. In dieser Phase wird die virtuelle Maschine in der Cloud ausgeschaltet und die verbleibenden Daten (einschließlich des letzten Backup-Inkrements) werden zum lokalen Standort übertragen. Wenn auf den Recovery-Server kein Backup-Plan angewendet wurde, wird automatisch während der Switchover-Phase ein Backup durchgeführt, was jedoch den Prozess verlangsamt.
4. **Validierung**. In dieser Phase ist die physische Maschine am lokalen Standort betriebsbereit und Sie können sie mit einem Linux-basierten Boot-Medium neu starten. Sie können überprüfen, ob die virtuelle Maschine korrekt funktioniert – und können Folgendes tun:
   - Falls alles wie erwartet funktioniert, bestätigen Sie das Failback. Nach der Failback-Bestätigung wird die virtuelle Maschine in der Cloud gelöscht und der Recovery-Server in das Stadium Standby **Standby** zurückversetzt. Damit ist der Failback-Prozess beendet.
   - Wenn etwas nicht stimmt, können Sie den Failover-Prozess abbrechen und zur Planungsphase zurückkehren.

Hinweis

Nachdem das Boot-Medium neu gestartet worden ist, können Sie es nicht mehr verwenden. Wenn Sie während der Validierungsphase einen Fehler feststellen, müssen Sie ein neues Boot-Medium registrieren und den Failback-Prozess neu starten.

Aufgrund der verwendeten Flashback-Technologie müssen jedoch die Daten, die sich bereits am lokalen Standort befinden, nicht noch einmal übertragen werden, sodass der Failback-Prozess wesentlich schneller verläuft.

Einen Failback zu einer physischen Maschine durchführen

Hinweis

Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Sie können einen automatischen Failback zu einer physischen Zielmaschine durchführen, die sich an Ihrem lokalen Standort befindet.

Hinweis
Der Datenübertragungsprozess verwendet eine Flashback-Technologie. Diese Technologie vergleicht die Daten, die auf der Zielmaschine vorhanden sind, mit den Daten der virtuellen Maschine in der Cloud. Wenn bereits ein Teil der Daten auf der Maschine vorhanden ist, werden diese nicht erneut übertragen. Durch diese Technologie wird die Datenübertragungsphase beschleunigt.

Aus diesem Grund empfehlen wir Ihnen, dass Sie den Server an Ihrem lokalen Standort zu der ursprünglichen Maschine wiederherstellen.

Voraussetzungen

- Der Agent, den Sie zur Durchführung des Failbacks verwenden wollen, ist online und wird aktuell für keine andere Failback-Aktion verwendet.
- Ihre Internetverbindung ist stabil.
- Es ist ein registriertes Boot-Medium verfügbar. Für weitere Informationen lesen Sie den Abschnitt 'Ein Boot-Medium zur Wiederherstellung von Betriebssystemen erstellen' in der Benutzeranleitung von Cyber Protection.
- Die physische Zielmaschine ist die ursprüngliche Maschine an Ihrem lokalen Standort oder hat die gleiche Firmware wie die ursprüngliche Maschine.
- Es gibt mindestens ein vollständiges Backup der virtuellen Maschine in der Cloud.

So können Sie einen Failback zu einer physischen Maschine durchführen

1. Gehen Sie in der Cyber Protect-Konsole zu **Disaster Recovery** –> **Server**.
2. Wählen Sie den Recovery-Server aus, der sich im **Failover**-Stadium befindet.
3. Klicken Sie auf die Registerkarte **Failback**.
4. Wählen Sie im Feld **Ziel** den Eintrag **Physische Maschine**.
5. Klicken Sie im Feld **Boot-Medium für das Ziel** auf **Spezifizieren**, wählen Sie das Boot-Medium aus und klicken Sie auf **Fertig**.

   Hinweis
   Wir empfehlen Ihnen, dass Sie ein vorgefertigtes Boot-Medium verwenden, weil dieses bereits vorkonfiguriert ist. Für weitere Informationen lesen Sie den Abschnitt 'Ein Boot-Medium zur Wiederherstellung von Betriebssystemen erstellen' in der Benutzeranleitung für Cyber Protection.

6. [Optional] Wenn Sie die standardmäßige Laufwerkzuordnung ändern wollen, klicken Sie im Feld **Laufwerkszuordnung** auf **Spezifizieren**, ordnen Sie dann die Laufwerke im Backup den Laufwerken der Zielmaschine zu und klicken Sie anschließend auf **Fertig**.
7. Klicken Sie zuerst auf **Datenübertragung starten** und dann im Bestätigungsfenster auf **Start**.

Hinweis
Wenn es kein Backup der virtuellen Maschine in der Cloud gibt, führt das System automatisch ein Backup durch, bevor die Datenübertragungsphase beginnt.

Die Datenübertragungsphase wird gestartet. In der Konsole werden folgende Informationen angezeigt:

Feld	Beschreibung
Fortschritt	Dieser Parameter zeigt an, wie viele Daten bereits zum lokalen Standort übertragen wurden und wie viele Daten insgesamt noch übertragen werden müssen. Die Gesamtmenge der Daten setzt sich folgendermaßen zusammen: Die Daten des letzten Backups, bevor die Datenübertragungsphase gestartet wurde, sowie die Backups von neu generierten Daten (also Backup-Inkremente), während die virtuelle Maschine in der Datenübertragungsphase weiter ausgeführt wird. Aus diesem Grund nehmen die **Fortschritt**-Werte mit der Zeit zu. Da das System während der Datenübertragung eine Flashback-Technologie verwendet und keine Daten mehr übertragen muss, die bereits auf der Zielmaschine vorhanden sind, kann der Fortschritt schneller sein, als von der Konsole anfänglich berechnet wurde.
Schätzung der Ausfallzeit	Dieser Parameter gibt an, wie lange die virtuelle Maschine in der Cloud nicht verfügbar sein wird, wenn Sie die Switchover-Phase zum jetzigen Zeitpunkt starten. Dieser Wert wird aus den Werten des Parameters **Fortschritt** berechnet – und wird mit der Zeit kleiner. Da das System während der Datenübertragung eine Flashback-Technologie verwendet und keine Daten mehr übertragen muss, die bereits auf der Zielmaschine vorhanden sind, kann die Ausfallzeit viel kürzer sein als der Wert, der anfänglich auf der Konsole angezeigt wird.

8. Klicken Sie zuerst auf **Switchover** und dann im Bestätigungsfenster erneut auf **Switchover**.
   Die Switchover-Phase wird gestartet. In der Konsole werden folgende Informationen angezeigt:

Feld	Beschreibung
Fortschritt	Dieser Parameter zeigt an, wie die Wiederherstellung der Maschine am lokalen Standort fortschreitet.
Geschätzte Zeit bis zur Fertigstellung	Dieser Parameter gibt an, wann die Switchover-Phase ungefähr abgeschlossen sein wird und wann Sie die Maschine am lokalen Standort starten können.

Hinweis
Wenn kein Backup-Plan auf die virtuelle Maschine in der Cloud angewendet wurde, wird automatisch während der Switchover-Phase ein Backup durchgeführt, was jedoch zu einer längeren Ausfallzeit führt.

9. Wenn die **Switchover**-Phase abgeschlossen wurde, starten Sie das Boot-Medium neu und überprüfen Sie dann, ob die physische Maschine an Ihrem lokalen Standort wie erwartet funktioniert.
   Für weitere Informationen lesen Sie den Abschnitt 'Laufwerke mithilfe eines Boot-Mediums wiederherstellen' in der Benutzeranleitung von Cyber Protection.
10. Klicken Sie zuerst auf **Failback bestätigen** und dann im Bestätigungsfenster auf **Bestätigen**, um den Prozess abzuschließen.
    Die virtuelle Maschine wird daraufhin in der Cloud gelöscht und der Recovery-Server in das Stadium Standby **Standby** zurückversetzt.

Hinweis
Das Anwenden eines Schutzplans auf den wiederhergestellten Server ist kein Bestandteil des Failback-Prozesses. Nach Abschluss des Failback-Prozesses können Sie aber einen Schutzplan auf den wiederhergestellten Server anwenden, damit dieser wieder geschützt ist. Sie können den gleichen Schutzplan anwenden, der auf den ursprünglichen Server angewendet wurde – oder einen neuen Schutzplan, bei dem das **Disaster Recovery**-Modul aktiviert ist.

Manueller Failback-Prozess

Hinweis
Wir empfehlen Ihnen, den Failback-Prozess nur dann im Handbetrieb zu verwenden, wenn Sie vom Support-Team dazu aufgefordert werden.

Sie können einen Failback-Prozess auch im manuellen Modus starten. In diesem Fall wird die Datenübertragung vom Backup in der Cloud zum lokalen Standort nicht automatisch durchgeführt. Dies muss manuell erfolgen, nachdem die virtuelle Maschine in der Cloud ausgeschaltet wurde. Dadurch wird der Failback-Prozess im manuellen Modus deutlich langsamer, sodass Sie mit einer längeren Ausfallzeit rechnen sollten.

Ein Failback-Prozess im manuellen Modus umfasst folgende Phasen:

1. **Planung**. In dieser Phase stellen Sie die IT-Infrastruktur (z.B. die Hosts und Netzwerkkonfigurationen) an Ihrem lokalen Standort wieder her, konfigurieren Sie die Failback-Parameter und planen Sie, wann die Datenübertragung beginnen soll.
2. **Switchover**. In dieser Phase wird die virtuelle Maschine in der Cloud ausgeschaltet und die neu generierten Daten werden gesichert. Wenn auf den Recovery-Server kein Backup-Plan angewendet wurde, wird automatisch während der Switchover-Phase ein Backup durchgeführt, was jedoch den Prozess verlangsamt. Wenn das Backup abgeschlossen wurde, stellen Sie die

Maschine zum lokalen Standort manuell wieder her. Sie können das Laufwerk entweder mithilfe eines Boot-Mediums wiederherstellen – oder die gesamte Maschine aus dem Cloud Backup Storage wiederherstellen.

3. **Validierung**. In dieser Phase überprüfen Sie, ob die physische oder virtuelle Maschine am lokalen Standort korrekt funktioniert, und bestätigen Sie den Failback-Prozess. Nach der Bestätigung wird die virtuelle Maschine in der Cloud-Site gelöscht und der Recovery-Server in das Stadium Standby **Standby** zurückversetzt.

Einen manuellen Failback-Prozess durchführen

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Sie können einen manuellen Failback-Prozess zu einer physischen oder virtuellen Zielmaschine durchführen, die sich an Ihrem lokalen Standort befindet.

So können Sie einen manuellen Failback-Prozess durchführen

1. Gehen Sie in der Cyber Protect-Konsole zu **Disaster Recovery** –> **Server**.
2. Wählen Sie den Recovery-Server aus, der sich im **Failover**-Stadium befindet.
3. Klicken Sie auf die Registerkarte **Failback**.
4. Wählen Sie im Feld **Ziel** den Eintrag **Physische Maschine**.
5. Klicken Sie auf das Zahnradsymbol und aktivieren Sie dann den Schalter **Manuellen Modus verwenden**.
6. [Optional] Berechnen Sie die geschätzte Ausfallzeit während des Failback-Prozesses, indem Sie den Wert für die **Backup-Größe** durch den Wert für Ihre Internet-Geschwindigkeit teilen.

   Hinweis
   Der Wert für die Internet-Geschwindigkeit wird kleiner, wenn Sie mehrere Failback-Prozesse gleichzeitig durchführen.

7. Klicken Sie zuerst auf **Switchover** und dann im Bestätigungsfenster erneut auf **Switchover**.
   Die virtuelle Maschine in der Cloud-Site wird ausgeschaltet.

   Hinweis
   Wenn kein Backup-Plan auf die virtuelle Maschine in der Cloud angewendet wurde, wird automatisch während der Switchover-Phase ein Backup durchgeführt, was jedoch zu einer längeren Ausfallzeit führt.

8. Stellen Sie den Server aus einem Cloud Backup zur physischen oder virtuellen Zielmaschine an Ihrem lokalen Standort wieder her. Für weitere Informationen lesen Sie den Abschnitt 'Eine Maschine wiederherstellen' in der Benutzeranleitung von Cyber Protection.

9. Überprüfen Sie, dass die Wiederherstellung abgeschlossen wurde und die wiederhergestellte Maschine korrekt funktioniert, und klicken Sie dann auf **Die Maschine wurde wiederhergestellt**.
10. Wenn alles wie erwartet funktioniert, können Sie auf **Failback bestätigen** und dann im Bestätigungsfenster noch einmal auf **Bestätigen** klicken.

    Der Recovery-Server und die Recovery-Punkte werden für den nächsten Failover bereit sein. Wenn Sie neue Recovery-Punkte erstellen wollen, müssen Sie dem neuen lokalen Server einen Schutzplan zuweisen.

Hinweis
Das Anwenden eines Schutzplans auf den wiederhergestellten Server ist kein Bestandteil des Failback-Prozesses. Nach Abschluss des Failback-Prozesses können Sie aber einen Schutzplan auf den wiederhergestellten Server anwenden, damit dieser wieder geschützt ist. Sie können den gleichen Schutzplan anwenden, der auf den ursprünglichen Server angewendet wurde – oder einen neuen Schutzplan, bei dem das **Disaster Recovery**-Modul aktiviert ist.

Mit verschlüsselten Backups arbeiten

Sie können Recovery-Server aus verschlüsselten Backups erstellen. Zu Ihrer Bequemlichkeit können Sie eine automatische Kennwort-Applikation für verschlüsselte Backups während des Failovers zu einem Recovery-Server einrichten.

Sie können bei der Erstellung eines Recovery-Servers das Kennwort spezifizieren, das für automatische Disaster-Recovery-Aktionen verwendet werden soll. Es wird im Anmeldedatenspeicher gespeichert, einem sicheren Storage für Anmeldedaten, der im Bereich **Einstellungen** –> **Anmeldedaten** gefunden werden kann.

Anmeldedaten können mit mehreren Backups verknüpft werden.

So können Sie die gespeicherten Kennwörter im Anmeldedatenspeicher verwalten

1. Gehen Sie zu **Einstellungen** –> **Anmeldedaten**.
2. Wenn Sie bestimmte Anmeldedaten verwalten wollen, klicken Sie auf das Symbol in der letzten Spalte. Sie können die Elemente sehen, die mit diesen Anmeldedaten verknüpft sind.
   - Wenn Sie die Verknüpfung des Backups mit den ausgewählten Anmeldedaten aufheben wollen, müssen Sie auf das Papierkorb-Symbol neben dem Backup klicken. Als Ergebnis dieser Aktion müssen Sie beim Failover zum Recovery-Server das Kennwort wieder manuell eingeben.
   - Um die Anmeldedaten zu bearbeiten, klicken Sie auf **Bearbeiten** und spezifizeiren Sie den Namen oder das Kennwort.
   - Um die Anmeldedaten zu verwerfen, klicken Sie auf **Löschen**. Beachten Sie, dass Sie dann das Kennwort beim Failover zum Recovery-Server wieder manuell eingeben müssen.

Aktionen mit virtuellen Microsoft Azure-Maschinen

Hinweis
In Abhängigkeit davon, welches Lizenzierungsmodell angewendet wird, kann für einige Funktionen eine zusätzliche Lizenzierung erforderlich sein.

Sie können Failover von virtuellen Microsoft Azure-Maschinen in die Acronis Cyber Protect Cloud durchführen. Weitere Informationen finden Sie im Abschnitt '"Einen Failover durchführen" (S. 864)'.

Anschließend können Sie einen Failback aus der Acronis Cyber Protect Cloud zurück zu virtuellen Azure-Maschinen durchführen. Ein solcher Failback-Prozess verläuft ebenso wie ein Failback-Prozess zu einer physischen Maschine. Weitere Informationen finden Sie im Abschnitt '"Voraussetzungen" (S. 875)'.

Hinweis
Wenn Sie eine neue virtuelle Azure-Maschine für Failbacks registrieren wollen, können Sie die Acronis Backup VM-Erweiterung verwenden, die in Azure verfügbar ist.

Sie können eine Multi-Site-IPsec-VPN-Konnektivität zwischen Acronis Cyber Protect Cloud und dem Azure VPN-Gateway konfigurieren. Weitere Informationen finden Sie im Abschnitt '"Multi-Site-IPsec-VPN konfigurieren" (S. 828)'.

Primäre Server einrichten

In diesem Abschnitt wird beschrieben, wie Sie Ihre primären Server erstellen und verwalten können.

Einen primären Server erstellen

Voraussetzungen

- Einer der Verbindungstypen zur Cloud-Site muss festgelegt sein.

So können Sie einen primären Server erstellen

1. Gehen Sie zur Registerkarte **Disaster Recovery** –> **Server** –> **Primäre Server**.
2. Klicken Sie auf **Erstellen**.
3. Wählen Sie eine Vorlage für die neue virtuelle Maschine aus.
4. Bestimmen Sie die Variante („Flavor“) der Konfiguration (die Anzahl der virtuellen Kerne und die Größe des RAMs). Die folgende Tabelle zeigt den maximalen Gesamtspeicherplatz (in GB) für jede Variante.

Typ	vCPU	RAM (GB)	Maximaler Gesamtspeicherplatz (GB)
V1	1	2	500

Typ	vCPU	RAM (GB)	Maximaler Gesamtspeicherplatz (GB)
V2	1	4	1000
V3	2	8	2000
V4	4	16	4000
V5	8	32	8000
V6	16	64	16000
V7	16	128	32000
V8	16	256	64000

Hinweis
Sie können die Berechnungspunkte für jede Option sehen. Die Anzahl der Berechnungspunkte spiegelt wieder, wie viel die Ausführung des primären Servers pro Stunde kostet. Weitere Informationen finden Sie im Abschnitt '"Berechnungspunkte" (S. 808)'.

5. [Optional] Ändern Sie die Größe der virtuellen Festplatte. Wenn Sie mehr als eine Festplatte benötigen, müssen Sie auf **Laufwerk hinzufügen** klicken und dann die Größe des neuen Laufwerks festlegen. Sie können derzeit nicht mehr als 10 Laufwerke für einen primären Server hinzufügen.
6. Spezifizieren Sie das Cloud-Netzwerk, mit dem der primäre Server eingebunden werden soll.
7. Wählen Sie die **DHCP**-Option.

DHCP-Option	Beschreibung
Von der Cloud-Site bereitgestellt	Standardeinstellung. Die IP-Adresse des Servers wird von einem automatisch konfigurierten DHCP-Server in der Cloud bereitgestellt.
Benutzerdefiniert	Die IP-Adresse des Servers wird von Ihrem eigenen DHCP-Server in der Cloud bereitgestellt.

8. [Optional] Spezifizieren Sie die **MAC-Adresse**.
   Die MAC-Adresse ist eine eindeutige Kennung, die dem Netzwerkadapter des Servers zugewiesen wird. Wenn Sie benutzerdefiniertes DHCP verwenden, können Sie es so konfigurieren, dass einer bestimmten MAC-Adresse immer eine bestimmte IP-Adresse zugewiesen wird. Dadurch wird sichergestellt, dass der primäre Server immer dieselbe IP-Adresse erhält. Dadurch können Sie Applikationen ausführen, die Lizenzen haben, die wiederum auf die MAC-Adresse registriert sind.
9. Spezifizieren Sie die IP-Adresse, die der Server im Produktionsnetzwerk haben wird. Als Standardeinstellung wird die erste freie IP-Adresse aus Ihrem Produktionsnetzwerk verwendet.

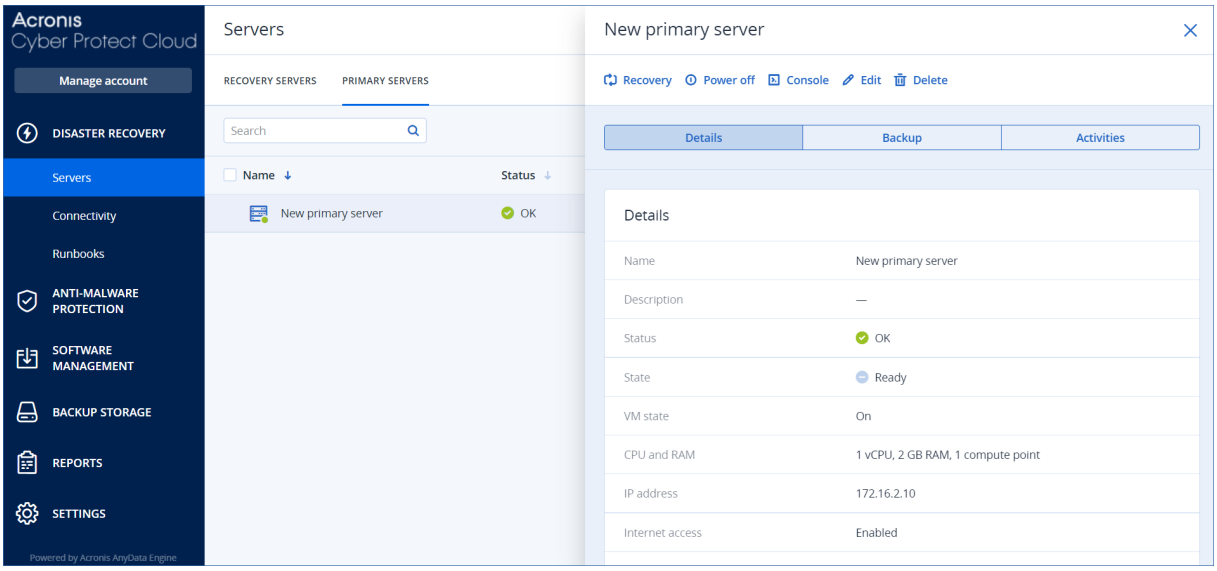
Hinweis
Falls Sie einen DHCP-Server verwenden, fügen Sie dessen IP-Adresse zu der Server-Ausschlussliste hinzu, um IP-Adressen-Konflikte zu vermeiden.
Wenn Sie einen benutzerdefinierten DHCP-Server verwenden, müssen Sie unter **IP-Adresse im Produktionsnetzwerk** dieselbe IP-Adresse spezifizieren, die im DHCP-Server konfiguriert ist. Ansonsten wird der Test-Failover nicht richtig funktionieren und der Server wird nicht über eine öffentliche IP-Adresse erreichbar sein.

10. [Optional] Aktivieren Sie das Kontrollkästchen **Internetzugriff**.
    Dadurch wird dem primären Server ermöglicht, auf das Internet zuzugreifen. Standardmäßig ist der TCP-Port 25 für ausgehende Verbindungen zu öffentlichen IP-Adressen geöffnet.
11. [Optional] Aktivieren Sie das Kontrollkästchen **Öffentliche IP-Adresse verwenden**.
    Wenn der primäre Server über eine öffentliche IP-Adresse verfügt, ist er aus dem Internet verfügbar. Wenn Sie das Kontrollkästchen deaktiviert lassen, wird der Server nur in Ihrem Produktionsnetzwerk verfügbar sein.
    Die öffentliche IP-Adresse wird angezeigt, nachdem Sie die Konfiguration abgeschlossen haben. Standardmäßig ist der TCP-Port 443 für eingehende Verbindungen zu öffentlichen IP-Adressen geöffnet.

    Hinweis
    Wenn Sie das Kontrollkästchen **Öffentliche IP-Adresse verwenden** deaktivieren oder den Recovery-Server löschen, wird dessen öffentliche IP-Adresse nicht reserviert.

12. [Optional] Wählen Sie **RPO-Grenzwert festlegen**.
    Der RPO-Grenzwert definiert also das maximal erlaubte Zeitintervall, das zwischen dem letzten Recovery-Punkt und dem aktuellen Zeitpunkt (an dem es zu einem Desaster kommen kann) zulässig ist. Der Wert kann zwischen 15–60 Minuten, 1–24 Stunden oder 1–14 Tagen eingestellt werden.
13. Definieren Sie einen Namen für den primären Server.
14. [Optional] Spezifizieren Sie eine Beschreibung für den primären Server.
15. [Optional] Klicken Sie auf die Registerkarte **Cloud-Firewall-Regeln**, um die Standard-Firewall-Regeln zu bearbeiten. Weitere Informationen finden Sie im Abschnitt '"Firewall-Regeln für Cloud Server einrichten" (S. 885)'.
16. Klicken Sie auf **Erstellen**.

Der primäre Server wird im Produktionsnetzwerk verfügbar gemacht. Sie können den Server über seine Konsole, über RDP, SSH oder den TeamViewer verwalten.



Aktionen mit einem primären Server

Der primäre Server wird in der -Konsole in der Registerkarte **Disaster Recovery** –> **Server** –> **Primäre Server** angezeigt.

Wenn Sie den Server starten oder stoppen wollen, müssen Sie im Fensterbereich des primären Servers auf **Einschalten** oder **Ausschalten** klicken.

Wenn Sie die primären Server-Einstellungen bearbeiten wollen, müssen Sie zuerst den Server stoppen und dann auf **Bearbeiten** klicken.

Wenn Sie dem primären Server einen Schutzplan zuweisen wollen, müssen Sie diesen auswählen und dann in der Registerkarte **Plan** auf **Erstellen** klicken. Daraufhin wird Ihnen ein vordefinierter Schutzplan angezeigt, indem Sie nur die Planung und Aufbewahrungsregeln ändern können. Weitere Informationen dazu finden Sie im Abschnitt 'Backup der Cloud-Server'.

Die Cloud Server verwalten

Wenn Sie die Cloud Server verwalten wollen, gehen Sie zu **Disaster Recovery** –> **Server**. Es gibt hier zwei Registerkarten: **Recovery-Server** und **Primäre Server**. Klicken Sie auf das Zahnradsymbol, damit alle optionalen Spalten in der Tabelle angezeigt werden.

Wenn Sie einen Cloud Server auswählen, können Sie die nachfolgenden Informationen finden.

Spaltenname	Beschreibung
Name	Ein von Ihnen definierter Cloud Server-Name
Status	Der Status, der das schwerwiegendste Problem mit einem Cloud Server anzeigt (basierend auf den aktiven Warnmeldungen).
Stadium	Ein Cloud Server-Stadium

VM-Zustand	Der Betriebszustand einer virtuellen Maschine, die mit einem Cloud Server assoziiert ist.
Aktiver Speicherort	Der Ort, wo ein Cloud Server gehostet wird. Beispiel: **Cloud**.
RPO-Grenzwert	Das maximal zulässige Zeitintervall zwischen dem letzten Recovery-Punkt, der für Failover geeignet ist, und der aktuellen Zeit. Der Wert kann zwischen 15–60 Minuten, 1–24 Stunden oder 1–14 Tagen eingestellt werden.
RPO-Compliance	Die RPO-Compliance ist das Verhältnis zwischen dem tatsächlichen RPO-Wert und dem RPO-Grenzwert. Die RPO-Compliance wird angezeigt, wenn der RPO-Grenzwert definiert ist. Sie wird folgendermaßen berechnet: **RPO-Compliance = Aktueller RPO-Wert / RPO-Grenzwert** wobei gilt: **Aktueller RPO-Wert = aktuelle Zeit – Zeit des letzten Recovery-Punkts** **RPO-Compliance-Statuszustände** Abhängig vom Verhältnis zwischen dem tatsächlichen RPO-Wert und dem RPO-Grenzwert werden folgende Statuszustände verwendet: • **Konform**. Die RPO-Compliance < 1x. Ein Server hält den RPO-Grenzwert ein. • **Überschritten**. Die RPO-Compliance <= 2x. Ein Server verstößt gegen den RPO-Grenzwert. • **Stark überschritten**. Die RPO-Compliance <= 4x. Ein Server überschreitet den RPO-Grenzwert um mehr als das Zweifache. • **Kritisch überschritten**. Die RPO-Compliance > 4x. Ein Server überschreitet den RPO-Grenzwert um mehr als das Vierfache. • **Ausstehend (keine Backups)**. Der Server ist durch den Schutzplan abgesichert, aber das Backup wird gerade erstellt und wurde noch nicht abgeschlossen.
Aktuelle RPO	Die Zeit, die seit Erstellung des letzten Recovery-Punktes vergangen ist
Neuester Recovery-Punkt	Datum und Uhrzeit, an dem der letzte Recovery-Punkt erstellt wurde.

Firewall-Regeln für Cloud Server

Sie können Firewall-Regeln konfigurieren, um den ein- und ausgehenden Datenverkehr der primären Server und Recovery-Server auf Ihrer Cloud-Site zu kontrollieren.

Sie können eingehende Regeln konfigurieren, nachdem Sie eine öffentliche IP-Adresse für den Cloud Server bereitgestellt haben. Standardmäßig ist der TCP-Port 443 erlaubt, während alle anderen eingehenden Verbindungen verweigert werden. Sie können die Standard-Firewall-Regeln

ändern und eingehende Ausnahmen hinzufügen oder entfernen. Wenn keine öffentliche IP-Adresse bereitgestellt wurde, können Sie die eingehenden Regeln nur einsehen, aber nicht konfigurieren.

Sie können ausgehende Regeln konfigurieren, wenn Sie den Internet-Zugriff für den Cloud Server bereitgestellt haben. Standardmäßig wird der TCP-Port 25 verweigert, während alle anderen ausgehenden Verbindungen erlaubt sind. Sie können die Standard-Firewall-Regeln ändern und ausgehende Ausnahmen hinzufügen oder entfernen. Wenn kein Internetzugriff bereitgestellt wurde, können Sie die ausgehenden Regeln nur einsehen, aber nicht konfigurieren.

Hinweis
Aus Sicherheitsgründen gibt es vordefinierte Firewall-Regeln, die Sie nicht ändern können.

Für ein- und ausgehende Verbindungen:

- Ping zulassen: ICMP-Echo-Anforderung (Typ 8, Code 0) und ICMP-Echo-Antwort (Typ 0, Code 0)
- ICMP-Antwort 'Fragmentierung erforderlich' zulassen (Typ 3, Code 4)
- 'TTL überschritten' zulassen (Typ 11, Code 0)

Nur für eingehende Verbindungen:

- Nicht konfigurierbarer Teil: Alle verweigern

Nur für ausgehende Verbindungen:

- Nicht konfigurierbarer Teil: Alle ablehnen

Firewall-Regeln für Cloud Server einrichten

Sie können die Standard-Firewall-Regeln für die primären Server und Recovery-Server in der Cloud bearbeiten.

So können Sie die Firewall-Regeln für einen Server auf Ihrer Cloud-Site bearbeiten

1. Gehen Sie in der Cyber Protect-Konsole zu **Disaster Recovery** –> **Server**.
2. Wenn Sie die Firewall-Regeln eines Recovery-Servers bearbeiten wollen, klicken Sie auf die Registerkarte **Recovery-Server**. Wenn Sie stattdessen die Firewall-Regeln eines primären Servers bearbeiten wollen, klicken Sie auf die Registerkarte **Primäre Server**.
3. Klicken Sie zuerst auf den Server und anschließend auf **Bearbeiten**.
4. Klicken Sie auf die Registerkarte **Cloud-Firewall-Regeln**.
5. Wenn Sie die Standardaktion für die eingehenden Verbindungen ändern wollen:

a. Wählen Sie im Listenfeld **Eingehend** die Standardaktion.

Aktion	Beschreibung
Alle verweigern	Verweigert jeden eingehenden Datenverkehr. Sie können Ausnahmen hinzufügen und Datenverkehr von bestimmten IP-Adressen, Protokollen und Ports zulassen.
Alle erlauben	Erlaubt jeden eingehenden TCP- und UDP-Datenverkehr. Sie können Ausnahmen hinzufügen und den Datenverkehr von bestimmten IP-Adressen, Protokollen und Ports verbieten.

Hinweis
Wenn Sie die Standardaktion ändern, wird die Konfiguration der vorhandenen Eingangsregeln ungültig und entfernt.

b. [Optional] Wenn Sie die vorhandenen Ausnahmen speichern wollen, müssen Sie im Bestätigungsfenster den Befehl **Eingegebene Ausnahmen speichern** auswählen.

c. Klicken Sie auf **Bestätigen**.

6. Wenn Sie eine Ausnahme hinzufügen wollen, dann:

a. Klicken Sie auf **Ausnahme hinzufügen**.

b. Spezifizieren Sie die Firewall-Parameter.

Firewall-Parameter	Beschreibung
Protokoll	Wählen Sie das Protokoll für die Verbindung aus. Folgende Optionen werden unterstützt: • **TCP** • **UDP:** • **TCP+UDP**
Server-Port	Wählen Sie die Ports aus, für die die Regel gelten soll. Sie können Folgendes spezifizieren: • eine bestimmte Port-Nummer (z.B. `2298`) • einen Port-Nummernbereich (z.B. `6000-6700`) • eine beliebige Portnummer. Verwenden Sie `*`, wenn die Regel auf jede Port-Nummer angewendet werden soll.
Client-IP-Adresse	Wählen Sie die IP-Adressen aus, für die die Regel gelten soll. Sie können Folgendes spezifizieren: • eine bestimmte IP-Adresse (z.B. `192.168.0.0`) • einen Bereich von IP-Adressen im CIDR-Format (z.B. `192.168.0.0/24`) • eine beliebige IP-Adresse. Verwenden Sie `*`, wenn die Regel auf jede IP-Adresse angewendet werden soll.

7. Wenn Sie eine vorhandene Eingangsausnahme entfernen wollen, klicken Sie auf das Papierkorb-Symbol neben der Ausnahme.
8. Wenn Sie die Standardaktion für die ausgehenden Verbindungen ändern wollen:
   a. Wählen Sie im Listenfeld **Ausgehend** die Standardaktion.

Aktion	Beschreibung
Alle verweigern	Verweigert jeden ausgehenden Datenverkehr. Sie können Ausnahmen hinzufügen und Datenverkehr zu bestimmten IP-Adressen, Protokollen und Ports zulassen.
Alle erlauben	Erlaubt jeden ausgehenden Datenverkehr. Sie können Ausnahmen hinzufügen und den Datenverkehr von bestimmten IP-Adressen, Protokollen und Ports verbieten.

Hinweis
Wenn Sie die Standardaktion ändern, wird die Konfiguration der vorhandenen Ausgangsregeln ungültig und entfernt.

   b. [Optional] Wenn Sie die vorhandenen Ausnahmen speichern wollen, müssen Sie im Bestätigungsfenster den Befehl **Eingegebene Ausnahmen speichern** auswählen.
   c. Klicken Sie auf **Bestätigen**.
9. Wenn Sie eine Ausnahme hinzufügen wollen, dann:
   a. Klicken Sie auf **Ausnahme hinzufügen**.
   b. Spezifizieren Sie die Firewall-Parameter.

Firewall-Parameter	Beschreibung
Protokoll	Wählen Sie das Protokoll für die Verbindung aus. Folgende Optionen werden unterstützt: • **TCP** • **UDP:** • **TCP+UDP**
Server-Port	Wählen Sie die Ports aus, für die die Regel gelten soll. Sie können Folgendes spezifizieren: • eine bestimmte Port-Nummer (z.B. `2298`) • einen Port-Nummernbereich (z.B. `6000-6700`) • eine beliebige Portnummer. Verwenden Sie `*`, wenn die Regel auf jede Port-Nummer angewendet werden soll.
Client-IP-Adresse	Wählen Sie die IP-Adressen aus, für die die Regel gelten soll. Sie können Folgendes spezifizieren: • eine bestimmte IP-Adresse (z.B. `192.168.0.0`) • einen Bereich von IP-Adressen im CIDR-Format (z.B. `192.168.0.0/24`)

Firewall-Parameter	Beschreibung
	• eine beliebige IP-Adresse. Verwenden Sie *, wenn die Regel auf jede IP-Adresse angewendet werden soll.

10. Wenn Sie eine vorhandene Ausgangsausnahme entfernen wollen, klicken Sie auf das Papierkorb-Symbol neben der Ausnahme.
11. Klicken Sie auf **Speichern**.

Die Aktivitäten der Cloud-Firewall prüfen

Wenn die Konfiguration der Firewall-Regeln eines Cloud Servers aktualisiert werden, ist anschließend in der Cyber Protect-Konsole ein Protokoll der Update-Aktivität verfügbar. Sie können das Protokoll einsehen und dabei folgende Informationen überprüfen:

- den Benutzernamen desjenigen Benutzers, der die Konfiguration aktualisiert hat
- den Zeitpunkt (Datum, Uhrzeit) des Updates
- die Firewall-Einstellungen für ein- und ausgehende Verbindungen
- die Standardaktionen für ein- und ausgehende Verbindungen
- die Protokolle, Ports und IP-Adressen der Ausnahmen für ein- und ausgehende Verbindungen

So können Sie die Details zu einer Konfigurationsänderung der Cloud-Firewall-Regeln einsehen

1. Klicken Sie in der Cyber Protect-Konsole auf **Monitoring** –> **Aktivitäten**.
2. Klicken Sie zuerst auf die entsprechende Aktivität und dann auf **Alle Eigenschaften**.
   Die Beschreibung der Aktivität sollte **Cloud Server-Konfiguration wird aktualisiert** lauten.
3. Überprüfen Sie im Feld **Kontext** die Informationen, für die Sie sich interessieren.

Backup der Cloud Server

Die primären Server und Recovery-Server werden agentenlos auf der Cloud-Site gesichert. Für diese Backups gelten die nachfolgenden Einschränkungen.

- Der einzig mögliche Backup-Speicherort ist der Cloud Storage. Primäre Server werden zum Storage **Backup der primären Server** gesichert.

  Hinweis
  Microsoft Azure-Backup-Speicherorte werden nicht unterstützt.

- Ein Backup-Plan kann nicht auf mehrere Server gleichzeitig angewendet werden. Jeder Server muss seinen eigenen Backup-Plan haben, auch wenn alle Backup-Pläne ansonsten die gleichen Einstellungen haben.
- Auf einen Server kann nur je ein Backup-Plan angewendet werden.
- Applikationskonforme Backups werden nicht unterstützt.
- Es ist keine Verschlüsselung verfügbar.
- Es sind keine Backup-Optionen verfügbar.

Wenn Sie einen primären Server löschen, werden auch dessen Backups gelöscht.

Ein Recovery-Server wird nur im Failover-Stadium per Backup gesichert. Seine Backups setzen die Backup-Sequenz des ursprünglichen Servers fort. Wenn ein Failback durchgeführt wird, kann der ursprüngliche Server diese Backup-Sequenz fortsetzen. Die Backups des Recovery-Servers können also nur manuell gelöscht werden – oder weil Aufbewahrungsregeln angewendet werden. Wenn ein Recovery-Server gelöscht wird, werden seine Backups immer aufbewahrt.

Hinweis
Die Backup-Pläne für Cloud Server werden nach UTC-Zeit durchgeführt.

Orchestrierung (Runbooks)

Hinweis
In Abhängigkeit davon, welches Lizenzierungsmodell angewendet wird, kann für einige Funktionen eine zusätzliche Lizenzierung erforderlich sein.

Ein Runbook ist eine Zusammenstellung von Anweisungen, die beschreibt, wie die Produktionsumgebung in die Cloud übertragen wird. Sie können Runbooks in der Cyber Protect-Konsole erstellen. Wenn Sie auf die Anzeige **Runbooks** zugreifen wollen, wählen Sie die Befehle **Disaster Recovery** –> **Runbooks**.

Warum sollte ich Runbooks verwenden?

Mit Runbooks können Sie Folgendes tun:

- Ein Failover von einem oder mehreren Servern automatisieren
- Das Failover-Ergebnis automatisch überprüfen, indem Sie die Server-IP-Adresse anpingen und die Verbindung zu dem von Ihnen spezifizierten Port überprüfen
- Die Reihenfolge der Aktionen mit den Servern festlegen, die verteilte Applikationen ausführen
- Manuelle Aktionen in den Workflow einbinden
- Die Integrität Ihrer Disaster Recovery-Lösung überprüfen, indem Sie die entsprechenden Runbooks im Testmodus ausführen.

Ein Runbook erstellen

Ein Runbook besteht aus Schritten, die nacheinander ausgeführt werden. Ein Schritt besteht aus Aktionen, die gleichzeitig gestartet werden.

Sie können die nachfolgende Anleitung befolgen oder sich das Video-Tutorial ansehen.

So können Sie ein Runbook erstellen

1. Gehen Sie in der Cyber Protection-Konsole zu **Disaster Recovery** –> **Runbooks**.
2. Klicken Sie auf **Runbook erstellen**.
3. Klicken Sie auf **Schritt hinzufügen**.
4. Klicken Sie zuerst auf **Aktion hinzufügen** und wählen Sie dann die Aktion aus, die Sie dem Schritt hinzufügen wollen.

Aktion	Beschreibung
Server-Failover ausführen	Führt eine Failover-Aktion mit einem Cloud Server durch. Wenn Sie diese Aktion definieren wollen, müssen Sie einen Cloud Server auswählen und die Runbook-Parameter konfigurieren, die für diese Aktion verfügbar sind. Weitere Informationen zu diesen Parametern finden Sie im Abschnitt '"Runbook-Parameter" (S. 892)'. **Hinweis** Wenn das Backup des von Ihnen ausgewählten Servers über die Maschinen-Eigenschaften verschlüsselt wurde, wird die Aktion **Server-Failover ausführen** pausiert und automatisch zu **Benutzereingriff erforderlich** geändert. Um mit der Ausführung des Runbooks fortfahren zu können, müssen Sie das Kennwort für das verschlüsselte Backup angeben.
Server-Failback ausführen	Führt eine Failback-Aktion mit einem Cloud Server durch. Wenn Sie diese Aktion definieren wollen, müssen Sie einen Cloud Server auswählen und die Runbook-Parameter konfigurieren, die für diese Aktion verfügbar sind. Weitere Informationen zu diese Einstellungen finden Sie im Abschnitt '"Runbook-Parameter" (S. 892)'. **Hinweis** Runbook-Aktionen unterstützen Failbacks nur im manuellen Modus. Das heißt, wenn Sie den Failback-Prozess durch die Ausführung eines Runbooks starten, in dem ein **Server-Failback ausführen**-Schritt enthalten ist, erfordert die Prozedur eine manuelle Interaktion: Sie müssen die Maschine zuerst manuell wiederherstellen und dann den Failback-Prozess über die Registerkarte **Disaster Recovery** –> **Server** bestätigen oder abbrechen.
Server starten	Startet einen Cloud Server. Wenn Sie diese Aktion definieren wollen, müssen Sie einen Cloud Server auswählen und die Runbook-Parameter konfigurieren, die für diese Aktion verfügbar sind. Weitere Informationen zu diese Einstellungen finden

Aktion	Beschreibung
	Sie im Abschnitt '"Runbook-Parameter" (S. 892)'. **Hinweis** Die Aktion **Server starten** ist bei Test-Failover-Aktionen in Runbooks nicht verfügbar. Wenn Sie versuchen, eine solche Aktion auszuführen, wird diese mit folgender Fehlermeldung fehlschlagen: Fehlgeschlagen: Die Aktion ist auf das aktuelle Server-Stadium nicht anwendbar.
Server stoppen	Stoppt einen Cloud Server. Wenn Sie diese Aktion definieren wollen, müssen Sie einen Cloud Server auswählen und die Runbook-Parameter konfigurieren, die für diese Aktion verfügbar sind. Weitere Informationen zu diese Einstellungen finden Sie im Abschnitt '"Runbook-Parameter" (S. 892)'. **Hinweis** Die Aktion **Server stoppen** ist bei Test-Failover-Aktionen in Runbooks nicht verfügbar. Wenn Sie versuchen, eine solche Aktion auszuführen, wird diese mit folgender Fehlermeldung fehlschlagen: Fehlgeschlagen: Die Aktion ist auf das aktuelle Server-Stadium nicht anwendbar.
Manuelle Aktion	Eine manuelle Aktion erfordert das Eingreifen eines Benutzers. Wenn Sie diese Aktion definieren wollen, müssen Sie eine Beschreibung eingeben. Wenn eine Runbook-Sequenz eine manuelle Aktion erreicht, wird das Runbook solange pausiert, bis ein Benutzer die erforderliche manuelle Aktion durchführt, z.B. durch Klicken auf die Bestätigungsschaltfläche.
Runbook ausführen	Führt ein anderes Runbook aus. Wenn Sie diese Aktion definieren wollen, müssen Sie ein Runbook auswählen. Ein Runbook kann nur eine (1) Ausführung eines bestimmten Runbooks enthalten. Wenn Sie beispielsweise die Aktion 'Runbook A ausführen' hinzugefügt haben, können Sie zwar die Aktion 'Runbook B ausführen' hinzufügen, aber keine weitere Aktion 'Runbook A ausführen'.

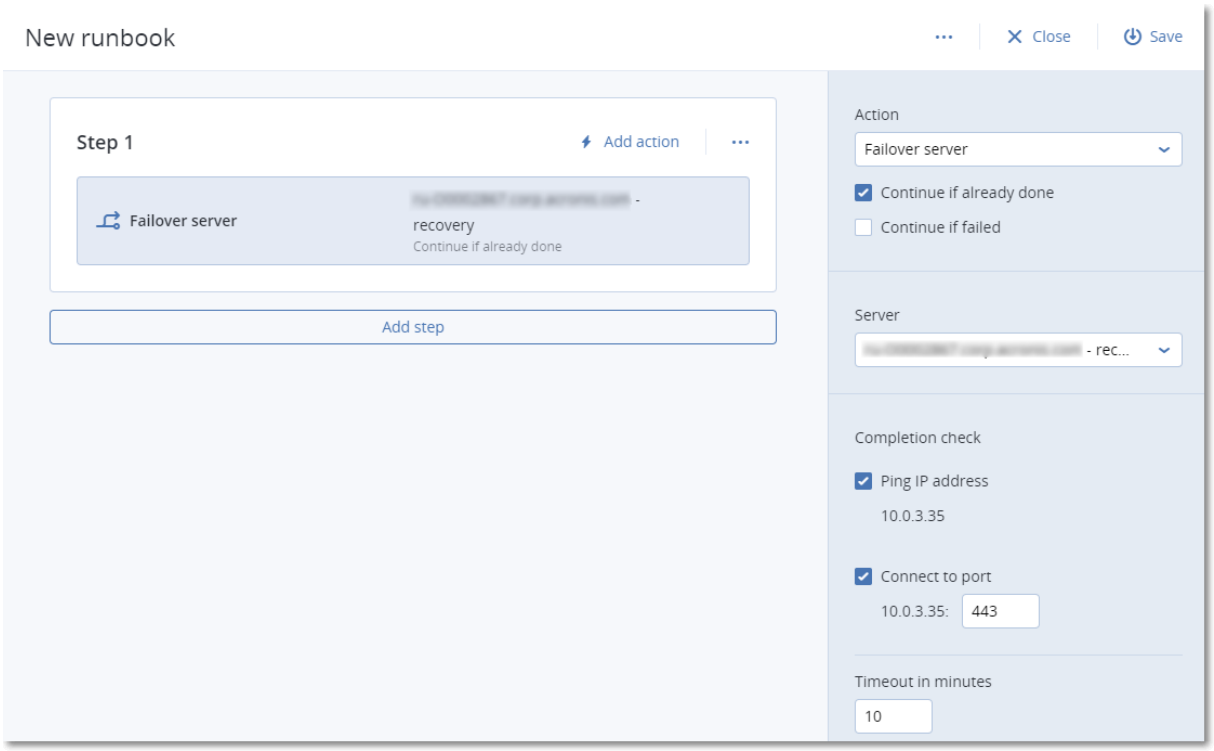
5. Definieren Sie die Runbook-Parameter für die Aktion. Weitere Informationen zu diesen Parametern finden Sie im Abschnitt '"Runbook-Parameter" (S. 892)'.
6. [Optional] So können Sie eine Beschreibung für den Schritt hinzufügen:
   a. Klicken Sie auf das Drei-Punkte-Symbol und anschließend auf **Beschreibung**.
   b. Geben Sie eine Beschreibung für den Schritt ein.
   c. Klicken Sie auf **Fertig**.
7. Wiederholen Sie die Schritte 3–6, bis Sie die gewünschte Abfolge von Schritten und Aktionen erstellt haben.
8. [Optional] So können Sie den Standardnamen des Runbooks ändern:
   a. Klicken Sie auf das Drei-Punkte-Symbol.
   b. Geben Sie den Namen des Runbooks ein.

c. Geben Sie eine Beschreibung für das Runbook ein.

d. Klicken Sie auf **Fertig**.

9. Klicken Sie auf **Speichern**.

10. Klicken Sie auf **Schließen**.



Runbook-Parameter

Runbook-Parameter sind spezifische Einstellungen, die Sie konfigurieren müssen, um eine Runbook-Aktion zu definieren. Es gibt zwei Kategorien von Runbook-Parametern: für Aktionen und für die Fertigstellungsprüfung.

Aktionsparameter definieren das Verhalten des Runbooks in Abhängigkeit vom anfänglichen Stadium oder dem Ergebnis einer Aktion.

Parameter für die Fertigstellungsprüfung stellen sicher, dass der Server verfügbar ist und die notwendigen Dienste bereitstellt. Wenn eine Fertigstellungsprüfung scheitert, wird die Aktion als fehlgeschlagen betrachtet.

Die folgende Tabelle beschreibt die konfigurierbaren Runbook-Parameter für jede Aktion.

Runbook-Parameter	Kategorie	Für Aktion verfügbar	Beschreibung
Fortsetzen, wenn bereits durchgeführt	Aktionsparameter	• **Server-Failover ausführen** • **Server starten**	Dieser Parameter definiert das Runbook-Verhalten, wenn die erforderliche Aktion bereits

Runbook-Parameter	Kategorie	Für Aktion verfügbar	Beschreibung
		• **Server stoppen** • **Server-Failback ausführen**	durchgeführt wurde (weil beispielsweise ein Failover bereits durchgeführt wurde oder ein Server bereits ausgeführt wird). Wenn dieser Parameter aktiviert ist, gibt das Runbook eine Warnung aus und fährt mit der Ausführung fort. Wenn der Parameter deaktiviert wurde, schlägt die Aktion und damit dann auch das Runbook fehl. Dieser Parameter ist standardmäßig aktiviert.
Fortsetzen, wenn fehlgeschlagen	Aktionsparameter	• **Server-Failover ausführen** • **Server starten** • **Server stoppen** • **Server-Failback ausführen**	Dieser Parameter definiert das Runbook-Verhalten, wenn die erforderliche Aktion fehlschlägt. Wenn dieser Parameter aktiviert ist, gibt das Runbook eine Warnung aus und fährt mit der Ausführung fort. Wenn der Parameter deaktiviert wurde, schlägt die Aktion und damit dann auch das Runbook fehl. Dieser Parameter ist standardmäßig deaktiviert.
IP-Adresse anpingen	Fertigstellungsprüfung	• **Server starten**	Die Software wird die Produktions-IP-Adresse des Cloud Servers solange anpingen, bis der Server antwortet oder es zu einem Timeout kommt (je nachdem, was zuerst eintritt).
Mit Port verbinden (standardmäßig 443)	Fertigstellungsprüfung	• **Server-Failover ausführen** • **Server starten**	Die Software wird versuchen, sich über die Produktions-IP-Adresse und den von Ihnen spezifizierten Port mit dem Cloud Server zu verbinden, bis die Verbindung hergestellt ist oder es zu einem Timeout kommt (je nachdem, was zuerst eintritt). Auf diese Weise können Sie überprüfen, ob die Applikation, die auf dem

Runbook-Parameter	Kategorie	Für Aktion verfügbar	Beschreibung
			angegebenen Port lauscht, auch ausgeführt wird.
Zeitlimit in Minuten	Fertigstellungsprüfung	• **Server-Failover ausführen** • **Server starten**	Der vorgegebene Timeout-Wert beträgt 10 Minuten.

Aktionen mit Runbooks

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Um auf die Liste der Aktionen zuzugreifen, bewegen Sie den Mauszeiger auf ein Runbook und klicken Sie auf das Drei-Punkte-Symbol. Wenn ein Runbook nicht ausgeführt wird, sind folgenden Aktionen verfügbar:

- **Ausführen**
- **Bearbeiten**
- **Klonen**
- **Löschen**

Ein Runbook ausführen

Jedes Mal, wenn Sie auf **Ausführen** klicken, werden Sie zur Eingabe von Ausführungsparametern aufgefordert. Diese Parameter gelten für alle Failover- und Failback-Operationen, die im Runbook enthalten sind. Diejenigen Runbooks, die mit der Operation **Runbook ausführen** spezifiziert werden, erben diese Parameter vom Haupt-Runbook.

- **Failover- und Failback-Modus**
  Wählen Sie, ob Sie einen Test-Failover (Standardvorgabe) oder einen tatsächlichen (Produktions-)Failover ausführen möchten. Der Failback-Modus entspricht dem gewählten Failover-Modus.
- **Failover-Recovery-Punkt**
  Wählen Sie den neuesten Recovery-Punkt (Standardvorgabe) oder wählen Sie einen bestimmten Zeitpunkt in der Vergangenheit. Bei letzterem werden für jeden Server diejenigen Recovery-Punkte ausgewählt, die dem spezifizierten Zeitpunkt am nächsten liegen.

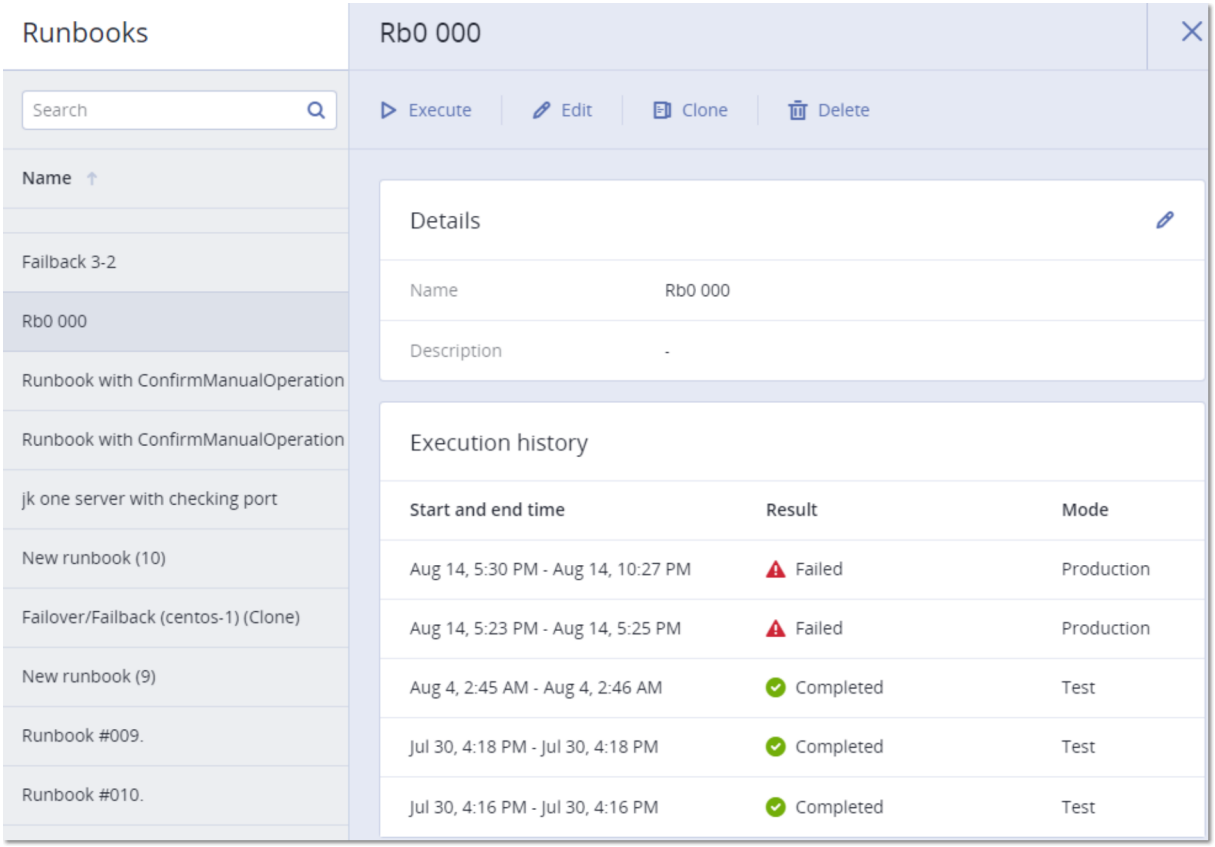
Eine Runbook-Ausführung stoppen

Sie können während einer Runbook-Ausführung den Befehl **Stopp** aus der Liste der verfügbaren Aktionen wählen. Die Software wird alle bereits gestarteten Aktionen abschließen – außer solche

Aktionen, die eine Benutzerinteraktion erfordern.

Den Ausführungsverlauf anzeigen

Wenn Sie ein Runbook in der Registerkarte **Runbooks** auswählen, wird Ihnen die Software Details und einen Ausführungsverlauf zu diesem Runbook anzeigen. Klicken Sie auf eine Zeile, die zu einer bestimmten Ausführung gehört, um das entsprechende Ausführungsprotokoll einzusehen.



Ihre Antivirus & Antimalware Protection konfigurieren

Hinweis
Auf Windows-Maschinen ist es für die Antimalware Protection-Funktion die Installation des Agenten für Antimalware Protection sowie für die URL-Filterungsfunktion die Installation des Agenten für URL-Filterung erforderlich. Diese Agenten werden automatisch auf den geschützten Workloads installiert, wenn die Module **Antivirus & Antimalware Protection** und/oder **URL-Filterung** in deren Schutzplänen aktiviert werden.

Die Antimalware Protection in Cyber Protection bietet Ihnen folgende Vorteile:

- Höchsten Schutz auf allen Ebenen: proaktiv, aktiv und reaktiv.
- Vier verschiedene integrierte Antimalware-Technologien versorgen Sie mit einem erstklassigen mehrschichtigen Schutz gegen Schadsoftware.
- Verwaltung von Microsoft Security Essentials und Microsoft Defender Antivirus.

  Hinweis
  Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Wichtig
Die EICAR-Testdatei wird nur erkannt, wenn im Schutzplan die Option **Advanced Antimalware** aktiviert ist. Wenn die EICAR-Datei nicht erkannt wird, hat dies jedoch keinen Einfluss auf die Antimalware-Funktionen von Cyber Protection.

Unterstützte Plattformen

Die Active Protection- und Antivirus & Antimalware Protection-Funktionen werden auf folgenden Plattformen unterstützt.

Betriebssystem	Version/Distribution
Windows	Windows 7 Service Pack 1 und höher Windows Server 2008 R2 Service Pack 1 und höher

Betriebssystem	Version/Distribution
	Hinweis Bei Windows 7 müssen Sie vor der Installation des Protection Agenten die nachfolgenden Updates von Microsoft installieren. • Windows 7 Extended Security Updates (ESU) • KB4474419 • KB4490628 Weitere Informationen zu den erforderlichen Updates finden Sie in diesem Knowledge Base-Artikel.
Linux	Red Hat Linux 7.x, 8.x, 9.x CloudLinux 6.10, 7.x, 8.x CentOS 6.5 und höhere 6.x-Versionen sowie 7.x, 8.x Ubuntu 16.04, 18.04, 20.04, 22.04, 22.10 Debian 8.x, 9.x, 10,x, 11.x Oracle Linux 7.x, 8.x, 9.x SUSE Enterprise Linux 15.x openSUSE Leap 15.x
macOS	macOS 10.13.x und höher

Unterstützte Funktionen je nach Plattform

Hinweis
Die Antimalware Protection-Funktionalität für Linux und macOS ist über das Advanced Antimalware-Paket verfügbar.

Funktionssatz	Windows	Linux	macOS
Antivirus & Antimalware Protection			
Voll integrierte Active Protection-Funktionalität	Ja	Nein	Nein
Antimalware Protection in Echtzeit	Ja	Ja, mit dem Advanced Antimalware-Paket	Ja, mit dem Advanced Antimalware-Paket
Advanced Realtime Antimalware Protection mit lokaler signaturbasierter Erkennung	Ja	Ja	Ja
Statische Analyse für übertragbare	Ja	Nein	Ja*

Funktionssatz	Windows	Linux	macOS
Antivirus & Antimalware Protection			
ausführbare Dateien			
On-Demand-Antimalware-Scanning	Ja	Ja**	Ja
Netzwerkordnerschutz	Ja	Ja	Nein
Serverseitiger Schutz	Ja	Nein	Nein
Scannen von Archivdateien	Ja	Nein	Ja
Scannen von Wechsellaufwerken	Ja	Nein	Ja
Scannen von nur neuen und geänderten Dateien	Ja	Nein	Ja
Ausschluss von Dateien/Ordnern	Ja	Ja	Ja***
Ausschluss von Prozessen	Ja	Nein	Ja
Behavioral Analysis Engine (Verhaltensanalyse-Modul)	Ja	Nein	Ja
Exploit-Prävention	Ja	Nein	Nein
Quarantäne	Ja	Ja	Ja
Quarantäne-Speicherort automatisch bereinigen	Ja	Ja	Ja
URL-Filterung (http/https)	Ja	Nein	Nein
Unternehmensweite Positivliste	Ja	Nein	Ja
Firewall-Verwaltung****	Ja	Nein	Nein
Microsoft Defender Antivirus-Verwaltung*****	Ja	Nein	Nein
Microsoft Security Essentials-Management	Ja	Nein	Nein
Antivirus & Antimalware Protection im Windows-Sicherheitscenter registrieren und verwalten	Ja	Nein	Nein
Für weitere Informationen über die unterstützten Betriebssysteme und deren Versionen finden Sie im Abschnitt '"Unterstützte Plattformen" (S. 896)'.			

* Statische Analyse für übertragbare ausführbare Dateien wird nur für geplante Scans auf macOS unterstützt.

** Unter Linux werden keine Startbedingungen für On-Demand-Scans unterstützt.

*** Der Ausschluss von Dateien/Ordnern wird nur dann unterstützt, wenn Sie Dateien/Ordner spezifizieren, die weder vom Echtzeitschutz (Realtime Protection, RTP) noch von geplanten Scans auf macOS überprüft werden.

**** Die Firewall-Verwaltung wird unter Windows 8 und höher unterstützt. Windows Server werden nicht unterstützt.

***** Die Windows Defender Antivirus-Verwaltung wird unter Windows 8.1 und höher unterstützt.

Funktionssatz	Windows	Linux	macOS
Active Protection			
Erkennung von Prozesseinschleusung	Ja	Nein	Nein
Automatisches Recovery von betroffenen Dateien aus lokalem Cache	Ja	Ja	Ja
Selbstschutzfunktion für Acronis Backup-Dateien	Ja	Nein	Nein
Selbstschutzfunktion für die Acronis Software	Ja	Nein	Ja (Nur Active Protection- und Antimalware-Komponenten)
Verwaltung vertrauenswürdiger/geblockter Prozesse	Ja	Nein	Ja
Ausschluss von Prozessen/Ordnern	Ja	Ja	Ja
Erkennung von Ransomware aufgrund von Prozessverhalten (KI-basiert)	Ja	Ja	Ja
Erkennung von Cryptomining-Prozessen anhand von Prozessverhalten	Ja	Nein	Nein
Schutz von externen Laufwerken (HDD, USB-Sticks, SD-Karten)	Ja	Nein	Ja
Netzwerkordnerschutz	Ja	Ja	Ja
Serverseitiger Schutz	Ja	Nein	Nein
Schutz für Cisco Webex, Citrix Workspace und Microsoft Teams	Ja	Nein	Nein
Für weitere Informationen über die unterstützten Betriebssysteme und deren Versionen finden Sie im Abschnitt '"Unterstützte Plattformen" (S. 896)'.			

Antivirus & Antimalware Protection

Hinweis
In Abhängigkeit davon, welches Lizenzierungsmodell angewendet wird, kann für einige Funktionen eine zusätzliche Lizenzierung erforderlich sein.

Das **Antivirus & Antimalware Protection**-Modul kann Ihre Windows-, Linux- und macOS-Maschinen vor allen aktuellen Malware-Bedrohungen schützen. Die vollständige Liste der unterstützten Antimalware-Funktionen finden Sie im Abschnitt '"Unterstützte Plattformen" (S. 896)'.

Die Antivirus & Antimalware Protection wird vom Windows-Sicherheitscenter unterstützt und in diesem registriert.

Antimalware-Funktionen

- Erkennen von Malware in Dateien – wahlweise im Echtzeit-Modus (Realtime Protection, RTP) oder manuell bei Bedarf ausgeführt (On-Demand-Modus)
- Erkennen von schädlichen Verhaltensmustern in Prozessen (für Windows)
- Blockieren von Zugriffen auf schädliche URLs (für Windows)
- Verschieben von gefährlichen Dateien in eine Quarantäne
- Verwalten einer Positivliste mit vertrauenswürdigen Unternehmensapplikationen

Scanning-Methoden

Sie können die Antivirus & Antimalware Protection so konfigurieren, dass diese entweder kontinuierlich im Hintergrund ausgeführt oder bei Bedarf manuell gestartet wird.

Echtzeitschutz

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Der Echtzeitschutz (auch Realtime Protection bzw. RTP genannt) überprüft alle Dateien, die auf einer Maschine ausgeführt oder geöffnet werden, um diese vor Malware-Bedrohungen zu schützen.

Um mögliche Kompatibilitäts- und Performance-Probleme zu vermeiden, kann Echtzeitschutz nicht parallel zu anderen Antivirus-Lösungen arbeiten, die ebenfalls Echtzeitschutzfunktionen verwenden. Die Statuszustände von anderen installierten Antivirus-Lösungen werden über das Windows-Sicherheitscenter bestimmt. Wenn die Windows-Maschine bereits von einer anderen Antivirus-Lösung geschützt ist, wird der Echtzeitschutz automatisch ausgeschaltet.

Wenn Sie den Echtzeitschutz aktivieren wollen, müssen Sie die andere Antivirus-Lösung deaktivieren oder deinstallieren. Unser Echtzeitschutz kann den Echtzeitschutz von Microsoft Defender automatisch ersetzen.

Hinweis
Auf Maschinen, die unter einem Windows Server-Betriebssystem laufen, wird der Microsoft Defender nicht automatisch abgeschaltet, wenn der Echtzeitschutz aktiviert ist. Ein Administrator muss den Microsoft Defender manuell ausschalten, um mögliche Kompatibilitätsprobleme zu vermeiden.

Sie können einen der folgenden Scan-Modi wählen:

- Eine Erkennung **Bei Zugriff (intelligent)** (Smart On-Access Detection) bedeutet, dass die Antimalware-Funktionalität im Hintergrund läuft und dabei das System Ihrer Maschine aktiv und kontinuierlich auf Viren und andere bösartige Bedrohungen scannt. Dies erfolgt während gesamten Betriebszeit Ihres Systems. Malware wird sowohl bei der Ausführung einer Datei als auch bei verschiedenen Aktionen mit einer Datei (etwa, wenn diese zum Lesen oder Bearbeiten geöffnet wird) erkannt.
- Eine Erkennung **Bei Ausführung** (On-Execution Detection) bedeutet, dass nur ausführbare Dateien gescannt werden – und zwar im Augenblick ihrer Ausführung. So wird sichergestellt, dass diese Dateien sauber sind und Ihre Maschine oder deren Daten nicht beschädigen können. Das Kopieren einer infizierten Datei wird jedoch nicht erkannt.

Geplanter Scan

Das Antimalware-Scanning wird auf Basis eines Zeitplans durchgeführt.

Sie können einen der nachfolgenden Scan-Modi wählen.

- Der **Schnellscan** – Überprüft nur die Systemdateien des Workloads.
- Der **Vollständige Scan** – Überprüft alle Dateien auf Ihrem Workload.
- Der **Benutzerdefinierte Scan** – Überprüft die Dateien/Ordner, die vom Administrator zum Schutzplan hinzugefügt wurden.

Nach Abschluss des Antimalware-Scans können Sie Details zu den Workloads, die von Bedrohungen betroffen waren, im Widget **Monitoring** –> **Überblick** –> Kürzlich betroffen einsehen.

Einstellungen für die Antivirus & Antimalware Protection

In diesem Abschnitt werden die Funktionen beschrieben, die Sie im **Antivirus & Antimalware Protection**-Modul eines Schutzplans konfigurieren können. Informationen zum Erstellen eines Schutzplans finden Sie im Abschnitt '"Einen Schutzplan erstellen" (S. 232)'.

Folgende Funktionen können im Antivirus & Antimalware Protection-Modul für einen Schutzplan konfiguriert werden:

- "Active Protection" (S. 902)
- "Advanced Antimalware" (S. 903)
- "Netzwerkordnerschutz" (S. 903)
- "Serverseitiger Schutz" (S. 904)
- "Selbstschutz" (S. 905)
- "Erkennung von Cryptomining-Prozessen" (S. 906)
- "Quarantäne" (S. 907)
- "Behavior Engine" (S. 907)
- "Exploit-Prävention" (S. 908)
- "Echtzeitschutz" (S. 910)
- "Scan planen" (S. 911)
- "Schutz-Ausschlüsse" (S. 915)

Hinweis
Nicht alle Betriebssysteme unterstützen die Antivirus & Antimalware Protection-Funktionen. Weitere Informationen zu den unterstützten Betriebssystemen und Funktionen finden Sie unter "Unterstützte Plattformen" (S. 896). Einige Funktionen erfordern eine bestimmte Lizenz, die in Ihrem Schutzplan verfügbar sein muss.

Active Protection

Active Protection schützt Ihr System vor Ransomware – einem speziellen Typ bösartiger Software (Malware), welche Dateien verschlüsselt und für die Herausgabe des Verschlüsselungscodes ein Lösegeld verlangt. Daher wird Ransomware auch als „Erpressungstrojaner“ bezeichnet.

Standardeinstellung: **Aktiviert**.

Hinweis
Auf der zu schützenden Maschine muss ein Protection Agent installiert sein. Für weitere Informationen über die unterstützten Betriebssysteme und Funktionen finden Sie im Abschnitt '"Unterstützte Plattformen" (S. 896)'.

So können Sie Active Protection konfigurieren

1. Erweitern Sie im Fenster **Schutzplan erstellen** das Modul **Antivirus & Antimalware Protection**.
2. Klicken Sie auf **Active Protection**.
3. Wählen Sie im Bereich **Aktion bei Erkennung** eine der verfügbaren Optionen:

   Standardeinstellung: **Aus Cache wiederherstellen**

   - **Nur benachrichtigen** – Die Software generiert einen Alarm, wenn ein Prozess eine mögliche Ransomware-Aktivität zeigt.

- **Den Prozess stoppen** – Die Software blockiert den Prozess und generiert einen Alarm, wenn ein Prozess eine mögliche Ransomware-Aktivität zeigt.
- **Aus Cache wiederherstellen** – Die Software generiert einen Alarm, stoppt den Prozess und setzt die erfolgten Dateiänderungen mithilfe des Service-Caches zurück.

4. Klicken Sie auf **Fertig**, um die ausgewählten Optionen auf Ihren Schutzplan anzuwenden.

Advanced Antimalware

Diese Engine verwendet eine erweiterte Datenbank mit Virensignaturen, um die Effizienz der Antimalware-Erkennung sowohl bei schnellen als auch bei vollständigen Scans zu verbessern.

Wichtig
Diese Funktion ist nur verfügbar, wenn Sie das Advanced Security-Schutzpaket aktiviert haben. Weitere Informationen finden Sie unter https://www.acronis.com/de-de/products/cloud/cyber-protect/security/

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

So können Sie Advanced Antimalware konfigurieren

1. Erweitern Sie im Fenster **Schutzplan erstellen** das Modul **Antivirus & Antimalware Protection**.
2. Verwenden Sie im Bereich **Advanced Antimalware** den Schalter, um die lokale signaturbasierte Engine zu aktivieren.

Hinweis
Die Antivirus & Antimalware Protection für macOS und Linux benötigt ebenfalls die lokale signaturbasierte Engine. Bei Windows ist die Antivirus & Antimalware Protection mit oder ohne diese Engine verfügbar.

Netzwerkordnerschutz

Die Funktion **Netzwerkordnerschutz** bestimmt, ob auch Netzwerkordner durch die Antivirus & Antimalware Protection-Funktion geschützt werden sollen, die als lokale Laufwerke zugeordnet (gemountet) sind. Der Schutz gilt für Ordner, die per SMB- oder NFS-Protokoll freigegeben/zugeordnet wurden.

So können Sie den Netzwerkordnerschutz konfigurieren

1. Erweitern Sie im Fenster **Schutzplan erstellen** das Modul **Antivirus & Antimalware Protection**.
2. Klicken Sie auf **Netzwerkordnerschutz**.
3. Fügen Sie die Dateien hinzu, wo Sie die Netzwerk Ordner sichern wollen:

- Wenn es sich bei Ihrem Workload beispielsweise um Windows handelt, müssen Sie im Feld **Windows** den Pfad für die Windows-Datei eingeben, wo Sie die Netzwerkordner sichern wollen. Standardwert: C:\ProgramData\Acronis\Restored Network Files.
- Wenn es sich bei Ihrem Workload beispielsweise um macOS handelt, müssen Sie im Feld **macOS** den Pfad für die macOS-Datei eingeben, wo Sie die Netzwerkordner sichern wollen. Standardwert: /Library/Application Support/Acronis/Restored Network Files/.

Hinweis
Geben Sie den Pfad eines lokalen Ordners ein. Netzwerkordner (einschließlich Ordnern auf zugeordneten Laufwerken) werden nicht als Backup-Ziele für die Netzwerkordner unterstützt.

4. Klicken Sie auf **Fertig**, um die ausgewählten Optionen auf Ihren Schutzplan anzuwenden.

Serverseitiger Schutz

Diese Funktion schützt Netzwerkordner, die Sie freigegeben haben, per Active Protection vor potentiellen Bedrohungen, die über externe Verbindungen (also von anderen Servern im Netzwerk) hereinkommen können.

Standardeinstellung: **Aus**.

Hinweis
Der serverseitige Schutz wird für Linux nicht unterstützt.

So können Sie vertrauenswürdige Verbindungen festlegen

1. Erweitern Sie im Fenster **Schutzplan erstellen** das Modul **Antivirus & Antimalware Protection**.
2. Klicken Sie auf **Serverseitiger Schutz**.
3. Verwenden Sie den Schalter **Serverseitiger Schutz**, um ihn zu aktivieren.
4. Wählen Sie die Registerlasche '**Vertrauenswürdig**'.
5. Klicken Sie im Feld **Vertrauenswürdige Verbindungen** auf **Hinzufügen**, um die Verbindungen zu definieren, wo Datenänderungen erlaubt sein sollen.
6. Geben Sie im Feld **ComputerName/Konto** den Namen des Computers sowie das Konto der Maschine ein, auf welcher der Protection Agent installiert ist. Beispielsweise: `MeinComputer\TestBenutzer`.
7. Geben Sie im Feld **Host-Name** den Host-Namen der Maschine ein, die über den Protection Agenten eine Verbindung zur Maschine herstellen darf.
8. Klicken Sie auf das Häkchensymbol rechts daneben, um die Verbindungsdefinition zu speichern.
9. Klicken Sie auf **Fertig**.

So können Sie blockierte Verbindungen festlegen

1. Erweitern Sie im Fenster **Schutzplan erstellen** das Modul **Antivirus & Antimalware Protection**.
2. Klicken Sie auf **Serverseitiger Schutz**.
3. Verwenden Sie den Schalter **Serverseitiger Schutz**, um ihn zu aktivieren.
4. Wählen Sie die Registerkarte **Blockiert**.
5. Klicken Sie im Feld **Blockierte Verbindungen** auf **Hinzufügen**, um die Verbindungen zu definieren, wo keine Datenänderungen erlaubt sind.
6. Geben Sie im Feld **ComputerName/Konto** den Namen des Computers sowie das Konto der Maschine ein, auf welcher der Protection Agent installiert ist. Beispielsweise: `MeinComputer\TestBenutzer`.
7. Geben Sie im Feld **Host-Name** den Host-Namen der Maschine ein, die über den Protection Agenten eine Verbindung zur Maschine herstellen darf.
8. Aktivieren Sie das Kontrollkästchen rechts daneben, um die Verbindungsdefinition zu speichern.
9. Klicken Sie auf **Fertig**.

Selbstschutz

Der Selbstschutz (Self-Protection) verhindert, dass die Prozesse, Registry-Einträge, ausführbaren Dateien und Konfigurationsdateien der Backup-Software selbst sowie Backups, die in Ihren lokalen Ordnern gespeichert sind, verändert werden können.

Administratoren können den **Selbstschutz** aktivieren, ohne die **Active Protection**-Funktionalität zu aktivieren.

Standardeinstellung: **An**.

Hinweis
Die Selbstschutzfunktion wird für Linux nicht unterstützt.

So können Sie den Selbstschutz aktivieren

1. Erweitern Sie im Fenster **Schutzplan erstellen** das Modul **Antivirus & Antimalware Protection**.
2. Klicken Sie auf **Selbstschutz**.
3. Verwenden Sie den Schalter **Selbstschutz**, um ihn zu aktivieren.

So können Sie den Kennwortschutz aktivieren

1. Sobald die **Selbstschutz**-Funktion aktiviert ist, können Sie auch die Funktion **Kennwortschutz** über den entsprechenden Schalter aktivieren.
2. Klicken Sie auf **Neues Kennwort generieren**, um ein Kennwort zu generieren, mit dem lokale Agenten geändert oder gelöscht werden können.

3. Klicken Sie auf **Kopieren** und fügen Sie es an einem sicheren Speicherort ein. Denn das Kennwort wird abgefragt, wenn Sie die Komponentenliste lokal ändern wollen.

   Wichtig
   Das Kennwort wird nicht mehr verfügbar sein, wenn Sie das Fenster schließen. Damit dieses Kennwort auf Geräte angewendet werden kann, müssen die Einstellungen des Schutzplans gespeichert werden.

4. Klicken Sie auf **Schließen**.

Der **Kennwortschutz** verhindert, dass unbefugte Benutzer oder Programme den Agenten für Windows deinstallieren oder dessen Komponenten ändern können. Diese Aktionen sind folglich nur noch mit dem passenden Kennwort möglich, welches ein Administrator bereitstellen kann.

Für folgende Aktionen ist niemals ein Kennwort erforderlich:

- Die Installation durch lokales Ausführen des Setup-Programms aktualisieren
- Die Installation mithilfe der Cyber Protect-Konsole aktualisieren
- Die Installation reparieren

Standardeinstellung: **Deaktiviert**

Weitere Informationen zur Aktivierung des **Kennwortschutzes** finden Sie im Abschnitt 'Unbefugte Deinstallationen oder Änderungen der Agenten verhindern'.

Erkennung von Cryptomining-Prozessen

Cryptomining-Malware kann die Performance nützlicher Applikationen beeinträchtigen, die Stromrechnung erhöhen, Systemabstürze oder sogar Hardware-Schäden (durch übermäßige Nutzung) verursachen. Die Funktion **Erkennung von Cryptomining-Prozessen** schützt Ihre Geräte vor Cryptomining-Malware, um die unberechtigte Nutzung von Computer-Ressourcen zu verhindern.

Administratoren können die **Erkennung von Cryptomining-Prozessen** aktivieren, ohne die **Active Protection**-Funktionalität zu aktivieren. Standardeinstellung: **Aktiviert**.

Hinweis
Die Erkennung von Cryptomining-Prozessen wird für Linux nicht unterstützt.

So können Sie den Netzwerkordnerschutz konfigurieren

1. Erweitern Sie im Fenster **Schutzplan erstellen** das Modul **Antivirus & Antimalware Protection**.
2. Klicken Sie auf **Erkennung von Cryptomining-Prozessen**.
3. Verwenden Sie den Schalter **Cryptomining-Prozesse erkennen**, um die Funktion zu aktivieren oder zu deaktivieren.

4. Bestimmen Sie, was mit Prozessen geschehen soll, bei denen der Verdacht auf Cryptomining-Aktivitäten besteht:
   Standardeinstellung: **Den Prozess stoppen**
   - **Nur benachrichtigen** – Die Software wird einen Alarm generieren.
   - **Den Prozess stoppen** – Die Software wird einen Alarm generieren und den Prozess stoppen.
5. Klicken Sie auf **Fertig**, um die ausgewählten Optionen auf Ihren Schutzplan anzuwenden.

Quarantäne

Die Quarantäne ist ein Ordner, in dem verdächtige (möglicherweise infizierte) oder potenziell gefährliche Dateien isoliert werden.

So können Sie die Quarantäne konfigurieren

1. Erweitern Sie im Fenster **Schutzplan erstellen** das Modul **Antivirus & Antimalware Protection**.
2. Klicken Sie auf **Quarantäne**.
3. Sie können im Feld **Dateien aus der Quarantäne entfernen nach** einen Zeitraum in Tagen definieren, nach dessen Ablauf die entsprechenden Dateien aus der Quarantäne gelöscht werden.
   Standardeinstellung: **30 Tage**
4. Klicken Sie auf **Fertig**.

Weiter Informationen über diese Funktion finden Sie im Abschnitt 'Quarantäne'.

Behavior Engine

Die **Behavior Engine**-Funktion schützt ein System vor Malware, indem sie mithilfe einer verhaltensbasierten Heuristik bösartige Prozesse identifiziert.

Standardeinstellung: **Aktiviert**.

Hinweis
Die Behavior Engine wird für Linux nicht unterstützt.

So können Sie den Netzwerkordnerschutz konfigurieren

1. Erweitern Sie im Fenster **Schutzplan erstellen** das Modul **Antivirus & Antimalware Protection**.
2. Klicken Sie auf **Behavior Engine**.
3. Verwenden Sie den Schalter **Behavior Engine**, um die Funktion zu aktivieren oder zu deaktivieren.
4. Wählen Sie im Bereich **Aktion bei Erkennung** diejenige Aktion aus, die die Software ausführen soll, wenn eine Malware-Aktivität erkannt wird:
   Standardeinstellung: **Quarantäne**

- **Nur benachrichtigen** – Die Software generiert einen Alarm, wenn ein Prozess eine mögliche Malware-Aktivität zeigt.
- **Den Prozess stoppen** – Die Software blockiert den Prozess und generiert einen Alarm, wenn ein Prozess eine mögliche Malware-Aktivität zeigt.
- **Quarantäne** – Die Software generiert einen Alarm, stoppt den Prozess und verschiebt die entsprechenden ausführbaren Dateien in den Quarantäne-Ordner.

5. Klicken Sie auf **Fertig**, um die ausgewählten Optionen auf Ihren Schutzplan anzuwenden.

Exploit-Prävention

Wichtig
Diese Funktion ist nur verfügbar, wenn Sie das Advanced Security-Schutzpaket aktiviert haben. Weitere Informationen finden Sie unter https://www.acronis.com/de-de/products/cloud/cyber-protect/security/

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Die Exploit-Prävention erkennt und verhindert, dass sich infizierte Prozesse ausbreiten und vorhandene Software-Schwachstellen in einem System ausnutzen. Wenn ein Exploit erkannt wird, kann die Software eine Alarmmeldung generieren und den Prozess stoppen, der mögliche Exploit-Aktivitäten zeigt.

Die Exploit-Prävention ist nur mit Agenten der Version12.5.23130 (21.08, im August 2020 veröffentlicht) oder höher verfügbar.

Standardeinstellung: **Aktiviert** für neu erstellte Schutzpläne – und **Deaktiviert** für bereits vorhandene Schutzpläne, die mit früheren Versionen des Protection Agenten erstellt wurden.

Hinweis
Die Exploit-Prävention wird für Linux nicht unterstützt.

Sie können auswählen, was das Programm tun soll, wenn ein Exploit entdeckt wird, und welche Methoden der Exploit-Prävention vom Programm angewendet werden.

So können Sie die Exploit-Prävention konfigurieren

1. Erweitern Sie im Fenster **Schutzplan erstellen** das Modul **Antivirus & Antimalware Protection**.
2. Klicken Sie auf **Exploit-Prävention**.
3. Wählen Sie im Bereich **Aktion bei Erkennung** eine der verfügbaren Optionen:

   Standardeinstellung: **Den Prozess stoppen**

- **Nur benachrichtigen**

  Die Software wird einen Alarm generieren, wenn ein Prozess im Verdacht steht, Exploit-Aktivitäten auszuführen.
- **Den Prozess stoppen**

  Die Software wird einen Alarm generieren und den Prozess stoppen, der im Verdacht steht, Exploit-Aktivitäten auszuführen.

4. Wählen Sie im Bereich **Aktivierte Exploit-Präventionstechniken** aus den verfügbaren Optionen diejenige aus, die angewendet werden soll:

   Standardeinstellung: **Alle Methoden sind aktiviert**

   - **Memory Protection**

     Erkennt und verhindert verdächtige Modifikationen der Ausführungsrechte von Arbeitsspeicherseiten (Memory Pages). Solche Modifikationen der Speicherseiten-Eigenschaften werden von schädlichen Prozessen vorgenommen, um die Ausführung von Shellcodes aus nicht ausführbaren Speicherbereichen (wie „Stack“ und „Heaps“) zu ermöglichen.
   - **ROP Protection**

     Erkennt und verhindert Angriffsversuche mit der ROP-Exploit-Technik.
   - **Privilege Escalation Protection**

     Erkennt und verhindert Versuche zur „Rechteausweitung“ (auch Privilegien-Erweiterung oder -Eskalation genannt), die von einem nicht autorisierten Code oder einer nicht autorisierten Applikation unternommen werden. Rechteausweitungstechniken werden von bösartigen Software-Codes verwendet, um vollen Zugriff auf eine angegriffene Maschine zu erhalten und dort dann kritische und sensible Tasks auszuführen. Nicht autorisierter Code darf normalerweise nicht auf kritische Systemressourcen zugreifen oder Systemeinstellungen ändern.
   - **Code Injection Protection**

     Erkennt und verhindert, dass bösartiger Software-Code in Remote-Prozesse eingeschleust („injiziert“) wird. Code-Injektion-Techniken werden verwendet, um die böswillige Absicht einer Applikation hinter vermeintlich sauberen oder ungefährlichen Prozessen zu verbergen, um so der Erkennung durch Antimalware-Produkte zu entgehen.

5. Klicken Sie auf **Fertig**, um die ausgewählten Optionen auf Ihren Schutzplan anzuwenden.

Hinweis
Prozesse, die in der Ausschlussliste als vertrauenswürdige Prozesse aufgeführt sind, werden nicht nach Exploits gescannt.

Prozessen erlauben, Backups zu modifizieren

Die Einstelllung **Bestimmten Prozessen erlauben, Backups zu modifizieren** ist nur verfügbar, wenn die Funktion **Selbstschutz** (Self-Protection) aktiviert ist.

Er gilt für Dateien mit den Endungen .tibx, .tib sowie .tia und die in lokalen Ordnern vorliegen.

Mit dieser Einstellung können Sie Prozesse spezifizieren, die berechtigt sind, Backup-Dateien zu modifizieren, auch wenn diese Dateien per Selbstschutz-Funktion grundsätzlich geschützt sind. Dies kann beispielsweise nützlich sein, wenn Sie Backup-Dateien entfernen oder per Skript zu einem anderen Speicherort verschieben wollen.

Wenn diese Einstellung deaktiviert ist, können die Backup-Dateien nur von solchen Prozessen modifiziert werden, die vom Hersteller der Backup-Software signiert wurden. Dadurch kann die Software Aufbewahrungsregeln anwenden und Backups entfernen, wenn ein Benutzer dies über die Weboberfläche anfordert. Andere Prozesse, egal ob diese verdächtig sind oder nicht, können die Backups nicht modifizieren.

Wenn diese Einstellung aktiviert ist, können Sie auch anderen Prozessen erlauben, Backups zu modifizieren. Spezifizieren Sie den vollständigen Pfad zur ausführbaren Datei des Prozesses (mit dem Laufwerksbuchstaben beginnend).

Standardeinstellung: **Deaktiviert**.

Echtzeitschutz

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Der **Echtzeitschutz** (Realtime Protection, RTP) überprüft Ihr Computersystem kontinuierlich auf Viren und andere bösartige Bedrohungen. Dies erfolgt während der gesamten Betriebszeit des Systems – außer, der Echtzeitschutz wird vom Benutzer des Computers pausiert.

Standardeinstellung: **Aktiviert**.

Wichtig
Diese Funktion ist nur verfügbar, wenn Sie das Advanced Security-Schutzpaket aktiviert haben. Weitere Informationen finden Sie unter https://www.acronis.com/de-de/products/cloud/cyber-protect/security/

So können Sie den Echtzeitschutz konfigurieren

1. Erweitern Sie im Fenster **Schutzplan erstellen** das Modul **Antivirus & Antimalware Protection**.
2. Klicken Sie auf **Echtzeitschutz**.
3. Wählen Sie im Listenfeld **Aktion bei Erkennung** eine der verfügbaren Optionen:

   Standardeinstellung: **Quarantäne**

   - **Nur benachrichtigen**

     Die Software generiert einen Alarm, wenn ein Prozess eine mögliche Ransomware-Aktivität zeigt.

   - **Blockieren und benachrichtigen**

Die Software blockiert den Prozess und generiert einen Alarm, wenn ein Prozess eine mögliche Malware-Aktivität zeigt.

- **Quarantäne**

4. Die Software generiert einen Alarm, stoppt den Prozess und verschiebt die entsprechende ausführbare Datei in den Quarantäne-Ordner
5. Wählen Sie im Bereich **Scan-Modus** diejenige Aktion aus, die die Software durchführen soll, wenn ein Virus oder eine andere bösartige Bedrohung erkannt wurde:
   Standardeinstellung: **Bei Zugriff (intelligent)**
   - **Bei Zugriff (intelligent)** – Überwacht alle Systemaktivitäten und scannt Dateien automatisch, wenn auf diese ein Lese- oder Schreibzugriff erfolgt oder wenn ein Programm gestartet wird.
   - **Bei Ausführung** – Überprüft ausführbare Dateien, wenn diese gestartet werden, um sicherzustellen, dass diese sauber sind und Ihren Computer oder Ihre Daten nicht beschädigen können.
6. Klicken Sie auf **Fertig**.

Scan planen

On-Demand-Scannen überprüft Ihr Computersystem entsprechend einer vorgegebenen Planung auf Viren. Ein vollständiger Scan überprüft alle Dateien auf Ihrer Maschine, während ein Schnellscan nur die Systemdateien der Maschine überprüft.

So können Sie die Planung eines Scans konfigurieren

Standardeinstellungen:

- die Option **Benutzerdefinierter Scan** ist deaktiviert.
- Es ist ein Scan vom Typ **Schnell** und **Vollständig** geplant.

1. Erweitern Sie im Fenster **Schutzplan erstellen** das Modul **Antivirus & Antimalware Protection**.
2. Klicken Sie auf **Scan plannen**.
3. Verwenden Sie den Schalter, um die Art von Scan zu aktivieren, den Sie auf Ihre Maschine anwenden wollen.

Verfügbare Scan-Typen:

- **Vollständig** – Dieser Scan dauert im Vergleich zum Schnellscan deutlich länger, weil jede Datei überprüft werden muss.
- **Schnell** – Bei diesem Scan werden nur allgemeine Bereiche überprüft, wo Malware normalerweise auf einer Maschine zu finden ist.
- **Benutzerdefiniert** — Bei dieser Variante werden die Dateien/Ordner gescannt, die vom Administrator für den Schutz-Plan ausgewählt wurden.

Hinweis
Sie können alle drei Scan-Typen – **Schnell**, **Vollständig** und **Benutzerdefiniert** – in einem Schutzplan planen.

So können Sie einen benutzerdefinierbaren Scan konfigurieren

- Verwenden Sie den **Schalter 'Benutzerdefinierter Scan'**, um diese Scan-Typ je nach Bedarf zu (de)aktivieren.
- Wählen Sie im Listenfeld **Aktion bei Erkennung** eine der verfügbaren Optionen:

Standardeinstellung: **Quarantäne**

Quarantäne

Die Software generiert einen Alarm und verschiebt die entsprechende ausführbare Datei in den Quarantäne-Ordner

Nur benachrichtigen

Die Software generiert einen Alarm über den Prozess, bei dem der Verdacht auf Malware-Aktivität besteht, dass es sich um eine Malware handelt.

Feld	Beschreibung
Die Task-Ausführung auf Basis folgender Ereignisse planen	Diese Einstellung definiert, wann der Task ausgeführt werden soll. Folgende Werte sind verfügbar: • **Planung nach Zeit** – Dies ist die Standardeinstellung. Der Task wird gemäß der spezifizierten Zeit ausgeführt. • **Wenn sich ein Benutzer am System anmeldet** – Die Task-Ausführung wird standardmäßig durch die Anmeldung eines (beliebigen) Benutzers ausgelöst. Sie können diese Einstellung so ändern, dass nur ein bestimmtes Benutzerkonto den Task auslösen kann. • **Wenn sich ein Benutzer vom System abmeldet** – Die Task-Ausführung wird standardmäßig durch die Abmeldung eines (beliebigen) Benutzers ausgelöst. Sie können diese Einstellung so ändern, dass nur ein bestimmtes Benutzerkonto den Task auslösen kann. **Hinweis** Der Task wird daher nicht beim Herunterfahren des Systems ausgeführt. Herunterfahren und Abmelden sind unterschiedliche Ereignisse in der Planungskonfiguration. • **Beim Systemstart** – Der Task wird ausgeführt, wenn das Betriebssystem startet. • **Beim Herunterfahren des Systems** – Der Task wird ausgeführt,

Feld	Beschreibung
	wenn das Betriebssystem herunterfährt.
Planungstyp	Das Feld wird angezeigt, wenn Sie bei **Die Task-Ausführung auf Basis folgender Ereignisse planen** die Option **Planung nach Zeit** gewählt haben. Folgende Werte sind verfügbar: • **Monatlich** – Wählen Sie die Monate und dann die jeweiligen Wochen oder Tage des Monats, in denen der Task ausgeführt werden soll. • **Täglich** – Dies ist die Standardeinstellung. Wählen Sie die Wochentage aus, an denen der Task ausgeführt werden soll. • **Stündlich** – Wählen Sie die Wochentage, die Anzahl der Wiederholungen sowie das Zeitintervall aus, in dem der Task ausgeführt werden soll.
Starten um	Das Feld wird angezeigt, wenn Sie bei **Die Task-Ausführung auf Basis folgender Ereignisse planen** die Option **Planung nach Zeit** gewählt haben. Bestimmen Sie den genauen Zeitpunkt, an dem der Task ausgeführt werden soll.
Innerhalb eines Zeitraums ausführen	Das Feld wird angezeigt, wenn Sie bei **Die Task-Ausführung auf Basis folgender Ereignisse planen** die Option **Planung nach Zeit** gewählt haben. Bestimmten Sie einen Datumsbereich, innerhalb dessen die konfigurierte Planung gültig sein soll.
Spezifizieren Sie einen Benutzer, dessen Anmeldung am Betriebssystem einen Task auslösen wird	Das Feld wird angezeigt, wenn Sie bei **Die Task-Ausführung auf Basis folgender Ereignisse planen** die Option **Wenn sich ein Benutzer am System anmeldet** gewählt haben. Folgende Werte sind verfügbar: • **Jeder Benutzer** – Verwenden Sie diese Option, wenn Sie wollen, dass der Task durch die Anmeldung eines beliebigen Benutzers ausgelöst wird. • **Der folgende Benutzer** – Verwenden Sie diese Option, wenn Sie wollen, dass der Task nur durch die Anmeldung eines bestimmten Benutzerkontos ausgelöst wird.
Spezifizieren Sie einen Benutzer, dessen Abmeldung vom Betriebssystem einen Task	Das Feld wird angezeigt, wenn Sie bei **Die Task-Ausführung auf Basis folgender Ereignisse planen** die Option **Wenn sich ein Benutzer vom System abmeldet** gewählt haben. Folgende Werte sind verfügbar: • **Jeder Benutzer** – Verwenden Sie diese Option, wenn Sie wollen,

Feld	Beschreibung
auslösen wird	dass der Task durch die Abmeldung eines beliebigen Benutzers ausgelöst wird. • **Der folgende Benutzer** – Verwenden Sie diese Option, wenn Sie wollen, dass der Task nur durch die Abmeldung eines bestimmten Benutzerkontos ausgelöst wird.
Startbedingungen	Definieren Sie alle Bedingungen, die gleichzeitig zutreffen müssen, damit der Task ausgeführt werden kann. Die Startbedingungen für Antimalware-Scans sind ähnlich wie die Startbedingungen für das **Backup-Modul**, die wiederum im Abschnitt 'Startbedingungen' beschrieben sind. Sie können folgende zusätzliche Startbedingungen definieren: • **Task-Startzeit innerhalb eines Zeitfensters verteilen**– Diese Option ermöglicht es Ihnen, einen Zeitrahmen für den Task festzulegen, um Netzwerkengpässe zu vermeiden. Sie können die Verzögerung in Stunden oder Minuten spezifizieren. Wenn beispielsweise die Standardstartzeit 10:00 Uhr morgens ist und die Verzögerung 60 Minuten beträgt, dann beginnt der Task zwischen 10:00 und 11:00 Uhr morgens. • **Task bei Neustart der Maschine ausführen, wenn die Maschine zur geplanten Zeit ausgeschaltet war** • **Standby- oder Ruhezustandsmodus während der Task-Ausführung verhindern** – Diese Option gilt nur für Maschinen, die unter Windows laufen. • **Wenn die Startbedingungen nicht erfüllt sind, Task trotzdem ausführen nach** – Spezifizieren Sie einen Zeitraum, nach dem der Task unabhängig von anderen Startbedingungen auf jeden Fall gestartet werden soll. **Hinweis** Für Linux werden keine Startbedingungen unterstützt.

- Aktivieren Sie das Kontrollkästchen **Nur neue und geänderte Dateien scannen**, wenn nur neu erstellte und geänderte Dateien gescannt werden sollen.

Standardeinstellung: **Aktiviert**

- Es werden zwei zusätzliche Optionen für **Benutzerdefinierter Scan** und für **Vollständiger Scan** angezeigt:

1. **Archivdateien scannen**

   Standardeinstellung: **Aktiviert**.

   Max. Rekursionstiefe

Standardeinstellung: **16**

Wie viele Ebenen von eingebetteten Archiven gescannt werden können. Beispiel: MIME-Dokument –> ZIP-Archiv –> Office-Archiv –> Dokumenteninhalt.

Maximale Größe

Standardeinstellung: **100**

Die maximale Größe einer zu scannenden Archivdatei.

2. **Wechsellaufwerke scannen**

Standardeinstellung: **Deaktiviert**

- **Zugeordnetes Netzlaufwerk (Remote-Laufwerk)**
- **USB-Speichergeräte** (wie etwa USB-Sticks und externe Festplatten)
- **CDs/DVDs**

Hinweis
Das Scannen von Wechsellaufwerken wird für Linux nicht unterstützt.

Schutz-Ausschlüsse

Mit Schutz-Ausschlüssen können Sie Falsch-Positiv-Erkennungen vermeiden, wenn ein vertrauenswürdiges Programm fälschlicherweise als Ransomware oder Malware eingestuft werden sollte. Sie können vertrauenswürdige und blockierte Elemente definieren, indem Sie sie in die Liste der Schutz-Ausschlüsse aufnehmen.

In die Liste der vertrauenswürdigen Elemente können Sie Dateien, Prozesse oder Ordner aufnehmen, um diese im System als sicher einzustufen und zu verhindern, dass sie zukünftig noch mal als falsch-positiv erkannt werden.

In die Liste der blockierten Elemente können Sie Prozesse und Hash-Werte aufnehmen. Diese Option gewährleistet, dass diese Prozesse blockiert werden und Ihr Workload abgesichert ist.

Schutz-Ausschlusselement	Blockiert	Vertrauenswürdig
Hash	Wenn ein Hash-Wert in die Blockliste aufgenommen wird, stoppt das System den Prozess auf der Grundlage des angegebenen Hash-Wertes. Wenn Sie beispielsweise den MD5-Hash-Wert '938c2cc0dcc05f2b68c4287040cfcf71' hinzufügen, wird der mit diesem	Wenn ein Hash-Wert in die vertrauenswürdige Liste aufgenommen wird, weiß das System anhand des bereitgestellten Hash-Wertes, welche Prozesse beim Monitoring ignoriert werden sollen. Wenn Sie beispielsweise den MD5-Hash-Wert '938c2cc0dcc05f2b68c4287040cfcf7

Schutz-Ausschlusselement	Blockiert	Vertrauenswürdig
	Hash-Wert assoziierte Prozess blockiert.	1' hinzufügen, wird der mit diesem Hash-Wert assoziierte Prozess als vertrauenswürdig eingestuft und vom Monitoring ausgeschlossen.
Prozess	Wenn ein Prozess in die Blockliste aufgenommen wird, weiß das System, dass diese Prozesse überwacht werden sollen, und die Prozesse werden dauerhaft blockiert. Wenn Sie beispielsweise den Pfad 'C:\Users\user1\application\nppInstaller.exe' zur Blockliste hinzufügen, wird dieser spezielle Prozess blockiert. Wenn Sie dennoch versuchen, ihn zu öffnen, wird sein Start nicht zugelassen.	Wenn ein Prozess in die vertrauenswürdige Liste aufgenommen wird, weiß das System, dass diese Prozesse vom Monitoring ausgeschlossen werden sollen. **Hinweis** Prozesse, die von Microsoft signiert wurden, werden immer als vertrauenswürdig eingestuft. Wenn Sie beispielsweise den Pfad 'C:\Users\user1\application\nppInstaller.exe' hinzufügen, wird dieser spezielle Prozess vom Monitoring ausgeschlossen, sodass die Antivirus-Funktion nicht mehr mit diesem Prozess interferiert.
Datei/Ordner		Wenn eine Datei oder ein Ordner in die vertrauenswürdige Liste aufgenommen wird, weiß das System, dass diese Dateien oder Ordner immer als sicher eingestuft werden sollen und nicht gescannt/überwacht werden müssen.

So können Sie die Elemente spezifizieren, die dauerhaft als vertrauenswürdig eingestuft werden sollen

1. Öffnen Sie den Schutzplan.
2. Erweitern Sie das Modul **Antivirus & Antimalware Protection**.
3. Wählen Sie die Option **Ausschlüsse** aus.
   Das Fenster **Schutz-Ausschlüsse** wird geöffnet.
4. Klicken Sie im Bereich **Vertrauenswürdige Elemente** auf **Hinzufügen**, um aus den verfügbaren Optionen auswählen zu können:

- Wenn Sie Dateien, Ordner oder Prozesse als vertrauenswürdig einstufen wollen, wählen Sie die Option **Datei/Ordner/Prozess**. Das Fenster **Datei/Ordner/Prozess hinzufügen** wird geöffnet.
  - Geben Sie im Feld **Datei/Ordner/Prozess** den Pfad für jede(n) Prozess, Order oder Datei in einer neuen Zeile ein. Geben Sie im Abschnitt **Beschreibung** eine kurze Erläuterung ein, damit Sie Ihre Änderung in der Liste der vertrauenswürdigen Elemente erkennen können.
  - Aktivieren Sie das Kontrollkästchen **Als Datei/Ordner hinzufügen**, um die Datei/den Ordner als vertrauenswürdig einzustufen.
    Beispiele für eine Ordnerbeschreibung: D:\Ordner\, /home/Ordner/Ordner2, F:\
  - Wählen Sie das Kontrollkästchen **Als Prozess hinzufügen**, um einen Prozess als vertrauenswürdig einzustufen. Die ausgewählten Prozesse werden vom Monitoring ausgeschlossen.

    Hinweis
    Spezifizieren Sie den vollständigen Pfad zur ausführbaren Datei des Prozesses (mit dem Laufwerksbuchstaben beginnend). Beispielsweise `C:\Windows\Temp\er76s7sdkh.exe`.

