Cyber Protection

Version 20.08

BENUTZERANLEITUNG

Revision: 29/08/2020

Inhaltsverzeichnis

1 Willkommen zu Cyber Protection

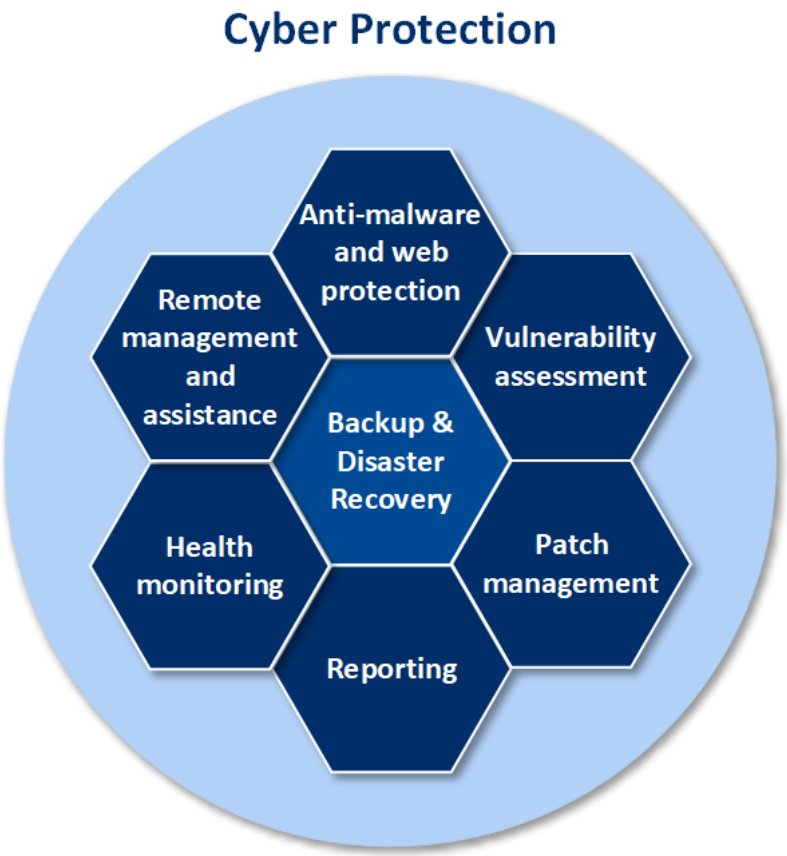
Cyber Protection ist eine All-in-one-Cyber-Protection-Lösung, die Data Protection (Backup und Recovery), Disaster Recovery, Malware-Prävention, Sicherheitskontrollen, Remote-Unterstützung, Monitoring und Berichtsfunktionalität integriert.

Es schützt Ihr komplettes Unternehmen und die Geschäfte Ihrer Kunden durch einen mehrschichtigen Schutzansatz, der eine innovative Kombination aus proaktiven, aktiven und reaktiven Data Protection-Technologien bietet:

- **Proaktive** Aktionen – wie Schwachstellenbewertung, Patch-Verwaltung und eine vorhersagende Analyse des Festplattenzustandes (auf Basis von Machine Learning-Technologien) – ermöglichen es Ihnen, Ihre Maschinen vor Bedrohungen zu bewahren.
- **Aktive** Aktionen – wie Malware-Abwehr- und Selbstschutz-Funktionen – ermöglichen Ihnen, entsprechende Bedrohungen zu erkennen.
- **Reaktive** Aktionen – wie Backup und Recovery (lokal oder Cloud-basiert), Disaster Recovery (lokal oder Cloud-basiert) – ermöglichen Ihnen, auf eventuelle Ausfälle zu reagieren.

Dafür stellt Ihnen Cyber Protection Folgendes bereit: einen Protection Agenten, eine anwenderfreundliche Service-Konsole und einen Schutzplan, der alle Sicherheits- und Data Protection-Aspekte abdeckt.

Kernfunktionalität



Cyber Protection stellt folgende Funktionalitäten bereit:

- Die Backup und Recovery-Funktionalität ermöglicht Ihnen, physische Maschinen, virtuelle Maschinen sowie Applikationen sichern und wiederherstellen zu können.
- Die Disaster Recovery-Funktionalität ermöglicht Ihnen, Ihre lokale Umgebung gegen schwerere Ausfälle/Desaster abzusichern. Dazu können Sie exakte Kopien der entsprechenden Maschinen in der Cloud starten und die entsprechenden Workloads zu den Cloud-Servern umschalten.
- Die Antimalware Protection- und Web Protection-Funktionalität bietet Ihnen einen erstklassigen mehrschichtigen Schadsoftware-Schutz, der auf vier verschiedenen Antimalware-Technologien basiert. Sie können zudem die Windows-Programme Microsoft Security Essentials sowie Windows Defender Antivirus direkt von der Service-Konsole aus verwalten. Mit der URL-Filterungsfunktionalität können Sie das Herunterladen schädlicher Dateien verhindern sowie Zugriffe auf verdächtige Webressourcen blockieren.
- Die automatische Erkennung von Maschinen ermöglicht Ihnen, eine große Anzahl von Maschinen automatisch zu registrieren sowie einen Protection Agenten und weitere Komponenten zu installieren.
- Mit der Schwachstellenbewertungsfunktion können Sie Software-Produkte von Microsoft und anderen Drittherstellern nach Schwachstellen (wie Sicherheitslücken) scannen.
- Die in Backups integrierte Patch-Verwaltung bietet Ihnen folgende Möglichkeiten: automatische und manuelle Genehmigung von Patches, planbare oder manuell angestoßene Installation von Patches, flexible Einstellungen für Maschinen-Neustarts und Wartungsfenster, gestaffelte Bereitstellungen.
- Die Funktionalität zur Kontrolle der Laufwerksintegrität ermöglichen Ihnen, den Status Ihrer Festplatten zu überwachen und so möglichen Ausfällen vorzubeugen. Die Laufwerkskontrolle verwendet eine Kombination aus Machine Learning-Algorithmen und S.M.A.R.T.-Daten der Festplatten, um mögliche Laufwerksausfälle vorherzusagen.
- Die Fernverwaltungs- und Remote-Unterstützungsfunktionalität ermöglicht Ihnen, sich aus der Ferne mit Maschinen zu verbinden und diese zu verwalten.
- Der #CyberFit-Score bietet Ihnen einen Sicherheitsbewertungs- und Scoring-Mechanismus, der die Sicherheitslage Ihrer Maschine bewertet.

Warum Cyber Protection besonders ist

Cyber Protection hat folgende einzigartige Fähigkeiten:

- Backup-Scanning in Nicht-Endpunkt-Umgebungen, um Malware-freie Wiederherstellungen zu gewährleisten. Dadurch wird die Möglichkeit verbessert, Rootkits und Bootkits zu erkennen, und die Belastung für Ihre Maschinen reduziert.
- Safe Recovery, basierend auf einem integrierten Antimalware-Scanning und Malware-Löschung, um das Wiederauftreten einer Infektionen zu verhindern.
- Smart Protection, basierend auf Alarmmeldungen, die vom Cyber Protection Operations Center (CPOC) empfangen werden. Dank dieser Funktion können Sie die Ausfallzeiten von Geschäftsprozessen durch Probleme wie Malware-Angriffe oder natürliche Desaster minimieren, Ihre Reaktionszeiten verkürzen und Datenverluste vermeiden.
- Schutz vor fehlerhaften Patches, indem Backups vor einem Update erstellt werden (Vor-Update-Backups).
- Die kontinuierliche Datensicherung (Continuous Data Protection, CDP) stellt sicher, dass Sie keine Datenänderungen verlieren, die zwischen geplanten Backups erstellt wurden. Sie können festlegen, was kontinuierlich gesichert werden soll – ob Office-Dokumente, Finanz-Formulare, Grafik-Dateien oder anderes. Kontinuierliche Backups ermöglichen Ihnen, bessere RPO-Werte zu erzielen.

- Eine Data Protection-Karte, mit der Sie die Datenverteilung auf den Maschinen sowie den Sicherungsstatus von Dateien überwachen und die gesammelten Daten als Grundlage für Compliance-Berichte verwenden können.
- Forensik-Backups, mit denen Sie digitale Beweisdaten sammeln und per Laufwerk-Backup erfassen können. Die so gesicherten Beweisdaten können dann für spätere Untersuchungen (z.B. von Kriminalermittlern) verwendet werden.
- Eine unternehmensweite Positivliste, auf Backups basierend, die es Ihnen ermöglicht, Fehlerkennungen zu verhindern. Diese Funktion macht das zeitaufwendige manuelle Erstellen einer Positivliste von Unternehmensapplikationen überflüssig, steigert die Produktivität und sorgt durch verbesserter Heuristik für bessere Erkennungsraten.