    Hinweis
    Es werden lokale Netzwerkpfade unterstützt, wie beispielsweise: \\localhost\ordnerpfad\datei.exe

- Wählen Sie die Option **Hash**, um MD5-Hash-Werte in die Liste der vertrauenswürdigen Elemente aufzunehmen. Daraufhin wird das Fenster **Hash hinzufügen** geöffnet.
  - Hier können Sie die MD5-Hashes als separate Zeilen einfügen, damit sie als vertrauenswürdig eingestuft in die Liste der Schutzausschlüsse aufgenommen werden. Auf der Grundlage dieser Hash-Werte wird Cyber Protection diejenigen Prozesse vom Monitoring ausschließen, die durch die MD5-Hash-Werte charakterisiert wurden.

Standardeinstellung: Standardmäßig sind keine Ausnahmen definiert.

So können Sie die Elemente spezifizieren, die dauerhaft geblockt werden sollen

1. Öffnen Sie den Schutzplan.
2. Erweitern Sie das Modul **Antivirus & Antimalware Protection**.
3. Wählen Sie die Option **Schutz-Ausschlüsse** aus. Das Fenster **Schutz-Ausschlüsse** wird geöffnet.

   Klicken Sie im Bereich **Blockierte Elemente** auf **Hinzufügen**, um aus den verfügbaren Optionen auswählen zu können:
   - Wenn Sie Prozesse blockieren wollen, müssen Sie die Option **Prozess** auswählen. Daraufhin wird das Fenster **Prozess hinzufügen** geöffnet.
     - Geben Sie im Feld **Prozess** den Pfad für jeden Prozess in einer neuen Zeile ein. Geben Sie in das Feld **Beschreibung** eine kurze Erläuterung ein, damit Sie Ihre Änderung in der Liste der blockierten Elemente erkennen können.

Hinweis
Solange Active Protection auf der Maschine aktiviert ist, können diese Prozesse nicht gestartet werden.

- Wenn Sie Hash-Werte blockieren wollen, müssen Sie die Option **Hash** auswählen. Das Fenster **Hash hinzufügen** wird angezeigt.
  - Geben Sie im Feld **Hash** den Hash-Wert für jeden Prozess in einer neuen Zeile ein. Geben Sie in das Feld **Beschreibung** eine kurze Erläuterung ein, damit Sie Ihre Änderung in der Liste der blockierten Elemente erkennen können.

Standardeinstellung: Standardmäßig sind keine Ausnahmen definiert.

Platzhalterzeichen

Sie können Platzhalterzeichen (* und ?) verwenden, um die Ordner zu spezifizieren. Der Asterisk (*) ersetzt null bis mehrere Zeichen. Das Fragezeichen (?) steht für exakt ein Zeichen. Umgebungsvariablen (wie etwa `%AppData%`) können nicht verwendet werden.

Sie können auch ein Platzhalterzeichen (*) verwenden, um Elemente zu den Ausschlusslisten hinzuzufügen.

- Platzhalterzeichen können in der Mitte oder am Ende einer Beschreibung verwendet werden.

Beispiele für Platzhalterzeichen, die in Beschreibungen akzeptiert werden:

C:*.pdf

D:\Ordner\Datei.*

C:\Benutzer*\AppData\Roaming

- Platzhalterzeichen können nicht am Anfang einer Beschreibung verwendet werden.

Beispiele für Platzhalterzeichen, die in Beschreibungen nicht akzeptiert werden:

*.docx

*:\Ordner\

Variablen

Sie können auch Variablen verwenden, um Elemente zur Liste der Schutzausschlüsse hinzuzufügen – allerdings mit folgenden Einschränkungen:

- Unter Windows werden nur SYSTEM-Variablen unterstützt. Benutzerspezifische Variablen (wie beispielsweise %USERNAME%, %APPDATA%) werden nicht unterstützt. Variablen mit {Benutzername} werden nicht unterstützt. Weitere Informationen finden Sie auf dieser Seite: https://ss64.com/nt/syntax-variables.html.
- Unter macOS werden keine Umgebungsvariablen unterstützt.
- Unter Linux werden keine Umgebungsvariablen unterstützt.

Beispiele für unterstützte Formate:

- %WINDIR%\Media
- %public%
- %CommonProgramFiles%\Acronis\

Beschreibung

Sie können das Feld **Beschreibung** verwenden, um sich Notizen über die Ausschlüsse zu machen, die Sie in die Liste der Schutzausschlüsse aufgenommen haben. Hier sind einige Vorschläge für Notizen, die Sie machen können:

- Gründe und Zwecke für den Ausschluss.
- Der tatsächliche Dateiname eines Hash-Ausschlusses.
- Zeitstempel.

Wenn mehrere Elemente als ein einzelner Eintrag hinzugefügt werden, kann nur ein (1) Kommentar für diese mehrfachen Elemente erfasst werden.

Active Protection in der Cyber Backup Standard-Editionen

In Cyber Backup Standard-Edition ist die Active Protection-Funktionalität ein separates Modul innerhalb eines Schutzplans. So kann sie separat konfiguriert und auf verschiedene Geräte oder Geräte-Gruppen angewendet werden.

In allen anderen Editionen des Cyber Protection Service ist die Active Protection-Funktionalität Bestandteil des **Antivirus & Antimalware**-Moduls im Schutzplan.

Standardeinstellung: **Aktiviert**.

Hinweis
Auf der zu schützenden Maschine muss ein Protection Agent installiert sein. Für weitere Informationen über die unterstützten Betriebssysteme und Funktionen finden Sie im Abschnitt '"Unterstützte Plattformen" (S. 896)'.

Und so funktioniert es

Active Protection überwacht die auf der geschützten Maschine laufenden Prozesse in Echtzeit. Wenn ein fremder Prozess versucht, Dateien auf der Maschine zu verschlüsseln oder eine digitale Crypto-Währung zu berechnen („schürfen“), generiert Active Protection eine Alarmmeldung und führt bestimmte, weitere Aktionen aus (wie im Schutzplan spezifiziert).

Zusätzlich verhindert die Selbstschutzfunktion (Self-Protection), dass die Prozesse, Registry-Einträge, ausführbaren Dateien und Konfigurationsdateien der Backup-Software selbst sowie vorhandene Backups, die in lokalen Ordnern gespeichert sind, verändert werden können.

Active Protection verwendet eine verhaltensbasierte Heuristik, um bösartige Prozesse zu erkennen. Dazu vergleicht Active Protection die von einem Prozess ausgeführten Aktionsketten (z.B. Ereignisse im Dateisystem) mit Aktionsketten, die in einer Referenzdatenbank mit bekannten schädlichen Verhaltensmustern gespeichert sind. Mit diesem Ansatz kann Active Protection auch neue (bisher unbekannte) Malware anhand typischer Verhaltensmuster als Schadsoftware erkennen.

Active Protection-Einstellungen in Cyber Backup Standard

In der Cyber Backup Standard-Editionen können Sie folgende Active Protection-Funktionen konfigurieren:

- Aktion bei Erkennung
- Selbstschutz
- Netzwerkordnerschutz
- Serverseitiger Schutz
- Erkennung von Cryptomining-Prozessen
- Ausschlüsse

Hinweis
Active Protection für Linux unterstützt folgende Einstellungen: Aktion bei Erkennung, Netzwerkordnerschutz und Ausschlüsse. Der Netzwerkordnerschutz ist immer eingeschaltet und kann nicht konfiguriert werden.

Aktion bei Erkennung

Wählen Sie im Bereich **Aktion bei Erkennung** eine der verfügbaren Optionen:

- **Nur benachrichtigen**
  Die Software wird einen Alarm generieren, wenn ein Prozess eine mögliche Ransomware-Aktivität zeigt.
- **Den Prozess stoppen**
  Die Software wird einen Alarm generieren und den Prozess stoppen, der eine mögliche Ransomware-Aktivität zeigt.
- **Aus Cache wiederherstellen**
  Die Software erstellt eine Alarmmeldung, stoppt den Prozess und setzt die erfolgten Dateiänderungen mithilfe des Service-Caches zurück.

Standardeinstellung: **Aus Cache wiederherstellen**.

Der Selbstschutz (Self-Protection) verhindert, dass die Prozesse, Registry-Einträge, ausführbaren Dateien und Konfigurationsdateien der Backup-Software selbst sowie Backups, die in Ihren lokalen Ordnern gespeichert sind, verändert werden können.

Administratoren können den **Selbstschutz** aktivieren, ohne die **Active Protection**-Funktionalität zu aktivieren.

Standardeinstellung: **An**.

Hinweis
Die Selbstschutzfunktion wird für Linux nicht unterstützt.

So können Sie den Selbstschutz aktivieren

1. Erweitern Sie im Fenster **Schutzplan erstellen** das Modul **Antivirus & Antimalware Protection**.
2. Klicken Sie auf **Selbstschutz**.
3. Verwenden Sie den Schalter **Selbstschutz**, um ihn zu aktivieren.

So können Sie den Kennwortschutz aktivieren

1. Sobald die **Selbstschutz**-Funktion aktiviert ist, können Sie auch die Funktion **Kennwortschutz** über den entsprechenden Schalter aktivieren.
2. Klicken Sie auf **Neues Kennwort generieren**, um ein Kennwort zu generieren, mit dem lokale Agenten geändert oder gelöscht werden können.
3. Klicken Sie auf **Kopieren** und fügen Sie es an einem sicheren Speicherort ein. Denn das Kennwort wird abgefragt, wenn Sie die Komponentenliste lokal ändern wollen.

   Wichtig
   Das Kennwort wird nicht mehr verfügbar sein, wenn Sie das Fenster schließen. Damit dieses Kennwort auf Geräte angewendet werden kann, müssen die Einstellungen des Schutzplans gespeichert werden.

4. Klicken Sie auf **Schließen**.

Der **Kennwortschutz** verhindert, dass unbefugte Benutzer oder Programme den Agenten für Windows deinstallieren oder dessen Komponenten ändern können. Diese Aktionen sind folglich nur noch mit dem passenden Kennwort möglich, welches ein Administrator bereitstellen kann.

Für folgende Aktionen ist niemals ein Kennwort erforderlich:

- Die Installation durch lokales Ausführen des Setup-Programms aktualisieren
- Die Installation mithilfe der Cyber Protect-Konsole aktualisieren
- Die Installation reparieren

Standardeinstellung: **Deaktiviert**

Weitere Informationen zur Aktivierung des **Kennwortschutzes** finden Sie im Abschnitt 'Unbefugte Deinstallationen oder Änderungen der Agenten verhindern'.

Netzwerkordnerschutz

Die Einstellung **Als lokale Laufwerke zugeordnete Netzwerkordner schützen** bestimmt, ob die Active Protection-Funktion auch Netzwerkordner, die als lokale Laufwerke gemounted wurden, vor

lokalen Schadprozessen schützen soll.

Diese Einstellung gilt für Ordner, die per SMB- oder NFS-Protokoll freigegeben/zugeordnet wurden.

Wenn sich eine Datei ursprünglich auf einem solchen Netzlaufwerk befand, kann diese nicht an ihrem ursprünglichen Speicherort wiederhergestellt werden, wenn die Datei aufgrund des Befehls **Aus Cache wiederherstellen** aus dem Cache extrahiert wird. Stattdessen wird die Datei aus dem Cache in demjenigen Ordner wiederhergestellt, der in dieser Einstellung spezifiziert wurde. Der Standardordner für Windows lautet `C:\ProgramData\Acronis\Restored Network Files` und für macOS `Library/Application Support/Acronis/Restored Network Files/`. Falls es diesen Ordner nicht gibt, wird er automatisch erstellt. Wenn Sie diesen Pfad ändern wollen, müssen Sie einen lokalen Ordner spezifizieren. Netzwerkordner werden nicht unterstützt (gilt auch für Ordner von Netzwerklaufwerken)

Standardeinstellung: **An**.

Diese Funktion schützt Netzwerkordner, die Sie freigegeben haben, per Active Protection vor potentiellen Bedrohungen, die über externe Verbindungen (also von anderen Servern im Netzwerk) hereinkommen können.

Standardeinstellung: **Aus**.

Hinweis
Der serverseitige Schutz wird für Linux nicht unterstützt.

So können Sie vertrauenswürdige Verbindungen festlegen

1. Erweitern Sie im Fenster **Schutzplan erstellen** das Modul **Antivirus & Antimalware Protection**.
2. Klicken Sie auf **Serverseitiger Schutz**.
3. Verwenden Sie den Schalter **Serverseitiger Schutz**, um ihn zu aktivieren.
4. Wählen Sie die Registerlasche '**Vertrauenswürdig**'.
5. Klicken Sie im Feld **Vertrauenswürdige Verbindungen** auf **Hinzufügen**, um die Verbindungen zu definieren, wo Datenänderungen erlaubt sein sollen.
6. Geben Sie im Feld **ComputerName/Konto** den Namen des Computers sowie das Konto der Maschine ein, auf welcher der Protection Agent installiert ist. Beispielsweise: `MeinComputer\TestBenutzer`.
7. Geben Sie im Feld **Host-Name** den Host-Namen der Maschine ein, die über den Protection Agenten eine Verbindung zur Maschine herstellen darf.
8. Klicken Sie auf das Häkchensymbol rechts daneben, um die Verbindungsdefinition zu speichern.
9. Klicken Sie auf **Fertig**.

So können Sie blockierte Verbindungen festlegen

1. Erweitern Sie im Fenster **Schutzplan erstellen** das Modul **Antivirus & Antimalware Protection**.
2. Klicken Sie auf **Serverseitiger Schutz**.
3. Verwenden Sie den Schalter **Serverseitiger Schutz**, um ihn zu aktivieren.
4. Wählen Sie die Registerkarte **Blockiert**.
5. Klicken Sie im Feld **Blockierte Verbindungen** auf **Hinzufügen**, um die Verbindungen zu definieren, wo keine Datenänderungen erlaubt sind.
6. Geben Sie im Feld **ComputerName/Konto** den Namen des Computers sowie das Konto der Maschine ein, auf welcher der Protection Agent installiert ist. Beispielsweise: `MeinComputer\TestBenutzer`.
7. Geben Sie im Feld **Host-Name** den Host-Namen der Maschine ein, die über den Protection Agenten eine Verbindung zur Maschine herstellen darf.
8. Aktivieren Sie das Kontrollkästchen rechts daneben, um die Verbindungsdefinition zu speichern.
9. Klicken Sie auf **Fertig**.

Cryptomining-Malware kann die Performance nützlicher Applikationen beeinträchtigen, die Stromrechnung erhöhen, Systemabstürze oder sogar Hardware-Schäden (durch übermäßige Nutzung) verursachen. Die Funktion **Erkennung von Cryptomining-Prozessen** schützt Ihre Geräte vor Cryptomining-Malware, um die unberechtigte Nutzung von Computer-Ressourcen zu verhindern.

Administratoren können die **Erkennung von Cryptomining-Prozessen** aktivieren, ohne die **Active Protection**-Funktionalität zu aktivieren. Standardeinstellung: **Aktiviert**.

Hinweis
Die Erkennung von Cryptomining-Prozessen wird für Linux nicht unterstützt.

So können Sie den Netzwerkordnerschutz konfigurieren

1. Erweitern Sie im Fenster **Schutzplan erstellen** das Modul **Antivirus & Antimalware Protection**.
2. Klicken Sie auf **Erkennung von Cryptomining-Prozessen**.
3. Verwenden Sie den Schalter **Cryptomining-Prozesse erkennen**, um die Funktion zu aktivieren oder zu deaktivieren.
4. Bestimmen Sie, was mit Prozessen geschehen soll, bei denen der Verdacht auf Cryptomining-Aktivitäten besteht:
   Standardeinstellung: **Den Prozess stoppen**
   - **Nur benachrichtigen** – Die Software wird einen Alarm generieren.

- **Den Prozess stoppen** – Die Software wird einen Alarm generieren und den Prozess stoppen.

5. Klicken Sie auf **Fertig**, um die ausgewählten Optionen auf Ihren Schutzplan anzuwenden.

Mit Schutz-Ausschlüssen können Sie Falsch-Positiv-Erkennungen vermeiden, wenn ein vertrauenswürdiges Programm fälschlicherweise als Ransomware oder Malware eingestuft werden sollte. Sie können vertrauenswürdige und blockierte Elemente definieren, indem Sie sie in die Liste der Schutz-Ausschlüsse aufnehmen.

In die Liste der vertrauenswürdigen Elemente können Sie Dateien, Prozesse oder Ordner aufnehmen, um diese im System als sicher einzustufen und zu verhindern, dass sie zukünftig noch mal als falsch-positiv erkannt werden.

In die Liste der blockierten Elemente können Sie Prozesse und Hash-Werte aufnehmen. Diese Option gewährleistet, dass diese Prozesse blockiert werden und Ihr Workload abgesichert ist.

Schutz-Ausschlusselement	Blockiert	Vertrauenswürdig
Hash	Wenn ein Hash-Wert in die Blockliste aufgenommen wird, stoppt das System den Prozess auf der Grundlage des angegebenen Hash-Wertes. Wenn Sie beispielsweise den MD5-Hash-Wert '938c2cc0dcc05f2b68c4287040cfcf71' hinzufügen, wird der mit diesem Hash-Wert assoziierte Prozess blockiert.	Wenn ein Hash-Wert in die vertrauenswürdige Liste aufgenommen wird, weiß das System anhand des bereitgestellten Hash-Wertes, welche Prozesse beim Monitoring ignoriert werden sollen. Wenn Sie beispielsweise den MD5-Hash-Wert '938c2cc0dcc05f2b68c4287040cfcf71' hinzufügen, wird der mit diesem Hash-Wert assoziierte Prozess als vertrauenswürdig eingestuft und vom Monitoring ausgeschlossen.
Prozess	Wenn ein Prozess in die Blockliste aufgenommen wird, weiß das System, dass diese Prozesse überwacht werden sollen, und die Prozesse werden dauerhaft blockiert. Wenn Sie beispielsweise den Pfad 'C:\Users\user1\application\nppInstaller.exe' zur Blockliste hinzufügen, wird dieser spezielle Prozess blockiert. Wenn Sie dennoch versuchen, ihn zu öffnen, wird sein Start nicht zugelassen.	Wenn ein Prozess in die vertrauenswürdige Liste aufgenommen wird, weiß das System, dass diese Prozesse vom Monitoring ausgeschlossen werden sollen. **Hinweis** Prozesse, die von Microsoft signiert wurden, werden immer als vertrauenswürdig eingestuft. Wenn Sie beispielsweise den Pfad 'C:\Users\user1\application\nppInst

Schutz-Ausschlusselement	Blockiert	Vertrauenswürdig
		aller.exe' hinzufügen, wird dieser spezielle Prozess vom Monitoring ausgeschlossen, sodass die Antivirus-Funktion nicht mehr mit diesem Prozess interferiert.
Datei/Ordner		Wenn eine Datei oder ein Ordner in die vertrauenswürdige Liste aufgenommen wird, weiß das System, dass diese Dateien oder Ordner immer als sicher eingestuft werden sollen und nicht gescannt/überwacht werden müssen.

So können Sie die Elemente spezifizieren, die dauerhaft als vertrauenswürdig eingestuft werden sollen

1. Öffnen Sie den Schutzplan.
2. Erweitern Sie das Modul **Antivirus & Antimalware Protection**.
3. Wählen Sie die Option **Ausschlüsse** aus.
   Das Fenster **Schutz-Ausschlüsse** wird geöffnet.
4. Klicken Sie im Bereich **Vertrauenswürdige Elemente** auf **Hinzufügen**, um aus den verfügbaren Optionen auswählen zu können:
   - Wenn Sie Dateien, Ordner oder Prozesse als vertrauenswürdig einstufen wollen, wählen Sie die Option **Datei/Ordner/Prozess**. Das Fenster **Datei/Ordner/Prozess hinzufügen** wird geöffnet.
     - Geben Sie im Feld **Datei/Ordner/Prozess** den Pfad für jede(n) Prozess, Order oder Datei in einer neuen Zeile ein. Geben Sie im Abschnitt **Beschreibung** eine kurze Erläuterung ein, damit Sie Ihre Änderung in der Liste der vertrauenswürdigen Elemente erkennen können.
     - Aktivieren Sie das Kontrollkästchen **Als Datei/Ordner hinzufügen**, um die Datei/den Ordner als vertrauenswürdig einzustufen.
       Beispiele für eine Ordnerbeschreibung: D:\Ordner\, /home/Ordner/Ordner2, F:\
     - Wählen Sie das Kontrollkästchen **Als Prozess hinzufügen**, um einen Prozess als vertrauenswürdig einzustufen. Die ausgewählten Prozesse werden vom Monitoring ausgeschlossen.

     Hinweis
     Spezifizieren Sie den vollständigen Pfad zur ausführbaren Datei des Prozesses (mit dem Laufwerksbuchstaben beginnend). Beispielsweise `C:\Windows\Temp\er76s7sdkh.exe`.

Hinweis
Es werden lokale Netzwerkpfade unterstützt, wie beispielsweise: \\localhost\ordnerpfad\datei.exe

- Wählen Sie die Option **Hash**, um MD5-Hash-Werte in die Liste der vertrauenswürdigen Elemente aufzunehmen. Daraufhin wird das Fenster **Hash hinzufügen** geöffnet.
  - Hier können Sie die MD5-Hashes als separate Zeilen einfügen, damit sie als vertrauenswürdig eingestuft in die Liste der Schutzausschlüsse aufgenommen werden. Auf der Grundlage dieser Hash-Werte wird Cyber Protection diejenigen Prozesse vom Monitoring ausschließen, die durch die MD5-Hash-Werte charakterisiert wurden.

Standardeinstellung: Standardmäßig sind keine Ausnahmen definiert.

So können Sie die Elemente spezifizieren, die dauerhaft geblockt werden sollen

1. Öffnen Sie den Schutzplan.
2. Erweitern Sie das Modul **Antivirus & Antimalware Protection**.
3. Wählen Sie die Option **Schutz-Ausschlüsse** aus. Das Fenster **Schutz-Ausschlüsse** wird geöffnet.

   Klicken Sie im Bereich **Blockierte Elemente** auf **Hinzufügen**, um aus den verfügbaren Optionen auswählen zu können:
   - Wenn Sie Prozesse blockieren wollen, müssen Sie die Option **Prozess** auswählen. Daraufhin wird das Fenster **Prozess hinzufügen** geöffnet.
     - Geben Sie im Feld **Prozess** den Pfad für jeden Prozess in einer neuen Zeile ein. Geben Sie in das Feld **Beschreibung** eine kurze Erläuterung ein, damit Sie Ihre Änderung in der Liste der blockierten Elemente erkennen können.

     Hinweis
     Solange Active Protection auf der Maschine aktiviert ist, können diese Prozesse nicht gestartet werden.

   - Wenn Sie Hash-Werte blockieren wollen, müssen Sie die Option **Hash** auswählen. Das Fenster **Hash hinzufügen** wird angezeigt.
     - Geben Sie im Feld **Hash** den Hash-Wert für jeden Prozess in einer neuen Zeile ein. Geben Sie in das Feld **Beschreibung** eine kurze Erläuterung ein, damit Sie Ihre Änderung in der Liste der blockierten Elemente erkennen können.

Standardeinstellung: Standardmäßig sind keine Ausnahmen definiert.

Platzhalterzeichen

Sie können Platzhalterzeichen (* und ?) verwenden, um die Ordner zu spezifizieren. Der Asterisk (*) ersetzt null bis mehrere Zeichen. Das Fragezeichen (?) steht für exakt ein Zeichen. Umgebungsvariablen (wie etwa `%AppData%`) können nicht verwendet werden.

Sie können auch ein Platzhalterzeichen (*) verwenden, um Elemente zu den Ausschlusslisten hinzuzufügen.

- Platzhalterzeichen können in der Mitte oder am Ende einer Beschreibung verwendet werden.

Beispiele für Platzhalterzeichen, die in Beschreibungen akzeptiert werden:

C:*.pdf

D:\Ordner\Datei.*

C:\Benutzer*\AppData\Roaming

- Platzhalterzeichen können nicht am Anfang einer Beschreibung verwendet werden.

Beispiele für Platzhalterzeichen, die in Beschreibungen nicht akzeptiert werden:

*.docx

*:\Ordner\

Variablen

Sie können auch Variablen verwenden, um Elemente zur Liste der Schutzausschlüsse hinzuzufügen – allerdings mit folgenden Einschränkungen:

- Unter Windows werden nur SYSTEM-Variablen unterstützt. Benutzerspezifische Variablen (wie beispielsweise %USERNAME%, %APPDATA%) werden nicht unterstützt. Variablen mit {Benutzername} werden nicht unterstützt. Weitere Informationen finden Sie auf dieser Seite: https://ss64.com/nt/syntax-variables.html.
- Unter macOS werden keine Umgebungsvariablen unterstützt.
- Unter Linux werden keine Umgebungsvariablen unterstützt.

Beispiele für unterstützte Formate:

- %WINDIR%\Media
- %public%
- %CommonProgramFiles%\Acronis\

Beschreibung

Sie können das Feld **Beschreibung** verwenden, um sich Notizen über die Ausschlüsse zu machen, die Sie in die Liste der Schutzausschlüsse aufgenommen haben. Hier sind einige Vorschläge für Notizen, die Sie machen können:

- Gründe und Zwecke für den Ausschluss.
- Der tatsächliche Dateiname eines Hash-Ausschlusses.
- Zeitstempel.

Wenn mehrere Elemente als ein einzelner Eintrag hinzugefügt werden, kann nur ein (1) Kommentar für diese mehrfachen Elemente erfasst werden.

URL-Filterung

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Malware wird häufig über bösartige oder infizierte Websites verbreitet und verwendet dafür eine Angriffsmethode, die Drive-by-Download-Infektion genannt wird.

Mit der Funktionalität 'URL-Filterung' können Sie Maschinen vor Bedrohungen wie Malware und Phishing schützen, die aus dem Internet kommen. Sie können Ihr Unternehmen schützen, indem Sie Benutzerzugriffe auf bestimmte Websites blockieren, die bösartige/schädliche Inhalte haben können.

Sie können mit der URL-Filterung auch die Nutzung des Webs (WWWs) kontrollieren, um beispielsweise externe Vorschriften (wie gesetzliche Bestimmungen) oder interne Unternehmensrichtlinien einzuhalten. Sie können den Zugriff auf die Websites nach Kategorien konfigurieren, in die sich die Websiten einordnen lassen. Die URL-Filterung unterstützt derzeit 44 Website-Kategorien und ermöglicht es über diese, den Zugriff auf die Websites zu verwalten.

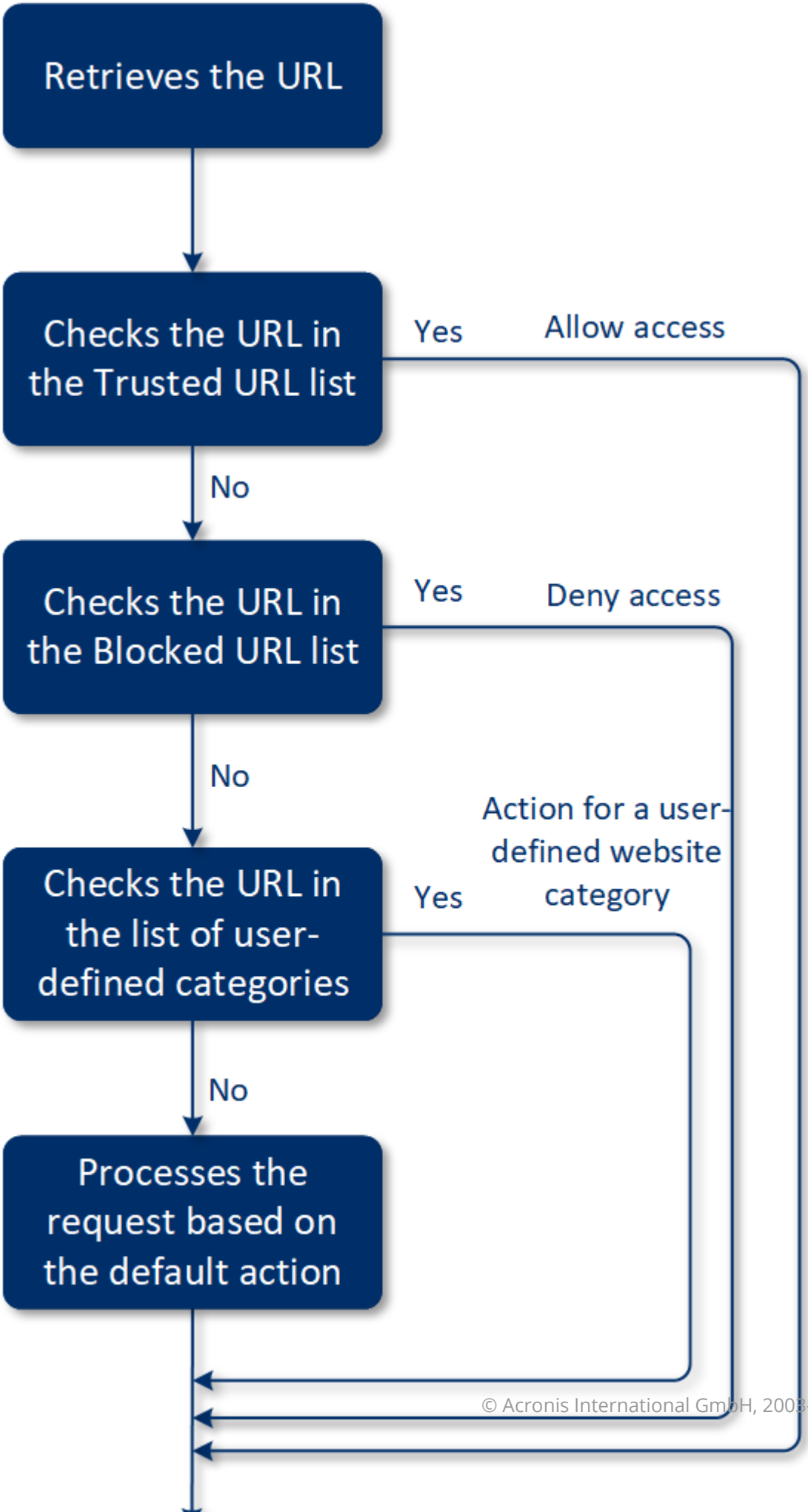
Derzeit werden nur HTTP/HTTPS-Verbindungen auf Windows-Maschinen vom entsprechenden Protection Agenten überprüft.

Für die URL-Filterungsfunktion ist eine Internetverbindung erforderlich.

Hinweis
Um mögliche Kompatibilitätsprobleme mit Protection Agenten mit der Build-Version 15.0.26692 (Release C21.03 HF1) und niedriger zu vermeiden, wird die Funktionalität der URL-Filterung automatisch deaktiviert, wenn eine andere Antivirus-Lösung erkannt wird oder wenn der Windows Security Center Service nicht auf dem System vorhanden ist.
Bei späteren Protection Agenten wurden die Kompatibilitätsprobleme behoben, sodass die URL-Filterung immer gemäß der Richtlinie aktiviert ist.

Und so funktioniert es

Ein Benutzer gibt einen URL-Link in einen Webbrowser ein. Der sogenannte Interceptor erhält den Link und sendet diesen an den Protection Agenten. Der Agent erhält die URL, analysiert sie und überprüft deren Bewertung. Der Interceptor leitet den Benutzer bei Bedarf auf eine Seite um, die eine Nachricht mit verfügbaren Aktionen anzeigt. Von dort kann er manuell zur angeforderten Seite weitergehen.

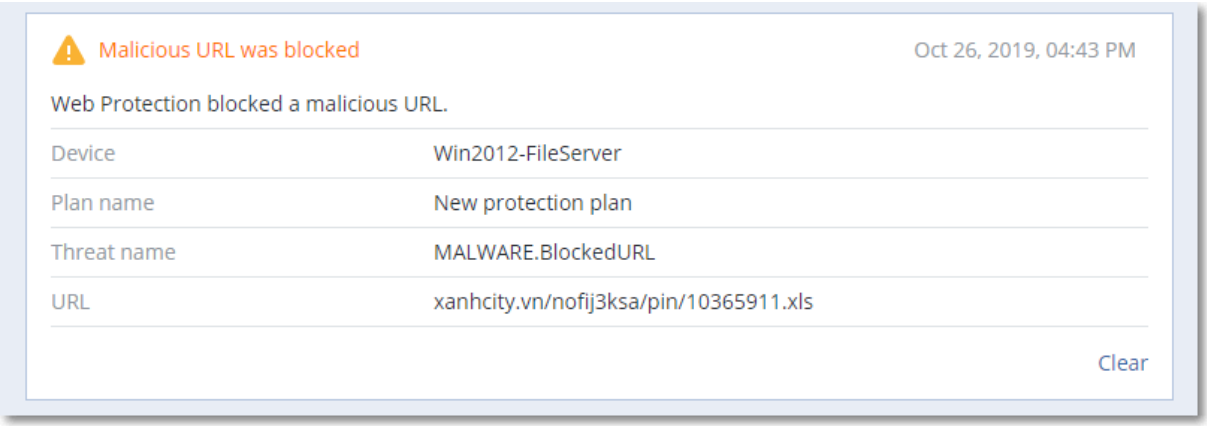


Die Konfiguration der URL-Filterung

Die Konfiguration der URL-Filterung besteht grundsätzlich aus den folgenden Schritten:

1. Sie erstellen einen Schutzplan, in dem Sie das Modul **URL-Filterung** aktivieren.
2. Sie spezifizieren die URL-Filter-Einstellungen (siehe unten).
3. Sie weisen den Maschinen den Schutzplan zu.

Wenn Sie überprüfen wollen, welche URLs geblockt wurden, gehen Sie zu **Monitoring** –> **Alarmmeldungen**.



URL-Filter-Einstellungen

Für das Modul 'URL-Filterung' können folgende Einstellungen spezifiziert werden:

Zugriff auf schädliche Website

Spezifizieren Sie, welche Aktionen ausgeführt werden, wenn ein Benutzer eine bösartige Website öffnet:

- **Nur benachrichtigen** – die Software generiert einen Alarm, wenn ein Prozess eine mögliche Ransomware-Aktivität zeigt.
- **Blockieren** – der Zugriff auf die bösartige Website wird blockiert. Der Benutzer wird nicht auf die Website zugreifen können und es wird eine Alarmmeldung generiert.
- **Immer den Benutzer fragen** – der Benutzer wird gefragt, ob die Website dennoch aufgerufen werden soll oder er zurückgehen will.

Zu filternde Kategorien

Es gibt 44 Website-Kategorien, für die Sie den Zugriff konfigurieren können:

- **Erlauben** – ermöglicht den Zugriff auf Websites, die der ausgewählten Kategorie entsprechen.
- **Verweigern** – blockiert den Zugriff auf Websites, die der ausgewählten Kategorie entsprechen.

Standardmäßig sind alle Kategorien erlaubt.

Alle Benachrichtigungen für blockierte URLs nach Kategorien anzeigen – wenn diese Option aktiviert ist, werden alle Benachrichtigungen für blockierte URLs, die in der Taskleiste angezeigt werden, nach Kategorien gruppiert. Wenn eine Website mehrere Subdomains hat, generiert das System auch Benachrichtigungen für diese Subdomains. Daher kann die Anzahl der Benachrichtigungen recht groß werden.

In der nachfolgenden Tabelle finden Sie Beschreibungen zu den Kategorien:

	Website-Kategorie	Beschreibung
1	**Werbung**	Diese Kategorie umfasst Domains, die hauptsächlich der Bereitstellung von Werbeanzeigen dienen.
2	**Message-Boards**	Diese Kategorie umfasst Foren, Diskussionsforen und Frage-Antwort-Portale. Diese Kategorie umfasst keine spezifischen Bereiche auf Unternehmens-Websites, in denen Kunden Fragen stellen.
3	**Persönliche Websites**	Diese Kategorie umfasst persönliche Websites und alle Arten von Blogs: von Einzelpersonen, Gruppen oder sogar Unternehmen. Ein Blog ist eine Art Journal, Magazin oder Tagebuch, das im World Wide Web veröffentlicht wird. Ein Blog besteht aus Beiträgen („Posts“), die in der Regel in umgekehrter chronologischer Reihenfolge angezeigt werden, sodass neuere (jüngere) Beiträge zuerst erscheinen.
4	**Unternehmens-Websites**	Dies ist eine umfangreiche Kategorie, die all die Unternehmens-Websites umfasst, die sich normalerweise in keine andere Kategorie einordnen lassen.
5	**Computer-Software**	Diese Kategorie umfasst Websites, die Computer-Software anbieten (in der Regel als Open Source, Freeware oder Shareware). Sie kann auch einige Online-Shops für Software umfassen.
6	**Arzneimittel**	Diese Kategorie umfasst Websites, die sich auf Medikamente/Alkohol/Tabakwaren beziehen und Diskussionen über den Gebrauch bzw. Verkauf von (legalen) Medikamenten, Drogen, Drogenutensilien, Alkohol oder Tabakwaren enthalten. Beachten Sie, dass illegale Drogen in der Kategorie Betäubungsmittel erfasst werden.
7	**Bildung**	Diese Kategorie umfasst Websites, die zu offiziellen Bildungseinrichtungen gehören (auch solche, die außerhalb der .edu-Domain liegen). Sie umfasst auch Websites, die der Bildung dienen (wie beispielsweise Enzyklopädien/Lexika).
8	**Unterhaltung**	Diese Kategorie umfasst Websites, die Informationen zu künstlerischen Aktivitäten und Museen bieten, sowie Websites, die Inhalte wie Filme, Musik oder Kunst bewerten bzw. besprechen.
9	**File-Sharing**	Diese Kategorie umfasst File-Sharing-Websites (auch Tauschbörsen genannt), auf denen Benutzer also Dateien hochladen und mit anderen

		teilen können. Dazu gehören auch sogenannte Torrent-File-Sharing-Websites und Torrent-Tracker.
10	**Finanzen**	Diese Kategorie umfasst Websites, die zu weltweit online zugänglichen Banken gehören. Dazu gehören auch bestimmte Kreditgenossenschaften und andere Finanzinstitute. Einige lokale Banken können jedoch unberücksichtigt bleiben.
11	**Glücksspiel**	Diese Kategorie umfasst Glücksspiel-Websites. Dabei handelt es sich um Websites vom Typ „Online-Casino“ oder „Online-Lotterie“, die normalerweise eine Zahlung verlangen, bevor ein Benutzer in Online-Spielen (wie Roulette, Poker, Blackjack) um/mit Geld spielen kann. Einige davon sind legal (soll heißen: es gibt eine Chance zu gewinnen) und einige betrügerisch (soll heißen: es gibt keine Chance zu gewinnen). Sie erkennt auch Websites vom Typ „Wett- und Schummeltipps“, die Möglichkeiten beschreiben, wie man auf/mit Glücksspiel- und Online-Lotterie-Websites Geld machen kann.
12	**Spiele**	Diese Kategorie umfasst Websites, die Online-Spiele („Games“) anbieten – meist auf der Basis von Adobe Flash oder Java-Applets. Für die Erkennung spielt es keine Rolle, ob das jeweilige Spiel kostenlos ist oder ein Abonnement erfordert. Websites vom Typ „Online-Casino“ werden dagegen über die Kategorie Glücksspiel erfasst. Folgende Websites werden nicht von dieser Kategorie erfasst: • Offizielle Websites von Unternehmen, die Videospiele/Videogames entwickeln (außer, sie produzieren Online-Spiele) • Diskussions-Websites, auf denen Spiele/Games diskutiert werden • Websites, auf denen Nicht-Online-Spiele heruntergeladen werden können (einige von diesen werden über die die Kategorie „Illegal" erfasst) • Spiele, die vom Benutzer das Herunterladen und Ausführen einer ausführbaren Datei erfordern (wie World of Warcraft); diese können durch andere Mittel (wie Firewalls) verhindert werden
13	**Behörde**	Diese Kategorie umfasst Websites von Behörden wie Regierungsinstitutionen, Botschaften und Stadtverwaltungen.
14	**Hacking**	Diese Kategorie umfasst Websites, die Hacker-Tools, Hacker-Beiträge und Diskussionsplattformen für Hacker bereitstellen. Sie umfasst auch Websites, die Exploits für gängige Plattformen anbieten, die das Hacken von Facebook- oder Gmail-Konten erleichtern.
15	**Illegale Aktivitäten**	Dies ist eine weit gefasste Kategorie, deren Inhalte mit Hass, Gewalt und Rassismus zu tun haben. Sie soll folgende Arten von Websites blockieren: • Websites von terroristischen Organisationen • Websites mit rassistischen oder fremdenfeindlichen Inhalten • Websites, die aggressive Sportarten diskutieren und/oder Gewalt

		befürworten
16	**Gesundheit und Fitness**	Diese Kategorie umfasst Websites, die sich auf medizinische Einrichtungen beziehen, die Prävention/Behandlung von Krankheiten behandeln, Produkte/Informationen zum Abnehmen, zu Diäten, Steroiden, Anabolika oder HGH-Produkten (menschliches Wachstumshormon) anbieten und Websites mit Informationen zur plastischen Chirurgie (Schönheitsoperationen).
17	**Hobbys**	Diese Kategorie umfasst Websites, die Ressourcen/Informationen zu Aktivitäten präsentieren, die Personen typischerweise in ihrer Freizeit ausüben (Sammeln, Kunst, Kunsthandwerk, Radfahren etc.)
18	**Webhosting**	Diese Kategorie umfasst die Websites von kommerziellen und nicht kommerzielle Webhosting-Anbietern, die es Privatanwendern und Unternehmen ermöglichen, Webseiten zu erstellen/veröffentlichen.
19	**Illegale Downloads**	Diese Kategorie umfasst Websites, die im Zusammenhang mit Software-Piraterie stehen – einschließlich: • Peer-to-Peer- und Tracker-Websites (BitTorrent, emule, DC++), die dafür bekannt sind, bei der Verbreitung urheberrechtlich geschützter Inhalte (ohne Zustimmung des Urheberrechtsinhabers) zu helfen • Warez-Websites (für raubkopierte kommerzielle Software) und entsprechende Diskussionsforen • Also Websites, die Benutzern sogenannte Cracks, Schlüsselgeneratoren und Seriennummern bereitstellen, um die illegale Nutzung von Software zu ermöglichen Einige dieser Websites können auch über die Kategorien Pornografie oder Alkohol/Zigarren erkannt werden, da sie häufig entsprechende Werbungen verwenden, um Geld zu verdienen.
20	**Instant Messaging**	Diese Kategorie umfasst Instant Messaging- und Chat-Websites, über die Benutzer in Echtzeit chatten können. Sie erkennt auch „yahoo.com“ und „gmail.com“, weil diese Portale einen eingebetteten Instant Messenger Service enthalten.
21	**Jobs/Anstellung**	Diese Kategorie umfasst Websites, die Jobbörsen, Stellenanzeigen und Informationen zu Karrieremöglichkeiten präsentieren (das umfasst auch die Aggregatoren solcher Dienste/Angebote). Sie umfasst aber weder Personalvermittlungsagenturen noch die „Jobs“-Unterseiten von normalen Unternehmens-Websites.
22	**Anstößige Inhalte**	Diese Kategorie umfasst Inhalte, die der Website-Ersteller mit „für Erwachsene“ gekennzeichnet hat. Sie deckt ein breites Spektrum von Websites ab – vom Kama-Sutra-Buch über Websites zur Sexualerziehung bis hin zu harter Pornografie.
23	**Betäubungsmittel**	Diese Kategorie umfasst Websites, die Informationen über illegale und Freizeit-Drogen bereitstellen. Zu dieser Kategorie gehören auch

		Websites, die sich mit der Entwicklung oder dem Anbau von Drogen befassen.
24	**News**	Diese Kategorie umfasst News-Websites, die Nachrichten in Text- oder Videoform bereitstellen. Sie versucht, globale und lokale News-Websites abzudecken. Einige kleinere Lokalzeitungen werden jedoch möglicherweise nicht abgedeckt.
25	**Online-Dating**	Diese Kategorie umfasst kostenlose oder kommerzielle Online-Dating-Websites, auf denen Benutzer mit bestimmten Kriterien nach Kontakten/Partnern suchen können. Oder die Benutzer stellen eigene Profile von sich ein, um gefunden zu werden. Zu dieser Kategorie gehören kostenlose und zahlungspflichtige Online-Dating-Websites. Weil die meisten populären sozialen Netzwerke (wie Facebook) ebenfalls zum Online-Dating verwendet werden können, werden auch sie über diese Kategorie erfasst. Wir empfehlen, dass Sie diese Kategorie zusammen mit der Kategorie 'Soziale Netzwerke' verwenden.
26	**Online-Zahlungen**	Diese Kategorie umfasst Websites, die Online-Zahlungen oder Geldüberweisungen ermöglichen. Sie erkennt beliebte Online-Zahlungsdienstleister wie PayPal oder Moneybookers. Sie erkennt mit heuristischen Verfahren auch solche Webseiten auf herkömmlichen Websites, die nach Kreditkarteninformationen fragen – und ermöglicht so die Aufdeckung unbekannter, verborgener oder sogar illegaler Online-Shops.
27	**Foto-Sharing**	Diese Kategorie umfasst die Websites von Foto-Sharing-Diensten, die primär das Hochladen und Teilen von Fotos ermöglichen.
28	**Online-Shops**	Diese Kategorie umfasst bekannte Online-Shops. Eine Website wird dann als Online-Shop betrachtet, wenn sie Waren oder Dienstleistungen online verkauft.
29	**Pornografie**	Diese Kategorie umfasst Websites mit erotischen und pornografischen Inhalten. Dazu gehören sowohl kostenlose als auch zahlungspflichtige Websites. Sie umfasst Websites, die Bilder, Geschichten und Videos anbieten – und erfasst auch pornografische Inhalte auf Websites mit gemischten Inhalten.
30	**Portale**	Diese Kategorie umfasst Websites, die Informationen aus vielen Quellen und diversen Domains aggregieren und üblicherweise Funktionen wie eine Suchmaschine, E-Mail-Funktionalität, Nachrichten und Unterhaltungsinformationen bereitstellen.
31	**Radio**	Diese Kategorie umfasst Websites, die Internet-Dienste zum Streamen von Musik anbieten – von Online-Radios bis zu Websites, die (kostenlos oder kommerziell) Audioinhalte auf Abruf anbieten.
32	**Religion**	Diese Kategorie umfasst Websites, die für bestimmte Religionen oder Sekten werben. Dazu gehören auch Diskussionsforen, die sich auf eine

		oder mehrere Religionen beziehen.
33	**Suchmaschinen**	Diese Kategorie umfasst Suchmaschinen-Websites wie Google, Yahoo oder Bing.
34	**Soziale Netzwerke**	Diese Kategorie umfasst Websites vom Typ 'Soziale Netzwerke'. Dazu gehören MySpace.com, Facebook.com, Bebo.com usw. Spezialisierte soziale Netzwerke (wie YouTube.com) werden jedoch in der Kategorie 'Video/Foto' aufgeführt.
35	**Sport**	Diese Kategorie umfasst Websites, die Informationen, Nachrichten und Tutorials zu Sportthemen anbieten.
36	**Selbstmord**	Diese Kategorie umfasst Websites, die Selbstmord befördern, befürworten oder anderweitig Unterstützung dafür anbieten. Nicht eingeschlossen sind Suizid-Präventionskliniken.
37	**Boulevardpresse**	Diese Kategorie ist hauptsächlich für Websites mit sanfter Pornographie sowie Klatsch und Tratsch über Prominente gedacht. Viele Nachrichten-Websites im Stil von Boulevardzeitungen können Unterkategorien haben, die hier aufgeführt sind. Die Erkennung für diese Kategorie basiert ebenfalls auf heuristischen Methoden.
38	**Zeitverschwendung**	Diese Kategorie umfasst Websites, auf denen Personen in der Regel viel Zeit verbringen. Dies kann auch Websites aus anderen Kategorien wie soziale Netzwerke/Social Media oder Unterhaltung umfassen.
39	**Reisen**	Diese Kategorie umfasst Websites, die Reiseangebote und Reiseausrüstungen sowie Besprechungen und Beurteilungen von Reisezielen präsentieren.
40	**Videos**	Diese Kategorie umfasst Websites, die verschiedenste Fotos oder Videos hosten – entweder von Benutzern hochgeladen oder von diversen Inhaltsanbietern bereitgestellt. Dazu gehören Websites wie YouTube, Metacafe, Google Video oder Foto-Websites wie Picasa und Flickr. Diese Kategorie erkannt auch entsprechende Videos, die in anderen Websites oder Blogs eingebettet sind.
41	**Gewalttätige Cartoons**	Diese Kategorie umfasst Websites, die gewalttätige Cartoons oder Mangas diskutieren, teilen und anbieten, die für Minderjährige wegen Gewalt, expliziter Sprache oder sexuellen Inhalten ungeeignet sein können. Diese Kategorie umfasst keine Websites, die Mainstream-Cartoons wie „Tom und Jerry“ anbieten.
42	**Waffen**	Diese Kategorie umfasst Websites, die Waffen zum Verkauf, Tausch, zur Herstellung oder zum Gebrauch anbieten. Dazu gehören auch Jagdrequisiten sowie der Einsatz von Luftpistolen/-gewehre, sogenannte „BB Guns“ oder Nahkampfwaffen.

43	**E-Mail**	Diese Kategorie umfasst Websites, die eine E-Mail-Funktionalität in Form einer Webanwendung bereitstellen.
44	**Webproxy**	Diese Kategorie umfasst Websites, die Webproxy-Dienste bereitstellen. Dies ist eine Website vom Typ „Browser in einem Browser“. Also wenn ein Benutzer eine Webseite öffnet, eine anzufordernde URL in ein Formular eingibt und dann auf 'Senden' klickt. Der Webproxy-Anbieter lädt dann die eigentliche Website herunter und zeigt diese im Browser des Benutzers an. Dieser Website-Typ wird erkannt, weil er für folgende Zwecke verwendet wird (und daher evtl. auch blockiert werden sollte): • Zum anonymen Browsen. Da Anfragen an einen Ziel-Webserver hier vom Proxy-Webserver aus gestellt werden, ist auch nur dessen IP-Adresse sichtbar. Wenn ein Administrator des Ziel-Webservers dann versuchen sollte, den betreffenden Benutzer zurückverfolgen, wird die Rückverfolgung beim Webproxy enden. Es kann dann zwar sein, dass der Webproxy eigene Protokolle führt, die das Ermitteln des tatsächlichen ursprünglichen Benutzers ermöglichen – aber sicher ist dies nicht (oder dass man an diese Protokolle herankommt). • Zum Standort-Spoofing. Die IP-Adressen von Internetnutzern werden häufig dafür verwendet, um Service-Angebote nach dem Herkunftsort des Nutzers zu regeln (beispielsweise, damit Regierungs-Websites nur über inländische IP-Adressen erreichbar sind). Dienstanbieter wie Webproxys können Benutzern daher ermöglichen, ihren wahren Standort zu verschleiern. • Um auf verbotene Inhalte zuzugreifen. Wenn ein einfacher URL-Filter verwendet wird, sieht dieser nur die URLs des Webproxys – und nicht die tatsächlichen Server, die der Benutzer besucht. • Zur Vermeidung einer Unternehmensüberwachung. Eine Unternehmensrichtlinie kann beispielsweise die Überwachung der Internetnutzung durch die Mitarbeiter vorschreiben. Wenn ein Mitarbeiter auf Webinhalte über einen Webproxy zugreift, könnte er die Überwachung aushebeln, weil diese keine korrekten Informationen erhält. Weil unser SDK auch die entsprechenden HTML-Seiten (sofern vorhanden) und nicht nur die URLs analysiert, kann das SDK bei einigen Kategorien dennoch die Inhalte erkennen. Andere Einsatzzwecke lassen sich jedoch nicht allein durch die Verwendung des SDK verhindern.

URL-Ausschlüsse

Webadressen (URLs), von denen bekannt ist, dass sie sicher sind, können in die Liste von vertrauenswürdigen Domains aufgenommen werden. Webadressen (URLs), die eine Bedrohung darstellen, können in die Liste von blockierten Domains aufgenommen werden.

So können Sie die URLs spezifizieren, die immer als vertrauenswürdig oder blockiert eingestuft werden

1. Klicken Sie im URL-Filterungsmodul eines Schutzplans auf **URL-Ausschlüsse**.
   Das Fenster **URL-Ausschlüsse** wird geöffnet.
   Folgende Optionen werden angezeigt:

Vertrauenswürdige Elemente – Klicken Sie auf **Hinzufügen**, um aus den verfügbaren Optionen auswählen zu können:

- **Domain** – Wenn Sie diese Option wählen, wird das Fenster **Domain hinzufügen** geöffnet.
  - Geben Sie im Feld **Domain** jede Domain in einer neuen Zeile ein. Geben Sie in das Feld **Beschreibung** eine kurze Erläuterung ein, damit Sie Ihre Änderung in der Liste der vertrauenswürdigen Elemente erkennen können.
- **Prozess** – Wenn Sie diese Option wählen, wird das Fenster **Prozess hinzufügen** angezeigt.
  - Geben Sie im Feld **Prozess** den Pfad für jeden Prozess in einer neuen Zeile ein. Geben Sie im Abschnitt **Beschreibung** eine kurze Erläuterung ein, damit Sie Ihre Änderung in der Liste der vertrauenswürdigen Elemente erkennen können.

Blockierte Elemente– Klicken Sie auf **Hinzufügen**. Das Fenster **Domain hinzufügen** wird angezeigt.

Geben Sie im Feld **Domain** jede Domain in einer neuen Zeile ein. Geben Sie in das Feld **Beschreibung** eine kurze Erläuterung ein, damit Sie Ihre Änderung in der Liste der blockierten Elemente erkennen können.

Hinweis
Es werden lokale Netzwerkpfade unterstützt. Beispielsweise \\localhost\folderpath\file.exe.

Beschreibung

Sie können das Feld **Beschreibung** verwenden, um sich Notizen über die Ausschlüsse zu machen, die Sie in die URL-Ausschlussliste aufgenommen haben. Hier sind einige Vorschläge für Notizen, die Sie machen können:

- Gründe und Zwecke für den Ausschluss.
- Zeitstempel.

Wenn mehrere Elemente als ein einzelner Eintrag hinzugefügt werden, kann nur ein (1) Kommentar für diese mehrfachen Elemente erfasst werden.

Microsoft Defender Antivirus und Microsoft Security Essentials

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Microsoft Defender Antivirus

Microsoft Defender Antivirus ist eine integrierte Antimalware-Komponente von Microsoft Windows, die seit Windows 8 mit dem Betriebssystem ausgeliefert wird.

Das Microsoft Defender Antivirus (WDA)-Modul ermöglicht Ihnen, eine Microsoft Defender Antivirus-Sicherheitsrichtlinie zu konfigurieren und deren Status über die Cyber Protect-Konsole zu verfolgen.

Dieses Modul ist auf Workloads anwendbar, auf denen Microsoft Defender Antivirus installiert ist.

Microsoft Security Essentials

Microsoft Security Essentials ist eine integrierte Antimalware-Komponente von Microsoft Windows, die mit Windows-Betriebssystemen vor Windows 8 ausgeliefert wurde.

Das Microsoft Security Essentials-Modul ermöglicht Ihnen, eine Microsoft Security Essentials-Sicherheitsrichtlinie zu konfigurieren und deren Status über die Cyber Protect-Konsole zu verfolgen.

Dieses Modul ist auf Workloads anwendbar, auf denen Microsoft Security Essentials installiert ist.

Die Einstellungen für Microsoft Security Essentials gleichen denen für Microsoft Defender Antivirus, aber Sie können keinen Echtzeitschutz konfigurieren und keine Ausschlüsse über die Cyber Protect-Konsole definieren.

Scan planen

Spezifizieren Sie eine Zeitplanung für das Scanning.

Scan-Modus:

- **Vollständig** – es erfolgt eine vollständige Überprüfung aller Dateien und Ordner (zusätzlich zu den im Schnellscan gescannten Elementen). Im Vergleich zum Schnellscan werden hier mehr Maschinen-Ressourcen zur Ausführung benötigt.
- **Schnell** – eine schnelle Überprüfung der Prozesse im Arbeitsspeicher sowie von Ordnern, in denen Malware üblicherweise anzufinden ist. Es werden weniger Maschinen-Ressourcen zur Ausführung benötigt.

Definieren Sie einen Zeitpunkt und Wochentag, an dem der Scan durchgeführt werden soll.

Täglicher Schnellscan – definieren Sie den Zeitpunkt, an dem der tägliche Schnellscan ausgeführt werden soll.

Sie können, abhängig von Ihren Anforderungen, folgende Optionen festlegen:

Geplanten Scan starten, wenn die Maschine online ist, aber nicht verwendet wird

Vor Ausführung eines geplanten Scans nach neuesten Viren- und Spyware-Definitionen suchen

CPU-Auslastung während des Scans begrenzen auf:

Weitere Informationen über die Einstellung für Microsoft Defender Antivirus finden Sie unter der Adresse https://docs.microsoft.com/de-de/sccm/protect/deploy-use/endpoint-antimalware-policies#scheduled-scans-settings.

Standardaktionen

Definieren Sie Standardaktionen, die für erkannte Bedrohungen mit unterschiedlichen Schweregraden durchgeführt werden sollen:

- **Bereinigen** – die auf einem Workload erkannte Malware wird entfernt.
- **Quarantäne** – die erkannte Malware wird nicht vollständig entfernt, sondern in den Quarantäne-Ordner verschoben.
- **Entfernen** – die auf einem Workload erkannte Malware wird gelöscht.
- **Erlauben** – die erkannte Malware wird nicht entfernt oder in Quarantäne verschoben
- **Benutzerdefiniert** – der Benutzer wird aufgefordert, die Aktion zu spezifizieren, die mit der erkannten Malware durchgeführt werden soll.
- **Keine Aktion** – es werden keine Aktionen durchgeführt.
- **Blockieren** – die erkannte Malware wird blockiert.

Weitere Informationen über die Standardeinstellungen für Microsoft Defender Antivirus-Aktionen finden Sie unter der Adresse https://docs.microsoft.com/de-de/mem/configmgr/protect/deploy-use/endpoint-antimalware-policies#default-actions-settings.

Echtzeitschutz

Aktivieren Sie den **Echtzeitschutz**, um Malware zu erkennen und zu unterbinden, dass diese auf Workloads installiert oder ausgeführt werden kann.

Alle Downloads scannen – wenn diese Option ausgewählt wurde, werden alle heruntergeladenen Dateien und Anhänge auf Malware überprüft.

Verhaltensüberwachung aktivieren – wenn diese Option ausgewählt wurde, wird das System auf verdächtiges Verhalten hin überwacht.

Netzwerkdateien scannen – wenn diese Option ausgewählt wurde, werden Netzwerkdateien überprüft.

Vollständigen Scan auf zugeordneten Netzwerklaufwerken erlauben – wenn diese Option ausgewählt wurde, werden als Laufwerke gemountete Netzwerkordner vollständig überprüft.

E-Mail-Scannen erlauben – wenn diese Option ausgewählt wurde, werden das Postfach und dessen E-Mail-Dateien (entsprechend ihrem spezifischen Format) analysiert, um die E-Mail-Inhalte und Dateianhänge auf Schadsoftware zu überprüfen.

Weitere Informationen über die Einstellungen für den Microsoft Defender Antivirus-Echtzeitschutz finden Sie unter der Adresse https://docs.microsoft.com/de-de/sccm/protect/deploy-use/endpoint-antimalware-policies#real-time-protection-settings.

Erweitert

Spezifizieren Sie die erweiterten Scan-Einstellungen:

- **Archivdateien scannen** – auch Archivdateien (wie .zip- oder .rar-Dateien) werden in den Scan-Vorgang mit einbezogen.
- **Wechsellaufwerke scannen** – auch entfernbare Laufwerke werden bei einem vollständigen Scan überprüft
- **Systemwiederherstellungspunkt erstellen** – es kann gelegentlich vorkommen, dass eine wichtige Datei oder ein Registry-Eintrag als 'falsch positiv' erkannt und dann entfernt wird. Mit einem Wiederherstellungspunkt können Sie Ihr System auf den entsprechenden Zustand davor zurücksetzen.
- **Dateien aus der Quarantäne entfernen nach** – definiert einen Zeitraum, nach dessen Ablauf die entsprechenden Dateien aus der Quarantäne gelöscht werden.
- **Beispiele automatisch senden, wenn eine weitere Untersuchung erforderlich ist:**
  - **Immer auffordern** – Sie werden vor dem Versenden der Datei aufgefordert, die Aktion zu bestätigen.
  - **Automatisch sichere Beispiele senden** – die meisten Beispiele werden automatisch gesendet. Ausgenommen davon sind Dateien, die persönliche Informationen enthalten könnten. Für solche Dateien ist eine zusätzliche Bestätigung erforderlich.
  - **Automatisch alle Beispiele senden** – alle Beispiele werden automatisch gesendet.
- **Windows Defender Antivirus-Benutzeroberfläche deaktivieren** – wenn diese Option ausgewählt ist, wird die WDA-Benutzeroberfläche nicht für den Benutzer verfügbar sein. Sie können die WDA-Richtlinien über die Cyber Protect-Konsole verwalten.
- **MAPS (Microsoft Active Protection Service)** – eine Online-Community, die Ihnen bei der Entscheidung hilft, wie Sie auf potenzielle Bedrohungen reagieren sollten.
  - **Ich möchte MAPS nicht verwenden** – es werden keine Informationen über die erkannte Software an Microsoft gesendet.
  - **Basis-Mitgliedschaft** – es werden grundlegende Informationen über die erkannte Software an Microsoft gesendet.
  - **Premium-Mitgliedschaft** – es werden ausführlichere Informationen über die erkannte Software an Microsoft gesendet.

Weitere Informationen dazu finden Sie unter der Adresse https://www.microsoft.com/security/blog/2015/01/14/maps-in-the-cloud-how-can-it-help-your-enterprise/

Weitere Informationen über die erweiterten Einstellung für Microsoft Defender Antivirus finden Sie unter der Adresse https://docs.microsoft.com/de-de/sccm/protect/deploy-use/endpoint-antimalware-policies#advanced-settings.

Ausschlüsse

Sie können folgende Dateien und Ordner definieren, die vom Scannen ausgeschlossen werden sollen:

- **Prozesse** – jede Datei, die von einem hier spezifizierten Prozess gelesen oder geschrieben wird, wird aus dem Scanvorgang ausgeschlossen. Sie müssen einen vollständigen Pfad zur ausführbaren Datei des entsprechenden Prozesses definieren.
- **Dateien und Ordner** – die hier spezifizierten Dateien und Ordner werden aus dem Scanvorgang ausgeschlossen. Sie müssen einen vollständigen Pfad zu einem Ordner/einer Datei spezifizieren – oder (eine) Datei-Erweiterung(en) definieren.

Weitere Informationen über die Ausschlusseinstellungen für Microsoft Defender Antivirus finden Sie unter der Adresse https://docs.microsoft.com/de-de/sccm/protect/deploy-use/endpoint-antimalware-policies#exclusion-settings.

Firewall-Verwaltung

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Die Firewall-Verwaltung ermöglicht Ihnen, die Firewall-Einstellungen für geschützte Workloads einfach zu konfigurieren.

Diese Funktionalität in Cyber Protect wird durch eine integrierte Microsoft Defender Firewall-Komponente von Microsoft Windows bereitgestellt. Die Microsoft Defender Firewall blockiert nicht autorisierten Netzwerkverkehr, der zu oder von Ihren Workloads fließt.

Die Firewall-Verwaltung ist auf Workloads anwendbar, auf denen die Microsoft Defender Firewall installiert ist.

Unterstützte Windows-Betriebssysteme

Folgende Windows-Betriebssysteme werden für die Firewall-Verwaltung unterstützt:

Windows

- Windows 8
- Windows 8.1
- Windows 10
- Windows 11

Windows Server werden nicht unterstützt.

Die Firewall-Verwaltung aktivieren oder deaktivieren

Sie können die Firewall-Verwaltung aktivieren, wenn Sie einen Schutzplan erstellen. Sie können auch einen bereits vorhandenen Schutzplan ändern, um die Firewall-Verwaltung zu aktivieren oder zu deaktivieren.

So können Sie die Firewall-Verwaltung aktivieren oder deaktivieren

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte** –> **Alle Geräte**.
2. Gehen Sie folgendermaßen vor, um das Schutzplan-Panel zu öffnen:
   - Wählen einen neuen Schutzplan erstellen wollen: wählen Sie die zu schützende Maschine aus, klicken Sie dann auf **Schützen** und anschließend auf **Plan erstellen**.
   - Wenn Sie einen vorhandenen Schutzplan ändern wollen: wählen Sie eine geschützte Maschine aus und klicken Sie dann auf **Schützen**. Klicken Sie anschließend neben dem Namen des Schutzplans auf das Drei-Punkte-Symbol (...) und wählen Sie abschließend den Befehl **Bearbeiten**.
3. Gehen Sie im Schutzplan-Panel zum Bereich **Firewall-Verwaltung** und aktivieren oder deaktivieren Sie die Option **Firewall-Verwaltung**.
4. Gehen Sie folgendermaßen vor, um Ihre Änderungen zu übernehmen:
   - Wenn Sie einen Schutzplan erstellen, dann klicken Sie auf **Erstellen**.
   - Wenn Sie einen Schutzplan bearbeiten, dann klicken Sie auf **Speichern**.

Der **Microsoft Defender Firewall-Status** im Bereich **Firewall-Verwaltung** des Schutzplan-Panels wird entweder mit **An** oder **Aus** angezeigt – in Abhängigkeit davon, ob Sie die Firewall-Verwaltung aktiviert oder deaktiviert haben.

Sie können auch über die Registerkarte Verwaltung auf das Schutzplan-Panel zugreifen. Diese Möglichkeit ist jedoch nicht in allen Editionen des Cyber Protection Service verfügbar.

Quarantäne

Die **Quarantäne** ist ein spezieller, isolierter Ordner auf dem internen Laufwerk einer Maschine, wo Dateien, die von der Antivirus & Antimalware Protection als verdächtig erkannt wurden, abgelegt werden, um die weitere Ausbreitung der entsprechenden Bedrohung zu verhindern.

Die Quarantäne ermöglicht es Ihnen, verdächtige und potenziell gefährliche Dateien von Maschinen zu überprüfen und in Ruhe zu entscheiden, ob diese entfernt oder wiederhergestellt werden sollen.

In Quarantäne befindliche Dateien werden automatisch gelöscht, wenn die entsprechende Maschine aus dem System entfernt wird.

Wie gelangen Dateien in den Quarantäne-Ordner?

1. Sie konfigurieren einen entsprechenden Schutzplan und definieren als Standardaktion für infizierte Dateien, dass diese unter Quarantäne gestellt werden sollen.
2. Das System erkennt während eines Scans (egal ob per Zeitplanung oder manuell ausgeführt) evtl. vorhandene bösartige Dateien und verschiebt diese in den sicheren Quarantäne-Ordner.
3. Das System aktualisiert die Quarantäne-Liste auf den geschützten Maschinen.
4. Die entsprechenden Dateien werden nach einem Zeitraum, der in der Option **Dateien aus der Quarantäne entfernen nach** des Schutzplans definiert wurde, automatisch aus dem Quarantäne-Ordner gelöscht ('Bereinigung').

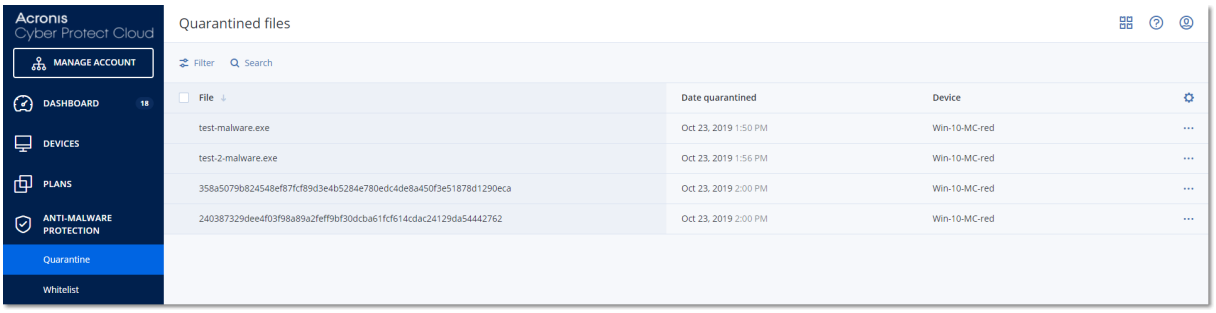
In Quarantäne befindliche Dateien verwalten

Wenn Sie die unter Quarantäne stehenden Dateien verwalten wollen, gehen Sie zu **Antimalware Protection** –> **Quarantäne**. Sie sehen eine Liste mit allen unter Quarantäne stehenden Dateien von allen Maschinen.

Name	Beschreibung
Datei	Der Dateiname.
Quarantäne-Datum	Datum und Uhrzeit, als die Datei unter Quarantäne gestellt wurde.
Gerät	Das Gerät, auf dem die infizierte Datei gefunden wurde.
Bedrohungsname	Der Name der Bedrohung.
Schutzplan	Der Schutzplan, auf dessen Basis die verdächtige Datei unter Quarantäne gestellt wurde.

Sie können zwei Aktionen mit den Dateien in der Quarantäne durchführen:

- **Löschen** – die entsprechende, unter Quarantäne stehende Datei wird von allen Maschinen dauerhaft entfernt. Sie können alle Dateien löschen, die den gleichen Datei-Hash haben. Sie können alle Dateien wiederherstellen, die den gleichen Datei-Hash haben. Gruppieren Sie die Dateien nach dem Hashwert, wählen Sie die gewünschten Dateien aus und löschen Sie diese dann.
- **Recovery** - Stellen Sie eine unter Quarantäne gestellte Datei ohne Änderungen am ursprünglichen Speicherort wieder her. Wenn sich bereits eine Datei mit demselben Namen am ursprünglichen Ort befindet, wird sie durch die wiederhergestellte Datei überschrieben. Beachten Sie, dass die wiederhergestellte Datei zur Positivliste hinzugefügt und bei weiteren Antimalware-Scans übersprungen wird.



Quarantäne-Speicherort auf den Maschinen

Der Standardspeicherort für die Quarantäne von verdächtigen Dateien ist:

- Für eine Windows-Maschine: `%programdata%\Acronis\NGMP\quarantine`
- Für eine Mac-Maschine: `/Library/Application Support/Acronis/NGMP/Quarantäne`
- Für eine Linux-Maschine: `/var/lib/Acronis/NGMP/Quarantäne`

Der Quarantäne-Speicherort wird durch die Selbstschutzfunktion (Self-Protection) des Service-Providers geschützt.

Manuelle Self-Service-Scans von benutzerdefinierten Ordnern

Sie können auf dem Workload benutzerdefinierte Ordner auswählen und diese dann direkt über deren Kontextmenü scannen lassen.

So können Sie über die Option Cyber Protect im Kontextmenü auf die Scan-Funktion zugreifen

Bei Workloads, in deren Schutzplan das Antivirus & Antimalware Protection-Modul aktiviert wurde, können Sie mit der rechten Maustaste auf die Dateien/Ordner klicken, die Sie auf Malware scannen lassen wollen.

Hinweis
Diese Option ist nur für Administratoren des Workloads verfügbar.

Positivliste für Unternehmensapplikationen

Eine Antivirus-Lösung könnte zulässige unternehmensspezifische Applikationen als verdächtig identifizieren. Um solche Falsch-Positiv-Erkennungen zu vermeiden, werden vertrauenswürdige Applikationen manuell zu einer Positivliste hinzugefügt, was zeitaufwendig sein kann.

Hinweis
Die Positivliste für Unternehmensapplikationen hat keinen Einfluss auf die Antimalware-Scans von Backups.

Cyber Protection kann diesen Prozess automatisieren: vorhandene Backups werden vom Antivirus & Antimalware Protection-Modul gescannt und die gescannten Daten analysiert, sodass diese Applikationen in die Positivliste aufgenommen werden und somit zukünftige Falsch-Positiv-Erkennungen unterbunden werden. Die unternehmensweite Positivliste verbessert außerdem die Performance zukünftiger Antimalware-Scans.

Die Positivliste wird für jeden Kunden erstellt und basiert nur auf den Daten dieses Kunden.

Die Positivliste kann jederzeit aktiviert und deaktiviert werden. Wenn sie deaktiviert wird, werden die hinzugefügten Dateien vorübergehend ausgeblendet.

Hinweis
Nur Konten mit der Rolle 'Administrator' (wie z.B. ein Cyber Protection-Administrator, Firmenadministrator, Abteilungsadministrator oder ein Partneradministrator, der im Auftrag eines Firmenadministrators handelt) können die Positivliste konfigurieren bzw. verwalten. Diese Funktionalität ist nicht für ein Nur-Lesen-Administrator-Konto oder ein Benutzerkonto verfügbar.

Automatisches Hinzufügen zur Positivliste

1. Führen Sie ein Cloud-Scanning von Backups auf mindestens zwei Maschinen durch. Sie können dafür Backup-Scanning-Pläne verwenden.
2. Aktivieren Sie in den Einstellungen der Positivliste den Schalter **Positivliste automatisch generieren**.

Manuelles Hinzufügen zur Positivliste

Wenn der Schalter **Positivliste automatisch generieren** deaktiviert ist, können Sie Dateien dennoch weiterhin manuell zur Positivliste hinzufügen.

1. Gehen Sie in der Cyber Protect-Konsole zu **Antimalware Protection** –> **Positivliste**.
2. Klicken Sie auf **Datei hinzufügen**.
3. Spezifizieren Sie den Pfad zu der Datei und klicken Sie dann auf **Hinzufügen**.

Unter Quarantäne stehende Dateien zur Positivliste hinzufügen

Sie können Dateien, die sich in der Quarantäne befinden, zur Positivliste hinzufügen.

1. Gehen Sie in der Cyber Protect-Konsole zu **Antimalware Protection** –> **Quarantäne**.
2. Wählen Sie eine unter Quarantäne stehende Datei aus und klicken Sie dann auf **Zur Positivliste hinzufügen**.

Einstellungen für die Positivliste

Wenn Sie den Schalter **Positivliste automatisch generieren** aktivieren, müssen Sie eine der folgenden Stufen des Heuristikschutzes spezifizieren:

- **Niedrig**
  Die Unternehmensapplikationen werden erst nach einer längeren Zeit und einigen Überprüfungen in die Positivliste aufgenommen. Solche Applikationen sind vertrauenswürdiger. Dieser Ansatz erhöht jedoch die Möglichkeit von Falsch-Positiv-Erkennungen. Die Kriterien, nach denen eine Datei als sauber und vertrauenswürdig eingestuft wird, sind hoch.
- **Standard**
  Die Unternehmensapplikationen werden der Positivliste entsprechend der empfohlenen Schutzstufe hinzugefügt, um das Risiko für Falsch-Positiv-Erkennungen zu senken. Die Kriterien, nach denen eine Datei als sauber und vertrauenswürdig eingestuft wird, sind mittelstark.
- **Hoch**
  Die Unternehmensapplikationen werden der Positivliste schneller hinzugefügt, um das Risiko für Falsch-Positiv-Erkennungen zu senken. Dies garantiert jedoch nicht, dass die Software wirklich sauber ist. Sie könnte später noch als verdächtig erkannt bzw. als Malware eingestuft werden. Die Kriterien, nach denen eine Datei als sauber und vertrauenswürdig eingestuft wird, sind niedrig.

Details zu Elementen in der Positivliste anzeigen

Sie können auf ein Element in der Positivliste klicken, um weitere Informationen zu diesem Element zu erhalten und es online zu analysieren.

Wenn Sie sich bei einem Element, welches Sie hinzugefügt haben, unsicher sind, können Sie es im VirusTotal Analyzer überprüfen. Wenn Sie auf **Auf VirusTotal überprüfen** klicken, wird die Website verdächtige Dateien und URLs analysieren, um Malware-Typen zu erkennen, wobei der Datei-Hash des von Ihnen hinzugefügten Elements verwendet wird. Sie können den Hash in der Zeichenfolge **Datei-Hash (MD5)** einsehen.

Der Wert **Maschinen** steht für die Anzahl der Maschinen, bei denen ein solcher Hash beim Backup-Scannen gefunden wurde. Dieser Wert wird nur angegeben, wenn ein Element aus dem Backup-Scanning oder der Quarantäne stammt. Dieses Feld bleibt leer, wenn die Datei manuell zur Positivliste hinzugefügt wurde.

Antimalware-Scan von Backups

Mit einem Antimalware-Scan von Backups können Sie verhindern, dass infizierte Dateien wiederhergestellt werden, indem Sie überprüfen lassen, ob Ihre Backups keine Malware enthalten. Antimalware-Scans werden von einem Cloud Agenten durchgeführt, der sich im Cyber Protection Datacenter befindet, sodass keine lokalen Computing-Ressourcen verwendet werden müssen.

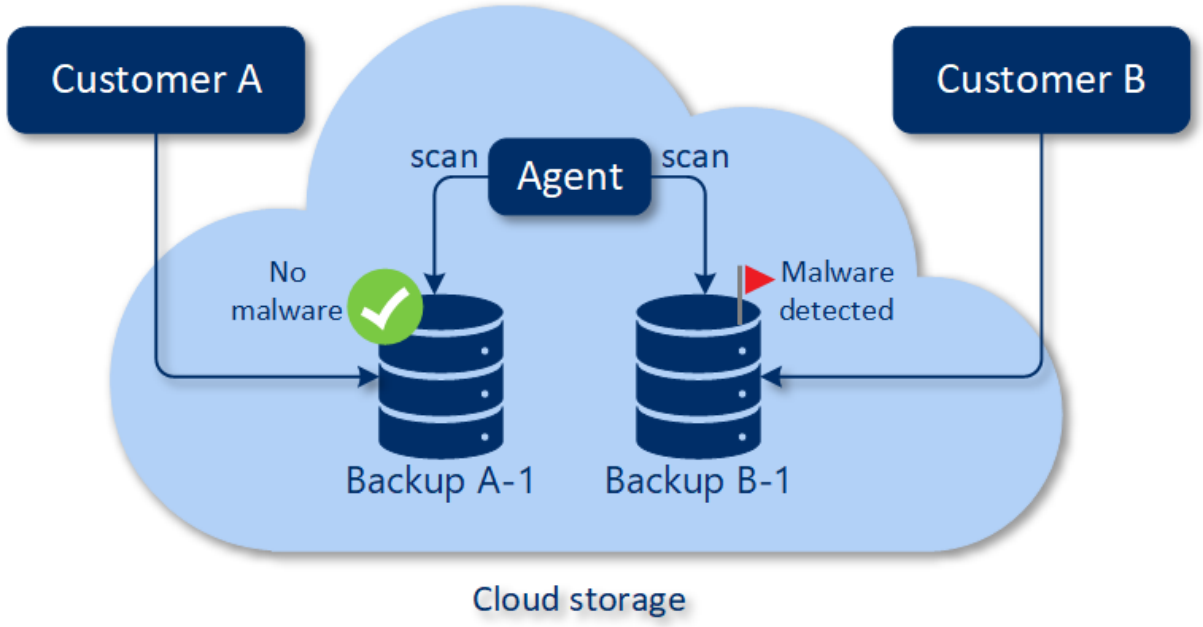
Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Wenn Sie einen Antimalware-Scan durchführen wollen, müssen Sie einen Backup-Scanning-Plan konfigurieren. Weitere Informationen über die entsprechende Durchführung finden Sie im Abschnitt '"Backup-Scanning-Pläne" (S. 213)'.

Jeder Backup-Scanning-Plan erstellt einen Scanning-Task für den Cloud Agenten und stellt diesen Task in eine Warteschlange, von der es eine pro Datacenter gibt. Die Scanning-Tasks werden entsprechend ihrer Reihenfolge in der Warteschlange abgearbeitet. Die Scan-Zeit hängt zudem von der Backup-Größe ab. Aus diesem Grund gibt es eine Verzögerung zwischen dem Erstellen eines Backup-Scanplans und der Fertigstellung des Scans.

Die Backups, die Sie zum Scannen ausgewählt haben, können sich in einem der folgenden Stadien befinden:

- Nicht gescannt
- Keine Malware
- Malware erkannt



Sie können die Ergebnisse eines Backup-Scans im 'Widget für die **Backup-Scanning-Details (Bedrohungen)**' überprüfen. Sie können das Widget in der Cyber Protect-Konsole auf der Registerkarte **Monitoring** –> **Überblick** finden.

Beschränkungen

- Antimalware-Scans werden für die Backup-Typen **Komplette Maschine** oder **Laufwerke/Volumes** von folgenden Workloads unterstützt:
  - Windows-Maschinen, auf denen ein Protection Agent installiert ist.
  - Virtuelle Windows-Maschinen, die auf Hypervisor-Ebene (agentenloses Backup) durch den Agenten für Hyper-V oder den Agenten für VMware (Windows) gesichert werden.

  Antimalware-Scans werden nicht für Backups unterstützt, die von virtuellen Appliances erstellt werden – wie etwa dem Agenten für VMware (virtuelle Appliance), dem Agenten für Virtuozzo oder dem Agenten für Scale Computing HC3.

- Es werden zudem nur Volumes mit dem NTFS-Dateisystem sowie einer GPT- oder MBR-Partitionierung gescannt.
- Als Backup-Speicherort wird nur der standardmäßige Cloud Storage unterstützt. Lokale Storages und Partner-eigene Cloud Storages werden nicht unterstützt.
- Bei der Auswahl der zu scannenden Backups können Sie auch Backup-Sets auswählen, die ein CDP-Backup (Backup aus einer kontinuierlichen Datensicherung) enthalten. Es werden jedoch nur die Nicht-CDP-Backups in diesen Backup-Sets gescannt. Weitere Informationen über CDP-Backups finden Sie im Abschnitt '"Kontinuierliche Datensicherung (CDP)" (S. 448)'.
- Wenn Sie eine sichere Wiederherstellung (Safe Recovery) einer kompletten Maschine durchführen wollen, können Sie auch ein Backup-Set auswählen, das ein CDP-Backup enthält. Bei dieser Recovery-Aktion werden die Daten im CDP-Backup jedoch nicht verwendet. Wenn Sie die CDP-Daten wiederherstellen wollen, müssen Sie eine zusätzliche Wiederherstellung von **Dateien/Ordnern** ausführen.

Mit Advanced Protection-Funktionen arbeiten

Cyber Protect enthält standardmäßig Funktionen, die die meisten Cyber Security-Bedrohungen abdecken. Sie können diese Funktionen ohne zusätzliche Kosten verwenden. Sie können jedoch zusätzliche Advanced-Funktionen aktivieren, um den Schutz Ihrer Workloads weiter zu verbessern.

- Wenn eine Advanced Protection-Funktion für Sie verfügbar ist, wird diese im Schutzplan mit folgendem Advanced Protection-Symbol gekennzeichnet:  .
- Wenn eine Advanced Protection-Funktion für Sie nicht verfügbar ist, kontaktieren Sie Ihren Administrator, um das erforderliche Advanced Protection-Paket freigeschaltet zu bekommen.
- Wenn der Administrator Ihnen ermöglicht hat, zusätzliche Sicherheitspakete zu kaufen, können Sie auswählen, dass die Advanced-Funktionen aktiviert werden sollen. Sie werden in einer Meldung darauf hingewiesen, dass zusätzliche Kosten anfallen.

Hinweis
Wenn mindestens eine Funktion aktiviert ist, müssen Sie das entsprechende Advanced Protection-Paket erwerben.

Hinweis
Wenn alle Advanced-Funktionen in Ihrem Schutzplan deaktiviert sind, wird auch das dazugehörige Advanced Protection-Paket deaktiviert.

Advanced Protection-Paket	Advanced Protection-Funktionen
Advanced Backup	Schützt Ihre Workloads kontinuierlich und stellt sicher, dass selbst kurzfristige Änderungen Ihrer Arbeit nicht verloren gehen. Zu den enthaltenen Funktionen gehören: • One-Click Recovery • Kontinuierliche Datensicherung (CDP) • Backup support for Microsoft SQL Server clusters and Microsoft Exchange clusters – AlwaysOn-Verfügbarkeitsgruppen (AAG) und Datenbankverfügbarkeitsgruppen (DAG) • Backup-Unterstützung für MariaDB, MySQL, Oracle DB und SAP HANA • Data Protection-Karte und Compliance-Berichterstattung • Off-Host Data Processing • Backup-Häufigkeit für Microsoft 365- und Google Workspace-Workloads • Remote-Aktionen mit einem Boot-Medium • Direktes Backup in den Microsoft Azure Public Cloud Storage
Advanced Security + EDR	Schützt Ihre Workloads kontinuierlich vor allen Malware-Bedrohungen. Zu den enthaltenen Funktionen gehören: • Verwalten Sie Vorfälle auf einer zentralen Vorfallsseite • Visualisieren Sie das Ausmaß und die Auswirkungen von Vorfällen • Empfehlungen und Behebungsmaßnahmen

	• Überprüfen Sie anhand von Bedrohungsfeeds, ob es öffentlich bekannte Angriffe auf Ihre Workloads gibt • Speichern Sie Sicherheitsereignisse für 180 Tage • Antivirus & Antimalware Protection mit lokaler signaturbasierter Erkennung (mit Echtzeitschutz) • Exploit-Prävention • URL-Filterung • Endpunkt-Firewall-Verwaltung • Forensik-Backup, Backups nach Malware scannen, Safe Recovery-Funktionalität, Positivliste für Unternehmensapplikationen • Intelligente Schutzpläne (Integration von CPOC-Alarmmeldungen) • Zentrales Backup-Scanning nach Malware • Remote-Löschung • Microsoft Defender Antivirus • Microsoft Security Essentials
Advanced Management	Ermöglicht Ihnen das Patchen von Schwachstellen auf den geschützten Workloads. Zu den enthaltenen Funktionen gehören: • Patch-Verwaltung • Laufwerksintegrität • Software-Inventarisierung • Ausfallsicheres Patching • Cyber Scripting • Remote-Unterstützung • Dateiübertragung und -freigabe • Eine Sitzung zum Verbinden auswählen • Workloads in der Mehrfachansicht beobachten • Verbindungsmodi: Steuerung, Nur-Anzeigen und Vorhang • Verbindung über die Quick Assist-Applikation • Remote-Verbindungsprotokolle: NEAR und Apple Bildschirmfreigabe • Sitzungsaufzeichnung für NEAR-Verbindungen • Screenshot-Übertragung • Sitzungsverlaufsbericht • 24 Monitore • Grenzwert-basiertes Monitoring • Anomalie-basiertes Monitoring
Advanced Data Loss Prevention	Verhindert das Durchsickern sensibler Informationen von den geschützten Workloads. Zu den enthaltenen Funktionen gehören: • Inhaltssensitiver Schutz vor dem unautorisierten Abfließen von Daten aus Workloads über Peripheriegeräte und Netzwerk-Kommunikation • Vorgefertigte automatische Erkennung von personenbezogenen Informationen (PII), geschützten Gesundheitsinformationen (PHI) und PCI DSS-Daten (Payment Card

	Industry Data Security Standard, Kreditkartenindustrie-Datensicherheitsstandard) sowie von Dokumenten der Kategorie 'Als vertraulich gekennzeichnet' • Automatische Erstellung von Data Loss Prevention-Richtlinien mit optionaler Unterstützung durch den Endbenutzer • Adaptive Erzwingung der Data Loss Prevention-Richtlinie mit einer automatischen, lernfähigen Richtlinien-Anpassung • Cloud-basierte zentrale Überwachungsprotokolle, Alarmmeldungen und Endbenutzer-Benachrichtigungen

Advanced Data Loss Prevention

Das Advanced Data Loss Prevention-Modul analysiert den Inhalt und den Kontext von Datenübertragungen auf geschützten Workloads und verhindert auf der Grundlage der Datenfluss-Richtlinie, dass sensible Daten über Peripheriegeräte oder Netzwerkübertragungen im und aus dem Unternehmensnetzwerk unautorisiert abfließen können.

Die Advanced Data Loss Prevention-Funktionen können in jeden Schutzplan für einen Kunden-Mandanten aufgenommen werden, wenn der Protection Service und das Advanced Data Loss Prevention-Paket für diesen Kunden aktiviert sind.

Bevor Sie das Advanced Data Loss Prevention-Modul erstmalig einsetzen, sollten Sie sich vergewissern, dass Sie die grundlegenden Konzepte und Logik der Advanced DLP-Verwaltung gelesen und verstanden haben, wie sie in der Grundlagen-Anleitung beschrieben sind.

Sie können zudem auch noch das Dokument zu den Technische Spezifikationen studieren.

Datenfluss-Richtlinie und Richtlinienregeln erstellen

Das Grundprinzip der Data Loss Prevention-Funktionalität besagt, dass die Anwender eines Unternehmens-IT-Systems sensible Daten nur in dem Maße handhaben dürfen, wie es zur Erfüllung ihrer beruflichen Aufgaben erforderlich ist. Alle anderen Übertragungen von sensiblen Daten, die für die geschäftlichen Prozesse nicht relevant sind, sollten blockiert werden. Daher ist es wesentlich, zwischen geschäftsrelevanten und unzulässigen Datenübertragungen bzw. Datenflüssen unterscheiden zu können.

Die Datenfluss-Richtlinie enthält Regeln, die spezifizieren, welche Datenflüsse erlaubt und welche verboten sind. Auf diese Weise wird die unbefugte Übertragung von sensiblen Informationen verhindert, wenn das Data Loss Prevention-Modul in einem Schutzplan aktiviert wurde und im Erzwingungsmodus läuft.

Jede Vertraulichkeitskategorie in der Richtlinie enthält eine Standardregel, die mit einem Sternchen (*) gekennzeichnet ist, sowie eine oder mehrere explizite (nicht standardmäßige) Regeln, die den Datenfluss für bestimmte Benutzer oder Gruppen definieren. Weitere Informationen zu den Arten von Richtlinienregeln finden Sie in der Grundlagen-Anleitung.

Die Datenfluss-Richtlinie wird üblicherweise automatisch erstellt, während die Advanced Data Loss Prevention-Funktionalität im Beobachtungsmodus läuft. Der Zeitaufwand für die Erstellung einer

repräsentativen Datenfluss-Richtlinie beträgt ungefähr einen Monat. Dies kann jedoch je nach den Prozessen in Ihrem Unternehmen variieren. Die Datenfluss-Richtlinie kann außerdem auch manuell von einem Firmen- oder Abteilungsadministrator erstellt, konfiguriert oder bearbeitet werden.

Wenn Sie mit dem automatischen Richtlinien-Erstellung beginnen wollen

1. Melden Sie sich als Administrator an der Cyber Protect-Konsole an.
2. Wechseln Sie zu **Verwaltung** > **Schutzpläne**.
3. Klicken Sie auf **Plan erstellen**.
4. Erweitern Sie den Bereich **Data Loss Prevention** und klicken Sie auf die Zeile **Modus**.
5. Wählen Sie im Modus-Dialog den **Beobachtungsmodus** aus und bestimmen Sie, wie die Datenübertragungen verarbeitet werden sollen:

Option	Beschreibung
Alle erlauben	Alle Übertragungen von sensiblen Daten aus Benutzer-Workloads werden als geschäftlich notwendig und sicher behandelt. Für jeden erkannten Datenfluss, der nicht mit einer bereits definierten Regel in der Richtlinie übereinstimmt, wird eine neue Regel erstellt.
Alle rechtfertigen	Alle Übertragungen von sensiblen Daten aus Benutzer-Workloads werden zwar als geschäftlich notwendig, aber auch riskant behandelt. Daher muss der Benutzer bei jeder abgefangenen Übertragung sensibler Daten an einen beliebigen Empfänger oder ein beliebiges Ziel innerhalb oder außerhalb des Unternehmens, die nicht mit einer zuvor erstellten Datenfluss-Regel übereinstimmt, eine einmalige geschäftliche Rechtfertigung abgeben. Wenn die Rechtfertigung übermittelt wird, wird in der Datenfluss-Richtlinie eine neue Datenfluss-Regel erstellt.
Gemischt	Die Logik 'Alle erlauben' gilt für alle internen sensiblen Datenflüsse – und die Logik 'Alle rechtfertigen' gilt für alle externen Datenflüsse. **Hinweis** Weitere Informationen über interne und externe Daten finden Sie unter Automatisierte Erkennung des Ziels

6. Speichern Sie den Schutzplan und wenden Sie ihn auf die Workloads an, von denen Sie Daten zur Erstellung der Richtlinie sammeln wollen.

Hinweis
Im Beobachtungsmodus werden keine Datenlecks verhindert.

Wenn Sie die Datenfluss-Richtlinie manuell spezifizieren wollen

1. Gehen Sie in der Cyber Protect-Konsole zu **Schutz** –> **Datenfluss-Richtlinie**.
2. Klicken Sie auf **Neue Datenfluss-Regel**.
   Auf der rechten Seite wird der Fensterbereich 'Neue Datenfluss-Regel' erweitert.

3. Wählen Sie eine Vertraulichkeitskategorie aus, fügen Sie einen Absender und einen Empfänger hinzu und definieren Sie anschließend für die ausgewählte Kategorie, den Absender sowie den Empfänger die Datenübertragungsberechtigung.

Option	Beschreibung
Erlauben	Diesem Absender erlauben, Daten dieser Vertraulichkeitskategorie an diesen Empfänger zu übertragen.
Ausnahme	Diesem Absender nicht erlauben, Daten dieser Vertraulichkeitskategorie an diesen Empfänger zu übertragen, aber dem Absender erlauben, für eine bestimmte Übertragung eine Regelausnahme zu beantragen. Wenn dieser Absender versucht, Daten dieser Vertraulichkeitskategorie an diesen Empfänger zu übertragen, soll die Übertragung blockiert und der Absender aufgefordert werden, eine Ausnahme einzureichen, um diese Übertragung zu erlauben. Wenn die Ausnahme übermittelt wurde, kann die Datenübertragung fortgesetzt werden. **Wichtig** Alle nachfolgenden Datenübertragungen zwischen diesem Absender und Empfänger für diese Vertraulichkeitskategorie werden für die Dauer von fünf Minuten nach Übermittlung der Ausnahme zugelassen.
Verweigern	Diesem Absender nicht erlauben, Daten dieser Vertraulichkeitskategorie an diesen Empfänger zu übermitteln, und dem Absender nicht erlauben, eine Ausnahme von dieser Regel zu beantragen.

4. (Optional) Wählen Sie eine Aktion aus, die ausgeführt werden soll, wenn die Regel aktiviert wird.

Aktion	Beschreibung
In Protokoll schreiben	Einen Ereignisdatensatz im Überwachungsprotokoll speichern, wenn die Regel ausgelöst wird. Wir empfehlen, diese Aktion für Regeln mit der Berechtigung **Ausnahme** auszuwählen.
Einen Alarm generieren	Einen Alarm in der Registerkarte **Alarmmeldungen** von Cyber Protect generieren, wenn die Regel ausgelöst wird. Wenn die Benachrichtigungsfunktion für den Administrator aktiviert ist, wird an diesen auch eine E-Mail-Benachrichtigung verschickt.
Den Endbenutzer benachrichtigen, wenn eine Datenübertragung verweigert wird	Der Benutzer in Echtzeit mit einer Bildschirmmeldung warnen, wenn er die Regel auslöst.

5. Klicken Sie auf **Speichern**.
6. Wiederholen Sie die Schritte 2 bis 5, um mehrere Regeln mit unterschiedlichen Vertraulichkeitskategorien und Optionen zu erstellen, und überprüfen Sie, ob die resultierenden Regeln den von Ihnen ausgewählten Optionen entsprechen.

Struktur der Datenfluss-Richtlinie

Richtlinienregeln werden in der Ansicht **Datenfluss-Richtlinie** nach der Kategorie der sensiblen Daten gruppiert, die von ihnen kontrolliert werden. Die Kennzeichnung für die Vertraulichkeitskategorie wird direkt über der Gruppe der Richtlinienregeln angezeigt.

- Sensibel
  - Geschützte Gesundheitsinformationen (PHI)
  - Personenbezogene Informationen (PII)
  - Kreditkartenindustrie-Datensicherheitsstandard (PCI DSS),
  - Als vertraulich gekennzeichnet
- Nicht sensibel

Weitere Informationen über das Konzept und die Funktionen der Datenfluss-Richtlinie finden Sie in der Grundlagen-Anleitung.

Regelstruktur

Jede Richtlinienregel besteht aus den nachfolgenden Elementen.

- **Vertraulichkeitskategorie**
  - **Geschützte Gesundheitsinformationen (PHI)**
  - **Personenbezogene Informationen (PII)**
  - **Kreditkartenindustrie-Datensicherheitsstandard (PCI DSS)**
  - **Als vertraulich gekennzeichnet**

    Siehe "Definitionen von sensiblen Daten" (S. 966)
- **Absender** – spezifiziert den Initiator einer Datenübertragung, die durch diese Regel kontrolliert wird. Dies kann ein einzelner Benutzer, eine Liste von Benutzern oder eine Benutzergruppe sein.
  - **Jede(r) interne** – eine Benutzergruppe, die alle internen Benutzer des Unternehmens umfasst.
  - **Kontakt / Aus Organisation** – ein Windows-Konto in der Organisation, das von der Advanced Data Loss Prevention-Funktionalität erkannt wird, sowie alle anderen Konten (einschließlich solcher, die von Drittanbieter-Kommunikationsanwendungen verwendet werden), die ein bestimmtes Windows-Konto zuvor verwendet hat.
  - **Kontakt / Benutzerdefinierte Identität** – Kennung eines internen Benutzers, spezifiziert in einem der folgenden Formate: E-Mail, Skype-ID, ICQ-Kennung, IRC-Kennung, Jabber-E-Mail, Mail.ru-Agent-E-Mail, Viber-Telefonnummer, Zoom-E-Mail.
    Folgende Platzhalterzeichen können verwendet werden, um eine Gruppe von Kontakten zu spezifizieren:
    - ***** – für eine beliebige Anzahl von Zeichen
    - **?** – für ein beliebiges einzelnes Zeichen

- **Empfänger** – spezifiziert das Ziel einer Datenübertragung, die durch diese Regel kontrolliert wird. Dabei kann es sich um einen einzelnen Benutzer, eine Liste von Benutzern, eine Benutzergruppe oder andere, weiter unten spezifizierte Zieltypen handeln.
  - **Jeder** - jeder der Empfängertypen, die von der Advanced DLP Funktionalität unterstützt werden.
  - **Kontakt / Jeder Kontakt** – jeder interne oder externe Kontakt.
  - **Kontakt / Jeder interne Kontakt** – jeder Kontakt eines internen Benutzers (siehe '"Automatisierte Erkennung des Ziels" (S. 966)').
  - **Kontakt / Jeder externe Kontakt** – jeder Kontakt einer externen Person oder Einrichtung.
  - **Kontakt / Aus Organisation** – das gleiche Prinzip, wie es für den Absender beschrieben wurde.
  - **Kontakt / Benutzerdefinierte Identität** – das gleiche Prinzip, wie es für den Absender beschrieben wurde.
  - **File Sharing Services** – die Kennung für einen kontrollierten File Sharing Service.
  - **Soziales Netzwerk** – die Kennung für ein kontrolliertes soziales Netzwerk.
  - **Host / Jeder Host** – jeder Computer, der von der Advanced DLP Funktionalität als intern oder extern erkannt wird.
  - **Host / Jeder interne Host** – jeder Computer, der von der Advanced DLP Funktionalität als intern erkannt wird.
  - **Host / Jeder externe Host** – jeder Computer, der von der Advanced DLP Funktionalität als extern erkannt wird.
  - **Host / Bestimmter Host** – eine Computer-Kennung, die als Host-Name (z.B. als vollqualifizierter Domain-Name, FQDN) oder als IP-Adresse (IPv4 oder IPv6) spezifiziert wird.
  - **Gerät / Jedes Gerät** – jedes Peripheriegerät, das an den Workload angeschlossen ist.
  - **Gerät / Externes Storage** – ein Wechsellaufwerk oder umgeleitetes Netzlaufwerk, das mit dem Workload verbunden ist.
  - **Gerät / Verschlüsseltes Wechsellaufwerk** – ein Wechselmedium, das mit BitLocker To Go verschlüsselt wurde.
  - **Gerät / Umgeleitete Zwischenablage** – eine umgeleitete Zwischenablage, die mit dem Workload verbunden ist.
  - **Drucker** – jeder lokale oder Netzwerk-Drucker, der an den Workload angeschlossen ist.
- **Berechtigung** – eine präventive Kontrolle, die bei einer Datenübertragung durchgesetzt wird, die von dieser Regel kontrolliert wird. Dies wird ausführlicher im Abschnitt 'Berechtigungen in Datenfluss-Richtlinienregeln' erläutert.
- **Aktion** – eine nicht präventive Aktion, die durchgeführt wird, wenn diese Regel ausgelöst wird. Das Feld ist standardmäßig auf 'Keine Aktion' festgelegt. Folgende Optionen sind verfügbar:
  - **In Protokoll schreiben** – speichert einen Ereigniseintrag in das Überwachungsprotokoll, wenn die Regel ausgelöst wird.

- **Den Endbenutzer benachrichtigen, wenn eine Datenübertragung verweigert wird** – benachrichtigt den Anwender mit einer Echtzeit-Warnung auf dem Bildschirm, wenn er die Regel auslöst.
- **Einen Alarm generieren** – alarmiert den Administrator, wenn die Regel ausgelöst wird.

Warnung!
Wenn die Option **Keine Aktion** ausgewählt ist und die Regel ausgelöst wird:

- wird dem Überwachungsprotokoll kein Ereignisdatensatz hinzugefügt;
- wird keine Alarmmeldung an den Administrator gesendet;
- wird dem Endanwender keine Benachrichtigung auf dem Bildschirm angezeigt.

Wodurch wird eine Richtlinienregel ausgelöst?

Eine Datenübertragung passt zu einer Datenfluss-Richtlinienregel, wenn alle folgenden Bedingungen erfüllt sind:

- Alle Absender dieser Datenübertragung sind im Feld **Absender** der Regel spezifiziert oder gehören zu einer entsprechenden Benutzergruppe.
- Alle Empfänger dieser Datenübertragung sind im Feld **Empfänger** der Regel spezifiziert oder gehören zu einer entsprechenden Benutzergruppe.
- Die übertragenen Daten gehören zu der **Vertraulichkeitskategorie** der Regel.

Die Berechtigungen in Datenfluss-Richtlinienregeln anpassen

Die Advanced Data Loss Prevention-Funktionalität unterstützt drei Arten von Berechtigungen in den Datenfluss-Richtlinienregeln. Die Berechtigungen werden in jeder Regel der Richtlinie einzeln konfiguriert.

Erlauben (zulassend)	Datenübertragungen, die der in der Regel definierten Kombination aus Vertraulichkeitskategorie, Absender und Empfänger entsprechen, werden zugelassen.
Ausnahme (verbietend)	Datenübertragungen, die der in der Regel definierten Kombination aus Vertraulichkeitskategorie, Absender und Empfänger entsprechen, werden nicht zugelassen, aber der Absender kann eine Ausnahme zur Regel beantragen, um eine bestimmte Übertragung zuzulassen. **Wichtig** Alle nachfolgenden Datenübertragungen zwischen diesem Absender und Empfänger für diese Vertraulichkeitskategorie werden für die Dauer von fünf Minuten nach Übermittlung der Ausnahme zugelassen.
Verweigern (verbietend)	Datenübertragungen, die der in der Regel definierten Kombination aus Vertraulichkeitskategorie, Absender und Empfänger entsprechen, werden nicht zugelassen und der Absender hat keine Möglichkeit, eine Ausnahme zu übermitteln.