2 Cyber Protection-Editionen

Um den Anforderungen und Budgets verschiedener Kunden gerecht zu werden, gibt es den Cyber Protection Service in verschiedenen Editionen. Ein Kundenunternehmen kann immer nur eine Edition gleichzeitig verwenden.

Edition	Beschreibung
Cyber Backup – Standard	Bietet: ▪ Backup-&-Recovery-Funktionalität, die die Anforderungen kleiner Umgebungen erfüllen. ▪ Funktionalität für Schwachstellenbewertung sowie grundlegende Ransomware Protection und Cryptomining Protection ▪ Remote-Installationsfunktionalität
Cyber Backup – Advanced	Bietet: ▪ Backup & Recovery-Funktionen zur Sicherung von anspruchsvollen Workloads wie Microsoft Exchange- und Microsoft SQL-Cluster, die für große Umgebungen entwickelt wurden ▪ Gruppenverwaltung und Planverwaltung ▪ Funktionalität für Schwachstellenbewertung sowie grundlegende Ransomware Protection und Cryptomining Protection ▪ Remote-Installationsfunktionalität
Cyber Backup – Disaster Recovery	Bietet: ▪ Backup & Recovery-Funktionen zur Sicherung von anspruchsvollen Workloads wie Microsoft Exchange- und Microsoft SQL-Cluster, die für große Umgebungen entwickelt wurden ▪ Gruppenverwaltung und Planverwaltung ▪ Funktionalität für Schwachstellenbewertung sowie grundlegende Ransomware Protection und Cryptomining Protection ▪ Remote-Installationsfunktionalität ▪ Disaster Recovery-Funktionalität für Unternehmen, die hohe Anforderungen an Wiederherstellungszeiten (RTOs) haben

Cyber Protect – Essentials	Bietet: ▪ Grundlegende Datei-Backup-Fähigkeiten ▪ Schwachstellenbewertung ▪ Grundlegende automatische Erkennung und Remote-Installation von Agenten ▪ Patch-Verwaltung ▪ Antivirus & Antimalware Protection ▪ URL-Filterung ▪ Remote-Desktop ▪ Remote-Löschen von Geräten ▪ Verwaltung von Windows Defender Antivirus und Microsoft Security Essentials
Cyber Protect – Standard	Bietet: ▪ Backup-&-Recovery-Funktionalität, die die Anforderungen kleiner Umgebungen erfüllen. ▪ Remote-Installationsfunktionalität ▪ Funktionalität für Schwachstellenbewertung und Patch-Verwaltung ▪ Erweiterte Antimalware Protection- und Web Protection-Funktionalität ▪ Remote-Desktop-Funktionalität ▪ Sicherheitskontrollfunktionalität wie das Windows Defender-Management ▪ Alarmmeldungen, die auf Daten vom Acronis Cyber Protection Operations Center basieren ▪ Datenerkennungsfunktionalität ▪ #CyberFit-Score
Cyber Protect – Advanced	Bietet: ▪ Backup & Recovery-Funktionen zur Sicherung von anspruchsvollen Workloads wie Microsoft Exchange- und Microsoft SQL-Cluster, die für große Umgebungen entwickelt wurden ▪ Gruppenverwaltung und Planverwaltung ▪ Remote-Installationsfunktionalität ▪ Funktionalität für Schwachstellenbewertung und Patch-Verwaltung ▪ Erweiterte Antimalware Protection- und Web Protection-Funktionalität ▪ Remote-Desktop-Funktionalität ▪ Sicherheitskontrollfunktionalität wie das Windows Defender-Management ▪ Alarmmeldungen, die auf Daten vom Acronis Cyber Protection Operations Center basieren ▪ Datenerkennungsfunktionalität ▪ #CyberFit-Score

Cyber Protect – Disaster Recovery	Bietet: ▪ Backup & Recovery-Funktionen zur Sicherung von anspruchsvollen Workloads wie Microsoft Exchange- und Microsoft SQL-Cluster, die für große Umgebungen entwickelt wurden ▪ Gruppenverwaltung und Planverwaltung ▪ Remote-Installationsfunktionalität ▪ Funktionalität für Schwachstellenbewertung und Patch-Verwaltung ▪ Erweiterte Antimalware Protection- und Web Protection-Funktionalität ▪ Remote-Desktop-Funktionalität ▪ Sicherheitskontrollfunktionalität wie das Windows Defender-Management ▪ Alarmmeldungen, die auf Daten vom Acronis Cyber Protection Operations Center basieren ▪ Datenerkennungsfunktionalität ▪ Disaster Recovery-Funktionalität für Unternehmen, die hohe Anforderungen an Wiederherstellungszeiten (RTOs) haben ▪ #CyberFit-Score

Folgende Backup & Recovery-Funktionen sind nur in der Advanced-Edition und in der Disaster Recovery-Edition verfügbar:

- Ein neuer Bereich in der Benutzeroberfläche zeigt alle Schutzpläne und VM-Replikationspläne an (S. 412)
- Unterstützung für Microsoft SQL Server-AlwaysOn-Verfügbarkeitsgruppen (AAG) (S. 228)
- Unterstützung für Microsoft Exchange Server-Datenbankverfügbarkeitsgruppen (DAG) (S. 230)
- Die Möglichkeit, statische und dynamische Gerätegruppen zu erstellen (S. 97)
- Die Backups einer jeden Maschine können in einem per Skript festgelegten Ordner gespeichert werden (bei unter Windows laufenden Maschinen) (S. 136)
- Sicherung von Oracle Database durch applikationskonformes Backup und Datenbank-Backup mit RMAN (S. 292)
- Sicherung von SAP HANA durch ein Backup der kompletten Maschine, welches den internen SAP HANA-Snapshot verwendet (S. 292)
- Mit der Beglaubigungsfunktion (Notarization) für Dateien können Sie überprüfen und belegen, ob und dass Ihre gesicherten Dateien seit dem Backup authentisch und unverändert geblieben sind (S. 154)
- Mit ASign kann eine gesicherte Datei von mehreren Personen signiert werden (S. 208)

Die Disaster Recovery-Funktionalität wird im Abschnitt 'Disaster Recovery (S. 319)' beschrieben.

3 Vergleich der Editionen

Die Unterschiede zwischen den verschiedenen Editionen des Cyber Protection Service sind nachfolgend aufgeführt.

Funktionen	Cyber Backup			Cyber Protect			
	Standard	Advanced	Disaster Recovery	Essentials	Standard	Advanced	Disas Recov
Schutzfunktionen							
Schwachstellenbewertung (S. 385)	✓	✓	✓	✓	✓	✓	✓
Ransomware Protection und Cryptomining Protection (S. 367)	✓	✓	✓	✓	✓	✓	✓
Antimalware Protection und Web Protection (S. 359)	–	–	–	✓	✓	✓	✓
Sicherheitskontrollfunktionalität wie die Windows Defender Antivirus-Verwaltung (S. 368)	–	–	–	✓	✓	✓	✓
Alarmmeldungen basierend auf Daten vom Cyber Protection Operations Center (S. 407)	–	–	–	✓	✓	✓	✓
Data Protection-Karte (S. 409)	–	–	–	–	✓	✓	✓
Patch-Verwaltung (S. 389)	–	–	–	✓	✓	✓	✓
Remote-Desktop-Zugriff (p. 400)	–	–	–	✓	✓	✓	✓
Antimalware-Backup-Scanning an einem zentralen Cloud-Speicherort (S. 381)	–	–	–	✓	✓	✓	✓
Vorhersage zur Laufwerksintegrität (S. 419)	–	–	–	✓	✓	✓	✓
#CyberFit-Score (p. 114)	–	–	–	✓	✓	✓	✓
Backup-Funktionen							
Backup und Recovery (S. 121)	Kleine Umgebung (bis zu 5)	Große Umgebung (mehr als 5)	Große Umgebung (mehr als 5)	Kleine Umgebung (bis zu 5)	Kleine Umgebung (bis zu 5)	Große Umgebung (mehr als 5)	Groß Umgeb (mehr a
Kontinuierliche Datensicherung (CDP) (S. 130)	–	–	–	✓	✓	✓	✓
Forensik-Backups (S. 171)	–	–	–	–	✓	✓	✓
Safe Recovery (S. 193)	–	–	–	✓	✓	✓	✓
Erweiterter Workload-Schutz (z.B. für MS Exchange, MS SQL-Cluster) (S. 223)	–	✓	✓	–	–	✓	✓
Verwaltungsfunktionen							
Remote-Installation (S. 62)	✓	✓	✓	✓	✓	✓	✓
Gruppenverwaltung (S. 97) und Planverwaltung (S. 412)	–	✓	✓	–	–	✓	✓
Disaster Recovery-Funktionen							

Disaster Recovery (S. 319)	–	–	✓	–	–	–	✓

4 Software-Anforderungen

4.1 Unterstützte Cyber Protect-Funktionen, nach Betriebssystem

Die Cyber Protect-Funktionen werden auf folgenden Betriebssystemen unterstützt:

- Windows: Windows 7 und höher, Windows 2008 R2 und höher.
  Die Windows Defender Antivirus-Verwaltung wird unter Windows 8.1 und höher unterstützt.
- Linux: CentOS 7.x, CentOS 8.0, Virtuozzo 7.x, Acronis Cyber Infrastructure 3.x.
  Andere Linux-Distributionen/-Versionen werden möglicherweise ebenfalls unterstützt, wurden aber nicht getestet.
- macOS: 10.13.x und höher (nur Antivirus & Antimalware Protection wird unterstützt).