Darüber hinaus kann den Berechtigungen **Erlauben** und **Ausnahme** eine Prioritätskennzeichnung zugewiesen werden, um die Flexibilität der Richtlinienverwaltung zu erhöhen. Mit dieser Einstellung können Sie die Berechtigungen überschreiben, die für bestimmte Gruppen in anderen Datenfluss-Regeln der Richtlinie festgelegt wurden. Sie können diese Einstellung verwenden, um die Datenfluss-Regel einer Gruppe nur auf einige ihrer Mitglieder anzuwenden. Um dies zu erreichen, müssen Sie eine Datenfluss-Regel für bestimmte Benutzer erstellen, die Sie von den Gruppenregeln ausschließen wollen, und anschließend deren Berechtigungen gegenüber den Datenfluss-Beschränkungen priorisieren, die in den Regeln für die Gruppe konfiguriert sind, zu der diese Benutzer gehören. Weitere Informationen über die Priorisierung von Berechtigungen beim Kombinieren von Regeln finden Sie unter '"Datenfluss-Richtlinienregeln kombinieren" (S. 957)'.

Wichtig
Bevor Sie eine Firmen- oder Abteilungsrichtlinie vom Beobachtungs- auf den Erzwingungsmodus umstellen, müssen Sie unbedingt die Standardregeln für jede Vertraulichkeitskategorie von einem zulassenden auf ein verbietendes Stadium umstellen. Standardregeln sind in der Ansicht **Datenfluss-Richtlinie** mit einem Sternchen (*) gekennzeichnet. Weitere Informationen zu den Arten von Richtlinienregeln finden Sie in der Grundlagen-Anleitung.

So können Sie Berechtigungen in Richtlinienregeln bearbeiten

1. Melden Sie sich als Administrator an der Cyber Protect-Konsole an.
2. Gehen Sie zu **Schutz** –> **Datenfluss-Richtlinie**.
3. Wählen Sie die zu bearbeitende Richtlinie aus und klicken Sie oberhalb der Regelliste auf den Befehl **Bearbeiten**.
   Daraufhin wird das Fenster **Datenfluss-Regel bearbeiten** geöffnet.
4. Wählen Sie im Bereich **Berechtigung** die Option **Erlauben**, **Ausnahme** oder **Verweigern**.
5. (Optional) Wenn Sie die Berechtigung **Erlauben** oder **Ausnahme** für diese Regel gegenüber den Berechtigungen in anderen Regeln priorisieren wollen, müssen Sie das Kontrollkästchen **Priorisieren** aktivieren.
   Sie müssen dieses Kontrollkästchen nicht verwenden, um einer Datenfluss-Regel gegenüber der Standardregel 'Alle –> Andere' Vorrang einzuräumen, weil diese in der Richtlinie standardmäßig die niedrigste Priorität hat.
   Weitere Informationen über die Priorisierung von Berechtigungen beim Kombinieren von Regeln finden Sie unter '"Datenfluss-Richtlinienregeln kombinieren" (S. 957)'.
6. (Optional) Wählen Sie eine Aktion aus, die ausgeführt werden soll, wenn die Regel aktiviert wird.
7. Speichern Sie die Änderungen an der Richtlinienregel.

Datenfluss-Richtlinienregeln kombinieren

Wenn eine Datenübertragung zu mehr als einer Regel passt, werden die Berechtigungen und Aktionen, die für alle Regeln konfiguriert wurden, kombiniert und wie nachstehend beschrieben angewendet.

Berechtigungen

Wenn die Datenübertragung zu mehr als einer Regel passt und diese Regeln unterschiedliche Berechtigungen für dieselbe Datenkategorie haben, hat die Regel mit der höheren Priorität Vorrang – wobei folgende Prioritätenliste (in absteigender Reihenfolge) angewendet wird:

1. Ausnahme mit der Kennzeichnung **Priorisiert**
2. Erlauben mit der Kennzeichnung **Priorisiert**
3. Verweigern
4. Ausnahme
5. Erlauben

Wenn die Datenübertragung zu mehr als einer Regel passt und diese Regeln unterschiedliche Berechtigungen für verschiedene Datenkategorien haben, wird folgende Logik für die Überschreibung angewendet:

1. Die restriktivste Regelberechtigung wird für jede der Vertraulichkeitskategorien definiert, auf die die Datenübertragung zutrifft.
2. Es wird die restriktivste der Regelberechtigungen, die in Punkt 1 definiert ist, durchgesetzt.

Beispiel

Eine Dateiübertragung entspricht folgendermaßen drei Regeln in verschiedenen Vertraulichkeitskategorien:

Vertraulichkeitskategorie	Berechtigung
PII	Erlauben - Priorisiert
PHI	Ausnahme - Priorisiert
PCI	Verweigern

Die Berechtigung, die angewendet wird, lautet 'Verweigern'.

Aktionen

Wenn eine Datenübertragung auf mehr als eine Regel zutrifft und für diese Regeln unterschiedliche Optionen im Feld **Aktion** konfiguriert sind, werden alle konfigurierten Aktionen in allen ausgelösten Regeln ausgeführt.

Richtlinien-Überprüfung und -Verwaltung

Bevor die automatisch erstellte grundlegende Datenfluss-Richtlinie durchgesetzt wird, muss sie vom Kunden überprüft, validiert und genehmigt werden, weil nur er alle Besonderheiten seiner Geschäftsprozesse kennt und beurteilen kann, ob diese in der grundlegenden Richtlinie konsistent berücksichtigt werden. Außerdem kann der Kunde Ungenauigkeiten feststellen, die dann vom Partner-Administrator behoben werden können.

Während der Richtlinien-Überprüfung präsentiert der Partner-Administrator die grundlegende Datenfluss-Richtlinie dem Kunden, der jeden Datenfluss in der Richtlinie überprüfen und deren Konsistenz mit seinen Geschäftsprozessen validieren sollte. Für die Validierung sind keine besonderen technischen Kenntnisse erforderlich, weil die Darstellung der Richtlinienregeln in der Cyber Protect-Konsole intuitiv verständlich ist: jede Regel beschreibt, wer der Absender und der Empfänger eines sensiblen Datenflusses ist.

Basierend auf den Anweisungen des Kunden kann der Partner-Administrator die Basisrichtlinie manuell anpassen, indem er Datenfluss-Richtlinienregeln nach Bedarf bearbeitet, löscht oder erstellt. Nach der Genehmigung durch den Kunden wird die überprüfte Richtlinie für geschützte Workloads durchgesetzt, indem der Schutzplan, der auf diese Workloads angewendet wird, in den Erzwingungsmodus umgeschaltet wird.

Vor der Erzwingung einer überprüften Richtlinie ist es wichtig, in allen automatisch erstellten Standard-Richtlinienregeln für sensible Datenkategorien die Berechtigung **Erlauben** auf **Verweigern** oder **Ausnahme** zu ändern. Die Berechtigung **Verweigern** kann von den Benutzern nicht übergangen werden, während die Berechtigung **Ausnahme** eine Übertragung blockiert, die der Regel entspricht, es den Benutzern aber erlaubt, diese Blockierung in einer Notsituation aufzuheben, indem sie eine geschäftsbezogene Ausnahme beantragen.

Erneuerung der Datenfluss-Richtlinie

Wenn sich der Geschäftsprozess des Unternehmens oder seiner Abteilungen erheblich geändert hat, müssen die entsprechenden DLP-Richtlinien erneuert werden, damit diese zu den Änderungen der sensiblen Datenflüsse des aktualisierten Geschäftsprozesses kompatibel sind. Eine Richtlinienerneuerung ist auch dann erforderlich, wenn sich das Aufgabengebiet eines Mitarbeiters ändert. In diesem Fall muss auch der Teil der Abteilungsrichtlinie erneuert werden, der den Workload des Mitarbeiters schützt.

Der Workflow für die Verwaltung der Advanced DLP-Richtlinien ermöglicht es Administratoren, die Richtlinien für das gesamte Unternehmen, eine Abteilung, einen Benutzer oder auch nur einen Teil der Benutzer innerhalb einer Abteilung automatisch zu erneuern.

Die Richtlinie für eine Firma oder Abteilung erneuern

Alle Optionen des Beobachtungsmodus können verwendet werden, um eine firmen- oder abteilungsweite Richtlinie zu erneuern. Ebenso kann auch nur ein Teil einer Abteilungsrichtlinie für einen oder mehrere Benutzer innerhalb einer Abteilung erneuert werden.

So können Sie die Richtlinie für eine Firma oder Abteilung erneuern

Der Erneuerungsprozess besteht aus folgenden Schritten, die von einem Firmenadministrator oder einem Partner, der die Firmen-Workloads verwaltet, durchgeführt werden müssen.

1. Löschen Sie alle nicht standardmäßigen Regeln in der erzwungenen Richtlinie.
2. Wenn Sie die Erneuerung starten wollen, schalten Sie den Schutzplan mit der Advanced DLP-Funktionalität, der auf die Firma oder Abteilung angewendet wird, auf eine der

Beobachtungsmodus-Optionen um (je nachdem, welche für diese bestimmte Firma oder Abteilung optimal ist) und wenden Sie den Plan dann auf alle Workloads in der Firma oder Abteilung an.

3. Überprüfen Sie nach Ablauf des Erneuerungszeitraums die neue Firmen- oder Abteilungsrichtlinie mit dem Kunden, passen Sie die Richtlinie gegebenenfalls an und lassen Sie sie vom Kunden genehmigen.
4. Schalten Sie den Schutzplan, der auf die Firmen- oder Abteilungs-Workloads angewendet wird, auf eine geeignete Erzwingungsmodus-Option um, die der Kunde für optimal hält, um das nicht autorisierte Abfließen von Daten aus den Workloads der Abteilung zu verhindern.

Die Richtlinie für einen oder mehrere Benutzer in der Firma oder Abteilung erneuern

Richtlinien auf Benutzerebene können mithilfe einer beliebigen Option des Beobachtungsmodus (und auch das adaptiven Erzwingungsmodus) erneuert werden.

Den Beobachtungsmodus zur Erneuerung einer Benutzerrichtlinie verwenden

Bei Verwendung des Beobachtungsmodus zur Erneuerung einer Richtlinie für einen bestimmten Benutzer oder einen Teil der Benutzer in einer Firma (oder Abteilung) gelten folgende Besonderheiten: Die Datenfluss-Richtlinie, die für die gesamte Firma (oder Abteilung) gilt, wird nicht für Datenübertragungen von Benutzern während des Verlängerungszeitraums durchgesetzt. Dadurch können bei der Erneuerung neue individuelle Regeln für den Benutzer erstellt werden, die im Widerspruch zu bestehenden Gruppenregeln in der erzwungenen Richtlinie für die Firma (oder Abteilung) stehen oder mit diesen übereinstimmen könnten. Nachdem die Erneuerung abgeschlossen wurde und die Richtlinie für die Datenübertragungen des Benutzers wieder in Kraft gesetzt ist, hängt es von ihren Prioritäten im Vergleich zu anderen Regeln in der Richtlinie, die zu diesen Datenübertragungen passen, ab, ob diese neuen individuellen Regeln, die für den Benutzer erstellt wurden, tatsächlich auf die Datenübertragungen des Benutzers angewendet werden oder nicht.

So können Sie die Richtlinie für einen Benutzer im Beobachtungsmodus erneuern

Der Erneuerungsprozess besteht aus folgenden Schritten, die von einem Firmenadministrator oder einem Partner, der die Firmen-Workloads verwaltet, durchgeführt werden müssen.

1. Löschen Sie alle nicht standardmäßigen Regeln in der für die Firma (oder Abteilung) erzwungenen Richtlinie, bei denen der Benutzer der einzige Absender ist.
2. Entfernen Sie den Benutzer aus den Absenderlisten aller nicht standardmäßigen Datenfluss-Regeln in der erzwungenen Richtlinie.
3. Erstellen Sie einen neuen Schutzplan mit der Advanced DLP-Funktionalität im Beobachtungsmodus und wenden Sie ihn auf den Workload des Benutzers an, um den Erneuerungs- bzw. Beobachtungszeitraum zu starten.
   Die Dauer des Erneuerungszeitraums hängt davon ab, wie lange es dauern kann, bis der Benutzer alle oder zumindest 90-95% seiner üblichen Geschäftsaktivitäten durchgeführt hat, bei denen sensible Daten aus seinen Workloads übertragen werden.

4. Überprüfen Sie nach Ablauf des Erneuerungszeitraums die neuen mit diesem Benutzer verbundenen Regeln, die der erzwungenen Richtlinie hinzugefügt wurden, passen Sie diese bei Bedarf an und lassen Sie sie vom Kunden genehmigen.
5. Schalten Sie den auf den Workload des Benutzers angewendeten Schutzplan auf den Modus **Strikte Erzwingung** oder den Modus **Adaptive Erzwingung** um – je nachdem, welche Option der Kunde als optimal erachtet, um das unautorisierte Abfließen von sensiblen Daten aus dem Benutzer-Workload zu verhindern.
   Alternativ können Sie auch den Schutzplan, der bisher auf die Firma (oder Abteilung) angewendet wurde, erneut auf den Workload des Benutzers anwenden.

Den adaptiven Erzwingungsmodus zur Erneuerung einer Benutzerrichtlinie verwenden

Die Richtlinienerneuerung für einen einzelnen Benutzer oder einen Teil aller Benutzer in der Firma (oder Abteilung) kann über den adaptiven Erzwingungsmodus eines Schutzplans mit aktivierter Advanced DLP-Funktionalität durchgeführt werden, der auf den Workload des Benutzers angewendet wird.

Hinweis
Für diese Richtlinienerneuerungsmethode gelten folgende Besonderheiten: die erzwungenen Firmen- bzw. Abteilungsrichtlinien für Absendergruppen, denen der Benutzer angehört (d.h. jede interne), werden auch für Datenübertragungen von diesem Benutzer während der Erneuerung erzwungen. Daher wird die Erneuerung keine neuen individuellen Regeln für den Benutzer erstellen, die im Widerspruch zu bereits bestehenden Richtlinienregeln für Absendergruppen stehen oder mit diesen übereinstimmen. Welche dieser beiden Methoden für die Erneuerung von Benutzer-Richtlinien für einen bestimmten Kunden effektiver ist, hängt von dessen spezifischen IT-Sicherheitsanforderungen ab.

So können Sie die Richtlinie für einen Benutzer im adaptiven Erzwingungsmodus erneuern

Der Erneuerungsprozess besteht aus folgenden Schritten, die von einem Firmenadministrator oder einem Partner, der die Firmen-Workloads verwaltet, durchgeführt werden müssen.

1. Löschen Sie alle nicht standardmäßigen Regeln in der für die Firma bzw. Abteilung erzwungenen Richtlinie, bei denen der Benutzer der einzige Absender ist.
2. Entfernen Sie den Benutzer aus den Absenderlisten aller nicht standardmäßigen Datenfluss-Regeln in der erzwungenen Richtlinie.
3. Setzen Sie für alle Standardregeln in der für die Firma (oder Abteilung) erzwungenen Richtlinie die Berechtigung auf **Ausnahme** – und wählen Sie dann im Feld **Aktion** die Aktion **In Protokoll schreiben**.
4. Wenn der derzeit auf den Workload des Benutzers angewendete Schutzplan auf den Modus **Strikte Erzwingung** eingestellt ist, erstellen Sie einen neuen Schutzplan mit aktivierter Advanced DLP-Funktionalität und wenden Sie diesen im Modus **Adaptive Erzwingung** auf den Workload des Benutzers an, um den Erneuerungszeitraum zu starten.

Die Dauer des Erneuerungszeitraums hängt davon ab, wie lange es dauern kann, bis der Benutzer alle oder zumindest 90-95% seiner üblichen Geschäftsaktivitäten durchgeführt hat, bei denen sensible Daten aus seinen Workloads übertragen werden.

5. Überprüfen Sie nach Ablauf des Erneuerungszeitraums die neuen mit diesem Benutzer verbundenen Regeln, die der erzwungenen Richtlinie hinzugefügt wurden, passen Sie diese bei Bedarf an und lassen Sie sie vom Kunden genehmigen.
6. Schalten Sie den auf den Workload des Benutzers angewendeten Schutzplan auf den Modus **Strikte Erzwingung** um oder lassen Sie ihn im Modus **Adaptive Erzwingung** – je nachdem, welche Option der Kunde als optimal erachtet, um das unautorisierte Abfließen von sensiblen Daten aus dem Benutzer-Workload zu verhindern.
   Alternativ können Sie auch den Schutzplan, der bisher auf die Firma (oder Abteilung) angewendet wurde, erneut auf den Workload des Benutzers anwenden.

Die Advanced Data Loss Prevention-Funktionalität in Schutzplänen aktivieren

Die Advanced Data Loss Prevention-Funktionen können in jeden Schutzplan für einen Kunden-Mandanten aufgenommen werden, wenn der Protection Service und das Advanced Data Loss Prevention-Paket für diesen Kunden aktiviert sind.

Die Advanced DLP-Funktionalität ist das Advanced-Modul der Data Loss Prevention-Funktionsgruppe. Die Advanced DLP-Funktionen und die Gerätekontrolle können unabhängig voneinander oder gemeinsam verwendet werden (in einem einzigen Schutzplan oder in zwei Plänen zum Schutz desselben Workloads). Wenn sie gemeinsam verwendet werden, sind ihre funktionalen Fähigkeiten folgendermaßen aufeinander abgestimmt.

- Die Gerätekontrolle beendet die Überwachung von Benutzerzugriffen auf solche lokalen Kanäle, in denen die Advanced DLP-Funktionalität die Inhalte von übertragenen Daten überprüft. Die Gerätekontrolle behält jedoch die Kontrolle über die nachfolgenden Gerätetypen, wenn der Zugriff auf diese als 'Nur Lesen' oder 'Verweigert' konfiguriert ist:
  - Wechsellaufwerk
  - Verschlüsseltes Wechsellaufwerk
  - Netzlaufwerk

  Wenn Sie beispielsweise sowohl die Gerätekontrolle als auch die Advanced DLP-Funktionalität in einem einzigen Schutzplan oder in zwei Plänen aktiviert haben, um denselben Workload zu schützen, und Sie in der Gerätekontrolle den Nur-Lesen-Zugriff für USB-Geräte konfiguriert haben, wird der Nur-Lesen-Zugriff unabhängig von den Zugriffseinstellungen im Advanced DLP-Modul auf alle USB-Geräte (mit Ausnahme solcher, die auf der Positivliste stehen) angewendet. Wenn in der Gerätekontrolle die Standardeinstellung 'Zugriff aktivieren' konfiguriert ist, wird die Zugriffseinstellung in der Advanced DLP-Funktionalität übernommen.
- Der Benutzerzugriff auf folgende lokale Kanäle und Peripheriegeräte in der Positivliste wird von der Gerätekontrolle erzwungen:

- Optische Laufwerke
- Diskettenlaufwerke
- Über MTP angeschlossene Mobilgeräte
- Bluetooth-Adapter
- Windows-Zwischenablage
- Screenshot-Aufnahmen
- USB-Geräte und -Gerätetypen (außer für Wechsellaufwerke und verschlüsselte Laufwerke)

So können Sie einen Schutzplan mit Advanced DLP-Funktionalität erstellen

1. Wechseln Sie zu **Verwaltung** > **Schutzpläne**.
2. Klicken Sie auf **Plan erstellen**.
3. Erweitern Sie den Bereich **Data Loss Prevention** und klicken Sie auf die Zeile **Modus**.
   Das Dialogfenster **Modus** wird geöffnet.
   - Wenn Sie das Erstellen oder Erneuern der Datenfluss-Richtlinie starten wollen, wählen Sie zuerst den **Beobachtungsmodus** und bestimmen Sie anschließend, wie die Datenübertragungen verarbeitet werden sollen:

Option	Beschreibung
Alle erlauben	Alle Übertragungen von sensiblen Daten aus Benutzer-Workloads werden als geschäftlich notwendig und sicher behandelt. Für jeden erkannten Datenfluss, der nicht mit einer bereits definierten Regel in der Richtlinie übereinstimmt, wird eine neue Regel erstellt.
Alle rechtfertigen	Alle Übertragungen von sensiblen Daten aus Benutzer-Workloads werden zwar als geschäftlich notwendig, aber auch riskant behandelt. Daher muss der Benutzer bei jeder abgefangenen Übertragung sensibler Daten an einen beliebigen Empfänger oder ein beliebiges Ziel innerhalb oder außerhalb des Unternehmens, die nicht mit einer zuvor erstellten Datenfluss-Regel übereinstimmt, eine einmalige geschäftliche Rechtfertigung abgeben. Wenn die Rechtfertigung übermittelt wird, wird in der Datenfluss-Richtlinie eine neue Datenfluss-Regel erstellt.
Gemischt	Die Logik 'Alle erlauben' wird auf alle internen Übertragungen von sensiblen Daten angewendet – und die Logik 'Alle rechtfertigen' auf alle externen Übertragungen von sensiblen Daten. Zur Definition der internen Ziele siehe '"Automatisierte Erkennung des Ziels" (S. 966)'.

Warnung!

- Wählen Sie den **Beobachtungsmodus** nur, wenn Sie bisher noch keine Datenfluss-Richtlinie erstellt haben oder wenn Sie die Richtlinie erneuern wollen. Bevor Sie mit der Richtlinienerneuerung beginnen, sollten Sie '"Erneuerung der Datenfluss-Richtlinie" (S. 959)' lesen.
- Im Beobachtungsmodus werden keine Datenlecks verhindert. Siehe auch den Abschnitt Beobachtungsmodus in der Grundlagen-Anleitung.

- Wenn Sie die bestehende Datenfluss-Richtlinie erzwingen wollen, wählen Sie zuerst den **Erzwingungsmodus** aus und bestimmen Sie anschließend, wie streng die Datenfluss-Richtlinienregeln durchgesetzt werden sollen:

Option	Beschreibung
Strikte Erzwingung	Die Datenfluss-Richtlinie wird wie vorliegend durchgesetzt und nicht mit neuen zulassenden Richtlinienregeln erweitert, wenn bisher noch nicht beobachtete sensible Datenflüsse entdeckt werden sollten. Siehe auch den Abschnitt Strikte Erzwingung in der Grundlagen-Anleitung.
Adaptive Erzwingung (Erzwingung mit Lernen)	Die erzwungene Richtlinie passt sich weiterhin automatisch an solche Geschäftsaktivitäten an, die während des Beobachtungszeitraums nicht durchgeführt wurden, oder an geänderte Geschäftsprozesse. Mit diesem Modus kann die erzwungene Datenfluss-Richtlinie basierend auf neu erlernten Datenflüssen, die auf den Workloads erkannt wurden, erweitert werden. Siehe auch den Abschnitt Adaptive Erzwingung in der Grundlagen-Anleitung.

Wichtig
Bevor Sie eine Firmen- oder Abteilungsrichtlinie vom Beobachtungs- auf den Erzwingungsmodus umstellen, müssen Sie unbedingt die Standardregeln für jede Vertraulichkeitskategorie von einem zulassenden auf ein verbietendes Stadium umstellen. Standardregeln sind in der Ansicht **Datenfluss-Richtlinie** mit einem Sternchen (*) gekennzeichnet. Weitere Informationen zu den Arten von Richtlinienregeln finden Sie in der Grundlagen-Anleitung.

4. Klicken Sie auf **Fertig**, um das Dialogfenster 'Modus' zu schließen.
5. (Optional) Wenn Sie die optische Zeichenerkennung (OCR-Funktion), Positivlisten und weitere Schutzoptionen konfigurieren wollen, können Sie auf **Erweiterte Einstellungen** klicken. Informationen zu den verfügbaren Optionen finden Sie unter '"Erweiterte Einstellungen" (S. 964)'.
6. Speichern Sie den Schutzplan und wenden Sie ihn auf alle Workloads an, die Sie schützen wollen.

Erweiterte Einstellungen

Sie können die erweiterten Einstellungen in Schutzplänen mit aktivierter Advanced Data Loss Prevention-Funktionalität verwenden, um die Qualität der Daten-Inhaltsinspektion in Kanälen zu

erhöhen, die von der Advanced Data Loss Prevention-Funktionalität kontrolliert werden. Des Weiteren können Sie Datenübertragungen an Peripheriegerätetypen in der Positivliste, an Kategorien der Netzwerkkommunikation, an Ziel-Hosts sowie Datenübertragungen, die von Applikationen in der Positivliste initiiert wurden, von allen präventiven Kontrollen ausschließen. Sie können folgende erweiterte Einstellungen konfigurieren:

- **Optische Zeichenerkennung (OCR)**
  Mit dieser Einstellung wird die optische Zeichenerkennung (OCR) ein- bzw. ausgeschaltet, mit der aus grafischen Dateien und Bildern, die sich in Dokumenten, Nachrichten, Scans, Screenshots und anderen Objekten befinden, Textabschnitte in 31 Sprachen zur weiteren Inhaltsinspektion extrahiert werden können.
- **Übertragung von kennwortgeschützten Daten**
  Die Inhalte von kennwortgeschützten Archiven und Dokumenten können nicht inspiziert werden. Über diese Einstellung der Advanced DLP-Funktionalität können Administratoren festlegen, ob ausgehende Übertragungen von kennwortgeschützten Daten zugelassen oder blockiert werden sollen.
- **Datenübertragung bei Fehlern verhindern**
  Manchmal kann die Analyse von gesendeten Inhalten fehlschlagen oder es kann ein anderer Kontrollfehler bei Aktionen des DLP-Agenten auftreten. Wenn diese Option aktiviert ist, wird die Übertragung dann blockiert. Wenn die Option deaktiviert ist, wird die Übertragung auch bei einem aufgetretenen Fehler zugelassen.
- **Positivliste für Gerätetypen und Netzwerk-Kommunikationen**
  Datenübertragungen an diejenigen Peripheriegeräte und innerhalb der Netzwerk-Kommunikationen, die in dieser Liste ausgewählt sind, werden unabhängig von ihrer Datenvertraulichkeit und der erzwungenen Datenfluss-Richtlinie zugelassen.

  Warnung!
  Diese Option wird verwendet, wenn es Probleme mit einem bestimmten Gerätetyp oder Protokoll gibt. Sie sollten diese Option nicht aktivieren, außer Sie werden von einem Support-Mitarbeiter dazu aufgefordert.

- **Positivliste für Remote-Hosts**
  Datenübertragungen zu denjenigen Ziel-Hosts, die in dieser Liste spezifiziert sind, werden unabhängig von ihrer Datenvertraulichkeit und der erzwungenen Datenfluss-Richtlinie zugelassen.
- **Positivliste für Applikationen**
  Datenübertragungen, die von den in dieser Liste spezifizierten Applikationen durchgeführt werden, werden unabhängig von ihrer Datenvertraulichkeit und der erzwungenen Datenfluss-Richtlinie zugelassen.

Der **Sicherheitsstufe**-Indikator der erweiterten Einstellungen, der in der Ansicht **Schutzplan erstellen** und in der Ansicht 'Details' eines Schutzplans angezeigt wird, verwendet folgende Logik für die Auswahl der verschiedenen Sicherheitsstufen:

- **Standard** – zeigt an, dass keine der erweiterten Einstellungen eingeschaltet ist.
- **Moderat** – zeigt an, dass eine oder mehrere Einstellung eingeschaltet ist, wobei jedoch nicht die Kombination aus **OCR**, **Übertragung von kennwortgeschützten Daten** und **Datenübertragung bei Fehlern verhindern** aktiviert ist.
- **Strikt** – dass mindestens die Kombination aus **OCR**, **Übertragung von kennwortgeschützten Daten** und **Datenübertragung bei Fehlern verhindern** aktiviert ist.

Automatisierte Erkennung des Ziels

Beim Modus 'Gemischte Beobachtung' wendet die Advanced Data Loss Prevention-Funktionalität unterschiedliche Regeln an, je nachdem, wohin die erkannte Datenübertragung geht (intern oder extern). Die Logik zur Bestimmung eines internen Ziels wird nachfolgend erläutert. Alle anderen Ziele werden als extern betrachtet.

Bei jeder abgefangenen Datenübertragung erkennt die Advanced Data Loss Prevention-Funktionalität automatisch, ob es sich bei dem HTTP-, FTP- oder SMB-Zielserver um einen internen Server handelt, indem sie eine DNS-Anfrage durchführt und die FQDN-Namen der Maschine, auf welcher der Data Loss Prevention Agent läuft, und des Remote-Servers vergleicht. Wenn die DNS-Anfrage fehlschlägt, wird zudem überprüft, ob sich der geschützte Workload und der Remote-Server im selben Netzwerk befinden. Server, die den gleichen Domain-Namen haben (oder die sich im selben Subnetz befinden) wie die Maschine, auf welcher der Data Loss Prevention Agent läuft, werden als intern betrachtet.

Bei E-Mail-Kommunikationen behandelt die Advanced Data Loss Prevention-Funktionalität alle E-Mails als interne Übertragungen, die von einer Unternehmens-E-Mail-Adresse unter Verwendung des Unternehmens-Mailservers gesendet werden, sofern sich die Empfänger-E-Mail in derselben Domain befindet wie die Absender-E-Mail und der Name des Empfänger-Mailservers derselbe ist.

Nicht-unternehmensbezogene E-Mails werden als externe Mitteilungen behandelt, außer wenn das Empfängerkonto bekannt ist. Bekannte E-Mail-Adressen werden aktualisiert, da die Data Loss Prevention-Funktionalität die Benutzeraktivitäten im Netzwerk überwacht und die Datenbank im Backend mit den Daten der mit dem Benutzer verbundenen E-Mail-Adressen aktualisiert.

Mitteilungen über Messenger werden als externe Mitteilungen behandelt, außer wenn das Empfängerkonto bekannt ist. Bekannte Konten werden aktualisiert, da die Data Loss Prevention-Funktionalität die Benutzeraktivitäten im Netzwerk überwacht und die Datenbank im Backend mit den Daten der mit dem Benutzer verbundenen Konten aktualisiert.

Definitionen von sensiblen Daten

Dieser Abschnitt beschreibt die Logik, anhand derer sensible Daten bei der Inhaltsanalyse identifiziert werden.

Um die Anzahl von Falsch-Positiv-Erkennungen zu reduzieren, werden identische Übereinstimmungen für alle Gruppen der beschriebenen logischen Ausdrücke als eine Übereinstimmung gezählt.

Wichtig
Die logischen Ausdrücke, die zur Inhaltsidentifizierung verwendet werden, dienen nur der Information und beschreiben die Lösung nicht in allen Einzelheiten.

Geschützte Gesundheitsinformationen (PHI)

Unterstützte Sprachen

- US, GB, Englisch-International
- Finnisch
- Italienisch
- Französisch
- Polnisch
- Russisch
- Ungarisch
- Norwegisch
- Spanisch

Daten, die als geschützte Gesundheitsinformationen gelten

Folgende Daten gelten als geschützte Gesundheitsinformationen.

- Vor- und Nachnamen
- Adresse (Straße, Stadt, Landkreis, Bezirk, Postleitzahl und entsprechende Geocodes)
- Telefonnummern
- E-Mail-Adressen
- Sozialversicherungsnummern
- Krankenversicherungsnummern
- Bankkontonummern
- URLs
- IP-Adressnummern
- ICD-10-CM-Codes
- ICD-10-PCS-and-GEMs
- HIPAA
- Andere gesundheitsbezogene Daten
- Kreditkartennummern

Logischer Ausdruck, der zur Inhaltserkennung verwendet wird

Der logische Ausdruck besteht aus folgenden Zeichenfolgen, die über den logischen Operator OR verbunden werden. Der Operator OR wird verwendet, um verschiedene Datengruppen in der oberen Liste zu verbinden, wenn der logische Operator AND nicht explizit spezifiziert wurde. Die Zahlen in Klammern geben die Anzahl der erkannten Instanzen an, die ein positives Erkennungsergebnis liefern würden.

- **Sozialversicherungsnummern** (5)
- (Vor- und Nachnamen (3) OR Adresse (3) OR Telefonnummern (3) OR E-Mail-Adresse (3) OR Bankkontonummern (3) OR Kreditkartennummern (3)) AND (Sozialversicherungsnummern (3) OR Krankenversicherungsnummern (3) * OR ICD-10-CM-Codes (3) OR ICD-10-PCS-and-GEMs (3) OR HIPAA (3) OR * Andere gesundheitsbezogene Daten (3))

Personenbezogene Informationen (PII)

Unterstützte Sprachen

- US, GB, Englisch-International
- Bulgarisch
- Chinesisch
- Tschechisch
- Dänisch
- Niederländisch
- Finnisch
- Französisch
- Deutsch
- Ungarisch
- Indonesisch
- Italienisch
- Koreanisch
- Malaysisch
- Norwegisch
- Polnisch
- Portugiesisch (Brasilien)
- Portugiesisch (Portugal)
- Rumänisch
- Russisch

- Serbisch
- Singapur
- Spanisch
- Schwedisch
- Taiwan
- Türkisch
- Thailändisch
- Japanisch

Daten, die als personenbezogene Informationen (PII) gelten

- Vor- und Nachnamen
- Adresse (Straße, Stadt, Landkreis, Postleitzahl)
- Bankkontonummern
- Personen- und Steueridentifikationsnummern
- Reisepassnummern
- Sozialversicherungsnummern
- Telefonnummern
- Autokennzeichen
- Führerscheinnummern
- IDs und Seriennummern
- IP-Adressen
- E-Mail-Adressen
- Kreditkartennummern

Logischer Ausdruck, der zur Inhaltserkennung verwendet wird

Logischer Ausdruck für alle unterstützten Sprachen (außer Japanisch)

Der logische Ausdruck besteht aus folgenden Zeichenfolgen, die über die logischen Operatoren OR oder AND verknüpft werden. Die Zahlen in Klammern geben die Anzahl der erkannten Instanzen an, die ein positives Erkennungsergebnis liefern würden.

- Personen- und Steueridentifikationsnummern (5)
- Vor- und Nachnamen (3) AND **(**Kreditkartennummer (3) OR Sozialversicherungsnummer (3) OR Bankkontonummer (3) OR Personen- und Steueridentifikationsnummern (3) OR Führerscheinnummern (3) OR Reisepassnummern (3) OR Sozialversicherungsnummern (3) OR IP-Adressen (3) OR Autokennzeichen (3) OR IDs und Seriennummern**)**

- Telefonnummern (3) AND **(**Kreditkartennummer (3) OR Sozialversicherungsnummer (3) OR Bankkontonummer (3) OR Adresse (3) OR Personen- und Steueridentifikationsnummern (3) OR Führerscheinnummern (3) OR Reisepassnummern (3) OR Sozialversicherungsnummern (3) OR Autokennzeichen (3) OR IDs und Seriennummern (3)**)**
- **(**Vornamen und Nachnamen (30) OR Adresse (30)**)** AND **(**E-Mail-Adressen (30) OR Telefonnummern (30) OR IP-Adressen (30) OR Adresse (30)**)**
- E-Mail-Adressen (3) AND **(**Kreditkartennummer (3) OR Sozialversicherungsnummer (3) OR Bankkontonummer (3) OR Personen- und Steueridentifikationsnummern (3) OR Führerscheinnummern (3) OR Reisepassnummern (3) OR Sozialversicherungsnummern (3) OR Autokennzeichen (3) OR IDs und Seriennummern (3)**)**
- E-Mail-Adresse (30) AND **(**Adresse (30) OR Telefonnummern (30)**)**
- Vor- und Nachnamen (30) AND Adresse (30)
- Telefonnummern (30) AND Adresse (30)
- Vor- und Nachnamen (3) AND Bankkontonummern (3)
- Telefonnummern (3) AND **(**Kreditkartennummer (3) OR Bankkontonummer (3) OR Sozialversicherungsnummern (3) OR Personen- und Steueridentifikationsnummern (3) OR Führerscheinnummern (3) OR Reisepassnummern (3)**)**

Logischer Ausdruck für Japanisch

Hinweis
Es werden nur eindeutige Übereinstimmungen bei der Inhaltserkennung gezählt.

Der logische Ausdruck besteht aus folgenden Zeichenfolgen, die über den logischen Operator OR verknüpft werden. Der Operator OR wird verwendet, um unterschiedliche Gruppen zu verbinden, wenn der logische Operator AND nicht explizit spezifiziert wurde.

- Sozialversicherungsnummern (5)
- Vor- und Nachnamen (3) AND **(**Kreditkartennummer (3) OR Bankkontonummer (3) OR Führerscheinnummern (3) OR Reisepassnummern (3) OR Sozialversicherungsnummern (3)**)**
- Vor- und Nachnamen (30) AND **(**E-Mail-Adressen (30) OR Telefonnummern (30) OR IP-Adressen (30) OR Adresse (30)**)**
- Adresse (3) AND **(**Kreditkartennummer (3) OR Bankkontonummer (3) OR Führerscheinnummern (3) OR Reisepassnummern (3) OR Sozialversicherungsnummern (3)**)**
- E-Mail-Adresse (3) AND **(**Kreditkartennummer (3) OR Bankkontonummer (3) OR Sozialversicherungsnummern (3) OR Führerscheinnummern (3)**)**
- Adresse (5) AND **(**E-Mail-Adresse (5) OR Vor- und Nachnamen (5) OR Telefonnummern (5) OR IP-Adressen (5)**)**
- Vor- und Nachnamen (3) AND Bankkontonummern (3)
- Telefonnummern (3) AND **(**Kreditkartennummer (3) OR Bankkontonummer (3) OR Adresse (3) OR Sozialversicherungsnummern (3) OR Führerscheinnummern (3)**)**

Kreditkartenindustrie-Datensicherheitsstandard (PCI DSS)

Unterstützte Sprachen

Diese Vertraulichkeitsgruppe ist sprachunabhängig. Die PCI DSS-Daten sind in allen Ländern auf Englisch.

Daten, die als PCI DSS-Daten (Kreditkartentransaktionsdaten) gelten

- Daten des Karteninhabers
  - Primäre Kontonummer (PAN)
  - Name des Karteninhabers
  - Ablaufdatum
  - Service-Code
- Sensible Authentifizierungsdaten
  - Vollständige Nachverfolgungsdaten (Magnetstreifendaten oder entsprechende Daten auf einem Chip)
  - CAV2/CVC2/CVV2/CID
  - PINs/PIN-Blöcke

Logischer Ausdruck, der zur Inhaltserkennung verwendet wird

Der logische Ausdruck besteht aus folgenden Zeichenfolgen, die über den logischen Operator OR verknüpft werden. Die Zahlen in Klammern geben die Anzahl der erkannten Instanzen an, die ein positives Erkennungsergebnis liefern würden.

- Kreditkartennummer (5)
- Kreditkartennummer (3) AND (Amerikanischer Name (Ex) (3) OR Amerikanischer Name (3) OR PCI DSS-Schlüsselwörter (3) OR Datum (Monat/Jahr) (3))
- Kreditkarten-Dump (5)

Als vertraulich gekennzeichnet

Daten, die als vertraulich gekennzeichnet sind, werden über eine Schlüsselwortgruppe erkannt.

Die Übereinstimmungsbedingung ist gewichtungsbasiert und jedes Wort hat die Gewichtung == 1. Die Inhaltserkennung gilt als positiv, wenn die Übereinstimmung eine Gewichtung > 3 hat.

Unterstützte Sprachen

- Englisch
- Bulgarisch
- Chinesisch (Vereinfacht)

- Chinesisch (Traditionell)
- Tschechisch
- Dänisch
- Niederländisch
- Finnisch
- Französisch
- Deutsch
- Ungarisch
- Indonesisch
- Italienisch
- Japanisch
- Koreanisch
- Malaysisch
- Norwegisch
- Polnisch
- Portugiesisch (Brasilien)
- Portugiesisch (Portugal)
- Russisch
- Serbisch
- Spanisch
- Schwedisch
- Türkisch

Schlüsselwortgruppen

Die Schlüsselwortgruppe für jede Sprache enthält die länderspezifischen Entsprechungen der folgenden Schlüsselwörter, die für die englische Sprache verwendet werden (Groß-/Kleinschreibung wird nicht berücksichtigt).

- vertraulich
- interne Verteilung
- nicht zur Verteilung
- nicht verteilen
- nicht für die Öffentlichkeit
- nicht zur externen Verteilung
- nur zur internen Verwendung

- hochqualifizierte Dokumentation
- vertraulich
- privilegierte Informationen
- nur zur internen Verwendung
- nur zur offiziellen Verwendung

Data Loss Prevention-Ereignisse

Die Advanced Data Loss Prevention-Funktionalität generiert Ereignisse in der DLP-Ereignisanzeige nach folgenden Regeln:

- Im Beobachtungsmodus werden Ereignisse für alle gerechtfertigten Datenübertragungen generiert.
- Im Erzwingungsmodus werden Ereignisse auf Basis der für jede ausgelöste Richtlinienregel konfigurierten Aktion **In Protokoll schreiben** generiert.

So können Sie die Ereignisse für eine Regel in der Datenfluss-Richtlinie einsehen

1. Melden Sie sich als Administrator an der Cyber Protect-Konsole an.
2. Gehen Sie zu **Schutz** –> **Datenfluss-Richtlinie**.
3. Suchen Sie die Regel, für die Sie die Ereignisse sehen wollen, und klicken Sie am Ende der Regelzeile auf das Drei-Punkte-Symbol.
4. Wählen Sie **Ereignisse anzeigen**.

So können Sie Details über ein Ereignis in der DLP-Ereignisanzeige einsehen

1. Melden Sie sich als Administrator an der Cyber Protect-Konsole an.
2. Wechseln Sie zu **Schutz** -> **DLP-Ereignisse**.
3. Klicken Sie auf ein Ereignis in der Liste, um weitere Details zu erhalten.
   Der Fensterbereich mit den Ereignisdetails wird rechts erweitert.
4. Scrollen Sie im Fensterbereich Ereignisdetails nach unten und oben, um die verfügbaren Informationen einzusehen.
   Die im Fensterbereich angezeigten Details hängen von der Art der Regel sowie von den Regeleinstellungen ab, die das Ereignis ausgelöst haben.

So können Sie Ereignisse in der DLP-Ereignisliste filtern

1. Melden Sie sich als Administrator an der Cyber Protect-Konsole an.
2. Wechseln Sie zu **Schutz** > **DLP-Ereignisse**.
3. Klicken Sie im oberen linken Fensterbereich auf **Filter**.
4. Wählen Sie die Vertraulichkeitskategorie, den Workload, den Aktionstyp, den Benutzer und den Kanal aus den Dropdown-Menüs aus.

Sie können mehr als ein Element in den Dropdown-Menüs auswählen. Bei der Filterung wird der logische Operator OR zwischen Elementen desselben Menüs angewendet, der logische Operator AND wird dagegen zwischen Elementen aus verschiedenen Menüs verwendet.

Wenn Sie beispielsweise die Vertraulichkeitskategorien **PHI** und **PII** auswählen, werden alle Ereignisse angezeigt, die PHI (für geschützte Gesundheitsinformationen) oder PII (für personenbezogene Informationen) oder beide enthalten. Wenn Sie die Vertraulichkeitskategorie **PHI** und die Aktion **Schreibzugriff** auswählen, werden nur Ereignisse, die beiden Kategorien entsprechen, im gefilterten Ergebnis angezeigt.

5. Klicken Sie auf **Anwenden**.
6. Wenn Sie wieder alle Ereignisse sehen wollen, müssen Sie zuerst auf **Filter** klicken, dann auf **Auf Standard zurücksetzen** und abschließend auf **Anwenden**.

So können Sie nach Ereignissen in der DLP-Ereignisliste suchen

1. Wiederholen Sie die Schritte 1–2 der oben beschriebenen Prozedur.
2. Wählen Sie aus dem Listenfeld rechts neben Filter eine Kategorie aus, in der Sie suchen wollen: **Absender**, **Ziel**, **Prozess**, **Nachrichtenbetreff** oder **Grund**.
3. Geben Sie in das Textfeld den gewünschten Suchbegriff ein und bestätigen Sie diesen mit der Eingabetaste.
   In der Liste werden nur diejenigen Ereignisse angezeigt, die dem von Ihnen eingegebenen Suchbegriff entsprechen.
4. Wenn Sie die Ereignisliste zurücksetzen wollen, klicken Sie auf das **X**-Zeichen Suchen-Textfeld und drücken Sie dann die Eingabetaste.

So können Sie eine Liste der Ereignisse anzeigen, die sich auf bestimmte Regeln in der Datenfluss-Richtlinie beziehen

1. Melden Sie sich als Administrator an der Cyber Protect-Konsole an.
2. Gehen Sie zu **Schutz** –> **Datenfluss-Richtlinie**.
3. Aktivieren Sie das Kontrollkästchen vor dem Namen der Richtlinie, die Sie interessiert.
   Sie können bei Bedarf auch mehrere Richtlinien auswählen.
4. Klicken Sie auf **Ereignisse anzeigen**.
   Die Ansicht wechselt zu **Schutz** –> **DLP-Ereignisse** und es werden die Ereignisse in der Liste angezeigt, die sich auf die von Ihnen ausgewählten Richtlinienregeln beziehen.

Die Advanced Data Loss Prevention-Widgets auf dem Dashboard 'Überblick'

Das Dashboard **Überblick** enthält eine Reihe benutzerdefinierbarer Widgets, die Ihnen einen Überblick über diejenigen Aktionen geben, die im Zusammenhang mit dem Cyber Protection Service stehen (einschließlich der Advanced Data Loss Prevention). Sie können folgende Advanced Data Loss Prevention-Widgets auf dem Dashboard **Überblick** (unter **Monitoring**) finden.

- **Übertragungen sensibler Daten** – zeigt die Gesamtzahl der Übertragungen sensibler Daten an interne und externe Empfänger an. Das Diagramm ist nach der Art der Berechtigung unterteilt: erlaubt, gerechtfertigt oder blockiert. Sie können dieses Widget anpassen, indem Sie den gewünschten Zeitraum auswählen (1 Tag, 7 Tage, 30 Tage oder dieser Monat).
- **Kategorien ausgehender sensibler Daten** – zeigt die Gesamtzahl der Übertragungen von sensiblen Daten an externe Empfänger an. Das Diagramm ist nach sensiblen Kategorien unterteilt: Geschützte Gesundheitsinformationen (PHI), personenbezogene Informationen (PII), PCI DSS und als vertraulich („Confidential“) gekennzeichnete Daten.
- **Die häufigsten Absender ausgehender sensibler Daten** – zeigt die Gesamtzahl der Übertragungen von sensiblen Daten aus dem Unternehmen an externe Empfänger an sowie eine Liste der fünf Benutzer, die die meisten Übertragungen aufweisen (mit den entsprechenden Zahlen). Diese Statistik umfasst sowohl erlaubte als auch gerechtfertigte Übertragungen. Sie können dieses Widget anpassen, indem Sie den gewünschten Zeitraum auswählen (1 Tag, 7 Tage, 30 Tage oder dieser Monat).
- **Die häufigsten Absender von blockierten Übertragungen sensibler Daten** – zeigt die Gesamtzahl der blockierten Übertragungen von sensiblen Daten sowie eine Liste der fünf Nutzer mit der größten Anzahl von Übertragungsversuchen an (mit den entsprechenden Zahlen). Sie können dieses Widget anpassen, indem Sie den gewünschten Zeitraum auswählen (1 Tag, 7 Tage, 30 Tage oder dieser Monat).
- **Neueste DLP-Ereignisse** – zeigt Details zu den jüngsten Data Loss Prevention-Ereignissen für den ausgewählten Zeitraum an. Sie können das Widget über folgende Optionen anpassen:
  - **Bereich (Veröffentlichungsdatum)** (1 Tag, 7 Tage, 30 Tage, oder dieser Monat).
  - Der Name des **Workloads**
  - **Aktionsstatus** (erlaubt, gerechtfertigt oder blockiert)
  - **Vertraulichkeit** (PHI [geschützte Gesundheitsinformationen], PII [Personenbezogene Informationen], Vertraulich, PCI DSS [Kreditkartentransaktionsdaten])
  - **Zieltyp** (extern, intern)
  - **Gruppierung** (Workload, Benutzer, Kanal, Zieltyp)

Die Widgets werden alle fünf Minuten aktualisiert. Die Widgets haben anklickbare Elemente, über die Sie Probleme untersuchen und beheben können. Sie können den aktuellen Zustand des Dashboards in Form einer .pdf- und/oder .xlsx-Datei herunterladen oder als E-Mail versenden.

Benutzerdefinierte Vertraulichkeitskategorien

Mit benutzerdefinierten Vertraulichkeitskategorien kann ein Unternehmen sein eigenes, spezielles geistiges Eigentum und seine vertraulichen Daten schützen, indem es den in der Advanced DLP-Funktionalität integrierten Katalog mit bestimmten Inhaltsdefinitionen zur Einhaltung gesetzlicher oder firmeninterner Vorschriften erweitert.

So können Sie eine eigene Vertraulichkeitskategorie erstellen

1. Melden Sie sich als Administrator an der Cyber Protect-Konsole an.
2. Gehen Sie zu **Schutz** –> **Data Loss Prevention** –> **Datenklassifizierer**.
3. Wählen Sie **Vertraulichkeitskategorie**.
4. Sie sehen eine Liste von Vertraulichkeitstypen – und zwar sowohl integrierte (wie geschützte Gesundheitsinformationen oder personenbezogene Informationen) als auch benutzerdefinierte.
5. Klicken Sie in der rechten oberen Fensterecke auf **Vertraulichkeit erstellen**.
6. Geben Sie im nächsten Fenster einen entsprechenden Namen ein.
7. Neue benutzerdefinierte Vertraulichkeiten sind standardmäßig immer deaktiviert. Sie können sie aktivieren, sobald Sie alle dazugehörigen Parameter konfiguriert haben.
8. Nachdem Sie eine neue Vertraulichkeit erstellt haben, müssen Sie deren Inhaltsdetektoren einrichten. Klicken Sie auf einen Pfeil, um den Inhalt Ihrer neuen Vertraulichkeit zu erweitern, und wählen Sie dann den Befehl **Inhaltsdetektor hinzufügen**.
9. Im nächsten Fenster können Sie entweder einen der vorhandenen Inhaltsdetektoren verwenden (indem Sie auf das Häkchen neben dessen Namen klicken und dann in der unteren rechten Ecke auf **Hinzufügen** klicken) oder einen neuen definieren.
10. Anstatt eine neue Vertraulichkeit komplett neu zu erstellen, können Sie auch eine bereits vorhandene Vertraulichkeit (entweder eine integrierte oder eine bereits vorhandene benutzerdefinierte) wiederverwenden, indem Sie diese klonen und dann deren Parameter anpassen.
    - Wenn Sie eine vorhandene Vertraulichkeit klonen wollen, müssen Sie zuerst auf das Häkchen neben dem dazugehörigen Namen klicken und dann den Befehl **Klonen** aus dem Aktionslistenfeld (das als Drei-Punkte-Symbol dargestellt ist) in der oberen linken Ecke wählen. Sie können auch mehrere Elemente auf einmal auswählen, wenn Sie mehrere Vertraulichkeiten gleichzeitig klonen wollen.
    - Im nächsten Fenster können Sie dann auswählen, welche Parameter der vorhandenen Vertraulichkeit Sie beibehalten wollen, indem Sie auf die entsprechenden Häkchen neben den einzelnen Parametern klicken.

    Hinweis
    Wenn Sie die integrierten Vertraulichkeiten innerhalb eines Mandanten kopieren, wird eine neue Vertraulichkeit erstellt, die sich aus denselben Detektoren zusammensetzt (sie werden nach dem Kopieren zum Typ 'Benutzerdefiniert').

So können Sie einen neuen Inhaltsdetektor erstellen

1. Melden Sie sich als Administrator an der Cyber Protect-Konsole an.
2. Gehen Sie zu **Schutz** –> **Data Loss Prevention** –> **Datenklassifizierer**.
3. Wählen Sie **Inhaltsdetektoren**.
4. Ihnen wird eine Liste der Inhaltsdetektoren angezeigt – und zwar sowohl integrierte als auch benutzerdefinierte.
5. Klicken Sie in der rechten oberen Fensterecke auf **Inhaltsdetektor erstellen**.

6. Es wird ein Listenfeld geöffnet, in dem Sie den zu erstellenden Detektortyp auswählen können. Derzeit ist hier nur der Inhaltsdetektor **Dateityp** verfügbar . Weitere Inhaltsdetektoren werden aber mit zukünftigen Updates folgen.
7. In dem nachfolgend angezeigten Fenster können Sie den Inhaltsdetektor konfigurieren.

Der Typ des Inhaltsdetektors	Beschreibung
Inhaltsdetektor 'Dateityp'	a. Es gibt zwei Listen: **Unterstützte Dateitypen** und **Ausgewählte Dateitypen**. Wenn Sie rechts neben dem unterstützten Dateityp auf ein 'Plus'-Symbol klicken, wird dieser in die Liste der ausgewählten Dateitypen verschoben. Sie können auch mehrere unterstützte Dateitypen auswählen, indem Sie neben deren Namen auf die entsprechenden Häkchen klicken und dann in der rechten oberen Ecke die Schaltfläche **Ausgewählte hinzufügen** verwenden. b. Wenn Sie einen Dateityp aus der Liste 'Ausgewählte Dateitypen' entfernen wollen, müssen Sie rechts neben dem entsprechenden Namen auf ein Mülleimer-Symbol klicken. Sie können außerdem mehrere Dateitypen auf einmal entfernen, indem Sie die Häkchen und die Schaltfläche **Ausgewählte entfernen** verwenden.
Inhaltsdetektor 'Schlüsselwörter'	a. Wenn Sie einen neuen Inhaltsdetektor vom Typ 'Schlüsselwörter' erstellen, müssen Sie die entsprechenden Schlüsselwörter aus einer Datei importieren. Nachdem Sie die Schlüsselwörter erfolgreich importiert haben, können Sie die neuen Schlüsselwörter entweder mit der Liste der vorhandenen Schlüsselwörter zusammenführen oder die vorhandenen Schlüsselwörter durch die importierten ersetzen. b. Sie müssen auch festlegen, ob für den Inhaltsdetektor alle Schlüsselwörter aus der Liste oder jedes einzelne Schlüsselwort aus der Liste oder eine benutzerdefinierte Anzahl von Schlüsselwörtern übereinstimmen sollen.

8. Anstatt einen neuen Inhaltsdetektor komplett neu zu erstellen, können Sie auch einen bereits vorhandenen (entweder einen integrierten oder eine bereits vorhandenen benutzerdefinierten) wiederverwenden, indem Sie diesen klonen und dann dessen Parameter anpassen.
   - Wenn Sie einen vorhandenen Inhaltsdetektor klonen wollen, müssen Sie zuerst auf das Häkchen neben dem dazugehörigen Namen klicken und dann den Befehl **Klonen** aus dem Aktionslistenfeld (das als Drei-Punkte-Symbol dargestellt ist) in der oberen linken Ecke wählen. Sie können auch mehrere Elemente auf einmal auswählen, wenn Sie mehrere Inhaltsdetektoren gleichzeitig klonen wollen.

Hinweis
Wenn Sie einen integrierten Inhaltsdetektor kopieren, wird dieser zu einem benutzerdefinierten Detektor.

Organisationskarte

Hinweis
Diese Funktionalität ist nur für Firmenadministrator-Benutzer verfügbar.

Die Organisationskarte ist eine Datenbank, die Daten für Benutzer und alle deren Konten enthält, die zur Übertragung von Daten über Instant Messaging, E-Mail oder andere Mittel verwendet werden, die von Advanced DLP abgefangen wurden.

Die Organisationskarte bietet Möglichkeiten zur Erstellung und Verwaltung von Benutzergruppen in Advanced DLP und zur Verwaltung von Benutzern und den mit Benutzern verbundenen Konten in Advanced DLP. Benutzergruppen können dann für die gruppenbasierte DLP-Richtlinienverwaltung verwendet werden.

So können Sie die Organisationskarte finden

- Gehen Sie In der Cyber Protect Cloud-Konsole zu **Schutz** > **Data Loss Prevention** > **Organisationskarte**.

Wie funktioniert das?

Hinweis
Die Organisationskarte wird befüllt, während das Advanced DLP-Modul im Beobachtungsmodus operiert.

Für jede vom DLP-Agenten abgefangene Datenübertragung werden die folgenden Attribute im Backend erfasst.

Attribut	Beschreibung	Bezeichnung in der Benutzeroberfläche
Organisationseinheit	Eine manuell erstellte Gruppe. Die Organisationseinheit kann eine oder mehrere untergeordnete Organisationseinheiten haben.	Gruppenname, wie definiert
Sicherheits-ID	Eine eindeutige Sicherheitskennung.	Auf der Seite 'Details' für den Benutzer > **SID**
	Ein benutzerfreundlicher Anzeigename, der aus den Kontonamen des Benutzers abgeleitet wird. Dieser Name ist nicht immer in der Organisationskarte verfügbar.	**Name**
PC\Benutzername	Der Name des Benutzers auf dem Endpunkt (Workload). Ein Benutzername kann nur einer Organisationseinheit zugewiesen werden.	**Benutzername**

Attribut	Beschreibung	Bezeichnung in der Benutzeroberfläche
Gerät (Workload)	Der Name des Endpunkts (Workload).	**Workload**
Konto	Konten, die von einem Benutzer zur Kommunikation über Instant Messaging und E-Mail verwendet wurden und vom DLP-Agenten abgefangen wurden. Zum Beispiel, wenn der Agent erkennt, dass der Benutzername 'PC\John' john@gmail.com verwendet, um eine E-Mail zu senden - dieses Konto ist mit dem Benutzernamen PC\John verknüpft.	**Konten**

In der Organisationskarte können Sie Konten, Benutzer und Gruppen anzeigen und suchen – sowie Gruppen erstellen, bearbeiten und löschen.

Nach spezifischen Konten suchen

Im Rahmen der Vorfalluntersuchung müssen Administratoren möglicherweise den Besitzer eines bestimmten Kontos ermitteln, das an einem möglichen Datenverstoß beteiligt war.

1. Gehen Sie In der Cyber Protect Cloud-Konsole zu **Schutz** > **Data Loss Prevention** > **Organisationskarte**.
2. Tippen Sie das Konto in das Textfeld **Suchen** über der Benutzerliste ein oder kopieren Sie dessen Namen über die Zwischenablage ein.
   Die Liste wird gefiltert, während Sie tippen.

So können Sie nach einem bestimmten Benutzernamen suchen

1. Gehen Sie In der Cyber Protect Cloud-Konsole zu **Schutz** > **Data Loss Prevention** > **Organisationskarte**.
2. Um in einer bestimmten Gruppe zu suchen, klicken Sie auf den Gruppennamen in der Liste.
3. Tippen Sie den Benutzernamen in das Textfeld **Suchen** über der Benutzerliste ein oder kopieren Sie diesen über die Zwischenablage ein.
   Die Liste wird gefiltert, während Sie tippen.

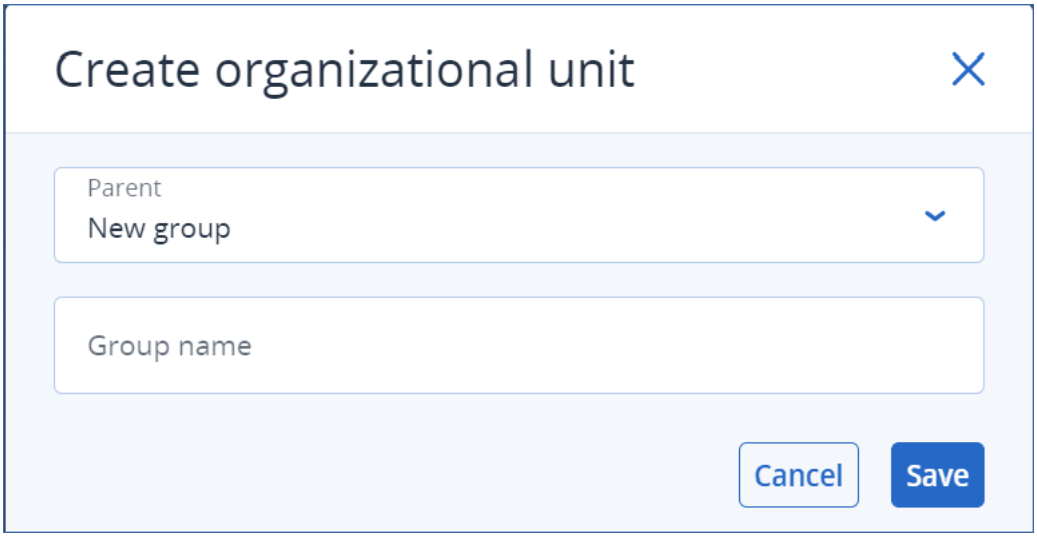
So können Sie die Konten einsehen, die von einem bestimmten Benutzernamen verwendet werden

1. Suchen Sie den Benutzer in der Benutzerliste.
2. Klicken Sie auf die drei Punkte am Ende der Benutzerzeile und wählen Sie **Anzeigen**.
3. Suchen Sie im Dialogfenster für Benutzerdetails den Bereich **Assoziierte Konten**.
4. Sie können Kommentare in das Textfeld "Beschreibung" einfügen.

So können Sie eine Benutzergruppe erstellen

1. Gehen Sie In der Cyber Protect Cloud-Konsole zu **Schutz** > **Data Loss Prevention** > **Organisationskarte**.

2. Klicken Sie im unteren linken Bereich der Gruppenliste auf **Gruppe erstellen**.
   Das Dialogfenster "Organisationseinheit erstellen" öffnet sich.



3. Wählen Sie aus dem übergeordneten Listenmenü den Kontext für die neue Gruppe aus.

   Hinweis
   Sie können den übergeordneten Bereich später nicht ändern. Die Gruppe bleibt in diesem Kontext eingebunden.

4. Geben Sie einen Gruppennamen ein und klicken Sie auf **Speichern**.

So können Sie einen Benutzer zu einer Gruppe hinzufügen

1. Gehen Sie In der Cyber Protect Cloud-Konsole zu **Schutz** > **Data Loss Prevention** > **Organisationskarte**.
2. In der Benutzerliste suchen Sie den Benutzer, den Sie hinzufügen möchten, und aktivieren Sie das Kontrollkästchen am Anfang der Benutzerzeile.
   Die Schaltflächen **Ausgewählte verschieben** und **Ausgewählte löschen** erscheinen über der Benutzerliste.
3. Klicken Sie auf **Ausgewählte verschieben**.
   Das Dialogfenster "Benutzer verschieben" öffnet sich.
4. Wählen Sie neues übergeordnetes Element für den ausgewählten Benutzer aus und klicken Sie auf **Speichern**.

Hinweis
Ein Benutzer kann nur zu einer Gruppe gehören.

So können Sie ein Konto löschen, dass mit einem Benutzer assoziiert ist

1. Suchen Sie den Benutzer in der Benutzerliste.
2. Klicken Sie auf die drei Punkte am Ende der Benutzerzeile und wählen Sie **Anzeigen**.

3. Suchen Sie im Dialogfenster für Benutzerdetails den Bereich **Assoziierte Konten**.
4. Suchen Sie das Konto, das Sie löschen möchten, und klicken Sie neben diesem auf die drei Punkte.
5. Wählen Sie aus der Dropdown-Liste **Löschen** aus.

So können Sie eine Benutzergruppe umbenennen

1. Gehen Sie In der Cyber Protect Cloud-Konsole zu **Schutz** > **Data Loss Prevention** > **Organisationskarte**.
2. Klicken Sie auf die drei Punkte neben dem Namen der Gruppe und klicken Sie auf **Umbenennen**.

So können Sie eine Benutzergruppe löschen

1. Gehen Sie In der Cyber Protect Cloud-Konsole zu **Schutz** > **Data Loss Prevention** > **Organisationskarte**.
2. Klicken Sie auf die drei Punkte neben dem Namen der Gruppe und klicken Sie dann auf **Löschen**. Alle Benutzer aus der Gruppe werden zur übergeordneten Einheit verschoben.

Bekannte Probleme und Einschränkungen

- [DEVLOCK-4028] Es gibt keine Steuerung für die Gruppenchats im Zoom Desktop Agenten.
- [DEVLOCK-4016] Der Anzeigename und die Sender-ID kann bei GMX Web Mail und Web.de Mail nicht erfasst werden, wenn ein Entwurf erstellt wird.
- [DEVLOCK-4447] Es gibt keinen Rechtfertigungsdialog für den WebMail-Dienst von naver.com, wenn ein Entwurf erstellt wird.
- [DEVLOCK-1033] DeviceLockDriver: Potenzieller Bugcheck DRIVER_POWER_STATE_FAILURE, verursacht durch einen Deadlock während der Verarbeitung von IRP_MN_QUERY_DEVICE_ RELATIONS.

Endpoint Detection & Response (EDR)

Hinweis
Diese Funktionalität ist Bestandteil des Advanced Security + EDR-Schutzpakets, das wiederum ein Bestandteil des Cyber Protection Service ist. Wenn Sie die EDR-Funktionalität zu einem Schutzplan hinzufügen, sollten Sie beachten, dass dafür zusätzliche Gebühren anfallen können.

Die EDR-Funktionalität kann verdächtige Aktivitäten auf einem Workload erkennen – wozu auch Angriffe gehören, die bisher unbemerkt geblieben sind. Die EDR-Funktionalität generiert dann Vorfälle, die einen schrittweisen Überblick über jeden Angriff liefern und Ihnen beim Verständnis helfen, wie es zu einem Angriff gekommen ist und wie Sie verhindern können, dass dieser erneut stattfindet. Dank der leicht verständlichen Interpretationen der einzelnen Angriffsstadien kann der Zeitaufwand für Angriffsuntersuchungen auf einige Minuten reduziert werden.

Warum Sie die Endpoint Detection & Response (EDR)-Funktionalität benötigen

In der heutigen Welt mit ihren ständig zunehmenden Cyberbedrohungen und böswilligen Angriffen garantiert eine herkömmliche Präventionslösung keinen 100%igen Schutz mehr. Einige Angriffe werden es immer schaffen, die vorhandenen Präventionsschichten zu überwinden und erfolgreich in das Netzwerk einzudringen. Herkömmliche Lösungen können nicht erkennen, wann dies der Fall ist, sodass sich die Angreifer tage-, wochen- oder gar monatelang in Ihrer Umgebung einnisten können.

Bisherige EDR-Lösungen können solche „stillen Fehler“ verhindern, indem sie die Angreifer bzw. deren Tools schnell finden und entfernen. Allerdings sind dafür üblicherweise ein hohes Maß an Sicherheitsexpertise oder teure Security Operation Center (SOC)-Analysten erforderlich. Hinzu kommt, dass die Analyse von Vorfällen extrem zeitaufwendig sein kann.

Die Advanced Security + EDR-Funktionalität von Acronis überwindet diese bisherigen Einschränkungen, indem sie bisher unbemerkt gebliebene Angriffe aufspürt und Ihnen dabei hilft, zu verstehen, wie es zu einem Angriff gekommen ist und wie Sie verhindern können, dass dieser erneut stattfindet. Und dadurch kann wiederum der Zeitaufwand für die Untersuchung von Angriffen reduziert werden.

Aus diesen Gründen brauchen Sie die EDR-Funktionalität:

- **Volle Sichtbarkeit**: Lernen Sie zu verstehen, was und wie etwas passiert ist (auch bei Angriffen, die bisher unbemerkt geblieben sind). Außerdem wird die Entwicklung eines Angriffs Schritt für Schritt visuell dargestellt (vom ersten Eindringen bis hin zur Anzeige der Daten, die anvisiert und/oder exfiltriert wurden). Dadurch können Sie den Umfang und die Auswirkungen eines Vorfalls schnell nachvollziehen. Weitere Informationen finden Sie im Abschnitt '"So können Sie Vorfälle in der Cyber Kill Chain untersuchen" (S. 996)'.
- **Die Untersuchungszeit minimieren**: Verringern Sie den Zeitaufwand für die Untersuchung von Vorfällen von Stunden auf nur wenige Minuten. Die EDR-Funktionalität informiert Sie detailliert über jeden Schritt des Angriffs in klarer, leicht verständlicher Sprache und macht so den Einsatz teurer Experten oder zusätzlicher Fachkräfte überflüssig. Weitere Informationen finden Sie im Abschnitt '"Vorfälle untersuchen" (S. 995)'
- **Ihre Workloads auf bekannte Bedrohungen überprüfen lassen**: Sie können Ihre Workloads automatisch nach Bedrohungen durch Malware, Schwachstellen und andere Arten von globalen Ereignissen durchsuchen lassen, die Ihre Data Protection beeinträchtigen könnten. Diese Bedrohungen werden als Kompromittierungsindikatoren (Incidents of Compromise, IoCs) bezeichnet und basieren auf Bedrohungsdaten, die von den Cyber Protection Operations Centern (CPOCs) übermittelt werden. Weitere Informationen finden Sie im Abschnitt '"Auf Kompromittierungsindikatoren (IoCs) für öffentlich bekannte Angriffe auf Ihre Workloads prüfen" (S. 1008)'.
- **Schneller auf Vorfälle reagieren**: Dank der Möglichkeit, auch die Aktivitäten nach einem Sicherheitseinbruch weiter verfolgen und jeden Schritt in der Kill Chain genauer aufschlüsseln zu

können, können Sie anschließend eine Reihe von Aktionen durchführen, um die Schäden auf den einzelnen Angriffspunkten wieder zu beheben. Unter anderem können Sie die betroffenen Workloads mithilfe von Remote-Control-Verbindungen und Forensik-Backups (diese Funktion ist in der Early Access-Version nicht verfügbar) untersuchen, die Workloads unter Quarantäne stellen und Malware-Prozesse abschießen. Sie können außerdem Geschäftsprozesse mithilfe von Cyber Disaster Recovery Cloud wiederherstellen. Weitere Informationen finden Sie im Abschnitt '"Vorfälle beheben" (S. 1012)'.

- **Zuverlässige Berichte über Ihre Sicherheitslage erstellen**: Eine aktivierte EDR-Funktionalität kann Ihnen einen Großteil der Unsicherheit und Angst nehmen, welche Folgen Cyberangriffe auf Ihr Unternehmen haben können. Darüber hinaus werden alle vorfallbezogenen Informationen für 180 Tage gespeichert, sodass diese für Audit-Zwecke verwendet werden können.

Funktionen

Die Endpoint Detection & Response (EDR)-Funktionalität bietet folgende Fähigkeiten:

- Alarmmeldungen empfangen, wenn es zu einer Sicherheitsverletzung kommt
- Ihre Vorfälle auf der Seite 'Vorfälle' verwalten
- Eine leicht verständliche Visualisierung des Angriffsverlaufs
- Empfehlungen und Behebungsmaßnahmen
- Überprüfen Sie anhand von Bedrohungsfeeds, ob es öffentlich bekannte Angriffe auf Ihre Workloads gibt
- Schneller Überblick im Dashboard
- Sicherheitsereignisse für 180 Tage speichern

Alarmmeldungen empfangen, wenn es zu einer Sicherheitsverletzung kommt

Die EDR-Funktionalität liefert Alarmmeldungen, wenn es zu einem Vorfall kommt. Diese Alarmmeldungen werden im Hauptmenü der Cyber Protect-Konsole hervorgehoben. Sie können einen Alarm dann untersuchen, indem Sie auf die Schaltfläche **Vorfall untersuchen** klicken. Dadurch werden Sie zur Anzeige für die Untersuchung von Vorfällen weitergeleitet, die auch als Cyber Kill Chain bezeichnet wird.

Weitere Informationen finden Sie im Abschnitt '"Vorfälle überprüfen" (S. 988)'.

Ihre Vorfälle auf der Seite 'Vorfälle' verwalten

Die EDR-Funktionalität ermöglicht es Ihnen, alle Vorfälle auf der Seite 'Vorfälle' zu verwalten. Der Zugriff auf diese Seite erfolgt über das Menü 'Schutz' in der Cyber Protect-Konsole. Die Seite 'Vorfälle' kann nach Ihren Anforderungen gefiltert werden. So können Sie sich schnell und einfach über den aktuellen Status Ihrer Vorfälle informieren – wie etwa den vorliegenden Schweregrad, welche Workloads betroffen sind und wie der Positivitätslevel aussieht. Sie können auch direkt zur Cyber Kill Chain gehen, um sich den Angriffsverlauf jeweils Knoten für Knoten anzusehen.

Weitere Informationen über die Seite 'Vorfälle' finden Sie im Abschnitt '"Vorfälle überprüfen" (S. 988)'.

Eine leicht verständliche Visualisierung des Angriffsverlaufs

Die EDR-Funktionalität bietet Ihnen zu jedem Angriff eine visuelle Darstellung mit leicht verständlichen Informationen. Dadurch wird sichergestellt, dass auch Mitarbeiter ohne besondere Sicherheitsausbildung verstehen können, was die Ziele und der Schweregrad eines Angriffs waren. Sie brauchen tatsächlich keinen speziellen SOC-Service (Security Operation Center) oder ausgebildete Sicherheitsexperten, denn die EDR-Funktionalität zeigt Ihnen genau, wie ein Angriff abgelaufen ist. Damit lassen sich etwa folgende Fragen beantworten:

- Wie der Angreifer eindringen konnte
- Wie der Angreifer seine Spuren verwischt hat
- Welcher Schaden wurde verursacht
- Wie sich der Angriff ausgebreitet hat

Weitere Informationen finden Sie im Abschnitt '"So können Sie Vorfälle in der Cyber Kill Chain untersuchen" (S. 996)'.

Empfehlungen und Behebungsmaßnahmen

Die EDR-Funktionalität liefert Ihnen klare und leicht umsetzbare Empfehlungen, wie Sie Angriffe auf einen Workload bekämpfen können. Wenn Sie einen Angriff schnell bekämpfen wollen, klicken Sie auf die Schaltfläche **Gesamten Vorfall beheben**. Daraufhin werden Ihnen Schritte empfohlen, mit denen Sie den Vorfall abschwächen können. Wenn Sie diese empfohlenen Schritte befolgen, können Sie die von einem Angriff betroffenen Workloads schnell wieder betriebsbereit machen. Wenn Sie jedoch detailliertere Behebungsmaßnahmen ergreifen wollen, können Sie jeden einzelnen Knoten ansteuern und Schäden auf diesen mit einer entsprechenden Aktion beheben.

Weitere Informationen finden Sie im Abschnitt '"Vorfälle beheben" (S. 1012)'.

Anhand von Bedrohungsfeeds überprüfen, ob es öffentlich bekannte Angriffe auf Ihre Workloads gibt

Die EDR-Funktionalität umfasst die Möglichkeit, Ihre Workloads auf vorhandene, bekannte Angriffe aus den Bedrohungsfeeds untersuchen zu lassen. Diese Bedrohungsfeeds werden automatisch anhand von Bedrohungsdaten generiert, die von den Cyber Protection Operations Centern (CPOCs) geliefert werden. Mit der EDR-Funktionalität können Sie überprüfen, ob Ihr Workload von einer solchen Bedrohung betroffen ist (oder nicht), und dann die notwendigen Maßnahmen zur Beseitigung der Bedrohung ergreifen.

Weitere Informationen finden Sie im Abschnitt '"Auf Kompromittierungsindikatoren (IoCs) für öffentlich bekannte Angriffe auf Ihre Workloads prüfen" (S. 1008)'.

Schneller Überblick im Dashboard

Die EDR-Funktionalität stellt Ihnen zahlreiche Statistiken im Dashboard der Cyber Protect-Konsole zur Verfügung. Ihnen werden folgende Informationen angezeigt:

- Der aktuelle Bedrohungsstatus – wie etwa die Anzahl der Vorfälle, die untersucht werden sollten.
- Die Entwicklung der Angriffe, aufgeschlüsselt nach Schweregrad, was auf mögliche Angriffskampagnen hinweisen kann.
- Die Effizienzrate bei der Schließung von Vorfällen.
- Die zielgerichtetsten Taktiken, um Ihre Kunden anzugreifen.
- Der Netzwerkstatus des Workloads, der angibt, ob er isoliert oder verbunden ist.

Sicherheitsereignisse für 180 Tage speichern

Die EDR-Funktionalität sammelt Workload- und Applikationsereignisse und speichert diese 180 Tage lang. Ereignisse, die älter als 180 Tage sind, werden gelöscht (das Löschen von Ereignissen richtet sich nur nach ihrem Alter und nicht nach dem Speicherplatz). Beachten Sie, dass auch bei ausgeschalteter EDR-Funktionalität alle bereits erfassten Ereignisse für einen Workload erhalten bleiben und damit weiter für die Untersuchung von Vorfällen verfügbar sind.

Software-Anforderungen

Die Endpoint Detection & Response (EDR)-Funktionalität unterstützt folgende Betriebssysteme:

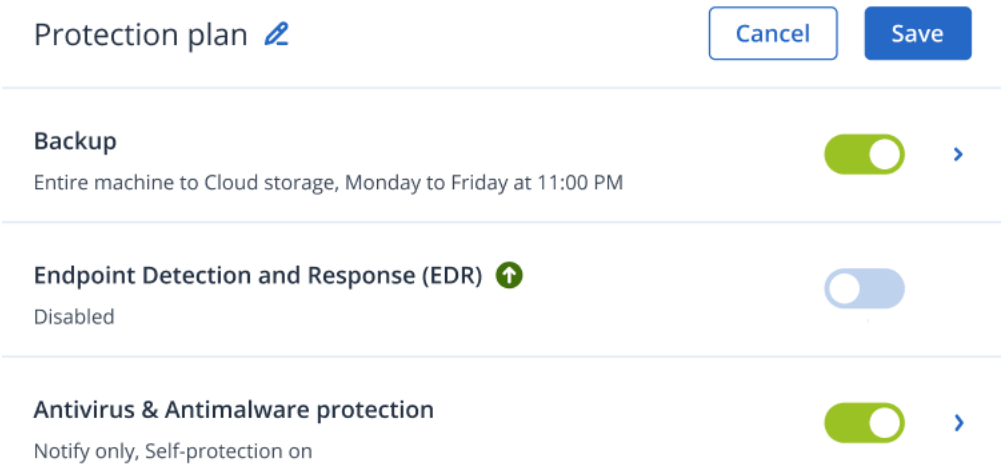
- Microsoft Windows 7 Service Pack 1 und höher
- Microsoft Windows Server 2008 R2 und höher

Die Endpoint Detection & Response (EDR)-Funktionalität aktivieren

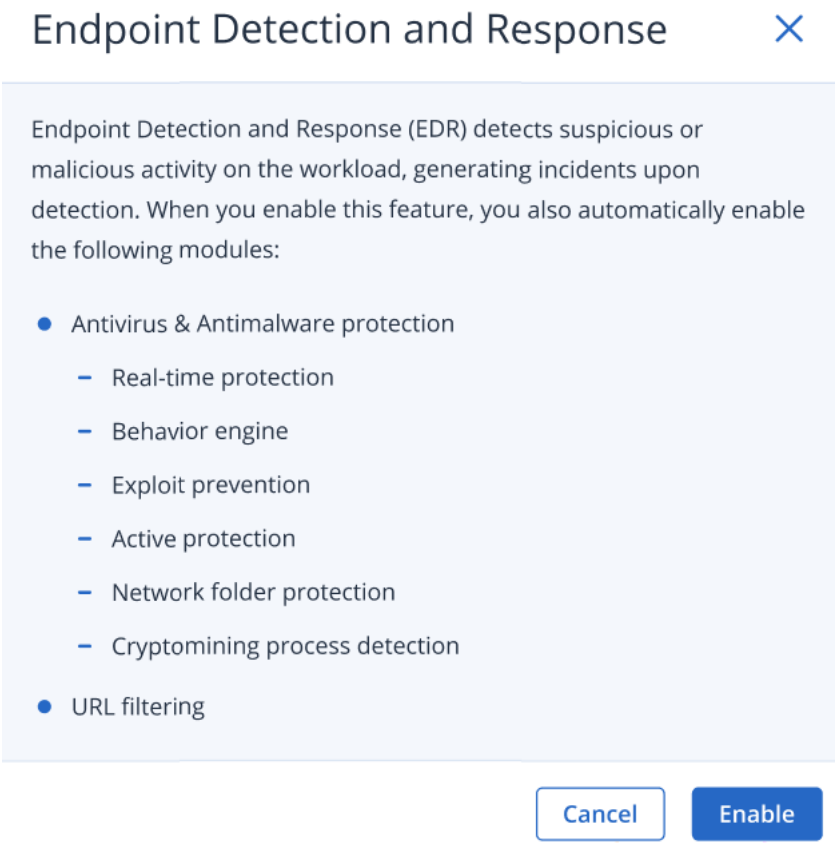
Sie können die EDR-Funktionalität in jedem Schutzplan aktivieren.

So können Sie die EDR-Funktionalität aktivieren

1. Gehen Sie in der Cyber Protect-Konsole zum Bereich **Verwaltung –> Schutzpläne**.
2. Wählen Sie den entsprechenden Schutzplan aus der angezeigten Liste aus und klicken Sie in der rechten Seitenleiste auf **Bearbeiten**.
   Alternativ können Sie auch einen neuen Schutzplan erstellen und mit dem nächsten Schritt fortfahren. Weitere Informationen über die Verwendung von Schutzplänen finden Sie im Abschnitt '"Schutzpläne und Module" (S. 231)'.
3. Aktivieren Sie in der Seitenleiste des Schutzplans das Modul **Endpoint Detection & Response (EDR)**, indem Sie neben dem Modulnamen auf den Schalter klicken.



4. Klicken Sie im angezeigten Dialog auf **Aktivieren**. Beachten Sie: Wenn die EDR-Funktionalität aktiviert wird, werden auch andere Schutzmodule aktiviert (wie im angezeigten Dialog zu sehen ist).



Hinweis
Wenn der Status eines der Module **Active Protection**, **Behavior Engine**, **Exploit-Prävention** oder **URL-Filterung** auf **Aus** geschaltet ist, wird auch die **Endpoint Detection & Response (EDR)**-Funktionalität auf **Aus** geschaltet.

5. Das Symbol des **Advanced Security + EDR**-Pakets wird (wie unten gezeigt) zur Liste derjenigen Schutzpakete hinzugefügt, die für die Implementierung des Schutzplans erforderlich sind (je nachdem, welche zusätzlichen Pakete Sie auswählen).

So können Sie die Endpoint Detection & Response (EDR)-Funktionalität verwenden

Mit der EDR-Funktionalität können Sie Angriffe aufspüren, die ansonsten unbemerkt bleiben würden, und dabei nachvollziehen, wie es zu einem Angriff gekommen ist und wie Sie verhindern können, dass dieser erneut stattfindet. Dank der leicht verständlichen Interpretationen der einzelnen Angriffsstadien kann der Zeitaufwand für Angriffsuntersuchungen auf einige Minuten reduziert werden.

Die nachfolgende Tabelle beschreibt den grundsätzlichen Workflow beim Arbeiten mit der EDR-Funktionalität. Sie beginnen damit, dass Sie alle Vorfälle überprüfen und priorisieren, diese dann in der Cyber Kill Chain weiter untersuchen und anschließend die entsprechenden Schadensbehebungsmaßnahmen ergreifen.

Schritt	So können Sie die EDR-Funktionalität verwenden
SCHRITT 1: Vorfälle überprüfen	In der EDR-Vorfallsliste: • Ermitteln Sie die Sicherheitslage einer Organisation: wie viele Vorfälle müssen untersucht werden? • Ermitteln Sie, welches die kritischsten Vorfälle sind, und priorisieren Sie deren Untersuchung nach ihrem Schweregrad. • Ermitteln Sie, welche Vorfälle neu oder noch andauern.
SCHRITT 2: Vorfälle untersuchen	In der EDR Cyber Kill Chain: • Ermitteln Sie die Ziele des Angreifers und analysieren Sie die verwendeten Angriffstechniken. • Überprüfen Sie, wie wahrscheinlich es sich bei einem Vorfall um einen echten schädlichen Angriff handelt. • Überprüfen Sie, ob ein Bedrohungsfeed Ihren Workload beeinträchtigt oder nicht. • Informieren Sie sich, welche Antwortaktionen bereits auf einen Vorfall angewendet wurden.
SCHRITT 3: Vorfälle beheben	In den entsprechenden EDR-Abschnitten zur Schadensbehebung können Sie Folgendes tun: • Entstandende Schäden schnell und einfach beheben, indem Sie globale Antwortaktionen auf einen gesamten Vorfall anwenden. • Die Schäden durch einzelne Angriffspunkte innerhalb eines Vorfalls beheben. • Maßnahmen ergreifen, um den aktuellen Angriff oder zukünftige daran zu hindern, sich auf andere Workloads auszubreiten, die bisher noch nicht im Visier des

Schritt	So können Sie die EDR-Funktionalität verwenden
	Angreifers geraten sind.

Vorfälle überprüfen

Die Endpoint Detection & Response (EDR)-Funktionalität stellt eine Vorfallsliste bereit, wozu auch Präventionsmaßnahmen (gegen Malware) und verdächtige Erkennungen auf einem Workload gehören. Die Vorfallsliste gibt Ihnen einen schnellen Überblick über alle Angriffe oder Bedrohungen, die Ihre Workloads betreffen. Dazu gehören auch Bedrohungen, die noch abgeschwächt werden müssen.

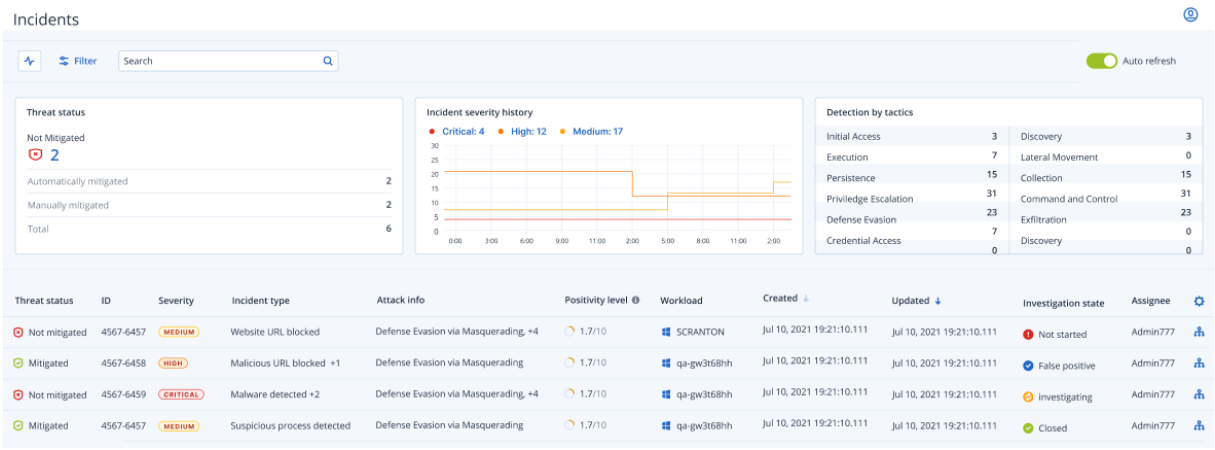
Mithilfe der Vorfallsliste können Sie folgende Dinge schnell feststellen:

- Die Sicherheitslage einer Organisation: wie viele Vorfälle müssen untersucht werden?
- Welches sind die kritischsten Vorfälle? Sie können deren Untersuchung nach deren jeweiligem Schweregrad priorisieren.
- Welche Vorfälle neu sind oder noch andauern.

Hinweis
Wenn Sie als Partner-Administrator angemeldet sind, können Sie alle EDR-Vorfälle auf einer einzigen Anzeige einsehen. Dort werden die Vorfälle aller Ihrer Kunden zusammengefasst, ohne dass Sie auf die einzelnen Vorfallansichten der jeweiligen Kunden zugreifen müssen. Es wird eine zusätzliche Spalte **Kunden** angezeigt, wo der Kundenname für jeden Vorfall angegeben wird. Darüber hinaus zeigen die Widgets auf dem Dashboard **Überblick** auch noch allgemeine Metrikdaten an, die von allen Kunden gesammelt werden.

Sie können auf die Vorfallsliste (wie unten gezeigt) über das Menü **Schutz** in der Cyber Protect-Konsole zugreifen. Weitere Informationen darüber, wie Sie die Vorfälle in der Vorfallsliste überprüfen können, finden Sie im Abschnitt '"Einsehen, welche Vorfälle bisher nicht abgeschwächt wurden" (S. 991)'. Wenn Sie mehr über die Erstellung von Vorfällen erfahren wollen, informieren Sie sich unter 'Was genau sind Vorfälle?'.

Hinweis
Wenn die Managed Detection & Response (MDR)-Funktionalität für Ihre Workloads aktiviert ist, wird eine zusätzliche Spalte namens **MDR-Ticket** angezeigt. In dieser wird die Ticketnummer angezeigt, die vom jeweiligen MDR-Anbieter bereitgestellt wird.



Hinweis
Die Cyber Protect-Konsole muss geöffnet sein, damit Sie Vorfallsbenachrichtigungen erhalten können.

Was genau sind Vorfälle?

Vorfälle bzw. Sicherheitsvorfälle können als eine Art *Container* mit mindestens einer Präventionsmaßnahme oder einem verdächtigen Erkennungspunkt (oder eine Mischung daraus) betrachtet werden und umfassen alle Ereignisse und Erkennungen, die mit einem einzelnen Angriff in Zusammenhang stehen. Diese Sicherheitsvorfälle können außerdem harmlose Ereignisse enthalten, die weiteren Aufschluss über das Geschehen geben können.

So können Sie alle Angriffsereignisse zusammen in einem einzelnen Vorfall betrachten und die logischen Schritte verstehen, die der jeweilige Angreifer durchgeführt hat. Außerdem hilft es, die Untersuchungszeit bei einem Angriff zu verkürzen.

Wenn die EDR-Funktionalität im Schutzplan aktiviert ist, werden Sicherheitsvorfälle erstellt, wenn:

- **Eine Präventionsschicht etwas gestoppt hat:** Diese Vorfälle werden entsprechend den Schutzplan-Einstellungen automatisch vom System geschlossen. Sie können jedoch untersuchen, was genau die jeweilige Malware getan hat, bevor sie gestoppt wurde. So kann es beispielsweise sein, dass eine Ransomware gestoppt wurde, als sie mit der Verschlüsselung von Dateien begann. Zuvor kann sie jedoch bereits Anmeldedaten gestohlen oder einen Dienst installiert haben.
- **Eine verdächtige Aktivität von der EDR-Funktionalität erkannt wurde:** Dies sind Erkennungen, die untersucht und behoben werden sollten. Indem Sie die visuell verbesserte Cyber Kill Chain untersuchen (weitere Informationen dazu finden Sie unter '"So können Sie Vorfälle in der Cyber Kill Chain untersuchen" (S. 996)'), können Sie die entsprechenden Schadensbehebungsmaßnahmen leicht anwenden.

Priorisieren Sie, welche Vorfälle eine sofortige Aufmerksamkeit erfordern

Die Vorfallsliste der Cyber Protect-Konsole ist jederzeit über das Menü **Schutz** in der Cyber Protect-Konsole abrufbar. Über diese Vorfallsliste können Sie sich nicht nur einen schnellen Überblick über

alle Angriffe und Bedrohungen verschaffen, sondern auch allen Vorfällen, die Ihrer Aufmerksamkeit bedürfen, eine entsprechende Priorität zuweisen.

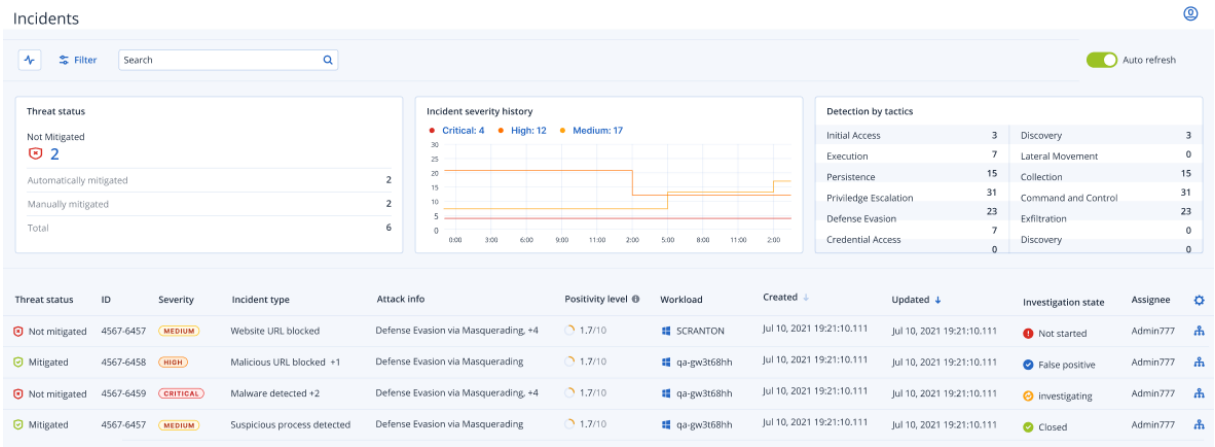
Wichtig
Um die Sicherheit Ihres Workloads zu gewährleisten, sollten Sie *immer* diejenigen Vorfälle analysieren und priorisieren, die noch andauern oder noch nicht abgeschwächt wurden.

So können Sie analysieren, welche Sicherheitsvorfälle Ihre sofortige Aufmerksamkeit erfordern

Anhand dieser Liste können Sie die Vorfälle, die eine besondere Aufmerksamkeit erfordern, analysieren und nach Prioritäten ordnen. Sie können:

- Einsehen, welche Vorfälle bisher nicht abgeschwächt wurden: Mithilfe der Vorfallsliste schnell ermitteln, ob derzeit irgendwelche Angriffe stattfinden. Sie sollten sich zuerst alle Vorfälle ansehen, die noch nicht abgeschwächt wurden, was über die Spalte **Bedrohungsstatus** ersichtlich ist. Die Vorfallsliste ist standardmäßig bereits so vorgefiltert, dass diese Vorfälle angezeigt werden.
- Das Ausmaß und die Auswirkungen von Vorfällen verstehen: Nutzen Sie die Möglichkeit, neue oder gerade ablaufende Angriffe zu filtern, um den Schweregrad der gefilterten Vorfälle sowie deren Auswirkungen auf Ihren Geschäftsbetrieb zu verstehen.

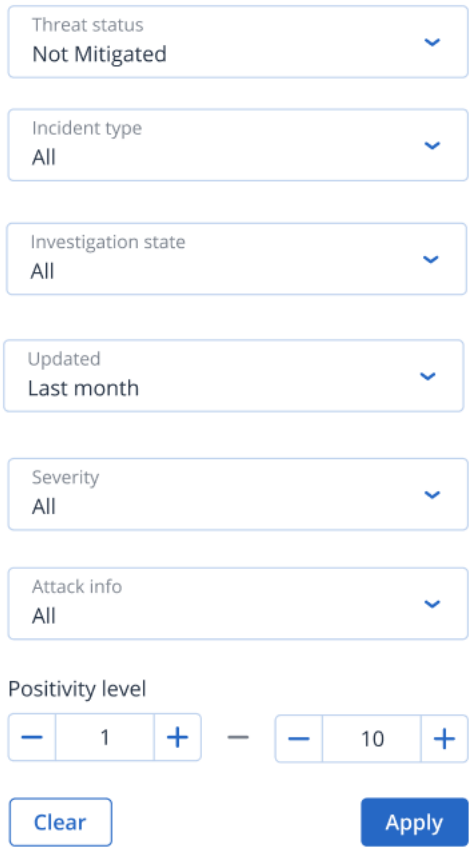
Indem Sie die Liste der wichtigsten Vorfälle verfeinern, können Sie den Vorfall genauer analysieren, um ein besseres Verständnis für dessen Ablauf und die vom Angreifer eingesetzten Techniken zu erhalten. Weitere Informationen finden Sie im Abschnitt '"Vorfalldetails analysieren" (S. 994)'.



Hinweis
Die Vorfallsliste wird standardmäßig nach der Spalte **Aktualisiert** sortiert. Diese gibt Auskunft darüber, wann der Vorfall zuletzt mit neuen Erkennungsdaten aktualisiert wurde, die innerhalb des Vorfalls aufgezeichnet wurden. Beachten Sie, dass ein bestehender Vorfall jederzeit aktualisiert werden kann. Das gilt auch dann, wenn der Vorfall erst kürzlich geschlossen wurde. Wie in der nachfolgenden Prozedur beschrieben, können Sie die Filterung der Liste so anpassen, dass neu eröffnete oder laufende Angriffe nach Ihren Anforderungen angezeigt werden.

So können Sie die Vorfallsliste filtern

1. Klicken Sie im oberen Bereich der Vorfallsliste auf **Filter**, um die angezeigte Liste der Vorfälle zu filtern. Wenn Sie beispielsweise im Feld **Erstellt** ein Start- und Enddatum auswählen, werden in der Vorfallsliste und den Widgets diejenigen Vorfälle angezeigt, die während des festgelegten Zeitraums angelegt wurden.



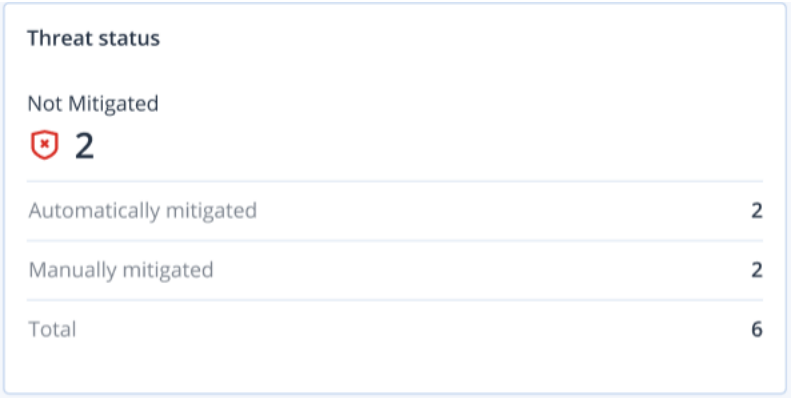
2. Klicken Sie auf **Anwenden**, wenn Sie fertig sind.

Einsehen, welche Vorfälle bisher nicht abgeschwächt wurden

Sie können den aktuellen Bedrohungsstatus eines Vorfalls in der Spalte **Bedrohungsstatus** einsehen. Hier wird angezeigt, ob der entsprechende Vorfall bereits den Status **Abgeschwächt** hat oder noch **Nicht abgeschwächt** wurde. Der Bedrohungsstatus wird automatisch von der EDR-Funktionalität definiert. Jeder Vorfall, der noch nicht abgeschwächt ist, sollte schnellstmöglich untersucht werden.

Sie können dann die angezeigte Vorfallsliste weiter verfeinern, indem Sie Filter anwenden. Sie können beispielsweise entsprechende Filteroptionen anwenden, um die Liste nach dem Bedrohungsstatus *und* einem bestimmten Schweregrad filtern zu lassen. Wenn Sie die Vorfälle nach Ihren Vorstellungen gefiltert haben, können Sie diese, wie im Abschnitt '"Vorfälle untersuchen" (S. 995)' beschrieben, weitergehend untersuchen.

Sie können außerdem (wie unten gezeigt) das Widget **Bedrohungsstatus** verwenden, um einen schnellen Überblick über den aktuellen Bedrohungsstatus zu erhalten. Beachten Sie, dass die Daten, die in diesem Widget angezeigt werden, ebenfalls die von Ihnen angewendeten Filter widerspiegeln. Vergleiche dazu den Abschnitt '"So können Sie die Vorfallsliste filtern" (S. 991)'.



Das Ausmaß und die Auswirkungen von Vorfällen verstehen

Sie können das Ausmaß und die Auswirkungen von Vorfällen schnell erfassen, indem Sie die Spalten **Schweregrad**, **Angriffsinfo** und **Positivitätslevel** überprüfen. Wie bereits oben erwähnt, können Sie, nachdem Sie ermittelt haben, welche Vorfälle gerade stattfinden, diese zusätzlichen Spalten filtern, um Folgendes zu tun:

- Mithilfe der Spalte **Schweregrad** überprüfen, welche Vorfälle besonders kritisch sind. Der Schweregrad eines Vorfalls kann **Kritisch**, **Hoch** oder **Mittel** sein.
  - **Kritisch**: Es besteht ein schwerwiegendes Risiko für schädliche Cyberaktivitäten und damit die Gefahr, dass geschäftskritische Hosts in Ihrer Umgebung kompromittiert werden.
  - **Hoch**: Es besteht ein hohes Risiko für schädliche Cyberaktivitäten und damit die Gefahr, dass Ihre Umgebung schwer beschädigt wird.
  - **Mittel**: Es besteht ein erhöhtes Risiko für schädliche Cyberaktivitäten.

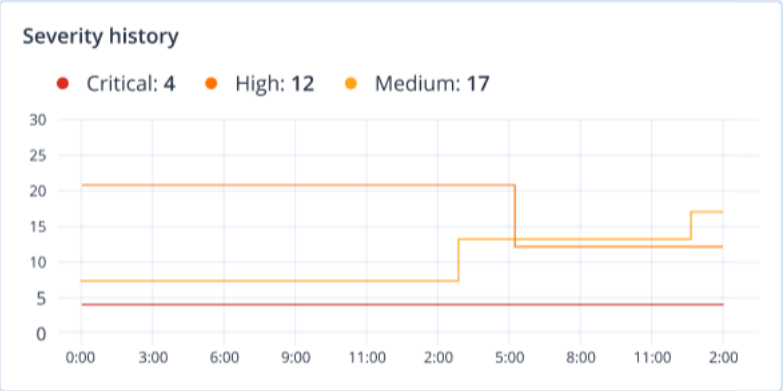
    Hinweis
    Der EDR-Algorithmus berücksichtigt zur Bestimmung des Schweregrads, welche Art von Workload vorliegt und welchen Umfang die einzelnen Schritte des Angriffs haben. Wenn bei einem Vorfall beispielsweise Anmeldedaten gestohlen werden, wird der Schweregrad auf **Kritisch** gesetzt.

- Verstehen Sie, warum ein Vorfall in der Spalte **Vorfallstyp** erstellt wurde. Der Vorfallstyp kann einen oder mehrere der folgenden Punkte enthalten:
  - **Ransomware erkannt**
  - **Malware erkannt**
  - **Verdächtiger Prozess erkannt**
  - **Schädlicher Prozess erkannt**

    - **Verdächtige URL blockiert**
    - **Schädliche URL blockiert**
- Mithilfe der Spalte **Angriffsinfo** können Sie die verwendeten Angriffstechniken ermitteln und feststellen, ob es bei den Angriffen ein bekanntes Schema oder Muster gibt.
- Bestimmen Sie, wie wahrscheinlich es sich bei einem Vorfall um einen echten schädlichen Angriff handelt. Die Spalte **Positivitätslevel** zeigt eine Bewertung (einen Score) mit einer Spanne von 1-10. Je höher dieser Score ist, desto eher handelt es sich tatsächlich um einen schädlichen Angriff.

Nachdem Sie ermittelt haben, welche Vorfälle eine sofortige Aufmerksamkeit erfordern, können Sie diese (wie im Abschnitt '"Vorfälle untersuchen" (S. 995)' beschrieben) genauer untersuchen.

Sie können auch die Widgets **Schweregradverlauf** und **Erkennung anhand von Taktiken** verwenden, um sich einen schnellen Überblick über den Schweregrad und die Angriffstechniken zu verschaffen.



Im Widget **Erkennung anhand von Taktiken** werden die verschiedenen eingesetzten Angriffstechniken angezeigt. Wobei mit roten bzw. grünen Farben angezeigt wird, ob die Werte im Vergleich zum zuvor spezifizierten Zeitraum gestiegen oder gesunken sind. Dieses Widget zeigt eine aggregierte Ansicht aller Ziele für die gefilterten Vorfälle an. Dadurch können Sie sich schnell einen Überblick darüber verschaffen, welche Auswirkungen die Vorfälle auf Ihre Kunden haben.