Wichtig: *Die Cyber Protect-Funktionen werden nur für Maschinen unterstützt, auf denen ein Protection Agent installiert ist. Für virtuelle Maschinen, die im agentenlosen Modus geschützt werden (z.B. durch den Agenten für Hyper-V, den Agenten für VMware oder den Agenten für Virtuozzo Infrastructure Platform) wird nur die Backup-Funktionalität unterstützt.*

Cyber Protect-Funktionen	Windows	Linux	macOS
Forensik-Backup			
Speicherabbilder sammeln	Ja	Nein	Nein
Snapshot der laufenden Prozesse	Ja	Nein	Nein
Forensik-Backup für Maschinen mit einem Laufwerk ohne Neustart	Ja	Nein	Nein
Beglaubigung von Forensik-Backups (lokale Images)	Ja	Nein	Nein
Beglaubigung von Forensik-Backups (Cloud-Images)	Ja	Nein	Nein
Kontinuierliche Datensicherung (CDP)			
CDP für Dateien und Ordner	Ja	Nein	Nein
CDP für geänderte Dateien über Anwendungsverfolgung	Ja	Nein	Nein
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
Active Protection			
Erkennung von Ransomware	Ja	Nein	Nein
Erkennung von Cryptomining-Prozessen	Ja	Nein	Nein
Erkennung von Prozesseinschleusung	Ja	Nein	Nein

Automatisches Recovery von betroffenen Dateien aus lokalem Cache	Ja	Nein	Nein
Selbstschutzfunktion für Acronis Backup-Dateien	Ja	Nein	Nein
Selbstschutzfunktion für Acronis Software	Ja	Nein	Nein
Verwaltung vertrauenswürdiger/geblockter Prozesse	Ja	Nein	Nein
Ausschluss von Prozessen/Ordnern	Ja	Nein	Nein
Erkennung von Ransomware aufgrund von Prozessverhalten (KI-basiert)	Ja	Nein	Nein
Erkennung von Cryptomining aufgrund von Prozessverhalten	Ja	Nein	Nein
Schutz von externen Laufwerken (HDD, USB-Sticks, SD-Karten)	Ja	Nein	Nein
Netzwerkordnerschutz	Ja	Nein	Nein
Serverseitiger Schutz	Ja	Nein	Nein
Antivirus & Antimalware Protection			
Voll integrierte Active Protection-Funktionalität	Ja	Nein	Nein
Antimalware Protection in Echtzeit	Ja	Nein	Ja
Statische Analyse für übertragbare ausführbare Dateien	Ja	Nein	Ja*
On-Demand-Antimalware-Scanning	Ja	Nein	Ja
Netzwerkordnerschutz	Ja	Nein	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	Nein	Ja**
Ausschluss von Prozessen	Ja	Nein	Nein
Behavioral Analysis Engine (Verhaltensanalyse-Modul)	Ja	Nein	Nein
Exploit-Prävention	Ja	Nein	Nein
Quarantäne	Ja	Nein	Ja
Quarantäne-Speicherort automatisch bereinigen	Ja	Nein	Ja
URL-Filterung (http/https)	Ja	Nein	Nein
Unternehmensweite Positivliste	Ja	Nein	Ja
Windows 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
Schwachstellen- und Konfigurationsbewertung			
Schwachstellenbewertung für Windows	Ja	Nein	Nein
Schwachstellenbewertung von Cyber Infrastructure (Linux)***	Nein	Ja	Nein

Schwachstellenbewertung für Windows-Applikationen von Drittherstellern	Ja	Nein	Nein
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
Abgesichertes Patching: Backup einer Maschine vor der Patch-Installation als Bestandteil eines Schutzplans	Ja	Nein	Nein
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
Laufwerksintegrität			
KI-basierte Kontrolle der HDD-/SSD-Laufwerksintegrität	Ja	Nein	Nein
Smart Protection-Pläne basierend auf Alarmmeldungen des Acronis Cyber Protection Operations Centers (CPOC)			
Bedrohungsfeed	Ja	Nein	Nein
Assistent zur Schwachstellenbehebung	Ja	Nein	Nein
Backup-Scanning			
Backup-Scanning-Plan: Scannen von Image-Backups (in der Cloud) nach Malware	Ja	Nein	Nein
Scannen nach Malware in verschlüsselten Backups	Ja	Nein	Nein
Safe Recovery			
Antimalware-Scanning mit Antivirus & Antimalware Protection bei Wiederherstellungsprozessen	Ja	Nein	Nein
Safe Recovery von verschlüsselten Backups	Ja	Nein	Nein
Remote-Desktop-Verbindung			
Eingehende Verbindung über HTML5-Client	Ja	Nein	Nein
Eingehende Verbindung über Windows-eigenen RDP-Client	Ja	Nein	Nein
Ausgehende Verbindung über HTML5-Client	Ja	Ja	Ja
Ausgehende Verbindung über Windows-eigenen RDP-Client	Ja****	Nein	Ja****
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

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

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

*** 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-announce/, https://lists.centos.org/pipermail/centos-cr-announce/ https://lists.centos.org/pipermail/centos-cr-announce/ und andere.

**** Der Desktopverbindungs-Client und die Microsoft Remote-Desktop-Applikation müssen auf der Maschine installiert sein, die die Verbindung initiiert. Siehe 'Remote-Zugriff (RDP- und HTML5-Clients) (S. 400)'.

4.2 Unterstützte Webbrowser

Die Weboberfläche unterstützt folgende Webbrowser:

- Google Chrome 29 (oder später)
- Mozilla Firefox 23 (oder höher)
- Opera 16 (oder höher)
- Windows Internet Explorer 11 (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.

4.3 Unterstützte Betriebssysteme und Umgebungen

Agent für Windows

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 Vista – alle Editionen

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 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

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 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

Agent für Office 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

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 Linux

Linux mit Kernel 2.6.9 bis 5.1 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, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 8.0*, 8.1*

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

Fedora 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31

SUSE Linux Enterprise Server 10 und 11

SUSE Linux Enterprise Server 12 – wird mit allen Dateisystemen unterstützt, außer Btrfs

Debian 4, 5, 6, 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

CentOS 5.x, 6.x, 7, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 8.0, 8.1

Oracle Linux 5.x, 6.x, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 8.0, 8.1 – sowohl Unbreakable Enterprise Kernel als auch Red Hat Compatible Kernel

CloudLinux 5.x, 6.x, 7, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7

ClearOS 5.x, 6.x, 7, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6

ALT Linux 7.0

Bevor Sie das Produkt auf einem System installieren, das keinen RPM-Paketmanager verwendet (wie etwa ein Ubuntu-System), müssen Sie diesen Manager manuell installieren – beispielsweise durch Ausführung folgenden Befehls (als Benutzer 'root'): **`apt-get install rpm`**

* Konfigurationen mit Stratis werden nicht unterstützt

Agent für Mac

OS X Mavericks 10.9

OS X Yosemite 10.10

OS X El Capitan 10.11

macOS Sierra 10.12

macOS High Sierra 10.13

macOS Mojave 10.14

macOS Catalina 10.15

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

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 – Pro, Education und Enterprise Editionen mit Hyper-V

Windows Server 2016 mit Hyper-V-Rolle – alle Installationsoptionen, mit Ausname des Nano Servers

Microsoft Hyper-V Server 2016

Windows Server 2019 mit Hyper-V-Rolle – alle Installationsoptionen, mit Ausname des Nano Servers

Microsoft Hyper-V Server 2019

Agent für Virtuozzo

Virtuozzo 6.0.10, 6.0.11, 6.0.12, 7.0.13, 7.0.14

Agent für Virtuozzo Infrastructure Platform

Virtuozzo Infrastructure Platform 3.5

4.4 Unterstützte Microsoft SQL Server-Versionen

- 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

4.5 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 später.
- **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.

4.6 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.

4.7 Unterstützte Oracle Database-Versionen

- Oracle Database-Version 11g, alle Editionen
- Oracle Database-Version 12c, alle Editionen.

Es werden nur Einzelinstanz-Konfigurationen unterstützt.

4.8 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.