Detection by tactics

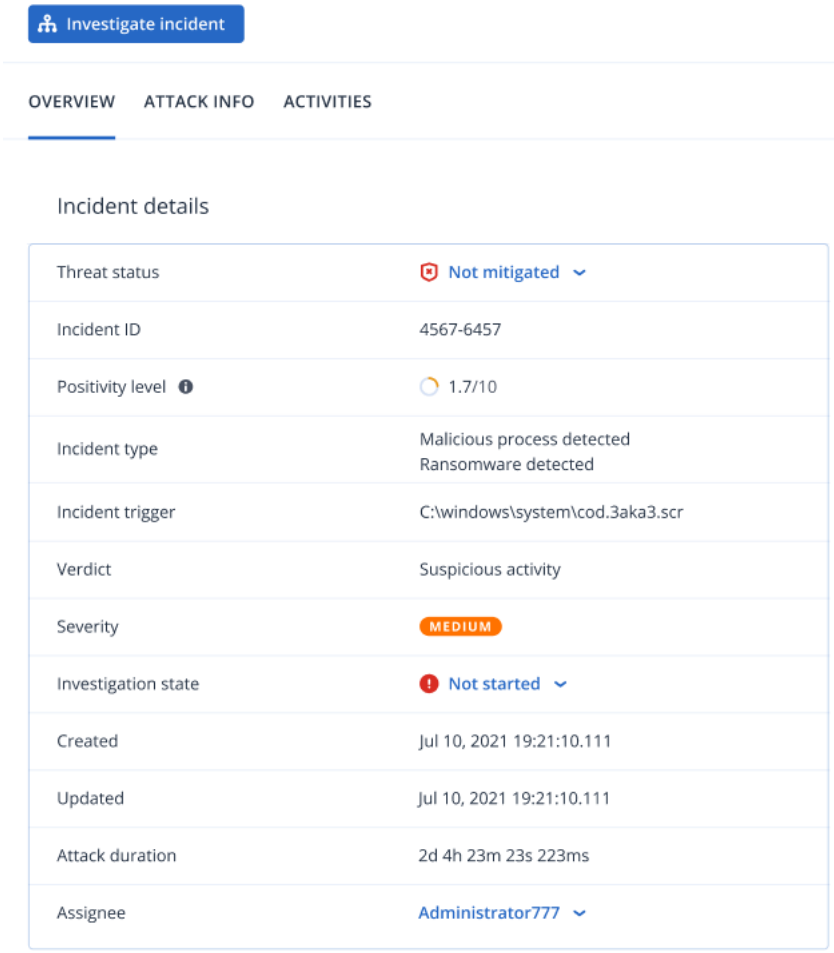
Initial Access	3	Discovery	3
Execution	7	Lateral Movement	0
Persistence	15	Collection	15
Priviledge Escalation	31	Command and Control	31
Defense Evasion	23	Exfiltration	23
Credential Access	7	Discovery	0
Impact	0	Resouce Development	0

Vorfalldetails analysieren

Während der Vorfallüberprüfungsphase können Sie auch die Details der einzelnen Vorfälle aus der Endpoint Detection & Response (EDR)-Vorfallsliste analysieren. Diese Details ermöglichen es Ihnen, den gesamten Vorfall genauer zu untersuchen und dadurch nachzuvollziehen, wie und wann genau er eingetreten ist. Darüber hinaus können Sie einen Vorfall bestimmten Benutzern zur genaueren Untersuchung zuweisen sowie den Untersuchungsstatus festlegen.

So können Sie Vorfallsdetails analysieren

1. Gehen Sie in der Cyber Protect-Konsole zu **Schutz –> Vorfälle**. Die Vorfallsliste wird angezeigt.
2. Klicken Sie auf den Vorfall, den Sie überprüfen wollen. Die Details zu dem ausgewählten Ereignis werden angezeigt.
3. Auf der angezeigten Registerkarte **Überblick** können Sie die Details zum Vorfall und Workload überprüfen – wie etwa den Status und Schweregrad der aktuellen Bedrohung. Sie können auch das **Untersuchungstadium** definieren (indem Sie eines der folgenden Stadien auswählen: **Wird untersucht**, **Nicht gestartet** (das Standardstadium), **Falsch positiv** oder **Geschlossen**) und einen Benutzer auswählen, dem Sie den Vorfall zuweisen wollen (wählen Sie den entsprechenden Benutzer aus dem Listenfeld **Beauftragter** aus).

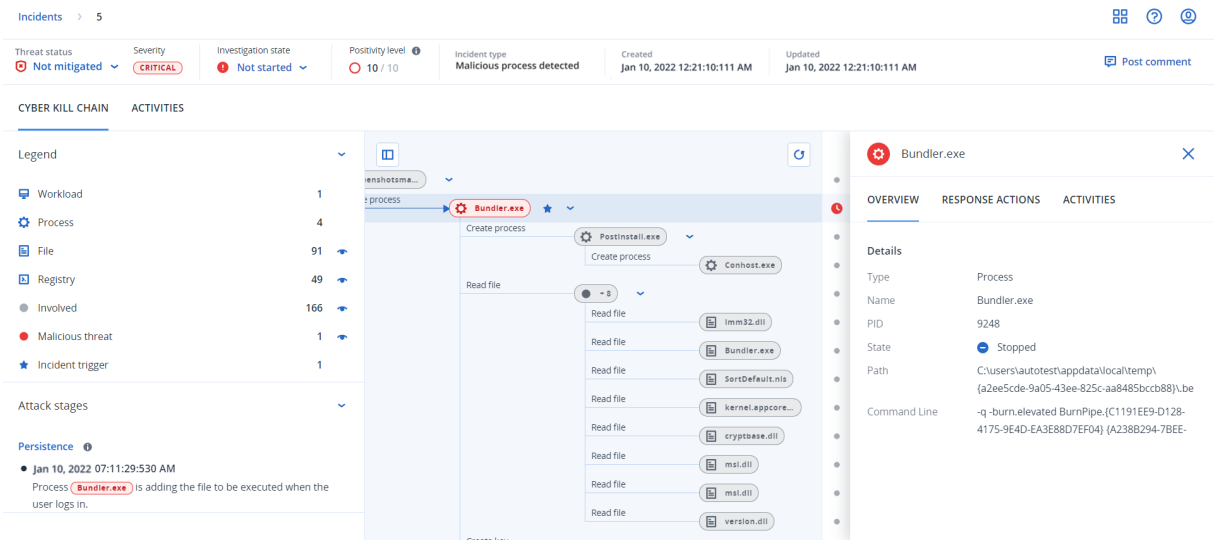


4. Klicken Sie auf die Registerkarte **Angriffsinfo**, wenn Sie Details zu dem Angriff und die dabei verwendeten Angriffstechniken einsehen wollen. Sie können neben jeder aufgeführten Angriffstechnik auf einen dazugehörigen Link klicken, um weitere Informationen über diese Technik auf MITRE.org zu erhalten.
5. Klicken Sie auf die Registerkarte **Aktivitäten**, wenn Sie eine der Maßnahmen überprüfen wollen, die in der Cyber Kill Chain zur Abschwächung eines Vorfalls ergriffen wurde. Weitere Informationen finden Sie im Abschnitt '"So können Sie Vorfälle in der Cyber Kill Chain untersuchen" (S. 996)'.
   Wenn beispielsweise ein Patch auf den Workload angewendet wurde, können Sie einsehen, wer den Patch durchgeführt hat, wie lange dies gedauert hat und welche Fehler möglicherweise bei der Implementierung des Patches aufgetreten sind.
6. Klicken Sie auf **Vorfall untersuchen**, wenn Sie auf die Cyber Kill Chain zugreifen wollen, wo Sie den Vorfall Knoten für Knoten untersuchen können. Weitere Informationen finden Sie im Abschnitt '"So können Sie Vorfälle in der Cyber Kill Chain untersuchen" (S. 996)'.

Vorfälle untersuchen

Mit der Endpoint Detection & Response (EDR)-Funktionalität können Sie ganze Vorfälle untersuchen – einschließlich aller Angriffsphasen und betroffener Objekte (Prozesse, Registry-Einträge, geplante Tasks und Domains). Diese Objekte werden (wie unten gezeigt) durch Knoten in der leicht

verständlichen Cyber Kill Chain dargestellt. Mithilfe der Cyber Kill Chain können Sie schnell nachvollziehen, was und wann genau etwas bei einem Angriff passiert ist.



In der Cyber Kill Chain wird jeder einzelne Schritt eines Angriffs dargestellt, wodurch Sie eine detaillierte Interpretation darüber erhalten, wie der Vorfall abgelaufen ist und warum. In der Cyber Kill Chain werden leicht verständliche Sätze und Diagramme verwendet, die jeden Angriffsschritt erläutern und Ihnen so helfen, den Zeitaufwand für die Vorfallsanalyse zu minimieren.

Sie können den Umfang und die Auswirkungen eines Vorfalls schnell verstehen und die Angriffsentwicklung den Klassifizierungen des bekannten MITRE-Frameworks zuordnen. Dies ermöglicht Ihnen, jeden Schritt eines Angriffs zu analysieren und dabei Dinge zu erfahren wie:

- Den anfänglichen Einstiegspunkt
- Wie der Angriff ausgeführt wurde
- Jede Rechteausweitung
- Techniken, um Erkennungen zu vermeiden
- Laterale Bewegungen zu anderen Workloads
- Diebstahl von Anmeldedaten
- Versuche zur Datenexfiltration

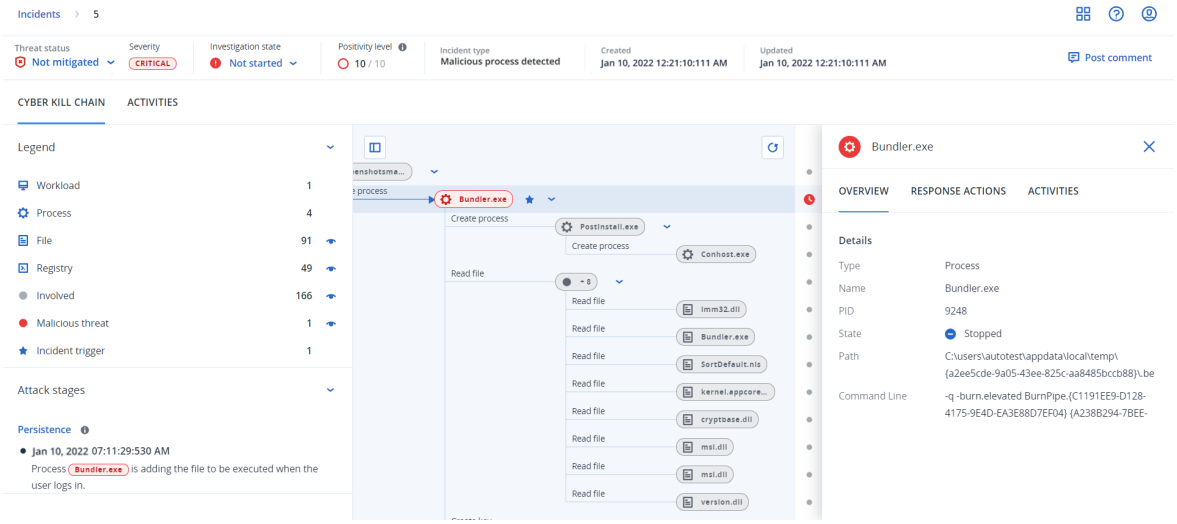
Hinweis
Alle bei einem Angriff betroffene Objekte (wie Prozesse, Registry-Einträge, geplante Tasks oder Domains) werden in der Cyber Kill Chain anhand von entsprechenden Knoten dargestellt.

So können Sie Vorfälle in der Cyber Kill Chain untersuchen

Sie können jeden einzelnen Schritt eines Angriffs in der Cyber Kill Chain untersuchen. Die leicht verständlichen Sätzen und Grafiken der Cyber Kill Chain helfen Ihnen, jeden Schritt des Angriffs zu verstehen und die Untersuchungszeit zu minimieren.

So können Sie eine Untersuchung in der Cyber Kill Chain beginnen

1. Gehen Sie in der Cyber Protect-Konsole zu **Schutz –> Vorfälle**.
2. Klicken Sie (innerhalb der angezeigten Vorfallsliste) in der ganz rechten Spalte des zu untersuchenden Vorfalls auf . Die Cyber Kill Chain für den ausgewählten Vorfall wird angezeigt.



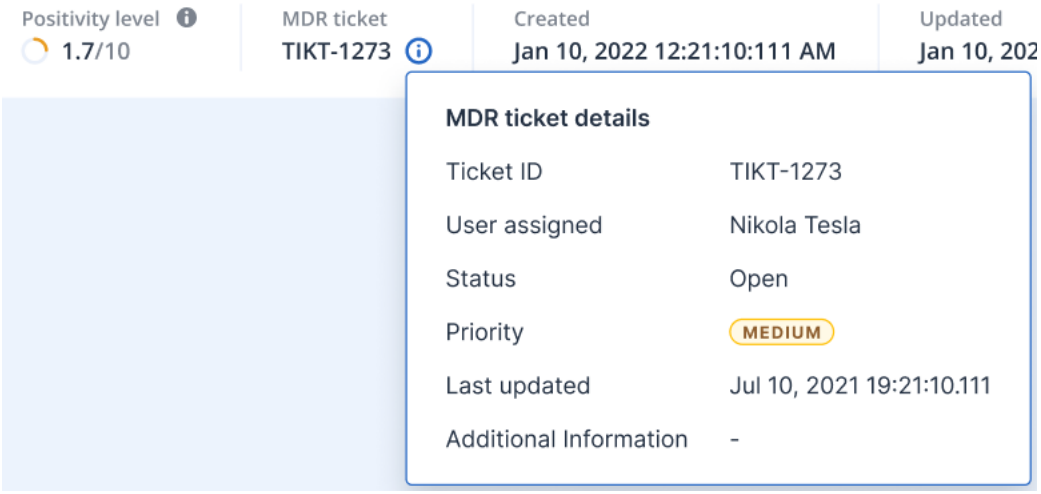
3. Die Bedrohungsstatusleiste im oberen Bereich der Seite zeigt eine Zusammenfassung des Vorfalls an. Die Bedrohungsstatusleiste enthält folgende Informationen:
   - Aktueller Bedrohungsstatus: Der Bedrohungsstatus wird automatisch vom System definiert. Jeder Vorfall, der **Nicht abgeschwächt** wurde, sollte möglichst schnell untersucht werden.

     Wichtig
     Ein Vorfall erhält den Status **Abgeschwächt**, wenn eine 'Wiederherstellung aus einem Backup' erfolgreich abgeschlossen wurde – oder wenn alle Erkennungen durch eine Aktion vom Typ 'Prozess stoppen', 'Unter Quarantäne stellen' oder 'Rollback durchführen' erfolgreich behoben wurde.

     Ein Vorfall erhält den Status **Nicht abgeschwächt**, wenn eine 'Wiederherstellung aus einem Backup' nicht erfolgreich abgeschlossen werden konnte – oder wenn mindestens eine Erkennung nicht durch eine Aktion vom Typ 'Prozess stoppen', 'Unter Quarantäne stellen' oder 'Rollback durchführen' behoben werden konnte.

     Sie können den Bedrohungsstatus außerdem manuell mit **Abgeschwächt** oder **Nicht abgeschwächt** festlegen. Wenn Sie einen der beiden Statuszustände auswählen, werden Sie aufgefordert, einen Kommentar einzugeben. Dieser Kommentar wird als Bestandteil der Untersuchungsaktivitäten gespeichert und kann auf der Registerkarte **Aktivitäten** eingesehen werden. Beachten Sie, dass die EDR-Funktionalität den Bedrohungsstatus weiterhin auf **Abgeschwächt** or **Nicht abgeschwächt** zurücksetzen kann, wenn neue Erkennungen für den Vorfall entdeckt wurden oder Antwortaktionen durchgeführt und erfolgreich abgeschlossen wurden.

- Vorfallsschweregrad: **Kritisch**, **Hoch** oder **Mittel**. Weitere Informationen finden Sie im Abschnitt '"Vorfälle überprüfen" (S. 988)'.
- Aktuelles Untersuchungsstadium: Eines der Stadien **Wird untersucht**, **Nicht gestartet** (das Standardstadium), **Falsch-positiv** oder **Geschlossen**. Sie sollten das Stadium ändern, wenn Sie mit der Untersuchung eines Vorfalls beginnen, um andere Kollegen über alle Änderungen am Vorfall zu informieren.
- Positivitätslevel: Gibt mit einem Wertebereich von 1-10 an, wie wahrscheinlich es sich bei einem Vorfall tatsächlich um einen schädlichen Angriff handelt. Weitere Informationen dazu finden Sie im Abschnitt '"Vorfälle überprüfen" (S. 988)'.
- Vorfallstyp: Wenn eins oder mehrere von **Ransomware erkannt**, **Malware erkannt**, **Verdächtiger Prozess erkannt**, **Schädlicher Prozess erkannt**, **Verdächtige URL blockiert** oder **Schädliche URL blockiert** zutreffen.
- Wenn Managed Detection & Response (MDR) auf dem Workload aktiviert wurde, wird ein Feld **MDR-Ticket** angezeigt. Sie können die Details des für den Vorfall erstellten MDR-Tickets (inkl. dem MDR-Sicherheitsanalysten, der dem Vorfall zugewiesen wurde) einsehen.



- Wann der Vorfall erstellt und aktualisiert wurde: Datum und Uhrzeit, als der Vorfall erkannt wurde, oder wann der Vorfall zuletzt aktualisiert wurde, weil neue Erkennungen innerhalb des Vorfalls erfasst wurden.

4. Klicken Sie auf die Registerkarte **Legend**, um die verschiedenen Knoten einzusehen, aus denen sich das Kill Chain-Diagramm zusammensetzt, und bestimmen Sie, welche Knoten angezeigt werden sollen. Weitere Informationen finden Sie im Abschnitt '"Die Cyber Kill Chain-Ansicht verstehen und anpassen" (S. 999)'.
5. Sie können den Vorfall untersuchen und beheben, indem Sie die nachfolgenden Schritte durchführen. Beachten Sie, dass dies ein typischer Arbeitsablauf für die Untersuchung und Behebung eines Vorfalls ist. Je nach Vorfall und Ihren eigenen Anforderungen kann dieser Ablauf jedoch variieren.
   a. Untersuchen Sie jeden Abschnitt des Angriffs auf der Registerkarte **Angriffsphasen**. Weitere Informationen finden Sie im Abschnitt '"So können Sie durch die Angriffsphasen navigieren"

(S. 1001)'.

b. licken Sie auf **Gesamten Vorfall beheben**, um Schadensbehebungsmaßnahmen anzuwenden. Weitere Informationen finden Sie im Abschnitt '"Einen gesamten Vorfall beheben" (S. 1013)'.

   Sie können auch Schäden auf einzelnen Knoten in der Cyber Kill Chain beheben, wie unter '"Antwortaktionen für einzelne Cyber Kill Chain-Knoten" (S. 1018)' beschrieben.

c. Überprüfen Sie die zur Abschwächung des Vorfalls vorgenommenen Maßnahmen auf der Registerkarte **Aktivitäten**. Weitere Informationen finden Sie im Abschnitt '"Die Aktionen verstehen, die zur Abschwächung eines Vorfalls ergriffen wurden" (S. 1005)'.

Die Cyber Kill Chain-Ansicht verstehen und anpassen

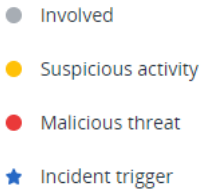
Wenn Sie mehr über die betroffenen Knoten in der Cyber Kill Chain erfahren wollen, greifen Sie auf die Legende zu. In der Legende werden alle an einem Vorfall beteiligten Knoten aufgeführt. So können Sie ermitteln, wie die verschiedenen Knoten durch den Angreifer beeinträchtigt wurden. Sie können auch festlegen, welche Knoten Sie in der Cyber Kill Chain ausblenden oder angezeigt haben wollen.

So können Sie auf die Legende zugreifen

1. Klicken Sie rechts neben dem Legenden-Bereich auf das Pfeilsymbol.
   Der Legenden-Bereich wird (wie unten gezeigt) erweitert.

2. Anhand der vier in der Legende verwendeten Hauptfarben (wie unten dargestellt) können Sie schnell erkennen, was mit jedem Knoten in der Cyber Kill Chain passiert ist. Diese farbcodierten Knoten sind auch in den Angriffsphasen enthalten, wie im Abschnitt '"So können Sie durch die

Angriffsphasen navigieren" (S. 1001)' erläutert.



So können Sie Knoten in der Cyber Kill Chain ausblenden oder anzeigen

1. Stellen Sie sicher, dass im erweiterten Legenden-Bereich das Symbol neben den Knoten zu sehen ist, die Sie in der Cyber Kill Chain anzeigen wollen. Sollte es sich bei dem angezeigten Symbol um handeln, dann klicken Sie auf das Symbol, um es zu zu ändern.
2. Wenn Sie einen Knoten in der Cyber Kill Chain ausblenden wollen, klicken Sie auf . Das Symbol wird daraufhin zu geändert und der Knoten wird nicht mehr in der Cyber Kill Chain angezeigt.

Die Angriffsphasen eines Vorfalls untersuchen

Über die Anzeige der Angriffsphasen eines Vorfalls wird Ihnen zu jedem Vorfall eine leicht verständliche Interpretation bereitgestellt.

Jede Angriffsphase fasst zusammen, was genau passiert ist und welche Objekte (die in der Cyber Kill Chain auch als *Knoten* bezeichnet werden) das Ziel des Angriffs waren. Wenn eine heruntergeladene Datei beispielsweise als etwas anderes getarnt war, wird dies in der Angriffsphase angezeigt und es werden Links zum entsprechenden Knoten in der Cyber Kill Chain (den Sie dann untersuchen können) sowie zur entsprechenden MITRE ATT&CK-Technik bereitgestellt.

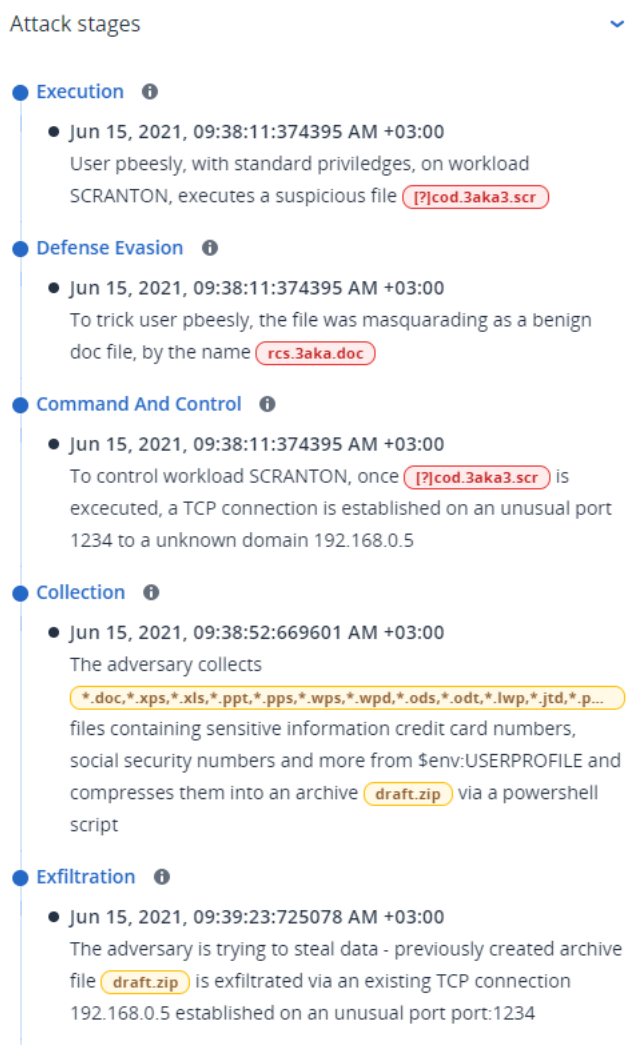
Jede Phase des Angriffs vermittelt Ihnen wichtige Informationen, um drei entscheidende Fragen zu klären:

- Welches Ziel hatte der Angreifer?
- Wie hat der Angreifer dieses Ziel erreicht?
- Welche Knoten wurden angegriffen?

Noch wichtiger ist, dass Sie durch die bereitgestellten Interpretationen den Zeitaufwand für die Untersuchung eines Vorfalls erheblich reduzieren können, da Sie Sicherheitsereignisse nicht mehr einzeln über eine Zeitleiste oder ein Knotendiagramm durchgehen und anhand dessen eine Interpretation des Angriffs erstellen müssen.

Die Angriffsphasen enthalten außerdem Informationen über kompromittierte Dateien, die sensible Daten (z.B. Kreditkarten- oder Sozialversicherungsnummern) enthalten, wie in der Phase **Sammlung** im unten stehenden Beispiel gezeigt.

Weitere Informationen finden Sie im Abschnitt '"Welche Informationen sind in einer Angriffsphase enthalten?" (S. 1001)'.



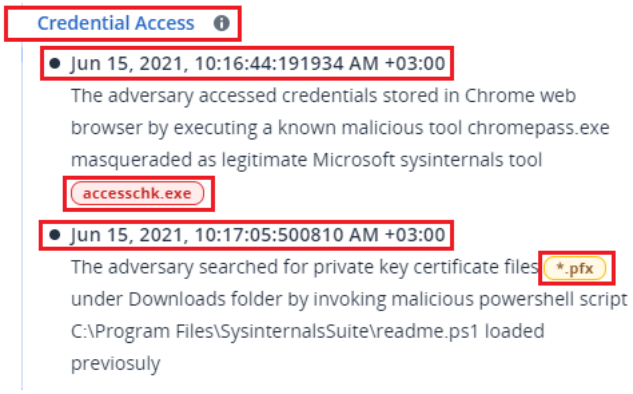
So können Sie durch die Angriffsphasen navigieren

Die Angriffsphasen werden in chronologischer Reihenfolge aufgeführt. Scrollen Sie nach unten, wenn Sie die vollständige Liste der Angriffsphasen für den Vorfall einsehen wollen.

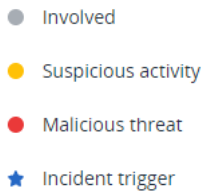
Wenn Sie eine bestimmte Angriffsphase genauer untersuchen wollen, klicken Sie auf eine beliebige Stelle in der Angriffsphase, um zum entsprechenden Knoten im Cyber Kill Chain-Diagramm zu wechseln. Weitere Informationen darüber, wie Sie durch das Cyber Kill Chain-Diagramm und bestimmte Knoten navigieren können, finden Sie im Abschnitt '"Einzelne Knoten in der Cyber Kill Chain untersuchen" (S. 1003)'.

Welche Informationen sind in einer Angriffsphase enthalten?

Jede Angriffsphase stellt Ihnen eine leicht verständliche Interpretation des Angriffs zur Verfügung, die in leicht lesbarer Sprache verfasst ist. Diese Interpretation besteht aus einer Reihe von Elementen, die nachfolgend dargestellt und in der unteren Tabelle beschrieben werden.



Angriffsphasen-Element	Beschreibung
Header	Liefert eine Beschreibung über die Aktivitäten und Absichten der Angreifers (im obigen Beispiel: **Zugriff auf Anmeldedaten**) und enthält zudem einen Link auf eine entsprechende MITRE ATT&CK-Technik. Klicken Sie auf den Link, wenn Sie mehr Informationen über die Technik auf der MITRE ATT&CK-Website erhalten wollen. **Hinweis** Wenn für eine Angriffsphase keine MITRE ATT&CK-Technik bekannt ist, wird im Text des Headers kein Link angezeigt. Dies ist bei allgemeinen Techniken relevant, z. B. bei Dateien, die in einem zufälligen Ordner entdeckt werden.
Zeitstempel	Der Zeitpunkt, an dem die Angriffsphase stattgefunden hat.
Technik	Wie der Angreifer sein Ziel technisch erreicht hat und welche Objekte (Registry-Einträge, Dateien oder geplante Tasks) betroffen waren. In der Textbeschreibung der Angriffstechnik befinden sich farbcodierte Links zu jedem betroffenen Knoten in der Cyber Kill Chain (wie im oberen Beispiel gezeigt). Über diese farbcodierten Links können Sie schnell zu dem betroffenen Knoten wechseln und untersuchen, was genau vorgefallen ist. Die in einer Angriffsphase verwendeten Farben kennzeichnen Folgendes:

Angriffsphasen-Element	Beschreibung
	 Anhand der obigen Legende ist ersichtlich, dass das Angriffsphasen-Beispiel 'Zugriff auf Anmeldedaten' je einen Link auf einen Malware-Knoten accesschk.exe und einen verdächtigen Datei-Knoten *.pfx enthält (wenn Sie auf die entsprechenden Links klicken, gelangen Sie zu dem dazugehörigen Knoten in der Cyber Kill Chain). Weitere Informationen darüber, wie Sie durch die Knoten navigieren können und welche Aktionen verfügbar sind, finden Sie im Abschnitt '"Einzelne Knoten in der Cyber Kill Chain untersuchen" (S. 1003)'. Beachten Sie, dass sich in den Angriffsphasen auch Links zu Dateiknoten befinden, die Informationen über kompromittierte Dateien mit sensiblen Daten (wie geschützte Gesundheitsinformationen [PHI], Kreditkartennummern und Sozialversicherungsnummern) enthalten.

Hinweis
Jede Angriffsphase ist ein einzelnes Erkennungsereignis. Die in jeder Phase aufgeführten Inhalte (Header, Zeitstempel, Technik) werden basierend auf bestimmten Parametern im Erkennungsereignis generiert, die auf Angriffsphasen-Vorlagen beruhen, die von der Endpoint Detection & Response (EDR)-Funktionalität gespeichert werden.

Einzelne Knoten in der Cyber Kill Chain untersuchen

Sie können nicht nur die Angriffsphasen überprüfen, sondern auch durch jeden einzelnen angegriffenen Knoten in der Cyber Kill Chain navigieren. Dadurch können Sie bis zu bestimmten Knoten in der Cyber Kill Chain gehen und (je nach Bedarf) jeden dieser Knoten einzeln untersuchen und dort aufgetretene Schäden beheben.

So können Sie beispielsweise bestimmen, wie wahrscheinlich es sich bei einem Vorfall um einen wirklich schädlichen Angriff handelt. In Abhängigkeit von Ihrer Untersuchung können Sie auch

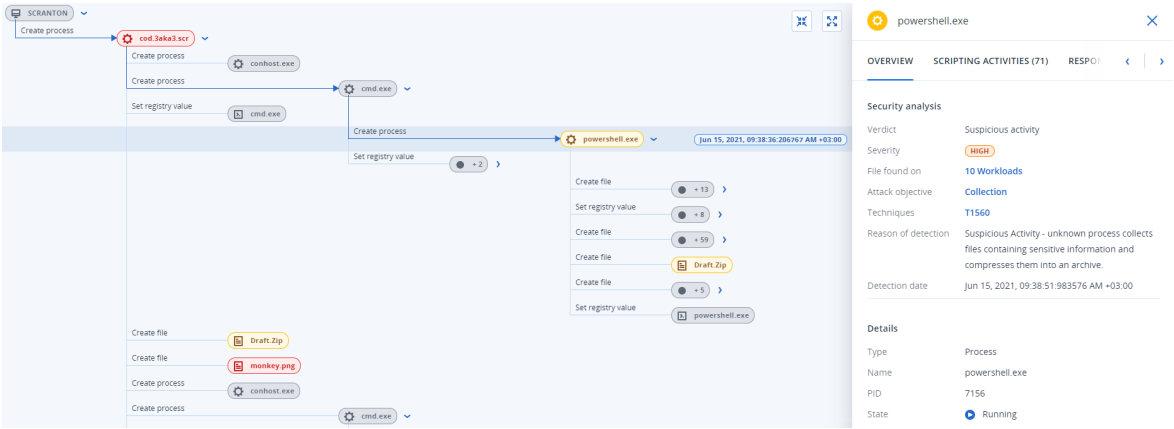
diverse Antwortaktionen auf den betreffenden Knoten anwenden – z.B. einen Workload zu isolieren oder eine verdächtige Datei unter Quarantäne zu stellen.

So können Sie einzelne Knoten in der Cyber Kill Chain untersuchen

1. Gehen Sie in der Cyber Protect-Konsole zu **Schutz –> Vorfälle**.
2. Klicken Sie (innerhalb der angezeigten Vorfallsliste) in der ganz rechten Spalte des zu untersuchenden Vorfalls auf . Die Cyber Kill Chain für den ausgewählten Vorfall wird angezeigt.
3. Navigieren Sie zu dem entsprechenden Knoten und klicken Sie auf diesen, damit die Seitenleiste für diesen Knoten angezeigt wird.

Hinweis
Klicken Sie auf den Knoten, damit dieser erweitert wird und die mit ihm assoziierten Knoten angezeigt werden.

Wenn Sie etwa im untenstehenden Beispiel auf den Knoten **powershell.exe** klicken, wird die Seitenleiste für diesen Knoten geöffnet. Sie können auch neben dem Knoten auf das Pfeilsymbol klicken, um sich die dazugehörigen Knoten anzeigen zu lassen – einschließlich der Dateien und Registry-Werte, die vom Knoten **powershell.exe** betroffen sein können. Sie können dann wiederum auf diese assoziierten Knoten klicken, wenn Sie weitere Untersuchungen durchführen wollen.



4. Untersuchen Sie die Informationen, die in den Registerkarten der Seitenleiste angezeigt werden:
   - **Überblick**: Enthält zwei Hauptabschnitte, die eine Sicherheitsübersicht über den angegriffenen Knoten bieten.
     - **Sicherheitsanalyse**: Zeigt eine Analyse des angegriffenen Knotens, einschließlich der EDR-Bewertung zur Bedrohung (wie z.B. verdächtige Aktivitäten), das Ziel des Angriffs gemäß den MITRE-Angriffstechniken (klicken Sie auf den Link, um zur MITRE-Website zu gelangen), den Grund für die Erkennung sowie die Anzahl der Workloads, die möglicherweise vom Angriff betroffen sind (klicken Sie auf den Link **n Workloads**, um sich die betroffenen Workloads anzeigen zu lassen).

Hinweis
Der **n Workloads**-Link verdeutlicht, dass ein bestimmtes schädliches oder verdächtiges Objekt auf anderen Workloads *gefunden* wurde. Das bedeutet nicht zwangsläufig, dass der Angriff auch auf diesen anderen Workloads stattfindet, sondern dass es einen Kompromittierungsindikator für diese Workloads gibt. Der Angriff kann auch schon stattgefunden haben (und damit einen weiteren Vorfall generiert haben) oder der Angreifer bereitet sich gerade darauf vor, diese anderen Workloads mit seinem Toolkit anzugreifen.

  - **Details**: Enthält Detailinformationen über den Knoten – wie etwa dessen Typ, Name und aktuelles Stadium, den Pfad zum Knoten sowie alle Datei-Hashes und digitalen Signaturen (z.B. MD5 und Zertifikatsseriennummern).
- **Skripting-Aktivitäten**: Enthält Details zu allen Skripten, die beim Angriff aufgerufen oder geladen wurden. Klicken Sie auf , um das Skript zur weiteren Untersuchung in Ihre Zwischenablage zu kopieren.

  Hinweis
  Die Registerkarte **Skripting-Aktivitäten** wird nur für solche Prozessknoten angezeigt, die Befehle oder Skripte ausführen (z.B. Befehle über die Eingabeaufforderung [cmd.exe] oder die PowerShell).

- **Antwortaktionen**: Enthält mehrere Bereiche, die (je nach Knotentyp) zusätzliche Untersuchungs-, Schadensbehebung- und Präventionsmaßnahmen ermöglichen.
  So können Sie beispielsweise für Workload-Knoten diverse Antwortaktionen (wie Forensik-Backups oder Wiederherstellungen aus Backups) definieren. Bei schädlichen oder verdächtigen Knoten können Sie beispielsweise den Knoten stoppen oder unter Quarantäne stellen, durch den Angriff verursachte Änderungen rückgängig machen und einen entsprechenden Prozess zu einer Positivliste oder Blockliste des Schutzplans hinzufügen.
  Weitere Informationen darüber, wie Sie Antwortaktionen auf bestimmte Knoten anwenden können, finden Sie im Abschnitt '"Antwortaktionen für einzelne Cyber Kill Chain-Knoten" (S. 1018)'.
- **Aktivitäten**: Zeigt die Aktionen an, die auf den Vorfall angewendet wurden - und zwar in chronologischer Reihenfolge. Weitere Informationen finden Sie im Abschnitt '"Die Aktionen verstehen, die zur Abschwächung eines Vorfalls ergriffen wurden" (S. 1005)'.

Die Aktionen verstehen, die zur Abschwächung eines Vorfalls ergriffen wurden

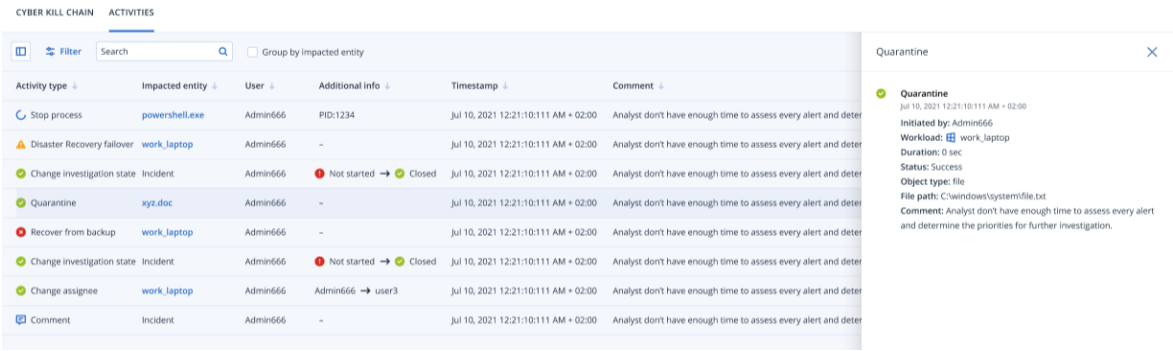
Nachdem Sie einen Vorfall überprüft und den Angriffsverlauf untersucht haben, werden Sie typischerweise Antwortaktionen anwenden. Nachdem die Antwortaktionen angewendet wurden, können Sie diese an verschiedenen Stellen einsehen, um ein besseres Verständnis dafür zu erhalten, welche Schritte ergriffen wurden, um den Vorfall abzuschwächen.

Hinweis
Bei Vorfällen, die von Präventionsschichten erstellt wurden, werden automatisch die Aktionen angewendet, die im entsprechenden Schutzplan konfiguriert wurden. Bei Erkennungspunkten müssen Sie die entsprechenden Antwortaktionen definieren, um jedes Angriffsszenario abzuschwächen.

Zum besseren Verständnis der ergriffenen Maßnahmen können Sie sich alle Antwortaktionen anzeigen lassen, die auf einen gesamten Vorfall angewendet wurden. Alternativ können Sie sich diejenigen Aktionen anzeigen lassen, die nur auf einen bestimmten Knoten in der Cyber Kill Chain des Vorfalls angewendet wurden.

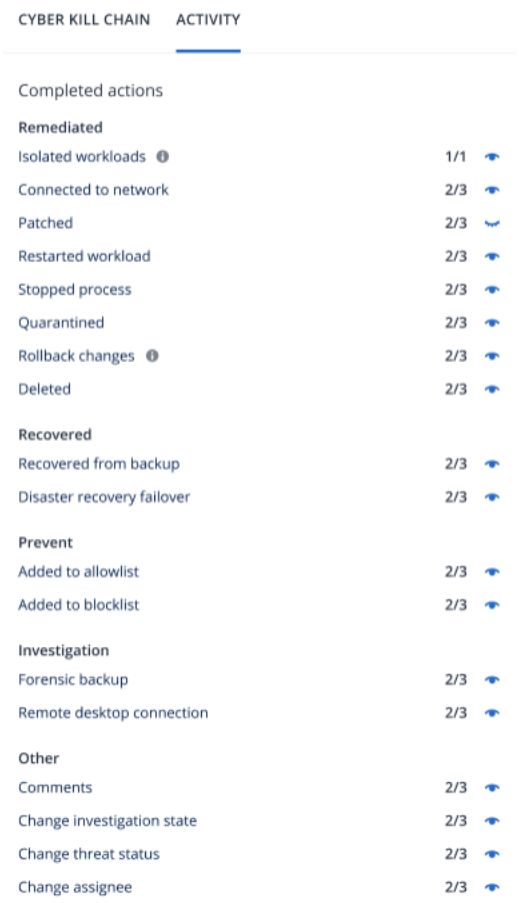
So können Sie sich alle Antwortaktionen anzeigen lassen, die auf einen Vorfall angewendet wurden

1. Gehen Sie in der Cyber Protect-Konsole zu **Schutz –> Vorfälle**.
2. Klicken Sie (innerhalb der angezeigten Vorfallsliste) in der ganz rechten Spalte des zu untersuchenden Vorfalls auf . Die Cyber Kill Chain für den ausgewählten Vorfall wird angezeigt.
3. Klicken Sie auf die Registerkarte **Aktivitäten**.
   Es wird eine Liste der Antwortaktionen angezeigt, die bereits auf den Vorfall angewendet wurden.



4. Sie können eine Reihe von Aktionen auf die angezeigte Liste anwenden:
   - Klicken Sie auf eine Zeile mit einem Aktivitätstyp, um sich weitere Informationen über die ausgewählte Aktivität anzeigen zu lassen. Die Informationen werden (wie in Schritt 3 gezeigt) in einer Seitenleiste angezeigt und enthalten Details darüber, wer die Aktion initiiert hat, wie deren Status sowie Dateipfad ist und welche Kommentare der Initiator hinzugefügt hat.
   - Sie können das Feld **Suchen** verwenden, um eine bestimmte Aktion zu finden.
   - Klicken Sie auf **Filter**, wenn Sie bestimmte Filter auf die Liste anwenden wollen.
   - Aktivieren Sie das Kontrollkästchen **Nach betroffener Entität gruppieren**, damit die relevanten Aktionen nach der jeweiligen Entität gruppiert werden.
   - Klicken Sie auf , wenn Sie die Liste der abgeschlossenen Aktionen ein- bzw. wieder ausblenden wollen.

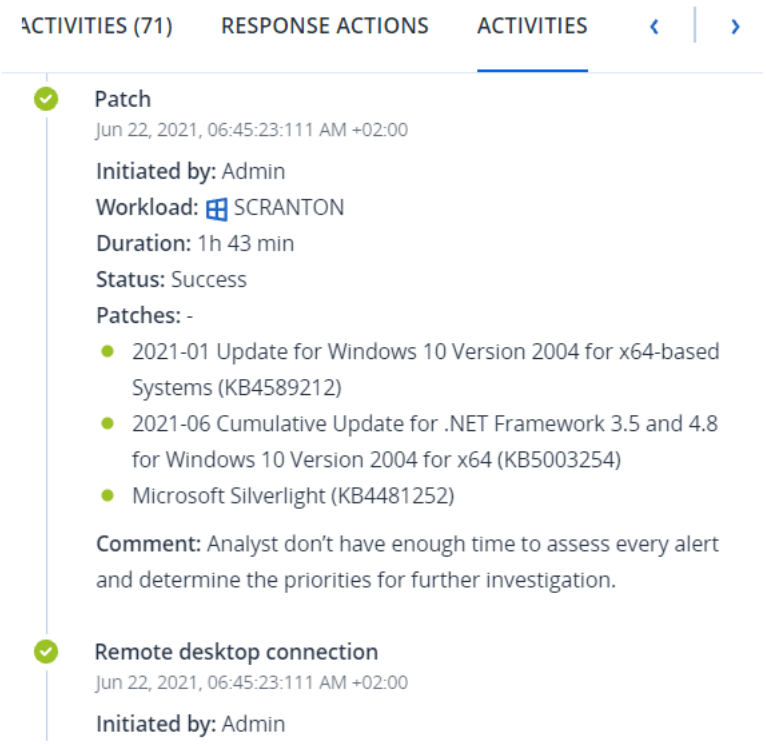
Stellen Sie sicher, dass das Symbol neben den Aktionen aufgeführt ist, die Sie anzeigen wollen. Wenn Sie eine Aktion aus der angezeigten Liste ausblenden wollen, müssen Sie erneut auf das Symbol klicken, damit es zu geändert wird.



So können Sie sich die Antwortaktionen anzeigen lassen, die auf einen bestimmten Knoten angewendet wurden

1. Klicken Sie in der Cyber Kill Chain auf einen Knoten, damit die Seitenleiste für diesen Knoten angezeigt wird.

2. Klicken Sie auf die Registerkarte **Aktivitäten**.



3. Wenn Sie ein umfassendes Verständnis darüber erhalten wollen, welche Aktionen angewandt wurden und warum dies erfolgte, müssen Sie ggf. durch die angewendeten Antwortaktionen für diesen Knoten blättern. Bei Remote-Desktop-Verbindungen können Sie beispielsweise einsehen, wer die Aktion gestartet hat und wann dies erfolgte, wie lange die Aktion gedauert hat und welchen Gesamtstatus sie hatte (ob sie erfolgreich war, fehlgeschlagen ist oder mit Fehlern abgeschlossen wurde).

Auf Kompromittierungsindikatoren (IoCs) für öffentlich bekannte Angriffe auf Ihre Workloads prüfen

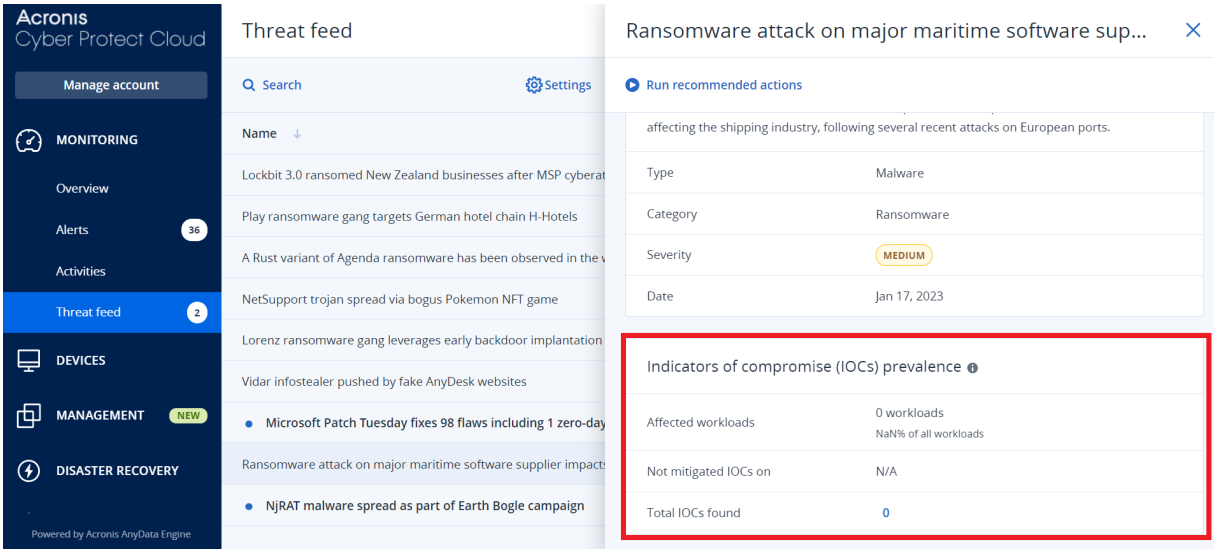
Die Endpoint Detection & Response (EDR)-Funktionalität umfasst die Möglichkeit, Ihre Workloads auf vorhandene, bekannte Angriffe aus den Bedrohungsfeeds untersuchen zu lassen. Diese Bedrohungsfeeds werden automatisch anhand von Bedrohungsdaten generiert, die von den Cyber Protection Operations Centern (CPOCs) geliefert werden. Mit der EDR-Funktionalität können Sie überprüfen, ob Ihr Workload von einer solchen Bedrohung betroffen ist (oder nicht), und dann die notwendigen Maßnahmen zur Beseitigung der Bedrohung ergreifen.

Sie können auf die Bedrohungsfeeds über das Menü **Monitoring** in der Cyber Protect-Konsole zugreifen. Weitere Informationen finden Sie im Abschnitt '"Bedrohungsfeed" (S. 331)'.

Klicken Sie auf einen Bedrohungsfeed, wenn Sie Details zu einer bestimmten Bedrohung überprüfen und feststellen wollen, ob Ihre Workloads davon betroffen sind. Sie können die Anzahl der erkannten IoCs sowie der betroffenen Workloads einsehen und bis zu den Workloads herunterblättern, die nicht abgeschwächte IoCs enthalten.

Hinweis

Wenn für den Schutzplan die EDR-Option nicht aktiviert wurde, wird diese zusätzliche Bedrohungsfeed-Funktionalität (wie unten dargestellt) nicht angezeigt.



Die Bedrohungsfeed-Einstellungen definieren

Sie können eine Reihe von Einstellungen für den Bedrohungsfeed festlegen, damit bekannte Bedrohungen automatisch aufgespürt und abgeschwächt werden.

So können Sie die Bedrohungsfeed-Einstellungen definieren

1. Gehen Sie in der Cyber Protect-Konsole zu **Monitoring –> Bedrohungsfeed**.
2. Klicken Sie in der angezeigten Bedrohungsfeed-Seite auf **Einstellungen**.

3. Wählen Sie im angezeigten Dialog eine der folgenden Optionen aus:

Option	Beschreibung
Nach Kompromittierungsindikatoren (IoCs) suchen	Klicken Sie auf den Schalter, damit die automatische Suche nach IoCs auf Ihren Workloads aktiviert wird. Wenn diese Option aktiviert ist, werden auch die Optionen **Aktion bei Erkennung** und **Alarm generieren** angezeigt.
Aktion bei Erkennung	Wählen Sie im Listenfeld diejenige Aktion aus, die auf die betreffenden Dateien angewendet werden soll, wenn auf einem Workload eine Bedrohung entdeckt wird: • **Keine Aktion** • **Quarantäne** • **Löschen** • **Workloads isolieren**
Alarm generieren	Aktivieren Sie das Kontrollkästchen, damit ein Alarm erzeugt wird, wenn ein IoC auf einem Workload gefunden wird. Der Alarm wird auf der Seite Alarmmeldungen angezeigt.

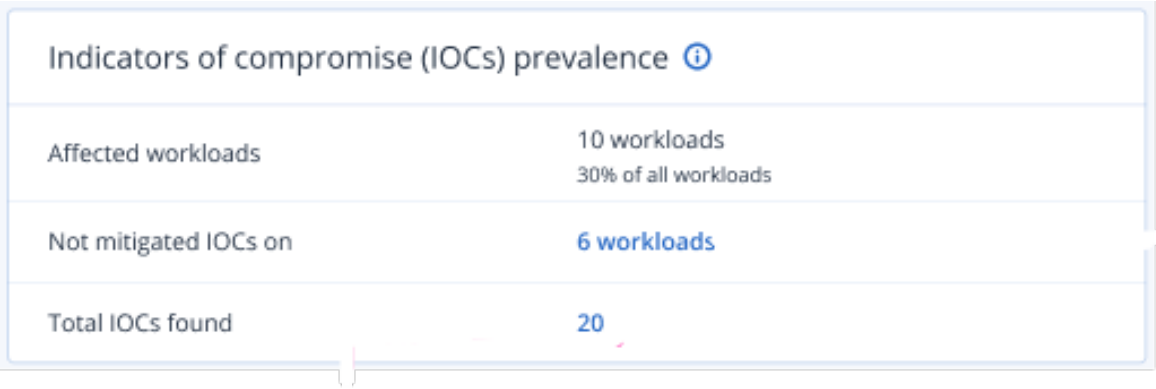
4. Klicken Sie auf **Anwenden**.

Die IoCs (Kompromittierungsindikatoren) eines betroffenen Workloads überprüfen und abschwächen

Wenn die Endpoint Detection & Response (EDR)-Funktionalität in einem Schutzplan aktiviert wurde, können Sie sich alle bekannten Bedrohungen anzeigen lassen, die die Workloads in dem Schutzplan betreffen. Sie können auch alle verbliebenen Kompromittierungsindikatoren (IoCs) abschwächen, die nicht automatisch abgeschwächt wurden. Informationen darüber, wie Sie IoCs automatisch abschwächen können, finden Sie im Abschnitt '"Die Bedrohungsfeed-Einstellungen definieren" (S. 1009)'.

So können Sie betroffene Workloads überprüfen und abschwächen

1. Gehen Sie in der Cyber Protect-Konsole zu **Monitoring –> Bedrohungsfeed**.
2. Klicken Sie auf einen Thread, um die Details zu diesem Threat einzusehen.
3. Klicken Sie im Bereich **Verbreitung der Kompromittierungsindikatoren (IoCs)** auf den Link ***n* Workloads**, um sich die Workloads mit nicht abgeschwächten IoCs anzeigen zu lassen.



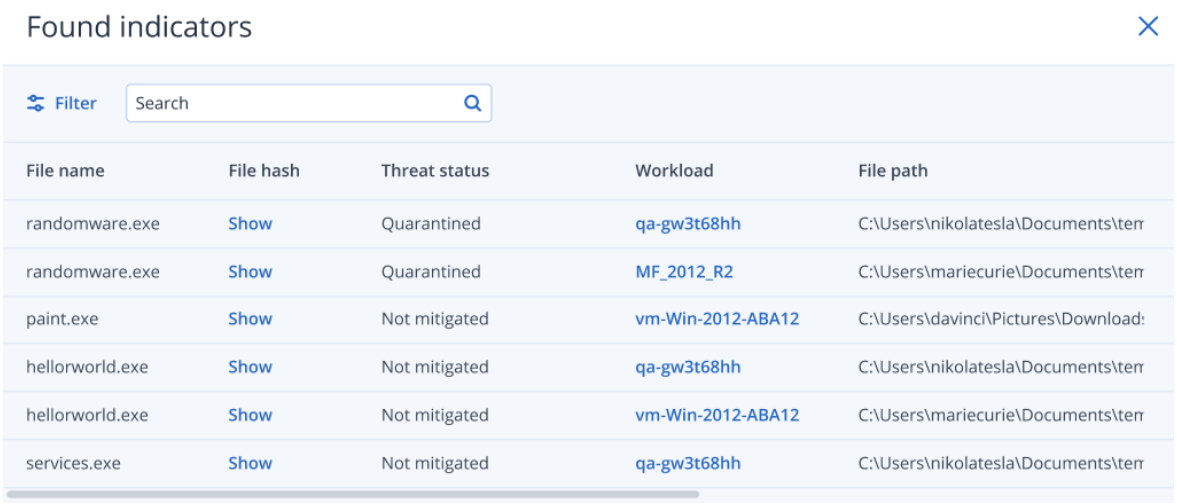
4. Klicken Sie auf der angezeigten Workloads-Seite auf den entsprechenden Workload und überprüfen Sie dessen Details. Sie können bestimmte Funktionalitäten auf dem Workload ausführen – wie etwa zusätzliche URL-Filter zu definieren (siehe Abschnitt '"URL-Filterung" (S. 928)') oder schädliche Prozesse zu blockieren (siehe den Abschnitt 'Ausschlusskriterien' unter "Einstellungen für die Antivirus & Antimalware Protection" (S. 901)).
   Ein Beispiel: Wenn ein Bedrohungsfeed signalisiert, dass ein Workload von einer IoC betroffen ist, dann müssen Sie diesen zuerst lokalisieren und dann (wie im Abschnitt '"Erkannte IoCs überprüfen und analysieren" (S. 1011)' beschrieben) analysieren. Anschließend gehen Sie zum entsprechenden Schutzplan für den Workload und definieren Sie eine zusätzliche Schutzfunktion – beispielsweise, dass schädliche Datei-Hashes oder Prozesse blockiert werden sollen.

Erkannte IoCs überprüfen und analysieren

Neben der Möglichkeit, alle von bekannten Bedrohungen betroffenen Workloads zu überprüfen, können Sie auch bestimmte Kompromittierungsindikatoren (IoCs) überprüfen und analysieren. Sie können so die einzelnen Workloads einsehen, die von einem IoC betroffen sind, und diesen abschwächen.

So können Sie IoCs überprüfen und analysieren

1. Gehen Sie in der Cyber Protect-Konsole zu **Monitoring –> Bedrohungsfeed**.
2. Klicken Sie auf einen Thread, um die Details zu diesem Threat einzusehen.
3. Klicken Sie im Bereich **Verbreitung der Kompromittierungsindikatoren (IoCs)** auf den Link **Insgesamt gefundene IoCs**.
   Die Seite 'Gefundene Indikatoren' wird angezeigt.



4. (Optional) Sie können die Option **Filter** verwenden, um die Liste der IoCs nach deren Status zu filtern. Mit der **Suchen**-Funktion können Sie außerdem nach bestimmten IoCs suchen.
5. Wenn Sie sich einen Workload genauer ansehen wollen, der von einem IoC betroffen ist, klicken Sie auf den dazugehörigen Link in der Spalte **Workload**. Sie können anschließend diverse Aktionen mit dem Workload durchführen – wie etwa die Patch-Verwaltung ausführen oder den entsprechenden Schutzplan ändern.
6. (Optional) Klicken Sie in der Spalte **Datei-Hash** auf **Anzeigen**, um die Datei-Hash-Werte einzusehen, die für einen bestimmten IoC gefunden wurden. Im angezeigten Dialogfeld können Sie dann auf klicken, um den Datei-Hash-Wert des IoCs in einen Texteditor zu kopieren.

Vorfälle beheben

Mit der Endpoint Detection & Response (EDR)-Funktionalität können Sie entweder einen gesamten Vorfall beheben oder nur die einzelnen Angriffspunkte eines Vorfalls.

Wenn Sie einen gesamten Vorfall beheben, können Sie die Schadensbehebungsmaßnahmen auswählen, die Sie global auf den Vorfall anwenden wollen. Wenn Sie den Vorfall deutlich genauer verwalten müssen, können Sie (je nach Bedarf) auch einzelne Angriffspunkte beheben. Ein Beispiel: Sie wollen einen Workload vom Netzwerk isolieren, um laterale Bewegungen oder Steuerungs- und Kontroll-Aktivitäten (auch C&C-Aktivitäten genannt, für Command and Control) zu unterbinden. Dadurch wird sichergestellt, dass trotz der Workload-Isolation alle Acronis Cyber Protect-Technologien weiterhin funktionieren und somit Untersuchungen durchgeführt werden können.

Die EDR-Funktionalität gewährleistet eine effektive Schadensbehebung durch folgende Maßnahmen:

- Abschwächen – um sicherzustellen, dass eine Bedrohung gestoppt wird.
- Wiederherstellen – um sicherzustellen, dass ausgefallene Services umgehend wieder online sind.
- Verhindern - um sicherzustellen, dass Techniken, die bei einem Angriff verwendet wurden, zukünftig unterbunden werden.

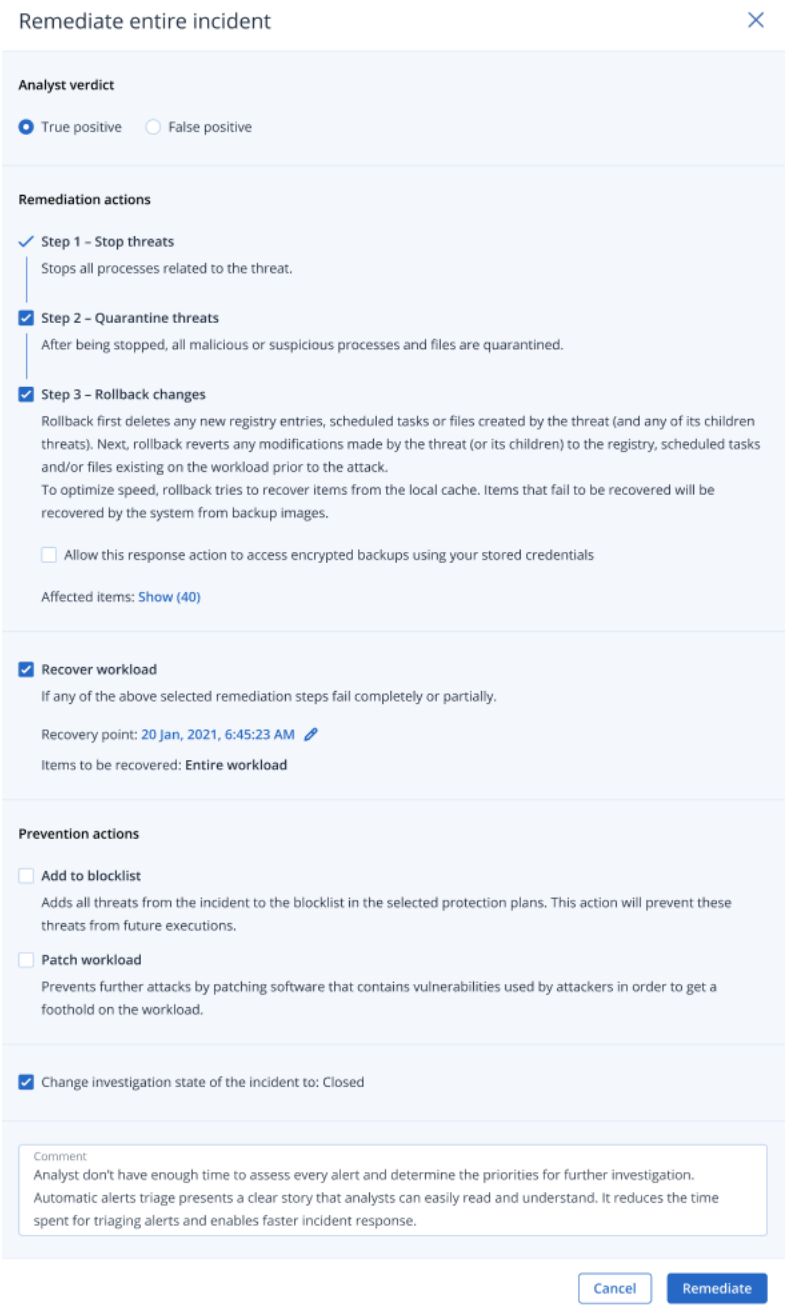
Einen gesamten Vorfall beheben

Wenn Sie einen gesamten Vorfall beheben, können Sie die Schadensbehebungsmaßnahme(n) schnell und einfach auswählen, die Sie global auf den Vorfall anwenden wollen. Die Endpoint Detection & Response (EDR)-Funktionalität führt Sie Schritt für Schritt durch den Schadensbehebungsprozess.

Wie Sie Ihr Netzwerk und einen Vorfall in mehr Details verwalten können, ist im Abschnitt '"Antwortaktionen für einzelne Cyber Kill Chain-Knoten" (S. 1018)' erläutert.

So können Sie einen gesamten Vorfall beheben

1. Gehen Sie in der Cyber Protect-Konsole zu **Schutz –> Vorfälle**.
2. Klicken Sie (innerhalb der angezeigten Vorfallsliste) in der ganz rechten Spalte des zu untersuchenden Vorfalls auf  . Die Cyber Kill Chain für den ausgewählten Vorfall wird angezeigt.
3. Klicken Sie auf **Gesamten Vorfall beheben**. Das Dialogfenster 'Gesamten Vorfall beheben' wird angezeigt.



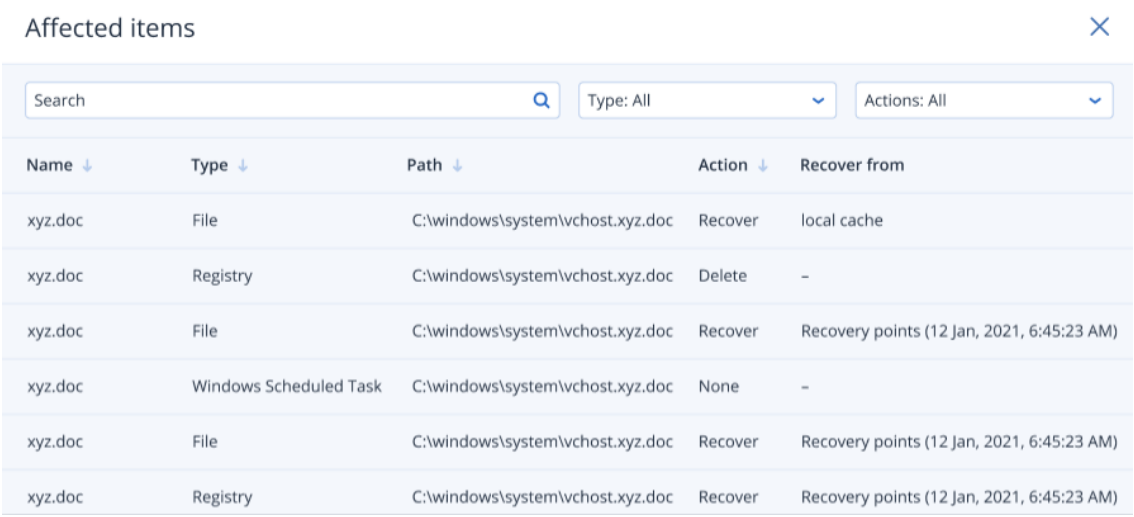
4. Wählen Sie in Abhängigkeit davon, was bei der Untersuchung des Vorfalls herausgekommen ist, im Bereich **Analystenbewertung** eine der folgenden Möglichkeiten:
   - **Echt positiv**: Wählen Sie diese Option, wenn Sie sicher sind, dass es sich um einen echten Angriff handelt. Nach dieser Festlegung können Sie dann, wie in den folgenden Schritten beschrieben, Schadensbehebung- und Präventionsmaßnahmen hinzufügen.
   - **Falsch positiv**: Wählen Sie diese Option, wenn Sie sicher sind, dass es sich nicht um einen echten Angriff handelt. Bei diesem Modus können Sie außerdem festlegen, wie verhindert werden soll, dass dieser Vorfall erneut erkannt wird. Dazu können Sie den Vorfall beispielsweise zur Positivliste des entsprechenden Schutzplans hinzufügen.

Hinweis
Wenn Sie die Einstellung **Falsch positiv** festlegen, können Sie nur noch Präventionsmaßnahmen definieren. Weitere Informationen finden Sie im Abschnitt '"Einen falsch-positiven Vorfall beheben" (S. 1017)'.

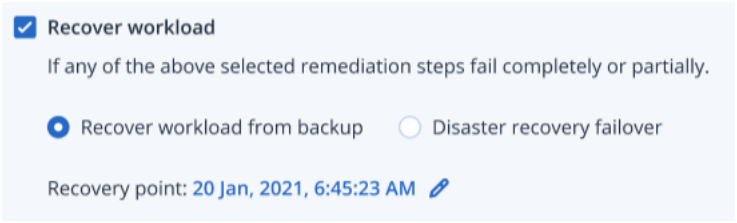
5. Im Bereich **Behebungsmaßnahmen** können Sie die nachfolgenden Schritte zur Schadensbehebung durchführen. Beachten Sie, dass diese in der richtigen Reihenfolge ausgeführt werden müssen. So ist es beispielsweise nicht möglich, Schritt 2 auszuwählen, bevor Schritt 1 abgeschlossen wurde.
   a. **Schritt 1 – Bedrohungen stoppen**: Aktivieren Sie das Kontrollkästchen, damit alle Prozesse gestoppt werden, die mit der Bedrohung zusammenhängen.
   b. **Schritt 2 – Bedrohungen unter Quarantäne stellen**: Sobald die Bedrohung gestoppt wurde, können Sie das Kontrollkästchen aktivieren, damit alle schädlichen und verdächtigen Prozesse bzw. Dateien unter Quarantäne gestellt werden.
   c. **Schritt 3 – Änderungen zurücksetzen**: Nachdem die Bedrohungen unter Quarantäne gestellt wurden, können Sie das Kontrollkästchen aktivieren, damit alle neuen Registry-Einträge, geplanten Tasks oder Dateien gelöscht werden, die von der Bedrohung (und deren untergeordneten Bedrohungen) erstellt wurden. Als Nächstes werden durch den Rollback-Prozess alle Änderungen zurückgesetzt, die von der Bedrohung (oder deren untergeordneten Bedrohungen) an der Registry, geplanten Tasks und/oder Dateien vorgenommen wurden und die vor dem Angriff auf dem Workload bereits vorhanden waren. Um den Prozess zu beschleunigen, wird der Rollback-Prozess versuchen, die entsprechenden Elemente aus dem lokalen Cache wiederherzustellen. Elemente, die nicht auf diese Weise wiederhergestellt werden können, werden vom System dann aus Backup-Images wiederhergestellt.

   Hinweis
   Der Rollback-Prozess verwendet für seine Wiederherstellung nur Elemente aus dem lokalen Cache. Die Durchführung eines Rollback-Prozesses aus Backup-Archiven wird in zukünftigen Versionen verfügbar sein.

   Aktivieren Sie das Kontrollkästchen **Diese Antwortaktionen erlauben, mithilfe gespeicherter Anmeldedaten auf verschlüsselte Backups zuzugreifen**, wenn der Zugriff auf die entsprechenden Backups verschlüsselt ist. Die EDR-Funktionalität greift auf die gespeicherten Anmeldedaten des Benutzers zu, um die verschlüsselten Archive zu dechiffrieren und nach den gewünschten Dateien zu suchen.
   Sie können außerdem noch auf **Betroffene Elemente** klicken. Dadurch können Sie die durch den Rollback-Prozess zurückgesetzten Elemente (Dateien, Registry-Einträge oder geplante Tasks) sowie die angewendeten Aktionen (**Löschen**, **Wiederherstellen** oder **Keine**) einsehen – und zudem, ob die betreffenden Elemente aus dem lokalen Cache oder aus Backup-Images wiederhergestellt werden.



d. **Workload wiederherstellen**: Sollte eine der oben genannten Schritte zur Schadensbehebung fehlschlagen (egal, ob ganz oder teilweise), können Sie dieses Kontrollkästchen aktivieren, um einen Workload wiederherstellen zu lassen.

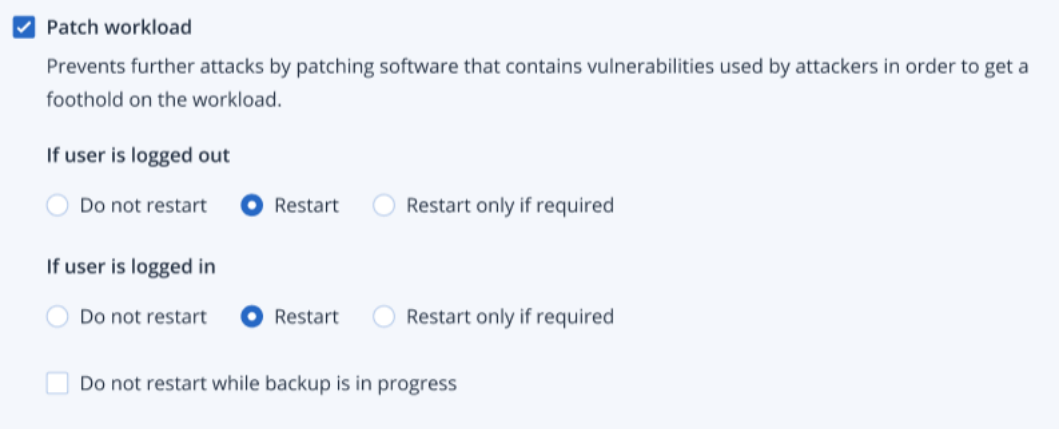


Wählen Sie eine der folgenden Recovery-Optionen:

- **Workload aus Backup wiederherstellen**: Ermöglicht Ihnen, einen Workload aus einem bestimmten Recovery-Punkt wiederherzustellen. Klicken Sie auf das Recovery-Punkt-Bearbeiten-Symbol, um diesen aus einer Liste von Recovery-Backups auswählen zu können.
- **Disaster Recovery-Failover**: Ermöglicht Ihnen, einen Disaster Recovery-Prozess auszuführen, sofern diese Funktionalität für Ihren Schutzplan aktiviert wurde. Wir empfehlen, dass Sie diese Option bei geschäftskritischen Workloads (wie etwa Active Directory- oder Datenbank-Server) verwenden. Weitere Informationen finden Sie im Abschnitt '"Disaster Recovery implementieren" (S. 804)'.

6. Im Bereich **Präventionsmaßnahmen** können Sie die nachfolgenden Schritte zur Schadensbehebung durchführen:
   - **Zur Blockliste hinzufügen**: Aktivieren Sie das Kontrollkästchen und wählen Sie dann aus der angezeigten Liste der Schutzpläne die passenden Schutzpläne aus. Diese Präventionsmaßnahme stellt sicher, dass alle Erkennungen des Vorfalls für die ausgewählten Schutzpläne blockiert werden.
   - **Workload patchen**: Aktivieren Sie dieses Kontrollkästchen, um Software-Schwachstellen zu beheben und Angreifer daran zu hindern, Zugriff auf den Workload zu erhalten. Sie können dann die passende Aktion auswählen, die durchgeführt werden soll, sobald der Patch erfolgreich implementiert wurde (**Nicht neu starten**, **Neustart** oder **Neustart nur bei Bedarf**) – je nachdem, ob der Benutzer angemeldet ist oder nicht.

Sie können außerdem das Kontrollkästchen **Kein Neustart, während ein Backup läuft** aktivieren, wenn Sie sicherstellen wollen, dass der Workload nicht neu gestartet wird, falls gerade ein Backup erstellt wird.



7. Aktivieren Sie das Kontrollkästchen **Untersuchungsstadium des Vorfalls ändern in: Geschlossen**. Wenn die Option nicht ausgewählt wird, behält das Untersuchungsstadium seinen vorherigen Wert bei.
8. Klicken Sie auf **Beheben**. Die von Ihnen ausgewählten Maßnahmen werden Schritt für Schritt ausgeführt, wobei der Fortschritt von jedem Schritt zur Schadensbehebung im Dialog 'Gesamten Vorfall beheben' angezeigt wird.
   Nach dem Anklicken wird auf der Schaltfläche **Zu 'Aktivitäten' gehen** angezeigt. Klicken Sie auf **Zu 'Aktivitäten' gehen**, um alle Antwortaktionen zu überprüfen, die auf den Vorfall angewendet wurden. Weitere Informationen finden Sie im Abschnitt '"Die Aktionen verstehen, die zur Abschwächung eines Vorfalls ergriffen wurden" (S. 1005)'.

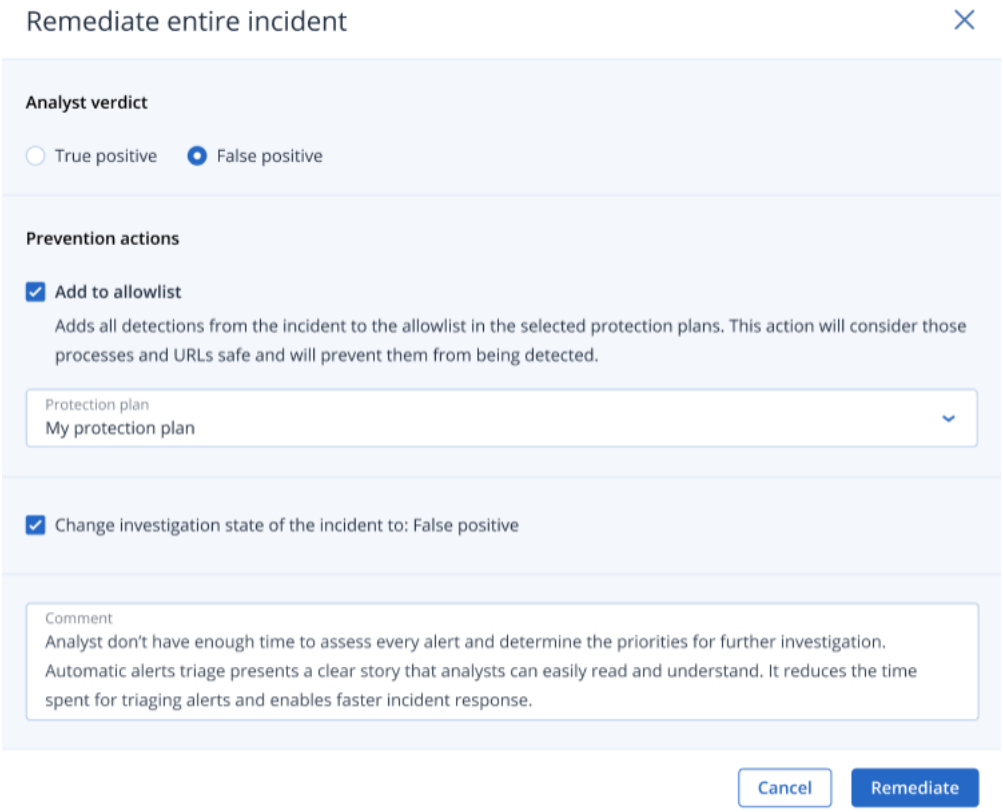
Einen falsch-positiven Vorfall beheben

Wenn Sie sicher sind, dass es sich bei einem Angriff nicht um einen echten Angriff handelt, sondern dieser falsch-positiv erkannt wurde, können Sie festlegen, wie verhindert werden soll, dass dieser Vorfall erneut erkannt wird. Dazu können Sie den Vorfall beispielsweise zur Positivliste des entsprechenden Schutzplans hinzufügen.

So können Sie einen falsch-positiven Vorfall beheben

1. Klicken Sie in der Cyber Kill Chain für den ausgewählten Vorfall auf den Befehl **Gesamten Vorfall beheben**. Das Dialogfenster 'Gesamten Vorfall beheben' wird angezeigt.

2. Wählen Sie im Bereich **Analystenbewertung** die Option **Falsch positiv**.



3. Aktivieren Sie im Bereich **Präventionsmaßnahmen** das Kontrollkästchen **Zur Positivliste hinzufügen**. Wählen Sie aus der Liste der angezeigten Schutzpläne die passenden Schutzpläne aus.
   Diese Präventionsmaßnahme stellt sicher, dass alle Erkennungen des Vorfalls für die ausgewählten Schutzpläne verhindert werden.
4. Aktivieren Sie das Kontrollkästchen **Untersuchungsstadium des Vorfalls ändern in: Falsch positiv**.
5. Klicken Sie auf **Beheben**.
   Nach dem Anklicken wird auf der Schaltfläche **Zu 'Aktivitäten' gehen** angezeigt. Klicken Sie auf **Zu 'Aktivitäten' gehen**, um die Antwortaktionen zu überprüfen, die auf den Vorfall angewendet wurden. Weitere Informationen finden Sie im Abschnitt '"Die Aktionen verstehen, die zur Abschwächung eines Vorfalls ergriffen wurden" (S. 1005)'.

Antwortaktionen für einzelne Cyber Kill Chain-Knoten

Wenn Sie den Vorfall noch genauer verwalten müssen, können Sie verschiedene Antwortaktionen auf einzelne Cyber Kill Chain-Knoten anwenden. Diese Antwortaktionen ermöglichen es Ihnen, jeden Knoten schnell und einfach zu reparieren.

Hinweis
Wie Sie globale Antwortaktionen auf einen gesamten Vorfall anwenden können, erfahren Sie in Abschnitt '"Einen gesamten Vorfall beheben" (S. 1013)'.

Die Antwortaktionen werden in die nachfolgenden Kategorien unterteilt, wobei nicht alle Knoten alle der folgenden Kategorien enthalten:

- **Beheben**: Mit den Aktionen in dieser Kategorie können Sie umgehend auf einen Angriff reagieren. Dazu gehören Maßnahmen wie die Netzwerk-Isolation für einen Workload zu verwalten oder Dateien, Prozesse und Registry-Werte zu löschen und unter Quarantäne zu stellen.
- **Untersuchen**: Mit den Aktionen in dieser Kategorie (nur auf Workloads anwendbar) können Sie ein Forensik-Backup oder eine Remote-Desktop-Verbindung erstellen, um tiefergehende Untersuchungen durchzuführen.
- **Untersuchen**: Mit den Aktionen in dieser Kategorie (nur auf Workloads anwendbar) können Sie eine Remote-Desktop-Verbindung erstellen, um tiefergehende Untersuchungen durchzuführen.
- **Recovery**: Mit den Aktionen in dieser Kategorie (nur auf Workloads anwendbar) können Sie auf intensive Angriffe reagieren, indem Sie eine Wiederherstellungen aus einem Backup oder einen Disaster Recovery-Failover-Prozess durchführen.
- **Verhindern**: Mit den Aktionen in dieser Kategorie können Sie zukünftige Bedrohungen oder Falsch-Positiv-Erkennungen verhindern, indem Sie letzere zur Positiv- oder Blockliste eines Schutzplans hinzufügen.

Hinweis
Wenn ein Vorfall geschlossen wird, können Sie auf einen Knoten keine Antwortaktionen mehr anwenden. Sie können einen geschlossenen Vorfall jedoch wieder öffnen, indem Sie dessen Untersuchungsstadium ändern – und zwar zu **Wird untersucht**. Wenn er neu geöffnet wird, können Sie Antwortaktionen anwenden.

In der nachfolgenden Tabelle werden die einzelnen Knotentypen in der Cyber Kill Chain, die anwendbaren Kategorien für jeden Knoten sowie die verfügbaren Antwortaktionen beschrieben.

Knoten	Kategorie	Antwortaktionen
Workload	Beheben	• Netzwerk-Isolation verwalten • Workload neu starten
	Untersuchen	• Forensik-Backup • Remote-Desktop-Verbindung
	Untersuchen	• Remote-Desktop-Verbindung
	Recovery	• Wiederherstellung aus einem Backup • Disaster Recovery-Failover

Knoten	Kategorie	Antwortaktionen
	Verhindern	• Patchen
Prozess	Beheben	• Prozess stoppen • Quarantäne
	Verhindern	• Zur Positivliste hinzufügen • Zur Blockliste hinzufügen
Datei	Beheben	• Löschen • Quarantäne
	Verhindern	• Zur Positivliste hinzufügen • Zur Blockliste hinzufügen
Registry	Beheben	• Löschen
Netzwerk	Verhindern	• Zur Positivliste hinzufügen • Zur Blockliste hinzufügen

Antwortaktionen für einen betroffenen Workload definieren

Als Teil Ihrer Abwehrmaßnahmen gegen einen Angriff können Sie folgende Aktionen auf betroffene Workloads anwenden:

- **Netzwerk-Isolation verwalten**: Ermöglicht Ihnen, die Netzwerk-Isolation eines Workloads zu verwalten, um laterale Bewegungen oder Steuerungs- und Kontroll-Aktivitäten (auch C&C-Aktivitäten genannt, für Command and Control) zu verhindern. Weitere Informationen finden Sie im Abschnitt '"Die Netzwerk-Isolation eines Workloads verwalten" (S. 1021)'.
- **Patch**: Ermöglicht Ihnen, einen Workload zu patchen, um zu verhindern, dass die entsprechende Schwachstelle bei zukünftigen potenziellen Angriffen ausgenutzt werden kann. Weitere Informationen finden Sie im Abschnitt '"Einen Workload patchen" (S. 1025)'.
- **Workload neu starten**: Ermöglicht Ihnen, einen Workload sofort oder nach einem festgelegten Zeitlimit neu zu starten. Weitere Informationen finden Sie im Abschnitt '"Einen Workload neu starten" (S. 1027)'.
- **Forensik-Backup**: Ermöglicht es Ihnen, bei Bedarf ein Forensik-Backup für Audits oder weitere Untersuchungen zu erstellen. Weitere Informationen finden Sie im Abschnitt '"Ein On-Demand-Forensik-Backup auf einem Workload ausführen" (S. 1028)'.

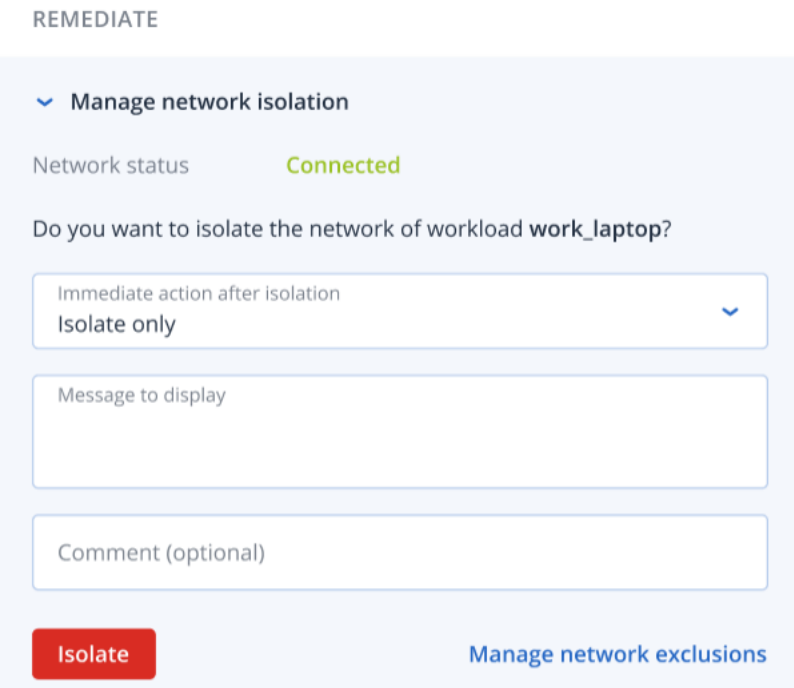
- **Remote-Desktop-Verbindung**: Ermöglicht Ihnen, über eine Remote-Verbindung auf den untersuchten Workload zuzugreifen. Weitere Informationen finden Sie im Abschnitt '"Remote-Verbindung zu einem Workload" (S. 1029)'.
- **Wiederherstellung aus einem Backup**: Ermöglicht Ihnen, einzelne Dateien und Ordner oder Ihre komplette Maschine aus einem Backup wiederherzustellen. Weitere Informationen finden Sie im Abschnitt '"Wiederherstellung aus einem Backup" (S. 1030)'.
- **Disaster Recovery-Failover**: Ermöglicht Ihnen, "Disaster Recovery implementieren" (S. 804) auszuführen. Beachten Sie, dass Ihr Workload dafür ein Abonnement für die Advanced Disaster Recovery-Funktionalität haben muss. Weitere Informationen finden Sie im Abschnitt '"Disaster Recovery-Failover" (S. 1031)'.

Die Netzwerk-Isolation eines Workloads verwalten

Die EDR-Funktionalität ermöglicht Ihnen, die Netzwerk-Isolation eines Workloads zu verwalten, um laterale Bewegungen oder Steuerungs- und Kontroll-Aktivitäten (auch C&C-Aktivitäten genannt, für Command and Control) zu verhindern. Beim Isolieren von Workloads stehen Ihnen je nach Bedarf mehrere Optionen zur Verfügung. Beim Isolieren von Workloads sollten Sie beachten, dass alle Acronis Cyber Protect-Technologien weiterhin funktionieren. Dadurch wird sichergestellt, dass Untersuchungen uneingeschränkt möglich sind.

So können Sie einen Workload vom Netzwerk isolieren

1. Klicken Sie in der Cyber Kill Chain auf den Workload-Knoten, dessen Schäden Sie beheben wollen.
2. Klicken Sie in der angezeigten Seitenleiste auf die Registerkarte **Antwortaktionen**.
3. Klicken Sie im Bereich **Beheben** auf den Befehl **Netzwerk-Isolation verwalten**.



Hinweis
Der Wert **Netzwerkstatus** zeigt an, ob ein Workload gerade verbunden ist oder nicht. Wenn der Wert **Isoliert** lautet, können Sie den isolierten Workload wieder mit dem Netzwerk verbinden (mit der nachfolgend beschriebenen Prozedur). Wenn ein Workload offline ist, können Sie ihn trotzdem isolieren. Er wird automatisch in das Stadium **Isoliert** versetzt, wenn der Workload wieder online geht.

4. Wählen Sie im Listenfeld **Sofortige Aktion nach der Isolation** eine der folgenden Optionen aus:
   - **Nur isolieren**
   - **Workload isolieren und sichern**
   - **Workload isolieren und mit forensischen Daten sichern**
   - **Workload isolieren und ausschalten**

   Weitere Informationen darüber, wo Sie das Workload-Backup speichern können und welche Verschlüsselungsoptionen es gibt, finden Sie im Abschnitt '"Die Backups und Wiederherstellungen von Workloads und Dateien verwalten" (S. 435)'.
5. [Optional] Geben Sie im Feld **Anzuzeigende Nachricht** eine Mitteilung ein, die die Endbenutzer erhalten, wenn sie auf den isolierten Workload zugreifen. Sie können die Benutzer beispielsweise darüber informieren, dass der Workload derzeit isoliert ist und dass ein- sowie ausgehende Netzwerkzugriffe für diesen Workload derzeit unterbunden sind. Beachten Sie, dass diese Meldung auch vom Tray Monitor in der Taskleiste angezeigt wird und so lange verfügbar bleibt, bis der Benutzer die Mitteilung löscht.
6. [Optional] Geben Sie im Feld **Kommentar** eine Anmerkung ein. Dieser Kommentar wird auf der Registerkarte **Aktivitäten** angezeigt (für einen einzelnen Knoten oder den gesamten Vorfall) und soll Ihnen (oder Ihren Kollegen) helfen, sich daran zu erinnern, warum Sie die Aktion durchgeführt haben, wenn Sie den Vorfall noch einmal betrachten.
7. Klicken Sie auf **Netzwerkausschlüsse verwalten**, wenn Sie Ports, URLs, Host-Namen und IP-Adressen hinzufügen wollen, die während der Isolationsphase Zugriff auf den Workload haben sollen. Weitere Informationen finden Sie unter 'So können Sie Netzwerkausschlüsse verwalten'.
8. Klicken Sie auf das **Isolieren**.
   Der Workload wird isoliert. Diese Aktion kann zudem auf den Registerkarten **Aktivitäten** des einzelnen Knotens und des gesamten Vorfalls eingesehen werden. Weitere Informationen finden Sie im Abschnitt '"Die Aktionen verstehen, die zur Abschwächung eines Vorfalls ergriffen wurden" (S. 1005)'.

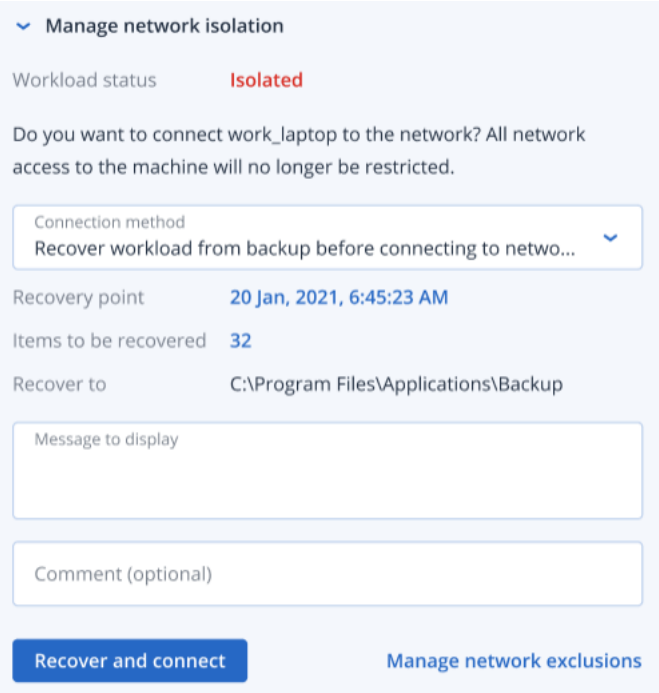
Hinweis
Der Workload wird außerdem auch in der Cyber Protect-Konsole im Menü **Workloads** als **Isoliert** angezeigt. Sie können Workloads (einzeln oder mehrere) auch über das Menü **Workloads –> Workloads mit Agenten** isolieren. Wählen Sie dazu erst den bzw. die entsprechenden Workload(s) aus und klicken Sie dann in der rechten Seitenleiste auf **Netzwerk-Isolation verwalten**. Im angezeigten Dialogfeld können Sie Netzwerkausschlüsse verwalten und die Befehle **Isolieren** bzw. **Alle isolieren** verwenden, um den oder die ausgewählten Workloads zu isolieren.

So können Sie einen isolierten Workload wieder mit dem Netzwerk verbinden

1. Klicken Sie in der Cyber Kill Chain auf den Workload-Knoten, den Sie wieder mit dem Netzwerk verbinden wollen.

   Hinweis
   Wenn der isolierte Workload gerade offline ist, können Sie ihn dennoch wieder mit dem Netzwerk verbinden. Denn er wird automatisch wieder in das Stadium **Verbunden** versetzt, wenn der Workload wieder online geht.

2. Klicken Sie in der angezeigten Seitenleiste auf die Registerkarte **Antwortaktionen**.
3. Klicken Sie im Bereich **Beheben** auf den Befehl **Netzwerk-Isolation verwalten**.
4. Wählen Sie eine der folgenden Möglichkeiten:
   - **Sofort mit Netzwerk verbinden**: Der Workload wird wieder mit dem Netzwerk verbunden.
   - **Workload aus Backup wiederherstellen, bevor er mit dem Netzwerk verbunden wird**: Wählen Sie einen Recovery-Punkt, aus dem der Workload wiederhergestellt werden soll.
     a. Klicken Sie im Feld **Recovery-Punkt** auf den Befehl **Auswahl**.
     b. Wählen Sie in der angezeigten Seitenleiste den entsprechenden Recovery-Punkt.
     c. Klicken Sie auf **Recovery –> Kompletter Workload**, wenn Sie alle Dateien und Ordner auf dem Workload wiederherstellen wollen.
     Oder
     Klicken Sie auf **Recovery –> Dateien/Ordner**, wenn Sie bestimmte Dateien und Ordner auf dem Workload wiederherstellen wollen. Sie werden dann aufgefordert, die entsprechenden Dateien bzw. Ordner auszuwählen. Sie können die Liste der ausgewählten Elemente noch einmal einsehen, indem Sie auf den entsprechenden Wert im Feld **Wiederherzustellende Elemente** klicken.



Hinweis
Wenn ein von Ihnen ausgewählter Recovery-Punkt verschlüsselt ist, werden Sie aufgefordert, das entsprechende Kennwort einzugeben.

5. [Optional] Aktivieren Sie das Kontrollkästchen **Workload bei Bedarf automatisch neu starten**. Diese Option ist nur dann relevant, wenn Sie im Schritt 4 den Befehl **Recovery –> Kompletter Workload** ausgewählt haben.
6. [Optional] Geben Sie im Feld **Anzuzeigende Nachricht** eine Mitteilung ein, die die Endbenutzer erhalten, wenn sie auf den verbundenen Workload zugreifen. So können Sie die Benutzer beispielsweise darüber informieren, dass auf dem Workload ein Backup wiederhergestellt wurde und dass die ein- und ausgehenden Netzwerkzugriffe für den Workload wieder möglich sind.
7. [Optional] Geben Sie im Feld **Kommentar** eine Anmerkung ein. Dieser Kommentar wird auf der Registerkarte **Aktivitäten** angezeigt (für einen einzelnen Knoten oder den gesamten Vorfall) und soll Ihnen (oder Ihren Kollegen) helfen, sich daran zu erinnern, warum Sie die Aktion durchgeführt haben, wenn Sie den Vorfall noch einmal betrachten.
8. Klicken Sie auf **Verbinden**, wenn Sie im Schritt 4 die Option **Sofort mit Netzwerk verbinden** ausgewählt haben.
   Oder
   Klicken Sie auf **Wiederherstellen und verbinden**, wenn Sie im Schritt 4 die Option **Workload aus Backup wiederherstellen, bevor er mit dem Netzwerk verbunden wird** ausgewählt haben.
   Der Workload wird wieder mit dem Netzwerk verbunden und alle Einschränkungen des Netzwerkzugriffs auf den Workload sind wieder aufgehoben.

Hinweis
Sie können isolierte Workloads (einzeln oder mehrere) in der Cyber Protect-Konsole auch über das Menü **Workloads –> Workloads mit Agenten** mit dem Netzwerk verbinden. Wählen Sie dazu erst den bzw. die entsprechenden Workload(s) aus und klicken Sie dann in der rechten Seitenleiste auf **Netzwerk-Isolation verwalten**. Klicken Sie dann im angezeigten Dialogfeld entweder auf **Verbinden** oder **Alle verbinden**, damit der bzw. die ausgewählten Workloads wieder mit dem Netzwerk verbunden werden.

So können Sie Netzwerkausschlüsse verwalten

Hinweis
Selbst wenn alle Acronis Cyber Protect-Technologien während der Workload-Isolationsphase funktionieren, kann es Szenarien geben, in denen Sie zusätzliche Netzwerkverbindungen benötigen (z.B. wenn Sie eine Datei von dem Workload zu einem freigegebenen Verzeichnis hochladen müssen). Für diese Szenarien können Sie einen Netzwerkausschluss hinzufügen. Sie sollten jedoch sicherstellen, dass alle Bedrohungen entfernt wurden, bevor Sie den Ausschluss hinzufügen.

1. Klicken Sie im Bereich **Beheben** der Registerkarte **Antwortaktionen** auf den Befehl **Netzwerkausschlüsse verwalten**.
2. Geben Sie in der Seitenleiste für die Netzwerkausschlüsse die entsprechenden Ausnahmen ein. Gehen Sie für jede der verfügbaren Optionen (Ports, URL-Adresse sowie Host-Name bzw. IP-Adresse) folgendermaßen vor:
   a. Klicken Sie auf **Hinzufügen** und geben Sie dann den/die entsprechenden Port(s), URL-Adressen, Host-Namen oder IP-Adressen ein.
   b. Wählen Sie im Listenfeld **Datenverkehrsrichtung** eine der folgenden Optionen: **Eingehende und ausgehende Verbindungen**, **Nur eingehende Verbindungen** oder **Nur ausgehende Verbindungen**.
   c. Klicken Sie auf **Hinzufügen**.
3. Klicken Sie auf **Speichern**.

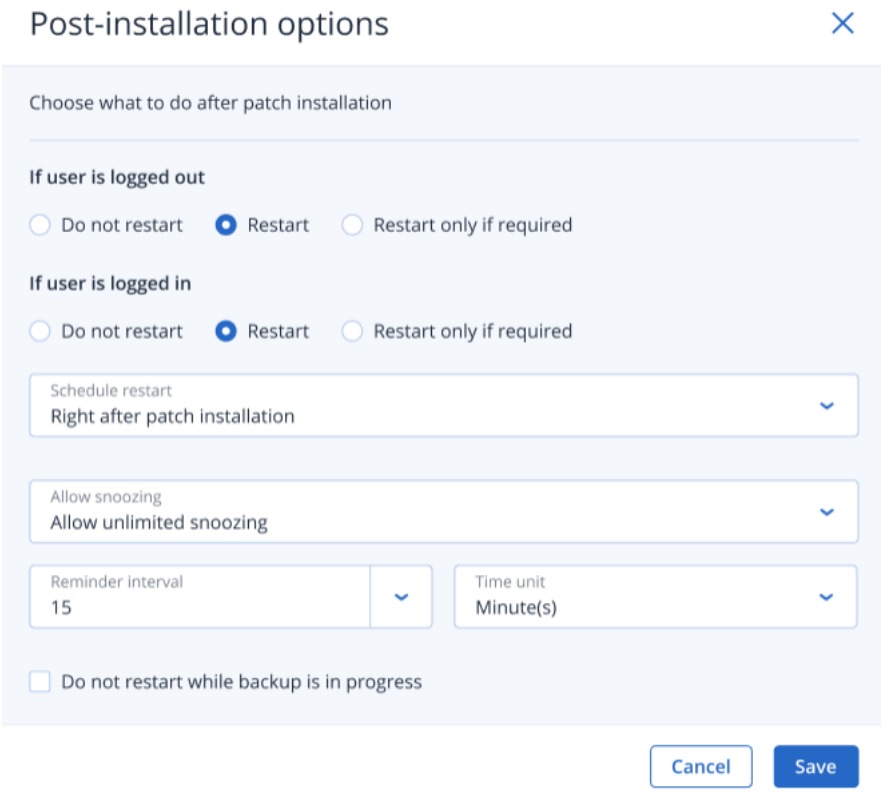
Einen Workload patchen

Die EDR-Funktionalität kann automatisch erkennen, ob ein Workload einen bestimmten Patch benötigt, und diesen dann auf dem Workload aufspielen. Dadurch können Sie verhindern, dass die jeweilige Schwachstelle bei zukünftigen potenziellen Angriffen weiter ausgenutzt wird. Beachten Sie, dass diese Funktion nur verfügbar ist, wenn der Workload des entsprechenden Partners ein Abonnement für das Advanced Management-Paket hat.

So können Sie einen Workload patchen

1. Klicken Sie in der Cyber Kill Chain auf den Workload-Knoten, den Sie mit einem Patch aktualisieren wollen.
2. Klicken Sie in der angezeigten Seitenleiste auf die Registerkarte **Antwortaktionen**.
3. Klicken Sie im Bereich **Beheben** auf den Befehl **Patchen**.

4. Klicken Sie im Feld **Zu installierende Patches** auf den Befehl **Auswahl**. Wählen Sie im angezeigten Dialogfeld die gewünschten Patches aus und klicken Sie anschließend auf **Auswahl**.
5. Klicken Sie im Feld **Nach-Installation-Optionen** auf den angezeigten Link. Das Dialogfenster mit den Optionen für Abläufe nach der Installation wird angezeigt.



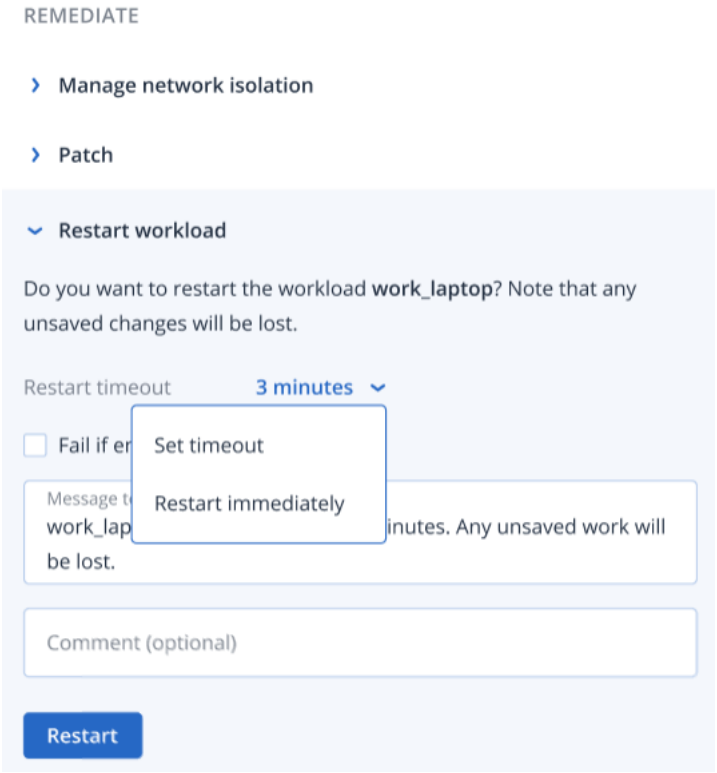
6. Wählen Sie die Aktion aus, die ausgeführt werden soll, nachdem der Patch installiert wurde:
   - **Wenn der Benutzer abgemeldet ist**: Wählen Sie entweder die Option **Nicht neu starten**, **Neustart** oder **Neustart nur bei Bedarf**.
   - **Wenn der Benutzer angemeldet ist**: Wählen Sie entweder die Option **Nicht neu starten**, **Neustart** oder **Neustart nur bei Bedarf**.
     Wenn Sie die Option **Neustart** wählen, können Sie zudem Folgendes festlegen:
     - Eine Planung für den Neustart festlegen.
     - Erneutes Erinnern erlauben, einschließlich festgelegter Erinnerungsintervalle.
7. [Optional] Aktivieren Sie das Kontrollkästchen **Kein Neustart, während ein Backup läuft**, um sicherzustellen, dass der Workload nicht neu gestartet wird, wenn gerade ein Backup erstellt wird.
8. Klicken Sie auf **Speichern**.
9. Klicken Sie in der Registerkarte **Antwortaktionen** auf **Patchen**.
   Der ausgewählte Patch wird angewendet. Diese Aktion kann zudem auf den Registerkarten **Aktivitäten** des einzelnen Knotens und des gesamten Vorfalls eingesehen werden. Weitere Informationen finden Sie im Abschnitt '"Die Aktionen verstehen, die zur Abschwächung eines Vorfalls ergriffen wurden" (S. 1005)'.

Einen Workload neu starten

Als Teil Ihrer Schadensbehebungsmaßnahmen auf einen Angriff können Sie mit der EDR-Funktionalität einen Workload umgehend neu starten oder nach einem vordefinierten Zeitlimit neu starten lassen.

So können Sie einen Workload neu starten

1. Klicken Sie in der Cyber Kill Chain auf den Workload-Knoten, für den Sie eine Neustart-Planung festlegen wollen.
2. Klicken Sie in der angezeigten Seitenleiste auf die Registerkarte **Antwortaktionen**.
3. Klicken Sie im Bereich **Beheben** auf den Befehl **Workload neu starten**.



4. Klicken Sie im Feld **Neustart-Zeitlimit** auf den angezeigten Link und wählen Sie anschließend eine der folgenden Optionen:
   - **Timeout festlegen**: Legen Sie im Dialog 'Neustart-Zeitlimit' einen den Zeitraum fest, nach dem der Workload neu gestartet werden soll, und klicken Sie anschließend auf **Speichern**.
   - **Sofort neu starten**: Wählen Sie diese Option, wenn der Workload umgehend neu gestartet werden soll.
5. [Optional] Aktivieren Sie das Kontrollkästchen **Schlägt fehl, wenn der Endbenutzer eingeloggt ist**, wenn Sie sicherstellen wollen, dass der Workload nicht neu gestartet wird, solange der Benutzer angemeldet ist.
6. Geben Sie im Feld **Anzuzeigende Nachricht** eine Mitteilung ein, die die Benutzer erhalten, wenn sie auf den isolierten Workload zugreifen.

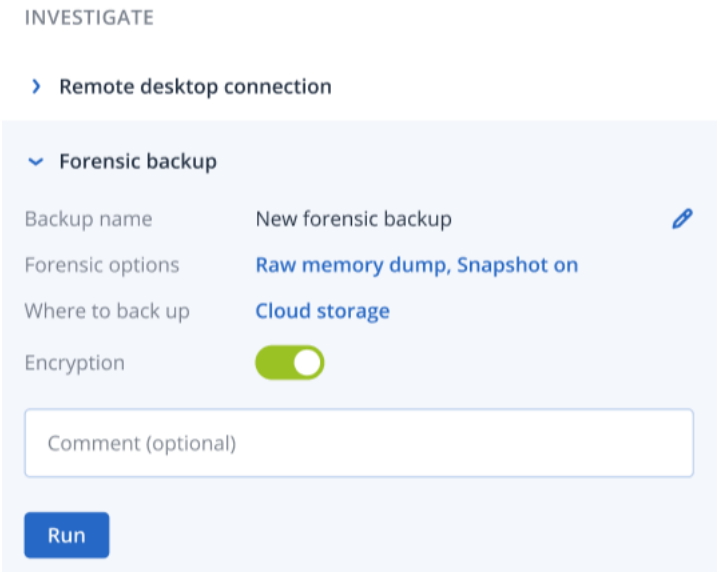
7. [Optional] Geben Sie im Feld **Kommentar** eine Anmerkung ein. Dieser Kommentar wird auf der Registerkarte **Aktivitäten** angezeigt (für einen einzelnen Knoten oder den gesamten Vorfall) und soll Ihnen (oder Ihren Kollegen) helfen, sich daran zu erinnern, warum Sie die Aktion durchgeführt haben, wenn Sie den Vorfall noch einmal betrachten.
8. Klicken Sie auf **Neustart**.
   Der Workload wird so konfiguriert, dass er gemäß der festgelegten Planung neu gestartet wird. Diese Aktion kann zudem auf den Registerkarten **Aktivitäten** des einzelnen Knotens und des gesamten Vorfalls eingesehen werden. Weitere Informationen finden Sie im Abschnitt '"Die Aktionen verstehen, die zur Abschwächung eines Vorfalls ergriffen wurden" (S. 1005)'.

Ein On-Demand-Forensik-Backup auf einem Workload ausführen

Um einen Angriff genauer untersuchen zu können, ermöglicht Ihnen die EDR Funktionalität, bei Bedarf („On-Demand“) ein Forensik-Backup für Audit- oder weitere Untersuchungszwecke durchzuführen. Beachten Sie, dass diese Funktion nur verfügbar ist, wenn der Workload des entsprechenden Partners ein Abonnement für das Advanced Backup-Paket hat.

So können Sie ein Forensik-Backup ausführen

1. Klicken Sie in der Cyber Kill Chain auf den Workload-Knoten, auf dem Sie ein Forensik-Backup erstellen wollen.
2. Klicken Sie in der angezeigten Seitenleiste auf die Registerkarte **Antwortaktionen**.
3. Klicken Sie im Bereich **Untersuchen** auf **Forensik-Backup**.



4. [Optional] Klicken Sie im Feld **Backup-Name** auf das Bearbeiten-Symbol, wenn Sie den Backup-Namen ändern wollen.
5. Klicken Sie im Feld **Forensische Optionen** auf den angezeigten Link. Wählen Sie im angezeigten Dialog für die forensischen Optionen eine der folgenden Möglichkeiten aus:
   - **Rohdaten-Speicherabbild sammeln**
   - **Kernel-Speicherabbild sammeln**

Sie können auch das Kontrollkästchen **Snapshot der laufenden Prozesse** aktivieren, wenn Sie zusätzlich Informationen in das Backup aufnehmen wollen, die die Prozesse betreffen, die beim Start des Backups ausgeführt werden. Diese Informationen werden in einem Backup-Image gespeichert.

Klicken Sie auf **Speichern**, um das Dialogfenster 'Forensik-Backup' zu schließen.

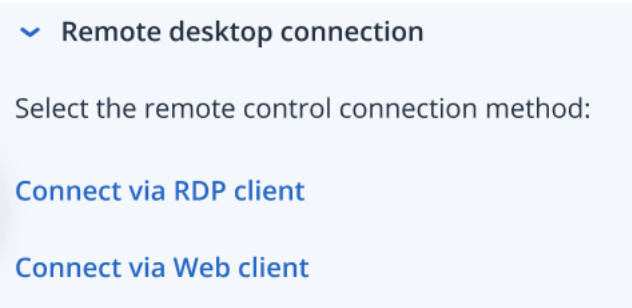
6. Klicken Sie im Feld **Backup-Ziel** auf den angezeigten Link, um festzulegen, wo das Backup gespeichert werden soll.
7. [Optional] Klicken Sie auf die Option **Verschlüsselung**, um zu aktivieren, dass das Backup chiffriert werden soll. Geben Sie im angezeigten Dialogfenster das Kennwort für das zu verschlüsselnde Backup ein und bestimmen Sie den entsprechenden Verschlüsselungsalgorithmus.
8. [Optional] Geben Sie im Feld **Kommentar** eine Anmerkung ein. Dieser Kommentar wird auf der Registerkarte **Aktivitäten** angezeigt (für einen einzelnen Knoten oder den gesamten Vorfall) und soll Ihnen (oder Ihren Kollegen) helfen, sich daran zu erinnern, warum Sie die Aktion durchgeführt haben, wenn Sie den Vorfall noch einmal betrachten.
9. Klicken Sie auf **Ausführen**.
   Das Forensik-Backup wird gestartet. Diese Aktion kann zudem auf den Registerkarten **Aktivitäten** des einzelnen Knotens und des gesamten Vorfalls eingesehen werden. Weitere Informationen finden Sie im Abschnitt '"Die Aktionen verstehen, die zur Abschwächung eines Vorfalls ergriffen wurden" (S. 1005)'.

Remote-Verbindung zu einem Workload

Um einen Angriff genauer untersuchen zu können, ermöglicht Ihnen die EDR Funktionalität, per Remote-Zugriff auf den zu untersuchenden Workload zuzugreifen.

So können Sie eine Remote-Verbindung zu einem Workload herstellen

1. Klicken Sie in der Cyber Kill Chain auf den Workload-Knoten, mit dem Sie sich aus der Ferne verbinden wollen.
2. Klicken Sie in der angezeigten Seitenleiste auf die Registerkarte **Antwortaktionen**.
3. Klicken Sie im Bereich **Untersuchen** auf **Remote-Desktop-Verbindung**.



4. Wählen Sie eine der folgenden Remote-Verbindungsmethoden:
   - **Über RDP-Client verbinden**: Bei dieser Methode werden Sie aufgefordert, den Remotedesktopverbindungs-Client herunterzuladen und zu installieren. Sie können sich dann von der -Konsole aus remote mit einem Workload verbinden.

- **Über Webclient verbinden**: Bei dieser Methode muss kein RDP-Client auf Ihrem Workload installiert werden. Sie werden zu einem Anmeldefenster weitergeleitet, wo Sie Ihre Anmeldedaten für die Remote-Maschine eingeben müssen.

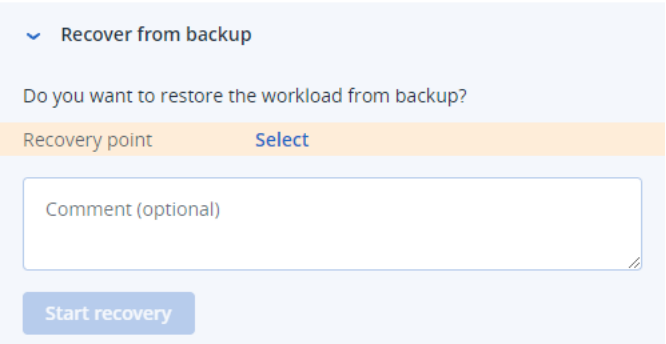
Wenn die Remote-Verbindung gestartet wurde, kann diese Aktion auf den Registerkarten **Aktivitäten** des einzelnen Knotens und des gesamten Vorfalls eingesehen werden. Weitere Informationen finden Sie im Abschnitt '"Die Aktionen verstehen, die zur Abschwächung eines Vorfalls ergriffen wurden" (S. 1005)'.

Wiederherstellung aus einem Backup

Als Teil Ihrer Wiederherstellungsmaßnahmen nach einem Angriff ermöglicht Ihnen die EDR-Funktionalität, Ihre komplette Maschine (oder auch nur bestimmte Dateien bzw. Ordner) aus einem Backup wiederherzustellen.

So können Sie Ihren Workload aus einem Backup wiederherstellen

1. Klicken Sie in der Cyber Kill Chain auf den Workload-Knoten, den Sie wiederherstellen wollen.
2. Klicken Sie in der angezeigten Seitenleiste auf die Registerkarte **Antwortaktionen**.
3. Klicken Sie im Bereich **Recovery** auf den Befehl **Aus Backup wiederherstellen**.



4. Klicken Sie im Feld **Recovery-Punkt** auf **Auswahl** und führen Sie dann folgende Schritte aus:
   a. Wählen Sie in der angezeigten Seitenleiste den entsprechenden Recovery-Punkt.
   b. Klicken Sie auf **Recovery –> Kompletter Workload**, wenn Sie alle Dateien und Ordner auf dem Workload wiederherstellen wollen.
   Oder
   Klicken Sie auf **Recovery –> Dateien/Ordner**, wenn Sie bestimmte Dateien und Ordner auf dem Workload wiederherstellen wollen. Sie werden dann aufgefordert, die entsprechenden Dateien bzw. Ordner auszuwählen. Sie können die Liste der für die Wiederherstellung ausgewählten Elemente noch einmal einsehen, indem Sie auf den entsprechenden Wert im Feld **Wiederherzustellende Elemente** klicken.

Hinweis
Wenn ein von Ihnen ausgewählter Recovery-Punkt verschlüsselt ist, werden Sie aufgefordert, das entsprechende Kennwort einzugeben.

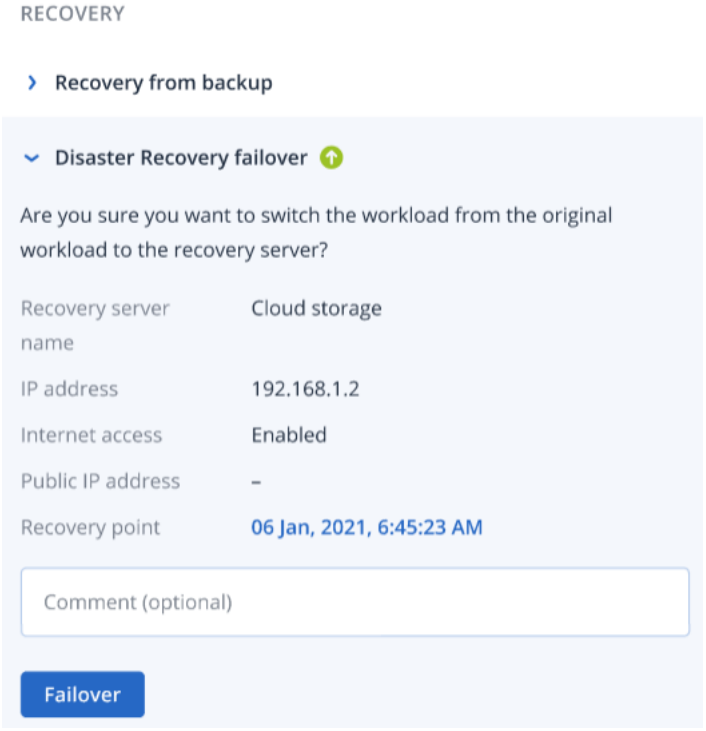
5. [Optional] Aktivieren Sie das Kontrollkästchen **Workload bei Bedarf automatisch neu starten**. Diese Option ist nur dann relevant, wenn Sie im Schritt 4 den Befehl **Recovery –> Kompletter Workload** ausgewählt haben.
6. [Optional] Geben Sie im Feld **Kommentar** eine Anmerkung ein. Dieser Kommentar wird auf der Registerkarte **Aktivitäten** angezeigt (für einen einzelnen Knoten oder den gesamten Vorfall) und soll Ihnen (oder Ihren Kollegen) helfen, sich daran zu erinnern, warum Sie die Aktion durchgeführt haben, wenn Sie den Vorfall noch einmal betrachten.
7. Klicken Sie auf **Recovery starten**.
   Der Wiederherstellungsprozess für den Workload wird gestartet. Der Fortschritt dieser Aktion kann auf den Registerkarten **Aktivitäten** des einzelnen Knotens und des gesamten Vorfalls eingesehen werden. Weitere Informationen finden Sie im Abschnitt '"Die Aktionen verstehen, die zur Abschwächung eines Vorfalls ergriffen wurden" (S. 1005)'.

Disaster Recovery-Failover

Als Teil Ihrer Wiederherstellungsmaßnahmen nach einem Angriff ermöglicht Ihnen die EDR-Funktionalität, "Disaster Recovery implementieren" (S. 804) auszuführen, wodurch Sie den Workload zu einem Recovery-Server umschalten können. Beachten Sie, dass Ihr Workload dafür ein Abonnement für die Advanced Disaster Recovery-Funktionalität haben muss.

So können Sie einen Disaster Recovery-Failover durchführen

1. Klicken Sie in der Cyber Kill Chain auf den Workload-Knoten, den Sie wiederherstellen wollen.
2. Klicken Sie in der angezeigten Seitenleiste auf die Registerkarte **Antwortaktionen**.
3. Klicken Sie im Bereich **Recovery** auf **Disaster Recovery-Failover**.



4. Führen Sie im Feld **Recovery-Punkt** folgende Schritte aus:
   a. Klicken Sie auf das aktuelle Recovery-Punkt-Datum, um einen Recovery-Punkt auszuwählen.
   b. Wählen Sie in der angezeigten Seitenleiste den entsprechenden Recovery-Punkt.

   Hinweis
   Wenn Sie ein Advanced Disaster Recovery-Abonnement haben, können Sie den entsprechenden Recovery-Server (die Offline-VM) auswählen, der unter Disaster Recovery erstellt wurde. Wenn Sie kein Abonnement haben, werden Sie aufgefordert, die Disaster Recovery-Funktionalität zu konfigurieren.

5. [Optional] Geben Sie im Feld **Kommentar** eine Anmerkung ein. Dieser Kommentar wird auf der Registerkarte **Aktivitäten** angezeigt (für einen einzelnen Knoten oder den gesamten Vorfall) und soll Ihnen (oder Ihren Kollegen) helfen, sich daran zu erinnern, warum Sie die Aktion durchgeführt haben, wenn Sie den Vorfall noch einmal betrachten.
6. Klicken Sie auf **Failover**.
   Der Workload wird auf den Recovery-Server umgeschaltet. Diese Aktion kann auf den Registerkarten **Aktivitäten** des einzelnen Knotens und des gesamten Vorfalls eingesehen werden. Weitere Informationen finden Sie im Abschnitt '"Die Aktionen verstehen, die zur Abschwächung eines Vorfalls ergriffen wurden" (S. 1005)'.

Antwortaktionen für einen verdächtigen Prozess definieren

Als Teil Ihrer Abwehrmaßnahmen gegen einen Angriff können Sie folgende Aktionen auf verdächtige Prozesse anwenden:

- Einen Prozess stoppen (siehe unten)
- Einen Prozess unter Quarantäne stellen (siehe unten)
- Änderungen zurücksetzen, die ein Prozess vorgenommen hat (siehe unten)
- Einen Prozess zur Positiv- oder Blockliste des Schutzplans hinzufügen (siehe Abschnitt '"So können einen Prozess, eine Datei oder ein Netzwerk zur Block- oder Positivliste des Schutzplans hinzufügen bzw. aus dieser wieder entfernen" (S. 1038)')

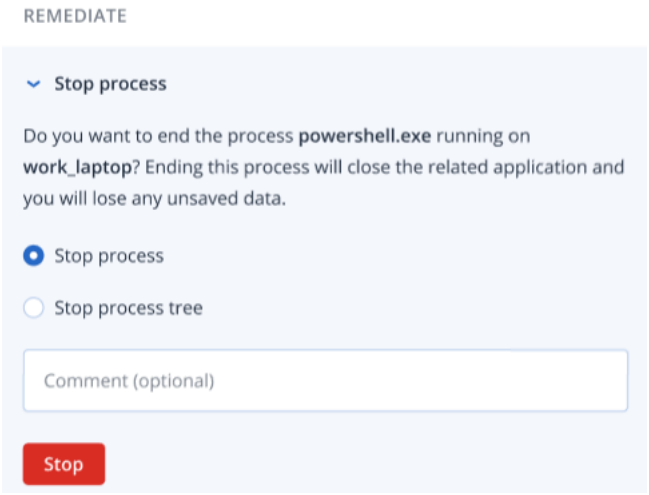
So können Sie einen verdächtigen Prozess stoppen

1. Klicken Sie in der Cyber Kill Chain auf den Prozessknoten, dessen Schäden Sie beheben wollen.

   Hinweis
   Kritische Windows-Prozesse oder nicht laufende Prozesse können nicht gestoppt werden und sind in der Cyber Kill Chain deaktiviert.

2. Klicken Sie in der angezeigten Seitenleiste auf die Registerkarte **Antwortaktionen**.

3. Klicken Sie im Bereich **Beheben** auf den Befehl **Prozess stoppen**.



4. Wählen Sie eine der folgenden Möglichkeiten:
   - **Prozess stoppen** (stoppt den spezifischen Prozess)
   - **Prozessbaum stoppen** (stoppt den spezifischen Prozess und alle dazugehörigen Unterprozesse)
5. [Optional] Geben Sie einen Kommentar ein. Dieser Kommentar wird auf der Registerkarte **Aktivitäten** angezeigt (für einen einzelnen Knoten oder den gesamten Vorfall) und soll Ihnen (oder Ihren Kollegen) helfen, sich daran zu erinnern, warum Sie die Aktion durchgeführt haben, wenn Sie den Vorfall noch einmal betrachten.
6. Klicken Sie auf **Stopp**. Der Prozess wird angehalten.

Hinweis
Die entsprechende Applikation wird geschlossen, wobei alle evtl. noch nicht gespeicherten Daten verloren gehen.

Diese Aktion kann zudem auf den Registerkarten **Aktivitäten** des einzelnen Knotens und des gesamten Vorfalls eingesehen werden. Weitere Informationen finden Sie im Abschnitt '"Die Aktionen verstehen, die zur Abschwächung eines Vorfalls ergriffen wurden" (S. 1005)'.

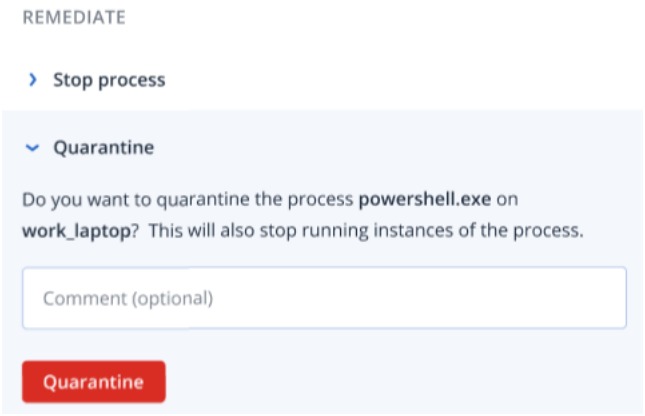
So können Sie einen verdächtigen Prozess unter Quarantäne stellen

1. Klicken Sie in der Cyber Kill Chain auf den Prozessknoten, den Sie unter Quarantäne stellen wollen.

Hinweis
Kritische Windows-Prozesse können nicht unter Quarantäne gestellt werden und sind in der Cyber Kill Chain deaktiviert.

2. Klicken Sie in der angezeigten Seitenleiste auf die Registerkarte **Antwortaktionen**.

3. Klicken Sie im Bereich **Beheben** auf den Befehl **Quarantäne**.



4. [Optional] Geben Sie einen Kommentar ein. Dieser Kommentar wird auf der Registerkarte **Aktivitäten** angezeigt (für einen einzelnen Knoten oder den gesamten Vorfall) und soll Ihnen (oder Ihren Kollegen) helfen, sich daran zu erinnern, warum Sie die Aktion durchgeführt haben, wenn Sie den Vorfall noch einmal betrachten.
5. Klicken Sie auf **Quarantäne**. Der Prozess wird angehalten und dann unter Quarantäne gestellt.

Hinweis
Der Prozess wird in den Quarantänebereich, der unter Antimalware Protection verfügbar ist, verschoben und kann dort verwaltet werden.

Diese Aktion kann zudem auf den Registerkarten **Aktivitäten** des einzelnen Knotens und des gesamten Vorfalls eingesehen werden. Weitere Informationen finden Sie im Abschnitt '"Die Aktionen verstehen, die zur Abschwächung eines Vorfalls ergriffen wurden" (S. 1005)'.

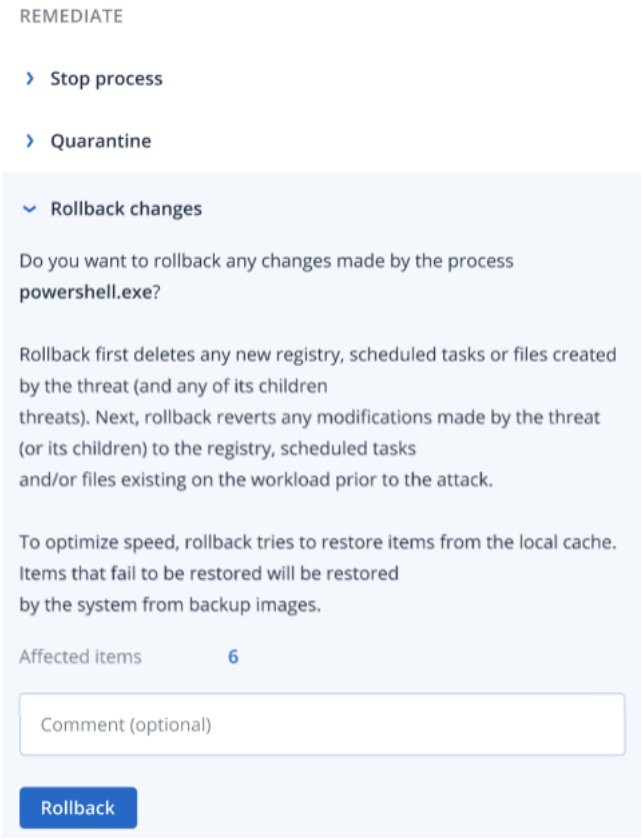
So können Sie Änderungen zurücksetzen

1. Klicken Sie in der Cyber Kill Chain auf den Prozessknoten, für den Sie die durchgeführten Änderungen zurücknehmen wollen.

Hinweis
Diese Aktion ist nur für Erkennungsknoten (die als rote oder gelbe Knoten angezeigt werden) verfügbar.

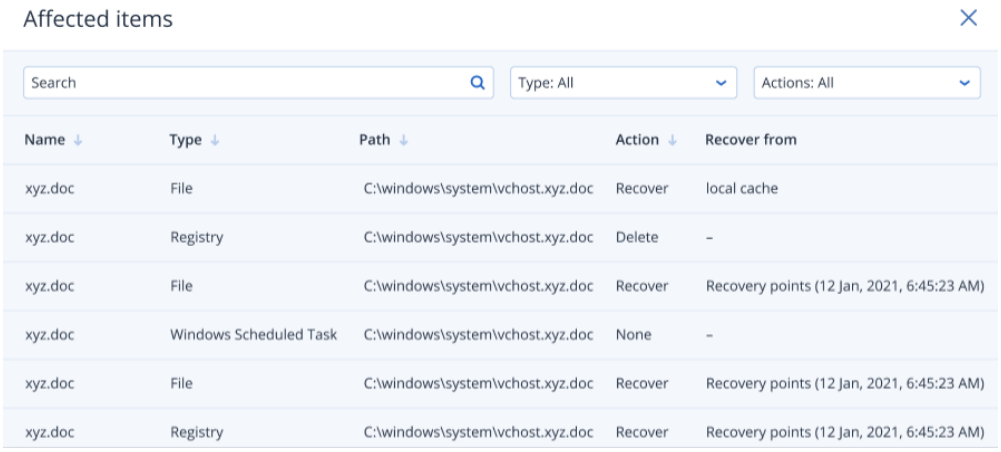
2. Klicken Sie in der angezeigten Seitenleiste auf die Registerkarte **Antwortaktionen**.

3. Klicken Sie im Bereich **Beheben** auf den Befehl **Änderungen zurücksetzen**.



Hinweis
Der Rollback-Prozess verwendet für seine Wiederherstellung nur Elemente aus dem lokalen Cache. Die Durchführung eines Rollback-Prozesses aus Backup-Archiven wird in zukünftigen Versionen verfügbar sein.

4. Wenn Sie die Elemente einsehen wollen, die vom Befehl 'Änderungen zurücksetzen' betroffen sind, klicken Sie auf den Link **Betroffene Elemente**. Im erscheinenden Dialog werden alle Elemente (Dateien, Registry-Elemente, geplante Tasks) angezeigt, die durch den Rollback-Vorgang wiederhergestellt werden und mit welcher Aktion (**Löschen**, **Wiederherstellen** oder **Keine**) dies geschieht. Außerdem können Sie einsehen, ob die wiederhergestellten Elemente aus dem lokalen Cache oder aus den Recovery-Punkten eines Backups wiederhergestellt werden.



5. [Optional] Geben Sie einen Kommentar ein. Dieser Kommentar wird auf der Registerkarte **Aktivitäten** angezeigt (für einen einzelnen Knoten oder den gesamten Vorfall) und soll Ihnen (oder Ihren Kollegen) helfen, sich daran zu erinnern, warum Sie die Aktion durchgeführt haben, wenn Sie den Vorfall noch einmal betrachten.
6. Klicken Sie auf **Rollback**. Die Rollback-Funktionalität macht mit folgenden Schritten alle Änderungen an Registry-Elementen, Dateien oder geplanten Tasks rückgängig, die der Prozess vorgenommen hat:
   a. Alle neuen Einträge (Registry-Werte, geplante Tasks, Dateien), die von der Bedrohung (und ihren Unterbedrohungen) erstellt wurden, werden gelöscht.
   b. Alle Änderungen, die die Bedrohung (und ihre Unterbedrohungen) an Registry-Einträgen, geplanten Tasks und/oder Dateien, die schon vor dem Angriff auf dem Workload vorlagen, vorgenommen hat, werden rückgängig gemacht.
   c. Der Rollback-Prozess wird versuchen, die Elemente aus dem lokalen Cache wiederherzustellen. Elemente, die nicht auf diese Weise wiederhergestellt werden können, werden von der EDR-Funktionalität automatisch aus Malware-freien Backup-Images wiederhergestellt.

   Diese Rollback-Aktion kann zudem auf den Registerkarten **Aktivitäten** des einzelnen Knotens und des gesamten Vorfalls eingesehen werden. Weitere Informationen finden Sie im Abschnitt '"Die Aktionen verstehen, die zur Abschwächung eines Vorfalls ergriffen wurden" (S. 1005)'.

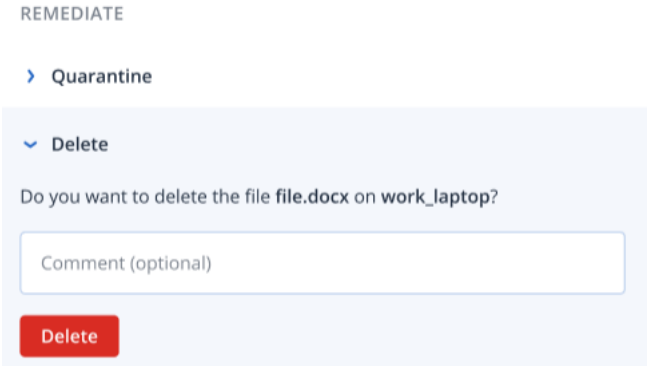
Antwortaktionen für eine verdächtige Datei definieren

Als Teil Ihrer Abwehrmaßnahmen gegen einen Angriff können Sie folgende Aktionen auf verdächtige Dateien anwenden:

- Eine Datei löschen (siehe unten)
- Eine Datei unter Quarantäne stellen (siehe unten)
- Eine Datei zur Positiv- oder Blockliste des Schutzplans hinzufügen (siehe Abschnitt '"So können einen Prozess, eine Datei oder ein Netzwerk zur Block- oder Positivliste des Schutzplans hinzufügen bzw. aus dieser wieder entfernen" (S. 1038)')

So können Sie eine verdächtige Datei löschen

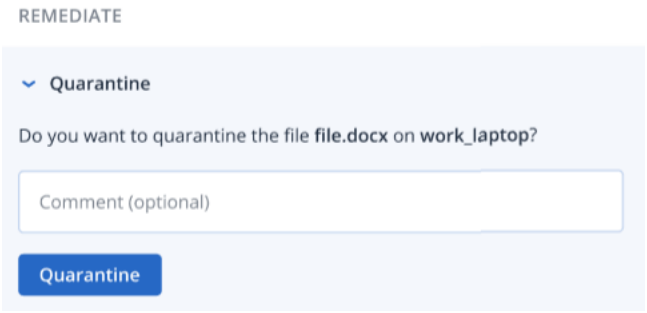
1. Klicken Sie in der Cyber Kill Chain auf den Dateiknoten, dessen Schäden Sie beheben wollen.
2. Klicken Sie in der angezeigten Seitenleiste auf die Registerkarte **Antwortaktionen**.
3. Klicken Sie im Bereich **Beheben** auf den Befehl **Löschen**.



4. [Optional] Geben Sie einen Kommentar ein. Dieser Kommentar wird auf der Registerkarte **Aktivitäten** angezeigt (für einen einzelnen Knoten oder den gesamten Vorfall) und soll Ihnen (oder Ihren Kollegen) helfen, sich daran zu erinnern, warum Sie die Aktion durchgeführt haben, wenn Sie den Vorfall noch einmal betrachten.
5. Klicken Sie auf **Löschen**.
   Die Datei wird gelöscht. Diese Aktion kann zudem auf den Registerkarten **Aktivitäten** des einzelnen Knotens und des gesamten Vorfalls eingesehen werden. Weitere Informationen finden Sie im Abschnitt '"Die Aktionen verstehen, die zur Abschwächung eines Vorfalls ergriffen wurden" (S. 1005)'.

So können Sie eine verdächtige Datei unter Quarantäne stellen

1. Klicken Sie in der Cyber Kill Chain auf den Dateiknoten, dessen Schäden Sie beheben wollen.
2. Gehen Sie in der angezeigten Seitenleiste zu **Antwortaktionen**.
3. Klicken Sie im Bereich **Beheben** auf den Befehl **Quarantäne**.



4. [Optional] Geben Sie einen Kommentar ein. Dieser Kommentar wird auf der Registerkarte **Aktivitäten** angezeigt (für einen einzelnen Knoten oder den gesamten Vorfall) und soll Ihnen (oder Ihren Kollegen) helfen, sich daran zu erinnern, warum Sie die Aktion durchgeführt haben, wenn Sie den Vorfall noch einmal betrachten.
5. Klicken Sie auf **Quarantäne**.
   Die Datei wird unter Quarantäne gestellt. Diese Aktion kann zudem auf den Registerkarten **Aktivitäten** des einzelnen Knotens und des gesamten Vorfalls eingesehen werden. Weitere

Informationen finden Sie im Abschnitt '"Die Aktionen verstehen, die zur Abschwächung eines Vorfalls ergriffen wurden" (S. 1005)'.

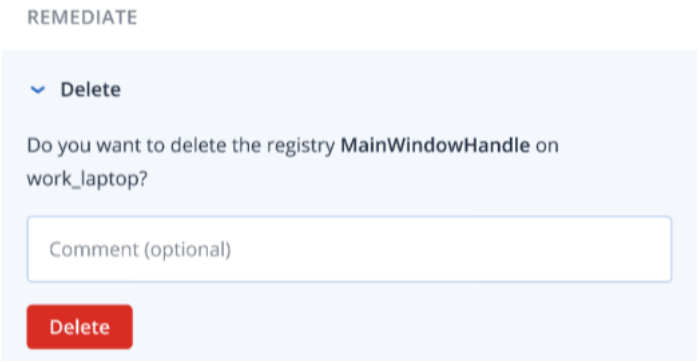
Antwortaktionen für einen verdächtigen Registry-Eintrag definieren

Als Teil Ihrer Abwehrmaßnahmen gegen einen Angriff können Sie verdächtige Registry-Einträge löschen.

Diese Option ist für Cyber Kill Chain-Registry-Knoten verfügbar.

So können Sie einen verdächtigen Registry-Eintrag löschen

1. Klicken Sie in der Cyber Kill Chain auf den Knoten, dessen Schäden Sie beheben wollen.
2. Klicken Sie in der angezeigten Seitenleiste auf die Registerkarte **Antwortaktionen**.
3. Klicken Sie im Bereich **Beheben** auf den Befehl **Löschen**.



4. [Optional] Geben Sie einen Kommentar ein. Dieser Kommentar wird auf der Registerkarte **Aktivitäten** angezeigt (für einen einzelnen Knoten oder den gesamten Vorfall) und soll Ihnen (oder Ihren Kollegen) helfen, sich daran zu erinnern, warum Sie die Aktion durchgeführt haben, wenn Sie den Vorfall noch einmal betrachten.
5. Klicken Sie auf **Löschen**.
   Der Registry-Eintrag wird gelöscht. Diese Aktion kann zudem auf den Registerkarten **Aktivitäten** des einzelnen Knotens und des gesamten Vorfalls eingesehen werden. Weitere Informationen finden Sie im Abschnitt '"Die Aktionen verstehen, die zur Abschwächung eines Vorfalls ergriffen wurden" (S. 1005)'.

So können einen Prozess, eine Datei oder ein Netzwerk zur Block- oder Positivliste des Schutzplans hinzufügen bzw. aus dieser wieder entfernen

Als Bestandteil Ihrer Präventionsmaßnahmen bei einem Angriff können Sie in Ihrem Schutzplan einen Knoten zur Positivliste oder Blockliste hinzufügen.

Sie können einen Knoten zu einer Positivliste hinzufügen, wenn Sie den Knoten für sicher halten und verhindern wollen, dass er zukünftig noch mal als falsch-positiv erkannt wird. Sie können einen Knoten zu einer Blockliste hinzufügen, wenn Sie verhindern wollen, dass der Knoten zukünftig ausgeführt werden kann.

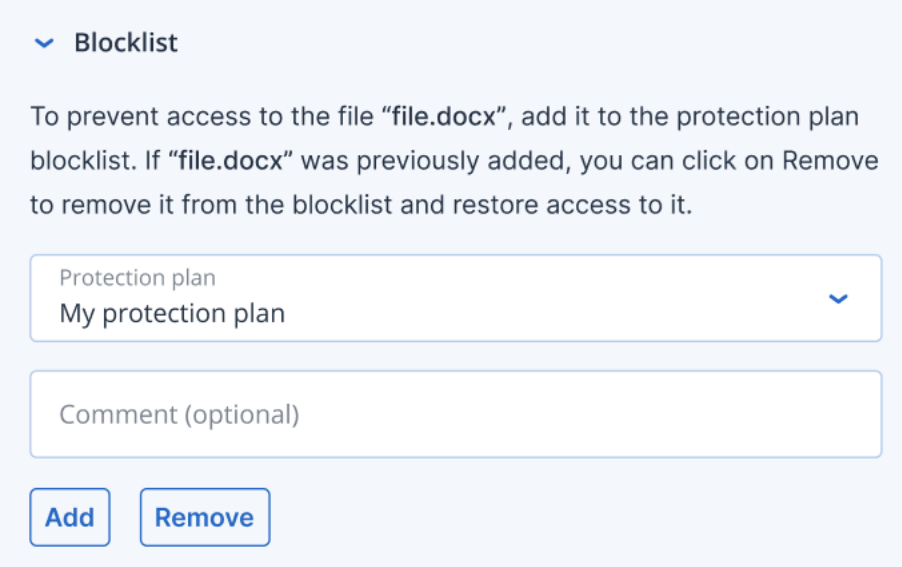
Sie können auch einen Knoten von der Positiv- oder Blockliste entfernen, um zukünftige Zugriffe auf den Knoten zu erlauben oder zu verbieten.

Diese Option ist für folgende Cyber Kill Chain-Knoten verfügbar:

- Prozess
- Datei
- Netzwerk

So können Sie einen Prozess, eine Datei oder ein Netzwerk zur Blockliste eines Schutzplans hinzuzufügen oder von dieser entfernen

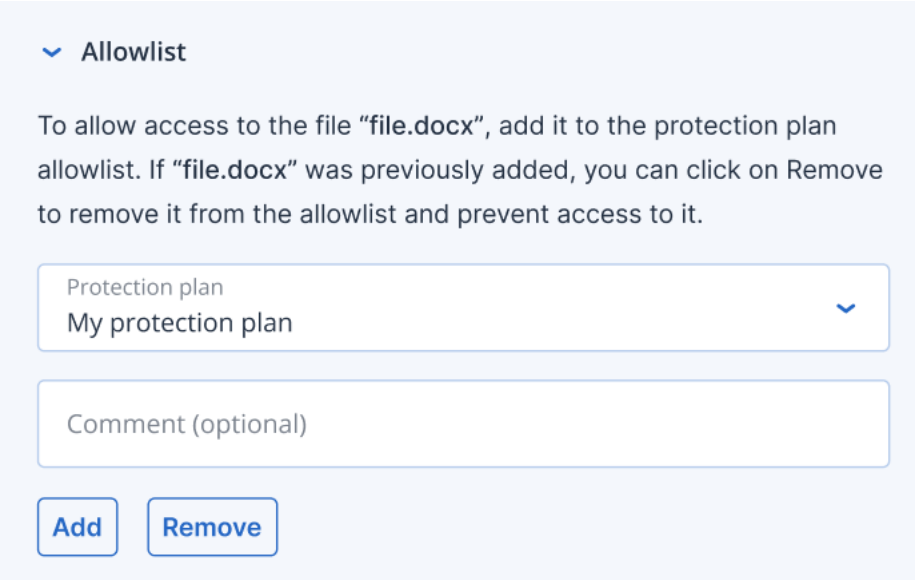
1. Klicken Sie in der Cyber-Kill-Chain Sie auf den Prozess, die Datei oder den Netzwerkknoten, auf die/den Sie eine Abwehrmaßnahme anwenden wollen.
2. Klicken Sie in der angezeigten Seitenleiste auf die Registerkarte **Antwortaktionen**.
3. Klicken Sie im Bereich **Verhindern** klicken Sie auf das Pfeilsymbol neben **Blockliste**.



4. Wählen Sie den entsprechenden Schutzplan bzw. die Schutzpläne aus, auf den/die Sie diese Aktion anwenden wollen.
5. [Optional] Geben Sie einen Kommentar ein. Dieser Kommentar wird auf der Registerkarte **Aktivitäten** angezeigt (für einen einzelnen Knoten oder den gesamten Vorfall) und soll Ihnen (oder Ihren Kollegen) helfen, sich daran zu erinnern, warum Sie die Aktion durchgeführt haben, wenn Sie den Vorfall noch einmal betrachten.
6. Klicken Sie auf **Hinzufügen**.
   Die Aktion wird umgesetzt und es wird in Zukunft verhindert, dass der Prozess, die Datei oder das Netzwerk ausgeführt wird.
   Alternativ, wenn der Prozess, die Datei oder das Netzwerk zuvor zur Blockliste hinzugefügt wurde und Sie diese nun von der Blockliste wieder entfernen möchten, klicken Sie auf **Entfernen**. Dadurch kann wieder auf die Elemente zugegriffen werden.
   Die Aktion zum Hinzufügen oder Entfernen kann auch in den Registerkarte **Aktivitäten** des einzelnen Knotens als auch des kompletten Vorfalls eingesehen werden. Für weitere Informationen siehe "Die Aktionen verstehen, die zur Abschwächung eines Vorfalls ergriffen wurden" (S. 1005).

So können Sie einen Prozess, eine Datei oder ein Netzwerk in die Positivliste eines Schutzplans aufnehmen oder von dieser wieder entfernen

1. Klicken Sie in der Cyber-Kill-Chain Sie auf den Prozess, die Datei oder den Netzwerkknoten, auf die/den Sie eine Abwehrmaßnahme anwenden wollen.
2. Klicken Sie in der angezeigten Seitenleiste auf die Registerkarte **Antwortaktionen**.
3. Klicken Sie im Bereich **Verhindern** auf das Pfeilsymbol neben **Positivliste**.



4. Wählen Sie den entsprechenden Schutzplan bzw. die Schutzpläne aus, auf den/die Sie diese Aktion anwenden wollen.
5. [Optional] Geben Sie einen Kommentar ein. Dieser Kommentar wird auf der Registerkarte **Aktivitäten** angezeigt (für einen einzelnen Knoten oder den gesamten Vorfall) und soll Ihnen (oder Ihren Kollegen) helfen, sich daran zu erinnern, warum Sie die Aktion durchgeführt haben, wenn Sie den Vorfall noch einmal betrachten.
6. Klicken Sie auf **Hinzufügen**.
   Die Aktion wird umgesetzt und der Prozess, die Datei oder das Netzwerk wird in Zukunft vor falschen Erkennungen geschützt.
   Alternativ, wenn der Prozess, die Datei oder das Netzwerk zuvor zur Positivliste hinzugefügt wurde und Sie diese(s) nun von der Positivliste wieder löschen möchten, können Sie auf **Entfernen** klicken. Dadurch kann zukünftig nicht mehr auf das Element zugegriffen werden.
   Die Aktion zum Hinzufügen oder Entfernen kann auch in den Registerkarte **Aktivitäten** des einzelnen Knotens als auch des kompletten Vorfalls eingesehen werden. Für weitere Informationen siehe "Die Aktionen verstehen, die zur Abschwächung eines Vorfalls ergriffen wurden" (S. 1005).

Den Überwachungsmodus für die EDR-Funktionalität (Endpoint Detection & Response) aktivieren

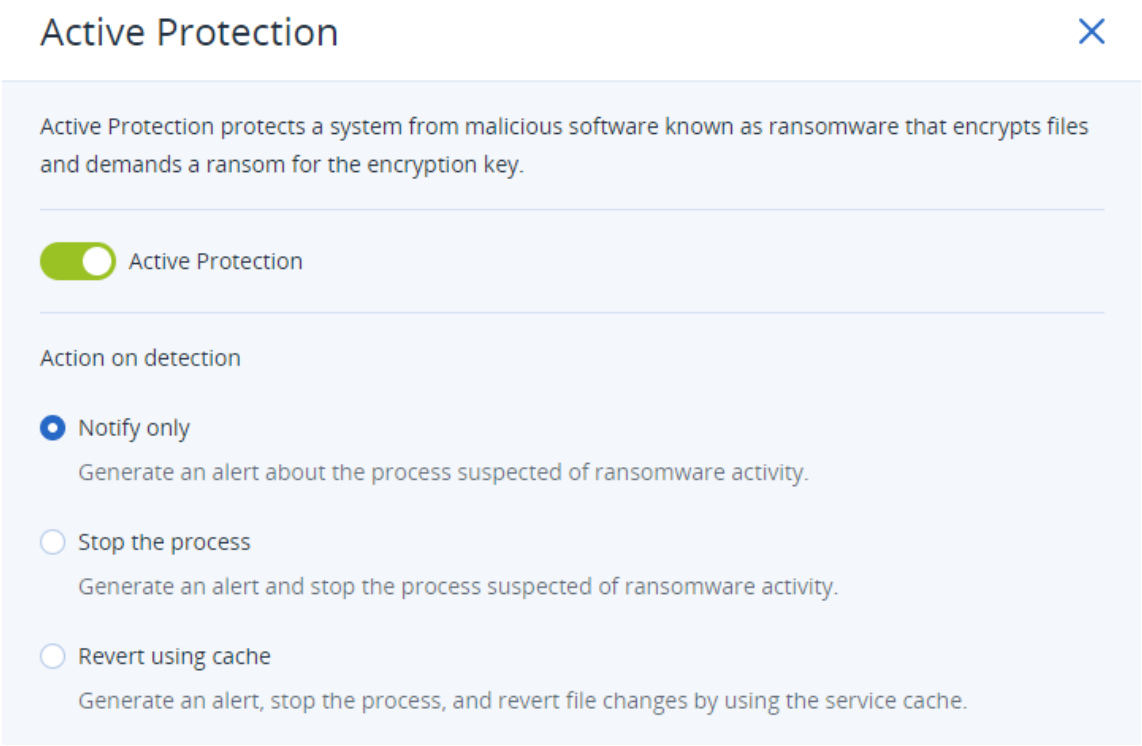
Mit dem Überwachungsmodus in Cyber Protection können Sie EDR-Funktionalität in einer Produktionsumgebung verwenden. Dies wiederum ermöglicht es Ihnen, auf Falsch-Positiv-

Erkennungen zu prüfen und notwendige Ausschlüsse vorzunehmen, bevor Sie die EDR-Funktionalität vollständig bereitstellen.

Im Überwachungsmodus wird nichts blockiert oder gestoppt. Es werden Vorfälle erstellt, aber keine Antwortreaktionen eingeleitet.

So können Sie den Überwachungsmodus für die EDR-Funktionalität aktivieren

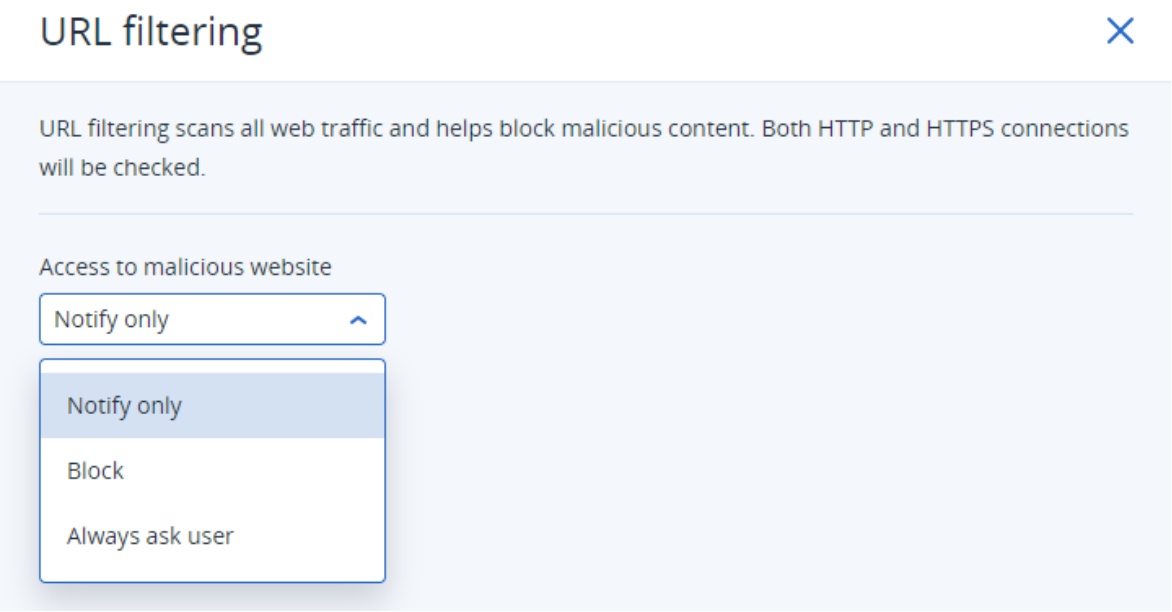
1. Stellen Sie im entsprechenden Schutzplan sicher, dass die EDR-Funktionalität aktiviert ist. Weitere Informationen finden Sie im Abschnitt '"Die Endpoint Detection & Response (EDR)-Funktionalität aktivieren" (S. 985)'.
2. Erweitern Sie das Modul **Antivirus & Antimalware Protection** und definieren Sie dann Folgendes:
   - Klicken Sie auf **Active Protection** und wählen Sie im Bereich **Aktion bei Erkennung** die Option **Nur benachrichtigen**. Klicken Sie anschließend auf **Fertig**. Weitere Informationen finden Sie im Abschnitt '"Active Protection" (S. 902)'.



   - Klicken Sie auf **Behavior Engine** und wählen Sie im Bereich **Aktion bei Erkennung** die Option **Nur benachrichtigen**. Klicken Sie anschließend auf **Fertig**. Weitere Informationen finden Sie im Abschnitt '"Behavior Engine" (S. 907)'.
   - Klicken Sie auf **Exploit-Prävention** und wählen Sie im Bereich **Aktion bei Erkennung** die Option **Nur benachrichtigen**. Klicken Sie anschließend auf **Fertig**. Weitere Informationen finden Sie im Abschnitt '"Exploit-Prävention" (S. 908)'.
   - Klicken Sie auf **Echtzeitschutz** und wählen Sie im Bereich **Aktion bei Erkennung** die Option **Nur benachrichtigen**. Klicken Sie anschließend auf **Fertig**. Weitere Informationen finden Sie im Abschnitt '"Echtzeitschutz" (S. 910)'.

- Klicken Sie auf **Scan planen** und wählen Sie im Bereich **Aktion bei Erkennung** die Option **Nur benachrichtigen**. Klicken Sie anschließend auf **Fertig**. Weitere Informationen finden Sie im Abschnitt '"Scan planen" (S. 911)'.

3. Erweitern Sie das Modul **URL-Filterung** und wählen Sie dann im Listenfeld **Zugriff auf schädliche Website** die Option **Nur benachrichtigen**. Klicken Sie anschließend auf **Fertig**. Weitere Informationen finden Sie im Abschnitt '"URL-Filterung" (S. 928)'.



So können Sie testen, ob die EDR-Funktionalität (Endpoint Detection & Response) korrekt funktioniert

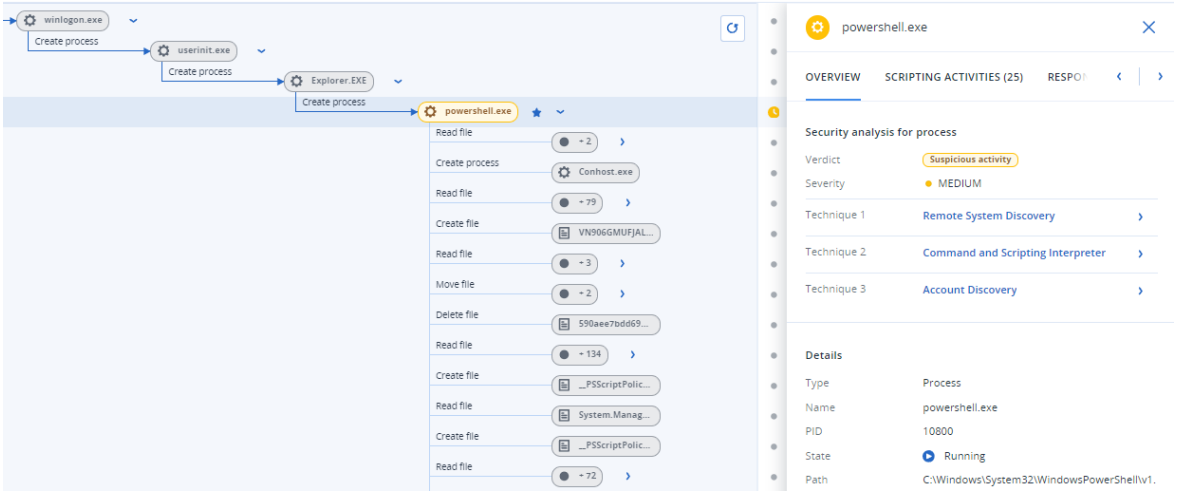
Um sicherzustellen, dass die EDR-Funktionalität korrekt bereitgestellt ist und funktioniert, können Sie verschiedene Befehle ausführen, die EDR-Erkennungen auslösen.

Hinweis
Wenn die EDR-Funktionalität bereitgestellt wurde, sollten Sie Vorfälle sofort erkennen können, wenn eine verdächtige Aktivität auftritt. Mit den folgenden Schritten können Sie überprüfen, ob die EDR-Funktionalität korrekt arbeitet, falls mehrere Tage lang keine neuen Vorfälle ausgelöst wurden.

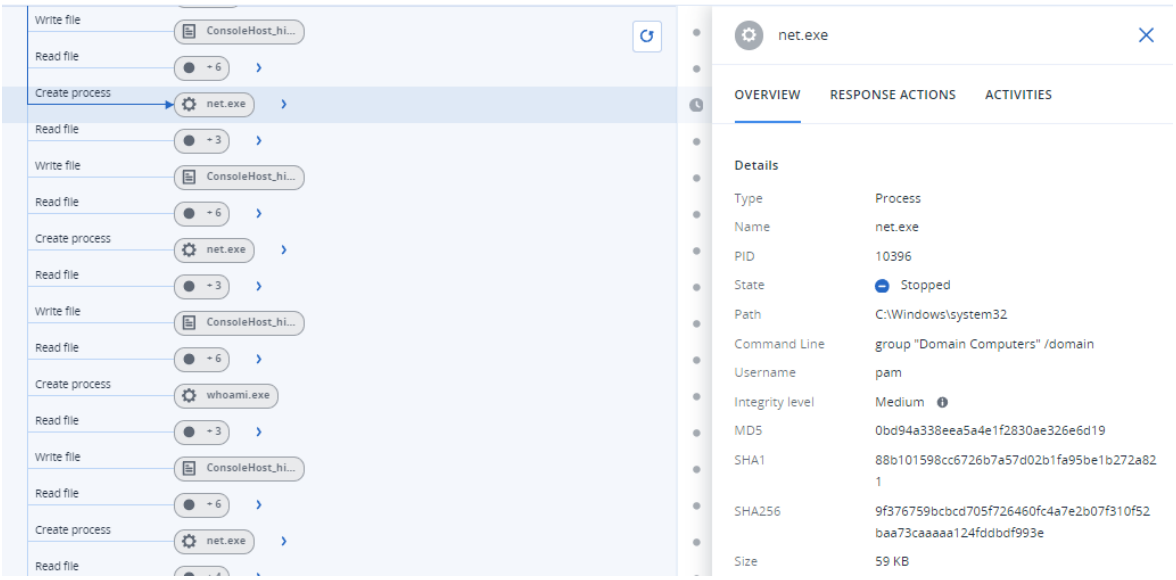
So können Sie testen, ob die EDR-Funktionalität bereitgestellt wurde und korrekt arbeitet

1. Melden Sie sich an dem entsprechenden Active Directory-Benutzerkonto an, das einer Domain beigetreten ist.
2. Führen Sie die folgenden beiden Befehle in der Windows PowerShell aus:
   - `net group "Domain Computers" /domain`
   - `net user administrator /domain`
3. Gehen Sie in der Cyber Protect-Konsole zu **Schutz –> Vorfälle**, um den generierten Vorfall einsehen zu können.

Sie können auch auf den ausgelösten Vorfall mit dem Schweregrad **Mittel** klicken, damit Sie diesen in der EDR Cyber Kill Chain angezeigt bekommen und die PowerShell-Befehle bestätigen können, die Sie im vorherigen Schritt ausgeführt haben (wie im nachfolgenden Beispiel gezeigt).



4. Führen Sie die folgenden Befehle in der Windows PowerShell aus:
   - `c:\>whoami`
   - `c:\>net localgroup`
   - `c:\>net localgroup administrators`
   - `c:\>powershell -command start-process cmd -verb runas`
   - `c:\WINDOWS\system32>net user administrator /active:yes`
   - `c:\>powershell -command Get-Hotfix`
5. Klicken Sie in der EDR Cyber Kill Chain auf die ausführbaren Knoten (z.B. **net.exe** oder **whoami.exe**), um die genauen PowerShell-Befehle einzusehen, die in der Befehlszeile ausgeführt wurden. Diese Befehle werden im nachfolgenden Beispiel im Bereich **Details** auf der Registerkarte **Überblick** angezeigt.



6. Wenn Sie bestätigt haben, dass ein EDR-Vorfall generiert wurde, sollten Sie den **Bedrohungsstatus** für den Vorfall manuell auf **Abgeschwächt** und das **Untersuchungsstadium** auf **Geschlossen** setzen. Weitere Informationen finden Sie im Abschnitt '"So können Sie Vorfälle in der Cyber Kill Chain untersuchen" (S. 996)'. Sie können den Vorfall auch mit einem Kommentar versehen, um zu vermerken, dass es sich um einen Testvorfall handelt.

Schwachstellen bewerten und Patches verwalten

Die **Schwachstellenbewertung** (SB, Englisch auch Vulnerability Assessment oder kurz VA) ist ein Prozess zum Identifizieren, Quantifizieren und Priorisieren von Schwachstellen, die in einem untersuchten System gefunden werden. Im Schwachstellenbewertungsmodul können Sie Ihre Maschinen nach Schwachstellen scannen lassen und so überprüfen, ob die Betriebssysteme und installierten Applikationen aktuell sind und ordnungsgemäß funktionieren.

Schwachstellenbewertungsscans werden für Maschinen mit folgenden Betriebssystemen unterstützt:

- Windows. Weitere Informationen finden Sie im Abschnitt '"Unterstützte Microsoft- und Drittanbieter-Produkte" (S. 1046)'.
- macOS. Weitere Informationen finden Sie im Abschnitt '"Unterstützte Apple- und Drittanbieter-Produkte" (S. 1048)'.
- Linux-Maschinen (CentOS 7/Virtuozzo/Acronis Cyber Infrastructure). Weitere Informationen finden Sie im Abschnitt '"Unterstützte Linux-Produkte" (S. 1048)'.

Verwenden Sie die **Patch-Verwaltungs**-Funktionalität (PV), um Patches (Updates) für die Betriebssysteme und Applikationen zu verwalten, die auf Ihren Maschinen installiert sind, und Ihre Systeme so auf dem neuesten Stand zu halten. Im Patch-Verwaltungsmodul können Sie automatisch oder manuell genehmigen, welche Updates auf Ihren Maschinen installiert werden sollen.

Die Patch-Verwaltung wird für Maschinen mit Windows-Betriebssystemen unterstützt. Weitere Informationen finden Sie im Abschnitt '"Unterstützte Microsoft- und Drittanbieter-Produkte" (S. 1046)'.

Schwachstellenbewertung

Der Schwachstellenbewertungsprozess besteht aus folgenden Schritten:

1. Sie erstellen einen Schutzplan mit aktiviertem Schwachstellenbewertungsmodul, spezifizieren die Einstellungen für die Schwachstellenbewertung und weisen den Plan den gewünschten Maschinen zu.
2. Das System sendet (per Planung oder manuell ausgelöst) einen Befehl zur Ausführung des Schwachstellenbewertungsscans an die Protection Agenten, die auf den Maschinen installiert sind.
3. Die Agenten erhalten den Befehl, starten mit dem Scannen nach Schwachstellen und generieren die Scan-Aktivität.
4. Wenn der Schwachstellenbewertungsscan abgeschlossen wurde, generieren die Agenten die entsprechenden Ergebnisse und senden diese an den Monitoring Service.

5. Der Monitoring Service verarbeitet die Daten von den Agenten, zeigt die Ergebnisse im Widget für Schwachstellenbewertung an und listet die gefundenen Schwachstellen auf.
6. Wenn Sie eine Liste von gefundenen Schwachstellen abrufen, können Sie diese verarbeiten und entscheiden, welche der gefundenen Schwachstellen behoben werden sollten.

Sie können die Ergebnisse des Scannens nach Schwachstellen im Widget **Monitoring** –> **Überblick** –> **Schwachstellen / Gefundene Schwachstellen** überwachen.

Unterstützte Microsoft- und Drittanbieter-Produkte

Folgende Microsoft-Produkte und Produkte von Drittanbietern für Windows-Betriebssysteme werden für die Schwachstellenbewertung und Patch-Verwaltung unterstützt:

Unterstützte Microsoft-Produkte

Windows-Betriebssysteme

- Windows 7 (Enterprise, Professional, Ultimate)
- Windows 8
- Windows 8.1
- Windows 10
- Windows 11

Windows Server-Betriebssysteme

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2

Microsoft Office und verwandte Komponenten

- Microsoft Office 2019 (x64, x86)
- Microsoft Office 2016 (x64, x86)
- Microsoft Office 2013 (x64, x86)
- Microsoft Office 2010 (x64, x86)

Mit Windows-Betriebssystemen verwandte Komponenten

- Internet Explorer
- Microsoft EDGE
- Windows Media Player

- .NET Framework
- Visual Studio und Applikationen
- Komponenten des Betriebssystems

Server-Applikationen

- Microsoft SQL Server 2008 R2
- Microsoft SQL Server 2012
- Microsoft SQL Server 2014
- Microsoft SQL Server 2016
- Microsoft SQL Server 2017
- Microsoft SQL Server 2019
- Microsoft Exchange Server 2013
- Microsoft Exchange Server 2016
- Microsoft Exchange Server 2019
- Microsoft SharePoint Server 2016
- Microsoft SharePoint Server 2019

Unterstützte Drittanbieter-Produkte für Windows-Betriebssysteme

Remote-Arbeit ist weltweit zunehmend verbreitet. Daher ist es wichtig, dass Kollaborations- und Kommunikationstools sowie VPN-Clients immer aktuell sind und auf mögliche Schwachstellen überprüft werden. Der Cyber Protection Service unterstützt eine Schwachstellenbewertung und Patch-Verwaltung für solche Applikationen.

Kollaborations- und Kommunikationstools sowie VPN-Clients

- Microsoft Teams
- Zoom
- Skype
- Slack
- Webex
- NordVPN
- TeamViewer

Weitere Informationen über unterstützte Drittanbieter-Produkte für Windows-Betriebssysteme finden Sie in diesem Knowledge Base-Artikel: Liste von Drittanbieter-Produkten, die von der Patch-Verwaltung unterstützt werden (62853).

Unterstützte Apple- und Drittanbieter-Produkte

Folgende Apple-Produkte und Produkte von Drittanbietern für macOS werden für die Schwachstellenbewertung unterstützt:

Unterstützte Apple-Produkte

macOS

- macOS 10.13.x und höher

In macOS integrierte Applikationen

- Safari, iTunes und andere.

Unterstützte Drittanbieter-Produkte für macOS

- Microsoft Office (Word, Excel, PowerPoint, Outlook, OneNote)
- Adobe Acrobat Reader
- Google Chrome
- Firefox
- Opera
- Zoom
- Skype
- Thunderbird
- VLC Media Player

Unterstützte Linux-Produkte

Folgende Linux-Distributionen/-Versionen werden für die Schwachstellenbewertung unterstützt:

- Virtuozzo 7.x
- CentOS 7.x
- CentOS 8.x

Einstellungen für die Schwachstellenbewertung

Eine Anleitung zum Erstellen eines Schutzplans mit aktiviertem Schwachstellenbewertungsmodul finden Sie im Abschnitt 'Einen Schutzplan erstellen'. Sie können Schwachstellenbewertungsscans per Planung oder bei Bedarf/manuell (mit der Aktion **Jetzt ausführen** in einem Schutzplan) durchführen lassen.

Sie können folgende Einstellungen im Schwachstellenbewertungsmodul spezifizieren.

Scan-Umfang

Definieren Sie, welche Software-Produkte nach Schwachstellen gescannt werden sollen:

- Windows-Maschinen:
  - **Microsoft-Produkte**
  - **Windows-Produkte von Drittanbietern** (weitere Informationen über unterstützte Drittanbieter-Produkte für Windows-Betriebssysteme finden Sie im Knowledge Base-Artikel Liste von Drittanbieter-Produkten, die von der Patch-Verwaltung unterstützt werden (62853)).
- macOS-Maschinen:
  - **Apple-Produkte**
  - **macOS-Produkte von Drittanbietern**
- Linux-Maschinen:
  - **Linux-Pakete scannen**

Planung

Definieren Sie eine Planung, auf deren Basis das Scannen nach Schwachstellen auf den ausgewählten Maschinen durchgeführt werden soll:

Feld	Beschreibung
Die Task-Ausführung auf Basis folgender Ereignisse planen	Diese Einstellung definiert, wann der Task ausgeführt werden soll. Folgende Werte sind verfügbar: • **Planung nach Zeit** – Dies ist die Standardeinstellung. Der Task wird gemäß der spezifizierten Zeit ausgeführt. • **Wenn sich ein Benutzer am System anmeldet** – Die Task-Ausführung wird standardmäßig durch die Anmeldung eines (beliebigen) Benutzers ausgelöst. Sie können diese Einstellung so ändern, dass nur ein bestimmtes Benutzerkonto den Task auslösen kann. • **Wenn sich ein Benutzer vom System abmeldet** – Die Task-Ausführung wird standardmäßig durch die Abmeldung eines (beliebigen) Benutzers ausgelöst. Sie können diese Einstellung so ändern, dass nur ein bestimmtes Benutzerkonto den Task auslösen kann. **Hinweis** Der Task wird daher nicht beim Herunterfahren des Systems ausgeführt. Herunterfahren und Abmelden sind unterschiedliche Ereignisse in der Planungskonfiguration. • **Beim Systemstart** – Der Task wird ausgeführt, wenn das Betriebssystem startet.

Feld	Beschreibung
	• **Beim Herunterfahren des Systems** – Der Task wird ausgeführt, wenn das Betriebssystem herunterfährt.
Planungstyp	Das Feld wird angezeigt, wenn Sie bei **Die Task-Ausführung auf Basis folgender Ereignisse planen** die Option **Planung nach Zeit** gewählt haben. Folgende Werte sind verfügbar: • **Monatlich** – Wählen Sie die Monate und dann die jeweiligen Wochen oder Tage des Monats, in denen der Task ausgeführt werden soll. • **Täglich** – Dies ist die Standardeinstellung. Wählen Sie die Wochentage aus, an denen der Task ausgeführt werden soll. • **Stündlich** – Wählen Sie die Wochentage, die Anzahl der Wiederholungen sowie das Zeitintervall aus, in dem der Task ausgeführt werden soll.
Starten um	Das Feld wird angezeigt, wenn Sie bei **Die Task-Ausführung auf Basis folgender Ereignisse planen** die Option **Planung nach Zeit** gewählt haben. Bestimmen Sie den genauen Zeitpunkt, an dem der Task ausgeführt werden soll.
Innerhalb eines Zeitraums ausführen	Das Feld wird angezeigt, wenn Sie bei **Die Task-Ausführung auf Basis folgender Ereignisse planen** die Option **Planung nach Zeit** gewählt haben. Bestimmten Sie einen Datumsbereich, innerhalb dessen die konfigurierte Planung gültig sein soll.
Spezifizieren Sie einen Benutzer, dessen Anmeldung am Betriebssystem einen Task auslösen wird	Das Feld wird angezeigt, wenn Sie bei **Die Task-Ausführung auf Basis folgender Ereignisse planen** die Option **Wenn sich ein Benutzer am System anmeldet** gewählt haben. Folgende Werte sind verfügbar: • **Jeder Benutzer** – Verwenden Sie diese Option, wenn Sie wollen, dass der Task durch die Anmeldung eines beliebigen Benutzers ausgelöst wird. • **Der folgende Benutzer** – Verwenden Sie diese Option, wenn Sie wollen, dass der Task nur durch die Anmeldung eines bestimmten Benutzerkontos ausgelöst wird.
Spezifizieren Sie einen Benutzer, dessen Abmeldung vom Betriebssystem	Das Feld wird angezeigt, wenn Sie bei **Die Task-Ausführung auf Basis folgender Ereignisse planen** die Option **Wenn sich ein Benutzer vom System abmeldet** gewählt haben. Folgende Werte sind verfügbar:

Feld	Beschreibung
einen Task auslösen wird	• **Jeder Benutzer** – Verwenden Sie diese Option, wenn Sie wollen, dass der Task durch die Abmeldung eines beliebigen Benutzers ausgelöst wird. • **Der folgende Benutzer** – Verwenden Sie diese Option, wenn Sie wollen, dass der Task nur durch die Abmeldung eines bestimmten Benutzerkontos ausgelöst wird.
Startbedingungen	Definieren Sie alle Bedingungen, die gleichzeitig zutreffen müssen, damit der Task ausgeführt werden kann. Die Startbedingungen für Antimalware-Scans sind ähnlich wie die Startbedingungen für das **Backup-Modul**, die wiederum im Abschnitt 'Startbedingungen' beschrieben sind. Sie können folgende zusätzliche Startbedingungen definieren: • **Task-Startzeit innerhalb eines Zeitfensters verteilen**– Diese Option ermöglicht es Ihnen, einen Zeitrahmen für den Task festzulegen, um Netzwerkengpässe zu vermeiden. Sie können die Verzögerung in Stunden oder Minuten spezifizieren. Wenn beispielsweise die Standardstartzeit 10:00 Uhr morgens ist und die Verzögerung 60 Minuten beträgt, dann beginnt der Task zwischen 10:00 und 11:00 Uhr morgens. • **Task bei Neustart der Maschine ausführen, wenn die Maschine zur geplanten Zeit ausgeschaltet war** • **Standby- oder Ruhezustandsmodus während der Task-Ausführung verhindern** – Diese Option gilt nur für Maschinen, die unter Windows laufen. • **Wenn die Startbedingungen nicht erfüllt sind, Task trotzdem ausführen nach** – Spezifizieren Sie einen Zeitraum, nach dem der Task unabhängig von anderen Startbedingungen auf jeden Fall gestartet werden soll. **Hinweis** Für Linux werden keine Startbedingungen unterstützt.

Schwachstellenbewertung für Windows-Maschinen

Sie können Windows-Maschinen und Drittanbieter-Produkte für Windows auf Schwachstellen scannen.

So können Sie die Schwachstellenbewertung für Windows-Maschinen konfigurieren

1. Erstellen Sie in der Cyber Protect-Konsole einen Schutzplan und aktivieren Sie das Modul für die **Schwachstellenbewertung**.
2. Spezifizieren Sie die Einstellungen für die Schwachstellenbewertung:

- **Scan-Umfang** – wählen Sie **Microsoft-Produkte**, **Windows-Produkte von Drittanbietern** oder beides.
- **Planung** – definieren Sie die Planung, auf deren Basis die Schwachstellenbewertung ausgeführt wird.

  Weitere Informationen über die **Planungs**-Optionen finden Sie im Abschnitt '"Einstellungen für die Schwachstellenbewertung" (S. 1048)'.

3. Weisen Sie den Windows-Maschinen den Plan zu.

Nach einem Schwachstellenbewertungsscan wird Ihnen eine Liste der gefundenen Schwachstellen angezeigt. Sie können die Informationen bearbeiten und entscheiden, welche der gefundenen Schwachstellen behoben werden sollen.

Wenn Sie die Ergebnisse der Schwachstellenbewertung einsehen bzw. überwachen wollen, nutzen Sie die Widgets **Monitoring** –> **Überblick** –> **Schwachstellen / Gefundene Schwachstellen**.

Schwachstellenbewertung für Linux-Maschinen

Sie können Linux-Maschinen nach Schwachstellen auf Applikations- und Kernel-Ebene scannen lassen.

So können Sie die Schwachstellenbewertung für Linux-Maschinen konfigurieren

1. Erstellen Sie in der Cyber Protect-Konsole einen Schutzplan und aktivieren Sie das Modul für die **Schwachstellenbewertung**.
2. Spezifizieren Sie die Einstellungen für die Schwachstellenbewertung:
   - **Scan-Umfang** – wählen Sie **Linux-Pakete scannen**.
   - **Planung** – definieren Sie die Planung, auf deren Basis die Schwachstellenbewertung ausgeführt wird.

     Weitere Informationen über die **Planungs**-Optionen finden Sie im Abschnitt '"Einstellungen für die Schwachstellenbewertung" (S. 1048)'.
3. Weisen Sie den Linux-Maschinen den Plan zu.

Nach einem Schwachstellenbewertungsscan wird Ihnen eine Liste der gefundenen Schwachstellen angezeigt. Sie können die Informationen bearbeiten und entscheiden, welche der gefundenen Schwachstellen behoben werden sollen.

Wenn Sie die Ergebnisse der Schwachstellenbewertung einsehen bzw. überwachen wollen, nutzen Sie die Widgets **Monitoring** –> **Überblick** –> **Schwachstellen / Gefundene Schwachstellen**.

Schwachstellenbewertung für macOS-Geräte

Sie können macOS-Geräte auf Betriebssystem- und Applikationsebene auf Schwachstellen scannen.

So können Sie die Schwachstellenbewertung für macOS-Geräte konfigurieren

1. Erstellen Sie in der Cyber Protect-Konsole einen Schutzplan und aktivieren Sie das Modul für die **Schwachstellenbewertung**.

2. Spezifizieren Sie die Einstellungen für die Schwachstellenbewertung:
   - **Scan-Umfang** – wählen Sie **Apple-Produkte**, **macOS-Produkte von Drittanbietern** oder beides.
   - **Planung** – definieren Sie die Planung, auf deren Basis die Schwachstellenbewertung ausgeführt wird.

   Weitere Informationen über die **Planungs**-Optionen finden Sie im Abschnitt '"Einstellungen für die Schwachstellenbewertung" (S. 1048)'.
3. Weisen Sie den macOS-Geräten den Plan zu.

Nach einem Schwachstellenbewertungsscan wird Ihnen eine Liste der gefundenen Schwachstellen angezeigt. Sie können die Informationen bearbeiten und entscheiden, welche der gefundenen Schwachstellen behoben werden sollen.

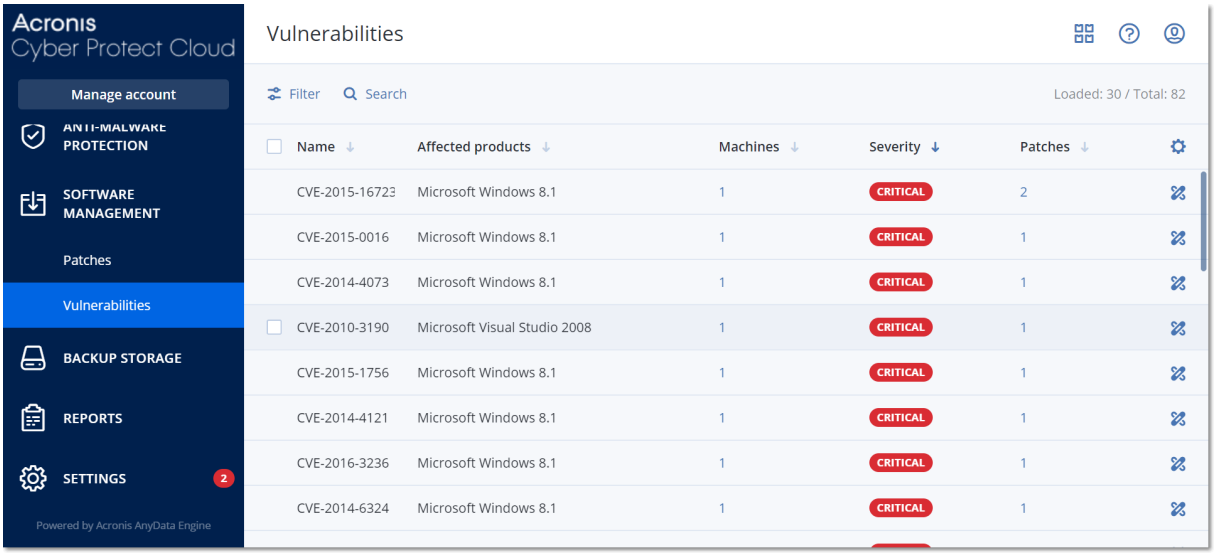
Wenn Sie die Ergebnisse der Schwachstellenbewertung einsehen bzw. überwachen wollen, nutzen Sie die Widgets **Monitoring** –> **Überblick** –> **Schwachstellen / Gefundene Schwachstellen**.

Gefundene Schwachstellen verwalten

Wenn die Schwachstellenbewertung mindestens einmal durchgeführt wurde und Schwachstellen gefunden wurden, können Sie diese unter **Software-Verwaltung** –> **Schwachstellen** einsehen. In der Liste der Schwachstellen werden sowohl Schwachstellen angezeigt, für die Patches installiert werden können, als auch Schwachstellen, für die es keine vorgeschlagenen Patches gibt. Sie können einen Filter verwenden, um nur Schwachstellen mit Patches anzuzeigen.

Name	Beschreibung
Name	Der Name der Schwachstelle.
Betroffene Produkte	Software-Produkte, bei denen Schwachstellen gefunden wurden.
Maschinen	Die Anzahl der betroffenen Maschinen.
Schweregrad	Der Schweregrad der gefundenen Schwachstelle. Folgende Schweregrade können gemäß CVSS (Common Vulnerability Scoring System) zugewiesen werden: • **Kritisch**: 9 - 10 CVSS • **Hoch**: 7 - 9 CVSS • **Mittel**: 3 - 7 CVSS • **Niedrig**: 0 - 3 CVSS • **Ohne**
Patches	Die Anzahl der geeigneten Patches.
Veröffentlicht	Datum und Uhrzeit, als die Schwachstelle gemäß CVE-Standard (Common Vulnerabilities and Exposures) veröffentlicht wurde.
Erkannt	Das erste Datum, an dem die vorhandene Schwachstelle auf Maschinen erkannt wurde.

Sie können eine Beschreibung der gefundenen Schwachstelle einsehen, wenn Sie auf deren Namen in der Liste klicken.



So können Sie den Prozess zur Schwachstellenbehebung starten

1. Gehen Sie in der Cyber Protect-Konsole zum Bereich **Software-Verwaltung** –> **Schwachstellen**.
2. Wählen Sie die Schwachstelle aus der Liste aus und klicken Sie dann auf **Patches installieren**. Der Assistent zur Schwachstellenbehebung wird geöffnet.
3. Wählen Sie die Patches aus, die auf den ausgewählten Maschinen installiert werden sollen, und klicken Sie dann auf **Weiter**.
4. Wählen Sie die Maschinen aus, auf denen die Patches installiert werden sollen.
5. Bestimmen Sie die Neustart-Optionen.
   a. Legen Sie fest, ob die Maschine nach der Installation der Patches neu gestartet werden soll.

Option	Beschreibung
Nein	Die Maschinen werden nicht automatisch neu gestartet, nachdem die Patches installiert wurden.
Bei Bedarf	Die Maschinen werden nur dann neu gestartet, wenn dies für die Anwendung der Patches erforderlich ist.
Ja	Die Maschinen werden automatisch neu gestartet, nachdem die Patches installiert wurden. Sie können außerdem eine Verzögerung für den Neustart spezifizieren.

   b. [Optional] Wenn Sie den Neustart der Maschine verzögern wollen, während ein Backup der Maschine durchgeführt wird, aktivieren Sie die Option **Nicht neu starten, bevor das Backup abgeschlossen wurde**.
6. Klicken Sie auf **Patches installieren**.

Als Ergebnis werden die ausgewählten Patches auf den ausgewählten Maschinen installiert.

Patch-Verwaltung

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Weitere Informationen über unterstützte Drittanbieter-Produkte für Windows-Betriebssysteme finden Sie in diesem Knowledge Base-Artikel: Liste von Drittanbieter-Produkten, die von der Patch-Verwaltung unterstützt werden (62853).

Sie können mit der Patch-Verwaltungsfunktionalität Folgendes tun:

- Updates auf Betriebssystem- und Applikationsebene installieren
- Patches manuell oder automatisch genehmigen
- Patches bei Bedarf (manuell) oder per Planung installieren
- genau definieren, welche Patches nach welchen unterschiedlichen Kriterien installiert werden sollen: Schweregrad, Kategorie und Genehmigungsstatus
- Vor-Update-Backups durchführen, um möglichweise erfolglose Updates zu verhindern
- die Neustart-Option definieren, die nach der Patch-Installation angewendet werden soll

Hinweis
Um mit Windows-Updates arbeiten zu können, muss für die Patch-Verwaltung auf dem entsprechenden Workload die Windows-Update-Funktion aktiviert sein.

Mit Cyber Protection wurde eine Peer-zu-Peer-Technologie für Komponenten-Updates eingeführt, um die Bandbreite des Netzwerkverkehrs zu minimieren. Sie können einen oder mehrere dedizierte Agenten bestimmen, die Updates aus dem Internet herunterladen und für die anderen Agenten im Netzwerk bereitstellen sollen. Alle Agenten werden außerdem die Updates als Peer-zu-Peer-Agenten mit den anderen teilen.

Der Workflow der Patch-Verwaltung

Der Workflow für die Patch-Verwaltung umfasst mehrere Arbeitsschritte: einen Schutzplan konfigurieren und anwenden, einen Schwachstellenbewertungsscan durchführen, Patch-Einstellungen konfigurieren, Patches genehmigen und abschließend die Installation der genehmigten Patches. Die genauen Schritte des Workflows sehen folgendermaßen aus.

1. Konfigurieren Sie einen Schutzplan, bei dem die Module **Schwachstellenbewertung** und **Patch-Verwaltung** aktiviert sind.
2. Konfigurieren Sie die Einstellungen für die Schwachstellenbewertung. Weitere Informationen zu diese Einstellungen finden Sie im Abschnitt '"Einstellungen für die Schwachstellenbewertung" (S. 1048)'.

3. Konfigurieren Sie die Einstellungen für die Patch-Verwaltung. Weitere Informationen zu diese Einstellungen finden Sie im Abschnitt '"Die Einstellungen für die Patch-Verwaltung im Schutzplan" (S. 1056)'
4. Wenden Sie den Schutzplan auf eine oder mehrere Maschinen an.
5. Warten Sie darauf, dass ein Schwachstellenbewertungsscan abgeschlossen wird. Der Scan wird automatisch gemäß der Planung gestartet, die im Schutzplan konfiguriert ist. Alternativ können Sie den Scan auch manuell starten, indem Sie im Modul **Schwachstellenbewertung** des Schutzplans auf den Button **Jetzt ausführen** klicken.
6. Genehmigen Sie die Patches. Sie können Einstellungen für die automatische Patch-Genehmigung definieren, wozu auch eine automatische Installation der Patches auf den Testmaschinen gehört. Weitere Informationen finden Sie im Abschnitt '"Automatische Patch-Genehmigung" (S. 1064)'. Alternativ können Sie Patches auch manuell genehmigen, indem Sie deren Genehmigungsstatus auf **Genehmigt** setzen. Weitere Informationen finden Sie im Abschnitt '"Patches manuell genehmigen" (S. 1069)'.
7. Installieren Sie die Patches. Die genehmigten Patches können gemäß der im Schutzplan konfigurierten Planung automatisch installiert werden. Alternativ können Sie Patches auch bei Bedarf manuell installieren. Weitere Informationen finden Sie im Abschnitt '"Patches bei Bedarf manuell installieren" (S. 1069)'.

Sie können die Ergebnisse der Patch-Installation im Widget **Monitoring** –> **Überblick** –> **Verlauf der Patch-Installation** überwachen.

Die Einstellungen für die Patch-Verwaltung im Schutzplan

Sie können im Modul **Patch-Verwaltung** des Schutzplans folgende Einstellungen für die Patch-Verwaltung vornehmen:

- Welche Updates für Microsoft- und Drittanbieter-Produkte für Windows-Betriebssysteme zu installieren sind.
- Wann die automatische Patch-Installation ausgeführt werden soll.
- Ob ein Vor-Update-Backup durchgeführt werden soll.

Weitere Informationen darüber, wie Sie einen Schutzplan erstellen und das Modul **Patch-Verwaltung** aktivieren können, finden Sie im Abschnitt '"Einen Schutzplan erstellen" (S. 232)'.

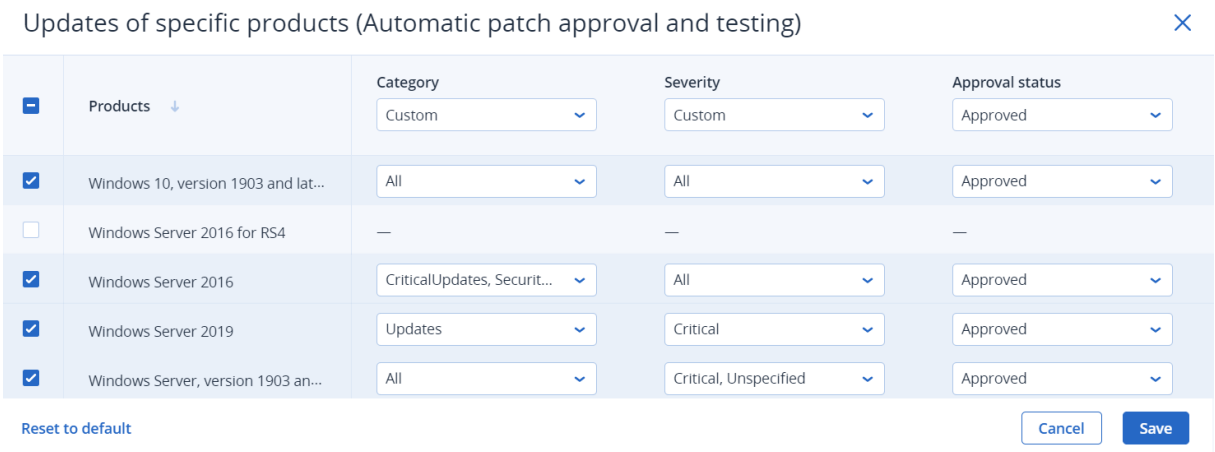
Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Microsoft-Produkte

Wenn Sie Microsoft-Updates auf den ausgewählten Maschinen installieren lassen wollen, aktivieren Sie die Option **Microsoft-Produkte aktualisieren**.

Wählen Sie die Installationsoption aus:

Option	Beschreibung
Alle Updates	Verwenden Sie diese Option, wenn Sie alle genehmigten Updates installieren wollen.
Nur kritische und Sicherheits-Updates	Verwenden Sie diese Option, wenn Sie alle genehmigten kritischen und Sicherheits-Updates installieren wollen.
Updates bestimmter Produkte (Automatische Genehmigen und Testen von Patches)	Verwenden Sie diese Option, wenn Sie für verschiedene Produkte individuelle Einstellungen definieren wollen. Wenn Sie bestimmte Produkte aktualisieren wollen, können Sie für jedes dieser Produkte anhand der Kriterien Kategorie, Schweregrad oder Genehmigungsstatus definieren, welche Updates installiert werden sollen. Wählen Sie diese Option, wenn Sie konfigurieren wollen, dass die automatische Genehmigung und Anwendung der Patches getestet werden soll.



Für die Verteilung von Patches für Microsoft-Produkte wird der Windows API-Dienst verwendet. Die Patches und Updates werden weder heruntergeladen noch intern oder auf den Verteilungsagenten gespeichert. Sie werden stattdessen direkt vom Microsoft Content Delivery Network (CDN) heruntergeladen. Daher kann ein Agent, selbst wenn ihm die Rolle 'Updater' zugewiesen wurde, keine Patches herunterladen und verteilen.

Windows-Produkte von Drittherstellern

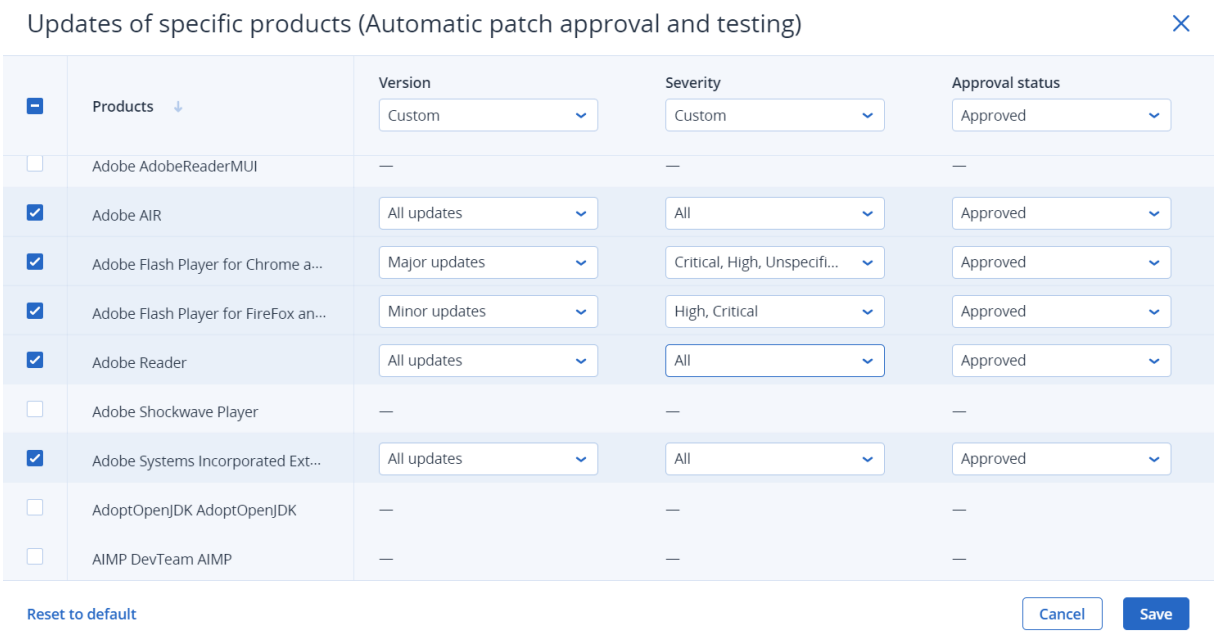
Wenn Sie Drittherstellers-Updates für Windows-Betriebssysteme auf den ausgewählten Maschinen installieren lassen wollen, aktivieren Sie die Option **Windows-Produkte von Drittherstellern**.

Wählen Sie die Installationsoptionen aus:

Option	Beschreibung
Alle Updates	Verwenden Sie diese Option, wenn Sie alle genehmigten Updates installieren wollen. *

Option	Beschreibung
Nur größere Updates	Verwenden Sie diese Option, wenn Sie alle genehmigten größeren Updates installieren wollen.
Nur kleinere Updates	Verwenden Sie diese Option, wenn Sie auch genehmigte kleinere Updates installieren wollen.
Updates bestimmter Produkte (Automatische Genehmigen und Testen von Patches)	Verwenden Sie diese Option, wenn Sie für verschiedene Produkte individuelle Einstellungen definieren wollen. Wenn Sie bestimmte Produkte aktualisieren wollen, können Sie für jedes dieser Produkte anhand der Kriterien Kategorie, Schweregrad oder Genehmigungsstatus definieren, welche Updates installiert werden sollen. Wählen Sie diese Option, wenn Sie konfigurieren wollen, dass die automatische Genehmigung und Anwendung der Patches getestet werden soll.
Die neuesten Versionen nur für Applikationen mit erkannten Schwachstellen installieren	Aktivieren Sie dieses Kontrollkästchen, wenn Sie nur bei solchen Applikationen, bei denen Schwachstellen entdeckt wurden, die neuesten Updates installieren wollen. *

* Für diese Option ist der Cyber Protect Agent in der Version 23.11.36772 oder höher erforderlich.



Die Patches für Windows-Produkte von Drittanbietern werden direkt aus einer internen Datenbank von Acronis an die verwalteten Workloads verteilt. Wenn einem Agenten die Rolle 'Updater' zugewiesen wird, wird dieser Agent eingesetzt, um Patches herunterzuladen und zu verteilen.

Planung

Definieren Sie eine Planung und Bedingungen, auf deren Basis die Updates auf den ausgewählten Maschinen installiert werden sollen.

Feld	Beschreibung
Die Task-Ausführung auf Basis folgender Ereignisse planen	Diese Einstellung definiert, wann der Task ausgeführt werden soll. Folgende Werte sind verfügbar: • **Planung nach Zeit** – Dies ist die Standardeinstellung. Der Task wird gemäß der spezifizierten Zeit ausgeführt. • **Wenn sich ein Benutzer am System anmeldet** – Die Task-Ausführung wird standardmäßig durch die Anmeldung eines (beliebigen) Benutzers ausgelöst. Sie können diese Einstellung ändern, damit nur ein bestimmtes Benutzerkonto den Task auslösen kann. • **Wenn sich ein Benutzer vom System abmeldet** – Die Task-Ausführung wird standardmäßig durch die Abmeldung eines (beliebigen) Benutzers ausgelöst. Sie können diese Einstellung so ändern, dass nur ein bestimmtes Benutzerkonto den Task auslösen kann. **Hinweis** Der Task wird daher nicht beim Herunterfahren des Systems ausgeführt. Herunterfahren und Abmelden sind unterschiedliche Ereignisse in der Planungskonfiguration. • **Beim Systemstart** – Der Task wird ausgeführt, wenn das Betriebssystem startet. • **Beim Herunterfahren des Systems** – Der Task wird ausgeführt, wenn das Betriebssystem herunterfährt.
Planungstyp	Das Feld wird angezeigt, wenn Sie bei **Die Task-Ausführung auf Basis folgender Ereignisse planen** die Option **Planung nach Zeit** gewählt haben. Folgende Werte sind verfügbar: • **Monatlich** – Wählen Sie die Monate und dann die jeweiligen Wochen oder Tage des Monats, in denen der Task ausgeführt werden soll. • **Täglich** – Dies ist die Standardeinstellung. Wählen Sie die Wochentage aus, an denen der Task ausgeführt werden soll. • **Stündlich** – Wählen Sie die Wochentage, die Anzahl der Wiederholungen sowie das Zeitintervall aus, in dem der Task ausgeführt werden soll.

Feld	Beschreibung
Starten um	Das Feld wird angezeigt, wenn Sie bei **Die Task-Ausführung auf Basis folgender Ereignisse planen** die Option **Planung nach Zeit** gewählt haben. Bestimmen Sie den genauen Zeitpunkt, an dem der Task ausgeführt werden soll.
Wartungsfenster für Patches konfigurieren	Das Feld wird angezeigt, wenn Sie bei **Die Task-Ausführung auf Basis folgender Ereignisse planen** die Option **Planung nach Zeit** gewählt haben. Wählen Sie diese Einstellung, wenn Sie wollen, dass die Patch-Installation nur während des von Ihnen spezifizierten Zeitintervalls ausgeführt wird. Wenn der Prozess der Patch-Installation nicht bis zum im Wartungsfenster für Patches definierten Endzeitpunkt abgeschlossen ist, wird er automatisch gestoppt.
Innerhalb eines Zeitraums ausführen	Das Feld wird angezeigt, wenn Sie bei **Die Task-Ausführung auf Basis folgender Ereignisse planen** die Option **Planung nach Zeit** gewählt haben. Bestimmten Sie einen Datumsbereich, innerhalb dessen die konfigurierte Planung gültig sein soll.
Spezifizieren Sie einen Benutzer, dessen Anmeldung am Betriebssystem einen Task auslösen wird	Das Feld wird angezeigt, wenn Sie bei **Die Task-Ausführung auf Basis folgender Ereignisse planen** die Option **Wenn sich ein Benutzer am System anmeldet** gewählt haben. Folgende Werte sind verfügbar: • **Jeder Benutzer** – Verwenden Sie diese Option, wenn Sie wollen, dass der Task durch die Anmeldung eines beliebigen Benutzers ausgelöst wird. • **Der folgende Benutzer** – Verwenden Sie diese Option, wenn Sie wollen, dass der Task nur durch die Anmeldung eines bestimmten Benutzerkontos ausgelöst wird.
Spezifizieren Sie einen Benutzer, dessen Abmeldung vom Betriebssystem einen Task auslösen wird	Das Feld wird angezeigt, wenn Sie bei **Die Task-Ausführung auf Basis folgender Ereignisse planen** die Option **Wenn sich ein Benutzer vom System abmeldet** gewählt haben. Folgende Werte sind verfügbar: • **Jeder Benutzer** – Verwenden Sie diese Option, wenn Sie wollen, dass der Task durch die Abmeldung eines beliebigen Benutzers ausgelöst wird. • **Der folgende Benutzer** – Verwenden Sie diese Option, wenn Sie wollen, dass der Task nur durch die Abmeldung eines bestimmten Benutzerkontos ausgelöst wird.

Feld	Beschreibung
Startbedingungen	Definieren Sie alle Bedingungen, die gleichzeitig zutreffen müssen, damit der Task ausgeführt werden kann. Die Startbedingungen für Antimalware-Scans sind ähnlich wie die Startbedingungen für das **Backup-Modul**, die wiederum im Abschnitt 'Startbedingungen' beschrieben sind. Sie können folgende zusätzliche Startbedingungen definieren: • **Task-Startzeit innerhalb eines Zeitfensters verteilen**– Diese Option ermöglicht es Ihnen, einen Zeitrahmen für den Task festzulegen, um Netzwerkengpässe zu vermeiden. Sie können die Verzögerung in Stunden oder Minuten spezifizieren. Wenn beispielsweise die Standardstartzeit 10:00 Uhr morgens ist und die Verzögerung 60 Minuten beträgt, dann beginnt der Task zwischen 10:00 und 11:00 Uhr morgens. • **Task bei Neustart der Maschine ausführen, wenn die Maschine zur geplanten Zeit ausgeschaltet war** • **Standby- oder Ruhezustandsmodus während der Task-Ausführung verhindern** – Diese Option gilt nur für Maschinen, die unter Windows laufen. • **Wenn die Startbedingungen nicht erfüllt sind, Task trotzdem ausführen nach** – Spezifizieren Sie einen Zeitraum, nach dem der Task unabhängig von anderen Startbedingungen auf jeden Fall gestartet werden soll. **Hinweis** Für Linux werden keine Startbedingungen unterstützt.
Nach dem Update neu starten	Definieren Sie, ob die Maschine nach Abschluss der Update-Installation automatisch neu gestartet werden soll. Folgende Werte sind verfügbar: • **Nie** – Es wird kein Neustart nach der Update-Installation initiiert. • **Bei Bedarf** – Es wird nur dann ein Neustart initiiert, wenn dies für die Anwendung der Updates erforderlich ist. • **Immer** – Es wird immer ein Neustart nach der Update-Installation initiiert. Sie können eine Verzögerung für den Neustart spezifizieren.
Nicht neu starten, bevor das Backup abgeschlossen wurde	Wenn Sie diese Option wählen, wird bei einem laufenden Backup-Prozess der Neustart der Maschine solange verzögert, bis das Backup abgeschlossen wurde.

Vor-Update-Backup

Backup vor der Installation von Software-Updates ausführen – das System wird ein inkrementelles Backup der Maschine erstellen, bevor irgendein Update auf dieser installiert wird. Wenn bisher noch kein Backup erstellt wurde, wird die Maschine über ein vollständiges Backup gesichert. Dadurch können Sie Fälle verhindern, in denen die Update-Installation nicht erfolgreich war und Sie zum vorherigen Zustand zurückgehen müssen. Damit die Option **Vor-Update-Backup** funktionieren kann, muss den entsprechenden Maschinen ein Schutzplan mit aktiviertem Patch-Verwaltungs- und Backup-Modul zugewiesen sein und in letzterem als Backup-Quelle entweder die komplette Maschine oder die Boot- und System-Volumes festgelegt sein. Wenn Sie ungeeignete Elemente für das Backup auswählen, wird das System verhindern, dass Sie die Option **Vor-Update-Backup** aktivieren können.

Die Liste der verfügbaren Patches anzeigen

Nachdem ein Schwachstellenbewertungsscan abgeschlossen wurde, können Sie die Informationen über die verfügbaren Patches im Bereich **Software-Verwaltung** –> **Patches** einsehen.

Wenn Sie Details zu einem bestimmten Patch sehen wollen, klicken Sie in der Liste der Patches auf den gewünschten Patch.

In der nachfolgenden Tabelle werden die Informationen für den Patch beschrieben, die Sie auf dem Bildschirm einsehen können.