4.9 Unterstützte Virtualisierungsplattformen

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

Plattform	Backup auf Hypervisor-Ebene (Backup ohne Agent)	Backup innerhalb eines Gastbetriebssystems
VMware		

Plattform	Backup auf Hypervisor-Ebene (Backup ohne Agent)	Backup innerhalb eines Gastbetriebssystems
VMware vSphere-Versionen: 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7 **VMware vSphere-Editionen:** VMware vSphere Essentials* VMware vSphere Essentials Plus* VMware vSphere Standard* VMware vSphere Advanced VMware vSphere Enterprise VMware vSphere Enterprise Plus	+	+
VMware vSphere Hypervisor (Free ESXi)**		+
VMware Server (VMware Virtual Server) VMware Workstation VMware ACE VMware Player		+
Microsoft		
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 Ausname des Nano Servers Microsoft Hyper-V Server 2016 Windows Server 2019 mit Hyper-V – alle Installationsoptionen, mit Ausname des Nano Servers Microsoft Hyper-V Server 2019	+	+
Microsoft Virtual PC 2004 und 2007 Windows Virtual PC		+
Microsoft Virtual Server 2005		+
Citrix		

Plattform	Backup auf Hypervisor-Ebene (Backup ohne Agent)	Backup innerhalb eines Gastbetriebssystems
Citrix XenServer 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		Nur vollständig virtualisierte Gäste (HVM). Paravirtualisierte Gäste (PV-Gäste) werden nicht unterstützt.
Red Hat und Linux		
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		+
Kernel-based Virtual Machines (KVM)		+
Parallels		
Parallels Workstation		+
Parallels Server 4 Bare Metal		+
Oracle		
Oracle VM Server 3.0, 3.3, 3.4		Nur vollständig virtualisierte Gäste (HVM). Paravirtualisierte Gäste (PV-Gäste) werden nicht unterstützt.
Oracle VM VirtualBox 4.x		+
Nutanix		
Nutanix Acropolis Hypervisor (AHV) 20160925.x bis 20180425.x		+
Virtuozzo		
Virtuozzo 6.0.10, 6.0.11, 6.0.12	+	Nur virtuelle Maschinen. Container werde nicht unterstützt.
Virtuozzo 7.0.13, 7.0.14	Nur Ploop-Container. Virtuelle Maschinen werden nicht unterstützt.	Nur virtuelle Maschinen. Container werde nicht unterstützt.
Virtuozzo Infrastructure Platform		
Virtuozzo Infrastructure Platform 3.5	+	+
Amazon		
Amazon EC2-Instanzen		+
Microsoft Azure		
Virtuelle Azure-Maschinen		+

* 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.

Einschränkungen

- **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.

- **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 VMware und der Agent für Hyper-V sichern keine LUN-Volumes, die über einen iSCSI-Initiator verbunden sind, der von innerhalb des Gastbetriebssystems aus arbeitet. Weil den ESXi- und Hyper-V-Hypervisoren 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.

- **Linux-Maschinen, die logische Volumes enthalten (LVM)**

  Folgende Aktionen für Linux-Maschinen mit LVM werden vom Agenten für VMware und dem Agenten für Hyper-V nicht unterstützt:

  - P2V-Migration, V2P-Migration und V2V-Migration von Virtuozzo. Den Agenten für Linux verwenden, um Backups und Boot-Medien für Wiederherstellungen zu erstellen.
  - Eine virtuelle Maschine direkt aus einem Backup ausführen, welches durch den Agenten für Linux erstellt wurde.

- **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 (S. 152) 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 6.7 unterstützt.

4.10 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

Es wird dringend empfohlen, die Verschlüsselungssoftware vor der Installation der Protection Agenten einzurichten.

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. Erstellen Sie die Secure Zone.
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

5 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		+	+	
ext2/ext3/ext4		+	-	
HFS+	Agent für Mac	-	+	
APFS		-	+	▪ 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	+	-	▪ Kein Ausschluss von Dateien von einem Laufwerk-Backup ▪ Schnelle inkrementelle/differentielle Backups werden nicht unterstützt.
ReiserFS3		+	-	
ReiserFS4		+	-	▪ Kein Ausschluss von Dateien von einem Laufwerk-Backup ▪ Schnelle inkrementelle/differentielle Backups werden nicht unterstützt. ▪ Keine Größenänderung von Volumes während einer Wiederherstellung
ReFS	Alle Agenten	+	+	
XFS		+	+	

Dateisystem	Unterstützt durch			Einschränkungen
	Agenten	Boot-Medien für Windows und Linux	Boot-Medien für Mac	
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 ▪ Es können keine Dateien aus einem Backup ausgeschlossen werden ▪ 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 (S. 296) oder das Backup auf einer Maschine mounten (S. 221), 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.

6 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:

- **Einen Link zur Kontoaktivierung.** Klicken Sie auf den Link und definieren Sie das Kennwort für das Konto. Stellen Sie sicher, dass Ihr Kennwort mindestens acht Zeichen lang ist. Merken Sie sich Ihren Anmeldenamen, der auf der Kontoaktivierungsseite angezeigt wird.

  Wenn Ihr Administrator die Zwei-Faktor-Authentifizierung aktiviert hat, werden Sie aufgefordert, die Zwei-Faktor-Authentifizierung für Ihr Konto (S. 30) einzurichten.
- **Einen Link zur Anmeldeseite der Service-Konsole.** Verwenden Sie diesen Link, um zukünftig auf die Konsole zuzugreifen. Die Anmeldedaten (Anmeldename, Kennwort) sind mit denen des vorherigen Schrittes identisch.

6.1 Zwei-Faktor-Authentifizierung

Die Zwei-Faktor-Authentifizierung bietet einen zusätzlichen Schutz gegen unbefugte Zugriffe auf Ihr Konto. Wenn die Zwei-Faktor-Authentifizierung eingerichtet ist, müssen Sie Ihr Kennwort (der erste Faktor) und einen Einmalcode (der zweite Faktor) eingeben, um sich an der Service-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 keinen Zugriff auf Ihr Zweit-Faktor-Geräte hat.

Der Einmalcode wird auf der Grundlage der aktuellen Uhrzeit des Gerätes sowie eines „Geheimnis“ (auch Secret oder geheimer Schlüssel genannt, hier ein QR- oder alphanumerischen Code), welches vom Cyber Protection Service bereitgestellt wird. Sie müssen diesen geheimen Schlüssel (das „Geheimnis“) bei der ersten Anmeldung in die Authentifizierungsapplikation eingeben.

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

1. Wählen Sie Ihr Zweit-Faktor-Gerät.

   Am gebräuchlichsten ist es ein Smartphone; Sie können jedoch auch ein Tablet, ein Notebook oder einen Desktop-PC verwenden.
2. Überprüfen Sie, dass die allgemeinen Zeiteinstellungen des Gerätes korrekt sind und der aktuellen Uhrzeit entsprechen. Stellen Sie sicher, dass sich das Gerät nach einer gewissen Inaktivitätszeit selbst sperrt.
3. Installieren Sie die Authentifizierungsapplikation auf dem Gerät. Empfehlenswerte Apps sind Google Authenticator oder Microsoft Authenticator.
4. Gehen Sie zur Anmeldeseite der Service-Konsole und legen Sie Ihr Kennwort fest.

   Die Service-Konsole zeigt den QR-Code und den alphanumerischen Code an.
5. Sichern Sie den QR-Code und den alphanumerischen Code auf eine beliebige Weise (z.B. durch Ausdrucken des Bildschirminhaltes, indem Sie den Code aufschreiben oder indem Sie einen Screenshot im Cloud Storage speichern). Wenn Sie Ihr Zweit-Faktor-Gerät verlieren sollten, können Sie die Zwei-Faktor-Authentifizierung mithilfe dieser Codes zurücksetzen.
6. Öffnen Sie die Authentifizierungsapplikation und führen Sie dann eine der folgenden Aktionen aus:
   - Scannen Sie den QR-Code

- Geben Sie den alphanumerischen Code manuell in die Applikation ein.

  Die Authentifizierungsapplikation generiert einen Einmalcode (ein Einmalkennwort). Alle 30 Sekunden wird ein neuer Code generiert.

7. Wechseln Sie wieder zur Anmeldeseite der Service-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. Dadurch müssen Sie keinen Einmalcode mehr eingeben, wenn Sie sich mit genau diesem Browser an diesem System anmelden.

Was ist, wenn...

...ich das Zweit-Faktor-Gerät verliere?

Wenn Sie einen als vertrauenswürdig gekennzeichneten Browser haben, können Sie sich mit diesem Browser anmelden. Wenn Sie aber ein neues Gerät haben, können Sie auch die Schritte 1-3 und 6-7 aus der oberen Prozedur wiederholen. Verwenden Sie dabei das neue Gerät und den gespeicherten QR-Code oder den alphanumerischen Code.