Feld	Beschreibung
Genehmigungsstatus	Der Genehmigungsstatus wird hauptsächlich für automatische Genehmigungsszenarien benötigt. Sie können folgende Statuszustände für einen Patch definieren: • **Genehmigt** – der Patch wurde auf mindestens einer Maschine installiert und mit 'Ok' eingestuft. • **Abgelehnt** – der Patch ist nicht sicher und kann das System einer Maschine beschädigen • **Warten a. Bestätigung** – der Patch-Status ist unklar und sollte validiert werden
Lizenzvereinbarung	• Zugestimmt • Keine Zustimmung. Wenn Sie der Lizenzvereinbarung nicht zustimmen, wird als Patch-Status **Abgelehnt** festgelegt und der Patch wird nicht installiert.
Schweregrad	Der Schweregrad des Patches: • **Kritisch** • **Hoch** • **Mittel**

	• **Niedrig** • **Ohne**
Anbieter	Der Anbieter oder Hersteller des Patches
Betroffenes Produkt	Das Produkt, für das der Patch verfügbar ist
Installierte Versionen	Die Produktversionen, die bereits installiert sind
Version	Die Version des Patches
Kategorie	Die Kategorie, zu der der Patch gehört: • **Kritisches Update** – allgemein veröffentlichte Fixes für spezifische Probleme, die kritische, nicht sicherheitsbezogene Fehler beheben. • **Sicherheitsupdate** – allgemein veröffentlichte Fixes für spezifische Produkte, die Sicherheitsprobleme beheben. • **Definitionsupdates** – Updates für Viren-Definitionen oder andere Definitionsdateien. • **Update-Rollups** – eine kumulative Zusammenstellung von Hotfixes, Sicherheitsupdates, kritischen Updates und anderen Updates, die für eine einfache Bereitstellung gebündelt wurden. Ein Rollup ist normalerweise für einen bestimmten Bereich (z.B. Sicherheit) oder eine bestimmte Komponente (z.B. die Internet-Informationsdienste (IIS)) ausgelegt. • **Service Packs** – eine kumulative Zusammenstellung von Hotfixes, Sicherheitsupdates, kritischen Updates und anderen Updates, die seit der Veröffentlichung des Produktes erstellt wurden. Service Packs können auch eine begrenzte Anzahl von Design- oder Funktionsänderungen enthalten, die Kunden gewünscht haben. • **Tools** – Hilfsprogramme (Utilities) oder Funktionen, die der Bewältigung einzelner oder mehrerer Aufgaben dienen. • **Feature Packs** – neue Funktionen, die zumeist auch in die nächste Produktversion integriert werden. • **Updates** – allgemein veröffentlichte Fixes für spezifische Probleme, die nicht kritische, nicht sicherheitsbezogene Fehler beheben. • **Applikation** – Patches für eine Applikation.
Veröffentlichungsdatum	Das Datum, an dem der Patch veröffentlicht wurde
Zuletzt gemeldet	Das Datum, an dem der Patch das letzte Mal gemeldet wurde
Zuerst installiert	Das Datum, an dem der Patch zum ersten Mal erfolgreich auf einer Maschine installiert wurde
Microsoft KB	Wenn der Patch für ein Microsoft-Produkt ist, wird in diesem Feld die ID des KB-Artikels angezeigt.
Maschinen	Anzahl der betroffenen Maschinen

Schwachstellen	Die Anzahl der Schwachstellen. Wenn Sie darauf klicken, werden Sie zur Liste der Schwachstellen weitergeleitet.
Größe	Die durchschnittliche Größe des Patches
Sprache	Die vom Patch unterstützte Sprache.
Anbieter-Website	Die offizielle Website des Anbieters/Herstellers

Die Patch-Lebensdauer in der Liste konfigurieren

Sie können die Liste der Patches auf dem neuesten Stand halten, indem Sie die Lebensdauer der Patches in der Liste auf der Anzeige **Patches** konfigurieren. Diese Einstellung definiert, wie lange der erkannte verfügbare Patch in der Liste der Patches angezeigt wird. Der Patch wird aus der Liste entfernt, wenn er auf allen Maschinen, auf denen er als fehlend angezeigt wurde, erfolgreich installiert wurde oder wenn die Lebensdauer in der Liste abgelaufen ist.

So können Sie die Patch-Lebensdauer in der Liste konfigurieren

1. Gehen Sie in der Cyber Protect-Konsole zum Bereich **Software-Verwaltung** –> **Patches**.
2. Klicken Sie auf **Einstellungen**.
3. Wählen Sie bei **Lebensdauer in der Liste** die entsprechende Option.

Option	Beschreibung
Unbegrenzt	Der Patch wird nie aus der Liste entfernt.
7 Tage	Der Patch wird sieben Tage nach seiner ersten Installation aus der Liste entfernt. Nehmen wir beispielsweise an, dass Sie zwei Maschinen haben, auf denen Patches installiert werden müssen. Eine davon ist online, die andere offline. Der Patch wurde auf der ersten Maschine installiert. Der Patch wird nach 7 Tagen aus der Liste der Patches entfernt, obwoh er nicht auf der zweiten Maschine installiert wurde (weil diese offline war).
30 Tage	Der Patch wird 30 Tage nach seiner ersten Installation aus der Liste entfernt.

Automatische Patch-Genehmigung

Die automatische Patch-Genehmigung macht die Installation von Updates auf den Maschinen einfacher. Mit einer automatischen Patch-Genehmigung wird die Installation von Patches nicht durch den manuellen Patch-Genehmigungsprozess verzögert. Wichtige Updates und Bugfixes werden schneller installiert, was die Zuverlässigkeit Ihres Systems erhöhen wird.

Sie können die automatische Patch-Genehmigung in Testszenarien für die automatische Installation von Patches verwenden. Wenn die Patches auf den Testmaschinen erfolgreich installiert wurden, werden sie auch automatisch auf den Produktionsmaschinen installiert. Weitere Informationen

über dieses Szenario finden Sie im Abschnitt '"Ein Anwendungsfall für das automatische Genehmigen und Testen von Patches" (S. 1065)'.

Sie können die automatische Patch-Genehmigung auch in Szenarien für die automatische Installation von Patches in Ihrer Produktionsumgebung verwenden und dabei die Testphase überspringen. Weitere Informationen über dieses Szenario finden Sie im Abschnitt '"Ein Anwendungsfall für das automatische Genehmigen von Patches ohne vorheriges Testen" (S. 1068)'.

Konfiguration der automatischen Patch-Genehmigung

Sie können die automatische Patch-Genehmigung konfigurieren und dadurch sicherstellen, dass die Installation von Patches nicht durch den manuellen Patch-Genehmigungsprozess verzögert wird.

So können Sie die automatische Patch-Genehmigung konfigurieren

1. Gehen Sie in der Cyber Protect-Konsole zum Bereich **Software-Verwaltung** –> **Patches**.
2. Klicken Sie auf **Einstellungen**.
3. Aktivieren Sie die **Automatische Patch-Genehmigung**.
4. Konfigurieren Sie die Einstellungen für die automatische Patch-Genehmigung.
   a. Bestimmen Sie die Option für die automatische Patch-Genehmigung.

Option	Beschreibung
Automatische Genehmigen und Testen von Patches	Der Genehmigungsstatus des Patches wird auf **Genehmigt** geändert, wenn die festgelegte Anzahl von Tagen verstrichen ist, nachdem der Patch erfolgreich installiert wurde. Wir empfehlen, dass Sie diese Einstellung verwenden, wenn Sie die Patches testen wollen, indem Sie diese zuerst auf einer Testmaschine installieren. Dadurch können Sie sicherstellen, dass alles erwartungsgemäß funktioniert, und dann die Patches in Ihrer Produktionsumgebung installieren.
Automatische Genehmigen von Patches ohne Testen	Der Genehmigungsstatus des Patches wird auf **Genehmigt** geändert, wenn die festgelegte Anzahl von Tagen verstrichen ist, nachdem der Patch gefunden wurde.

   b. Bestimmen Sie die Anzahl der Tage, die verstreichen müssen, nachdem die Bedingung für die automatische Patch-Genehmigung erfüllt ist. Nach dieser Frist wird der Status der Patches automatisch von **Warten a. Bestätigung** zu **Genehmigt** geändert.
5. Wählen Sie die Option **Lizenzvereinbarungen automatisch akzeptieren**.
6. Klicken Sie auf **Anwenden**.

Ein Anwendungsfall für das automatische Genehmigen und Testen von Patches

Wenn Sie die neuen Patches auf einer Testmaschine ausprobieren wollen, bevor diese auf Ihren Produktionsmaschinen aufgespielt werden, können Sie zwei Schutzpläne konfigurieren – einen Plan

für die Installation der Patches für Testzwecke sowie einen Plan für die Installation der getesteten Patches auf Produktionsmaschinen. So können Sie sicherstellen, dass die Patches, die Sie in Ihrer Produktionsumgebung installieren, auch sicher sind und Ihre Produktionsmaschinen nach der Patch-Installation korrekt funktionieren.

Der Anwendungsfall besteht aus den folgenden Phasen:

1. Konfigurieren Sie die Einstellungen für die automatische Patch-Genehmigung. Wählen Sie die Option **Automatische Genehmigen und Testen von Patches**. Weitere Informationen finden Sie im Abschnitt '"Konfiguration der automatischen Patch-Genehmigung" (S. 1065)'.
2. Konfigurieren Sie einen Schutzplan für Testzwecke (beispielsweise mit der Bezeichnung 'Patch-Test'), in dem das Modul **Patch-Verwaltung** aktiviert ist, und wenden Sie den Schutzplan auf die Maschinen in der Testumgebung an. Spezifizieren Sie folgende Bedingung für die Patch-Installation: der Patch-Genehmigungsstatus muss **Warten a. Bestätigung** sein. Dieser Schritt ist erforderlich, um die Patches zu validieren und zu überprüfen, ob die Maschinen nach der Patch-Installation noch ordnungsgemäß funktionieren. Weitere Informationen finden Sie im Abschnitt '"Den Schutzplan 'Patch-Test' konfigurieren" (S. 1066)'.
3. Konfigurieren Sie einen Schutzplan für die Produktionsumgebung (beispielsweise mit der Bezeichnung 'Produktion patchen'), in dem das Modul **Patch-Verwaltung** aktiviert ist, und wenden Sie den Schutzplan dann auf die Maschinen in der Produktionsumgebung an. Spezifizieren Sie folgende Bedingung für die Patch-Installation: der Patch-Status muss **Genehmigt** sein. Weitere Informationen finden Sie im Abschnitt '"Den Schutzplan 'Produktion patchen' konfigurieren" (S. 1067)'.
4. Führen Sie den Schutzplan 'Patch-Test' aus und überprüfen Sie die Ergebnisse. Belassen Sie den Genehmigungsstatus der Maschinen, bei denen keine Probleme aufgetreten sind, auf **Warten a. Bestätigung**, aber ändern Sie den Genehmigungsstatus der Maschinen, die fehlerhaft arbeiten zu **Abgelehnt**. Entsprechend der Anzahl der Tage, die in der Einstellung **Automatische Patch-Genehmigung** festgelegt wurde, wird der Status der Patches automatisch von **Warten a. Bestätigung** auf **Genehmigt** geändert. Wenn Sie den Schutzplan 'Produktion patchen' ausführen, werden nur die Patches mit dem Status **Genehmigt** auf den Produktionsmaschinen installiert. Weitere Informationen finden Sie im Abschnitt '"Den Schutzplan 'Patch-Test' ausführen und unsichere Patches ablehnen" (S. 1068)'.
5. Führen Sie den Schutzplan 'Produktion patchen' aus.

Den Schutzplan 'Patch-Test' konfigurieren

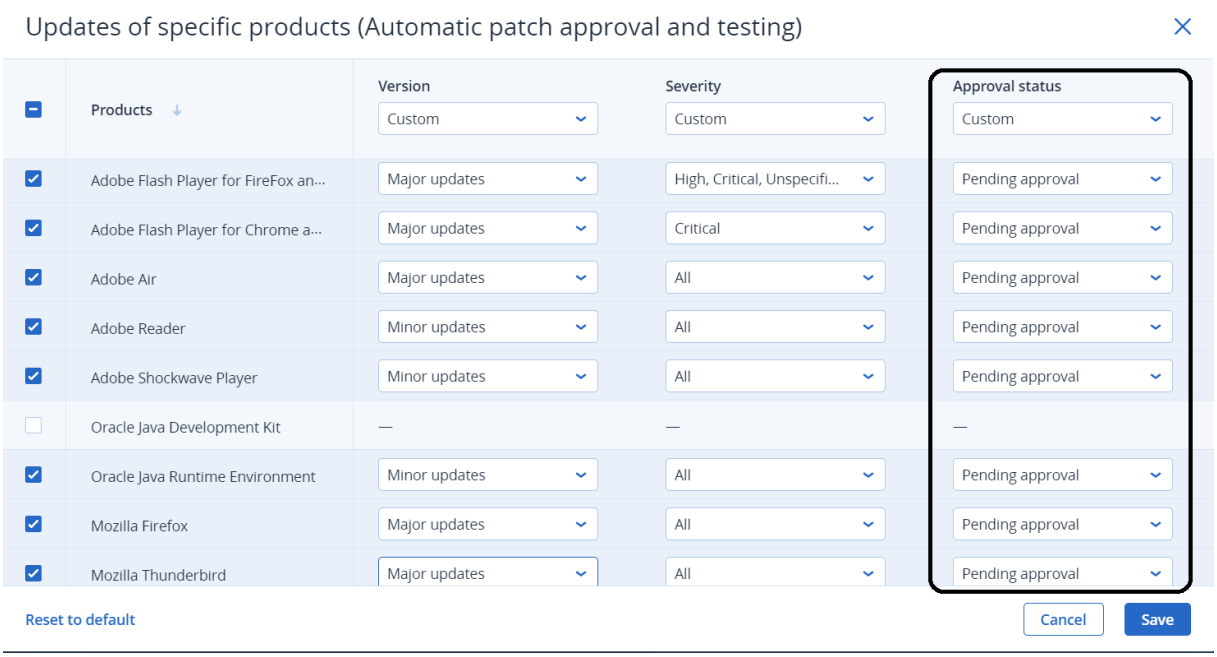
Sie können einen Schutzplan mit Einstellungen zur Patch-Installation für die Maschinen in Ihrer Testumgebung konfigurieren.

So können Sie den Schutzplan 'Patch-Test' konfigurieren

1. Gehen Sie in der Cyber Protect-Konsole zum Bereich **Verwaltung** –> **Schutzpläne**.
2. Klicken Sie auf **Plan erstellen**.
3. Aktivieren Sie das Modul **Patch-Verwaltung**.

4. Definieren Sie, welche Updates für Microsoft- und Drittanbieter-Produkte installiert werden sollen, welche Planung verwendet werden soll und ob ein 'Vor-Update-Backup' ausgeführt werden soll. Weitere Informationen zu diesen Einstellungen finden Sie in Abschnitt '"Die Einstellungen für die Patch-Verwaltung im Schutzplan" (S. 1056)'.

Wichtig
Legen Sie für alle zu aktualisierenden Produkte den Genehmigungsstatus als **Warten a. Bestätigung** fest. Dadurch wird der Agent nur Patches mit dem Status **Warten a. Bestätigung** auf den ausgewählten Maschinen in der Testumgebung installieren.



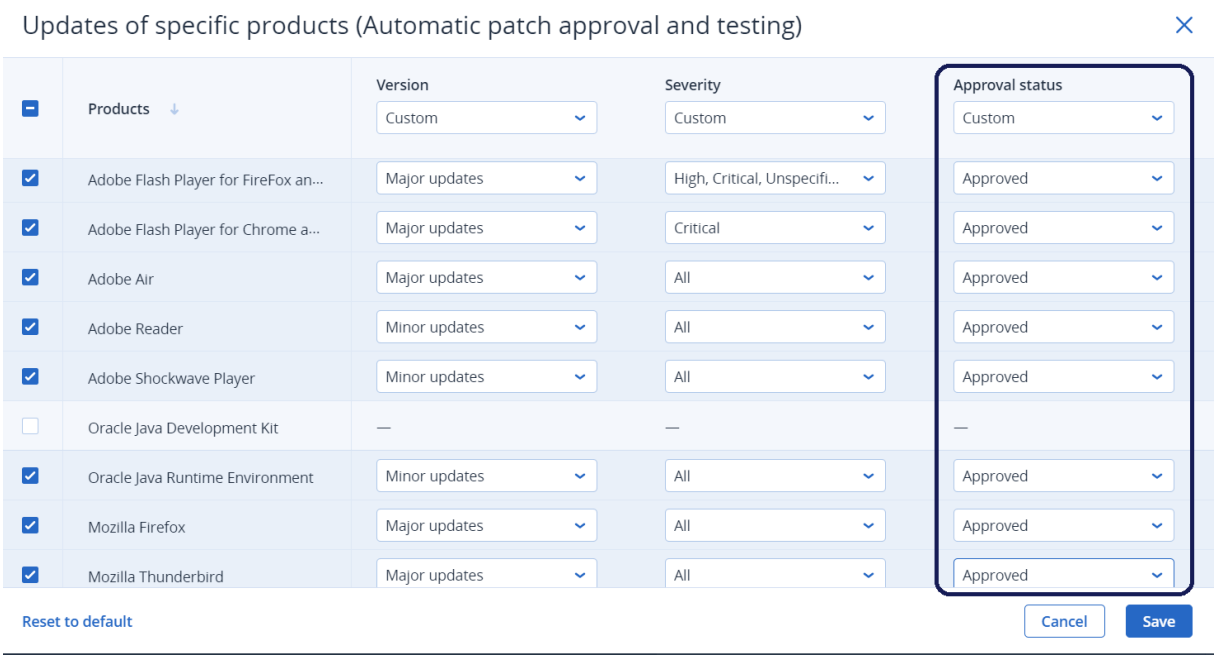
Den Schutzplan 'Produktion patchen' konfigurieren

Sie können einen Schutzplan mit Einstellungen zur Patch-Installation für die Maschinen in Ihrer Produktionsumgebung konfigurieren.

So können Sie den Schutzplan 'Produktion patchen' konfigurieren

1. Gehen Sie in der Cyber Protect-Konsole zum Bereich **Verwaltung** –> **Schutzpläne**.
2. Klicken Sie auf **Plan erstellen**.
3. Aktivieren Sie das Modul **Patch-Verwaltung**.
4. Definieren Sie, welche Updates für Microsoft- und Drittanbieter-Produkte installiert werden sollen, welche Planung verwendet werden soll und ob ein 'Vor-Update-Backup' ausgeführt werden soll. Weitere Informationen zu diesen Einstellungen finden Sie in Abschnitt '"Die Einstellungen für die Patch-Verwaltung im Schutzplan" (S. 1056)'.

Wichtig
Legen Sie für alle zu aktualisierenden Produkte den **Genehmigungsstatus** als **Genehmigt** fest. Dadurch wird der Agent nur Patches mit dem Status **Genehmigt** auf den ausgewählten Maschinen in der Produktionsumgebung installieren.



Den Schutzplan 'Patch-Test' ausführen und unsichere Patches ablehnen

Nachdem die Patches auf den Maschinen in Ihrer Testumgebung installiert wurden, können Sie überprüfen, ob alles erwartungsgemäß funktioniert. Sie können den Genehmigungsstatus der Maschinen, bei denen keine Probleme aufgetreten sind, auf **Warten a. Bestätigung**belassen, aber den Genehmigungsstatus der Maschinen, die fehlerhaft arbeiten, zu **Abgelehnt** ändern.

So können Sie den Schutzplan 'Patch-Test' ausführen und unsichere Patches ablehnen

1. Führen Sie den Schutzplan zum Patchen der Testumgebung aus (nach Planung oder manuell).
2. Je nach Ergebnis können Sie sehen, welche der installierten Patches sicher sind.
3. Gehen Sie zu **Software-Verwaltung** –> **Patches** und legen Sie den **Genehmigungsstatus** der nicht sicheren Patches als **Abgelehnt** fest.

Ein Anwendungsfall für das automatische Genehmigen von Patches ohne vorheriges Testen

Wenn Sie neue Patches möglichst schnell auf Ihren Produktionsmaschinen automatisch installieren wollen, ohne dass diese zuerst auf Testmaschinen installiert werden, müssen Sie nur einen Schutzplan konfigurieren.

Der Anwendungsfall besteht aus den folgenden Phasen:

1. Konfigurieren Sie die Einstellungen für die automatische Patch-Genehmigung. Wählen Sie die Option **Automatische Genehmigen von Patches ohne Testen**. Weitere Informationen finden Sie im Abschnitt '"Konfiguration der automatischen Patch-Genehmigung" (S. 1065)'.
2. Konfigurieren Sie einen Schutzplan für die Produktionsumgebung (beispielsweise mit der Bezeichnung 'Produktion patchen'), in dem das Modul **Patch-Verwaltung** aktiviert ist, und wenden Sie den Schutzplan dann auf die Maschinen in der Produktionsumgebung an. Spezifizieren Sie folgende Bedingung für die Patch-Installation: der Patch-Status muss **Genehmigt** sein. Weitere Informationen finden Sie im Abschnitt '"Den Schutzplan 'Produktion patchen' konfigurieren" (S. 1067)'.
3. Führen Sie den Schutzplan 'Produktion patchen' aus.

Patches manuell genehmigen

Sie können einen Patch manuell genehmigen und dessen Installation beschleunigen, indem Sie die Testphase überspringen.

Voraussetzungen

- Ein Schutzplan, bei dem das Modul **Patch-Verwaltung** aktiviert ist, wird auf mindestens eine Windows-Maschine angewendet.
- Es gibt Patches, die noch nicht auf der Maschine oder den Maschinen installiert sind, auf die der Schutzplan angewendet wurde.

So können Sie Patches manuell genehmigen

1. Gehen Sie in der Cyber Protect-Konsole zum Bereich **Software-Verwaltung** –> **Patches**.
2. Wählen Sie die zu installierenden Patches aus und akzeptieren Sie dann deren Lizenzvereinbarungen.
3. Setzen Sie den **Genehmigungsstatus** der Patches auf **Genehmigt**.
   Der Genehmigungsstatus der Patches wird auf **Genehmigt** gesetzt. Die Patches werden gemäß der im Schutzplan definierten Planung automatisch auf den Maschinen installiert. Wenn Sie wollen, dass die Patches sofort installiert werden, befolgen Sie die im Abschnitt '"Patches bei Bedarf manuell installieren" (S. 1069)' beschriebene Prozedur.

Patches bei Bedarf manuell installieren

Sie können Patches bei Bedarf manuell installieren, wenn Sie nicht auf den geplanten Installationszeitpunkt warten wollen.

Sie können die manuelle Patch-Installation über drei Anzeigen starten: **Patches**, **Schwachstellen** und **Alle Geräte**.

So können Sie einen Patch manuell installieren

Von Patches aus

1. Gehen Sie in der Cyber Protect-Konsole zum Bereich **Software-Verwaltung** –> **Patches**.
2. Akzeptieren Sie die Lizenzvereinbarungen derjenigen Patches, die Sie installieren wollen.
3. Wählen Sie im Assistenten **Patches installieren** diejenigen Patches aus, die Sie installieren wollen, und klicken Sie anschließend auf **Installieren**.
4. Wählen Sie die Maschinen aus, auf denen die Patches installiert werden sollen.
5. Bestimmen Sie die Neustart-Optionen.
   a. Legen Sie fest, ob die Maschine nach der Installation der Patches neu gestartet werden soll.

Option	Beschreibung
Nein	Die Maschinen werden nicht automatisch neu gestartet, nachdem die Patches installiert wurden.
Bei Bedarf	Die Maschinen werden nur dann neu gestartet, wenn dies für die Anwendung der Patches erforderlich ist.
Ja	Die Maschinen werden automatisch neu gestartet, nachdem die Patches installiert wurden. Sie können außerdem eine Verzögerung für den Neustart spezifizieren.

   b. [Optional] Wenn Sie den Neustart der Maschine verzögern wollen, während ein Backup der Maschine durchgeführt wird, aktivieren Sie die Option **Nicht neu starten, bevor das Backup abgeschlossen wurde**.
6. Klicken Sie auf **Patches installieren**.

Von Schwachstellen aus

1. Gehen Sie in der Cyber Protect-Konsole zum Bereich **Software-Verwaltung** –> **Schwachstellen**.
2. Führen Sie den Prozess zur Schwachstellenbehebung aus (wie im Abschnitt '"Gefundene Schwachstellen verwalten" (S. 1053)' beschrieben).

Von 'Alle Geräte' ausgehend

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte** –> **Alle Geräte**.
2. Wählen Sie die Maschine aus, auf die Patches installiert werden sollen.
3. Klicken Sie auf **Patchen**.
4. Wählen Sie die Patches aus, die Sie installieren wollen, und klicken Sie dann auf **Weiter**.
5. Bestimmen Sie die Neustart-Optionen.

a. Legen Sie fest, ob die Maschine nach der Installation der Patches neu gestartet werden soll.

Option	Beschreibung
Nein	Die Maschinen werden nicht automatisch neu gestartet, nachdem die Patches installiert wurden.
Bei Bedarf	Die Maschinen werden nur dann neu gestartet, wenn dies für die Anwendung der Patches erforderlich ist.
Ja	Die Maschinen werden automatisch neu gestartet, nachdem die Patches installiert wurden. Sie können außerdem eine Verzögerung für den Neustart spezifizieren.

b. [Optional] Wenn Sie den Neustart der Maschine verzögern wollen, während ein Backup der Maschine durchgeführt wird, aktivieren Sie die Option **Nicht neu starten, bevor das Backup abgeschlossen wurde**.

6. Klicken Sie auf **Patches installieren**.

Ihre Software- und Hardware-Inventarisierung verwalten

Software-Inventarisierung

Die Software-Inventarisierungsfunktion ist für Geräte verfügbar, auf denen das Advanced-Paket aktiviert wurde oder die über eine frühere (Legacy) Cyber Protect-Lizenz verfügen. Mit dieser Funktion können Sie alle Applikationen einsehen, die auf allen Windows- und macOS-Geräten installiert sind.

Zur Ermittlung der Software-Inventardaten können Sie automatische oder manuelle Scans auf den entsprechenden Geräten durchführen.

Mithilfe der Software-Inventardaten können Sie Folgendes tun:

- die Informationen über alle Applikationen, die auf den Geräten des Unternehmens installiert sind, durchsuchen und vergleichen
- ermitteln, ob eine Applikation aktualisiert werden muss
- ermitteln, ob eine nicht verwendete Applikation entfernt werden sollte
- sicherstellen, dass die Software-Version auf mehreren Geräten des Unternehmens identisch ist
- Änderungen beim Software-Status zwischen aufeinanderfolgenden Scans überwachen.

Den Software-Inventarisierungsscan aktivieren

Wenn für Geräte ein Inventarisierungsscan aktiviert ist, wird das System alle 12 Stunden automatisch die entsprechenden Software-Daten sammeln.

Die Funktionalität für Software-Inventarisierungsscans ist standardmäßig für alle Geräte aktiviert, die über die erforderliche Lizenz verfügen. Sie können die Einstellung jedoch bei Bedarf ändern.

Hinweis
Kunden-Mandanten können den Software-Inventarisierungsscan aktivieren oder deaktivieren. Abteilungs-Mandanten können die Einstellungen für den Software-Inventarisierungsscan zwar einsehen, aber diese nicht ändern.

So können Sie den Software-Inventarisierungsscan aktivieren

1. Gehen Sie in der Cyber Protect-Konsole zu **Einstellungen**.
2. Klicken Sie auf **Schutz**.
3. Klicken Sie auf **Inventarisierungsscan**.
4. Aktivieren Sie das Modul **Software-Inventarisierungsscan**, indem Sie auf den Schalter neben dem Namen des Moduls klicken.

So können Sie den Software-Inventarisierungsscan deaktivieren

1. Gehen Sie in der Cyber Protect-Konsole zu **Einstellungen**.
2. Klicken Sie auf **Schutz**.
3. Klicken Sie auf **Inventarisierungsscan**.
4. Deaktivieren Sie das Modul **Software-Inventarisierungsscan**, indem Sie auf den Schalter neben dem Namen des Moduls klicken.

Einen Software-Inventarisierungsscan manuell ausführen

Sie können einen Software-Inventarisierungsscan manuell über die Anzeige **Software-Inventarisierung** oder über die Registerkarte **Software** in der Anzeige **Inventarisierung** ausführen.

Voraussetzungen

- Das Gerät verwendet Windows oder macOS als Betriebssystem.
- Das Gerät verfügt über die erforderliche (Legacy) Cyber Protect-Lizenz oder hat das Advanced Management-Paket aktiviert.

So können Sie einen Software-Inventarisierungsscan über die Anzeige Software-Inventarisierung ausführen

1. Gehen Sie in der Cyber Protect-Konsole zum Bereich **Software-Verwaltung**.
2. Klicken Sie auf **Software-Inventarisierung**.
3. Wählen Sie im Listenfeld **Gruppieren nach:** den Eintrag **Geräte**.
4. Klicken Sie zuerst auf das Gerät, das Sie scannen wollen, und anschließend auf **Jetzt scannen**.

So können Sie einen Software-Inventarisierungsscan über die Registerkarte Software in der Anzeige Inventarisierung ausführen

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte**.
2. Klicken Sie zuerst auf das Gerät, das Sie scannen wollen, und anschließend auf **Inventarisierung**.
3. Klicken Sie in der Registerkarte **Software** auf den Befehl **Jetzt scannen**.

Das Software-Inventar durchsuchen

Sie können die Daten für alle Software-Applikationen einsehen und durchsuchen, die auf allen Geräten des Unternehmens vorhanden sind.

Voraussetzungen

- Die Geräte verwenden Windows oder macOS als Betriebssystem.
- Die Geräte verfügen über die erforderliche (Legacy) Cyber Protect-Lizenz oder haben das

Advanced Management-Paket aktiviert.

- Der Software-Inventarisierungsscan auf den Geräten wurde erfolgreich abgeschlossen.

So können Sie alle Software-Applikationen einsehen, die auf den Windows- und macOS-Geräten des Unternehmens verfügbar sind

1. Gehen Sie in der Cyber Protect-Konsole zum Bereich **Software-Verwaltung**.
2. Klicken Sie auf **Software-Inventarisierung**.
   Standardmäßig werden die Daten nach Geräten gruppiert. Die folgende Tabelle beschreibt die Daten, die in der Ansicht **Software-Inventarisierung** angezeigt werden.

Spalte	Beschreibung
Name	Name der Applikation.
Version	Version der Applikation.
Status	Status der Applikation. • **Neu**. • **Aktualisiert**. • **Entfernt**. • **Keine Änderung**.
Anbieter	Der Anbieter oder Hersteller der Applikation.
Installationsdatum	Datum und Zeitpunkt, als die Applikation installiert wurde.
Letzte Ausführung	Nur für macOS-Geräte. Datum und Zeitpunkt, als die Applikation zuletzt aktiv war.
Speicherort	Das Verzeichnis, in dem die Applikation installiert ist.
Benutzer	Der Anwender, der die Applikation installiert hat.
Systemtyp	Nur für Windows-Geräte. Der Bit-Typ der Applikation. • **X86** für 32-Bit-Applikationen. • **X64** für 64-Bit-Applikationen.

3. Wenn Sie die Daten nach Applikation gruppieren wollen, wählen Sie im Listenfeld **Gruppieren nach:** den Eintrag **Applikationen**.
4. Sie können die auf dem Bildschirm angezeigten Informationen einschränken, indem Sie einen einzelnen Filter oder eine Filterkombination verwenden.
   a. Klicken Sie auf **Filter**.
   b. Wählen Sie einen bestimmten Filter oder eine Kombination aus mehreren Filtern.
   Die folgende Tabelle beschreibt Filter in der Ansicht **Software-Inventarisierung**.

Filtern	Beschreibung
Gerätename	Gerätename. Es ist eine Mehrfachauswahl möglich.

Filtern	Beschreibung
	Verwenden Sie diesen Filter, wenn Sie die Software auf bestimmten Geräten miteinander vergleichen wollen.
Applikation	Applikationsname. Es ist eine Mehrfachauswahl möglich. Verwenden Sie diesen Filter, wenn Sie die Daten für eine bestimmte Applikation auf bestimmten oder allen Geräten vergleichen wollen.
Anbieter	Der Anbieter oder Hersteller der Applikation. Es ist eine Mehrfachauswahl möglich. Verwenden Sie diesen Filter, wenn Sie alle Applikationen eines bestimmten Anbieters auf bestimmten oder allen Geräten einsehen wollen.
Status	Applikationsstatus. Es ist eine Mehrfachauswahl möglich. Verwenden Sie diesen Filter, wenn Sie alle Applikationen mit dem ausgewählten Status auf bestimmten oder allen Geräten einsehen wollen.
Installationsdatum	Das Datum, als die Applikation installiert wurde. Verwenden Sie diesen Filter, wenn Sie alle Applikationen einsehen wollen, die an einem bestimmten Datum auf bestimmten oder allen Geräten installiert wurden.
Scan-Datum	Datum des Software-Inventarisierungsscans. Verwenden Sie diesen Filter, wenn Sie die Informationen über die Software auf bestimmten oder allen Geräten einsehen wollen, die an diesem Datum gescannt wurden.

c. Klicken Sie auf **Anwenden**.

5. Wenn Sie die komplette Software-Inventarliste durchblättern wollen, verwenden Sie die Paginierung im linken unteren Bildschirmbereich.

- Klicken Sie auf die Nummer derjenigen Seite, die Sie öffnen wollen.
- Wählen Sie im Listenfeld die Nummer derjenigen Seite aus, die Sie öffnen wollen.

Das Software-Inventar eines einzelnen Gerätes anzeigen

Sie können eine Liste aller Software-Applikationen einsehen, die auf einem bestimmten Gerät installiert sind, sowie ausführliche Informationen über die Applikationen (wie den Status, die Version, den Hersteller, das Installationsdatum, die letzte Ausführung und den Speicherort).

Voraussetzungen

- Das Gerät verwendet Windows oder macOS als Betriebssystem.
- Das Gerät verfügt über die erforderliche (Legacy) Cyber Protect-Lizenz oder hat das Advanced

Management-Paket aktiviert.

- Der Software-Inventarisierungsscan auf dem Gerät wurde erfolgreich abgeschlossen.

So können Sie sich das Software-Inventar eines einzelnen Gerätes über die Anzeige Software-Inventarisierung anzeigen lassen

1. Gehen Sie in der Cyber Protect-Konsole zum Bereich **Software-Verwaltung**.
2. Klicken Sie auf **Software-Inventarisierung**.
3. Wählen Sie im Listenfeld **Gruppieren nach:** den Eintrag **Geräte**.
4. Suchen Sie das Gerät, welches Sie untersuchen wollen, mit einer der nachfolgenden Methoden:
   - Suchen Sie das Gerät mithilfe eines **Filters**:
     a. Klicken Sie auf **Filter**.
     b. Wählen Sie im Feld **Gerätename** den Namen des Gerätes aus, welches Sie einsehen wollen.
     c. Klicken Sie auf **Anwenden**.
   - Suchen Sie das Gerät mithilfe der dynamischen **Suche**:
     a. Klicken Sie auf **Suche**.
     b. Geben Sie den Gerätenamen vollständig oder teilweise ein.

So können Sie sich das Software-Inventar eines einzelnen Gerätes über die Anzeige Geräte anzeigen lassen

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte**.
2. Klicken Sie zuerst auf das Gerät, das Sie einsehen wollen, und anschließend auf **Inventarisierung**.
3. Klicken Sie auf die Registerkarte **Software**.

Hardware-Inventarisierung

Die Hardware-Inventarisierungsfunktion ermöglicht es Ihnen, alle Hardware-Komponenten einzusehen, die auf folgenden Geräten/Maschinen verfügbar sind:

- physische Windows- und macOS-Geräte mit einer Lizenz, die die Hardware-Inventarisierungsfunktion unterstützt.
- virtuelle Windows- und macOS-Maschinen, die auf folgenden Virtualisierungsplattformen laufen: VMware, Hyper-V, Citrix, Parallels, Oracle, Nutanix, Virtuozzo und Virtuozzo Hybrid Infrastructure. Weitere Informationen zu den unterstützten Versionen der Virtualisierungsplattformen finden Sie unter '"Unterstützte Virtualisierungsplattformen" (S. 33)'.

Hinweis
Die Hardware-Inventarisierungsfunktion für virtuelle Maschinen wird in den älteren Cyber Protect-Editionen (Legacy-Editionen) nicht unterstützt.

Die Hardware-Inventarisierungsfunktion wird nur für solche Geräte unterstützt, auf denen ein Protection Agent installiert ist.

Zur Ermittlung der Hardware-Inventardaten können Sie automatische oder manuelle Scans auf den entsprechenden Geräten durchführen.

Mithilfe der Hardware-Inventardaten können Sie Folgendes tun:

- alle Hardware-Ressourcen des jeweiligen Unternehmens ermitteln
- das Hardware-Inventar auf allen Geräten in Ihrem Unternehmen durchsuchen
- die Hardware-Komponenten mehrerer Unternehmensgeräte miteinander vergleichen
- ausführliche Informationen über eine Hardware-Komponente einsehen.

Den Hardware-Inventarisierungsscan aktivieren

Wenn die Hardware-Inventarisierungsfunktion für physische Geräte und virtuelle Maschinen aktiviert ist, ermittelt das System automatisch alle 12 Stunden die Hardware-Daten dieser Geräte/Maschinen.

Die Funktionalität für Hardware-Inventarisierungsscans ist standardmäßig aktiviert, aber Sie können diese Einstellung bei Bedarf auch jederzeit ändern.

Hinweis
Kunden-Mandanten können den Hardware-Inventarisierungsscan aktivieren oder deaktivieren. Abteilungs-Mandanten können die Einstellungen für den Hardware-Inventarisierungsscan zwar einsehen, aber diese nicht ändern.

So können Sie den Hardware-Inventarisierungsscan aktivieren

1. Gehen Sie in der Cyber Protect-Konsole zu **Einstellungen**.
2. Klicken Sie auf **Schutz**.
3. Klicken Sie auf **Inventarisierungsscan**.
4. Aktivieren Sie das Modul **Hardware-Inventarisierungsscan**, indem Sie auf den Schalter neben dem Namen des Moduls klicken.

So können Sie den Hardware-Inventarisierungsscan deaktivieren

1. Gehen Sie in der Cyber Protect-Konsole zu **Einstellungen**.
2. Klicken Sie auf **Schutz**.
3. Klicken Sie auf **Inventarisierungsscan**.
4. Deaktivieren Sie das Modul **Hardware-Inventarisierungsscan**, indem Sie auf den Schalter neben dem Namen des Moduls klicken.

Einen Hardware-Inventarisierungsscan manuell ausführen

Sie können einen Hardware-Inventarisierungsscan für ein einzelnes Gerät manuell ausführen und sich dann die aktuellen Daten über die Hardware-Komponenten des Gerätes anzeigen lassen.

Hinweis
Die Hardware-Inventarisierungsfunktion für virtuelle Maschinen wird nur unterstützt, wenn Datum und Uhrzeit der virtuellen Maschine mit dem aktuellen Datum und der aktuellen Uhrzeit in UTC übereinstimmen. Wenn Sie sicherstellen wollen, dass die virtuelle Maschine die korrekten Zeiteinstellungen verwendet, deaktivieren Sie die Option **Zeitsynchronisierung** der virtuellen Maschine, stellen Sie das aktuelle Datum, die Uhrzeit und die Zeitzone ein und starten Sie dann die Dienste **Acronis Agent Core Service** und **Acronis Managed Machine Service** neu.

Voraussetzungen

- (Für alle Geräte) Die Geräte verwenden ein Windows- oder macOS-Betriebssystem.
- (Für alle Geräte) Die Geräte haben eine Lizenz, die die Hardware-Inventarisierungsfunktion unterstützt. Beachten Sie, dass die Hardware-Inventarisierungsfunktion für virtuelle Maschinen nicht in den älteren Cyber Protect-Editionen (Legacy-Editionen) unterstützt wird.
- (Für alle Geräte) Auf dem Gerät ist ein Protection Agent installiert.
- (Für virtuelle Maschinen) Die Maschine läuft auf einer der unterstützten Virtualisierungsplattformen. Weitere Informationen finden Sie im Abschnitt '"Hardware-Inventarisierung" (S. 1076)'.

So können Sie einen Hardware-Inventarisierungsscan für ein einzelnes Gerät ausführen

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte**.
2. Klicken Sie auf das Gerät, das Sie scannen wollen, und anschließend auf **Inventarisierung**.
3. Klicken Sie in der Registerkarte **Hardware** auf den Befehl **Jetzt scannen**.

Das Hardware-Inventar durchsuchen

Sie können die Daten für alle Hardware-Komponenten einsehen und durchsuchen, die auf allen Geräten des Unternehmens vorhanden sind.

Voraussetzungen

- (Für alle Geräte) Die Geräte verwenden Windows oder macOS als Betriebssystem.
- (Für alle Geräte) Die Geräte haben eine Lizenz, die die Hardware-Inventarisierungsfunktion unterstützt. Beachten Sie, dass die Hardware-Inventarisierungsfunktion für virtuelle Maschinen nicht in den älteren Cyber Protect-Editionen (Legacy-Editionen) unterstützt wird.
- (Für alle Geräte) Auf dem Gerät ist ein Protection Agent installiert.

- (Für alle Geräte) Der Hardware-Inventarisierungsscan auf den Geräten wurde erfolgreich abgeschlossen.
- (Für virtuelle Maschinen) Die Maschine läuft auf einer der unterstützten Virtualisierungsplattformen. Weitere Informationen finden Sie im Abschnitt '"Hardware-Inventarisierung" (S. 1076)'.

So können Sie alle Hardware-Komponenten einsehen, die auf den Windows- und macOS-Geräten des Unternehmens verfügbar sind

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte**.
2. Wählen Sie im Listenfeld **Ansicht:** den Eintrag **Hardware**.

Hinweis
Diese Ansicht ist eine Gruppe von Spalten, mit der bestimmt wird, welche Daten auf dem Bildschirm angezeigt werden. Die vordefinierten Ansichten heißen **Standard** und **Hardware**. Sie können benutzerdefinierte Ansichten erstellen und speichern, die andere Spaltengruppen enthalten und besser für Ihre jeweiligen Bedürfnisse geeignet sind.

Die folgende Tabelle beschreibt die Daten, die in der Ansicht **Hardware** angezeigt werden.

Spalte	Beschreibung
Name	Gerätename.
Hardware-Scan-Status	Status des Hardware-Scans. • **Abgeschlossen**. • **Nicht gestartet**. • **Nicht unterstützt**. Dieser Status wird bei Workloads angezeigt, für die keine Hardware-Inventarisierungsfunktionalität verfügbar ist – also bei virtuellen Maschinen, Mobilgeräten und Linux-Geräten. • **Agent aktualisieren**. Dies wird angezeigt, wenn auf dem Gerät eine veraltete Version des Agenten installiert ist. Wenn Sie auf diese Aktion klicken, werden Sie zur Seite 'Einstellungen' –> 'Agenten' weitergeleitet, wo der Administrator das Agenten-Update durchführen kann. • **Quota upgraden**. Wenn Sie darauf klicken, wird ein Dialog geöffnet, in dem der Administrator die aktuelle Lizenz auf eine der anderen für den Mandanten verfügbare Lizenz umstellen kann.
Prozessor	Die Modelle aller Prozessoren des Gerätes.

Spalte	Beschreibung
Prozessorkerne	Die Anzahl der Kerne aller Prozessoren des Gerätes.
Laufwerksspeicher	Der verwendete Storage (belegte Speicherplatz) und der Storage insgesamt von allen Laufwerken des Gerätes.
Arbeitsspeicher	Die gesamte Arbeitsspeichermenge (RAM) des Gerätes.
Scan-Datum	Datum und Zeitpunkt des letzten Hardware-Inventarisierungsscans.
Mainboard	Das Mainboard des Gerätes.
Mainboard-Seriennummer	Die Seriennummer des Mainboards.
BIOS-Version	Die Version des BIOS auf dem System.
Organisation	Die Organisation bzw. das Unternehmen, zu dem das Gerät gehört.
Besitzer	Der Besitzer des Gerätes.
Domain	Die Domain des Gerätes.
Betriebssystem	Das Betriebssystem des Gerätes.
Betriebssystembuild	Die genaue Version des Betriebssystems des Gerätes.

3. Wenn Sie der Tabelle weitere Spalten hinzufügen wollen, klicken Sie auf das Symbol für die Spaltenoptionen und wählen Sie diejenigen Spalten aus, die in der Tabelle angezeigt werden sollen.
4. Sie können die auf dem Bildschirm angezeigten Informationen einschränken, indem Sie einen oder mehrere Filter verwenden.
   a. Klicken Sie auf **Suche**.
   b. Klicken Sie auf den Pfeil und anschließend auf **Hardware**.
   c. Wählen Sie einen bestimmten Filter oder eine Kombination aus mehreren Filtern.
   Die nachfolgende Tabelle beschreibt die verfügbaren **Hardware**-Filter.

Filtern	Beschreibung
Prozessormodell	Es ist eine Mehrfachauswahl möglich. Verwenden Sie diesen Filter, wenn Sie die Hardware-Daten solcher Geräte angezeigt bekommen wollen, die über das spezifizierte Prozessormodell verfügen.

Filtern	Beschreibung
Prozessorkerne	Verwenden Sie diesen Filter, wenn Sie die Hardware-Daten solcher Geräte angezeigt bekommen wollen, die über die spezifizierte Anzahl von Prozessoren verfügen.
Gesamtgröße Laufwerksspeicher	Verwenden Sie diesen Filter, wenn Sie die Hardware-Daten solcher Geräte angezeigt bekommen wollen, die über die spezifizierte Menge an Laufwerksspeicherplatz verfügen.
Arbeitsspeicherkapazität	Verwenden Sie diesen Filter, wenn Sie die Hardware-Daten solcher Geräte angezeigt bekommen wollen, die über die spezifizierte Menge von Arbeitsspeicher (RAM) verfügen.

d. Klicken Sie auf **Anwenden**.

5. Klicken Sie auf einen Spaltennamen, wenn Sie die Daten in aufsteigender Reihenfolge sortieren wollen.

Die Hardware eines einzelnen Gerätes anzeigen

Sie können ausführliche Informationen über das Mainboard, den Prozessor, den Arbeitsspeicher, die Grafikkarte(n), die Storage-Laufwerke, das Netzwerk sowie das System eines bestimmten Gerätes einsehen.

Voraussetzungen

- (Für alle Geräte) Das Gerät verwendet Windows oder macOS als Betriebssystem.
- (Für alle Geräte) Die Geräte haben eine Lizenz, die die Hardware-Inventarisierungsfunktion unterstützt. Beachten Sie, dass die Hardware-Inventarisierungsfunktion für virtuelle Maschinen nicht in den älteren Cyber Protect-Editionen (Legacy-Editionen) unterstützt wird.
- (Für alle Geräte) Auf dem Gerät ist ein Protection Agent installiert.
- (Für alle Geräte) Der Hardware-Inventarisierungsscan auf dem Gerät wurde erfolgreich abgeschlossen.
- (Für virtuelle Maschinen) Die Maschine läuft auf einer der unterstützten Virtualisierungsplattformen. Weitere Informationen finden Sie im Abschnitt '"Hardware-Inventarisierung" (S. 1076)'.

So können Sie sich ausführliche Informationen über die Hardware eines bestimmten Gerätes anzeigen lassen

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte** –> **Alle Geräte**.
2. Wählen Sie im Listenfeld **Ansicht:** den Eintrag **Hardware**.
3. Suchen Sie das Gerät, welches Sie untersuchen wollen, mit einer der unten beschriebenen Methoden.

- Suchen Sie das Gerät mithilfe eines **Filters**:
  a. Klicken Sie auf **Filter**.
  b. Wählen Sie nur einen oder eine Kombination von Filterparametern, um das Gerät zu finden.
  c. Klicken Sie auf **Anwenden**.
- Suchen Sie das Gerät mithilfe der **Suche**:
  a. Klicken Sie auf **Suche**.
  b. Geben Sie den Gerätenamen vollständig oder teilweise ein und aktivieren Sie dann die **Eingabetaste**.

4. Klicken Sie zuerst auf die Zeile, in der das Gerät aufgeführt ist, und anschließend auf **Inventarisierung**.
5. Klicken Sie auf die Registerkarte **Hardware**.
   Folgende Hardware-Daten sind verfügbar:

Hardware-Komponente	Angezeigte Information
Mainboard	Name, Hersteller, Modell und Seriennummer vom Mainboard des Gerätes.
Prozessoren	Hersteller, Modell, maximale Taktrate und Anzahl der Kerne eines jeden Prozessors des jeweiligen Gerätes.
Arbeitsspeicher	Name, Hersteller, Modell und Seriennummer vom Mainboard des Gerätes.
Grafikkarten	Hersteller und Modell der GPUs des Gerätes.
Storage-Laufwerke	Modell, Datenträgertyp, verfügbarer Speicherplatz und Größe der Storage-Laufwerke des Gerätes.
Netzwerk	MAC-Adresse, IP-Adresse und Art des Netzwerkadapters des Gerätes.
System	Produkt-ID, ursprüngliches Installationsdatum, Systemstartzeit, Systemhersteller, Systemmodell, BIOS-Version, Boot-Gerät, Systemgebietsschema und Zeitzone des Systems.

Mit einem Workload für Remote-Desktop- oder Remote-Unterstützungszwecke verbinden

Die Remote-Desktop- und Remote-Unterstützungsfunktionalität ist eine praktische Möglichkeit, um sich aus der Ferne mit den Workloads in Ihrem Unternehmen zu verbinden, damit Sie diese fernsteuern können oder dem Anwender auf diesem System Unterstützung bieten können. Seit Dezember 2022 unterstützt diese Funktionalität die Fernwartungsprotokolle NEAR, RDP und Apple Bildschirmfreigabe. Weitere Informationen finden Sie im Abschnitt '"Remote-Verbindungsprotokolle" (S. 1089)'.

Sie können mit der Remote-Desktop-Funktionalität folgende Aufgaben durchführen:

- Sich über das NEAR-Protokoll im Nur-Anzeigen-Modus mit Windows-, macOS- oder Linux-basierten Remote-Workloads verbinden.
- Sich über das RDP-Protokoll mit Windows-basierten Remote-Workloads verbinden.
- Sich über das Apple Bildschirmfreigabe-Protokoll im Nur-Anzeigen- oder Vorhangsmodus mit macOS-basierten Remote-Workloads verbinden.
- Sich über Cloud-Remote-Verbindungen mit verwalteten Workloads verbinden und diese fernsteuern.
- Sich über direkte Remote-Verbindungen mit unverwalteten Workloads verbinden und diese fernsteuern.
- Sich über Acronis Quick Assist mit Windows-basierten unverwalteten Remote-Workloads verbinden.
- Bei Verbindungen mit Remote-Workloads verschiedene Authentifizierungsmethoden verwenden: mit Remote-Workload-Anmeldedaten; mit einer Anfrage, ob der Desktop beobachtet oder gesteuert werden darf, oder mit einem Zugriffscode (für Quick Assist).
- Mehrere Bildschirme gleichzeitig in der Mehrfachansicht beobachten.
- Remote-Sitzungen aufzuzeichnen (bei Verbindung über NEAR).
- Den Sitzungsverlaufsbericht einzusehen.

Weitere Informationen zu den Funktionen, die Bestandteil der Standard Protection- und Advanced Management-Pakete sind, finden Sie im Abschnitt '"Unterstützte Remote-Desktop- und Remote-Unterstützungsfunktionen" (S. 1085)'.

Sie können mit der Remote-Unterstützungsfunktionalität folgende Aufgaben durchführen:

- Sich über das NEAR-Protokoll im Steuermodus mit Windows-, macOS- oder Linux-basierten Remote-Workloads verbinden.
- Sich über das Apple Bildschirmfreigabe-Protokoll im Steuermodus mit macOS-basierten Remote-Workloads verbinden.
- Remote-Unterstützung für Workloads über Cloud-Remote-Verbindungen bereitstellen.
- Dateien zwischen lokalen und Remote-Workloads übertragen.

- Grundlegende Verwaltungsaktionen auf dem Remote-Workload durchführen: neu starten, herunterfahren, in den Ruhezustand versetzen, den Papierkorb leeren oder den Remote-Benutzer abmelden.
- Den Remote-Workloads überwachen, indem regelmäßige Screenshots von dessen Desktop erstellt werden.

Weitere Informationen zu den Funktionen, die Bestandteil der Standard Protection- und Advanced Management-Pakete sind, finden Sie im Abschnitt '"Unterstützte Remote-Desktop- und Remote-Unterstützungsfunktionen" (S. 1085)'.

Wichtig
Wenn Sie die komplette Remote-Desktop- und Remote-Unterstützungsfunktionalität für verwaltete Workloads aktivieren wollen, müssen Sie einen Remote-Verwaltungsplan konfigurieren und diesen auf die Workloads anwenden. Sie können zwar nur einen Remote-Verwaltungsplan auf einen Workload anwenden, aber je nach Bedarf unterschiedliche Remote-Verwaltungspläne konfigurieren und diese auf unterschiedliche Workloads anwenden.

So können Sie beispielsweise einen Remote-Verwaltungsplan erstellen, in dem nur das RDP-Protokoll aktiviert ist, und diesen dann auf bestimmte Workloads anwenden. Auf diese Weise können Sie eine Remote-Verbindung zu diesen Workloads herstellen, ohne die Advanced Management-Lizenz pro Workload aktivieren und ohne zusätzliche Gebühren zahlen zu müssen.

Alternativ können Sie einen anderen Remote-Verwaltungsplan erstellen, in dem die NEAR- und Apple Bildschirmfreigabe-Protokolle aktiviert sind. In diesem Fall wird die Advanced Management-Lizenz pro Workload aktiviert und eine Gebühr für jeden Workload berechnet, auf den dieser Remote-Verwaltungsplan angewendet wird.

Weitere Informationen über Remote-Verwaltungspläne und wie Sie diesen arbeiten können, finden Sie im Abschnitt '"Remote-Verwaltungspläne" (S. 1092)'.

Hinweis
Die Remote-Desktop- und Remote-Unterstützungsfunktionalität erfordert:

- eine einmalige Installation des Connect Clients auf dem verwaltenden Workload (Host). Wenn Sie zum ersten Mal versuchen, eine Remote-Aktion (Fernsteuerung oder Remote-Unterstützung) auf einem Ziel-Workload durchzuführen, wird Ihnen das System vorschlagen, den Client herunterzuladen. Sie können den Connect Client alternativ auch über das **Downloads**-Fenster in der Schutz-Konsole herunterladen. Weitere Informationen zu den Einstellungen, die Sie konfigurieren können, finden Sie im Abschnitt '"Die Connect Client-Einstellungen konfigurieren" (S. 1127)'.
- Installation des Connect Agenten auf den verwalteten Workloads. Der Connect Agent ist ein Modul, das zum Schutz Agenten gehört – und zwar ab Version 15.0.31266.
- für macOS-basierte Remote-Workloads müssen dem Connect Agenten die erforderlichen Systemberechtigungen erteilt werden. Weitere Informationen finden Sie im Abschnitt '"Protection Agenten in macOS installieren" (S. 87)'.
- Ausführung der Acronis Quick Assist-Applikation auf den nicht verwalteten Workloads. Sie können den Installer für Acronis Quick Assist von dieser Website herunterladen.

Weitere Informationen darüber, welche Plattformen von den einzelnen Remote-Desktop- und Remote-Unterstützungskomponenten unterstützt werden, finden Sie im Abschnitt '"Unterstützte Plattformen" (S. 1088)'.

Unterstützte Remote-Desktop- und Remote-Unterstützungsfunktionen

Die nachfolgende Tabelle enthält weitere Informationen über die Änderungen, die im Dezember 2022 bei den unterstützten Funktionen der Remote-Desktop- und Remote-Unterstützungsfunktionalität eingeführt wurden.

Funktion	Standard Protection vor Dezember 2022	Advanced Management vor Dezember 2022	Standard Protection nach Dezember 2022	Advanced Management nach Dezember 2022
Remote-Unterstützung über RDP für Windows	Ja	Nein	Nein	Nein
Eine Remote-Verbindung für Benutzer freigeben	Nein	Ja	Nein	Nein
Remote-Verbindungen				
Remote-Aktionen	Nein	Nein	Ja	Ja

Funktion	Standard Protection vor Dezember 2022	Advanced Management vor Dezember 2022	Standard Protection nach Dezember 2022	Advanced Management nach Dezember 2022
Eine Sitzung auswählen, um sich mit Windows/macOS/Linux zu verbinden	Nein	Nein	Nein	Ja
Direkte Verbindung über RDP und Apple Bildschirmfreigabe	Nein	Nein	Nein	Ja
Multi-Fenster-Kontrolle	Nein	Nein	Nein	Ja
Verbindungsmodi: Steuerung/Nur anzeigen/Vorhang	Nein	Nein	Nein	Ja
Unterstützung von gemeinsamen Anmeldedaten für Remote-Verbindungen	Nein	Nein	Ja	Ja
Gleichzeitige Verbindungen pro Techniker				
über RDP	Ja	Ja	Ja	Ja
über NEAR	Nein	Nein	Nein	Ja
Dateiübertragung und -freigabe				
von Windows zu Windows/macOS/Linux	Nein	Nein	Nein	Ja
von macOS zu Windows/macOS/Linux	Nein	Nein	Nein	Ja
von Linux zu Windows/macOS/Linux	Nein	Nein	Nein	Ja
Über die Quick Assist-Applikation verbinden				
von Windows zu Windows/macOS/Linux	Nein	Nein	Nein	Ja
von macOS zu Windows/macOS/Linux	Nein	Nein	Nein	Ja
von Linux zu	Nein	Nein	Nein	Ja

Funktion	Standard Protection vor Dezember 2022	Advanced Management vor Dezember 2022	Standard Protection nach Dezember 2022	Advanced Management nach Dezember 2022
Windows/macOS/Linux				
Remote-Verbindungen über Protokolle				
Remote-Verbindung über NEAR				
von Windows zu Windows/macOS/Linux	Nein	Nein	Nein	Ja
von macOS zu Windows/macOS/Linux	Nein	Nein	Nein	Ja
von Linux zu Windows/macOS/Linux	Nein	Nein	Nein	Ja
Remote-Verbindung über RDP (Desktop-Client)				
von Windows zu Windows	Ja	Ja	Ja	Ja
von macOS zu Windows	Ja	Ja	Ja	Ja
von Linux zu Windows	Nein	Nein	Ja	Ja
Remote-Verbindung über RDP (Webclient)				
von Windows zu Windows	Ja	Ja	Ja	Ja
von macOS zu Windows	Ja	Ja	Ja	Ja
von Linux zu Windows	Nein	Nein	Ja	Ja
Remote-Verbindung über Apple Bildschirmfreigabe				
von Windows/macOS/Linux zu macOS	Nein	Nein	Nein	Ja
Sitzungsverwaltung				
Sitzungsaufzeichnung	Nein	Nein	Nein	Ja
Berichts- und Überwachungsfunktionalität				
Sitzungsverlauf und Suchfunktion	Nein	Nein	Nein	Ja
Screenshot-Übertragung	Nein	Nein	Nein	Ja

Unterstützte Plattformen

In der nachfolgenden Tabelle sind die Betriebssysteme aufgeführt, die von den einzelnen Komponenten der Remote-Desktop- und Remote-Unterstützungsfunktionalität unterstützt werden.

Remote-Desktop-Komponente	Unterstützte Plattformen
Connect Client	• Windows 7 oder höher • macOS 10.13 oder höher • Linux: openSUSE 8 Debian 9, 10 Ubuntu 18.0-20.10 Red Hat Enterprise Linux 8 CentOS 8 Fedora 31-33 SUSE Linux Enterprise Server 15 SP2 Linux Mint 20 Manjaro 20
Connect Agent	• Windows 7 oder höher • Windows Server 2008 R2 oder höher • macOS 10.13 oder höher • Linux: Red Hat Enterprise Linux 8, 8.1 Fedora 30 Ubuntu 18.4 LTS (Bionic Beaver) -19.04 (Disco Dingo) Debian 9, 10 CentOS 8 openSUSE 15.1
Acronis Quick Assist	• Windows 7 oder höher • Windows Server 2008 R2 oder höher • macOS 10.13 oder höher • Linux: Red Hat Enterprise Linux 8, 8.1 Fedora 30 Ubuntu 18.4 LTS (Bionic Beaver) -19.04 (Disco Dingo) Debian 9, 10 CentOS 8 openSUSE 15.1

Remote-Verbindungsprotokolle

Die Remote-Desktop-Funktionalität verwendet folgende Protokolle für Remote-Verbindungen.

NEAR

NEAR ist ein von Acronis entwickeltes, hochsicheres Protokoll, das folgende Eigenschaften aufweist:

- ### H.264

  NEAR verfügt über drei Qualitätsmodi: **Glatt**, **Ausbalanciert** und **Scharf**. Im Modus **Glatt** verwendet NEAR unter macOS und Windows eine Hardware-H.264-Encodierung, um das Desktop-Bild zu verarbeiten. Wenn kein Hardware-Encoder verfügbar ist, wird auf einen Software-Encoder umgeschaltet. Die Bildqualität ist derzeit auf die Full HD-Auflösung (1920x1080) beschränkt.

- ### Adaptiver Codec

  Bei den Qualitätsmodi **Ausbalanciert** und **Scharf** verwendet NEAR einen adaptiven Codec, der (im Vergleich zum Modus 'Video') die volle Bildqualität in 32 Bit bietet.

  Im Modus **Ausbalanciert** wird die Bildqualität automatisch an die aktuellen Netzwerkbedingungen angepasst und die aktuelle Framerate beibehalten.

  Im Modus **Scharf** wird die beste Anzeigequalität erreicht. Wenn Ihr Netzwerk, Ihr Prozessor oder Ihre Grafikkarte jedoch überlastet sind, kann die Bildwiederholrate reduziert werden.

  Der adaptive Codec verwendet OpenCL unter Windows und macOS, sofern diese Funktion in den jeweiligen Grafiktreibern verfügbar ist.

- ### Sound-Übertragung

  Das NEAR-Protokoll kann die Sound-Ausgabe des Remote-Computers aufzeichnen und an den Host weiterleiten. Weitere Informationen darüber, wie Sie die Remote-Sound-Umleitung unter Windows, macOS und Linux aktivieren können, finden Sie im Abschnitt '"Remote-Sound-Umleitung" (S. 1090)'.

- ### Verschiedene Anmeldeoptionen

  Sie können die folgenden Methoden verwenden, um sich auf dem Remote-Workload anzumelden.

  Zugriffscode: der Benutzer, der auf dem Remote-Workload angemeldet ist, führt Quick Assist aus und teilt Ihnen den Zugriffscode mit. Bei dieser Methode verbinden Sie sich immer mit der Sitzung des aktuell angemeldeten Benutzers.

  Workload-Anmeldedaten: melden Sie sich auf dem Remote-Workload mit Administrator-Anmeldedaten an, die im Workload registriert sind.

Berechtigung zum Beobachten oder Steuern anfordern: der Benutzer, der auf dem Remote-Workload angemeldet ist, wird gefragt, ob er die Verbindung erlauben oder ablehnen will.

- Sicherheit

  Ihre Daten werden bei NEAR immer in beide Richtungen per AES-Verschlüsselung geschützt.

RDP

Das RDP (Remote Desktop Protocol) ist ein von Microsoft entwickeltes proprietäres Protokoll, mit dem Verbindungen zu entfernten Windows-Computern über ein Netzwerk hergestellt werden können.

Apple Bildschirmfreigabe

Die Apple Bildschirmfreigabe-Funktionalität entspricht einem von Apple angepasstem VNC-Client, der Bestandteil von macOS Version 10.5 und höher ist.

Remote-Sound-Umleitung

Der Connect Client unterstützt das Streaming von Audiodaten über das NEAR-Verbindungsprotokoll. Weitere Informationen über NEAR finden Sie im Abschnitt '"Remote-Verbindungsprotokolle" (S. 1089)'.

Die Sound-Ausgabe von einem Windows-basierten Remote-Workload umleiten

Bei Windows-Workloads sollte der Remote-Sound automatisch übertragen werden. Stellen Sie sicher, dass an den Remote-Workload entsprechende Sound-Ausgabegeräte (wie Lautsprecher oder Kopfhörer) angeschlossen sind.

Die Sound-Ausgabe von einem macOS-basierten Remote-Workload umleiten

Wenn Sie die Sound-Umleitung von einem macOS-Workload aktivieren wollen, müssen Sie sicherstellen, dass folgende Voraussetzungen erfüllt sind:

- Auf dem Workload ist der Schutz Agent installiert.
- Auf dem Workload ist ein Sound Capture-Treiber installiert.
- Der Workload verwendet das NEAR-Protokoll für Remote-Verbindungen.

Hinweis
Für macOS 10.15 Catalina muss dem Connect Agenten die Berechtigung 'Mikrofon' gewährt werden. Weitere Informationen darüber, wie Sie dem Connect Agenten die Berechtigung 'Mikrofon' gewähren können, finden Sie im Abschnitt '"Dem Connect Agenten die erforderlichen Systemberechtigungen gewähren" (S. 88)'.

Der Agent funktioniert mit folgenden Sound Capture-Treibern: Soundflower oder Blackhole.

Der Installationsprozess für die neuesten Versionen wird auf der Wiki-Seite zu Blackhole beschrieben: https://github.com/ExistentialAudio/BlackHole/wiki/Installation.

Hinweis
Der Connect Client unterstützt derzeit nur die 2-Kanal-Version von Blackhole.

Wenn Homebrew auf dem Workload installiert ist, können Sie Blackhole außerdem mit folgendem Befehl installieren:

```
brew install --cask blackhole-2ch
```

Hinweis
Während die Sound-Ausgabe eines macOS-basierten Remote-Workloads umgeleitet wird, wird der Benutzer, der auf dem Remote-Workload angemeldet ist, keinen Ton mehr hören.

Die Sound-Ausgabe von einem Linux-basierten Remote-Workload umleiten

Die Remote-Sound-Umleitung sollte bei den meisten Linux-Distributionen automatisch funktionieren. Wenn die Remote-Sound-Umleitung nicht direkt mit der Standardeinstellung funktioniert, sollten Sie den PulseAudio-Treiber installieren, indem Sie folgenden Befehl ausführen:

```
sudo apt-get install pulseaudio
```

Verbindungen zu Remote-Workloads für Remote-Desktop- oder Remote-Unterstützungszwecke

Die Remote-Desktop- oder Remote-Unterstützungsfunktionalität bietet zahlreiche Möglichkeiten, um direkte Remote- oder Cloud-Verbindungen zu Ihren Workloads herzustellen.

Direkte Verbindungen werden per TCP/IP im lokalen Netzwerk (LAN) zwischen dem Connect Client und einem Remote-Workload hergestellt, auf dem kein Agent installiert ist. Sie benötigen keinen Internet-Zugriff.

Cloud-Verbindungen werden zwischen dem Connect Client und dem Agenten oder Quick Assist auf dem Workload über die Acronis Cloud hergestellt.

In der nachfolgenden Tabelle finden Sie weitere Informationen zu den Cloud-Verbindungsoptionen.

Cloud-Verbindung	Cloud-Verbindungsoption	Ansichtsmodus	Unterstützte Remote-Aktion	Verfügbar für
über NEAR	von Connect Client zu Connect Agent von Connect Client zu Quick Assist	Steuern Nur anzeigen	Remote-Desktop Remote-Unterstützung	verwaltete Workloads
über RDP	von Connect Client zu Connect Agent vom Webclient zum Connect Agenten	Steuern	Remote-Desktop	verwaltete Workloads
über Apple Bildschirmfreigabe	von Connect Client zu Connect Agent	Steuern Nur anzeigen Vorhang	Remote-Desktop Remote-Unterstützung	verwaltete Workloads

In der nachfolgenden Tabelle finden Sie weitere Informationen zu den direkten Verbindungsoptionen.

Direkte Verbindung	Direktverbindungsoption	Unterstützte Remote-Aktion	Verfügbar für
über RDP	vom Connect Client zum RDP-Server	Remote-Desktop	unverwaltete Workloads
über Apple Bildschirmfreigabe	vom Connect Client zum Apple Bildschirmfreigabe-Server	Remote-Desktop Remote-Unterstützung	unverwaltete Workloads

Remote-Verwaltungspläne

Remote-Verwaltungspläne sind Pläne, die Sie auf den Schutz Agenten anwenden, um die Remote-Desktop- und Remote-Unterstützungsfunktionalität auf Ihren verwalteten Workloads zu aktivieren und zu konfigurieren.

Wenn kein Remote-Verwaltungsplan auf einen Workload angewendet wird, ist die Remote-Desktop- und Remote-Unterstützungsfunktionalität auf reine Remote-Aktionen (neu starten, herunterfahren, in den Energiesparmodus versetzen, den Papierkorb leeren oder den Remote-Benutzer abmelden) beschränkt.

Hinweis
Die Verfügbarkeit der Einstellungen, die Sie in dem jeweiligen Remote-Verwaltungsplan konfigurieren können, hängt von dem Service-Paket ab, das auf den Mandanten angewendet wurde. Wenn Sie auf alle Einstellungen zugreifen wollen, müssen Sie das Advanced Management-Paket aktivieren. Weitere Informationen zu den Funktionen, die Bestandteil der Standard Protection- und Advanced Management-Pakete sind, finden Sie im Abschnitt '"Unterstützte Remote-Desktop- und Remote-Unterstützungsfunktionen" (S. 1085)'.

Einen Remote-Verwaltungsplan erstellen

Sie können einen Remote-Verwaltungsplan erstellen und diesen dann einem Workload zuweisen, um die Remote-Desktop- und Remote-Unterstützungsfunktionalität auf dem verwalteten Workload konfigurieren zu können.

Hinweis
Welche Einstellungen des Remote-Verwaltungsplans verfügbar sind, hängt von der Service-Quota ab, die dem Mandanten zugewiesen wurde. Wenn Sie die Standardfunktionalität verwenden, können Sie nur Verbindungen über RDP konfigurieren.

Voraussetzungen

Für Ihr Benutzerkonto ist die Zwei-Faktor-Authentifizierung aktiviert.

So können Sie einen Remote-Verwaltungsplan erstellen

Aus Remote-Verwaltungsplänen

1. Gehen Sie in der Cyber Protect-Konsole zum Bereich **Verwaltung** –> **Remote-Verwaltungspläne**.
2. Erstellen Sie einen Remote-Verwaltungsplan, indem Sie eine der beiden Optionen verwenden.
   - Wenn es in der Liste keine Remote-Verwaltungspläne gibt, klicken Sie auf **Erstellen**.
   - Wenn es in der Liste noch keine Remote-Verwaltungspläne gibt, klicken Sie auf **Plan erstellen**.
3. [Optional] Wenn Sie den Standardnamen für den Plan ändern wollen, müssen Sie auf das Stiftsymbol klicken, den gewünschten Namen eingeben und dann auf **Fortsetzen** klicken.
4. Klicken Sie auf **Verbindungsprotokolle** und aktivieren Sie diejenigen Protokolle, die in diesem Remote-Verwaltungsplan für Remote-Verbindungen verfügbar sein sollen – NEAR, RDP oder Apple Bildschirmfreigabe.
5. [Optional] Aktivieren oder deaktivieren Sie für das NEAR-Protokoll im Bereich **Sicherheitseinstellungen** die Kontrollkästchen, um die entsprechende Einstellung zu aktivieren bzw. zu deaktivieren, und klicken Sie anschließend auf **Fertig**.

Einstellung	Beschreibung	Verfügbar für
Workload sperren, wenn	Wenn Sie diese Einstellung	Windows, macOS

Einstellung	Beschreibung	Verfügbar für
der Benutzer die Verbindung zur Konsolensitzung trennt	wählen, wird der Remote-Workload gesperrt, wenn Sie die Verbindung zur Konsolensitzung trennen.	
Nur einem Benutzer gleichzeitig erlauben, sich über NEAR zu verbinden oder Dateien zu übertragen	Wenn Sie diese Einstellung wählen, sind keine weiteren Verbindungen über NEAR und keine Dateiübertragungen möglich, wenn bereits eine Remote-Verbindung zum Workload aktiv ist.	Windows, macOS, Linux
Workload-Administrator erlauben, sich mit jeder Nicht-Administrator-Benutzersitzung zu verbinden	Wenn Sie diese Einstellung wählen, darf sich der Administrator mit jeder Standard-Benutzersitzung auf dem Workload verbinden. Wenn die Option **Workload-Administrator erlauben, sich mit jeder Nicht-Administrator-Benutzersitzung zu verbinden** und **Erstellung von Systemsitzungen erlauben** deaktiviert sind, können Sie nur Verbindungen zu aktiven Administrator-Sitzungen auf den macOS-Remote-Workloads herstellen.	Windows, macOS
Erstellung von Systemsitzungen erlauben	Wenn Sie diese Einstellung wählen, wird der Administrator bei Remote-Verbindungen mit einer neuen Sitzung verbunden, anstatt mit einer der bestehenden aktiven Sitzungen.	macOS
Synchronisierung der Zwischenablage erlauben	Wenn Sie diese Einstellung wählen, können Sie Daten	Windows, macOS, Linux

Einstellung	Beschreibung	Verfügbar für
	zwischen Ihrer Zwischenablage und der Zwischenablage des Remote-Workloads übertragen. So ist es beispielsweise möglich, Text aus einer Datei auf dem Remote-Workload zu kopieren und ihn in eine Datei auf Ihrem Workload einzufügen (und umgekehrt).	

6. Aktivieren oder deaktivieren Sie im Bereich **Sicherheitseinstellungen** die Kontrollkästchen, um die entsprechende Einstellung zu aktivieren bzw. zu deaktivieren, und klicken Sie anschließend auf **Fertig**.

Einstellung	Beschreibung
Anzeigen, ob der Workload remote gesteuert wird	Wenn Sie diese Einstellung auswählen, wird auf dem Desktop des Remote-Workloads eine Benachrichtigung angezeigt, wenn es bereits eine aktive Remote-Desktop-Verbindung zu diesem Workload gibt.
Den Benutzer um Erlaubnis bitten, dass Screenshots vom Workload erstellt werden dürfen	Wenn Sie diese Einstellung auswählen, wird der Benutzer des Remote-Workloads benachrichtigt, wenn der Administrator eine Screenshot-Übertragung vom Workload anfordert.

7. Klicken Sie auf **Workload-Verwaltung** und wählen Sie dann diejenigen Funktionen aus, die auf den Remote-Workloads verfügbar sein sollen. Klicken Sie dann abschließend auf **Fertig**.

Einstellung	Beschreibung	Verfügbar auf
Dateiübertragung	Ermöglicht Dateiübertragungen zwischen lokalen und Remote-Workloads.	Windows, macOS, Linux
Screenshot-Übertragung	Ermöglicht es, Screenshots vom Desktop des Remote-Workloads an die Cyber Protect-Konsole zu übertragen.	Windows, macOS, Linux

8. Aktivieren oder deaktivieren Sie im Bereich **Anzeigeeinstellungen** die Kontrollkästchen, um die entsprechende Einstellung zu aktivieren bzw. zu deaktivieren, und klicken Sie anschließend auf

Fertig.

Hinweis
Die **Anzeigeeinstellungen** sind nur bei Verbindungen über NEAR verfügbar.

Einstellung	Beschreibung	Verfügbar auf
Desktop-Deduplizierung für die Desktop-Erfassung verwenden	Die Desktop-Duplizierung ist eine der verfügbaren Bildschirmaufnahme-Methoden unter Windows. Diese kann jedoch in manchen Umgebungen instabil sein. Wenn Sie keine Desktop-Deduplizierung verwenden, werden Sie stattdessen die Basismethode (BitBlt) verwenden. Diese ist zwar deutlich langsamer, dafür aber stabiler.	Windows
OpenCL-Beschleunigung verwenden	Die OpenCL-Beschleunigung kann den adaptiven Codec, der für den Qualitätsmodus **Ausbalanciert** verantwortlich ist, beschleunigen, indem einige Berechnungen auf der GPU (Graphics Processing Unit) ausgeführt werden. Dafür ist es jedoch erforderlich, dass auf dem Remote-Linux ein OpenCL-Treiber installiert wird. Der adaptive Codec verwendet OpenCL unter Windows und macOS, sofern diese Funktion in deren Grafiktreibern verfügbar ist.	Linux
H.264-Hardware-Encodierung verwenden	NEAR unterstützt drei Qualitätsmodi: **Glatt**, **Ausbalanciert** und **Scharf**. Im Modus **Glatt** wird eine Hardware-basierte H.264-Encodierung verwendet, um	Windows, macOS

Einstellung	Beschreibung	Verfügbar auf
	das Desktop-Bild zu übermitteln. Der Modus **Ausbalanciert** verwendet einen adaptiven Codec, der (im Vergleich zum von H.264 verwendeten Modus 'Video') die volle Bildqualität in 32 Bit bietet. Die Bildqualität wird automatisch an die aktuellen Netzwerkbedingungen angepasst und die aktuelle Framerate beibehalten. Der Modus **Scharf** verwendet einen adaptiven Codec, der (im Vergleich zum von H.264 verwendeten Modus 'Video') die volle Bildqualität in 32 Bit bietet. Hier wird die beste Bildqualität erreicht, aber möglicherweise mit reduzierter Bildwiederholrate (pro Sek.), wenn Ihr Netzwerk, Prozessor oder Ihre Grafikkarte dabei überlastet sein sollten.	

9. Wenn Sie wollen, dass die Informationen über die Benutzer, die sich zuletzt an den Workloads angemeldet haben, in den Details des Workloads aufgeführt werden, klicken Sie auf **Toolbox**, aktivieren Sie die Option **Zuletzt angemeldete Benutzer anzeigen** und klicken Sie abschließend auf **Fertig**.

   Weitere Informationen über die zuletzt angemeldeten Benutzer finden Sie im Abschnitt '"Den zuletzt angemeldeten Benutzer finden" (S. 433)'.
10. [Optional] So können Sie dem Plan Workloads hinzufügen:
    a. Klicken Sie auf **Workloads hinzufügen**.
    b. Wählen Sie die Workloads aus und klicken Sie dann auf **Hinzufügen**.
    c. Wenn es Kompatibilitätsprobleme gibt, die Sie beheben wollen, befolgen Sie die im Abschnitt '"Kompatibilitätsprobleme mit Remote-Verwaltungsplänen beheben" (S. 1106)' beschriebene Prozedur.
11. Klicken Sie auf **Erstellen**.

Von 'Alle Geräte' ausgehend

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte** –> **Alle Geräte**.
2. Klicken Sie auf den Workload, auf den ein Remote-Verwaltungsplan angewendet werden soll.
3. Klicken Sie zuerst auf **Schützen** und anschließend auf **Plan hinzufügen**.
4. Klicken Sie auf **Plan erstellen** und wählen Sie dann **Remote-Verwaltung**.
5. [Optional] Wenn Sie den Standardnamen für den Plan ändern wollen, müssen Sie auf das Stiftsymbol klicken, den gewünschten Namen eingeben und dann auf **Fortsetzen** klicken.
6. Klicken Sie auf **Verbindungsprotokolle** und aktivieren Sie diejenigen Protokolle, die in diesem Remote-Verwaltungsplan für Remote-Verbindungen verfügbar sein sollen – NEAR, RDP oder Apple Bildschirmfreigabe.
7. [Optional] Aktivieren oder deaktivieren Sie für das NEAR-Protokoll im Bereich **Sicherheitseinstellungen** die Kontrollkästchen, um die entsprechende Einstellung zu aktivieren bzw. zu deaktivieren, und klicken Sie anschließend auf **Fertig**.

Einstellung	Beschreibung	Verfügbar für
Workload sperren, wenn der Benutzer die Verbindung zur Konsolensitzung trennt	Wenn Sie diese Einstellung wählen, wird der Remote-Workload gesperrt, wenn Sie die Verbindung zur Konsolensitzung trennen.	Windows, macOS
Nur einem Benutzer gleichzeitig erlauben, sich über NEAR zu verbinden oder Dateien zu übertragen	Wenn Sie diese Einstellung wählen, sind keine weiteren Verbindungen über NEAR und keine Dateiübertragungen möglich, wenn bereits eine Remote-Verbindung zum Workload aktiv ist.	Windows, macOS, Linux
Workload-Administrator erlauben, sich mit jeder Nicht-Administrator-Benutzersitzung zu verbinden	Wenn Sie diese Einstellung wählen, darf sich der Administrator mit jeder Standard-Benutzersitzung auf dem Workload verbinden. Wenn die Option **Workload-Administrator erlauben, sich mit jeder Nicht-Administrator-Benutzersitzung zu verbinden** und **Erstellung von Systemsitzungen erlauben** deaktiviert sind, können Sie nur	Windows, macOS

Einstellung	Beschreibung	Verfügbar für
	Verbindungen zu aktiven Administrator-Sitzungen auf den macOS-Remote-Workloads herstellen.	
Erstellung von Systemsitzungen erlauben	Wenn Sie diese Einstellung wählen, wird der Administrator bei Remote-Verbindungen mit einer neuen Sitzung verbunden, anstatt mit einer der bestehenden aktiven Sitzungen.	macOS
Synchronisierung der Zwischenablage erlauben	Wenn Sie diese Einstellung wählen, können Sie Daten zwischen Ihrer Zwischenablage und der Zwischenablage des Remote-Workloads übertragen. So ist es beispielsweise möglich, Text aus einer Datei auf dem Remote-Workload zu kopieren und ihn in eine Datei auf Ihrem Workload einzufügen (und umgekehrt).	Windows, macOS, Linux

8. Aktivieren oder deaktivieren Sie im Bereich **Sicherheitseinstellungen** die Kontrollkästchen, um die entsprechende Einstellung zu aktivieren bzw. zu deaktivieren, und klicken Sie anschließend auf **Fertig**.

Einstellung	Beschreibung
Anzeigen, ob der Workload remote gesteuert wird	Wenn Sie diese Einstellung auswählen, wird auf dem Desktop des Remote-Workloads eine Benachrichtigung angezeigt, wenn es bereits eine aktive Remote-Desktop-Verbindung zu diesem Workload gibt.
Den Benutzer um Erlaubnis bitten, dass Screenshots vom Workload erstellt werden dürfen	Wenn Sie diese Einstellung auswählen, wird der Benutzer des Remote-Workloads benachrichtigt, wenn der Administrator eine Screenshot-Übertragung vom Workload anfordert.

9. Klicken Sie auf **Workload-Verwaltung** und wählen Sie dann diejenigen Funktionen aus, die auf den Remote-Workloads verfügbar sein sollen. Klicken Sie dann abschließend auf **Fertig**.

Einstellung	Beschreibung	Verfügbar auf
Dateiübertragung	Ermöglicht Dateiübertragungen zwischen lokalen und Remote-Workloads.	Windows, macOS, Linux
Screenshot-Übertragung	Ermöglicht es, Screenshots vom Desktop des Remote-Workloads an die Cyber Protect-Konsole zu übertragen.	Windows, macOS, Linux

10. Aktivieren oder deaktivieren Sie im Bereich **Anzeigeeinstellungen** die Kontrollkästchen, um die entsprechende Einstellung zu aktivieren bzw. zu deaktivieren, und klicken Sie anschließend auf **Fertig**.

Hinweis
Die **Anzeigeeinstellungen** sind nur bei Verbindungen über NEAR verfügbar.

Einstellung	Beschreibung	Verfügbar auf
Desktop-Deduplizierung für die Desktop-Erfassung verwenden	Die Desktop-Duplizierung ist eine der verfügbaren Bildschirmaufnahme-Methoden unter Windows. Diese kann jedoch in manchen Umgebungen instabil sein. Wenn Sie keine Desktop-Deduplizierung verwenden, werden Sie stattdessen die Basismethode (BitBlt) verwenden. Diese ist zwar deutlich langsamer, dafür aber stabiler.	Windows
OpenCL-Beschleunigung verwenden	Die OpenCL-Beschleunigung kann den adaptiven Codec, der für den Qualitätsmodus **Ausbalanciert** verantwortlich ist, beschleunigen, indem einige Berechnungen auf der GPU (Graphics Processing Unit) ausgeführt werden. Dafür ist es jedoch erforderlich, dass	Linux

Einstellung	Beschreibung	Verfügbar auf
	auf dem Remote-Linux ein OpenCL-Treiber installiert wird. Der adaptive Codec verwendet OpenCL unter Windows und macOS, sofern diese Funktion in deren Grafiktreibern verfügbar ist.	
H.264-Hardware-Encodierung verwenden	NEAR unterstützt drei Qualitätsmodi: **Glatt**, **Ausbalanciert** und **Scharf**. Im Modus **Glatt** wird eine Hardware-basierte H.264-Encodierung verwendet, um das Desktop-Bild zu übermitteln. Der Modus **Ausbalanciert** verwendet einen adaptiven Codec, der (im Vergleich zum von H.264 verwendeten Modus 'Video') die volle Bildqualität in 32 Bit bietet. Die Bildqualität wird automatisch an die aktuellen Netzwerkbedingungen angepasst und die aktuelle Framerate beibehalten. Der Modus **Scharf** verwendet einen adaptiven Codec, der (im Vergleich zum von H.264 verwendeten Modus 'Video') die volle Bildqualität in 32 Bit bietet. Hier wird die beste Bildqualität erreicht, aber möglicherweise mit reduzierter Bildwiederholrate (pro Sek.), wenn Ihr Netzwerk, Prozessor oder Ihre Grafikkarte dabei überlastet sein sollten.	Windows, macOS

11. Wenn Sie wollen, dass die Informationen über die Benutzer, die sich zuletzt an den Workloads angemeldet haben, in den Details des Workloads aufgeführt werden, klicken Sie auf **Toolbox**, aktivieren Sie die Option **Zuletzt angemeldete Benutzer anzeigen** und klicken Sie abschließend auf **Fertig**.
    Weitere Informationen über die zuletzt angemeldeten Benutzer finden Sie im Abschnitt '"Den zuletzt angemeldeten Benutzer finden" (S. 433)'.
12. Klicken Sie auf **Erstellen**.

Einen Workload zu einem Remote-Verwaltungsplan hinzufügen

Nachdem ein Remote-Verwaltungsplan erstellt wurde, können Sie diesem je nach Bedarf Workloads hinzufügen.

Voraussetzungen

Für Ihr Benutzerkonto ist die Zwei-Faktor-Authentifizierung aktiviert.

So können Sie einen Workload zu einem Remote-Verwaltungsplan hinzufügen

Aus Remote-Verwaltungsplänen

1. Gehen Sie in der Cyber Protect-Konsole zum Bereich **Verwaltung** –> **Remote-Verwaltungspläne**.
2. Klicken Sie auf den Remote-Verwaltungsplan.
3. Gehen Sie je nachdem, ob der Plan bereits auf einen Workload angewendet wurde oder nicht, folgendermaßen vor:
    - Klicken Sie auf **Workloads hinzufügen**, wenn der Plan bisher noch auf keinen Workload angewendet wurde.
    - Klicken Sie auf **Workloads verwalten**, wenn der Plan schon auf Workloads angewendet wurde.
4. Wählen Sie zuerst auf einen Workload aus der Liste aus und klicken Sie anschließend auf **Hinzufügen**.
5. Klicken Sie auf **Speichern**.
6. Klicken Sie auf **Bestätigen**, um die erforderliche Service-Quota auf den Workload anzuwenden.

Von 'Alle Geräte' ausgehend

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte** –> **Alle Geräte**.
2. Klicken Sie auf den Workload, auf den ein Remote-Verwaltungsplan angewendet werden soll.
3. Klicken Sie zuerst auf **Schützen** und anschileßend auf **Plan hinzufügen**.
4. Wählen Sie bei **Wählen Sie einen Plan aus der unteren Liste aus** den Eintrag **Remote-Verwaltung**, damit nur die Remote-Verwaltungspläne angezeigt werden.
5. Klicken Sie auf **Anwenden**.
6. Klicken Sie auf **Bestätigen**, um die erforderliche Service-Quota auf den Workload anzuwenden.

Workloads aus einem Remote-Verwaltungsplan entfernen

Sie können (je nach Bedarf) Workloads aus einem Remote-Verwaltungsplan entfernen.

Voraussetzungen

Für Ihr Benutzerkonto ist die Zwei-Faktor-Authentifizierung aktiviert.

So können Sie Workloads aus einem Remote-Verwaltungsplan entfernen

1. Gehen Sie in der Cyber Protect-Konsole zum Bereich **Verwaltung** –> **Remote-Verwaltungspläne**.
2. Klicken Sie auf den Remote-Verwaltungsplan.
3. Klicken Sie auf **Workloads verwalten**.
4. Wählen Sie einen oder mehrere Workloads aus, die Sie aus dem Remote-Verwaltungsplan entfernen wollen, und klicken Sie anschließend auf **Entfernen**.
5. Klicken Sie auf **Fertig**.
6. Klicken Sie auf **Speichern**.

Zusätzliche Aktionen mit vorhandenen Remote-Verwaltungsplänen

Sie können von der Anzeige **Remote-Verwaltungspläne** aus folgende zusätzliche Aktionen mit den Remote-Verwaltungsplänen durchführen: Details anzeigen, bearbeiten, die Aktivitäten anzeigen, die Alarmmeldungen anzeigen, umbenennen, aktivieren, deaktivieren, klonen, exportieren und löschen.

Details anzeigen

Voraussetzungen

Für Ihr Benutzerkonto ist die Zwei-Faktor-Authentifizierung aktiviert.

So können Sie die Details zu einem Remote-Verwaltungsplan einsehen

1. Klicken Sie in der Anzeige **Remote-Verwaltungspläne** auf das Symbol **Mehr Aktionen** des Remote-Verwaltungsplans.
2. Klicken Sie auf **Details anzeigen**.

Bearbeiten

Voraussetzungen

Für Ihr Benutzerkonto ist die Zwei-Faktor-Authentifizierung aktiviert.

So können Sie einen Plan bearbeiten

1. Klicken Sie in der Anzeige **Remote-Verwaltungspläne** auf das Symbol **Mehr Aktionen** des Remote-Verwaltungsplans.
2. Klicken Sie auf **Bearbeiten**.

Aktivitäten

So können Sie die zu einem Remote-Verwaltungsplan gehörenden Aktivitäten einsehen

1. Klicken Sie in der Anzeige **Remote-Verwaltungspläne** auf das Symbol **Mehr Aktionen** des Remote-Verwaltungsplans.
2. Klicken Sie auf **Aktivitäten**.
3. Klicken Sie auf eine Aktivität, um sich weitere Details zu dieser anzeigen zu lassen.

Alarmmeldungen

So können Sie die Alarmmeldungen einsehen

1. Klicken Sie in der Anzeige **Remote-Verwaltungspläne** auf das Symbol **Mehr Aktionen** des Remote-Verwaltungsplans.
2. Klicken Sie auf **Alarmmeldungen**.

Umbenennen

Voraussetzungen

Für Ihr Benutzerkonto ist die Zwei-Faktor-Authentifizierung aktiviert.

So können Sie einen Remote-Verwaltungsplan umbenennen

1. Klicken Sie in der Anzeige **Remote-Verwaltungspläne** auf das Symbol **Mehr Aktionen** des Remote-Verwaltungsplans.
2. Klicken Sie auf **Umbenennen**.
3. Geben Sie den neuen Plan-Namen ein und klicken Sie dann auf **Fortsetzen**.

Aktivieren

Voraussetzungen

Für Ihr Benutzerkonto ist die Zwei-Faktor-Authentifizierung aktiviert.

So können Sie einen Remote-Verwaltungsplan aktivieren

1. Klicken Sie in der Anzeige **Remote-Verwaltungspläne** auf das Symbol **Mehr Aktionen** des Remote-Verwaltungsplans.
2. Klicken Sie auf **Aktivieren**.

Deaktivieren

Voraussetzungen

Für Ihr Benutzerkonto ist die Zwei-Faktor-Authentifizierung aktiviert.

So können Sie einen Remote-Verwaltungsplan deaktivieren

1. Klicken Sie in der Anzeige **Remote-Verwaltungspläne** auf das Symbol **Mehr Aktionen** des Remote-Verwaltungsplans.
2. Klicken Sie auf **Deaktivieren**.

Klonen

Voraussetzungen

Für Ihr Benutzerkonto ist die Zwei-Faktor-Authentifizierung aktiviert.

So können Sie einen Remote-Verwaltungsplan klonen

1. Klicken Sie in der Anzeige **Remote-Verwaltungspläne** auf das Symbol **Mehr Aktionen** des Remote-Verwaltungsplans.
2. Klicken Sie auf **Klonen**.
3. Klicken Sie auf **Erstellen**.

Exportieren

Voraussetzungen

Für Ihr Benutzerkonto ist die Zwei-Faktor-Authentifizierung aktiviert.

So können Sie einen Remote-Verwaltungsplan exportieren

1. Klicken Sie in der Anzeige **Remote-Verwaltungspläne** auf das Symbol **Mehr Aktionen** des Remote-Verwaltungsplans.
2. Klicken Sie auf **Exportieren**.
   Die Plan-Konfiguration wird im JSON-Format auf die lokale Maschine exportiert.

Löschen

Voraussetzungen

Für Ihr Benutzerkonto ist die Zwei-Faktor-Authentifizierung aktiviert.

So können Sie einen Remote-Verwaltungsplan löschen

1. Klicken Sie in der Anzeige **Remote-Verwaltungspläne** auf das Symbol **Mehr Aktionen** des Remote-Verwaltungsplans.
2. Klicken Sie auf **Löschen**.
3. Wählen Sie **Ich bestätige** und klicken Sie anschließend auf **Löschen**.

Kompatibilitätsprobleme mit Remote-Verwaltungsplänen

In einigen Fällen kann es zu Kompatibilitätsproblemen kommen, wenn Sie einen Remote-Verwaltungsplan auf einen Workload anwenden. Sie werden möglicherweise folgende Kompatibilitätsprobleme feststellen:

- Pläne mit Konflikten – zu diesem Problem kommt es, wenn auf den Workload bereits ein anderer Remote-Verwaltungsplan angewendet wurde. Denn es darf nur jeweils ein Remote-Verwaltungsplan auf einen Workload angewendet werden.
- Inkompatibles Betriebssystem – zu diesem Problem kommt es, wenn das Betriebssystem des Workloads nicht unterstützt wird.
- Nicht unterstützter Agent – zu diesem Problem kommt es, wenn die Version des Protection Agenten auf dem Workload veraltet ist und die Remote-Desktop-Funktionalität nicht unterstützt.
- Unzureichende Quota – zu diesem Problem kommt es, wenn im Mandanten die Service-Quota nicht ausreicht, um sie den ausgewählten Workloads zuweisen zu können.

Wenn der Remote-Verwaltungsplan auf bis zu 150 persönlich ausgewählte Workloads angewendet wird, werden Sie aufgefordert, die bestehenden Konflikte zu lösen, bevor Sie den Plan speichern. Sie können einen Konflikt auflösen, indem Sie entweder dessen Ursache beseitigen oder indem Sie die betroffenen Workloads aus dem Plan entfernen. Weitere Informationen finden Sie im Abschnitt '"Kompatibilitätsprobleme mit Remote-Verwaltungsplänen beheben" (S. 1106)'. Wenn Sie den Plan speichern, ohne die Konflikte zu lösen, wird er automatisch für die inkompatiblen Workloads deaktiviert und werden entsprechende Alarmmeldungen angezeigt.

Wenn der Remote-Verwaltungsplan auf mehr als 150 Workloads oder Gerätegruppen angewendet wird, wird der Plan zuerst gespeichert und dann auf Kompatibilität überprüft. Der Plan wird automatisch für die nicht unterstützten Workloads deaktiviert und es werden entsprechende Alarmmeldungen angezeigt.

Kompatibilitätsprobleme mit Remote-Verwaltungsplänen beheben

Je nach Art der Kompatibilitätsprobleme können Sie beim Erstellen eines neuen Remote-Verwaltungsplans verschiedene Aktionen durchführen, um diese Kompatibilitätsprobleme zu beheben.

Hinweis
Wenn Sie ein Kompatibilitätsproblem beheben wollen, indem Sie Workloads aus einem Plan entfernen, können Sie keine Workloads entfernen, die zu einer Gerätegruppe gehören.

So können Sie die Kompatibilitätsprobleme beheben

1. Klicken Sie auf **Probleme überprüfen**.
2. [So können Sie Kompatibilitätsprobleme mit vorhandenen Remote-Verwaltungsplänen lösen, indem Sie Workloads aus dem neuen Plan entfernen]
   a. Wählen Sie auf der Registerkarte **Pläne mit Konflikten** diejenige Workloads aus, die Sie entfernen wollen.
   b. Klicken Sie auf **Workloads aus dem Plan entfernen**.
   c. Klicken Sie zuerst auf **Entfernen** und dann auf **Schließen**.
3. [So können Sie Kompatibilitätsprobleme mit Remote-Verwaltungsplänen lösen, indem Sie die Pläne deaktivieren, die bereits auf die Workloads angewendet wurden]

a. Klicken Sie auf **Angewendete Pläne deaktivieren**.

b. Klicken Sie zuerst auf **Deaktivieren** und dann auf **Schließen**.

4. [So können Sie Kompatibilitätsprobleme mit inkompatiblen Betriebssystemen lösen]
   a. Wählen Sie auf der Registerkarte **Inkompatibles Betriebssystem** diejenigen Workloads aus, die Sie entfernen wollen.
   b. Klicken Sie auf **Workloads aus dem Plan entfernen**.
   c. Klicken Sie zuerst auf **Entfernen** und dann auf **Schließen**.
5. [So können Sie Kompatibilitätsprobleme mit nicht unterstützten Agenten beheben, indem Sie Workloads aus dem Plan entfernen]
   a. Wählen Sie auf der Registerkarte **Nicht unterstützte Agenten** diejenige Workloads aus, die Sie entfernen wollen.
   b. Klicken Sie auf **Workloads aus dem Plan entfernen**.
   c. Klicken Sie zuerst auf **Entfernen** und dann auf **Schließen**.
6. [Wenn Sie Kompatibilitätsprobleme mit nicht unterstützten Agenten durch Aktualisierung der Agenten-Version beheben wollen] Klicken Sie auf **Zur Agenten-Liste gehen**.

   Hinweis
   Diese Option ist nur für Kunden-Administratoren verfügbar.

7. [So können Sie Kompatibilitätsprobleme durch eine unzureichende Quota beheben, indem Sie Workloads aus dem Plan entfernen]
   a. Wählen Sie auf der Registerkarte **Unzureichende Quota** diejenige Workloads aus, die Sie entfernen wollen.
   b. Klicken Sie auf **Workloads aus dem Plan entfernen**.
   c. Klicken Sie zuerst auf **Entfernen** und dann auf **Schließen**.
8. [So können Sie Kompatibilitätsprobleme mit einer unzureichenden Quota lösen, indem Sie die Quota des Mandanten vergrößern]

   Hinweis
   Diese Option ist nur für Partner-Administratoren verfügbar.

   a. Klicken Sie auf der Registerkarte **Unzureichende Quota** auf den Befehl **Zum Management-Portal gehen**.
   b. Vergrößern Sie die Service-Quota für den Kunden.

Workload-Anmeldedaten

Sie können Anmeldedaten (Benutzername und Kennwort bzw. VNC-Kennwort) von Administratoren oder Nicht-Administratoren der Remote-Workloads hinzufügen, diese im Cloud-Anmeldedatenspeicher (Cloud Credentials Store) speichern und sie dann für automatische Authentifizierungen verwenden, wenn Sie sich mit den von Ihnen verwalteten Workloads verbinden.

Dadurch müssen Sie diese Anmeldedaten nicht jedes Mal manuell eingeben, wenn die Sitzung während des Verbindungsaufbaus authentifiziert werden soll. Sie können diese Anmeldedaten einmalig im Anmeldedatenspeicher speichern und sie dann mehreren Workloads zuweisen. Der Connect Client wird die Anmeldedaten dann jedes Mal verwenden, wenn Sie eine Remote-Verbindung zu den betreffenden Workloads herstellen wollen.

Hinweis
Anmeldedaten, die im Anmeldedatenspeicher gespeichert sind, werden nicht zwischen den verschiedenen Mandanten-Ebenen geteilt. Sie werden nur innerhalb derselben Mandanten-Ebene für denselben Kunden- oder Partner-Mandanten freigegeben.

Falls ein Kunden-Mandant also mehrere Administratoren haben sollte, können diese die Anmeldedaten im Anmeldedaten-Speicher sehen und gemeinsam nutzen. Andere Partner-Administratoren oder die Kunden-Administratoren anderer Mandanten können diese Anmeldedaten dagegen weder sehen noch nutzen.

Anmeldedaten hinzufügen

Sie können Anmeldedaten hinzufügen und diese dann für Remote-Verbindungen zu mehreren Workloads verwenden.

So können Sie Anmeldedaten zu einem Workload hinzufügen und diese im Anmeldedatenspeicher hinterlegen

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte** –> **Alle Geräte**.
2. Klicken Sie auf den Workload, für den Sie Anmeldedaten hinzufügen wollen.
3. Sie können auf folgende Weise auf Menü **Einstellungen** zugreifen:
   - Klicken Sie auf **Remote-Desktop** und dann auf **Einstellungen**.
   - Klicken Sie auf **Verwalten** und dann auf **Einstellungen**.
4. Klicken Sie auf **Anmeldedaten hinzufügen**.
5. Klicken Sie im **Anmeldedatenspeicher** auf **Anmeldedaten hinzufügen**.

6. Geben Sie die Anmeldedaten ein.

Feld	Beschreibung
Anmeldedatenname	Die Kennung der Anmeldedaten, die im Anmeldedatenspeicher sichtbar sein werden.
Benutzername	Der Benutzername, der für die Remote-Verbindungen mit dem Ziel-Workload verwendet werden soll.
Kennwort	Das Kennwort, das für die Remote-Verbindungen mit dem Ziel-Workload verwendet werden soll.
VNC-Kennwort	Dieses Feld ist nur für das Apple Bildschirmfreigabe-Protokoll verfügbar.

7. Klicken Sie auf **Speichern**.

Anmeldedaten einem Workload zuweisen

Wenn Sie Anmeldedaten hinzufügen, können Sie diese verwenden, um sich automatisch zu authentifizieren, wenn Sie sich mit einem von Ihnen verwalteten Workload verbinden wollen.

So können Sie einem Workload gespeicherte Anmeldedaten für eine automatische Authentifizierung zuweisen

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte** –> **Alle Geräte**.
2. Sie können auf folgende Weise auf Menü **Einstellungen** zugreifen:
   - Klicken Sie auf **Remote-Desktop** und dann auf **Einstellungen**.
   - Klicken Sie auf **Verwalten** und dann auf **Einstellungen**.
3. Klicken Sie auf der Registerkarte des unterstützten Protokolls (NEAR, RDP oder Apple Bildschirmfreigabe) auf **Anmeldedaten hinzufügen**.
4. Wählen Sie im **Anmeldedatenspeicher** die Anmeldedaten aus der Liste aus und klicken Sie dann auf **Anmeldedaten auswählen**.

Anmeldedaten löschen

Sie können Anmeldedaten, die nicht mehr benötigt werden, löschen.

So können Sie Anmeldedaten aus dem Anmeldedatenspeicher löschen

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte** –> **Alle Geräte**.
2. Sie können auf folgende Weise auf Menü **Einstellungen** zugreifen:
   - Klicken Sie auf **Remote-Desktop** und dann auf **Einstellungen**.
   - Klicken Sie auf **Verwalten** und dann auf **Einstellungen**.
3. Klicken Sie auf der Registerkarte des unterstützten Protokolls (NEAR, RDP oder Apple

Bildschirmfreigabe) auf **Löschen**.

4. Klicken Sie im Bestätigungsfenster auf **Löschen**.

Die Zuweisung von Anmeldedaten für einen Workload aufheben

Sie können die Zuweisung von Anmeldedaten für einen Workload aufheben, diese aber dennoch im Anmeldedatenspeicher behalten.

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte** –> **Alle Geräte**.
2. Sie können auf folgende Weise auf Menü **Einstellungen** zugreifen:
   - Klicken Sie auf **Remote-Desktop** und dann auf **Einstellungen**.
   - Klicken Sie auf **Verwalten** und dann auf **Einstellungen**.
3. Klicken Sie auf der Registerkarte des unterstützten Protokolls (NEAR, RDP oder Apple Bildschirmfreigabe) auf **Zuweisung aufheben**.
4. Klicken Sie im Bestätigungsfenster auf **Zuweisung aufheben**.

Mit verwalteten Workloads arbeiten

Als verwaltete Workloads werden Workloads bezeichnet, auf denen der Schutz Agent installiert ist.

Sie können folgende Aktionen auf verwalteten Remote-Workloads durchführen:

- sich über das NEAR-Protokoll im Steuerungs- oder Nur-Anzeigen-Modus für Remote-Unterstützungs- oder Remote-Desktop-Zwecke verbinden
- sich über RDP im Steuerungsmodus für Remote-Desktop-Zwecke verbinden
- sich über das Apple Bildschirmfreigabe-Protokoll im Steuerungs-, Nur-Anzeigen- oder Vorhangmodus für Remote-Unterstützungs- oder Remote-Desktop-Zwecke verbinden
- sich über einen Webclient für Remote-Desktop-Zwecke verbinden
- neu starten, herunterfahren, in den Ruhezustand versetzen, den Papierkorb leeren, den Remote-Benutzer vom Remote-Workload abmelden
- Dateien zwischen Ihrem Workload und den Remote-Workloads übertragen
- diese überwache, indem Sie Screenshots aufnehmen

Hinweis
Für Remote-Desktop-Verbindungen zu verwalteten Workloads ist es erforderlich, dass ein Schutz Agent auf dem Workload installiert ist und ein Remote-Verwaltungsplan auf diesen angewendet wird.

Die RDP-Einstellungen konfigurieren

Sie können die Einstellungen konfigurieren, die automatisch für die RDP-basierte Remote-Desktop-Verbindungen eines verwalteten Workloads angewendet werden sollen.

So können Sie die RDP-Einstellungen eines Workloads konfigurieren

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte** –> **Maschinen mit Agenten**.
2. Sie können auf folgende Weise auf Menü **Einstellungen** zugreifen:
   - Klicken Sie auf **Remote-Desktop** und dann auf **Einstellungen**.
   - Klicken Sie auf **Verwalten** und dann auf **Einstellungen**.
3. Konfigurieren Sie auf der Registerkarte **RDP** die gewünschten Einstellungen.

Einstellung	Beschreibung
Audio-Wiedergabe	Mit dieser Einstellung kann die Umleitung der Sound-Ausgabe vom Remote-Workloads zu Ihrem lokalen Workload aktiviert oder deaktiviert werden.
Audio-Aufzeichnung	Diese Einstellung legt fest, ob Audio-Aufzeichnungen (Sprechen in das Mikrofon) zum Remote-Workload übertragen werden sollen.
Drucker umleiten	Wenn Sie diese Einstellung auswählen, werden die Drucker Ihres Workloads auch auf dem Remote-Workload verfügbar gemacht.
Dateien umleiten	Diese Einstellung legt fest, ob Dateien von Ihrem lokalen Workload für den Remote-Workload freigegeben werden sollen.
Farbtiefe	Diese Einstellung legt fest, wie viele Farben für die übertragene RDP-Anzeige verwendet werden sollen. Höhere Werte erfordern eine höhere Bandbreite. **High Color**: 16 Bit **True Color**: • 24 Bit für RDP-Verbindungen über den Webclient • 32 Bit für RDP-Verbindungen über den Connect Client

4. Klicken Sie auf die Schaltfläche 'Schließen'.

Mit einem verwalteten Workload für Remote-Desktop- oder Remote-Unterstützungszwecke verbinden

Hinweis
Welche Verbindungsprotokolle Sie für Ihre Remote-Verbindungen verwenden können, hängt von der Konfiguration des Remote-Verwaltungsplans und vom Betriebssystem des Remote-Workloads ab.

Voraussetzungen

- Ein Remote-Verwaltungsplan, bei dem das entsprechende Verbindungsprotokoll aktiviert ist, wurde auf den verwalteten Workload angewendet.
- Dem Workload wurde die erforderliche Service-Quota zugewiesen. (Die Service-Quota wird automatisch erworben, wenn Sie einen Remote-Verwaltungsplan auf den Workload anwenden.)

- [Für Verbindungen über die Apple Bildschirmfreigabe] Die Apple Bildschirmfreigabe ist auf dem macOS-Workload aktiviert.
- Für Ihr Benutzerkonto ist die Zwei-Faktor-Authentifizierung in Acronis Cyber Protect Cloud aktiviert.

So können Sie eine Remote-Verbindung zu einem verwalteten Workload für Remote-Desktop- oder Remote-Unterstützungszwecke herstellen

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte** –> **Maschinen mit Agenten**.
2. Klicken Sie auf den Workload, zu dem Sie eine Verbindung aufbauen wollen.
3. Klicken Sie auf **Remote-Desktop**.
   Standardmäßig ist NEAR als Verbindungsprotokoll ausgewählt.
4. [Optional] Wählen Sie in der Dropdown-Liste **Verbindungsprotokoll** das Verbindungsprotokoll aus, das Sie verwenden möchten.
5. Klicken Sie auf den Ansichtsmodus, den Sie verwenden möchten.

Protokoll	Remote-Verbindungen zu	Ansichtsmodus	Unterstützte Remote-Aktion
NEAR	Windows Linux macOS	**Steuern** – In diesem Modus können Sie den Remote-Workload beobachten und Aktionen auf diesem durchführen. **Nur anzeigen** – In diesem Modus können Sie den Remote-Workload nur beobachten.	Remote-Desktop Remote-Unterstützung
RDP	Windows	**Steuern** – In diesem Modus können Sie den Remote-Workload anzeigen und Aktionen auf diesem durchführen.	Remote-Desktop

Protokoll	Remote-Verbindungen zu	Ansichtsmodus	Unterstützte Remote-Aktion
		Hinweis Wenn RDP in den Betriebssystemeinstellungen des Workloads deaktiviert ist, wird ein entsprechendes Pop-up-Fenster angezeigt. Verwenden Sie dieses Fenster, um die RDP-Funktion für den Workload entweder nur für die gerade aktuelle Sitzung oder generell zu aktivieren: • Wenn Sie für diesen Workload die RDP-Funktion nur für die gerade aktuelle Sitzung aktivieren wollen, müssen Sie die Option **Deaktivieren, wenn die Sitzung vorbei ist**auswählen und dann auf **Erlauben** klicken. • Wenn Sie die RDP-Funktion für diesen Workload grundsätzlich aktivieren wollen, müssen Sie auf **Erlauben** klicken.	
Apple Bildschirmfreigabe	macOS	**Steuern** – In diesem Modus können Sie den Remote-Workload beobachten und Aktionen auf diesem durchführen. **Nur anzeigen** – In diesem Modus können Sie den Remote-Workload nur beobachten. **Vorhang** – nur für macOS-Workloads verfügbar. Wenn Sie sich im Vorhangmodus mit dem Remote-Workload verbinden, wird die	Remote-Desktop Remote-Unterstützung

Protokoll	Remote-Verbindungen zu	Ansichtsmodus	Unterstützte Remote-Aktion
		Bildschirmanzeige des Remote-Workloads abgedunkelt, sodass der Remote-Benutzer Ihre Aktionen auf dem Workload nicht sehen kann.	

6. Gehen Sie folgendermaßen vor, je nachdem, ob der Connect Client auf Ihrem Workload installiert ist oder nicht:
   - Sollte der Connect Client nicht installiert sein, dann laden Sie diesen herunter, installieren Sie ihn und wählen Sie im anschließenden angezeigten Bestätigungsfenster den Befehl **Erlauben**.
   - Sollte der Connect Client bereits installiert sein, dann klicken Sie im angezeigten Bestätigungsfenster auf **Connect Client öffnen**.
7. Wählen Sie im Fenster **Authentifizierung** eine Authentifizierungsoption aus und geben Sie anschließend die benötigten Anmeldedaten ein.

Hinweis
Wenn Sie dem Workload Anmeldedaten zugewiesen haben, wird die Authentifizierung automatisch durchgeführt und dieser Schritt übersprungen. Weitere Informationen finden Sie im Abschnitt '"Anmeldedaten einem Workload zuweisen" (S. 1109)'.

Authentifizierungsoption	Beschreibung
Mit Remote-Workload-Anmeldedaten	Ihnen wird der Aufbau einer Remote-Verbindung erlaubt, nachdem Sie den Benutzernamen und das Kennwort eines administrativen Benutzers auf dem Remote-Workload angegeben haben. Diese Option ist für NEAR-, RDP- und Apple Bildschirmfreigabe-Verbindungen verfügbar. Mit dieser Option können Sie sich für Remote-Desktop- oder Remote-Unterstützungszwecke authentifizieren.
Berechtigung zum Beobachten anfordern	Ihnen wird der Aufbau einer Remote-Verbindung im Beobachtungsmodus erlaubt, nachdem der Benutzer, der am Remote-Workload angemeldet ist, dies gestattet hat. Diese Option ist für NEAR-, und Apple Bildschirmfreigabe-Verbindungen verfügbar. Mit dieser Option können Sie sich für Remote-Unterstützungszwecke authentifizieren.
Berechtigung zur Steuerung anfordern	Ihnen wird der Aufbau einer Remote-Verbindung im Steuermodus erlaubt, nachdem der Benutzer, der am

Authentifizierungsoption	Beschreibung
	Remote-Workload angemeldet ist, dies gestattet hat. Diese Option ist für NEAR-, und Apple Bildschirmfreigabe-Verbindungen verfügbar. Mit dieser Option können Sie sich für Remote-Unterstützungszwecke authentifizieren.

8. Klicken Sie zuerst auf **Verbinden** und dann auf die anzuzeigende Sitzung (wenn mehrere Benutzersitzungen auf dem Workload verfügbar sind).

   Der Connect Client wird ein neues Viewer-Fenster öffnen, in dem Sie den Desktop des Remote-Workloads sehen können. Der Viewer verfügt über eine Symbolleiste mit zusätzlichen Aktionen, die Sie auf dem Remote-Workload durchführen können (nachdem die Remote-Verbindung hergestellt wurde). Weitere Informationen finden Sie im Abschnitt '"Die Symbolleiste im Viewer-Fenster verwenden" (S. 1124)'.

Eine Verbindung zu einem verwalteten Workload über einen Webclient herstellen

Sie können eine Remote-Desktop-Verbindung zu einem verwalteten Workload über einen Webclient herstellen.

Voraussetzungen

- Dem Workload wurde die Standard-Service-Quota zugewiesen.
- Auf den verwalteten Workload wurde ein Remote-Verwaltungsplan angewendet, für den RDP aktiviert ist.
- Auf dem verwalteten Workload ist die RDP-Funktion aktiviert.
- Ihr Browser unterstützt HTML5.
- Für Ihr Benutzerkonto ist die Zwei-Faktor-Authentifizierung in Acronis Cyber Protect Cloud aktiviert.

So können Sie über einen Webclient eine Remote-Verbindung zu einem Workload herstellen

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte** –> **Alle Geräte**.
2. Klicken Sie zuerst auf den Workload, zu dem Sie eine Remote-Verbindung aufbauen wollen, und anschließend auf **Remote-Desktop** –>**Über Webclient verbinden**.
3. Geben Sie die Anmeldedaten (Benutzername, Kennwort) ein, um auf den Workload zugreifen zu können, und klicken Sie anschließend auf den Befehl **Verbinden**.

   Hinweis
   Wenn Sie dem Workload Anmeldedaten zugewiesen haben, wird die Authentifizierung automatisch durchgeführt und dieser Schritt übersprungen. Weitere Informationen finden Sie im Abschnitt '"Anmeldedaten einem Workload zuweisen" (S. 1109)'.

Dateien übertragen

Sie können Dateien mühelos zwischen Ihrem lokalen Workload und einem verwalteten Workload übertragen.

Voraussetzungen

- Ein Remote-Verwaltungsplan, bei dem das NEAR-Protokoll und die Dateiübertragung aktiviert ist, wurde auf den Workload angewendet.
- Die Quota 'Advanced Management' wurde auf den Workload angewendet.
- Für Ihr Benutzerkonto ist die Zwei-Faktor-Authentifizierung in Acronis Cyber Protect Cloud aktiviert.

So können Sie Dateien remote zwischen Ihrem Workload und einem verwalteten Workload übertragen

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte** –> **Maschinen mit Agenten**.
2. Klicken Sie auf den Workload, mit dem Sie Dateien übertragen wollen.
3. Klicken Sie auf **Verwalten** und dann auf **Dateien übertragen**.
4. Gehen Sie folgendermaßen vor, je nachdem, ob der Connect Client auf Ihrem Workload installiert ist oder nicht:
   - Sollte der Connect Client nicht installiert sein, dann laden Sie diesen herunter, installieren Sie ihn und klicken Sie im anschließenden angezeigten Bestätigungsfenster den Befehl **Erlauben**.
   - Sollte der Connect Client bereits installiert sein, dann klicken Sie im angezeigten Bestätigungsfenster auf **Connect Client öffnen**.
5. Wählen Sie im Fenster **Authentifizierung** eine Authentifizierungsoption aus und geben Sie anschließend die benötigten Anmeldedaten ein.

Authentifizierungsoption	Beschreibung
Mit Remote-Workload-Anmeldedaten	Ihnen wird der Aufbau einer Remote-Verbindung erlaubt, nachdem Sie den Benutzernamen und das Kennwort eines administrativen Benutzers auf dem Remote-Workload angegeben haben.
Berechtigung zur Übertragung von Dateien anfordern	Sie können die Dateien erst dann übertragen, wenn der Benutzer, der auf dem Remote-Workload angemeldet ist, dies ausdrücklich erlaubt.

6. Durchsuchen Sie im Fenster **Dateiübertragung** die Dateien und übertragen Sie diese per Drag & Drop zum gewünschten Ziel.

Hinweis
Die Dateien des lokalen Workloads werden im linken Fensterbereich aufgelistet, die Dateien des Remote-Workloads dagegen im rechten.
Wenn eine Dateiübertragung beginnt, wird diese im Fensterbereich **Tasks** aufgelistet.

7. [Optional] Wenn Sie die abgeschlossenen Tasks aus dem Fensterbereich **Tasks** entfernen wollen, klicken Sie auf **Abgeschlossene Elemente bereinigen**.
8. Wenn alle Übertragungen abgeschlossen wurden, können Sie das Fenster schließen.

Steuerungsaktionen auf verwalteten Workloads durchführen

Sie können einen Remote-Workload verwalten, indem Sie folgende grundlegende Steuerungsaktionen auf ihm durchführen: den Papierkorb leeren, in den Energiesparmodus versetzen, neu starten, herunterfahren oder den Remote-Benutzer abmelden.

Voraussetzungen

- Auf den Workload wurde die Standard-Service-Quota angewendet.
- Für Ihr Benutzerkonto ist die Zwei-Faktor-Authentifizierung in Acronis Cyber Protect Cloud aktiviert.

Papierkorb leeren

So können Sie den Papierkorb auf dem Remote-Workload leeren

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte** –> **Maschinen mit Agenten**.
2. Klicken Sie auf den Workload, auf dem Sie diese Aktion durchführen wollen.
3. Klicken Sie auf **Verwalten** und dann auf **Papierkorb leeren**.
4. Wählen Sie die Benutzersitzung, für die Sie diese Aktion durchführen wollen, und klicken Sie dann auf **Papierkorb leeren**.

Energiesparmodus

So können Sie einen Remote-Workload in den Energiesparmodus versetzen

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte** –> **Maschinen mit Agenten**.
2. Klicken Sie auf den Workload, auf dem Sie diese Aktion durchführen wollen.
3. Klicken Sie auf **Verwalten** und anschließend auf **Energiesparmodus**.

Neustart

So können Sie einen Remote-Workload neu starten

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte** –> **Maschinen mit Agenten**.
2. Klicken Sie auf den Workload, auf dem Sie diese Aktion durchführen wollen.
3. Klicken Sie auf **Verwalten** und anschließend auf **Neustart**.

- Bestimmen Sie bei Windows-Workloads, ob Sie dem derzeit auf dem Workload lokal angemeldeten Benutzer erlauben wollen, durchgeführte Änderungen zu speichern, bevor der Workload neu gestartet wird. Wählen Sie den Benutzer aus und klicken Sie dann erneut auf **Neustart**.
- Bestimmen Sie bei macOS-Workloads, ob Sie dem derzeit auf dem Workload lokal angemeldeten Benutzer erlauben wollen, durchgeführte Änderungen zu speichern, bevor der Workload neu gestartet wird, und klicken Sie dann erneut auf **Neustart**.
- Klicken Sie bei Linux-Workloads auf **Neustart**.

Herunterfahren

So können Sie einen Remote-Workload herunterfahren

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte** –> **Maschinen mit Agenten**.
2. Klicken Sie auf den Workload, auf dem Sie diese Aktion durchführen wollen.
3. Klicken Sie auf **Verwalten** und anschließend auf **Herunterfahren**.
   - Bestimmen Sie bei Windows-Workloads, ob Sie dem derzeit auf dem Workload lokal angemeldeten Benutzer erlauben wollen, durchgeführte Änderungen zu speichern, bevor der Workload heruntergefahren wird. Wählen Sie den Benutzer aus und klicken Sie dann erneut auf **Herunterfahren**.
   - Bestimmen Sie bei macOS-Workloads, ob Sie dem derzeit auf dem Workload lokal angemeldeten Benutzer erlauben wollen, durchgeführte Änderungen zu speichern, bevor der Workload heruntergefahren wird, und klicken Sie dann erneut auf **Herunterfahren**.
   - Klicken Sie bei Linux-Workloads erneut auf **Herunterfahren**.

Remote-Benutzer abmelden

So können Sie den Benutzer eines Remote-Workloads abmelden

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte** –> **Maschinen mit Agenten**.
2. Klicken Sie auf den Workload, auf dem Sie diese Aktion durchführen wollen.
3. Klicken Sie auf **Verwalten** und anschließend auf **Remote-Benutzer abmelden**.
4. Wählen Sie den abzumeldenden Benutzer aus und klicken Sie dann auf **Abmelden**.

Workloads per Screenshot-Übertragung überwachen

Sie können den Status eines Workloads mithilfe der Funktion Screenshot-Übertragung überwachen.

Voraussetzungen

- Ein Remote-Verwaltungsplan mit aktivierter Screenshot-Übertragungsfunktion wurde auf den Workload angewendet.
- Die Version des Protection Agenten ist aktuell und unterstützt die Screenshot-Übertragungsfunktion.
- Die Service-Quota 'Advanced Management' wurde auf den Workload angewendet.

- Der Workload ist online.
- Für Ihr Benutzerkonto ist die Zwei-Faktor-Authentifizierung in Acronis Cyber Protect Cloud aktiviert.

Einen Workload per Screenshot-Übertragung überwachen

So können Sie einen Workload per Screenshot-Übertragung überwachen

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte** –> **Screenshot-Übertragung**.
2. Klicken Sie auf den Workload, den Sie überwachen wollen.
3. Wählen Sie die Benutzersitzung aus.
4. Wählen Sie die Anzeige aus.
5. Bestimmen Sie die Aktualisierungsrate, mit der jeweils ein neuer Screenshot vom Desktop erstellt werden soll.
6. Bestimmen Sie die Bildqualität.
7. Klicken Sie auf das Download-Symbol, wenn Sie den Screenshot herunterladen wollen.

Einen Screenshot von einem Workload aufnehmen

So können Sie einen Screenshot von einem verwalteten Workload aufnehmen

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte** –> **Maschinen mit Agenten**.
2. Klicken Sie auf den Workload, von dem Sie einen Screenshot erfassen wollen.
3. Klicken Sie zuerst auf **Verwalten** und dann auf **Desktop-Screenshot erstellen**.
   Die Anzeige **Screenshot-Übertragung** wird geöffnet, wobei der entsprechende Workload vorausgewählt ist. Je nach Einstellung des Remote-Verwaltungsplans, der auf den Workload angewendet wurde, wird Ihnen der Screenshot direkt angezeigt oder Sie sehen den Screenshot erst, nachdem der jeweilige Benutzer des Remote-Workloads der Anforderung zugestimmt hat.

Mehrere verwaltete Workloads gleichzeitig beobachten

Sie können die Desktops mehrerer Remote-Workloads gleichzeitig in einem Fenster beobachten.

Hinweis
Die Anzahl der Desktops, die gleichzeitig in dem Fenster angezeigt werden können, hängt von der Größe Ihres Monitors ab.

Voraussetzungen

- In den Remote-Verwaltungsplänen, die auf die Workloads angewendet wurden, ist das NEAR-/Apple Bildschirmfreigabe-Protokoll aktiviert.
- Die Service-Quota 'Advanced Management' wurde auf den Workload angewendet.
- Für Ihr Benutzerkonto ist die Zwei-Faktor-Authentifizierung in Acronis Cyber Protect Cloud aktiviert.

So können Sie mehrere Workloads gleichzeitig beobachten

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte** –> **Alle Geräte**.
2. Wählen Sie die Workloads aus, die Sie beobachten wollen.
3. Klicken Sie auf **Mehrfachansicht**.
4. Gehen Sie folgendermaßen vor, je nachdem, ob der Connect Client auf Ihrem Workload installiert ist oder nicht:
   - Sollte der Connect Client nicht installiert sein, dann laden Sie diesen herunter, installieren Sie ihn und wählen Sie im anschließenden angezeigten Bestätigungsfenster den Befehl **Erlauben**.
   - Sollte der Connect Client bereits installiert sein, dann klicken Sie im angezeigten Bestätigungsfenster auf **Connect Client öffnen**.
5. Wählen Sie im Fenster **Authentifizierung** eine Authentifizierungsoption aus und geben Sie anschließend die benötigten Anmeldedaten ein.

Authentifizierungsoption	Beschreibung
Mit Remote-Workload-Anmeldedaten	Ihnen wird der Aufbau einer Remote-Verbindung erlaubt, nachdem Sie den Benutzernamen und das Kennwort eines administrativen Benutzers auf dem Remote-Workload angegeben haben.
Berechtigung zum Beobachten anfordern	Ihnen wird der Aufbau einer Remote-Verbindung im Beobachtungsmodus erlaubt, nachdem der Benutzer, der am Remote-Workload angemeldet ist, dies gestattet hat.

6. Wenn Sie dieselbe Authentifizierungsmethode und dieselben Anmeldedaten bei allen Verbindungen zu Remote-Workloads verwenden wollen, die Sie in Schritt 2 ausgewählt haben, wählen Sie **Auf den anderen Computern verwenden**.
7. Klicken Sie auf **Verbinden**.

   In der Symbolleiste des Mehrfachansichtfensters können Sie einen Ansichtsmodus auswählen, in dem eine Verbindung zu einem Workload hergestellt werden soll. Durch diese Aktion wird ein separates Viewer-Fenster für diesen Workload geöffnet.

Hinweis
Sollte einer der ausgewählten Workloads offline sein oder auf diesem eine veraltete Agenten-Version installiert sein, dann wird er nicht im Mehrfachansichtsfenster angezeigt.
Alle Mehrfachansichtsverbindungen mit Remote-Workloads befinden sich im Ansichtsmodus **Nur anzeigen**.

Mit nicht verwalteten Workloads arbeiten

Als nicht verwaltete Workloads werden Workloads bezeichnet, auf denen kein Schutz Agent installiert ist.

Sie können folgende Aktionen auf nicht verwalteten Remote-Workloads durchführen:

- sich über Acronis Quick Assist für Remote-Unterstützungszwecke verbinden
- sich über eine IP-Adresse für Remote-Desktop- oder Remote-Unterstützungszwecke verbinden
- Dateien mithilfe von Quick Assist zwischen Ihrem Workload und dem Remote-Workload übertragen

Hinweis
Wenn Sie eine Remote-Verbindung zu unverwalteten Workloads mit Quick Assist herstellen wollen, müssen Sie sicherstellen, dass:

- Das Advanced Management-Paket für Ihren Kunden-Mandanten aktiviert ist.
- Die Quick Assist-Applikation auf dem Remote-Workload läuft, mit dem Sie sich verbinden wollen.

Verbindungen zu unverwalteten Workloads über Acronis Quick Assist herstellen

Mit der Quick Assist-Funktion können Sie bei Bedarf eine Remote-Verbindung zu einem nicht verwalteten Workload herstellen, um Unterstützung zu leisten.

Voraussetzungen

- Das Advanced Management-Paket ist Ihrem Kunden-Mandanten zugewiesen.
- Für Ihr Benutzerkonto ist die Zwei-Faktor-Authentifizierung in Acronis Cyber Protect Cloud aktiviert.
- Der Remote-Benutzer hat die Workload-ID und den Zugriffscode von Quick Assist angegeben.
- Der Remote-Benutzer hat Acronis Quick Assist heruntergeladen und ausgeführt.

So können Sie sich über Quick Assist mit einem Workload für Remote-Unterstützungszwecke verbinden

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte** –> **Alle Geräte**.
2. Klicken Sie auf **Quick Assist**.
3. Geben Sie im Fenster **Quick Assist** die Workload-ID ein, die Ihnen der Endbenutzer gegeben hat, und wählen Sie dann die Option **Verbinden**.
4. Klicken Sie auf **Verbinden**.
5. Gehen Sie folgendermaßen vor, je nachdem, ob der Connect Client auf Ihrem Workload installiert ist oder nicht:
   - Sollte der Connect Client nicht installiert sein, dann laden Sie diesen herunter, installieren Sie ihn und wählen Sie im anschließenden angezeigten Bestätigungsfenster den Befehl **Erlauben**.
   - Sollte der Connect Client bereits installiert sein, dann klicken Sie im angezeigten Bestätigungsfenster auf **Connect Client öffnen**.
6. Geben Sie im Fenster **Authentifizierung** den Zugriffscode ein.

7. Der Connect Client wird ein neues Viewer-Fenster öffnen, in dem Sie den Desktop des Remote-Workloads sehen können. Der Viewer verfügt über eine Symbolleiste mit zusätzlichen Aktionen, die Sie auf dem Remote-Workload durchführen können (nachdem die Remote-Verbindung hergestellt wurde). Weitere Informationen finden Sie im Abschnitt '"Die Symbolleiste im Viewer-Fenster verwenden" (S. 1124)'.

Eine Verbindung zu nicht verwalteten Workloads über eine IP-Adresse herstellen

Wenn sich in Ihrem LAN ein nicht verwalteter Workload befindet, können Sie für Remote-Desktop- oder Remote-Unterstützungszwecke über dessen IP-Adresse eine Verbindung zu ihm herstellen. Für diese Verbindung ist kein Internet-Zugriff erforderlich.

Voraussetzungen

- Das Advanced Management-Paket ist Ihrem Kunden-Mandanten zugewiesen.
- Für Ihr Benutzerkonto ist die Zwei-Faktor-Authentifizierung in Acronis Cyber Protect Cloud aktiviert.

So können Sie sich über eine IP-Adresse mit einem Workload für Remote-Unterstützungszwecke verbinden

1. Gehen Sie in der Cyber Protect-Konsole zu **Alle Geräte**.
2. Klicken Sie auf **Quick Assist**.
3. Klicken Sie auf die Registerkarte **Über die IP-Adresse**.
4. Geben Sie die IP-Adresse und den Port des Workloads ein.
5. Wählen Sie (je nach Betriebssystem des Remote-Workloads) ein Verbindungsprotokoll aus – entweder RDP (für Windows-Workloads) oder Apple Bildschirmfreigabe (für macOS-Workloads).

   Hinweis
   Verbindungen über das RDP-Protokoll unterstützen die Remote-Desktop-Funktionalität, während Verbindungen über das Apple Bildschirmfreigabe-Protokoll die Remote-Desktop- und die Remote-Unterstützungsfunktionalität unterstützen.

6. Klicken Sie auf **Verbinden**.
7. Geben Sie im Fenster **Authentifizierung** die erforderlichen Anmeldedaten an.

Für Apple Bildschirmfreigabe-Verbindungen wird der Connect Client ein neues Viewer-Fenster öffnen, in dem Sie den Desktop des Remote-Workloads sehen können. Der Viewer verfügt über eine Symbolleiste mit zusätzlichen Aktionen, die Sie auf dem Remote-Workload durchführen können (nachdem die Remote-Verbindung hergestellt wurde). Weitere Informationen finden Sie im Abschnitt '"Die Symbolleiste im Viewer-Fenster verwenden" (S. 1124)'.

Dateien mithilfe von Acronis Quick Assist übertragen

Sie können die Quick Assist-Funktion verwenden, um Dateien zwischen Ihrem Workload und nicht verwalteten Workloads auszutauschen.

Voraussetzungen

- Das Advanced Management-Paket ist Ihrem Kunden-Mandanten zugewiesen.
- Für Ihr Benutzerkonto ist die Zwei-Faktor-Authentifizierung in Acronis Cyber Protect Cloud aktiviert.
- Der Remote-Benutzer hat Acronis Quick Assist heruntergeladen und ausgeführt.
- Der Remote-Benutzer hat die Computer-ID und den Zugriffscode von Quick Assist angegeben.

So können Sie Dateien mithilfe von Quick Assist zu einem Workload übertragen

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte** –> **Alle Geräte**.
2. Klicken Sie auf **Quick Assist**.
3. Geben Sie im Fenster **Quick Assist** die Workload-ID ein, die Ihnen der Endbenutzer gegeben hat, und wählen Sie dann die Option **Dateiübertragung**.
4. Klicken Sie auf **Verbinden**.
5. Gehen Sie folgendermaßen vor, je nachdem, ob der Connect Client auf Ihrem Workload installiert ist oder nicht:
   - Sollte der Connect Client nicht installiert sein, dann laden Sie diesen herunter, installieren Sie ihn und wählen Sie im anschließenden angezeigten Bestätigungsfenster den Befehl **Erlauben**.
   - Sollte der Connect Client bereits installiert sein, dann klicken Sie im angezeigten Bestätigungsfenster auf **Connect Client öffnen**.
6. Geben Sie im Fenster **Authentifizierung** den Zugriffscode ein.
7. Durchsuchen Sie im Fenster **Dateiübertragung** die Dateien und übertragen Sie diese per Drag & Drop zum gewünschten Ziel.

   Hinweis
   Die Dateien des lokalen Workloads werden im linken Fensterbereich aufgelistet, die Dateien des Remote-Workloads dagegen im rechten.
   Wenn eine Dateiübertragung beginnt, wird diese im Fensterbereich **Tasks** aufgelistet.

8. [Optional] Wenn Sie die abgeschlossenen Tasks aus dem Fensterbereich **Tasks** entfernen wollen, klicken Sie auf **Abgeschlossene Elemente bereinigen**.
9. Wenn alle Übertragungen abgeschlossen wurden, können Sie das Fenster schließen.

Die Symbolleiste im Viewer-Fenster verwenden

Wenn Sie eine Verbindung zu einem Remote-Workload hergestellt haben, können Sie die Symbolleiste des Viewer-Fensters verwenden, um unterschiedliche Aktionen schnell durchführen zu können.

Symbol	Beschreibung
	**Tatsächliche Größe** Skaliert die Desktop-Anzeige des Remote-Workloads so, dass ein Pixel des Remote-Desktops einem Pixel des Viewer-Fensters entspricht.
	**Zoom anpassen** Skaliert den Remote-Desktop des Workloads so, dass er genau in das Viewer-Fenster passt.
	**Sperren** und **Bildschirm entsperren** Zeigt einen Platzhalter auf der Anzeige des Remote-Workloads an, damit der entsprechende Remote-Benutzer Ihre Aktionen nicht sieht.
	**Screenshot erstellen** Speichern Sie ein Abbild des Desktops vom Remote-Server als lokale Datei.
	**Anzeige auswählen** Wählen Sie die Remote-Workload-Anzeige aus, die Sie einsehen wollen, und die gewünschte Auflösung. Für Apple Bildschirmfreigabe-Verbindungen zu macOS sowie NEAR-Verbindungen zu einem beliebigen anderen Betriebssystem verfügbar.
	**Bildqualität** Passt die Bildqualität der Remote-Anzeige bei Apple Bildschirmfreigabe-Verbindungen von Schwarz-Weiß bis zur höchstmöglichen Qualität an.
	**NEAR-Bildqualität** Passt das Qualitäts-/Performance-Verhältnis bei NEAR-Verbindungen an. Die linke Seite des Schiebereglers ('Glatt') gibt der Performance Vorrang vor der Bildqualität, während die rechte Seite ('Scharf') die Qualität der Remote-Desktop-Anzeige optimiert, worunter jedoch die Performance leiden kann.

Symbol	Beschreibung
	**Strg+Alt+Entf senden** Sendet die Tastenkombination Strg+Alt+Entf an den Remote-Workload. Für Windows- und Linux-Workloads verfügbar.
	**Dateiübertragung** Öffnet das Fenster des Datei-Managers, um Dateien zwischen dem Remote-Workload und dem lokalen Workload austauschen zu können. Für NEAR-Verbindungen verfügbar.
	**Symbolleiste anheften** Schaltet das automatische Ausblenden der Viewer-Symbolleiste aus. Für Windows-Workloads verfügbar.
	**Vollbild** Wechselt in den Vollbildmodus und skaliert den Remote-Workload so, dass er Ihre lokale Anzeige vollständig ausfüllt. Für Windows-Workloads verfügbar.
	**Schließen** Schließt das Viewer-Fenster und beendet die Fernsteuerungssitzung. Für Windows-Workloads verfügbar.

Je nach Verbindungstyp stehen Ihnen zusätzliche Optionen zur Verfügung, wenn Sie auf das Symbol **Andere(s)** klicken.

Option	Beschreibung
Aufzeichnung starten / Aufzeichnung stoppen	Zeichnen Sie die aktuelle Remote-Desktop-Sitzung auf. Sitzungsaufzeichnungen werden als .crec Dateien auf dem lokalen Workload gesichert. Sie können .crec Dateien mit Acronis Connect Client öffnen. Für NEAR-Verbindungen verfügbar
Automatische Zwischenablage-Synchronisierung	Wenn diese Option eingeschaltet ist, wird der Client Ihre lokale Zwischenablage und die Zwischenablage des Remote-Computers automatisch synchronisieren. Für NEAR- und Apple Bildschirmfreigabe-Verbindungen verfügbar
Zwischenablage senden **Zwischenablage abrufen**	Der Befehl **Zwischenablage senden** ersetzt den Inhalt der Zwischenablage des Remote-Computers durch den Inhalt der

Option	Beschreibung
	lokalen Zwischenablage. Der Befehl **Zwischenablage abrufen** übermittelt den Inhalt der Zwischenablage des Remote-Computers an die lokale Zwischenablage.
Smart Keyboard / Raw-Tasten / Raw-Tasten mit allen Tastaturkurzbefehlen	Ändert den Tastatur-Eingabemodus für die aktuelle Verbindung. **Smart Keyboard** – der Client überträgt die Unicode-Steuerzeichen der lokal eingegebenen Tasten an den Remote-Computer **Raw-Tasten** – der Client verwendet die Raw-Codes der Tasten, die Sie auf der Tastatur drücken. **Raw-Tasten mit allen Tastaturkurzbefehlen** – der Client deaktiviert die lokalen System-Tastaturkurzbefehle, damit auch diese an das Remote-Betriebssystem übertragen werden.
Tastaturfokus beim Überfahren mit der Maus	Wenn diese Option aktiviert ist, erfasst der Client die Tastatureingaben nur, wenn sich Ihr lokaler Mauszeiger über dem Viewer-Fenster befindet. Wenn diese Funktion deaktiviert ist, erfasst der Client Ihre Tastatureingaben, wenn sein Fenster aktiv ist.
Verbindungsinformationen anzeigen / Verbindungsinformationen ausblenden	Wenn die Option **Verbindungsinformationen anzeigen** aktiviert ist, wird über der Remote-Desktop-Anzeige ein kleines Informationsfenster eingeblendet, das die wichtigsten Informationen zur aktuellen Verbindung anzeigt.
Remote-Sound	Ermöglicht es dem Client, die Tonausgabe vom Remote-Computer zum lokalen Computer umzuleiten. Für NEAR-Verbindungen verfügbar
Einstellungen	Konfigurieren Sie die Einstellungen des Connect Clients. Weitere Informationen finden Sie im Abschnitt '"Die Connect Client-Einstellungen konfigurieren" (S. 1127)'.

Remote-Sitzungen aufzeichnen und wieder abspielen

Sie können eine Remote-Sitzung über NEAR in Acronis Connect Client aufzeichnen.

So können Sie eine Remote-Sitzung aufzeichnen

1. Klicken Sie in der Viewer-Symbolleiste von Connect Client auf auf **Andere(s)** und wählen Sie **Aufzeichnung starten**.
2. Wählen Sie einen Namen und einen Speicherort für die Aufzeichnung.

Standardmäßig wird die Datei mit dem aktuellen Datum und der aktuellen Uhrzeit benannt und im Ordner **Dokumente** im Stammverzeichnis des aktuellen Benutzers gesichert. Während die Aufzeichnung aktiv ist, wird in der **Viewer**-Symbolleiste ein blinkendes rotes Kreis über der oberen rechten Ecke des Remote-Anzeige und ein Timer für die Aufnahmedauer angezeigt.

3. Um die Aufzeichnung zu stoppen, klicken Sie auf **Andere(s)** und dann auf **Aufzeichnung stoppen**. Auf einem Mac können Sie auch in der Symbolleiste auf **Stop** klicken.
   Alle .crec Dateien, die von Acronis Connect Client erstellt wurden, werden standardmäßig mit Acronis Connect Client geöffnet.

So können Sie eine Aufzeichnung abspielen

1. Suchen Sie die entsprechende Aufnahmedatei.
2. Öffne es.
   Der Recording Player von Acronis Connect Client wird geöffnet. Beachten Sie, dass es nicht möglich ist, durch die Aufzeichnung zu spulen. Wenn Sie einen bestimmten Aufnahme-Moment suchen, müssen Sie warten, bis dieser vom Player erreicht wird.
3. [Optional] Sie können Symbole **<<** und **>>** in der Wiedergabesteuerung verwenden, um die Abspielgeschwindigkeit zu beeinflussen.
   Die Aufzeichnung wird als eine Folge von Ereignissen gespeichert, die während einer Verbindung zum und vom Remote-Server übertragen wurden. Dies gewährleistet die beste Aufzeichnungsqualität bei minimaler Dateigröße. Dies bedeutet jedoch auch, dass es nicht möglich ist, durch die Aufzeichnung zu navigieren. Zurzeit ist es auch nicht möglich, die Aufzeichnungen in ein anderes Videoformat zu konvertieren.

Die Connect Client-Einstellungen konfigurieren

Nachdem Sie den Connect Client auf Ihrem Workload installiert haben, können Sie dessen Einstellungen nach Ihren Vorstellungen konfigurieren.

So können Sie die Einstellungen des Connect Clients konfigurieren

1. Suchen Sie im Startmenü den **Connect Client** und starten Sie diesen.
2. Konfigurieren Sie die Einstellungen auf der Registerkarte **Allgemein**.

Option	Beschreibung
Ausführliche Protokolle schreiben	Wählen Sie diese Option, um dem Connect Client zu erlauben, ausführliche Protokolle zu schreiben. Wenn diese Option deaktiviert ist, wird der Client nur allgemeine Informationen in die Protokolldatei schreiben.
Proxy-Einstellungen	Bestimmen Sie, ob Sie den Standard-Proxy des Systems verwenden oder einen benutzerdefinierten SOCKSS-Proxy konfigurieren wollen.

3. Konfigurieren Sie die Einstellungen auf der Registerkarte **Viewer**.

Option	Beschreibung
Eine Bestätigung anfordern, wenn ein Viewer geschlossen wird	Aktivieren Sie diese Option, wenn Sie wollen, dass der Connect Client eine Bestätigungsmeldung anzeigt, wenn Sie versuchen, das Viewer-Fenster zu schließen. So soll ein versehentliches Schließen verhindert werden.
Wenn minimiert	Bestimmen Sie, ob die Viewer-Aktivität beim Minimieren pausiert werden soll, um die CPU-Auslastung zu verringern.
Wenn maximiert	Bestimmen Sie, ob der Vollbildmodus aktiviert werden soll, wenn das Fenster maximiert wird.
Zwischenablage-Übertragung	Aktivieren Sie, dass der Indikator für die Zwischenablage-Übertragung im Viewer-Fenster angezeigt wird, wenn Sie Texte oder Bilder kopieren oder einfügen.
Tastaturmodus	Aktivieren Sie, dass der Indikator für den Eingabemodus im Fenstertitel des Viewers angezeigt wird, wenn Maus- und Tastaturereignisse an die Remote-Maschine gesendet werden.
Zwischenablage	Wählen Sie **Zwischenablage automatisch synchronisieren**, um die automatische Zwischenablage-Synchronisierung zu aktivieren (sofern verfügbar).
Tastaturereignisse senden	Bestimmen Sie, ob Ihre lokale Tastatureingabe immer erfasst werden soll, wenn das Connect Client-Fenster aktiv ist, oder nur, wenn sich Ihr lokaler Mauszeiger über dem Fenster befindet.
Hintergrundfarbe des Viewers	Ändern Sie bei Bedarf die Hintergrundfarbe des Viewer-Fensters.
Automatisch neu verbinden	Wählen Sie **Aktivieren, um die Verbindung automatisch wiederherzustellen**, wenn der Connect Client eine unterbrochene Verbindung automatisch wiederherstellen soll.
H.264	Sie können die Verwendung von Hardware-Decodern deaktivieren.
Schließen, wenn im Leerlauf	Bestimmen Sie, nach welchem Zeitraum das Viewer-Fenster geschlossen werden soll, wenn es zwischenzeitlich inaktiv war.

4. Konfigurieren Sie die Einstellungen auf der Registerkarte **Tastatur**.

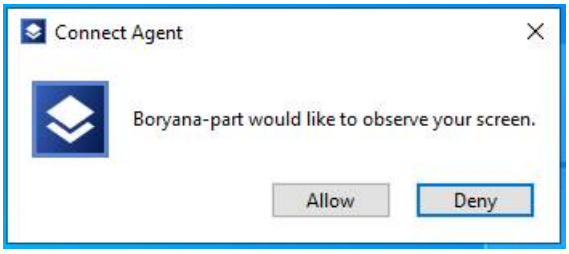
Option	Beschreibung
Sondertasten-Zuordnungen	Ändern Sie das Verhalten der Zusatztasten mit einem Pop-up-Menü. Diese Einstellungen werden jeweils für die NEAR-, Apple Bildschirmfreigabe- und RDP-Verbindungen getrennt gespeichert.
Eingabemodus	Wählen Sie für jede Verbindungsart (im Kopf des Fensterbereichs ausgewählt) den standardmäßigen Tastatur-Eingabemodus.

5. Klicken Sie auf **OK**.

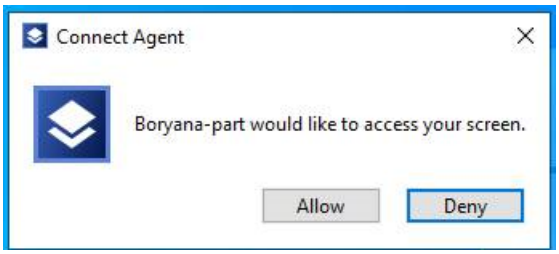
Die Remote-Desktop-Notifier

Der Connect Agent zeigt in folgenden Fällen Aktionsdialoge (Notifier) auf dem Desktop des Remote-Workloads an:

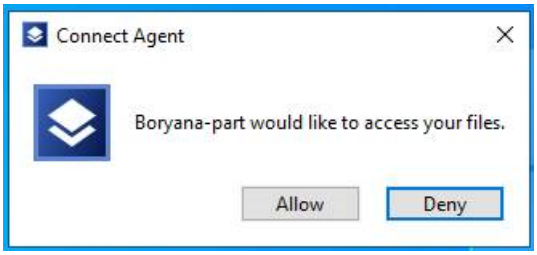
- wenn Sie versuchen, eine Remote-Verbindung zum Workload herzustellen, indem Sie die 'Berechtigung zum Beobachten' anfordern. Der Benutzer, der auf dem Remote-Workload lokal angemeldet ist, kann die Anforderung entweder zulassen oder ablehnen.



- wenn Sie versuchen, eine Remote-Verbindung zum Workload herzustellen, indem Sie die 'Berechtigung zur Steuerung' anfordern. Der Benutzer, der auf dem Remote-Workload lokal angemeldet ist, kann die Anforderung entweder zulassen oder ablehnen.



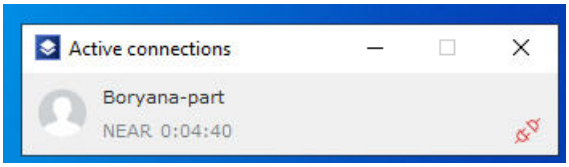
- wenn Sie versuchen, Dateien zwischen Ihrem Workload und dem Remote-Workload auszutauschen, indem Sie die 'Berechtigung zur Übertragung von Dateien' anfordern Der Benutzer, der auf dem Remote-Workload lokal angemeldet ist, kann die Anforderung entweder zulassen oder ablehnen.



Wenn Sie eine Remote-Desktop-Verbindung zu einem Workload aufbauen, wird dem Benutzer, der auf dem Workload angemeldet ist, ein anderer Verbindungsmelder angezeigt, der folgende Informationen enthält:

- der Name des Benutzers, der remote verbunden ist
- das Verbindungsprotokoll, das für den Aufbau der Remote-Verbindung verwendet wird
- die Dauer der Remote-Verbindung

Der Benutzer, der lokal auf dem Remote-Workload angemeldet ist, kann die Verbindung jederzeit beenden, indem er auf das Symbol **Trennen** oder das Symbol **Schließen** klickt.



Den Zustand und die Performance von Workloads überwachen

Sie können die Systemparameter und den Zustand der Workloads in Ihrem Unternehmen überwachen. Wenn ein Parameter außerhalb der Norm liegt, werden Sie umgehend benachrichtigt und können das Problem schnell beheben. Sie können außerdem benutzerdefinierte Alarmmeldungen und automatische Antwortaktionen konfigurieren. Dies sind Aktionen, die automatisch durchgeführt werden, um Anomalien beim Workload-Verhalten zu beheben.

Hinweis
Für die Monitoring-Funktionalität muss der Schutz Agent in der Version 15.0.35324 oder höher auf den Workloads installiert sein.

Monitoring-Pläne

Wenn Sie die Performance-, Hardware-, Software-, System- und Sicherheitsparameter Ihrer verwalteten Workloads überwachen wollen, müssen Sie einen Monitoring-Plan auf diese anwenden. Die Monitoring-Pläne bestehen aus unterschiedlichen Monitoren, die Sie aktivieren und konfigurieren können. Einige Monitore unterstützen den Monitoring-Typ 'Anomalie-basiert'. Weitere Informationen über Monitoring-Pläne finden Sie im Abschnitt '"Monitoring-Pläne" (S. 1170)'. Weitere Informationen zu den verfügbaren Monitoren, die Sie in den Monitoring-Plänen konfigurieren können, finden Sie im Abschnitt '"Konfigurierbare Monitore" (S. 1132)'.

Wenn der Agent aus irgendeinem Grund keine Daten von einem Workload sammeln kann, wird das System eine Alarmmeldung generieren.

Monitoring-Typen

Sie müssen den Monitoring-Typ für jeden Monitor konfigurieren, den Sie im Plan aktivieren. Der Monitoring-Typ bestimmt den Algorithmus, den der Monitor verwenden wird, um das normale Verhalten und die Abweichung des Workloads zu bestimmen. Es gibt zwei verschiedene Monitoring-Typen: Grenzwert-basiert und Anomalie-basiert. Einige Monitore unterstützen nur den Monitoring-Typ 'Grenzwert-basiert'.

Das Grenzwert-basierte Monitoring verfolgt, ob die Werte der Parameter über oder unter einem von Ihnen konfigurierten Grenzwert liegen. Bei diesem Monitoring-Typ sind Sie dafür verantwortlich, die richtigen Grenzwerte für die Workloads zu definieren. Das System bestimmt das normale Verhalten nur anhand dieser statischen Grenzwerte und ohne andere spezifische Bedingungen, die das Verhalten verursachen könnten, zu berücksichtigen. Aus diesem Grund ist das Grenzwert-basierte Monitoring im Vergleich zum Anomalie-basierten Monitoring möglicherweise weniger genau.

Das Anomalie-basierte Monitoring verwendet Maschinelles Lernen (ML), um die normalen Verhaltensmuster eines Workloads zu erstellen und dann davon abweichendes Verhalten zu erkennen. Weitere Informationen finden Sie im Abschnitt '"Anomalie-basiertes Monitoring" (S. 1132)'.

Anomalie-basiertes Monitoring

Das Anomalie-basierte Monitoring verwendet Machine Learning-Modelle, um die normalen Verhaltensmuster für einen Workload zu festzulegen und dann davon abweichende Anomalien (unerwartete Spitzen in den Zeitseriendaten) im Verhalten des Workloads zu erkennen. Wenn Sie diesen Monitoring-Typ aktivieren, wird das System ein Modell erstellen und damit beginnen, sich selbst zu trainieren und das Modell für den spezifischen Workload anzupassen. Dies geschieht anhand der Daten, die das System vom Workload sammelt. Das bedeutet, dass die Daten zu Beginn des Trainingszeitraums möglicherweise nicht ganz genau sind. Um ein zuverlässiges Modell zu erstellen, benötigt das Modell mindestens drei Wochen Training. Während das System mehr Daten sammelt und historische Datensätze analysiert, verfeinert es nach und nach sein Modell und erstellt die dynamischen oberen und unteren Grenzwerte für jede Metrik des Workloads. Dieser Monitoring-Typ ist im Vergleich zum Grenzwert-basierten Monitoring flexibler, weil das System die Werte der Parameter und deren Kontext überwacht. So kann es beispielsweise normal sein, dass ein bestimmter Workload zu bestimmten Stunden des Tages stärker ausgelastet ist. Ein Grenzwert-basierter Monitoring-Typ würde dies fälschlicherweise als anormales Verhalten interpretieren und eine Alarmmeldung auslösen.

Sie können Sie die Machine Learning-Modelle eines Workloads zurücksetzen. In diesem Fall wird das System alle Daten und Modelle für diejenigen Monitore löschen, die auf den Workload angewendet wurden. Weitere Informationen finden Sie im Abschnitt '"Die Machine Learning-Modelle zurücksetzen" (S. 1181)'.

Unterstützte Plattformen für das Monitoring

Die Monitoring-Funktionalität wird für die nachfolgenden Betriebssysteme unterstützt.

Unterstützte Windows-Versionen	Unterstützte macOS-Versionen
• Windows 7 SP1 • Windows 8, 8.1 • Windows 10 • Windows 11 • Windows Server 2008 R2 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 • Windows Server 2019 • Windows Server 2022	• macOS 10.14 (Mojave) • macOS 10.15 (Catalina) • macOS 11.x (Big Sur) • macOS 12.x (Monterey) • macOS 13.x (Ventura)

Konfigurierbare Monitore

Die Monitoring-Funktionalität unterstützt folgende Monitore, die in sechs Kategorien unterteilt werden können: Hardware, Performance, Software, System, Sicherheit und Benutzerdefiniert.

Monitor	Beschreibung	Unterstützte Betriebssysteme	Häufigkeit der Datensammlung	Unterstützung des Anomalie-basierten Monitorings	Verfügbarkeit im Standard Protection- oder Advanced Management-Paket
Hardware					
Laufwerksspeicherplatz	Überwacht den freien Speicherplatz auf einem bestimmten Laufwerk des Workloads.	Windows macOS	1 Minute	Ja	Standard Protection
CPU-Temperatur	Überwacht die CPU-Temperatur.	Windows macOS	30 Sek.	Ja	Advanced Management
GPU-Temperatur	Überwacht die GPU-Temperatur.	Windows macOS	30 Sek.	Ja	Advanced Management
Hardware-Änderungen	Überwacht Hardware-Änderungen – wie etwa das Hinzufügen, Entfernen oder Ersetzen von Hardware auf einem Workload	Windows macOS	24 Stunden	Nein	Standard Protection
Performance					
CPU-Nutzung	Überwacht die gesamte CPU-Nutzung (durch alle CPUs des Workloads).	Windows macOS	30 Sek.	Ja	Advanced Management
Arbeitsspeicher-Nutzung	Überwacht die gesamte Arbeitsspeicher-Nutzung (durch alle	Windows macOS	30 Sek.	Ja	Advanced Management

Monitor	Beschreibung	Unterstützte Betriebssysteme	Häufigkeit der Datensammlung	Unterstützung des Anomalie-basierten Monitorings	Verfügbarkeit im Standard Protection- oder Advanced Management-Paket
	Speichersteckplätze auf dem Workload).				
Laufwerk-Übertragungsrate	Überwacht die Lese- und Schreibgeschwindigkeit von jedem physischen Laufwerk auf dem Workload.	Windows macOS	30 Sek.	Ja	Advanced Management
Netzwerknutzung	Überwacht den ein- und ausgehenden Datenverkehr für jeden Netzwerkadapter des Workloads.	Windows macOS	30 Sek.	Ja	Advanced Management
CPU-Nutzung nach Prozess	Überwacht die CPU-Nutzung durch einen bestimmten Prozess.	Windows macOS	30 Sek.	Nein	Advanced Management
Arbeitsspeicher-Nutzung nach Prozess	Überwacht die Arbeitsspeicher-Nutzung durch den ausgewählten Prozess.	Windows macOS	30 Sek.	Nein	Advanced Management
Laufwerk-Übertragungsrate nach Prozess	Überwacht die Lese- und Schreibgeschwindigkeit des ausgewählten Prozesses.	Windows macOS	30 Sek.	Nein	Advanced Management

Monitor	Beschreibung	Unterstützte Betriebssysteme	Häufigkeit der Datensammlung	Unterstützung des Anomalie-basierten Monitorings	Verfügbarkeit im Standard Protection- oder Advanced Management-Paket
Netzwerknutzung nach Prozess	Überwacht den ein- und ausgehenden Datenverkehr des ausgewählten Prozesses.	Windows macOS	30 Sek.	Nein	Advanced Management
Software					
Windows-Dienst-Status	Überwacht den Status des ausgewählten Windows-Dienstes ('Wird ausgeführt' oder 'Gestoppt').	Windows	30 Sek.	Nein	Advanced Management
Prozessstatus	Überwacht den Status des ausgewählten Prozesses ('Wird ausgeführt' oder 'Gestoppt').	Windows macOS	30 Sek.	Nein	Advanced Management
Installierte Software	Überwacht die Installation, Aktualisierung oder Löschung von Software-Applikationen.	Windows macOS	24 Stunden	Nein	Advanced Management
System					
Letzter System-Neustart	Überwacht, wann der Workload neu gestartet wurde.	Windows macOS	1 Stunde	Nein	Standard Protection
Windows-Ereignisprotokoll	Überwacht bestimmte	Windows	10 min	Nein	Advanced Managem

Monitor	Beschreibung	Unterstützte Betriebssysteme	Häufigkeit der Datensammlung	Unterstützung des Anomalie-basierten Monitorings	Verfügbarkeit im Standard Protection- oder Advanced Management-Paket
	geschäftskritische Ereignisse in den Windows-Ereignisprotokollen.				ent
Größe der Dateien und Ordner	Überwacht die Gesamtgröße von ausgewählten Dateien oder Ordnern.	Windows macOS	10 min	Nein	Standard Protection
Sicherheit					
Windows Update-Status	Überwacht den Windows Update-Status des Workloads und ob auf diesem die neuesten Updates installiert sind.	Windows	15 min	Nein	Advanced Management
Firewall-Status	Überwacht den Status der integrierten Firewall oder der Firewall eines Drittanbieters, die auf dem Workload installiert ist.	Windows macOS	5 min	Nein	Advanced Management
Antimalware-Software-Status	Überwacht den Status der integrierten Antimalware-	Windows macOS	5 min	Nein	Advanced Management

Monitor	Beschreibung	Unterstützte Betriebssysteme	Häufigkeit der Datensammlung	Unterstützung des Anomalie-basierten Monitorings	Verfügbarkeit im Standard Protection- oder Advanced Management-Paket
	Software oder der Antimalware-Software eines Drittanbieters, die auf dem Workload installiert ist.				
Fehlgeschlagene Anmeldungen	Überwacht fehlgeschlagene Anmeldeversuche auf dem Workload.	Windows	1 Stunde	Nein	Advanced Management
AutoRun-Status	Überwacht, ob die AutoRun-Funktion für Wechselmedien aktiviert ist.	Windows	1 Stunde	Nein	Advanced Management
Benutzerdefiniert					
Benutzerdefiniert	Überwacht benutzerdefinierte Objekte durch die Ausführung von Skripten.	Windows macOS	benutzerdefiniert	Nein	Advanced Management

Die Einstellungen des Monitors 'Laufwerksspeicherplat'

Der Monitor **Laufwerksspeicherplatz** überwacht den freien Speicherplatz auf einem bestimmten Laufwerk des Workloads.

Hinweis
Bei der Berechnung des Speicherplatzes verwendet der Monitor sowohl für Windows- als auch für macOS-Workloads Binärbytes (1024 Byte pro KB, 1024 KB pro MB und 1024 MB pro GB).

Sie können folgende Einstellungen für den Monitor konfigurieren.

Einstellung	Beschreibung
Grenzwert-basiertes Monitoring	
Laufwerk	Das Laufwerk, das Sie überwachen wollen. Die nachfolgenden Werte sind verfügbar. • **Systemlaufwerk** —Dies ist der Standardwert. • **Jedes Laufwerk**
Operator	Der Operator ist eine bedingte Funktion, die definiert, wie die Performance der Metrik gemessen werden soll. Die nachfolgenden Werte sind verfügbar. • **Weniger als** —Dies ist der Standardwert. • **Kleiner als oder ist gleich**
Grenzwert für freien Laufwerksspeicherplatz	Der Grenzwert und der **Operator**-Wert bestimmen die normale Performance der überwachten Metrik. Wenn der Wert der überwachten Metrik außerhalb der Norm liegt, wird das System eine Alarmmeldung generieren. Geben Sie einen ganzzahligen Wert im Bereich 1–100 (%) ein. Der Standardwert ist 20.
Wechsellaufwerke einschließen	Diese Einstellung ist verfügbar, wenn der Wert **Laufwerk** auf **Jedes Laufwerk** steht. Wählen Sie diese Einstellung, wenn Sie Wechsellaufwerke (wie USB-Sticks) zum Monitoring hinzufügen wollen. Die Einstellung ist standardmäßig deaktiviert.
Zeitraum	Das System wird nur dann eine Alarmmeldung für ein erkanntes Problem generieren, wenn der Metrikwert während des spezifizierten Zeitraums außerhalb der Norm liegt. Geben Sie einen ganzzahligen Wert im Bereich 1–60 (min) ein. Der Standardwert ist 30.
Anomalie-basiertes Monitoring	
Laufwerk	Das Laufwerk, das Sie überwachen wollen. Die nachfolgenden Werte sind verfügbar. • **Systemlaufwerk** —Dies ist der Standardwert. • **Jedes Laufwerk**
Trainingszeitraum für das Modell	Der Zeitraum, in dem das System die Machine Learning-Modelle mithilfe der Daten trainieren wird, die von den Agenten gesammelt wurden, und dann das normale Verhaltensmuster des Workloads erstellen wird. Je länger der Trainingszeitraum für

Einstellung	Beschreibung
	das Modell ist, desto präziser wird das Langzeitverhaltensmuster sein, welches das System erstellen wird. Wir empfehlen eine Mindesttrainingszeit für das Modell von einundzwanzig Tagen. Geben Sie einen ganzzahligen Wert (Tage) ein. Der Standardwert ist 21.
Alarmmeldungen bei Anomalien während des Trainingszeitraums erhalten	Wenn Sie diese Einstellung wählen, werden Sie während des Modell-Trainingszeitraums Alarmmeldungen über Anomalien erhalten. Diese Alarmmeldungen können jedoch auch falsch sein, weil die Modelle noch trainiert werden und daher möglicherweise nicht genau genug sind. Die Einstellung ist standardmäßig vorausgewählt.
Empfindlichkeitsstufe	Die Empfindlichkeitsstufe dient als eine Art Vorfilter für Anomalien, sofern deren Werte innerhalb eines bestimmten Bereichs liegen. Dieser Filter arbeitet unabhängig vom Anomalie-Erkennungsalgorithmus. Er soll verhindern, dass Anomalien, die innerhalb des spezifizierten Bereichs liegen, vom Anomalie-Erkennungsalgorithmus verarbeitet werden. Während des Trainingszeitraums: 1. Der Algorithmus wird anhand der Daten trainiert, die während des Trainings gesammelt werden. 2. Der Algorithmus führt die Anomalie-Erkennung anhand der Trainingsdaten durch. 3. Es wird ein Filterprozess angewendet, der auf dem Mittelwert und der Standardabweichung basiert. 4. Alle Anomalien, die im spezifizierten Intervall liegen, werden gefiltert. 5. Aus den verbleibenden anomalen Datenpunkten wird die Anomalie mit der niedrigsten Anomaliestufe ausgewählt. Diese Stufe (eine Gleitkommazahl zwischen 0 und 1) wird im Modell aufgezeichnet. Während der Vorhersage: 1. Der Algorithmus sagt Anomalien bei den Inferenzdaten voraus. 2. Die vorhergesagten Anomalien werden anhand des Mittelwerts und der Standardabweichung sowie entsprechend der Empfindlichkeitsstufe gefiltert. 3. Die verbleibenden Anomalien werden nach folgendem Prinzip weiter gefiltert: Werte oberhalb der Grenzwertstufe werden als Anomalie betrachtet, während Werte unterhalb der Grenzwertstufe als normales Verhalten angesehen

Einstellung	Beschreibung
	werden. Die nachfolgenden Werte sind verfügbar. • **Niedrig** — Die niedrige Stufe entspricht dem Mittelwert und dem Wert der Standardabweichung. • **Normal** — Dies ist der Standardwert. Die normale Stufe entspricht dem Mittelwert und dem zweifachen Wert der Standardabweichung. • **Hoch** — Die hohe Stufe entspricht dem Mittelwert und dem dreifachen Wert der Standardabweichung.
Anomalie-Dauer	Das System wird nur dann eine Alarmmeldung für eine erkannte Anomalie generieren, wenn das anormale Verhalten über den angegebenen Zeitraum anhält. Der Standardwert ist 30 Minuten.

Die Einstellungen des Monitors 'CPU-Temperatur'

Der Monitor **CPU-Temperatur** überwacht die CPU-Temperatur des Workloads.

Sie können folgende Einstellungen für den Monitor konfigurieren.

Einstellung	Beschreibung
Grenzwert-basiertes Monitoring	
Die CPU-Temperatur wurde überschritten (°C)	Der Höchstwert der überwachten Metrik. Wenn der Wert überschritten wird, wird das System einen Alarm generieren. Geben Sie einen ganzzahligen Wert (C°) ein. Der Standardwert ist 80.
Zeitraum	Das System wird nur dann eine Alarmmeldung für ein erkanntes Problem generieren, wenn der Metrikwert während des spezifizierten Zeitraums außerhalb der Norm liegt. Geben Sie einen ganzzahligen Wert im Bereich 1–60 (min) ein. Der Standardwert ist 5.
Anomalie-basiertes Monitoring	
Trainingszeitraum für das Modell	Der Zeitraum, in dem das System die Machine Learning-Modelle mithilfe der Daten trainieren wird, die von den Agenten gesammelt wurden, und dann das normale Verhaltensmuster des Workloads erstellen wird. Je länger der Trainingszeitraum für das Modell ist, desto präziser wird das Langzeitverhaltensmuster sein, welches das System erstellen wird. Wir empfehlen eine Mindesttrainingszeit für das Modell von einundzwanzig Tagen.

Einstellung	Beschreibung
	Geben Sie einen ganzzahligen Wert (Tage) ein. Der Standardwert ist 21.
Empfindlichkeitsstufe	Die Empfindlichkeitsstufe dient als eine Art Vorfilter für Anomalien, sofern deren Werte innerhalb eines bestimmten Bereichs liegen. Dieser Filter arbeitet unabhängig vom Anomalie-Erkennungsalgorithmus. Er soll verhindern, dass Anomalien, die innerhalb des spezifizierten Bereichs liegen, vom Anomalie-Erkennungsalgorithmus verarbeitet werden. Während des Trainingszeitraums: 1. Der Algorithmus wird anhand der Daten trainiert, die während des Trainings gesammelt werden. 2. Der Algorithmus führt die Anomalie-Erkennung anhand der Trainingsdaten durch. 3. Es wird ein Filterprozess angewendet, der auf dem Mittelwert und der Standardabweichung basiert. 4. Alle Anomalien, die im spezifizierten Intervall liegen, werden gefiltert. 5. Aus den verbleibenden anomalen Datenpunkten wird die Anomalie mit der niedrigsten Anomaliestufe ausgewählt. Diese Stufe (eine Gleitkommazahl zwischen 0 und 1) wird im Modell aufgezeichnet. Während der Vorhersage: 1. Der Algorithmus sagt Anomalien bei den Inferenzdaten voraus. 2. Die vorhergesagten Anomalien werden anhand des Mittelwerts und der Standardabweichung sowie entsprechend der Empfindlichkeitsstufe gefiltert. 3. Die verbleibenden Anomalien werden nach folgendem Prinzip weiter gefiltert: Werte oberhalb der Grenzwertstufe werden als Anomalie betrachtet, während Werte unterhalb der Grenzwertstufe als normales Verhalten angesehen werden. Die nachfolgenden Werte sind verfügbar. • **Niedrig** — Die niedrige Stufe entspricht dem Mittelwert und dem Wert der Standardabweichung. • **Normal** — Dies ist der Standardwert. Die normale Stufe entspricht dem Mittelwert und dem zweifachen Wert der Standardabweichung. • **Hoch** — Die hohe Stufe entspricht dem Mittelwert und dem dreifachen Wert der Standardabweichung.

Einstellung	Beschreibung
Anomalie-Dauer	Das System wird nur dann eine Alarmmeldung für eine erkannte Anomalie generieren, wenn das anormale Verhalten über den angegebenen Zeitraum anhält. Geben Sie einen ganzzahligen Wert im Bereich 1–60 (min) ein. Der Standardwert ist 15.

Die Einstellungen des Monitors 'GPU-Temperatur'

Der Monitor **GPU-Temperatur** überwacht die GPU-Temperatur des Workloads.

Sie können folgende Einstellungen für den Monitor konfigurieren.

Einstellung	Beschreibung
Grenzwert-basiertes Monitoring	
Die GPU-Temperatur wurde überschritten	Der Höchstwert der überwachten Metrik. Wenn der Wert überschritten wird, wird das System eine Anomalie erkennen. Geben Sie einen ganzzahligen Wert (C°) ein. Der Standardwert ist 80.
Zeitraum	Das System wird nur dann eine Alarmmeldung für ein erkanntes Problem generieren, wenn der Metrikwert während des spezifizierten Zeitraums außerhalb der Norm liegt. Geben Sie einen ganzzahligen Wert im Bereich 1–60 (min) ein. Der Standardwert ist 5.
Anomalie-basiertes Monitoring	
Trainingszeitraum für das Modell	Der Zeitraum, in dem das System die Machine Learning-Modelle mithilfe der Daten trainieren wird, die von den Agenten gesammelt wurden, und dann das normale Verhaltensmuster des Workloads erstellen wird. Je länger der Trainingszeitraum für das Modell ist, desto präziser wird das Langzeitverhaltensmuster sein, welches das System erstellen wird. Wir empfehlen eine Mindesttrainingszeit für das Modell von einundzwanzig Tagen. Geben Sie einen ganzzahligen Wert (Tage) ein. Der Standardwert ist 21.
Empfindlichkeitsstufe	Die Empfindlichkeitsstufe dient als eine Art Vorfilter für Anomalien, sofern deren Werte innerhalb eines bestimmten Bereichs liegen. Dieser Filter arbeitet unabhängig vom Anomalie-Erkennungsalgorithmus. Er soll verhindern, dass Anomalien, die innerhalb des spezifizierten Bereichs liegen, vom Anomalie-Erkennungsalgorithmus verarbeitet werden.

Einstellung	Beschreibung
	Während des Trainingszeitraums: 1. Der Algorithmus wird anhand der Daten trainiert, die während des Trainings gesammelt werden. 2. Der Algorithmus führt die Anomalie-Erkennung anhand der Trainingsdaten durch. 3. Es wird ein Filterprozess angewendet, der auf dem Mittelwert und der Standardabweichung basiert. 4. Alle Anomalien, die im spezifizierten Intervall liegen, werden gefiltert. 5. Aus den verbleibenden anomalen Datenpunkten wird die Anomalie mit der niedrigsten Anomaliestufe ausgewählt. Diese Stufe (eine Gleitkommazahl zwischen 0 und 1) wird im Modell aufgezeichnet. Während der Vorhersage: 1. Der Algorithmus sagt Anomalien bei den Inferenzdaten voraus. 2. Die vorhergesagten Anomalien werden anhand des Mittelwerts und der Standardabweichung sowie entsprechend der Empfindlichkeitsstufe gefiltert. 3. Die verbleibenden Anomalien werden nach folgendem Prinzip weiter gefiltert: Werte oberhalb der Grenzwertstufe werden als Anomalie betrachtet, während Werte unterhalb der Grenzwertstufe als normales Verhalten angesehen werden. Die nachfolgenden Werte sind verfügbar. • **Niedrig** — Die niedrige Stufe entspricht dem Mittelwert und dem Wert der Standardabweichung. • **Normal** — Dies ist der Standardwert. Die normale Stufe entspricht dem Mittelwert und dem zweifachen Wert der Standardabweichung. • **Hoch** — Die hohe Stufe entspricht dem Mittelwert und dem dreifachen Wert der Standardabweichung.
Anomalie-Dauer	Das System wird nur dann eine Alarmmeldung für eine erkannte Anomalie generieren, wenn das anormale Verhalten über den angegebenen Zeitraum anhält. Geben Sie einen ganzzahligen Wert im Bereich 1–60 (min) ein. Der Standardwert ist 15.

Die Einstellungen des Monitors 'Hardware-Änderungen'

Der Monitor **Hardware-Änderungen** überwacht Hardware-Änderungen – wie etwa das Hinzufügen, Entfernen oder Ersetzen von Hardware auf einem Workload.

Sie können folgende Einstellungen für den Monitor konfigurieren.

Einstellung	Beschreibung
Hardware-Komponenten	Wählen Sie einen oder mehrere Hardware-Komponenten aus, die Sie auf mögliche Änderungen überwachen wollen. Die nachfolgenden Werte sind verfügbar. • **Alle** — Dies ist der Standardwert. • **Mainboard** • **CPU** • **RAM** • **Laufwerk** • **GPU** • **Netzwerkadapter**
Zu überwachende Objekte	Spezifizieren Sie die Änderungen, auf die Sie die ausgewählten Hardware-Komponenten überwachen wollen. Sie können auch mehrere Elemente aus der Liste auswählen. Die nachfolgenden Werte sind verfügbar. • **Beliebige Änderung** —Dies ist der Standardwert. • **Neu hinzugefügte Komponenten** • **Ersetzte Komponenten** • **Entfernte Komponenten**

Die Einstellungen des Monitors 'CPU-Nutzung'

Der Monitor **CPU-Nutzung** überwacht die CPU-Gesamtnutzung (die Prozessorauslastung) des Workloads. Wenn der Workload über mehrere CPUs verfügt, wird die CPU-Gesamtnutzung berechnet, indem die CPU-Nutzung der einzelnen CPUs addiert wird.

Sie können folgende Einstellungen für den Monitor konfigurieren.

Einstellung	Beschreibung
Grenzwert-basiertes Monitoring	
Operator	Der Operator ist eine bedingte Funktion, die definiert, wie die Performance der Metrik gemessen werden soll. Die nachfolgenden Werte sind verfügbar. • **Mehr als** —Dies ist der Standardwert. • **Größer als oder ist gleich** • **Weniger als** • **Kleiner als oder ist gleich**
Grenzwert für die CPU-Nutzung	Der Grenzwert und der **Operator**-Wert bestimmen die normale Performance der überwachten Metrik. Wenn der Wert der überwachten Metrik außerhalb der Norm liegt, wird das System

Einstellung	Beschreibung
	eine Alarmmeldung generieren. Geben Sie einen ganzzahligen Wert im Bereich 1–100 (%) ein. Der Standardwert ist 90.
Zeitraum	Das System wird nur dann eine Alarmmeldung für ein erkanntes Problem generieren, wenn der Metrikwert während des spezifizierten Zeitraums außerhalb der Norm liegt. Geben Sie einen ganzzahligen Wert im Bereich 1–60 (min) ein. Der Standardwert ist 5.
Anomalie-basiertes Monitoring	
Trainingszeitraum für das Modell	Der Zeitraum, in dem das System die Machine Learning-Modelle mithilfe der Daten trainieren wird, die von den Agenten gesammelt wurden, und dann das normale Verhaltensmuster des Workloads erstellen wird. Je länger der Trainingszeitraum für das Modell ist, desto präziser wird das Langzeitverhaltensmuster sein, welches das System erstellen wird. Wir empfehlen eine Mindesttrainingszeit für das Modell von einundzwanzig Tagen. Geben Sie einen ganzzahligen Wert (Tage) ein. Der Standardwert ist 21.
Alarmmeldungen bei Anomalien während des Trainingszeitraums erhalten	Wenn Sie diese Einstellung wählen, werden Sie während des Modell-Trainingszeitraums Alarmmeldungen über Anomalien erhalten. Diese Alarmmeldungen können jedoch auch falsch sein, weil die Modelle noch trainiert werden und daher möglicherweise nicht genau genug sind. Die Einstellung ist standardmäßig vorausgewählt.
Empfindlichkeitsstufe	Die Empfindlichkeitsstufe dient als eine Art Vorfilter für Anomalien, sofern deren Werte innerhalb eines bestimmten Bereichs liegen. Dieser Filter arbeitet unabhängig vom Anomalie-Erkennungsalgorithmus. Er soll verhindern, dass Anomalien, die innerhalb des spezifizierten Bereichs liegen, vom Anomalie-Erkennungsalgorithmus verarbeitet werden. Während des Trainingszeitraums: 1. Der Algorithmus wird anhand der Daten trainiert, die während des Trainings gesammelt werden. 2. Der Algorithmus führt die Anomalie-Erkennung anhand der Trainingsdaten durch. 3. Es wird ein Filterprozess angewendet, der auf dem Mittelwert und der Standardabweichung basiert. 4. Alle Anomalien, die im spezifizierten Intervall liegen, werden gefiltert.

Einstellung	Beschreibung
	5. Aus den verbleibenden anomalen Datenpunkten wird die Anomalie mit der niedrigsten Anomaliestufe ausgewählt. Diese Stufe (eine Gleitkommazahl zwischen 0 und 1) wird im Modell aufgezeichnet. Während der Vorhersage: 1. Der Algorithmus sagt Anomalien bei den Inferenzdaten voraus. 2. Die vorhergesagten Anomalien werden anhand des Mittelwerts und der Standardabweichung sowie entsprechend der Empfindlichkeitsstufe gefiltert. 3. Die verbleibenden Anomalien werden nach folgendem Prinzip weiter gefiltert: Werte oberhalb der Grenzwertstufe werden als Anomalie betrachtet, während Werte unterhalb der Grenzwertstufe als normales Verhalten angesehen werden. Die nachfolgenden Werte sind verfügbar. • **Niedrig** — Die niedrige Stufe entspricht dem Mittelwert und dem Wert der Standardabweichung. • **Normal** — Dies ist der Standardwert. Die normale Stufe entspricht dem Mittelwert und dem zweifachen Wert der Standardabweichung. • **Hoch** — Die hohe Stufe entspricht dem Mittelwert und dem dreifachen Wert der Standardabweichung.
Anomalie-Dauer	Das System wird nur dann eine Alarmmeldung für eine erkannte Anomalie generieren, wenn das anormale Verhalten über den angegebenen Zeitraum anhält. Geben Sie einen ganzzahligen Wert im Bereich 1–60 (min) ein. Der Standardwert ist 15.

Die Einstellungen des Monitors 'Arbeitsspeicher-Nutzung'

Der Monitor **Arbeitsspeicher-Nutzung** überwacht die gesamte Arbeitsspeicher-Nutzung durch alle Arbeitsspeicher-Module des Workloads.

Sie können folgende Einstellungen für den Monitor konfigurieren.

Einstellung	Beschreibung
Grenzwert-basiertes Monitoring	
Operator	Der Operator ist eine bedingte Funktion, die definiert, wie die Performance der Metrik gemessen werden soll. Die nachfolgenden Werte sind verfügbar. • **Mehr als** —Dies ist der Standardwert.

Einstellung	Beschreibung
	• **Größer als oder ist gleich** • **Weniger als** • **Kleiner als oder ist gleich**
Grenzwert für die Arbeitsspeicher-Nutzung	Der Grenzwert und der **Operator**-Wert bestimmen die normale Performance der überwachten Metrik. Wenn der Wert der überwachten Metrik außerhalb der Norm liegt, wird das System eine Alarmmeldung generieren. Geben Sie einen ganzzahligen Wert im Bereich 1–100 (%) ein. Der Standardwert ist 90.
Zeitraum	Das System wird nur dann eine Alarmmeldung für ein erkanntes Problem generieren, wenn der Metrikwert während des spezifizierten Zeitraums außerhalb der Norm liegt. Geben Sie einen ganzzahligen Wert im Bereich 1–60 (min) ein. Der Standardwert ist 5.
Anomalie-basiertes Monitoring	
Trainingszeitraum für das Modell	Der Zeitraum, in dem das System die Machine Learning-Modelle mithilfe der Daten trainieren wird, die von den Agenten gesammelt wurden, und dann das normale Verhaltensmuster des Workloads erstellen wird. Je länger der Trainingszeitraum für das Modell ist, desto präziser wird das Langzeitverhaltensmuster sein, welches das System erstellen wird. Wir empfehlen eine Mindesttrainingszeit für das Modell von einundzwanzig Tagen. Geben Sie einen ganzzahligen Wert (Tage) ein. Der Standardwert ist 21.
Alarmmeldungen bei Anomalien während des Trainingszeitraums erhalten	Wenn Sie diese Einstellung wählen, werden Sie während des Modell-Trainingszeitraums Alarmmeldungen über Anomalien erhalten. Diese Alarmmeldungen können jedoch auch falsch sein, weil die Modelle noch trainiert werden und daher möglicherweise nicht genau genug sind. Die Einstellung ist standardmäßig vorausgewählt.
Empfindlichkeitsstufe	Die Empfindlichkeitsstufe dient als eine Art Vorfilter für Anomalien, sofern deren Werte innerhalb eines bestimmten Bereichs liegen. Dieser Filter arbeitet unabhängig vom Anomalie-Erkennungsalgorithmus. Er soll verhindern, dass Anomalien, die innerhalb des spezifizierten Bereichs liegen, vom Anomalie-Erkennungsalgorithmus verarbeitet werden. Während des Trainingszeitraums: 1. Der Algorithmus wird anhand der Daten trainiert, die während

Einstellung	Beschreibung
	des Trainings gesammelt werden. 2. Der Algorithmus führt die Anomalie-Erkennung anhand der Trainingsdaten durch. 3. Es wird ein Filterprozess angewendet, der auf dem Mittelwert und der Standardabweichung basiert. 4. Alle Anomalien, die im spezifizierten Intervall liegen, werden gefiltert. 5. Aus den verbleibenden anomalen Datenpunkten wird die Anomalie mit der niedrigsten Anomaliestufe ausgewählt. Diese Stufe (eine Gleitkommazahl zwischen 0 und 1) wird im Modell aufgezeichnet. Während der Vorhersage: 1. Der Algorithmus sagt Anomalien bei den Inferenzdaten voraus. 2. Die vorhergesagten Anomalien werden anhand des Mittelwerts und der Standardabweichung sowie entsprechend der Empfindlichkeitsstufe gefiltert. 3. Die verbleibenden Anomalien werden nach folgendem Prinzip weiter gefiltert: Werte oberhalb der Grenzwertstufe werden als Anomalie betrachtet, während Werte unterhalb der Grenzwertstufe als normales Verhalten angesehen werden. Die nachfolgenden Werte sind verfügbar. • **Niedrig** — Die niedrige Stufe entspricht dem Mittelwert und dem Wert der Standardabweichung. • **Normal** — Dies ist der Standardwert. Die normale Stufe entspricht dem Mittelwert und dem zweifachen Wert der Standardabweichung. • **Hoch** — Die hohe Stufe entspricht dem Mittelwert und dem dreifachen Wert der Standardabweichung.
Anomalie-Dauer	Das System wird nur dann eine Alarmmeldung für eine erkannte Anomalie generieren, wenn das anormale Verhalten über den angegebenen Zeitraum anhält. Geben Sie einen ganzzahligen Wert im Bereich 1–60 (min) ein. Der Standardwert ist 30 Minuten.

Die Einstellungen des Monitors 'Laufwerk-Übertragungsrate'

Der Monitor **Laufwerk-Übertragungsrate** überwacht die Lese- und Schreibgeschwindigkeit von jedem physischen Laufwerk auf dem Workload.

Sie können folgende Einstellungen für den Monitor konfigurieren.

Einstellung	Beschreibung
Grenzwert-basiertes Monitoring	
Zu überwachende Objekte	Wählen Sie die Geschwindigkeit aus, die Sie überwachen wollen. Die nachfolgenden Werte sind verfügbar. • **Lesegeschwindigkeit und Schreibgeschwindigkeit**. Dies ist der Standardwert. • **Lesegeschwindigkeit** • **Schreibgeschwindigkeit**
Lesegeschwindigkeit-Operator	Der Operator ist eine bedingte Funktion, die definiert, wie die Performance der Metrik gemessen werden soll. Die nachfolgenden Werte sind verfügbar. • **Mehr als**. Dies ist der Standardwert. • **Größer als oder ist gleich** • **Weniger als** • **Kleiner als oder ist gleich**
Lesegeschwindigkeit-Grenzwert	Der Grenzwert und der **Operator**-Wert bestimmen die normale Performance der überwachten Metrik. Wenn der Wert der überwachten Metrik außerhalb der Norm liegt, wird das System eine Alarmmeldung generieren. Geben Sie einen ganzzahligen Wert (kb/s) ein. Der Standardwert ist 0 kb/s.
Lesegeschwindigkeit-Zeitraum	Das System wird nur dann eine Alarmmeldung für ein erkanntes Problem generieren, wenn der Metrikwert während des spezifizierten Zeitraums außerhalb der Norm liegt. Geben Sie einen ganzzahligen Wert im Bereich 1–60 (min) ein. Der Standardwert ist 5.
Schreibgeschwindigkeit-Operator	Der Operator ist eine bedingte Funktion, die definiert, wie die Performance der Metrik gemessen werden soll. Die nachfolgenden Werte sind verfügbar. • **Mehr als** —Dies ist der Standardwert. • **Größer als oder ist gleich** • **Weniger als** • **Kleiner als oder ist gleich**
Schreibgeschwindigkeit-Grenzwert	Der Grenzwert und der **Operator**-Wert bestimmen die normale Performance der überwachten Metrik. Wenn der Wert der überwachten Metrik außerhalb der Norm liegt, wird das System eine Alarmmeldung generieren.

Einstellung	Beschreibung
	Geben Sie einen ganzzahligen Wert (kb/s) ein. Der Standardwert ist 0 kb/s.
Schreibgeschwindigkeit-Zeitraum	Das System wird nur dann eine Alarmmeldung für ein erkanntes Problem generieren, wenn der Metrikwert während des spezifizierten Zeitraums außerhalb der Norm liegt. Geben Sie einen ganzzahligen Wert im Bereich 1–60 (min) ein. Der Standardwert ist 5.
Anomalie-basiertes Monitoring	
Trainingszeitraum für das Modell	Der Zeitraum, in dem das System die Machine Learning-Modelle mithilfe der Daten trainieren wird, die von den Agenten gesammelt wurden, und dann das normale Verhaltensmuster des Workloads erstellen wird. Je länger der Trainingszeitraum für das Modell ist, desto präziser wird das Langzeitverhaltensmuster sein, welches das System erstellen wird. Wir empfehlen eine Mindesttrainingszeit für das Modell von einundzwanzig Tagen. Geben Sie einen ganzzahligen Wert (Tage) ein. Der Standardwert ist 21.
Alarmmeldungen bei Anomalien während des Trainingszeitraums erhalten	Wenn Sie diese Einstellung wählen, werden Sie während des Modell-Trainingszeitraums Alarmmeldungen über Anomalien erhalten. Diese Alarmmeldungen können jedoch auch falsch sein, weil die Modelle noch trainiert werden und daher möglicherweise nicht genau genug sind. Die Einstellung ist standardmäßig vorausgewählt.
Zu überwachende Objekte	Wählen Sie die Geschwindigkeit aus, die Sie überwachen wollen. Die nachfolgenden Werte sind verfügbar. • **Lesegeschwindigkeit und Schreibgeschwindigkeit**. Dies ist der Standardwert. • **Lesegeschwindigkeit** • **Schreibgeschwindigkeit**
Empfindlichkeitsstufe	Die Empfindlichkeitsstufe dient als eine Art Vorfilter für Anomalien, sofern deren Werte innerhalb eines bestimmten Bereichs liegen. Dieser Filter arbeitet unabhängig vom Anomalie-Erkennungsalgorithmus. Er soll verhindern, dass Anomalien, die innerhalb des spezifizierten Bereichs liegen, vom Anomalie-Erkennungsalgorithmus verarbeitet werden. Während des Trainingszeitraums:

Einstellung	Beschreibung
	1. Der Algorithmus wird anhand der Daten trainiert, die während des Trainings gesammelt werden. 2. Der Algorithmus führt die Anomalie-Erkennung anhand der Trainingsdaten durch. 3. Es wird ein Filterprozess angewendet, der auf dem Mittelwert und der Standardabweichung basiert. 4. Alle Anomalien, die im spezifizierten Intervall liegen, werden gefiltert. 5. Aus den verbleibenden anomalen Datenpunkten wird die Anomalie mit der niedrigsten Anomaliestufe ausgewählt. Diese Stufe (eine Gleitkommazahl zwischen 0 und 1) wird im Modell aufgezeichnet. Während der Vorhersage: 1. Der Algorithmus sagt Anomalien bei den Inferenzdaten voraus. 2. Die vorhergesagten Anomalien werden anhand des Mittelwerts und der Standardabweichung sowie entsprechend der Empfindlichkeitsstufe gefiltert. 3. Die verbleibenden Anomalien werden nach folgendem Prinzip weiter gefiltert: Werte oberhalb der Grenzwertstufe werden als Anomalie betrachtet, während Werte unterhalb der Grenzwertstufe als normales Verhalten angesehen werden. Die nachfolgenden Werte sind verfügbar. • **Niedrig** — Die niedrige Stufe entspricht dem Mittelwert und dem Wert der Standardabweichung. • **Normal** — Dies ist der Standardwert. Die normale Stufe entspricht dem Mittelwert und dem zweifachen Wert der Standardabweichung. • **Hoch** — Die hohe Stufe entspricht dem Mittelwert und dem dreifachen Wert der Standardabweichung.
Anomalie-Dauer (Lesegeschwindigkeit)	Das System wird nur dann eine Alarmmeldung für eine erkannte Anomalie generieren, wenn das anormale Verhalten über den angegebenen Zeitraum anhält. Geben Sie einen ganzzahligen Wert im Bereich 1–60 (min) ein. Der Standardwert ist 25.
Anomalie-Dauer (Schreibgeschwindigkeit)	Das System wird nur dann eine Alarmmeldung für eine erkannte Anomalie generieren, wenn das anormale Verhalten über den angegebenen Zeitraum anhält. Geben Sie einen ganzzahligen Wert im Bereich 1–60 (min) ein.

Einstellung	Beschreibung
	Der Standardwert ist 25.

Die Einstellungen des Monitors 'Netzwerknutzung'

Der Monitor **Netzwerknutzung** überwacht den ein- und ausgehenden Datenverkehr für jeden Netzwerkadapter des Workloads.

Sie können folgende Einstellungen für den Monitor konfigurieren.

Einstellung	Beschreibung
Grenzwert-basiertes Monitoring	
Datenverkehrsrichtung	Die Datenverkehrsrichtung, die Sie überwachen wollen. Die nachfolgenden Werte sind verfügbar. • **Eingehender und ausgehender Datenverkehr**. Dies ist der Standardwert. • **Eingehender Datenverkehr** • **Ausgehender Traffic**
Operator für eingehenden Datenverkehr	Der Operator ist eine bedingte Funktion, die definiert, wie die Performance der Metrik gemessen werden soll. Die nachfolgenden Werte sind verfügbar. • **Mehr als** —Dies ist der Standardwert. • **Größer als oder ist gleich** • **Weniger als** • **Kleiner als oder ist gleich**
Grenzwert für eingehenden Datenverkehr	Der Grenzwert und der **Operator**-Wert bestimmen die normale Performance der überwachten Metrik. Wenn der Wert der überwachten Metrik außerhalb der Norm liegt, wird das System eine Alarmmeldung generieren. Geben Sie einen ganzzahligen Wert (kb/s) ein. Der Standardwert ist 0 kb/s.
Zeitraum für eingehenden Datenverkehr	Das System wird nur dann eine Alarmmeldung für ein erkanntes Problem generieren, wenn der Metrikwert während des spezifizierten Zeitraums außerhalb der Norm liegt. Geben Sie einen ganzzahligen Wert im Bereich 1–60 (min) ein. Der Standardwert ist 5.
Operator für ausgehenden Datenverkehr	Der Operator ist eine bedingte Funktion, die definiert, wie die Performance der Metrik gemessen werden soll. Die nachfolgenden Werte sind verfügbar.

Einstellung	Beschreibung
	• **Mehr als** —Dies ist der Standardwert. • **Größer als oder ist gleich** • **Weniger als** • **Kleiner als oder ist gleich**
Grenzwert für ausgehenden Datenverkehr	Der Grenzwert und der **Operator**-Wert bestimmen die normale Performance der überwachten Metrik. Wenn der Wert der überwachten Metrik außerhalb der Norm liegt, wird das System eine Alarmmeldung generieren. Geben Sie einen ganzzahligen Wert (kb/s) ein. Der Standardwert ist 0 kb/s.
Zeitraum für ausgehenden Datenverkehr	Der Grenzwert und der **Operator**-Wert bestimmen die normale Performance der überwachten Metrik. Wenn der Wert der überwachten Metrik außerhalb der Norm liegt, wird das System eine Alarmmeldung generieren. Geben Sie einen ganzzahligen Wert im Bereich 1–60 (min) ein. Der Standardwert ist 5.
Anomalie-basiertes Monitoring	
Trainingszeitraum für das Modell	Der Zeitraum, in dem das System die Machine Learning-Modelle mithilfe der Daten trainieren wird, die von den Agenten gesammelt wurden, und dann das normale Verhaltensmuster des Workloads erstellen wird. Je länger der Trainingszeitraum für das Modell ist, desto präziser wird das Langzeitverhaltensmuster sein, welches das System erstellen wird. Wir empfehlen eine Mindesttrainingszeit für das Modell von einundzwanzig Tagen. Geben Sie einen ganzzahligen Wert (Tage) ein. Der Standardwert ist 21.
Alarmmeldungen bei Anomalien während des Trainingszeitraums erhalten	Wenn Sie diese Einstellung wählen, werden Sie während des Modell-Trainingszeitraums Alarmmeldungen über Anomalien erhalten. Diese Alarmmeldungen können jedoch auch falsch sein, weil die Modelle noch trainiert werden und daher möglicherweise nicht genau genug sind. Die Einstellung ist standardmäßig vorausgewählt.
Datenverkehrsrichtung	• **Eingehender und ausgehender Datenverkehr**. Dies ist der Standardwert. • **Eingehender Datenverkehr** • **Ausgehender Traffic**
Empfindlichkeitsstufe	Die Empfindlichkeitsstufe dient als eine Art Vorfilter für Anomalien, sofern deren Werte innerhalb eines bestimmten

Einstellung	Beschreibung
	Bereichs liegen. Dieser Filter arbeitet unabhängig vom Anomalie-Erkennungsalgorithmus. Er soll verhindern, dass Anomalien, die innerhalb des spezifizierten Bereichs liegen, vom Anomalie-Erkennungsalgorithmus verarbeitet werden. Während des Trainingszeitraums: 1. Der Algorithmus wird anhand der Daten trainiert, die während des Trainings gesammelt werden. 2. Der Algorithmus führt die Anomalie-Erkennung anhand der Trainingsdaten durch. 3. Es wird ein Filterprozess angewendet, der auf dem Mittelwert und der Standardabweichung basiert. 4. Alle Anomalien, die im spezifizierten Intervall liegen, werden gefiltert. 5. Aus den verbleibenden anomalen Datenpunkten wird die Anomalie mit der niedrigsten Anomaliestufe ausgewählt. Diese Stufe (eine Gleitkommazahl zwischen 0 und 1) wird im Modell aufgezeichnet. Während der Vorhersage: 1. Der Algorithmus sagt Anomalien bei den Inferenzdaten voraus. 2. Die vorhergesagten Anomalien werden anhand des Mittelwerts und der Standardabweichung sowie entsprechend der Empfindlichkeitsstufe gefiltert. 3. Die verbleibenden Anomalien werden nach folgendem Prinzip weiter gefiltert: Werte oberhalb der Grenzwertstufe werden als Anomalie betrachtet, während Werte unterhalb der Grenzwertstufe als normales Verhalten angesehen werden. Die nachfolgenden Werte sind verfügbar. • **Niedrig** — Die niedrige Stufe entspricht dem Mittelwert und dem Wert der Standardabweichung. • **Normal** — Dies ist der Standardwert. Die normale Stufe entspricht dem Mittelwert und dem zweifachen Wert der Standardabweichung. • **Hoch** — Die hohe Stufe entspricht dem Mittelwert und dem dreifachen Wert der Standardabweichung.
Anomalie-Dauer (Eingehend)	Das System wird nur dann eine Alarmmeldung für eine erkannte Anomalie generieren, wenn das anormale Verhalten über den angegebenen Zeitraum anhält. Geben Sie einen ganzzahligen Wert im Bereich 1–60 (min) ein.

Einstellung	Beschreibung
	Der Standardwert ist 25.
Anomalie-Dauer (Ausgehend)	Das System wird nur dann eine Alarmmeldung für eine erkannte Anomalie generieren, wenn das anormale Verhalten über den angegebenen Zeitraum anhält. Geben Sie einen ganzzahligen Wert im Bereich 1–60 (min) ein. Der Standardwert ist 25.

Die Einstellungen des Monitors 'CPU-Nutzung nach Prozess'

Der Monitor **CPU-Nutzung nach Prozess** überwacht die Nutzung der CPU durch den ausgewählten Prozess. Wenn es von einem Prozess mehrere Instanzen gibt, wird das System die Gesamtnutzung von allen Prozessinstanzen gemeinsam überwachen und eine Alarmmeldung generieren, wenn die entsprechenden Bedingungen erfüllt sind.

Sie können folgende Einstellungen für den Monitor konfigurieren.

Einstellung	Beschreibung
Prozessname	Der Name des Prozesses, den Sie überwachen wollen. Geben Sie den Prozessnamen ohne dessen Erweiterung ein.
Operator	Der Operator ist eine bedingte Funktion, die definiert, wie die Performance der Metrik gemessen werden soll. Die nachfolgenden Werte sind verfügbar. • **Mehr als** —Dies ist der Standardwert. • **Größer als oder ist gleich** • **Weniger als** • **Kleiner als oder ist gleich**
Grenzwert	Der Grenzwert und der **Operator**-Wert bestimmen die normale Performance der überwachten Metrik. Wenn der Wert der überwachten Metrik außerhalb der Norm liegt, wird das System eine Alarmmeldung generieren. Geben Sie einen ganzzahligen Wert im Bereich 1–100 (%) ein. Der Standardwert ist 90.
Zeitraum	Das System wird nur dann eine Alarmmeldung für ein erkanntes Problem generieren, wenn der Metrikwert während des spezifizierten Zeitraums außerhalb der Norm liegt. Geben Sie einen ganzzahligen Wert im Bereich 1–60 (min) ein. Der Standardwert ist 5.

Die Einstellungen des Monitors 'Arbeitsspeicher-Nutzung nach Prozess'

Der Monitor **Arbeitsspeicher-Nutzung nach Prozess** überwacht die Nutzung des Arbeitsspeichers durch den ausgewählten Prozess. Wenn es von einem Prozess mehrere Instanzen gibt, wird das System die Gesamtnutzung von allen Prozessinstanzen gemeinsam überwachen und eine Alarmmeldung generieren, wenn die entsprechenden Bedingungen erfüllt sind.

Hinweis
Die Agenten verwenden den gesamten Prozessarbeitssatz (privat und freigegeben), um die Größe der Arbeitsspeicher-Nutzung pro Prozess zu schätzen. Deshalb kann sich die Größe der Arbeitsspeicher-Nutzung, die vom Widget angezeigt wird, von der Größe unterscheiden, die im Windows Task-Manager angezeigt wird (privater Arbeitssatz).

Sie können folgende Einstellungen für den Monitor konfigurieren.

Einstellung	Beschreibung
Prozessname	Der Name des Prozesses, den Sie überwachen wollen. Geben Sie den Prozessnamen ohne dessen Erweiterung ein.
Operator	Der Operator ist eine bedingte Funktion, die definiert, wie die Performance der Metrik gemessen werden soll. Die nachfolgenden Werte sind verfügbar. • **Mehr als** —Dies ist der Standardwert. • **Größer als oder ist gleich** • **Weniger als** • **Kleiner als oder ist gleich**
Grenzwert	Der Grenzwert und der **Operator**-Wert bestimmen die normale Performance der überwachten Metrik. Wenn der Wert der überwachten Metrik außerhalb der Norm liegt, wird das System eine Alarmmeldung generieren. Geben Sie einen ganzzahligen Wert (kb) ein. Der Standardwert ist 1.
Zeitraum	Das System wird nur dann eine Alarmmeldung für ein erkanntes Problem generieren, wenn der Metrikwert während des spezifizierten Zeitraums außerhalb der Norm liegt. Geben Sie einen ganzzahligen Wert im Bereich 1–60 (min) ein. Der Standardwert ist 5.

Die Einstellungen des Monitors 'Laufwerk-Übertragungsrate nach Prozess'

Der Monitor **Laufwerk-Übertragungsrate nach Prozess** überwacht die Lese- und Schreibgeschwindigkeit durch den ausgewählten Prozess. Wenn es von einem Prozess mehrere Instanzen gibt, wird das System die Gesamtnutzung von allen Prozessinstanzen gemeinsam überwachen und eine Alarmmeldung generieren, wenn die entsprechenden Bedingungen erfüllt sind.

Sie können folgende Einstellungen für den Monitor konfigurieren.

Einstellung	Beschreibung
Prozessname	Der Name des Prozesses, den Sie überwachen wollen. Geben Sie den Prozessnamen ohne dessen Erweiterung ein.
Zu überwachende Objekte	Die Geschwindigkeit, die Sie überwachen wollen. Die nachfolgenden Werte sind verfügbar. • **Lesegeschwindigkeit und Schreibgeschwindigkeit**. Dies ist der Standardwert. • **Lesegeschwindigkeit** • **Schreibgeschwindigkeit**
Lesegeschwindigkeit-Operator	Der Operator ist eine bedingte Funktion, die definiert, wie die Performance der Metrik gemessen werden soll. Die nachfolgenden Werte sind verfügbar. • **Mehr als** —Dies ist der Standardwert. • **Größer als oder ist gleich** • **Weniger als** • **Kleiner als oder ist gleich**
Lesegeschwindigkeit-Grenzwert	Der Grenzwert und der **Operator**-Wert bestimmen die normale Performance der überwachten Metrik. Wenn der Wert der überwachten Metrik außerhalb der Norm liegt, wird das System eine Alarmmeldung generieren. Geben Sie einen ganzzahligen Wert (kb/s) ein. Der Standardwert ist 0 kb/s.
Lesegeschwindigkeit-Zeitraum	Das System wird nur dann eine Alarmmeldung für ein erkanntes Problem generieren, wenn der Metrikwert während des spezifizierten Zeitraums außerhalb der Norm liegt. Geben Sie einen ganzzahligen Wert im Bereich 1–60 (min) ein. Der Standardwert ist 5.
Schreibgeschwindigkeit-	Der Operator ist eine bedingte Funktion, die definiert, wie die

Einstellung	Beschreibung
Operator	Performance der Metrik gemessen werden soll. Die nachfolgenden Werte sind verfügbar. • **Mehr als** —Dies ist der Standardwert. • **Größer als oder ist gleich** • **Weniger als** • **Kleiner als oder ist gleich**
Schreibgeschwindigkeit-Grenzwert	Der Grenzwert und der **Operator**-Wert bestimmen die normale Performance der überwachten Metrik. Wenn der Wert der überwachten Metrik außerhalb der Norm liegt, wird das System eine Alarmmeldung generieren. Geben Sie einen ganzzahligen Wert (kb/s) ein. Der Standardwert ist 0 kb/s.
Schreibgeschwindigkeit-Zeitraum	Das System wird nur dann eine Alarmmeldung für ein erkanntes Problem generieren, wenn der Metrikwert während des spezifizierten Zeitraums außerhalb der Norm liegt. Geben Sie einen ganzzahligen Wert im Bereich 1–60 (min) ein. Der Standardwert ist 5.

Die Einstellungen des Monitors 'Netzwerknutzung nach Prozess'

Der Monitor **Netzwerknutzung nach Prozess** überwacht den ein- und ausgehenden Datenverkehr durch den ausgewählten Prozess. Wenn es von einem Prozess mehrere Instanzen gibt, wird das System die Gesamtnutzung von allen Prozessinstanzen gemeinsam überwachen und eine Alarmmeldung generieren, wenn die entsprechenden Bedingungen für alle Instanzen erfüllt sind.

Sie können folgende Einstellungen für den Monitor konfigurieren.

Einstellung	Beschreibung
Prozessname	Der Name des Prozesses, den Sie überwachen wollen. Geben Sie den Prozessnamen ohne dessen Erweiterung ein.
Datenverkehrsrichtung	Die Datenverkehrsrichtung, die Sie überwachen wollen. Die nachfolgenden Werte sind verfügbar. • **Eingehender und ausgehender Datenverkehr**. Dies ist der Standardwert. • **Eingehender Datenverkehr** • **Ausgehender Traffic**
Operator für eingehenden Datenverkehr	Der Operator ist eine bedingte Funktion, die definiert, wie die Performance der Metrik gemessen werden soll.

Einstellung	Beschreibung
	Die nachfolgenden Werte sind verfügbar. • **Mehr als** —Dies ist der Standardwert. • **Größer als oder ist gleich** • **Weniger als** • **Kleiner als oder ist gleich**
Grenzwert für eingehenden Datenverkehr	Der Grenzwert und der **Operator**-Wert bestimmen die normale Performance der überwachten Metrik. Wenn der Wert der überwachten Metrik außerhalb der Norm liegt, wird das System eine Alarmmeldung generieren. Geben Sie einen ganzzahligen Wert (kb/s) ein. Der Standardwert ist 0 kb/s.
Zeitraum für eingehenden Datenverkehr	Das System wird nur dann eine Alarmmeldung für ein erkanntes Problem generieren, wenn der Metrikwert während des spezifizierten Zeitraums außerhalb der Norm liegt. Geben Sie einen ganzzahligen Wert im Bereich 1–60 (min) ein. Der Standardwert ist 5.
Operator für ausgehenden Datenverkehr	Der Operator ist eine bedingte Funktion, die definiert, wie die Performance der Metrik gemessen werden soll. Die nachfolgenden Werte sind verfügbar. • **Mehr als** —Dies ist der Standardwert. • **Größer als oder ist gleich** • **Weniger als** • **Kleiner als oder ist gleich**
Grenzwert für ausgehenden Datenverkehr	Der Grenzwert und der **Operator**-Wert bestimmen die normale Performance der überwachten Metrik. Wenn der Wert der überwachten Metrik außerhalb der Norm liegt, wird das System eine Alarmmeldung generieren. Geben Sie einen ganzzahligen Wert (kb/s) ein. Der Standardwert ist 0 kb/s.
Zeitraum für ausgehenden Datenverkehr	Das System wird nur dann eine Alarmmeldung für ein erkanntes Problem generieren, wenn der Metrikwert während des spezifizierten Zeitraums außerhalb der Norm liegt. Geben Sie einen ganzzahligen Wert im Bereich 1–60 (min) ein. Der Standardwert ist 5.

Einstellungen des Monitors 'Windows-Dienst-Status'

Der **Windows-Dienst-Status** überwacht, ob der ausgewählte Windows-Dienst läuft oder gestoppt ist.