Wenn Sie den Code nicht gespeichert haben, bitten Sie Ihren Administrator oder Service-Provider, die Zwei-Faktor-Authentifizierung für Ihr Konto zurückzusetzen. Danach können Sie dann die Schritte 1-3 und 6-7 der oberen Prozedur mit Ihrem neuen Gerät durchführen.

...ich das Zweit-Faktor-Gerät wechseln möchte?

Klicken Sie bei der Anmeldung auf den Link **Zwei-Faktor-Authentifizierung zurücksetzen**, bestätigen Sie die Aktion durch Eingabe des Einmalcodes und wiederholen Sie dann die obere Prozedur mit dem neuen Gerät.

7 Auf den Cyber Protection Service zugreifen

Sie können sich am Cyber Protection Service anmelden, wenn Sie Ihr Konto aktiviert haben.

So können Sie sich am Cyber Protection Service anmelden

1. Gehen Sie zur Anmeldeseite des Cyber Protection Service. Die Adresse der Anmeldeseite war in der Aktivierungs-E-Mail-Nachricht enthalten.
2. Geben Sie den Anmeldenamen ein und klicken Sie dann auf **Weiter**.
3. Geben Sie das Kennwort ein und klicken Sie dann auf **Weiter**.
4. Wenn Sie die Administrator-Rolle im Cyber Protection Service haben, klicken Sie auf **Cyber Protection**.

   Benutzer, die keine Administrator-Rolle haben, melden sich direkt an der Service-Konsole an.

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

So können Sie Ihr Kennwort zurücksetzen

1. Gehen Sie zur Anmeldeseite des Cyber Protection Service.
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. Stellen Sie sicher, dass Ihr Kennwort mindestens acht Zeichen lang ist.

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

Wenn **Cyber Protection** nicht der einzige Service ist, den Sie abonniert 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.

Wenn Sie eine der Cyber Protection-Editionen abonniert haben, können Sie von der Service-Konsole aus ein Feedback über das Produkt senden. Klicken Sie im linken Navigationsmenü auf **Feedback senden**, füllen Sie die Formularfelder aus, hängen Sie (bei Bedarf) Dateien an und klicken Sie auf **Senden**.

8 Die Installation der Software

Verwandte Themen

Zu installierende Komponenten auswählen 67

8.1 Vorbereitung

Schritt 1:

Wählen Sie einen Agenten danach aus, welche Art von Daten Sie per Backup sichern wollen. Die nachfolgende Tabelle soll Ihnen durch eine Zusammenfassung aller relevanten Informationen bei dieser Entscheidung helfen.

Beachten Sie, dass unter Windows der Agent für Windows zusammen mit dem Agenten für Exchange, dem Agenten für SQL, dem Agenten für Active Directory und dem Agenten für Oracle 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.

Unter Linux erfordern der Agent für Oracle und der Agent für Virtuozzo, dass zusätzlich der Agent für Linux (64 Bit) installiert wird. Diese drei Agenten teilen einen gemeinsamen Installer.

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	
Applikationen		
SQL-Datenbanken	Agent für SQL	Auf der Maschine, die den Microsoft SQL Server ausführt.

Was möchten Sie sichern?	Welchen Agenten soll ich installieren?	Wo soll die Installation erfolgen?
Exchange-Datenbanken	Agent für Exchange	Auf der Maschine, auf der die Postfachrolle des Microsoft Exchange Servers ausgeführt wird.*
Microsoft Office 365-Postfächer	Agent für Office 365	Auf einer Windows-Maschine, die über eine Internetverbindung verfügt. Sie müssen – abhängig von der gewünschten Funktionalität – möglicherweise den Agenten für Office 365 installieren. Weitere Informationen dazu finden Sie im Abschnitt 'Office 365-Daten sichern' (S. 251).
Microsoft Office 365 OneDrive-Dateien und SharePoint Online-Websites	—	Diese Daten können nur von einem Agenten gesichert werden, in der Cloud installiert ist. Weitere Informationen finden Sie im Abschnitt 'Office 365-Daten sichern (S. 251)'.
G Suite Gmail-Postfächer, Google Drive-Dateien und Shared Drive-Dateien	—	Diese Daten können nur von einem Agenten gesichert werden, in der Cloud installiert ist. Weitere Informationen finden Sie im Abschnitt 'G Suite sichern (S. 277)'.
Maschinen, auf denen die Active Directory Domain Services (Active Directory-Domänendienste) laufen	Agent für Active Directory	Auf dem Domain Controller.
Maschinen, auf denen Oracle Database läuft	Agent für Oracle	Auf der Maschine, die Oracle Database ausführt.
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 Virtuozzo-Maschinen und -Container***	Agent für Virtuozzo	Auf dem Virtuozzo-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		

Was möchten Sie sichern?	Welchen Agenten soll ich installieren?	Wo soll die Installation erfolgen?
Red Hat Virtualization (RHV/RHEV)		
Kernel-based Virtual Machines (KVM)		
Virtuelle Oracle-Maschinen		
Virtuelle Nutanix AHV-Maschinen		
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. Ausführliche Informationen finden Sie im Abschnitt 'Agent für VMware – LAN-freies Backup (S. 305)'.

***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. Davon unabhängig wird die Maschine jedoch als virtuelle Maschine gezählt, wenn Sie Quotas für eine bestimmte Anzahl von Maschinen festlegen.

Schritt 2:

Überprüfen Sie die Systemanforderungen für die Agenten.

Agent	Durch den/die Agent(en) belegter Speicherplatz
Agent für Windows	550 MB
Agent für Linux	500 MB
Agent für Mac	450 MB
Agent für SQL	600 MB (50 MB + 550 MB Agent für Windows)
Agent für Exchange	750 MB (200 MB + 550 MB Agent für Windows)
Agent für Office 365	550 MB
Agent für Active Directory	600 MB (50 MB + 550 MB Agent für Windows)
Agent für VMware	700 MB (150 MB + 550 MB Agent für Windows)
Agent für Hyper-V	600 MB (50 MB + 550 MB Agent für Windows)
Agent für Virtuozzo	500 MB
Agent für Oracle	450 MB

Die typische Arbeitsspeicherbelegung beträgt 300 MB ('oberhalb' des Betriebssystems und anderer ausgeführter Applikationen). Der Speicherverbrauch kann – abhängig von der Art und Menge der Daten, die die Agenten verarbeiten – kurzzeitig auf bis zu 2 GB steigen.

Bei einer Wiederherstellung mit einem Boot-Medium oder einer Laufwerkswiederherstellung mit Neustart werden mindestens 1 GB Arbeitsspeicher benötigt.

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' beschrieben.

Um das Setup-Programm des Agenten für Office 365 herunterzuladen, klicken Sie in der oberen rechten Ecke zuerst auf das Kontosymbol und dann auf **Downloads** –> **Agent für Office 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) eingehende und ausgehende Verbindungen über folgende TCP-Ports erlauben:

- **443** und **8443** – diese Ports werden verwendet, um auf die Service-Konsole zuzugreifen, die Agenten zu registrieren, Zertifikate herunterzuladen, Benutzer zu autorisieren und Dateien aus dem Cloud Storage herunterzuladen.
- **7770...7800** – die Agenten verwenden diese Ports, um mit dem Backup Management Server zu kommunizieren.
- **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 im Abschnitt 'Proxy-Server-Einstellungen (S. 39)' 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

- **TCP 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.
- **TCP 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.
- **TCP 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 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 (S. 304)'). 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.

Schritt 6:

Überprüfen Sie auf derjenigen Maschine, auf der Sie den Cyber 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 Cyber Protection Agenten verwendeten Ports ändern

Es kann sein, dass einige der für den Cyber Protection Agenten erforderlichen Ports von anderen Applikationen in Ihrer Umgebung verwendet werden. Um Konflikte zu vermeiden, können Sie die standardmäßig vom Cyber 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

8.2 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 ist, wie die **`gcc version`** 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 wie bei **`Linux version`** im Schritt 1 sind.
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-<Paketversion>`
		`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.

8.3 Proxy-Server-Einstellungen

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 oder schon vorher bereitgestellt werden.

Unter Windows:

Wenn in Windows ein Proxy-Server konfiguriert ist (**Systemsteuerung** –> **Internetoptionen** –> **Verbindungen**), liest das Setup-Programm die entsprechenden Proxy-Server-Einstellungen aus der Registry aus und übernimmt diese automatisch. Sie können die Proxy-Einstellungen auch während der Installation eingeben oder sie im Voraus (wie nachfolgend beschrieben) festlegen. Wenn Sie die Proxy-Einstellungen nach der Installation ändern wollen, gehen Sie genauso vor.