Sie können folgende Einstellungen für den Monitor konfigurieren.

Einstellung	Beschreibung
Dienstname	Der Name des Windows-Dienstes, den Sie überwachen wollen. Sie können den Namen eines Dienstes aus der Liste der Windows-Dienste auswählen. Die Liste wird von allen Agenten des Mandanten ausgefüllt, nachdem der Software-Inventarisierungsscan für die Workloads erfolgreich abgeschlossen wurde. Sie können auch einen Dienstnamen hinzufügen, der nicht in der Liste enthalten ist. Diese Option ist die einzige, die verfügbar ist, wenn auf den Workloads keine Software-Inventarisierungsprüfung durchgeführt werden konnte.
Dienststatus	Wenn sich der Dienst in dem ausgewählten Status befindet, wird das System ein Ereignis generieren. Die nachfolgenden Werte sind verfügbar. • **Wird ausgeführt** • **Gestoppt**—Dies ist der Standardwert.
Zeitraum	Das System wird nur dann eine Alarmmeldung für ein erkanntes Problem generieren, wenn der Metrikwert während des spezifizierten Zeitraums außerhalb der Norm liegt. Geben Sie einen ganzzahligen Wert im Bereich 1–60 (min) ein. Der Standardwert ist 1.

Die Einstellungen des Monitors 'Prozessstatus'

Der Monitor **Prozessstatus** überwacht, ob der ausgewählte Prozess läuft oder gestoppt ist. Wenn es von einem Prozess mehrere Instanzen gibt, wird das System jede Instanz des Prozesses überwachen und eine Alarmmeldung generieren, wenn die entsprechenden Bedingungen für alle Instanzen des Prozesses erfüllt sind.

Sie können folgende Einstellungen für den Monitor konfigurieren.

Einstellung	Beschreibung
Prozessname	Der Name des Prozesses, den Sie überwachen wollen. Geben Sie den Namen der ausführbaren Datei ohne Erweiterung ein.
Prozessstatus	Wenn sich der Prozess in dem ausgewählten Status befindet, wird das System ein Ereignis generieren.

Einstellung	Beschreibung
	Die nachfolgenden Werte sind verfügbar. • **Wird ausgeführt** • **Gestoppt**—Dies ist der Standardwert.
Zeitraum	Das System wird nur dann eine Alarmmeldung für ein erkanntes Problem generieren, wenn der Metrikwert während des spezifizierten Zeitraums außerhalb der Norm liegt. Geben Sie einen ganzzahligen Wert im Bereich 1–60 (min) ein. Der Standardwert ist 1.

Die Einstellungen des Monitors 'Installierte Software'

Der Monitor **Installierte Software** überwacht, ob Software-Applikationen auf dem Workload installiert, aktualisiert oder gelöscht werden.

Sie können folgende Einstellungen für den Monitor konfigurieren.

Einstellung	Beschreibung
Zu überwachende Software	Spezifizieren Sie die Software, die Sie überwachen lassen wollen. Die nachfolgenden Werte sind verfügbar. • **Jede Software** —Dies ist der Standardwert. • **Spezifische Software**
Software-Namen	Diese Einstellung wird verfügbar, wenn Sie bei **Zu überwachende Software** als Wert **Spezifische Software** festlegen. Geben Sie den Namen einer oder mehrerer Software-Applikationen ein. Sie können den Namen einer Software-Applikation aus der Liste der Windows-Dienste auswählen. Die Liste wird von allen Agenten des Mandanten ausgefüllt, nachdem der Software-Inventarisierungsscan für die Workloads erfolgreich abgeschlossen wurde. Sie können auch einen Software-Applikationsnamen hinzufügen, der nicht in der Liste enthalten ist. Diese Option ist die einzige, die verfügbar ist, wenn auf den Workloads keine Software-Inventarisierungsprüfung durchgeführt werden konnte.
Installationsstatus	Spezifizieren Sie, ob Sie installierte, nicht installierte oder aktualisierte Software überwachen wollen. Die nachfolgenden Werte sind verfügbar. • **Installiert** – Dies ist der Standardwert. Wenn Sie diesen Wert auswählen, wird der Monitor einen Alarm generieren, wenn eine neue Software-Applikation auf dem Workload installiert wird.

Einstellung	Beschreibung
	• **Aktualisiert** – Wenn Sie diesen Wert auswählen, wird der Monitor einen Alarm generieren, wenn eine Software-Applikation aktualisiert wird. • **Nicht installiert** - Wenn Sie diesen Wert auswählen, wird der Monitor einen Alarm auslösen, wenn eine Software-Applikation deinstalliert wird oder auf dem Workload nicht verfügbar ist.

Die Einstellungen des Monitors 'Letzter System-Neustart'

Letzter System-Neustart – wenn der Workload zuletzt neu gestartet wurde.

Sie können die folgende Einstellung für den Monitor konfigurieren.

Einstellung	Beschreibung
Der Workload wurde nicht mehr neu gestartet seit	Der Zeitraum (Anzahl der Tage), der seit dem letzten Neustart des Workloads vergangen ist. Wenn der Zeitraum, seit dem der Workload das letzte Mal neu gestartet wurde, länger ist, als der Zeitraum, den Sie hier spezifizieren, wird das System eine Alarmmeldung generieren. Geben Sie einen ganzzahligen Wert im Bereich 1–180 (Tage) ein. Der Standardwert ist 30.

Einstellungen des Monitors 'Windows-Ereignisprotokoll'

Das **Windows-Ereignisprotokoll** überwacht bestimmte geschäftskritische Ereignisse in den Windows-Ereignisprotokollen.

Sie können folgende Einstellungen für den Monitor konfigurieren.

Einstellung	Beschreibung
Ereignisprotokollname	Wählen Sie ein bestimmtes Ereignisprotokoll aus einer Liste von Windows-Ereignisprotokollen aus, die in der Windows-Ereignisanzeige verfügbar sind. Die nachfolgenden Werte sind verfügbar. • **Beliebig** —Dies ist der Standardwert. • **Applikation** • **Sicherheit** • **System**
Ereignisquelle	Ereignisquellname Sie können den Wert aus einer Liste von Ereignisquellen auswählen, die von allen Agenten des Mandanten gesammelt werden, oder einen neuen Quellnamen manuell eingeben.

Einstellung	Beschreibung
	Wenn der Software-Inventarisierungsscan für den Mandanten deaktiviert ist, wird die Liste der Ereignisquellen leer sein.
Übereinstimmungsmodus	In diesem Feld können Sie spezifizieren, ob Sie die Einstellungen für **Ereignis-IDs**, **Ereignistyp** und **Ereignisbeschreibung**, indem Sie den Operator **Beliebig** oder **Alle** verwenden. Die nachfolgenden Werte sind verfügbar. • **Beliebig** —Dies ist der Standardwert. Es wird nur dann eine Alarmmeldung generiert, wenn irgendeines der ausgewählten Kriterien erfüllt ist. • **Alle** — Es wird eine Alarmmeldung generiert, wenn alle ausgewählten Kriterien erfüllt sind.
Ereignis-IDs	Geben Sie eine oder mehrere (durch Komma getrennte) Ereignis-IDs ein. Wenn das System im Ereignisprotokoll irgendeinen der Ereigniscodes findet, die Sie in diesem Feld eingegeben haben, erzeugt es eine Alarmmeldung.
Ereignistyp	Wählen Sie einen oder mehrere Ereignistypen, die Sie überwachen wollen. Die nachfolgenden Werte sind verfügbar. • **Beliebig** —Dies ist der Standardwert. • **Fehler** • **Warnung** • **Informationen** • **Erfolgsüberwachung** • **Fehlerüberwachung**
Ereignisbeschreibung	Bestimmte Schlüsselwörter oder Phrasen in der Ereignisbeschreibung, nach denen Sie suchen wollen. Jedes Schlüsselwort oder jede Phrase, die Sie eingeben, muss in Anführungszeichen gesetzt und per Komma getrennt werden. Wenn das System eines der von Ihnen eingegebenen Schlüsselwörter oder Phrasen findet, wird es eine Alarmmeldung generieren.
Anzahl der Vorkommen	Die Mindestanzahl, mit der ein Ereignis innerhalb des Zeitraums im Protokoll vorkommen muss, damit das System eine Alarmmeldung generiert. Geben Sie einen ganzzahligen Wert im Bereich 1–1000 ein.
Zeitraum	Das System wird nur dann eine Alarmmeldung für ein erkanntes Problem generieren, wenn der Metrikwert während

Einstellung	Beschreibung
	des spezifizierten Zeitraums außerhalb der Norm liegt. Geben Sie einen ganzzahligen Wert ein und bestimmen Sie dann die Einheit: Minuten oder Stunden. Der Standardwert ist 60 Minuten.

Die Einstellungen des Monitors 'Größe der Dateien und Ordner'

Der Monitor **Größe der Dateien und Ordner** überwacht die Gesamtgröße aller ausgewählten Dateien und Ordner.

Sie können folgende Einstellungen für den Monitor konfigurieren.

Einstellung	Beschreibung
Zu überwachende Dateien oder Ordner	Die Pfade zu den Dateien oder Ordnern, die Sie überwachen wollen. Sie können auch Dateien oder Ordner spezifizieren, die Sie vom Monitoring ausschließen wollen. Sie können die nachfolgenden Platzhalterzeichen (Wildcards) verwenden. • * — für null oder mehr Zeichen in einem Datei- oder Ordnernamen • ? — für genau ein Zeichen in einem Datei- oder Ordnernamen Für Windows-Workloads: • Der vollständige Pfad sollte mit dem Laufwerksbuchstaben beginnen, gefolgt von den Trennzeichen :\. • Sie können einen Schrägstrich (/) oder Backslash (\) als Trennzeichen innerhalb des Pfades verwenden. • Der Datei- oder Ordnername darf nicht mit einem Leerzeichen oder einem Punkt enden. Für MacOS-Workloads: • Der vollständige Pfad sollte mit dem Stammverzeichnis (Root-Verzeichnis) beginnen. • Sie können einen Schrägstrich (/) als Trennzeichen innerhalb des Pfades verwenden. • Der Datei- oder Ordnername darf nicht mit einem Leerzeichen oder einem Punkt enden. Es ist nicht zwingend erforderlich, einen bestimmten Speicherort in den Ausschlussfiltern zu spezifizieren. Dateien, die ohne einen bestimmten Speicherort eingegeben werden, werden von den überwachten Ordnern ausgeschlossen.
Operator	Der Operator ist eine bedingte Funktion, die definiert, wie die Performance der Metrik gemessen werden soll.

Einstellung	Beschreibung
	Die nachfolgenden Werte sind verfügbar. • **Mehr als** —Dies ist der Standardwert. • **Weniger als**
Grenzwert	Der Grenzwert und der **Operator**-Wert bestimmen die normale Performance der überwachten Metrik. Wenn der Wert der überwachten Metrik außerhalb der Norm liegt, wird das System eine Alarmmeldung generieren. Geben Sie einen ganzzahligen Wert (MB) ein.
Zeitraum	Das System wird nur dann eine Alarmmeldung für ein erkanntes Problem generieren, wenn der Metrikwert während des spezifizierten Zeitraums außerhalb der Norm liegt. Geben Sie einen ganzzahligen Wert im Bereich 10–60 (min) ein. Der Standardwert ist 10.

Einstellungen des Monitors 'Windows Update-Status'

Der **Windows Update-Status** überwacht den Status des Windows Updates auf dem Workload und ob auf diesem die neuesten Updates installiert sind.

Wenn Sie diesen Monitor aktivieren, wird das System in den nachfolgenden Fällen eine Alarmmeldung generieren.

- Das Windows Update auf dem Workload ist ausgeschaltet.
- Das Windows Update auf dem Workload ist aktiviert, aber die neuesten Updates sind nicht installiert.

Die Einstellungen des Monitors 'Firewall-Status'

Der Monitor **Firewall-Status** überwacht den Status der integrierten Firewall oder der Firewall eines Drittanbieters, die auf dem Workload installiert ist.

Wenn Sie diesen Monitor aktivieren, wird das System in den nachfolgenden Fällen eine Alarmmeldung generieren.

- Die integrierte Firewall des Betriebssystems (Windows Defender Firewall oder macOS Firewall) ist deaktiviert und es wird keine Firewall eines Drittanbieters ausgeführt.
- Windows Defender Firewall ist für öffentliche Netzwerke deaktiviert.
- Windows Defender Firewall ist für private Netzwerke deaktiviert.
- Windows Defender Firewall ist für Domain-Netzwerke deaktiviert.

Die Einstellungen des Monitors 'Fehlgeschlagene Anmeldungen'

Der Monitor **Fehlgeschlagene Anmeldungen** überwacht fehlgeschlagene Anmeldeversuche auf dem Workload.

Sie können folgende Einstellungen für den Monitor konfigurieren.

Einstellung	Beschreibung
Grenzwert für fehlgeschlagene Anmeldeversuche	Der Grenzwert bestimmt die Grenzen für die normale Performance der überwachten Metrik. Wenn der Grenzwert überschritten wird, liegt der Wert außerhalb des Normbereichs. Geben Sie einen ganzzahligen Wert ein. Der Standardwert ist 60.
Zeitraum	Das System wird nur dann eine Alarmmeldung für ein erkanntes Problem generieren, wenn der Metrikwert während des spezifizierten Zeitraums außerhalb der Norm liegt. Geben Sie einen ganzzahligen Wert aus dem Bereich 1–24 ein und bestimmen Sie eine Einheit: Stunden oder Tage. Der Standardwert ist 12.

Die Einstellungen des Monitors 'Antimalware-Software-Status'

Der Monitor **Antimalware-Software-Status** überwacht die integrierte Antimalware-Software oder die Antimalware-Software eines Drittanbieters, die auf dem Workload installiert ist.

Wenn Sie diesen Monitor aktivieren, wird das System einen Alarm generieren, sobald es eine der nachfolgenden Bedingungen feststellt.

- Auf dem Workload ist keine Antimalware-Software installiert.
- Es ist eine Antimalware-Software installiert, aber sie wird nicht ausgeführt.
- Eine Antimalware-Software ist installiert und wird ausgeführt, aber die Antimalware-Definitionen sind nicht aktuell.

Hinweis
Diese Bedingung wird für Windows- und Windows Server-Betriebssysteme überprüft.

Betriebssystem	Unterstützte Antimalware-Software
Windows	• Acronis Cyber Protect • Windows Defender • Symantec Endpoint Security • Norton 360 • Norton Antivirus • SentinelOne

Betriebssystem	Unterstützte Antimalware-Software
	• Trend Micro Endpoint Security mit Apex One • Trend Micro Worry-Free Business • McAfee Endpoint Security • McAfee Endpoint Protection for SMB • FireEye Endpoint Security • F-Secure SAFE • F-Secure Client Security • CrowdStrike Falcon • Kaspersky Endpoint Security Cloud • BitDefender Antivirus • Sophos Intercept X Endpoint • Avast Business Antivirus • AVG Antivirus Business Edition • AVG Internet Security Business Edition • Panda Endpoint Protection • Tencent PC Manager • Webroot Business Endpoint Protection • ESET Endpoint Security • Avira Antivirus • Comodo Internet Security • Comodo Business Antivirus • K7 Business Security • K7 Total Security • Vipre Endpoint Protection • Total AV
Windows Server	• Acronis Cyber Protect • Windows Defender • ESET Endpoint Security **Hinweis** Der Monitor kann möglicherweise auch mit anderen Antimalware-Applikationen zusammenarbeiten, dies ist jedoch nicht garantiert.
macOS	• Acronis Cyber Protect • F-Secure Safe • BitDefender Antivirus for Mac • Sophos Home • Sophos Endpoint Protection • Avast Security für Mac • AVG AntiVirus für Mac • Webroot SecureAnywhere

Betriebssystem	Unterstützte Antimalware-Software
	• ESET Cybersecurity • Avira Antivirus für Mac • Comodo Antivirus for Mac • K7 Antivirus for Mac • Vipre Advanced Security • Total AV für Mac **Hinweis** Der Monitor kann möglicherweise auch mit anderen Antimalware-Applikationen zusammenarbeiten, dies ist jedoch nicht garantiert.

Die Einstellungen des Monitors 'Status der AutoRun-Funktion'

Der Monitor **Status der AutoRun-Funktion** überwacht, ob die AutoRun-Funktion für Wechselmedien aktiviert ist.

Aus Sicherheitsgründen empfehlen wir, dass Sie die AutoRun-Funktion für Wechselmedien auf dem Workload deaktivieren. Wenn die Funktion aktiviert ist, wird das System einen Alarm generieren.

Die Einstellungen des Monitors 'Benutzerdefiniert'

Der Monitor **Benutzerdefiniert** überwacht benutzerdefinierte Objekte über die Ausführung eines Skriptes.

Sie können folgende Einstellungen für den Monitor konfigurieren.

Einstellung	Beschreibung
Auszuführendes Skript	Liste der vordefinierten Skripte aus dem Skript-Repository.
Planung	Der Zeitpunkt, zu dem das Skript ausgeführt werden soll sowie optional zusätzliche Bedingungen, die erfüllt sein müssen, damit das Skript ausgeführt wird. Die nachfolgenden Werte sind verfügbar. • **Planung nach Zeit** — Das Skript wird genau zu dem Zeitpunkt (festlegbar nach Uhrzeit, Tagen, Wochen oder Monaten) ausgeführt, den Sie spezifizieren. Dies ist der Standardwert. **Planungstyp** — **Stündlich**, **Täglich** oder **Monatlich** **Innerhalb eines Zeitraums ausführen** — Ein Zeitraum, innerhalb dessen das Skript ausgeführt werden soll. • **Wenn sich ein Benutzer am System anmeldet** — Das Skript wird ausgeführt, wenn sich ein Benutzer am Workload anmeldet. • **Wenn sich ein Benutzer vom System abmeldet** — Das Skript

Einstellung	Beschreibung
	wird ausgeführt, wenn sich ein Benutzer vom Workload abmeldet. • **Beim Systemstart** — Das Skript wird ausgeführt, wenn das Betriebssystem des Workloads startet. • **Wenn das System heruntergefahren wird** — Das Skript wird ausgeführt, wenn der Workload heruntergefahren wird. • **Wenn das System online geht** — Das Skript wird ausgeführt, wenn der Workload online verfügbar wird. **Startbedingungen** — Der Task wird nur dann zu einem bestimmten Zeitpunkt oder Ereignis ausgeführt, wenn die entsprechende Bedingung erfüllt ist. Bei mehreren Bedingungen müssen diese alle gleichzeitig zutreffen, damit der Task gestartet werden kann. Standardmäßig ist die Bedingung **Standby- oder Ruhezustandsmodus verhindern, um einen geplanten Task zu starten** ausgewählt. **Wenn die Startbedingungen nicht erfüllt sind, Task trotzdem ausführen** — Diese Bedingung ist standardmäßig aktiviert. Der Standardwert ist 1 Stunde.
Konto zur Ausführung des Skripts	Das Konto, unter dem das Skript ausgeführt werden soll. Die nachfolgenden Werte sind verfügbar. • **Systemkonto** — Dies ist der Standardwert. • **Derzeit angemeldetes Konto**
Maximale Dauer	Der maximale Zeitraum, innerhalb dessen das Skript auf dem Workload ausgeführt werden darf. Wenn das Skript nicht innerhalb dieses Zeitraums abgeschlossen wird, wird die Operation fehlschlagen. Geben Sie einen ganzzahligen Wert im Bereich 1–1440 (Minuten) ein. Der Standardwert ist 3 Minuten.
PowerShell-Ausführungsrichtlinie	Die PowerShell-Ausführungsrichtlinie. Die nachfolgenden Werte sind verfügbar. • **Undefined** • **AllSigned** • **Bypass** — Dies ist der Standardwert. • **RemoteSigned** • **Restricted** • **Unrestricted** Weitere Informationen zu diesen Werten finden Sie in der

Einstellung	Beschreibung
	Microsoft-Dokumentation.

Monitoring-Pläne

Monitoring-Pläne sind Pläne, die Sie auf Ihre verwalteten Workloads anwenden, um die Monitoring-Funktionalität zu aktivieren und zu konfigurieren.

Wenn kein Monitoring-Plan auf einen Workload angewendet wird, sind für den Workload auch keine Monitoring-Funktionen verfügbar.

Hinweis
Die Verfügbarkeit der Einstellungen, die Sie in dem jeweiligen Monitoring-Plan konfigurieren können, hängt von dem Service-Paket ab, das auf den Mandanten angewendet wurde. Wenn Sie auf alle Einstellungen zugreifen wollen, müssen Sie das Advanced Management-Paket aktivieren.

Einen Monitoring-Plan erstellen

Sie können einen Monitoring-Plan erstellen und diesem dann Workloads hinzufügen, um die Monitoring-Funktionalität für die verwalteten Workloads zu konfigurieren.

Voraussetzungen

Die auf dem Workload installierte Version des Agenten unterstützt die Monitoring-Funktionalität.

So können Sie einen Monitoring-Plan erstellen

Von Monitoring-Pläne ausgehend

1. Gehen Sie in der Schutz-Konsole zum Bereich **Verwaltung** –> **Monitoring-Pläne**.
2. Erstellen Sie einen Monitoring-Plan, indem Sie eine der beiden Optionen verwenden.
   - Wenn es in der Liste keine Monitoring-Pläne gibt, klicken Sie auf **Erstellen**.
   - Wenn es in der Liste bereits Monitoring-Pläne gibt, klicken Sie auf **Plan erstellen**.
3. Gehen Sie im Fenster **Monitoring-Plan erstellen**, je nachdem, ob das Advanced Management-Paket für Ihren Mandanten aktiviert ist, folgendermaßen vor:
   - Wenn Ihr Mandant die Standard Protection-Funktionalität verwendet, werden dem Monitoring-Plan die folgenden vier Monitore automatisch hinzugefügt: Speicherplatz, Hardware-Änderungen, letzter System-Neustart sowie Größe der Dateien und Ordner.
   - Wenn das Advanced Management-Paket für Ihren Mandanten aktiviert ist, wählen Sie zuerst eine der Vorlagenoptionen aus, und klicken Sie anschließend auf **Weiter**.

Option	Beschreibung
Empfohlen	Wählen Sie diese Option, um einen Monitoring-Plan mit der Standard-Monitoring-Konfiguration zu erstellen.

Option	Beschreibung
Benutzerdefiniert	Verwenden Sie diese Option, um einen Monitoring-Plan komplett neu zu erstellen.

4. [Optional] Wenn Sie den Standardnamen für den Plan ändern wollen, müssen Sie auf das Stiftsymbol klicken, den gewünschten Namen eingeben und dann auf **OK** klicken.
5. [Optional] Wenn Sie dem Plan einen Monitor hinzufügen wollen, klicken Sie zuerst auf **Monitor hinzufügen**, dann auf den gewünschten Monitor in der Liste und anschließend auf **Hinzufügen**.

   Hinweis
   Die Einstellungen des Monitors werden automatisch mit den Standardwerten ausgefüllt.
   Sie können maximal drei Monitore desselben Typs und insgesamt bis zu 30 Monitore zu einem Monitoring-Plan hinzufügen.

6. [Optional] Ändern Sie in der Anzeige der Monitor-Parameter die Standardeinstellungen für den Monitor sowie die Alarmmeldungen – und klicken Sie anschließend auf **Fertig**.

   Hinweis
   Sie können für jeden Monitor unterschiedliche Einstellungen konfigurieren. Weitere Informationen dazu finden Sie in den Abschnitten '"Konfigurierbare Monitore" (S. 1132)' und '"Monitoring-Alarmmeldungen konfigurieren" (S. 1181)'.

7. [Optional] Wenn Sie einen Monitor löschen wollen, klicken Sie zuerst auf das Papierkorb-Symbol und anschließend auf **Löschen**.
8. [Optional] So können Sie dem Plan Workloads hinzufügen:
   a. Klicken Sie auf **Workloads hinzufügen**.
   b. Wählen Sie die Workloads aus und klicken Sie dann auf **Hinzufügen**.
   c. Wenn es Kompatibilitätsprobleme gibt, die Sie beheben wollen, befolgen Sie die im Abschnitt '"Kompatibilitätsprobleme mit Monitoring-Plänen beheben" (S. 1180)' beschriebene Prozedur.
9. Klicken Sie auf **Erstellen**.

Von 'Alle Geräte' ausgehend

1. Gehen Sie in der Schutz-Konsole zu **Geräte** –> **Alle Geräte**.
2. Klicken Sie auf den Workload, auf den ein Monitoring-Plan angewendet werden soll.
3. Klicken Sie auf den Befehl **Schützen**.
4. Gehen Sie – in Abhängigkeit davon, ob ein Monitoring-Plan auf den Workload angewendet wurde – folgendermaßen vor:
   - Wenn bereits ein Monitoring-Plan auf den Workload angewendet wurde, dann klicken Sie zuerst auf **Plan erstellen** und wählen Sie anschließend die Option **Monitoring**.
   - Wenn noch kein Monitoring-Plan auf den Workload angewendet wurde, dann klicken Sie

zuerst auf **Plan hinzufügen** und anschließend auf **Plan erstellen**. Danach müssen Sie **Monitoring** auswählen.

5. Wählen Sie im Fenster **Monitoring-Plan erstellen** eine der Vorlagenoptionen und klicken Sie anschließend auf **Weiter**.

Option	Beschreibung
Empfohlen	Wählen Sie diese Option, um einen Monitoring-Plan mit der Standard-Monitoring-Konfiguration zu erstellen.
Benutzerdefiniert	Verwenden Sie diese Option, um einen Monitoring-Plan komplett neu zu erstellen.

6. [Optional] Wenn Sie den Standardnamen für den Plan ändern wollen, müssen Sie auf das Stiftsymbol klicken, den gewünschten Namen eingeben und dann auf **OK** klicken.
7. [Optional] Wenn Sie die Standardeinstellungen des Monitors und der Alarmmeldungen ändern wollen, müssen Sie zuerst die neuen Werte konfigurieren und anschließend auf **Fertig** klicken.

   Hinweis
   Sie können maximal drei Monitore desselben Typs und insgesamt bis zu 30 Monitore zu einem Monitoring-Plan hinzufügen.

8. [Optional] Ändern Sie in der Anzeige der Monitor-Parameter die Standardeinstellungen für den Monitor sowie die Alarmmeldungen – und klicken Sie anschließend auf **Fertig**.

   Hinweis
   Sie können für jeden Monitor unterschiedliche Einstellungen konfigurieren. Weitere Informationen dazu finden Sie in den Abschnitten '"Konfigurierbare Monitore" (S. 1132)' und '"Monitoring-Alarmmeldungen konfigurieren" (S. 1181)'.

9. [Optional] Wenn Sie einen Monitor löschen wollen, klicken Sie zuerst auf das Papierkorb-Symbol und anschließend auf **Löschen**.
10. Klicken Sie auf **Erstellen**.

Workloads zu Monitoring-Plänen hinzufügen

Nachdem ein Monitoring-Plan erstellt wurde, können Sie diesem je nach Bedarf Workloads hinzufügen.

Voraussetzungen

- Für Ihr Benutzerkonto ist die Zwei-Faktor-Authentifizierung aktiviert.
- Die auf dem Workload installierte Version des Agenten unterstützt die Monitoring-Funktionalität.
- Es ist mindestens ein Monitoring-Plan verfügbar.

So können Sie einen Workload zu einem Monitoring-Plan hinzufügen

Von Monitoring-Pläne ausgehend

1. Gehen Sie in der Schutz-Konsole zum Bereich **Verwaltung** –> **Monitoring-Pläne**.
2. Klicken Sie auf den Monitoring-Plan.
3. Gehen Sie je nachdem, ob der Plan bereits auf einen Workload angewendet wurde, folgendermaßen vor:
   - Klicken Sie auf **Workloads hinzufügen**, wenn der Plan bisher noch auf keinen Workload angewendet wurde.
   - Klicken Sie auf **Workloads verwalten**, wenn der Plan schon auf einen beliebigen Workloads angewendet wurde.
4. Wählen Sie zuerst auf einen Workload aus der Liste aus und klicken Sie anschließend auf **Hinzufügen**.
5. Klicken Sie auf **Speichern**.
6. Klicken Sie bei Bedarf auf **Bestätigen**, um die erforderliche Service-Quota auf den Workload anzuwenden.

Von Alle Geräte ausgehend

1. Gehen Sie in der Schutz-Konsole zu **Geräte** –> **Alle Geräte**.
2. Klicken Sie auf den Workload, auf den ein Monitoring-Plan angewendet werden soll.
3. Klicken Sie auf den Befehl **Schützen.**
4. Suchen Sie den Monitoring-Plan, dem Sie den Workload hinzufügen wollen, und klicken Sie anschließend auf **Anwenden**.
5. Klicken Sie bei Bedarf auf **Bestätigen**, um die erforderliche Service-Quota auf den Workload anzuwenden.

Monitoring-Pläne widerrufen

Sie können einen Monitoring-Plan von einem Workload widerrufen, auf den der Plan angewendet wurde.

Voraussetzungen

Es wird mindestens ein Monitoring-Plan auf den Workload angewendet.

So können Sie einen Monitoring-Plan widerrufen

1. Gehen Sie in der Schutz-Konsole zu **Geräte** –> **Alle Geräte**.
2. Klicken Sie zuerst auf den Workload und anschließend auf **Schützen**.
3. Klicken Sie auf das Symbol **Mehr Aktionen** des Monitoring-Plans, den Sie widerrufen wollen, und anschließend auf **Widerrufen**.

Automatische Antwortaktionen konfigurieren

Automatische Antwortaktionen auf die per Alarm gemeldeten Ereignisse sind vordefinierte Aktionen oder Maßnahmen, die automatisch als Reaktion auf erkannte Ereignisse oder Vorfälle ausgelöst werden. Diese Maßnahmen sind darauf ausgelegt, potenzielle Bedrohungen abzuschwächen und Schäden zu minimieren.

Sie können eine oder mehrere automatische Antwortaktionen konfigurieren, die auf per Alarm gemeldete Ereignisse ausgelöst werden sollen. Die maximale Anzahl der automatischen Antwortaktionen pro Monitor beträgt 20.

So können Sie automatische Antwortaktionen konfigurieren

1. Gehen Sie in der Schutz-Konsole zum Bereich **Verwaltung** –> **Monitoring-Pläne**.
2. Wählen Sie den Monitoring-Plan aus, für den Sie automatische Antwortaktionen konfigurieren wollen.
3. Wählen Sie den Monitor aus, für den Sie automatische Antwortaktionen konfigurieren wollen. Wenn Sie noch keine Monitore hinzugefügt haben, können Sie alternativ auch auf **Monitor hinzufügen** klicken, den gewünschten Monitor in der Liste auswählen, dann auf **Hinzufügen** klicken und abschließend den Monitor auswählen.
4. Klicken Sie auf den Link neben **Automatische Antwortaktionen**.
5. Fügen Sie im Fenster **Automatische Antwortaktionen** eine oder mehrere Antwortaktionen hinzu, die automatisch ausgeführt werden sollen, wenn ein Alarm ausgelöst wird.
6. Konfigurieren Sie jede der Antwortaktionen. Gehen Sie beispielsweise folgendermaßen vor, wenn Sie die Antwortaktion **Einen Windows-Dienst starten** hinzugefügt haben:
   a. Klicken Sie neben **Windows-Dienst** auf **Spezifizieren**.
   b. Wählen Sie im Feld **Dienst** einen Dienst aus, der als Antwortaktion gestartet werden soll.
   c. Klicken Sie auf **Fertig**.
7. Verwenden Sie in der Liste der hinzugefügten Antwortaktionen die Auf- und Abwärtspfeile oder verschieben Sie diese per Drag & Drop, um die Reihenfolge der Antwortaktionen einzustellen.
8. Konfigurieren Sie, wie aufeinanderfolgende Antwortaktionen behandelt werden sollen, wenn eine vorherige Antwortaktion fehlschlagen sollte. Wählen Sie eine der folgenden Möglichkeiten:
   a. **Mit der nächsten Antwortaktion fortfahren**.
   b. **Nicht mit der nächsten Antwortaktion fortfahren**.
9. Klicken Sie auf **Fertig**.

   Neben der Einstellung **Automatische Antwortaktionen** Ihres Monitoring-Plans wird Ihnen die Anzahl der konfigurierten Aktionen angezeigt. Sie können diese Aktionen bearbeiten oder löschen – oder auch zu einem späteren Zeitpunkt neue Aktionen hinzufügen.

In der nachfolgenden Tabelle werden alle automatischen Antwortaktionen aufgelistet und beschrieben, die in den Monitor-Einstellungen verfügbar sind.

Automatische Antwortaktion	Beschreibung	Unterstütztes Betriebssystem
Ein Skript ausführen	Wenn Sie diese Aktion hinzufügen, können Sie: 1. Ein bestimmtes Skript auswählen, das auf dem Workload ausgeführt werden soll. 2. Das Benutzerkonto spezifizieren, unter dem Sie das Skript ausführen wollen. 3. Die maximale Dauer der Aktion spezifizieren. 4. Die PowerShell-Ausführungsrichtlinie spezifizieren. 5. Ein Skript ausführen. Wenn Sie diese Aktion durchführen wollen, benötigen Sie eine Lizenz für das Advanced Management-Paket für den betreffenden Workload (falls noch keine Lizenz zugewiesen wurde). Das System wird das ausgewählte Remote-Skript mit den spezifizierten Parametern ausführen, wenn die Bedingungen erfüllt sind.	Windows, macOS
Den Workload neu starten	Wenn Sie diese Aktion hinzufügen, wird das System den Workload per Remote-Steuerung neu starten, wenn die Bedingungen erfüllt sind.	Windows, macOS
Den Prozess stoppen	Wenn Sie diese Aktion hinzufügen, können Sie den Prozess, der gestoppt werden soll, durch manuelle Eingabe des Prozessnamens spezifizieren. Das System wird den Prozess stoppen, wenn die Bedingungen erfüllt sind.	Windows, macOS
Den Windows-Dienst starten	Wenn Sie diese Aktion hinzufügen, können Sie aus einer dynamischen Liste von Diensten, die von den Agenten zusammengestellt wurden, auswählen, welcher Windows-Dienst gestartet werden soll. Das System wird den Dienst starten, wenn die Bedingungen erfüllt sind.	Windows

Automatische Antwortaktion	Beschreibung	Unterstütztes Betriebssystem
Den Windows-Dienst stoppen	Wenn Sie diese Aktion hinzufügen, können Sie aus einer dynamischen Liste von Diensten, die von den Agenten zusammengestellt wurden, auswählen, welcher Windows-Dienst gestoppt werden soll. Das System wird den Dienst stoppen, wenn die Bedingungen erfüllt sind.	Windows
Windows Update aktivieren	Wenn Sie diese Aktion hinzufügen, wird das System das Windows Update aktivieren, wenn die Bedingungen erfüllt sind. Diese Aktion ist nur für den Monitor 'Windows Update-Status' verfügbar.	Windows
AutoRun auf Wechsellaufwerken deaktivieren	Wenn Sie diese Aktion hinzufügen, wird das System die AutoRun-Funktion für Wechselmedien auf dem Workload deaktivieren, wenn die Bedingungen erfüllt sind. Diese Aktion ist nur für den Monitor 'Status der AutoRun-Funktion' verfügbar.	Windows

Zusätzliche Aktionen mit Monitoring-Plänen

Sie können von der Anzeige **Monitoring-Pläne** aus folgende zusätzliche Aktionen mit den Monitoring-Plänen durchführen: Details anzeigen, bearbeiten, die Aktivitäten anzeigen, die Alarmmeldungen anzeigen, umbenennen, aktivieren, deaktivieren, klonen, exportieren und löschen.

Details anzeigen

So können Sie die Details zu einem Monitoring-Plan einsehen

1. Klicken Sie in der Anzeige **Monitoring-Pläne** auf das Symbol **Mehr Aktionen** des Monitoring-Plans.
2. Klicken Sie auf **Details anzeigen**.
3. [Optional] Wenn Sie die Details zu einem Monitor einsehen wollen, der im Plan aktiviert ist, müssen Sie auf den Namen des Monitors klicken.

Bearbeiten

Voraussetzungen

Für Ihr Benutzerkonto ist die Zwei-Faktor-Authentifizierung aktiviert.

So können Sie einen Plan bearbeiten

1. Klicken Sie in der Anzeige **Monitoring-Pläne** auf das Symbol **Mehr Aktionen** des Monitoring-Plans.
2. Klicken Sie auf **Bearbeiten**.
3. [Optional] Wenn Sie einen Monitor aus dem Plan löschen wollen, klicken Sie auf das Papierkorb-Symbol, das sich rechts neben dem Namen des Monitors befindet.
4. [Optional] Wenn Sie einen Monitor in dem Plan (de)aktivieren wollen, müssen Sie den Schalter neben dem Namen des Monitors umschalten.
5. [Optional] Gehen Sie folgendermaßen vor, um die Monitor-Parameter zu bearbeiten.
   a. Klicken Sie auf den Namen des Monitors.
   b. Klicken Sie auf den Überblick für die Monitor-Parameter.
   c. Konfigurieren Sie in der Anzeige **Monitor-Parameter** die gewünschten Parameter und klicken Sie dann auf **Fertig**.

      Hinweis
      Sie können für jeden Monitor unterschiedliche Einstellungen konfigurieren. Weitere Informationen dazu finden Sie in den Abschnitten '"Konfigurierbare Monitore" (S. 1132)' und '"Monitoring-Alarmmeldungen konfigurieren" (S. 1181)'.

   d. Schließen Sie die Anzeige und bestätigen Sie die Änderungen.
6. [Optional] Wenn Sie einen Monitor hinzufügen wollen, müssen Sie auf den Befehl **Monitor hinzufügen** klicken und anschließend, falls erforderlich, die Parameter bearbeiten (wie im vorherigen Schritt erläutert).
7. Klicken Sie auf **Speichern**.

Aktivitäten

So können Sie die zu einem Monitoring-Plan gehörenden Aktivitäten einsehen

1. Klicken Sie in der Anzeige **Monitoring-Pläne** auf das Symbol **Mehr Aktionen** des Monitoring-Plans.
2. Klicken Sie auf **Aktivitäten**.
3. Klicken Sie auf eine Aktivität, um sich weitere Details zu dieser anzeigen zu lassen.

Alarmmeldungen

So können Sie die Alarmmeldungen einsehen

1. Klicken Sie in der Anzeige **Monitoring-Pläne** auf das Symbol **Mehr Aktionen** des Monitoring-Plans.
2. Klicken Sie auf **Alarmmeldungen**.

Umbenennen

Voraussetzungen

Für Ihr Benutzerkonto ist die Zwei-Faktor-Authentifizierung aktiviert.

So können Sie einen Monitoring-Plan umbenennen

1. Klicken Sie in der Anzeige **Monitoring-Pläne** auf das Symbol **Mehr Aktionen** des Monitoring-Plans.
2. Klicken Sie auf **Umbenennen**.
3. Geben Sie den neuen Plan-Namen ein und klicken Sie dann auf **OK**.

Aktivieren

Voraussetzungen

- Für Ihr Benutzerkonto ist die Zwei-Faktor-Authentifizierung aktiviert.
- Der Monitoring-Plan wird auf mindestens einen Workload angewendet.

So können Sie einen Monitoring-Plan aktivieren

1. Klicken Sie in der Anzeige **Monitoring-Pläne** auf das Symbol **Mehr Aktionen** des Monitoring-Plans.
2. Klicken Sie auf **Aktivieren**.

Deaktivieren

Voraussetzungen

Für Ihr Benutzerkonto ist die Zwei-Faktor-Authentifizierung aktiviert.

So können Sie einen Monitoring-Plan deaktivieren

1. Klicken Sie in der Anzeige **Monitoring-Pläne** auf das Symbol **Mehr Aktionen** des Monitoring-Plans.
2. Klicken Sie auf **Deaktivieren**.

Klonen

Voraussetzungen

Für Ihr Benutzerkonto ist die Zwei-Faktor-Authentifizierung aktiviert.

So können Sie einen Monitoring-Plan klonen

1. Klicken Sie in der Anzeige **Monitoring-Pläne** auf das Symbol **Mehr Aktionen** des Monitoring-Plans.
2. Klicken Sie auf **Klonen**.
3. Klicken Sie auf **Erstellen**.

Exportieren

Voraussetzungen

Für Ihr Benutzerkonto ist die Zwei-Faktor-Authentifizierung aktiviert.

So können Sie einen Monitoring-Plan exportieren

1. Klicken Sie in der Anzeige **Monitoring-Pläne** auf das Symbol **Mehr Aktionen** des Monitoring-Plans.
2. Klicken Sie auf **Exportieren**.
   Die Plan-Konfiguration wird im JSON-Format auf die lokale Maschine exportiert.

Löschen

Voraussetzungen

Für Ihr Benutzerkonto ist die Zwei-Faktor-Authentifizierung aktiviert.

So können Sie einen Monitoring-Plan löschen

1. Klicken Sie in der Anzeige **Monitoring-Pläne** auf das Symbol **Mehr Aktionen** des Monitoring-Plans.
2. Klicken Sie auf **Löschen**.
3. Wählen Sie **Ich bestätige** und klicken Sie anschließend auf **Löschen**.

Kompatibilitätsprobleme mit Monitoring-Plänen

In einigen Fällen kann es zu Kompatibilitätsproblemen kommen, wenn Sie einen Monitoring-Plan auf einen Workload anwenden. Sie werden möglicherweise folgende Kompatibilitätsprobleme feststellen:

- Inkompatibles Betriebssystem – zu diesem Problem kommt es, wenn das Betriebssystem des Workloads nicht unterstützt wird.
- Nicht unterstützter Agent – zu diesem Problem kommt es, wenn die Version des Protection Agenten auf dem Workload veraltet ist und die Monitoring-Funktionalität nicht unterstützt.
- Unzureichende Quota – zu diesem Problem kommt es, wenn im Mandanten die Service-Quota nicht ausreicht, um sie den ausgewählten Workloads zuweisen zu können.

Wenn der Monitoring-Plan auf bis zu 150 persönlich ausgewählte Workloads angewendet wird, werden Sie aufgefordert, die bestehenden Konflikte zu lösen, bevor Sie den Plan speichern. Sie können einen Konflikt auflösen, indem Sie entweder dessen Ursache beseitigen oder indem Sie die betroffenen Workloads aus dem Plan entfernen. Weitere Informationen finden Sie im Abschnitt '"Kompatibilitätsprobleme mit Monitoring-Plänen beheben" (S. 1180)'. Wenn Sie den Plan speichern, ohne die Konflikte zu lösen, wird er automatisch für die inkompatiblen Workloads deaktiviert und werden entsprechende Alarmmeldungen angezeigt.

Wenn der Monitoring-Plan auf mehr als 150 Workloads oder Gerätegruppen angewendet wird, wird der Plan zuerst gespeichert und dann auf Kompatibilität überprüft. Der Plan wird automatisch für die nicht unterstützten Workloads deaktiviert und es werden entsprechende Alarmmeldungen angezeigt.

Kompatibilitätsprobleme mit Monitoring-Plänen beheben

Je nach Art der Kompatibilitätsprobleme können Sie beim Erstellen eines neuen Monitoring-Plans verschiedene Aktionen durchführen, um diese Kompatibilitätsprobleme zu beheben.

So können Sie die Kompatibilitätsprobleme beheben

1. Klicken Sie auf **Probleme überprüfen**.
2. [Optional] So können Sie Kompatibilitätsprobleme mit inkompatiblen Betriebssystemen beheben, indem Sie Workloads aus dem Plan entfernen:
   a. Wählen Sie auf der Registerkarte **Inkompatibles Betriebssystem** diejenigen Workloads aus, die Sie entfernen wollen.
   b. Klicken Sie auf **Workloads aus dem Plan entfernen**.
   c. Klicken Sie zuerst auf **Entfernen** und dann auf **Schließen**.
3. [Optional] So können Sie Kompatibilitätsprobleme mit inkompatiblen Betriebssystemen beheben, indem Sie einen Monitor im Plan deaktivieren:
   a. Wählen Sie auf der Registerkarte **Inkompatibles Betriebssystem** diejenigen Monitore aus, die Sie entfernen wollen.
   b. Klicken Sie auf **Monitor deaktivieren**.
   c. Klicken Sie zuerst auf **Deaktivieren** und dann auf **Schließen**.
4. [Optional] So können Sie Kompatibilitätsprobleme mit nicht unterstützten Agenten beheben, indem Sie Workloads aus dem Plan entfernen:
   a. Wählen Sie auf der Registerkarte **Nicht unterstützte Agenten** diejenige Workloads aus, die Sie entfernen wollen.
   b. Klicken Sie auf **Workloads aus dem Plan entfernen**.
   c. Klicken Sie zuerst auf **Entfernen** und dann auf **Schließen**.
5. [Optional] Wenn Sie Kompatibilitätsprobleme mit nicht unterstützten Agenten durch Aktualisierung der Agenten-Version beheben wollen, klicken Sie auf **Zur Agenten-Liste gehen**.

   Hinweis
   Diese Option ist nur für Kunden-Administratoren verfügbar.

6. [Optional] So können Sie Kompatibilitätsprobleme durch eine unzureichende Quota beheben, indem Sie Workloads aus dem Plan entfernen:
   a. Wählen Sie auf der Registerkarte **Unzureichende Quota** diejenige Workloads aus, die Sie entfernen wollen.
   b. Klicken Sie auf **Workloads aus dem Plan entfernen**.
   c. Klicken Sie zuerst auf **Entfernen** und dann auf **Schließen**.
7. [Optional] So können Sie Kompatibilitätsprobleme mit einer unzureichenden Quota lösen, indem Sie die Quota des Mandanten vergrößern:

a. Klicken Sie auf der Registerkarte **Unzureichende Quota** auf den Befehl **Zum Management-Portal gehen**.
b. Vergrößern Sie die Service-Quota für den Kunden.

Hinweis
Diese Option ist nur für Partner-Administratoren verfügbar.

Die Machine Learning-Modelle zurücksetzen

Sie können die Modelle eines Workloads zurücksetzen, wenn sie aus irgendeinem Grund veraltet oder ungültig geworden sind. Durch diese Aktion werden die erstellten Modelle und die Daten gelöscht, die von den Monitoren mit Anomalie-basierter Überwachung für den Workload gesammelt wurden. Anschließend werden die Machine Learning-Modelle für den Workload ganz neu trainiert.

So können Sie die Machine Learning-Modelle für einen Workload zurücksetzen

1. Gehen Sie in der Schutz-Konsole zu **Geräte** –> **Alle Geräte**.
2. Klicken Sie zuerst auf einen Workload in der Liste und anschließend auf die Registerkarte **Details**.
3. Klicken Sie im Bereich **Machine Learning-Modelle zurücksetzen** auf **Zurücksetzen**.
4. Klicken Sie im Bestätigungsfenster erneut auf **Zurücksetzen**.

Monitoring-Alarmmeldungen

Monitoring-Alarmmeldungen werden in der Schutz-Konsole angezeigt und per E-Mail versendet, wenn das überwachte Verhalten von Workloads außerhalb des Normbereichs liegt. Die Alarmmeldungen sorgen dafür, dass die Betroffenen so schnell wie möglich informiert werden, wenn es Probleme in der IT-Umgebung der Organisation gibt.

Hinweis
Um Monitoring-Alarmmeldungen über E-Mail zu aktivieren, müssen Sie mindestens eine E-Mail-Benachrichtigungsrichtlinie für den entsprechenden Alarmtyp konfigurieren. Weitere Informationen finden Sie im Abschnitt '"E-Mail-Benachrichtigungsrichtlinien konfigurieren" (S. 1189)'.

Monitoring-Alarmmeldungen konfigurieren

Sie können die Alarmeinstellungen des Monitors konfigurieren, wenn Sie einen Monitor zu einem Monitoring-Plan hinzufügen – oder wenn Sie einen Monitor bearbeiten, der bereits in einem Monitoring-Plan vorhanden ist.

So können Sie Monitoring-Alarmmeldungen konfigurieren

1. Gehen Sie im Fenster **Monitor-Parameter** zum Abschnitt **Alarmmeldungen generieren**.
2. Wählen Sie bei **Alarmschweregrad** den Schweregrad aus, der der Priorität des Alarms entspricht.

Option	Beschreibung
Kritisch	Diese Alarmmeldungen haben die höchste Priorität und beziehen sich auf Probleme, die kritisch für den Betrieb des Workloads sind. Sie sollten diese Probleme so schnell wie möglich beheben.
Fehler	Eine Fehlermeldung ist weniger schwerwiegend und gibt an, dass etwas fehlerhaft ist oder nicht normal funktioniert. Sie sollten die betreffenden Probleme zeitnah beheben, um zu verhindern, dass sie noch größere Probleme verursachen.
Warnung	Eine Warnmeldung bedeutet, dass ein Zustand vorliegt, den Sie beachten sollten, der aber möglicherweise noch kein Problem darstellt. Sie sollten diese Probleme beheben, nachdem Sie die Probleme behoben haben, die kritische Alarmmeldungen und Fehlermeldungen verursachen. Dies ist der Standardwert.
Informationell	Diese Alarmmeldungen haben die niedrigste Priorität. Dieser informative Schweregrad zeigt kein Problem an. Solche Alarmmeldungen informieren Sie über Aktionen, die mit einem überwachten Objekt zusammenhängen.

3. Wählen Sie unter **Alarm-Häufigkeit**, wie oft das System eine Alarmmeldung generieren soll, wenn die entsprechende Bedingung erfüllt ist.

Option	Beschreibung
Einmal, bis die Prüfung bestanden ist	Das System wird ein Mal eine Alarmmeldung generieren, bis die Prüfung erfolgreich abgeschlossen ist. Dies ist der Standardwert.
Nach X aufeinanderfolgenden Fehlschlägen	Das System wird einen Alarm generieren, nachdem X aufeinanderfolgende Prüfungen fehlgeschlagen sind – wobei X für eine ganze Zahl steht.

4. Klicken Sie bei **Alarmmeldung** auf das Stiftsymbol, um die Standard-Alarmmeldung zu bearbeiten. Auf diese wird zurückgegriffen, wenn das System eine Alarmmeldung generiert. Sie können eine benutzerdefinierte Alarmmeldung spezifizieren, die Variablen enthält. Weitere Informationen zu den verwendbaren Variablen finden Sie im Abschnitt '"Monitoring-Alarmvariablen" (S. 1183)'.

   Hinweis
   Für einige der Monitore können Sie mehr als eine Alarmmeldung konfigurieren.

5. Aktivieren Sie die Option **Alarm-Auto-Auflösung**, wenn Sie wollen, dass das System die Alarmmeldungen automatisch auflöst, wenn die überwachte Metrik in den normalen Zustand zurückkehrt und das Verhalten wieder normal ist. Die Einstellung ist standardmäßig aktiviert.

Monitoring-Alarmvariablen

Sie können verschiedene Alarmvariablen für unterschiedliche Monitore konfigurieren. Wenn Sie eine Variable verwenden wollen, muss diese in die Zeichen {{}} eingeschlossen werden.

Die nachfolgende Tabelle gibt Ihnen weitere Informationen über die verfügbaren Variablen.

Variable	Beschreibung	Verfügbar für den Monitor
plan_name	Der Name der Richtlinie	Alle Monitore
monitor_name	Der Name der Unterrichtlinie im Monitoring-Plan	Alle Monitore
workload_ name	Der Name des Workloads	Alle Monitore
threshold_ value	Bestimmte Monitoring-Bedingungen oder Grenzwerte für die Generierung einer Alarmmeldung	Alle Monitore, die Grenzwert-basiertes Monitoring unterstützen.
threshold_unit	Die Einheit, die mit dem Grenzwert zugeordnet wird. Beispielsweise %, MB oder mb/s.	Alle Monitore, die Grenzwert-basiertes Monitoring unterstützen.
time_period	Das System wird nur dann eine Alarmmeldung für ein erkanntes Problem generieren, wenn der Metrikwert während des spezifizierten Zeitraums außerhalb der Norm liegt.	Alle Monitore, die Grenzwert-basiertes Monitoring unterstützen.
time_unit	Die Einheit, die dem Zeitraum zugeordnet wird (Sekunden/Minuten/Stunden/Tag).	Alle Monitore, die Grenzwert-basiertes Monitoring unterstützen.
anomaly_value	Der Anomaliewert	Alle Monitore, die Anomalie-basiertes Monitoring unterstützen.
anomaly_unit	Die Einheit, die dem Anomaliewert zugeordnet wird	Alle Monitore, die Anomalie-basiertes Monitoring unterstützen.
deviation_value	Der Abweichungswert	Alle Monitore, die Anomalie-basiertes Monitoring unterstützen.
deviation_unit	Die Einheit, die dem Abweichungswert zugeordnet wird	Alle Monitore, die Anomalie-basiertes Monitoring unterstützen.

Variable	Beschreibung	Verfügbar für den Monitor
drive_name	Das Laufwerk bei Windows bzw. die Partition bei macOS	Laufwerksspeicherplatz,
CPU_model	Das Modell der überwachten CPU	CPU-Temperatur
GPU_model	Das Modell der überwachten GPU	GPU-Temperatur
hardware_ model	Das Modell der überwachten Komponente	Hardware-Änderungen
hardware_ component	Der Typ der überwachten Hardware	Hardware-Änderungen
hardware_ model_old	Das Modell der überwachten Komponente, die ausgetauscht wurde	Hardware-Änderungen
hardware_ model_new	Das Modell der überwachten neuen Komponente, die hinzugefügt wurde	Hardware-Änderungen
disk_model	Das Modell des Laufwerks	Laufwerk-Übertragungsrate
network_ adapter_model	Das Modell des Netzwerkadapters	Netzwerknutzung
process_name	Der Name des Prozesses	CPU-Nutzung nach Prozess Arbeitsspeicher-Nutzung nach Prozess Laufwerk-Übertragungsrate nach Prozess Netzwerknutzung nach Prozess Prozessstatus
service_name	Der Name des Dienstes	Windows-Dienst-Status
software_name	Der Name der Software-Applikation	Installierte Software
software_ version	Die Version der Software-Applikation	Installierte Software
software_ version_old	Die Version der Software-Applikation vor dem Update	Installierte Software

Variable	Beschreibung	Verfügbar für den Monitor
software_ version_new	Die Version der neuen oder aktualisierten Software-Applikation	Installierte Software
number_of_ occurrences	Die Anzahl, wie oft ein Ereignis im Protokoll enthalten ist	Windows-Ereignisprotokoll
event_types	Der Typ des Ereignisses	Windows-Ereignisprotokoll
event_source	Die Quelle des Ereignisses	Windows-Ereignisprotokoll
event_log_ name	Der Name des Ereignisses	Windows-Ereignisprotokoll
firewall_ software_name	Der Name der Firewall-Software	Firewall-Status
antimalware_ software_name	Der Name der Antimalware-Software	Antimalware-Software-Status
user_name	Der Name des Benutzers	Status der AutoRun-Funktion
script_name	Der Name des Skripts	Benutzerdefiniert

Manuelle Antwortaktionen

Wenn Sie einen Alarm sehen, können Sie eine Antwortaktion auswählen, die Sie auf die per Alarm gemeldeten Ereignisse anwenden wollen.

So können Sie eine manuelle Antwortaktion durchführen

1. Gehen Sie in der Schutz-Konsole zu **Alarmmeldungen**.
2. Öffnen Sie die Alarmmeldungen, die Sie einsehen wollen.
3. Klicken Sie auf **Antwortaktion** und wählen Sie dann im Listenfeld eine gewünschte Antwortaktion aus.

Die Liste der Antwortaktionen, die für eine bestimmte Alarmmeldung verfügbar sind, hängt davon ab, welcher Alarmtyp vorliegt, welche Funktionen für einen bestimmten Mandanten verfügbar sind und mit welchem Betriebssystem der Workload läuft.

Die nachfolgende Tabelle soll Ihnen als Referenz dienen und listet alle manuellen Antwortaktionen auf.

Manuelle Antwortaktion	Beschreibung	Unterstütztes Betriebssystem
Speicherplatz-Nutzungstrend durchsuchen	Öffnet ein Fenster mit dem Diagramm **Speicherplatznutzung**, in dem Sie Folgendes tun können: • Durchsuchen, wie sich die Speicherplatznutzung im Laufe der Zeit (für den/die letzten einen Tag / sieben Tage / einen Monat) verändert hat. • Die Veränderung („Delta“) der Speicherplatznutzung als relativer Wert (%) für den ausgewählten Zeitraum durchsuchen.	Windows, macOS
Den Dateigrößen-Wachstumstrend durchsuchen	Öffnet ein Fenster mit dem Diagramm **Dateigrößen-Wachstum**, in dem Sie Folgendes tun können: • Durchsuchen, wie sich die Gesamtgröße der überwachten Dateien und Ordner im Laufe der Zeit (für den/die letzten einen Tag / sieben Tage / einen Monat) verändert hat. • Die Veränderung („Delta“) der Gesamtgröße der Dateien als relativer Wert (%) für den ausgewählten Zeitraum durchsuchen.	Windows, macOS
Ein Skript ausführen	Öffnet ein Fenster, in welchem Sie Folgendes tun können: 1. Ein bestimmtes Skript auswählen, das auf dem Workload ausgeführt werden soll. 2. Das Benutzerkonto spezifizieren, unter dem Sie das Skript ausführen wollen. 3. Die maximale Dauer der Aktion spezifizieren. 4. Die PowerShell-Ausführungsrichtlinie spezifizieren. 5. Ein Skript ausführen. Wenn Sie diese Aktion durchführen wollen, benötigen Sie eine Lizenz für das Advanced Management-Paket für den	Windows, macOS

Manuelle Antwortaktion	Beschreibung	Unterstütztes Betriebssystem
	betreffenden Workload (falls noch keine Lizenz zugewiesen wurde).	
Über NEAR verbinden	Acronis Connect Client stellt eine Remote-Verbindung her.	Windows, macOS
Über RDP verbinden	Acronis Connect Client stellt eine Remote-Verbindung her.	Windows
Hardware-Inventar öffnen	Sie werden zur Registerkarte **Hardware-Inventarisierung** für den aktuellen Workload weitergeleitet.	Windows, macOS
Die Top 10 der CPU-belastenden Prozesse durchsuchen	Öffnet ein Fenster mit den 10 wichtigsten Prozessen, die die CPU belastet haben und daher eine Überhitzung verursacht haben könnten (der System-Snapshot zum Zeitpunkt der Alarm-Generierung).	Windows, macOS
Die Top 10 der GPU-belastenden Prozesse durchsuchen	Öffnet ein Fenster mit den 10 wichtigsten Prozessen, die die GPU belastet haben und daher eine Überhitzung verursacht haben könnten (der System-Snapshot zum Zeitpunkt der Alarm-Generierung).	Windows, macOS
Die Top 10 der Arbeitsspeicher-belastenden Prozesse durchsuchen	Öffnet ein Fenster mit den 10 wichtigsten Prozessen, die den Arbeitsspeicher (RAM) belastet haben (der System-Snapshot zum Zeitpunkt der Alarm-Generierung).	Windows, macOS
Die Top 10 der Laufwerk-belastenden Prozesse durchsuchen	Öffnet ein Fenster mit den 10 wichtigsten Prozessen, die das Laufwerk belastet haben (der System-Snapshot zum Zeitpunkt der Alarm-Generierung).	Windows, macOS
Die Top 10 der Netzwerk-belastenden Prozesse durchsuchen	Öffnet ein Fenster mit den 10 wichtigsten Prozessen, die den Netzwerkadapter belastet haben (der System-Snapshot zum Zeitpunkt der Alarm-Generierung).	Windows, macOS
Ressourcennutzung nach Prozess durchsuchen	Öffnet ein Fenster mit detaillierten Informationen über die Nutzung der Hardware-Ressourcen durch den	Windows, macOS

Manuelle Antwortaktion	Beschreibung	Unterstütztes Betriebssystem
	entsprechenden Prozess: CPU-, Arbeitsspeicher-, Laufwerks- und Netzwerkadapter-Nutzung.	
Workload neu starten	Öffnet ein Bestätigungsfenster. Der Workload wird nach der Bestätigung neu gestartet.	Windows, macOS
Windows-Dienst starten	Öffnet ein Bestätigungsfenster. Startet nach einer Bestätigung den Windows-Dienst.	Windows
Windows-Dienst stoppen	Öffnet ein Bestätigungsfenster. Stoppt nach einer Bestätigung den Windows-Dienst.	Windows
Prozess stoppen	Öffnet ein Bestätigungsfenster. Hält nach einer Bestätigung den Prozess an, auf den sich der Alarm bezieht.	Windows, macOS
Windows Update aktivieren	Öffnet ein Bestätigungsfenster. Aktiviert nach einer Bestätigung das Windows Update.	Windows
AutoRun-Funktion auf Wechsellaufwerken aktivieren	Öffnet ein Bestätigungsfenster. Deaktiviert nach einer Bestätigung die AutoRun-Funktion auf der Systemebene des Workloads.	Windows

Wichtig
Zur Durchführung der nachfolgenden manuellen Antwortaktionen ist aus Sicherheitsgründen eine Zwei-Faktor-Authentifizierung erforderlich:

- Ein Skript ausführen
- Über NEAR verbinden
- Über RDP verbinden
- Workload neu starten
- Windows-Dienst starten
- Windows-Dienst stoppen
- Prozess stoppen
- Windows Update aktivieren
- AutoRun-Funktion auf Wechsellaufwerken aktivieren

Die Monitoring-Alarmmeldungen für einen Workload einsehen

Auf der Registerkarte **Alarmmeldungen** können Sie die Monitoring-Alarmmeldungen für einen bestimmten Workload einsehen und verschiedene Alarmaktionen durchführen.

So können Sie die Monitoring-Alarmmeldungen für einen Workload einsehen

1. Gehen Sie in der Schutz-Konsole zu **Alle Geräte**.
2. Klicken Sie auf einen Workload und wählen Sie dann die Registerkarte **Alarmmeldungen** aus.
3. [Optional] Führen Sie im Monitoring-Alarm-Fensterbereich eine der folgenden Aktionen aus:
   - Wenn Sie den Alarm löschen wollen, klicken Sie auf **Bereinigen**.
   - Wenn Sie eine Antwortaktion ausführen wollen, klicken Sie zuerst auf **Antwortaktion** und dann auf die jeweilige Aktion.
   - Wenn Sie das Support-Team kontaktieren wollen, klicken Sie auf **Support anfordern**.
4. [Optional] Wenn Sie alle Monitoring-Alarmmeldungen für den Workload entfernen wollen, klicken Sie auf **Alle löschen**.

Das Alarmprotokoll der Monitoring-Alarmmeldungen einsehen

Sie können alle Ereignisse, die mit einem Monitoring-Alarm zusammenhängen, in chronologischer Reihenfolge einsehen: die Antwortaktionen (sowohl automatische als auch manuelle), die durchgeführt wurden, sowie die gesendeten E-Mail-Benachrichtigungen.

So können Sie das Überwachungsprotokoll eines Monitoring-Alarms einsehen

1. Gehen Sie in der Schutz-Konsole zu **Alarmmeldungen**.
2. Öffnen Sie die **Tabellenansicht**.
3. Klicken Sie in der Liste der Alarmmeldungen auf den Monitoring-Alarm, den Sie einsehen wollen.
4. Klicken Sie auf **Details** und dann auf **Alarmprotokoll**.

E-Mail-Benachrichtigungsrichtlinien konfigurieren

E-Mail-Benachrichtigungsrichtlinien spezifizieren, welche Benutzer E-Mail-Benachrichtigungen von unterschiedlichen Monitoren erhalten.

Über die Anzeige **E-Mail-Benachrichtigungen** können Sie folgende Aktionen mit E-Mail-Benachrichtigungsrichtlinien durchführen: hinzufügen, bearbeiten, aktivieren, deaktivieren und löschen.

Hinzufügen

So können Sie eine neue E-Mail-Benachrichtigungsrichtlinie hinzufügen

1. Gehen Sie in der Schutz-Konsole zu **Einstellungen** –> **E-Mail-Benachrichtigungen**.
2. Klicken Sie auf **Richtlinie hinzufügen**.

3. Klicken Sie auf **Empfänger auswählen**.
4. Wählen Sie auf der Anzeige **Empfänger auswählen** die Benutzer aus, die E-Mail-Alarmmeldungen erhalten sollen, und klicken Sie dann auf **Auswählen**.
5. Wählen Sie bei **Alarmtypen** die Monitore aus, für die Sie wollen, dass das System E-Mail-Alarmmeldungen versendet.
6. Klicken Sie auf **Hinzufügen**.

Bearbeiten

So können Sie eine E-Mail-Benachrichtigungsrichtlinie bearbeiten

1. Gehen Sie in der Schutz-Konsole zu **Einstellungen** –> **E-Mail-Benachrichtigungen**.
2. Klicken Sie auf das Drei-Punkte-Symbol der Benachrichtigungsrichtlinie und dann auf den Befehl **Bearbeiten**.
3. [Optional] Wenn Sie die Empfänger ändern wollen, müssen Sie auf **Empfänger bearbeiten** klicken, die entsprechenden Benutzer zur Liste hinzufügen oder aus ihr entfernen und dann auf **Auswahl** klicken.
4. [Optional] Wählen Sie bei **Alarmtypen** die Arten von Monitoring-Alarmmeldungen aus, die an die ausgewählten Empfänger gesendet werden sollen.
5. Klicken Sie auf **Speichern**.

Aktivieren

So können Sie eine E-Mail-Benachrichtigungsrichtlinie aktivieren

1. Gehen Sie in der Schutz-Konsole zu **Einstellungen** –> **E-Mail-Benachrichtigungen**.
2. Klicken Sie in der Anzeige **E-Mail-Benachrichtigungen** auf das Symbol **...** der entsprechenden E-Mail-Benachrichtigungsrichtlinie.
3. Klicken Sie auf **Aktivieren**.

Deaktivieren

So können Sie eine E-Mail-Benachrichtigungsrichtlinie deaktivieren

1. Gehen Sie in der Schutz-Konsole zu **Einstellungen** –> **E-Mail-Benachrichtigungen**.
2. Klicken Sie in der Anzeige **E-Mail-Benachrichtigungen** auf das Symbol **...** der entsprechenden E-Mail-Benachrichtigungsrichtlinie.
3. Klicken Sie auf **Deaktivieren**.

Löschen

So können Sie eine E-Mail-Benachrichtigungsrichtlinie löschen

1. Gehen Sie in der Schutz-Konsole zu **Einstellungen** –> **E-Mail-Benachrichtigungen**.
2. Klicken Sie in der Anzeige **E-Mail-Benachrichtigungen** auf das Symbol **...** der entsprechenden E-Mail-Benachrichtigungsrichtlinie.
3. Klicken Sie zuerst auf **Löschen** und dann auf **Bestätigen**.

Monitor-Daten anzeigen

Sie können für jeden Workload die Liste der angewandten Monitore, den aktuellen Status der Monitore sowie die historischen Performance-Details in einer grafischen Ansicht einsehen. Sie können mit diesen Informationen das Stadium des Workloads analysieren und ermitteln, wie sich dieses Stadium im Laufe der Zeit verändert hat.

Voraussetzungen

- Es wurde ein Monitoring-Plan auf den Workload angewendet.
- Die Workload ist online und verfügt über Daten für den entsprechenden Monitor.
- Die auf dem Workload installierte Version des Agenten unterstützt die Monitoring-Pläne.

So können Sie die Monitore, die auf einen Workload angewendet wurden, und die entsprechenden Monitor-Daten einsehen

1. Gehen Sie in der Schutz-Konsole zu **Geräte** –> **Alle Geräte**.
2. Klicken Sie auf einen Workload und dann auf die Registerkarte **Monitoring**.
   In der Registerkarte **Monitoring** wird für jeden Monitor, der für den Workload aktiviert ist, ein Widget angezeigt. In jedem Widget werden folgende Informationen angezeigt.

Angezeigte Informationen	Beschreibung
Monitor-Name	Der Name des Monitors
Letztes Ergebnis	Der letzte Wert der überwachten Metrik oder das letzte Stadium des jeweiligen Ereignisses
Letzte Überprüfung	Der Zeitpunkt (Datum und Uhrzeit), an dem der Monitor die letzten Daten erfasst hat
Alarmmeldungen	Die Anzahl der Alarmmeldungen, die vom Monitor generiert wurden und noch nicht gelöst wurden. Wenn mindestens ein ungelöster Alarm von diesem Monitor generiert wurde, können Sie durch Klicken auf die entsprechende Nummer die Registerkarte **Alarmmeldungen** öffnen. Die Alarmmeldungen werden gefiltert und es werden nur die Alarmmeldungen für diesen Monitor aufgelistet.

Hinweis
Die Widgets werden auf der Registerkarte nach 15 Minuten (oder nach dem Zeitintervall, das über den Parameter 'Minimale Monitor-Häufigkeit' für den betreffenden Monitor festgelegt wurde) sichtbar, nachdem Sie einen Monitoring-Plan auf den Workload angewendet haben.

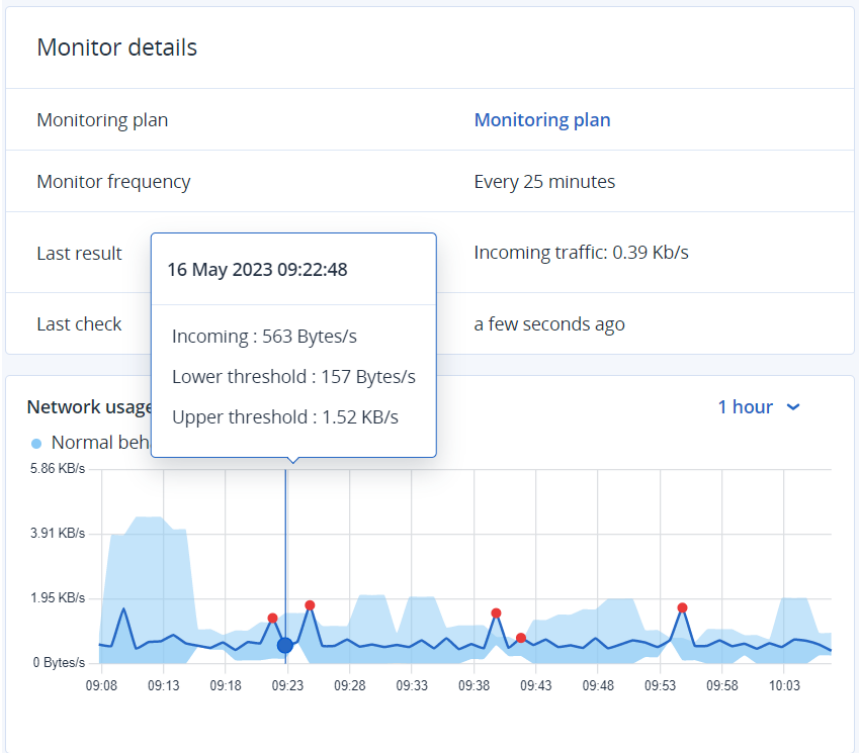
3. [Optional] Wenn Sie mehr Details über den Monitor und gegebenenfalls die Verlaufsdaten, die für die überwachte Metrik gesammelt wurden, einsehen wollen, müssen Sie im Widget des Monitors auf das Drei-Punkte-Symbol und dann auf **Details** klicken.

   Weitere Informationen zu den in den Widgets angezeigten Monitor-Details finden Sie im Abschnitt '"Monitor-Widgets" (S. 1192)'.

Monitor-Widgets

Im Monitor-Widget werden die nachfolgenden Details über den Monitor angezeigt.

Detail	Beschreibung
Monitoring-Plan	Der Name des Monitoring-Plans, der den Monitor enthält. Der Name des Monitoring-Plans entspricht auch einem Link, durch den der Monitoring-Plan im Ansichtsmodus geöffnet werden kann.
Monitor-Häufigkeit	Das Zeitintervall, in dem die Daten des Workloads vom Monitor gesammelt werden
Letztes Ergebnis	Der letzte Wert der überwachten Metrik oder das letzte Stadium des jeweiligen Ereignisses
Letzte Überprüfung	Der Zeitpunkt (Datum und Uhrzeit), an dem der Monitor die letzten Daten erfasst hat
Letzter Alarm	Datum und Uhrzeit, an dem die letzte Alarmmeldung generiert wurde. Das Feld wird nur angezeigt, wenn mindestens eine Alarmmeldung für den Monitor generiert wurde.
Historisches Diagramm	Bei Monitoren, die Zeitseriendaten sammeln, zeigt das Widget die Verlaufsdaten für einen ausgewählten Zeitraum (1 Stunde, 6 Stunden, 12 Stunden, 1 Tag, 1 Woche oder 1 Monat) in einer grafischen Ansicht an. Das Diagramm zeigt die tatsächlichen Werte der Metrik für einen von Ihnen gewählten Zeitraum an. Wenn der Agent die gesammelten Daten aus irgendeinem Grund nicht in die Cloud gesendet hat, werden die fehlenden Werte in Form einer gepunkteten Linie dargestellt, in der die Datenpunkte mit den tatsächlichen Werten verbunden sind, die vor und nach dem fehlenden Wert liegen. Bei Monitoren, die ein **Anomalie-basiertes** Monitoring verwenden, zeigt das Diagramm den Basislinienbereich, eine Linie mit den aktuellen Werten der Metrik und die Anomalien an. Die Anomalien sind die Spitzen oder Werte, die außerhalb der Basislinien liegen und als rote Punkte im Diagramm angezeigt werden. Wenn Sie mit der Maus über das Diagramm fahren, werden Ihnen der entsprechende aktuelle Wert und die Grenzwerte für einen bestimmten Zeitpunkt angezeigt.

Detail	Beschreibung
	 **Hinweis** Die Daten in den Diagrammen werden gemäß der Zeitzone des lokalen Systems angezeigt. Das entspricht der Zeitzone des Browsers auf dem Workload, über den Sie auf die Schutz-Konsole zugreifen.

Zusätzliche Cyber Protection-Tools

Compliance-Modus

Der Compliance-Modus ist für Kunden mit höheren Sicherheitsanforderungen konzipiert. Dieser Modus erfordert zwingend eine Verschlüsselung aller Backups und erlaubt nur lokal festgelegte Verschlüsselungskennwörter.

Im Compliance-Modus werden alle in einem Kunden-Mandanten und seinen Abteilungen erstellten Backups automatisch mit dem AES-Algorithmus und einer Tiefe von 256 Bit verschlüsselt. Die Anwender können die Verschlüsselungskennwörter nur auf den geschützten Geräten festlegen. Sie können keine Verschlüsselungskennwörter über Schutzpläne vergeben.

Wichtig
Der Compliance-Modus kann nicht deaktiviert werden.

Einschränkungen

- Der Compliance-Modus ist nur mit Agenten der Version 15.0.26390 oder höher kompatibel.
- Der Compliance-Modus ist nicht für Geräte verfügbar, die unter Red Hat Enterprise Linux 4.x oder 5.x (und deren Derivaten) laufen.
- Cloud Services können nicht auf Verschlüsselungskennwörter zugreifen. Aufgrund dieser Einschränkung sind einige Funktionen für Mandanten im Compliance-Modus nicht verfügbar.

Nicht unterstützte Funktionen

Folgende Funktionen sind für Mandanten im Compliance-Modus nicht verfügbar:

- Wiederherstellungen über die Cyber Protect-Konsole
- Durchsuchen von Backups auf Dateiebene über die Cyber Protect-Konsole
- Cloud-zu-Cloud-Backup
- Website-Backup
- Applikations-Backup
- Backup für Mobilgeräte
- Antimalware-Scan von Backups
- Safe Recovery
- Automatisches Erstellen von Positivlisten für Unternehmensapplikationen
- Data Protection-Karte
- Disaster Recovery
- Berichte und Dashboards, die sich auf die nicht verfügbaren Funktionen beziehen

Das Verschlüsselungskennwort festlegen

Sie müssen das Verschlüsselungskennwort lokal festlegen, also auf dem geschützten Gerät. Sie können das Verschlüsselungskennwort nicht in einem Schutzplan festlegen. Ohne ein Kennwort wird das Erstellen von Backups fehlschlagen.

Warnung!
Falls Sie Ihr Kennwort verlieren, gibt es keine Möglichkeit, Ihre verschlüsselten Backups wiederherzustellen!

Sie können das Verschlüsselungskennwort auf folgende Weise festlegen:

1. Während der Installation eines Protection Agenten (für Windows, macOS und Linux).
2. Über die Befehlszeile (für Windows und Linux).
   Dies ist die einzige Möglichkeit, ein Verschlüsselungskennwort auf einer virtuellen Appliance festzulegen.
   Weitere Informationen zum Festlegen von Verschlüsselungskennworten mit dem Tool **Acropsh** finden Sie im Abschnitt '"Verschlüsselung" (S. 484)'.
3. Im Cyber Protect Monitor (für Windows und macOS).

So können Sie das Verschlüsselungskennwort im Cyber Protect Monitor festlegen

1. Melden Sie sich auf dem geschützten Gerät als Administrator an.
2. Klicken Sie im Infobereich der Taskleiste (Windows) oder in der Menüleiste (macOS) auf das Symbol für den Cyber Protect Monitor.
3. Klicken Sie auf das Zahnradsymbol.
4. Klicken Sie auf die Option **Verschlüsselung**.
5. Legen Sie das Verschlüsselungskennwort fest.
6. Klicken Sie auf **OK**.

Das Verschlüsselungskennwort ändern

Sie können das Verschlüsselungskennwort solange noch ändern, bis ein Schutzplan entsprechende Backups erstellt.

Wir raten davon ab, das Verschlüsselungskennwort nach dem Erstellen von Backups zu ändern, weil dann die nachfolgenden Backups fehlschlagen würden. Um dieselbe Maschine auch weiterhin schützen zu können, müss(t)en Sie dann einen neuen Schutzplan für diese erstellen. Wenn Sie sowohl das Verschlüsselungskennwort als auch den Schutzplan ändern, resultiert dies in der Erstellung ganz neuer Backups, die dann mit dem geänderten Kennwort verschlüsselt sind. Die Backups, die vor diesen Änderungen erstellt wurden, sind davon unbetroffen.

Alternativ können Sie auch den angewendeten Schutzplan beibehalten und nur den Namen der Backup-Datei darin ändern. Auch dies führt dazu, dass neue Backups erstellt werden, die mit dem

geänderten Kennwort verschlüsselt werden. Weitere Informationen über Backup-Dateinamen finden Sie im Abschnitt '"Backup-Dateiname" (S. 493)'.

Sie können das Verschlüsselungskennwort auf folgende Weise ändern:

1. Im Cyber Protect Monitor (für Windows und macOS).
2. Über die Befehlszeile (für Windows und Linux).
   Weitere Informationen zum Festlegen von Verschlüsselungskennworten mit dem Tool **Acropsh** finden Sie im Abschnitt '"Verschlüsselung" (S. 484)'.

Backups für Mandanten im Compliance-Modus wiederherstellen

Im Compliance-Modus können Sie Backups nicht über die Cyber Protect-Konsole wiederherstellen.

Folgende Optionen sind verfügbar:

- Eine komplette Maschine, deren Laufwerke oder Dateien mithilfe eines Boot-Mediums wiederherstellen.
- Dateien aus lokalen Backups von Windows-Maschinen mit einem installierten Agenten extrahieren, indem Sie den Windows Explorer verwenden.

Unveränderlicher Storage

Über den unveränderlichen Storage können Sie während einer spezifizierten Aufbewahrungsdauer auf gelöschte Backups zugreifen. Sie können die Inhalte dieser Backups wiederherstellen, aber Sie können diese nicht ändern, verschieben oder löschen. Wenn die Aufbewahrungsdauer endet, werden die gelöschten Backups dauerhaft gelöscht.

Der unveränderliche Storage enthält folgende Backups:

- Backups, die manuell gelöscht wurden.
- Backups, die – gemäß den Einstellungen im Bereich **Aufbewahrungsdauer** in einem Schutzplan oder im Bereich **Aufbewahrungsregeln** in einem Bereinigungsplan – automatisch gelöscht wurden.

Gelöschte Backups im unveränderlichen Storage belegen weiterhin Speicherplatz und werden entsprechend abgerechnet.

Gelöschten Mandanten wird keine Speicherplatz-Belegung (auch nicht im unveränderlichen Storage) in Rechnung gestellt.

Die Modi für den unveränderlichen Storage

Für Kunden-Mandanten ist der unveränderliche Storage in folgenden Modi verfügbar:

Der unveränderliche Storage ist in folgenden Modi verfügbar:

- **Governance-Modus**
  Sie können den unveränderlichen Storage erst deaktivieren und wieder aktivieren. Sie können die Aufbewahrungsdauer ändern oder auf den Compliance-Modus umschalten.
- **Compliance-Modus**

  Warnung!
  Die Auswahl des Compliance-Modus kann nicht rückgängig gemacht werden.

  Sie können den unveränderlichen Storage nicht wieder deaktivieren. Sie können weder die Aufbewahrungsdauer ändern noch zurück in den Governance-Modus wechseln.

Unterstützte Storages und Agenten

- Der unveränderliche Storage wird nur auf dem Cloud Storage unterstützt.
  Der unveränderliche Storage ist sowohl für von Acronis gehostete als auch für von Partnern gehostete Cloud Storages verfügbar, die Acronis Cyber Infrastructure 4.7.1 oder höher verwenden.
  Alle Storages, die mit dem Acronis Cyber Infrastructure Backup Gateway verwendet werden können, werden unterstützt. Zum Beispiel der Acronis Cyber Infrastructure Storage, Amazon S3- und EC2-Storages sowie der Microsoft Azure Storage.
  Der unveränderliche Storage erfordert, dass der TCP-Port 40440 für den Backup Gateway Service in Acronis Cyber Infrastructure geöffnet ist. Ab Version 4.7.1 wird der TCP-Port 40440 automatisch mit dem Traffic-Typ **Backup (ABGW) öffentlich** geöffnet. Weitere Informationen über die Traffic-Typen finden Sie in der Acronis Cyber Infrastructure-Dokumentation.
- Für den unveränderlichen Storage muss der Protection Agent in Version 21.12 (Build 15.0.28532) oder höher installiert sein.
- Es werden nur TIBX-Backups (Version 12) unterstützt.

Den unveränderlichen Storage aktivieren

Sie können die Einstellungen für den unveränderlichen Storage in der Cyber Protect-Konsole oder im Management-Portal konfigurieren. Beide bieten Zugang zu den gleichen Einstellungen. Das untenstehende Verfahren verwendet die Cyber Protect-Konsole. Um zu erfahren, wie Sie die Einstellungen für den unveränderlichen Storage im Management-Portal konfigurieren können, informieren Sie sich im Abschnitt Den nveränderlichen Storage konfigurieren in der Anleitung für Administratoren.

Zur Konfiguration der unveränderlichen Storage-Einstellungen ist eine Zwei-Faktor-Authentifizierung in dem Mandanten erforderlich, zu dem das Administratorkonto gehört.

So können Sie den unveränderlichen Storage aktivieren

1. Melden Sie sich als Administrator an der Cyber Protect-Konsole an.
2. Gehen Sie zu **Einstellungen** > **Systemeinstellungen**.

3. Scrollen Sie durch die Liste der vorgegebenen Backup-Optionen und klicken Sie dann auf **Unveränderlicher Storage**.
4. Aktivieren Sie den Schalter **Unveränderlicher Storage**.
5. Spezifizieren Sie eine Aufbewahrungsdauer zwischen 14 und 3650 Tagen.

   Die standardmäßige Aufbewahrungsdauer beträgt 14 Tage. Eine längere Aufbewahrungsdauer führt zu einer erhöhten Speichernutzung.
6. Wählen Sie den Modus 'Unveränderlicher Storage' aus und bestätigen Sie bei Aufforderung Ihre Auswahl.

   Im Governance-Modus können Sie den unveränderlichen Storage aktivieren oder deaktivieren und die Aufbewahrungsdauer ändern. Sie können vom Governance-Modus auch in den Compliance-Modus wechseln.

   Warnung!
   Der Wechsel in den Compliance-Modus kann nicht rückgängig gemacht werden. Nachdem Sie den Compliance-Modus ausgewählt haben, können Sie den unveränderlichen Storage nicht wieder deaktivieren oder dessen Modus oder Aufbewahrungsdauer ändern.
7. Klicken Sie auf **Speichern**.
8. Wenn Sie erreichen wollen, dass ein vorhandenes Archiv den unveränderlichen Storage unterstützt, müssen Sie ein neues Backup in diesem Archiv erstellen.

   Führen Sie zum Erstellen eines neuen Backups den Schutzplan entweder manuell oder über eine Planung aus.

   Warnung!
   Wenn Sie ein Backup löschen, bevor Sie bewirkt haben, dass das Archiv den unveränderlichen Storage unterstützt, wird das Backup endgültig gelöscht.

Den unveränderlichen Storage deaktivieren

Hinweis
Sie können den unveränderlichen Storage nur im Governance-Modus deaktivieren.

So können Sie den unveränderlichen Storage deaktivieren

1. Melden Sie sich als Administrator an der Cyber Protect-Konsole an.
2. Klicken Sie im Navigationsmenü auf **Einstellungen** –> **Systemeinstellungen**.
3. Scrollen Sie durch die Liste der vorgegebenen Backup-Optionen und klicken Sie dann auf **Unveränderlicher Storage**.
4. Deaktivieren Sie den Schalter **Unveränderlicher Storage**.
5. Bestätigen Sie Ihre Auswahl, indem Sie auf **Deaktivieren** klicken.

Warnung!
Eine Deaktivierung des unveränderlichen Storage tritt nicht sofort in Kraft. Der unveränderliche Storage bleibt für eine Frist von 14 Tagen aktiv, sodass Sie entsprechend der ursprünglichen Aufbewahrungsdauer auf die entsprechenden gelöschten Backups zugreifen können. Wenn die Frist endet, werden alle Backups im unveränderlichen Storage dauerhaft gelöscht.

Auf gelöschte Backups im unveränderlichen Storage zugreifen

Innerhalb der Aufbewahrungsdauer können Sie auf gelöschte Backups zugreifen und Daten aus diesen wiederherstellen.

Hinweis
Wenn Sie den Zugriff auf gelöschte Backups zulassen wollen, sollte der Port 40440 für eingehende Verbindungen auf dem Backup Storage aktiviert sein.

So können Sie auf ein gelöschtes Backup zugreifen

1. Wählen Sie in der Registerkarte **Backup Storage** den Cloud Storage aus, wo das gelöschte Backup gespeichert ist.
2. [Nur für gelöschte Archive] Um die gelöschten Archive zu sehen, klicken Sie auf **Gelöschte anzeigen**.
3. Wählen Sie das Archiv aus, welches das wiederherzustellende Backup enthält.
4. Klicken Sie zuerst auf **Backups anzeigen** und dann auf **Gelöschte anzeigen**.
5. Wählen das Backup aus, das Sie wiederherstellen wollen.
6. Fahren Sie mit der Wiederherstellungsaktion fort (wie in Abschnitt '"Recovery" (S. 541)' erläutert).

Georedundanter Storage

Der georedundante Storage gewährleistet die Dauerhaftigkeit von gespeicherten Daten, indem diese asynchron zu einem sekundären Speicherort kopiert werden, der geografisch vom primären Speicherort entfernt liegt. Dank der Georedundanz bleiben Ihre Daten auch dann verfügbar, wenn der primäre Standort nicht mehr erreichbar ist.

Wichtig
Die replizierten Daten belegen den gleichen Speicherplatz wie die Originaldaten.

Den georedundanten Storage aktivieren oder deaktivieren

Voraussetzungen

- Der georedundante Storage wird in der Cyber Protect-Konsole erst dann verfügbar, wenn ein Partner-Administrator ihn im Management-Portal oder per API aktiviert.

- Nur Administratoren können den georedundanten Storage in der Cyber Protect-Konsole aktivieren oder deaktivieren. Stellen Sie sicher, dass Sie über Administratorrechte verfügen.

So können Sie den georeundanten Storage aktivieren

1. [Nur wenn der georedundante Storage per API aktiviert wurde] Klicken Sie in der oben angezeigten Alarmmeldung 'Die Georedundanz ist für all Ihre Daten in der Cloud verfügbar' auf **Geo-redundant Cloud Storage aktivieren**.
2. Gehen Sie in der Cyber Protect-Konsole zu **Einstellungen** –> **Systemeinstellungen**.
3. Scrollen Sie durch die Liste der vorgegebenen Backup-Optionen und klicken Sie dann auf **Geo-redundant Cloud Storage**.
4. Aktivieren Sie den Schalter **Geo-redundant Cloud Storage**.
5. Klicken Sie auf **Speichern**.
   Jetzt werden Ihre Daten zu einem sekundären Standort repliziert. Sie bleiben dort auch dann verfügbar, wenn der primäre Standort ausfallen sollte.

So können Sie den georeundanten Storage deaktivieren

Warnung!
Die replizierten Daten werden innerhalb eines Tages gelöscht, nachdem Sie die Georedundanz deaktiviert haben.

1. Gehen Sie in der Cyber Protect-Konsole zu **Einstellungen** –> **Systemeinstellungen**.
2. Scrollen Sie durch die Liste der Backup-Optionen und klicken Sie dann auf **Geo-redundant Cloud Storage**.
3. Deaktivieren Sie den Schalter **Geo-redundant Cloud Storage**.
4. Bestätigen Sie Ihre Entscheidung, indem Sie **Deaktivieren** eingeben, und klicken Sie dann auf **Deaktivieren**.

Georeplikationsstatus

Georedundanz bedeutet, dass Daten zu einem sekundären Standort repliziert werden. Der Georeplikationsstatus zeigt die Phasen dieses Prozesses an. Folgende Statuszustände sind möglich:

- **Synchronisiert** — Die Daten wurden zum sekundären Standort repliziert.
- **Wird synchronisiert** — Die Daten werden gerade zum sekundären Standort repliziert. Die Dauer dieser Aktion hängt von der Datenmenge ab.
- **Zurückgestellt** — Die Datenreplikation wurde vorübergehend angehalten.
- **Deaktiviert** — Die Datenreplikation ist deaktiviert.

So können Sie den Replikationsstatus in der Cyber Protect-Konsole überprüfen

1. Gehen Sie in der Cyber Protect-Konsole zu **Backup Storage**.
2. Wählen Sie den Speicherort und Backup-Satz aus.

3. Klicken Sie auf **Details** und überprüfen Sie dann den Status unter **Georeplikationsstatus**.

Einschränkungen

- Derzeit sind sekundäre Standorte für replizierte Daten nur in den Vereinigten Staaten und Kanada verfügbar.
- Weitere Informationen zu Einschränkungen des Disaster Recovery Service bei Verwendung der Georedundanz-Funktion finden Sie in der Disaster Recovery-Dokumentation.

Glossar

A

Agent für Data Loss Prevention

Die Client-Komponente eines Data Loss Prevention-Systems, die den jeweiligen Host-Computer vor der unbefugten Nutzung, Übertragung und Speicherung von vertraulichen, geschützten oder sensiblen Daten schützt, indem sie eine Kombination aus kontext- und inhaltsbezogenen Analysetechniken anwendet und zentral verwaltete Data Loss Prevention-Richtlinien durchsetzt. Zur Cyber Protection-Funktionalität gehört ein vollwertiger Data Loss Prevention Agent. Die tatsächliche Funktionalität des Agenten auf einem geschützten Computer ist jedoch auf denjenigen Satz von Data Loss Prevention-Funktionen beschränkt, der in der jeweiligen Cyber Protection-Lösung je nach Lizenzierung verfügbar ist – und sie hängt zudem von dem Schutzplan ab, der auf den betreffenden Computer angewendet wird.

B

Backup-Format 'Einzeldatei'

Ein Backup-Format, in dem das anfängliche Voll-Backup sowie alle nachfolgenden inkrementellen Backups gemeinsam in Form einer einzigen/einzelnen tibx-Datei gespeichert werden. Dieses Format nutzt die Geschwindigkeit der inkrementellen Backup-Methode und vermeidet dabei gleichzeitig deren größten Nachteil: das schwierige Löschen veralteter Backups. Die Software kennzeichnet diejenigen Blöcke, die von veralteten Backups verwendet werden, als 'frei' und schreibt neue Backups in diese neuen Blöcke. Dies führt zu einer extrem schnellen Bereinigung, bei gleichzeitig minimalem Ressourcenverbrauch. Das Backup-Format 'Einzeldatei' ist nicht verfügbar, wenn als Backup-Ziel ein Storage (wie beispielsweise ein Bandlaufwerk) verwendet wird, der keine wahlfreien Lese- und Schreib-Zugriffe (Random Access Read and Write) zulässt.

Backup-Set

Eine Gruppe von Backups, auf die eine einzelne Aufbewahrungsregel angewendet werden kann. Beim Backup-Schema 'Benutzerdefiniert' entsprechen die Backup-Sets den Backup-Methoden ('Vollständig', 'Differentiell' und 'Inkrementell'). In allen anderen Fällen sind die Backups-Sets 'Monatlich', 'Täglich', 'Wöchentlich' und 'Stündlich'. Ein 'monatliches' Backup ist dasjenige Backup, das als erstes in einem bestimmten Monat erstellt wird. Ein 'wöchentliches' Backup ist das erste Backup, welches an demjenigen Wochentag erstellt wird, wie er über die Option 'Wöchentliches Backup' festgelegt wurde (klicken Sie auf das Zahnradsymbol und dann auf die Befehle 'Backup-Optionen' –> 'Wöchentliche Backups'). Wenn ein 'wöchentliches' Backup das erste Backup ist, welches seit Anbruch eines Monats erstellt wurde, so wird dieses Backup als 'monatliches' Backup betrachtet. In diesem Fall wird ein wöchentliches Backup an dem ausgewählten Tag der nächsten Woche erstellt. Ein 'tägliches' Backup ist das erste Backup, welches nach Anbruch eines Tages erstellt wird – es sei denn, dieses Backup fällt unter die Definition eines monatlichen oder wöchentlichen Backups. Ein 'stündliches' Backup ist das erste Backup, welches nach Anbruch einer Stunde erstellt wird – es sei denn, dieses Backup fällt unter die Definition eines 'monatlichen', 'wöchentlichen' oder 'täglichen' Backups.

C

Cloud-Site (oder DR-Site)

[Disaster Recovery] Ein in der Cloud gehosteter Remote-Standort, der dazu verwendet wird, im Desasterfall eine Recovery- Infrastruktur auszuführen.

Cloud Server

[Disaster Recovery] Allgemeiner Begriff für eine primären Server oder Recovery- Server (auch Wiederherstellungsserver genannt).

D

Data Loss Prevention (früher auch Data Leak Prevention genannt)

Ein System integrierter Technologien und organisatorischer Maßnahmen, das darauf abzielt, versehentliche oder absichtliche Offenlegungen/Zugriffe auf vertrauliche, geschützte oder sensible Daten durch unberechtigte Entitäten außerhalb oder innerhalb des Unternehmens oder die Übertragung solcher Daten zu nicht vertrauenswürdigen Umgebungen zu erkennen und zu unterbinden.

Differentielles Backup

Ein differentielles Backup speichert Änderungen an den Daten im Vergleich zum letzten vorangegangenen Voll- Backup. Sie müssen auf das entsprechende Voll- Backup zugreifen können, um Daten aus einem differentiellen Backup wiederherstellen zu können.

F

Failback

Umschalten eines Workloads von einem Ersatzserver (z.B. das Replikat einer virtuellen Maschine oder eines Recovery-Servers, der in der Cloud läuft) zurück auf den ursprünglichen Produktionsserver.

Failover

Umschalten eines Workloads von einem Produktionsserver zu einem Ersatzserver (z.B. das Replikat einer virtuellen Maschine oder eines Recovery-Servers, der in der Cloud läuft).

Finalisierung

Eine Operation, die aus einer temporären virtuellen Maschine, die aus einem Backup ausgeführt wird, eine permanente virtuelle Maschine erstellt. Physisch bedeutet dies, dass alle virtuellen Laufwerke der Maschine zusammen mit allen Änderungen, die während ihrer Ausführung aufgetreten sind, zu dem Datenspeicher wiederhergestellt werden, auf dem diese Änderungen gespeichert werden.

G

Gerätekontrolle-Modul

Als Bestandteil eines Schutzplans verwendet das Modul 'Gerätekontrolle' eine funktionale Teilmenge des Data Loss Prevention Agenten auf jedem entsprechend geschützten Computer, um unautorisierte Zugriffe auf und Übertragungen von Daten über lokale Computer- Datenkanäle zu erkennen und zu unterbinden. Dazu gehören Benutzerzugriffe auf Peripheriegeräte und Ports, das Ausdrucken von Dokumenten, Zwischenablage-Aktionen (Kopieren, Einfügen), bestimmte Aktionen mit Medien (Formatieren, Auswerfen)

und die Synchronisierung von Daten mit lokal angeschlossenen Mobilgeräten. Das Modul 'Gerätekontrolle' bietet granulare, kontextbezogene Kontrollmöglichkeiten über die Art der Geräte und Ports, auf die Benutzer auf dem geschützten Computer zugreifen dürfen, sowie über die Aktionen, die Benutzer auf diesen Geräten ausführen können.

I

Inkrementelles Backup

Ein Backup, das Datenänderungen in Bezug zum letzten Backup speichert. Um Daten von einem inkrementellen Backup wiederherstellen zu können, müssen Sie auch Zugriff auf andere Backups (in derselben Backup-Kette) haben.

L

Lokaler Standort

[Disaster Recovery] Die lokale Infrastruktur, die „on-premise“ (auf den lokalen Systemen/am lokalen Standort) Ihres Unternehmens bereitgestellt wird.

M

Modul

Ein Modul ist ein Bestandteil eines Schutzplans, der eine bestimmte Data Protection-Funktionalität bereitstellt. Typische Beispiele sind das Backup-Modul oder das Antivirus & Antimalware Protection-Modul.

O

Öffentliche IP-Adresse

[Disaster Recovery] Eine IP-Adresse, die erforderlich ist, um Cloud Server aus dem Internet verfügbar zu machen.

P

Physische Maschine

Eine Maschine, die von einem Agenten gesichert wird, der im Betriebssystem installiert ist.

Point-to-Site-Verbindung (P2S)

[Disaster Recovery] Eine sichere VPN-Verbindung von außen zur Cloud-Site und Ihrem lokalen Standort über Ihre Endgeräte (z.B. einen Desktop-Computer oder Laptop).

Primärer Server

[Disaster Recovery] Eine virtuelle Maschine, die keine verknüpfte Maschine am lokalen Standort hat (wie etwa einen Recovery-Server). Primäre Server werden zum Schutz einer Applikation oder zur Ausführung verschiedener Hilfsdienste (z.B. als Webserver) verwendet.

Produktionsnetzwerk

[Disaster Recovery] Das per VPN-Tunneling erweiterte interne Netzwerk, das sowohl den lokale Standort als auch die Cloud-Site umfasst. Lokale Server und Cloud Server können im Produktionsnetzwerk miteinander kommunizieren.

Protection Agent

Der Protection Agent ist der Agent, der auf Maschinen zu deren Data Protection installiert werden muss.

R

Recovery-Server

[Disaster Recovery] Das VM-Replikat einer ursprünglichen Maschine, das auf den (in der

Cloud gespeicherten) Backups eines geschützten Servers basiert. Recovery-Server werden verwendet, um bei einem Desaster die Workloads der ursprünglichen Server in die Cloud umschalten zu können.

RPO (Recovery Point Objective)

[Disaster Recovery] Auf Deutsch etwas „Wiederherstellungspunktvorgabe“. Bestimmt, welche Datenmenge bei einem Ausfall höchstens verloren gehen darf. Wird an der Zeitspanne bemessen, die nach einem geplanten Ausfall oder einem zufälligen Desasterereignis höchstens verstreichen darf. Der RPO-Grenzwert definiert also das maximale Zeitintervall, das zwischen dem letzten (für ein Failover verwendbaren) Recovery-Punkt und dem aktuellen Zeitpunkt (an dem es zu einem Desaster kommen kann) zulässig ist.

Runbook

[Disaster Recovery] Ein geplantes Szenario, das aus konfigurierbaren Schritten besteht, um Disaster Recovery-Aktionen zu automatisieren.

S

Schutzplan

Ein Schutzplan ist ein Plan, der Data Protection-Module kombiniert. Dazu gehören: Backup, Antivirus & Antimalware Protection, URL-Filterung, Windows Defender-Antivirus-Steuerung, Microsoft Security Essentials-Steuerung, Schwachstellenbewertung, Patch-Verwaltung, Data Protection-Karte und Gerätekontrolle.

Site-to-Site-Verbindung (S2)

[Disaster Recovery] Eine Verbindung zur Erweiterung des lokalen Netzwerks über einen sicheren VPN-Tunnel in die Cloud.

T

Test-IP-Adresse

[Disaster Recovery] Eine IP-Adresse, die bei einem Test-Failover benötigt wird, um die Duplizierung der Produktions-IP-Adresse zu vermeiden.

Testnetzwerk

[Disaster Recovery] Isoliertes virtuelles Netzwerk, das zum Testen des Failover-Prozesses verwendet wird.

U

USB-Geräte-Datenbank

[Gerätekontrolle] Das Modul 'Gerätekontrolle' verwaltet eine Datenbank von USB-Geräten, aus der diese dann in eine Liste aufgenommen werden können, die Ausschlüsse von der Gerätezugriffskontrolle enthält. Die Datenbank registriert die USB-Geräte anhand ihrer Geräte-ID, die manuell eingegeben eingegeben oder aus einer Liste bekannter Geräte in der Cyber Protect-Konsole ausgewählt werden kann.

V

Validierung

Aktion, mit der die Möglichkeit einer Datenwiederherstellung aus einem Backup geprüft wird. Die Validierung eines Datei-Backups imitiert die Wiederherstellung aller Dateien aus einem Backup an einen imitierten Zielort. Bei einer Validierung eines Laufwerk-Backups wird für jeden Datenblock, der in dem Backup gespeichert ist, eine Prüfsumme berechnet. Beide Prozeduren sind ressourcenintensiv. Obwohl eine erfolgreiche

Validierung bedeutet, dass eine Wiederherstellung mit hoher Wahrscheinlichkeit möglich sein wird, werden nicht alle Faktoren überprüft, die den zukünftigen Recovery-Prozess beeinflussen können.

Verwaistes Backup

Ein verwaistes Backup ist ein Backup, das nicht mehr mit einem Schutzplan assoziiert ist.

Virtuelle Maschine

Eine virtuelle Maschine, die auf Hypervisor-Ebene von einem externen Agenten (wie dem Agenten für VMware oder dem Agenten für Hyper-V) gesichert wird. Eine virtuelle Maschine, in der ein Agent installiert ist, wird aus Backup-Sicht wie eine physische Maschine behandelt.

Voll-Backup

Ein selbstständiges Backup, das alle für ein Backup ausgewählten Daten enthält. Sie benötigen kein weiteres Backup, um die Daten aus einem Voll-Backup wiederherzustellen.

VPN-Appliance

[Disaster Recovery] Eine spezielle virtuelle Maschine, die eine Verbindung (über einen sicheren VPN-Tunnel) zwischen dem lokalen Netzwerk und der Cloud-Site ermöglicht. Die VPN-Appliance wird am lokalen Standort bereitgestellt.

VPN-Gateway (früher auch VPN-Server oder Verbindungsgateway genannt)

[Disaster Recovery] Eine spezielle virtuelle Maschine, die eine Verbindung (über einen sicheren VPN-Tunnel) zwischen dem lokalen Standort und den Cloud-Site-Netzwerken bereitstellt. Das VPN-Gateway wird in der Cloud-Site bereitgestellt.

Index

B

C

D

E

H

I

K

L

M

Q

R

S

T

U

V

W

Z