So können Sie die Proxy-Server-Einstellungen in Windows spezifizieren

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. Sollte der Protection Agent bisher noch nicht installiert sein, können Sie die Installation jetzt durchführen.
9. Öffnen Sie die Datei **%programdata%\Acronis\Agent\etc\aakore.yaml** in einem Text-Editor.
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
```

Unter Linux:

Starten Sie die Installationsdatei mit den Parametern **--http-proxy-host=**ADRESSE **--http-proxy-port=**PORT **--http-proxy-login=**ANMELDENAME **--http-proxy-password=**KENNWORT. Wenn Sie die Proxy-Einstellungen nach der Installation ändern wollen, verwenden Sie die unten beschriebene Prozedur.

So können Sie die Proxy-Server-Einstellungen in Linux ändern

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">"ADRESSE"</value>
    <value name="Port" type="Tdword">"PORT"</value>
    <value name="Login" type="TString">"ANMELDENAME"</value>
    <value name="Password" type="TString">"KENNWORT"</value>
</key>
```

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

3. Ersetzen Sie ADRESSE 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 ANMELDENAME und KENNWORT 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 folgendem 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
```

Unter macOS:

Sie können die Proxy-Einstellungen auch während der Installation eingeben oder sie im Voraus (wie nachfolgend beschrieben) festlegen. Wenn Sie die Proxy-Einstellungen nach der Installation ändern wollen, gehen Sie genauso vor.

So können Sie die Proxy-Server-Einstellungen in macOS spezifizieren

1. Erstellen Sie die Datei '**/Library/Application Support/Acronis/Registry/Global.config**' und öffnen Sie diese in einem Text-Editor (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. Sollte der Protection Agent bisher noch nicht installiert sein, können Sie die Installation jetzt durchführen.
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 **Programme** –> **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
    ```

Unter einem Boot-Medium

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 festlegen wollen, müssen Sie auf **Extras** –> **Proxy-Server** klicken und dann den Host-Namen/die IP-Adresse, den Port und die Anmeldedaten des Proxy-Servers spezifizieren.

8.4 Installation der Agenten

Sie können Agenten auf Maschinen installieren, die eines der im Abschnitt 'Unterstützte Betriebssysteme und Umgebungen (S. 18)' aufgeführten Betriebssysteme ausführen. Die Betriebssysteme, die die Cyber Protect-Funktionen unterstützen, sind im Abschnitt 'Unterstützte Cyber Protect-Funktionen, nach Betriebssystem (S. 15)' aufgeführt.

Unter Windows:

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 ist möglicherweise ein Neustart der Maschine erforderlich. Das Microsoft Visual C++ Redistributable-Paket kann unter dieser Adresse gefunden werden: https://support.microsoft.com/help/2999226/update-for-universal-c-runtime-in-windows.

1. Überprüfen Sie, dass die Maschine mit dem Internet verbunden ist.
2. Melden Sie sich als Administrator an und starten Sie das Setup-Programm.

3. [Optional] Klicken Sie auf **Installationseinstellungen anpassen**, um (sofern gewünscht) eine oder mehrere der folgenden Änderungen durchzuführen:
   - Um die installierenden Komponenten zu ändern (insbesondere, um die Installation des Cyber Protection Monitors und des Befehlszeilenwerkzeugs zu deaktivieren).
   - Um die Methode zu ändern, mit der die Maschine 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 Agenten-Dienst ausgeführt werden soll. Weitere Informationen dazu finden Sie im Abschnitt 'Das Anmeldekonto auf Windows-Maschinen ändern (S. 46)'.
   - 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, dessen virtuelle Maschinen der Agent sichern soll – und klicken Sie dann auf **Fertig**. Wir empfehlen, dass Sie ein Konto verwenden, dem die Rolle **Administrator** zugewiesen ist. Alternativ können Sie auch ein Konto angeben, welches über die notwendigen Berechtigungen (S. 312) auf dem vCenter Server oder ESXi-Host verfügt.
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.
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:
   - Klicken Sie auf **Die Maschine registrieren**. Melden Sie sich im geöffneten Browserfenster an der Service-Konsole an, überprüfen Sie die Registrierungsinformationen und klicken Sie dann auf **Registrierung bestätigen**.
   - Klicken Sie auf **Registrierungsinfo anzeigen**. Im Setup-Programm werden der Registrierungslink und Registrierungscode angezeigt. Sie können diese kopieren und die Registrierungsschritte dann 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.

   Tipp: *Beenden Sie das Setup-Programm nicht, bevor Sie die Registrierung bestätigt haben! Um die Registrierung neu initiieren zu können, müssen Sie das Setup-Programm neu starten. Klicken Sie anschließend auf* ***Die Maschine registrieren****.*

   Dadurch wird die Maschine dem Konto zugewiesen, welches zur Anmeldung an die Service-Konsole verwendet wurde.

- Registrieren Sie die Maschine manuell unter Verwendung der Befehlszeile. Weitere Informationen über die entsprechende Durchführung finden Sie im Abschnitt 'Maschinen manuell registrieren (S. 59)'.

Unter Linux:

1. Überprüfen Sie, dass die Maschine mit dem Internet verbunden ist.
2. Starten Sie die Installationsdatei als Benutzer 'root'.

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

   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**

   Der Agent für Oracle und der Agent für Virtuozzo 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:

   - Klicken Sie auf **Die Maschine registrieren**. Melden Sie sich im geöffneten Browserfenster an der Service-Konsole an, überprüfen Sie die Registrierungsinformationen und klicken Sie dann auf **Registrierung bestätigen**.
   - Klicken Sie auf **Registrierungsinfo anzeigen**. Im Setup-Programm werden der Registrierungslink und Registrierungscode angezeigt. Sie können diese kopieren und die Registrierungsschritte dann 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.

   Tipp: *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 die Maschine dem Konto zugewiesen, welches zur Anmeldung an die Service-Konsole verwendet wurde.

- Registrieren Sie die Maschine manuell unter Verwendung der Befehlszeile. Weitere Informationen über die entsprechende Durchführung finden Sie im Abschnitt 'Maschinen manuell registrieren (S. 59)'.

6. 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: *Während der Installation wird ein neuer Schlüssel zur Signierung des* ***snapapi****-Modul generiert und als sogenannter MOK (Machine Owner Key) registriert. Der Neustart ist zwingend erforderlich, damit der Schlüssel registriert werden kann. Ohne die Registrierung des Schlüssels ist der Agent nicht funktionsfähig. Wenn Sie UEFI Secure Boot nach der Installation des Agenten aktivieren, müssen Sie die Installation (einschließlich Schritt 6) wiederholen.*

7. 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 (üblicherweise 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

Unter macOS:

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 **Fortsetzen**.
8. Warten Sie, bis die Registrierungsanzeige erscheint.
9. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Klicken Sie auf **Die Maschine registrieren**. Melden Sie sich im geöffneten Browserfenster an der Service-Konsole an, überprüfen Sie die Registrierungsinformationen und klicken Sie dann auf **Registrierung bestätigen**.
   - Klicken Sie auf **Registrierungsinfo anzeigen**. Im Setup-Programm werden der Registrierungslink und Registrierungscode angezeigt. Sie können diese kopieren und die Registrierungsschritte dann 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.

Tipp: *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 die Maschine dem Konto zugewiesen, welches zur Anmeldung an die Service-Konsole verwendet wurde.

- Registrieren Sie die Maschine manuell unter Verwendung der Befehlszeile. Weitere Informationen über die entsprechende Durchführung finden Sie im Abschnitt 'Maschinen manuell registrieren (S. 59)'.

10. 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 unter http://kb.acronis.com/content/62133 https://kb.acronis.com/content/62133.

8.4.1 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.

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. Die Berechtigung **Vollzugriff** muss für den Ordner **`%PROGRAMDATA%\Acronis`** (in Windows XP und Server 2003: **`%ALLUSERSPROFILE%\Application Data\Acronis`**) und dessen Unterordner gewährt sein.

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 es nicht empfehlenswert ist, Anmeldekonten nach Abschluss der Installation noch mal manuell zu ändern.

8.5 Unbeaufsichtigte Installation oder Deinstallation

8.5.1 Unbeaufsichtigte Installation oder Deinstallation unter Windows

Dieser Abschnitt beschreibt, wie Sie die Protection Agenten auf einer unter Windows laufenden Maschine und mithilfe des Windows Installers (dem Programm **msiexec**) im unbeaufsichtigten Modus installieren oder deinstallieren können. In einer Active Directory-Domain können Sie unbeaufsichtigte Installationen auch über die Gruppenrichtlinien durchführen – siehe den Abschnitt 'Agenten per Gruppenrichtlinie bereitstellen (S. 84)'.

Sie können während der Installation eine Datei verwenden, die als **Transform** bezeichnet wird (eine .mst-Datei). Ein Transform ist eine Datei mit Installationsparametern. Alternativ können Sie die Installationsparameter auch direkt im Befehlszeilenmodus eingeben.

Die .mst-Transform-Datei erstellen und die Installationspakete erstellen

1. Melden Sie sich als Administrator an und starten Sie das Setup-Programm.
2. Klicken Sie auf **.mst- und .msi-Dateien für eine unbeaufsichtigte Installation erstellen**.
3. Bestimmen Sie bei **Zu installierende Komponenten**, was Sie installieren wollen. Die Installationspakete für diese Komponenten werden vom Setup-Programm extrahiert.
4. Wählen Sie bei den **Registrierungseinstellungen** den Befehl **Anmeldedaten verwenden** oder **Registrierungstoken verwenden**. Weitere Informationen darüber, wie Sie ein Registrierungstoken generieren können, finden Sie im Abschnitt 'Agenten per Gruppenrichtlinie bereitstellen (S. 84)'.
5. Überprüfen oder ändern Sie weitere Installationseinstellungen, die der .mst-Datei hinzugefügt werden sollen.
6. Klicken Sie auf **Fortsetzen** und wählen Sie dann den Ordner aus, wo die .mst-Transform-Datei erstellt wird und die .msi- und .cab-Installationspakete extrahiert werden.
7. Klicken Sie auf **Generieren**.

Das Produkt mithilfe der .mst-Transform-Datei installieren

Führen Sie in der Kommandozeile den nachfolgenden Befehl aus.

Befehlsvorlage:

```
msiexec /i <Paket-Name> TRANSFORMS=<Transform-Name>
```

Wobei:

- `<Paket-Name>` der Name der .msi-Datei ist.
- `<Transform-Name>` die Bezeichnung der Transform-Datei ist.

Befehlsbeispiel:

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

Das Produkt durch manuelle Spezifikation der Parameter installieren oder deinstallieren

Führen Sie in der Kommandozeile den nachfolgenden Befehl aus.

Befehlsvorlage (Installation):

```
msiexec /i <Paket-Name> <PARAMETER 1>=<Wert 1> ... <PARAMETER N>=<Wert n>
```

Wobei `<Paket-Name>` der Name der .msi-Datei ist. Alle verfügbaren Parameter und deren Werte sind im Abschnitt 'Parameter für eine unbeaufsichtigte Installation oder Deinstallation (S. 49)' beschrieben.

Befehlsvorlage (Deinstallation):

```
msiexec /x <Paket-Name> <PARAMETER 1>=<Wert 1> ... <PARAMETER N>=<Wert n>
```

Das .msi-Paket muss dieselbe Version wie das Produkt haben, welches Sie deinstallieren wollen.

8.5.1.1 Parameter für eine unbeaufsichtigte Installation oder Deinstallation

Dieser Abschnitt beschreibt die Parameter, die bei einer unbeaufsichtigten Installation oder Deinstallation unter Windows verwendet werden können. Neben diesen Parametern können Sie auch noch weitere Parameter von **`msiexec`** verwenden, die in diesem Artikel beschrieben sind: https://msdn.microsoft.com/en-us/library/windows/desktop/aa367988(v=vs.85).aspx.

Installationsparameter

Grundlegende Parameter

`ADDLOCAL=``<Liste der Komponenten>`

Die zu installierenden Komponenten, durch Kommata getrennt und ohne Leerzeichen. Alle spezifizierten Komponenten müssen vor der Installation vom Setup-Programm extrahiert werden.

Die vollständige Liste der Komponenten sieht folgendermaßen aus:

Komponente	Musst gemeinsam installiert werden mit	Bit-Anzahl	Komponenten-Name/ -Beschreibung
MmsMspComponents		32 Bit/64 Bit	Kernkomponenten für Agenten
BackupAndRecoveryAgent	MmsMspComponents	32 Bit/64 Bit	Agent für Windows
ArxAgentFeature	BackupAndRecoveryAgent	32 Bit/64 Bit	Agent für Exchange
ArsAgentFeature	BackupAndRecoveryAgent	32 Bit/64 Bit	Agent für SQL
ARADAgentFeature	BackupAndRecoveryAgent	32 Bit/64 Bit	Agent für Active Directory
ArxOnlineAgentFeature	MmsMspComponents	32 Bit/64 Bit	Agent für Office 365
OracleAgentFeature	BackupAndRecoveryAgent	32 Bit/64 Bit	Agent für Oracle
AcronisESXSupport	MmsMspComponents	64 Bit	Agent für VMware ESX(i) (Windows)
HyperVAgent	MmsMspComponents	32 Bit/64 Bit	Agent für Hyper-V
CommandLineTool		32 Bit/64 Bit	Befehlszeilenwerkzeug
TrayMonitor	BackupAndRecoveryAgent	32 Bit/64 Bit	Cyber Protection Monitor

`TARGETDIR=``<Pfad>`

Der Ordner, wo das Produkt installiert werden soll. Standardmäßig heißt der Ordner: `C:\Programme\BackupClient`.

`REBOOT=ReallySuppress`

Wird der Parameter spezifiziert, dann ist ein Neustart der Maschine verboten.

`/l*v` `<Protokolldatei>`

Wird der Parameter spezifiziert, dann wird das Installationsprotokoll (Log) im ausführlichen Modus (Verbose-Modus) in der spezifizierten Datei gespeichert. Die Protokolldatei kann verwendet werden, um Installationsprobleme zu analysieren.

CURRENT_LANGUAGE=<Sprach-ID>

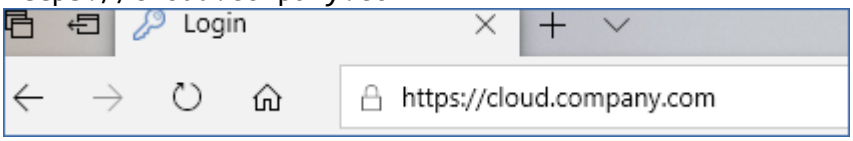
Die Sprache für das Produkt. Die verfügbaren Werte sind: **en, bg, cs, da, de, es, fr, hu, id, it, ja, ko, ms, nb, nl, pl, pt, pt_BR, ru, fi, sr, sv, tr, zh, zh_TW.** Wenn der Parameter nicht spezifiziert wird, wird die Produktsprache durch die Sprache Ihres Systems definiert (vorausgesetzt, dass diese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

Registrierungsparameter

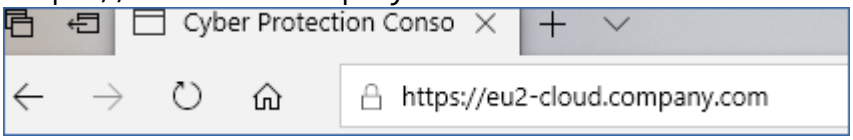
REGISTRATION_ADDRESS

Dies ist die URL für den 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 **REGISTRATION_ADDRESS** mit den Parametern **REGISTRATION_LOGIN** und **REGISTRATION_PASSWORD** verwenden, müssen Sie die Adresse spezifizieren, die Sie zur **Anmeldung** am Cyber Protection Service verwenden. Beispielsweise `https://cloud.company.com`:



- Wenn Sie **REGISTRATION_ADDRESS** mit dem Parameter **REGISTRATION_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 hier nicht die Adresse `https://cloud.company.com` verwenden.

REGISTRATION_LOGIN und **REGISTRATION_PASSWORD**

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

REGISTRATION_PASSWORD_ENCODED

Kennwort für das Konto, unter dem der Agent im Cyber Protection Service registriert wird (codiert in Base64). Weitere Informationen über die Codierung Ihres Kennworts finden Sie im Abschnitt 'Maschinen manuell registrieren (S. 59)'.

REGISTRATION_TOKEN

Das Registrierungstoken ist eine Folge von 12 Zeichen, die durch Bindestriche in 3 Segmente separiert sind. Sie können ein Token in der Service-Konsole generieren, wie im Abschnitt 'Agenten per Gruppenrichtlinie bereitstellen (S. 84)' erläutert.

REGISTRATION_REQUIRED={0,1}

Definiert, wie die Installation beendet wird, falls die Registrierung fehlschlägt. Wenn der Wert **1** beträgt, schlägt auch die Installation fehl. Der Standardwert ist **0**. Wenn Sie diesen Parameter also nicht spezifizieren, wird die Installation erfolgreich abgeschlossen, auch wenn der Agent nicht registriert ist.

Zusätzliche Parameter

Verwenden Sie einen der folgenden Parameter, um das Anmeldekonto für den Agenten-Dienst in Windows zu definieren:

- **MMS_USE_SYSTEM_ACCOUNT={0,1}**

  Wenn der Wert **1** beträgt, wird der Agent unter dem Konto **Lokales System** ausgeführt.
- **MMS_CREATE_NEW_ACCOUNT={0,1}**

  Wenn der Wert **1** beträgt, wird der Agent unter einem neu erstellten Konto namens **Acronis Agent User** ausgeführt.
- **MMS_SERVICE_USERNAME=**<Benutzername> und **MMS_SERVICE_PASSWORD=**<Kennwort>

  Verwenden Sie diese Parameter, um ein vorhandenes Konto zu spezifizieren, unter dem der Agent laufen soll.

Weitere Informationen über Anmeldekonten finden Sie im Abschnitt 'Das Anmeldekonto auf Windows-Maschinen ändern (S. 46)'.

SET_ESX_SERVER={0,1}

Lautet der Wert **0**, dann wird der zu installierende Agent für VMware nicht mit einem vCenter Server oder ESXi-Host verbunden. Lautet der Wert **1**, dann spezifizieren Sie folgende Parameter:

- **ESX_HOST=**<Host-Name>

  Der Host-Name oder die IP-Adresse des vCenter Servers oder ESXi-Hosts.
- **ESX_USER=**<Benutzername> und **ESX_PASSWORD=**<Kennwort>

  Die Anmeldedaten, um auf den vCenter Server oder ESXi-Host zugreifen zu können.

HTTP_PROXY_ADDRESS=<IP-Adresse> und **HTTP_PROXY_PORT=**<Port>

Der HTTP-Proxy-Server, der vom Agenten verwendet werden soll. 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.

HTTP_PROXY_ONLINE_BACKUP={0,1}

Wenn der Wert **0** beträgt oder der Parameter nicht spezifiziert wurde, wird der Agent den Proxy-Server nur für Backups in die Cloud und Wiederherstellungen aus der Cloud verwenden. Wenn der Wert **1** beträgt, wird der Agent den Proxy-Server auch für Verbindungen zum Management Server verwenden.

Deinstallationsparameter

REMOVE={<Liste der Komponenten>**|ALL}**

Die zu entfernenden Komponenten, durch Kommata getrennt und ohne Leerzeichen. Lautet der Wert **ALL**, dann werden alle Produkt-Komponenten deinstalliert.

Sie können zusätzlich noch folgende Parameter spezifizieren:

DELETE_ALL_SETTINGS={0, 1}

Lautet der Wert **1**, dann werden auch die Protokolle (Logs), Tasks und Konfigurationseinstellungen des Produkts entfernt.

Beispiele

- Den Agent für Windows, das Befehlszeilenwerkzeug und den Cyber Protection Monitor installieren. Die Maschine 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,CommandLineTool,TrayMonitor
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 Agent für Windows, das Befehlszeilenwerkzeug und den Cyber Protection Monitor installieren. Ein neues Anmeldekonto für den Agenten-Dienst in Windows erstellen. Die Maschine 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 Agent für Windows, das Befehlszeilenwerkzeug, den Agenten für Oracle und den Cyber Protection Monitor installieren. Die Maschine im Cyber Protection Service unter Verwendung eines Benutzernamens und eines Base64-codierten Kennworts registrieren.

```
msiexec.exe /i BackupClient64.msi /l*v my_log.txt /qn
ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,CommandLineTool,OracleAgentFea
ture,TrayMonitor 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 Agent für Windows, das Befehlszeilenwerkzeug und den Cyber Protection 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
```

- Alle Agenten deinstallieren und deren Protokolle, Tasks und Konfigurationseinstellungen löschen.

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

8.5.2 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 Protection Agenten installieren oder deinstallieren

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:

  ```
  <Paket-Name> -a <Parameter 1> ... <Parameter N>
  ```

  Wobei `<Paket-Name>` die Bezeichnung der Installationspakete ist (eine .i686- oder .x86_64-Datei). Alle verfügbaren Parameter und deren Werte sind im Abschnitt 'Parameter für eine unbeaufsichtigte Installation oder Deinstallation (S. 53)' beschrieben.
- Führen Sie folgenden Befehl aus, um die Installation mit Parametern zu starten, die in einer separaten Textdatei spezifiziert wurden:

  ```
  <Paket-Name> -a --options-file=<Pfad zur Datei>
  ```

  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 vom gewünschten Wert. 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.

8.5.2.1 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** bzw. die Parameter **--rain** und **--token**). Sie können weitere Parameter verwenden, um Ihre Installation anzupassen.

Installationsparameter

Grundlegende Parameter

{-i |--id=}<Liste der Komponenten>

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

Ohne diesen Parameter werden alle oberen Komponenten installiert.

Der Agent für Oracle und der Agent für Virtuozzo 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 Service-Konsole generieren, wie im Abschnitt 'Agenten per Gruppenrichtlinie bereitstellen (S. 84)' erläutert.

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

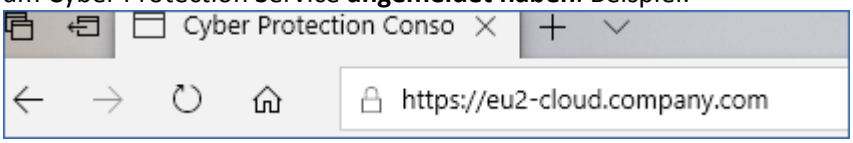
  - **`{-C|--rain=}`**<Service-Adresse>

    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 (S. 59)'.

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. Es wird nicht empfohlen, 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
```

8.5.2.2 Unbeaufsichtigte Installation oder Deinstallation unter macOS

Dieser Abschnitt beschreibt, wie Sie den Acronis Cyber Protection Agenten auf einer unter macOS laufenden Maschine und mithilfe der Befehlszeile im unbeaufsichtigten Modus installieren, registrieren und deinstallieren können. Informationen darüber, wie Sie die Installationsdatei (.dmg) herunterladen können, finden Sie im Abschnitt 'Eine unter macOS laufende Maschine hinzufügen'.

So können Sie den Agenten für Mac installieren

1. Erstellen Sie ein temporäres Verzeichnis, wo Sie die Installationsdatei (.dmg) mounten werden.

   ```
   mkdir <dmg_root>
   ```

   Wobei `<dmg_root>` ein Name Ihrer Wahl ist.
2. Mounten Sie die .dmg-Datei.

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

   Wobei `<dmg_file>` der Name der Installationsdatei ist. Beispiel: **AcronisAgentMspMacOSX64.dmg**.
3. Starten Sie den Installer.

   ```
   sudo installer -pkg <dmg_root>/Install.pkg -target LocalSystem
   ```
4. Trennen Sie die Installationsdatei (.dmg).

   ```
   hdiutil detach <dmg_root>
   ```

Beispiele

```
mkdir mydirectory

hdiutil attach /Users/JohnDoe/AcronisAgentMspMacOSX64.dmg -mountpoint mydirectory

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

hdiutil detach mydirectory
```

So können Sie den Agenten für Mac registrieren

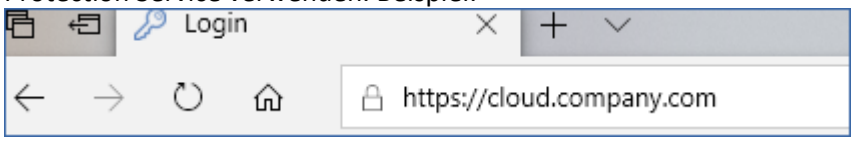
Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:

- Registrieren Sie den Agenten mit einem Benutzernamen und Kennwort unter einem bestimmten Konto.

  ```
  sudo
  /Library/Application\ Support/BackupClient/Acronis/RegisterAgentTool/RegisterAg
  ent -a <Cyber Protection Service-Adresse> -t cloud -u <Benutzername> -p <Kennwort>
  -o register
  ```

  Wobei:

  `<Cyber Protection Service-Adresse>` die Adresse ist, die Sie zum **Anmelden** am Cyber Protection Service verwenden. Beispiel:

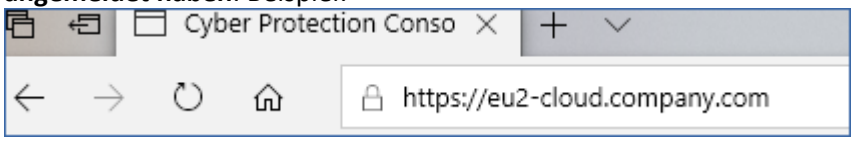
  `<Benutzername>` und `<Kennwort>` die Anmeldedaten für das Konto sind, unter dem der Agent registriert wird. Dies darf kein Partner-Administrator-Konto sein.

- Registrieren Sie den Agenten mit einem Registrierungstoken.

  ```
  sudo
  /Library/Application\ Support/BackupClient/Acronis/RegisterAgentTool/RegisterAg
  ent -a <Cyber Protection Service-Adresse> -t cloud -o register --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 Protection Webkonsole generieren, wie im Abschnitt 'Agenten per Gruppenrichtlinie bereitstellen' erläutert.

  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**. Beispiel:

Beispiele

Registrierung mit einem Benutzernamen und Kennwort.

```
sudo
/Library/Application\ Support/BackupClient/Acronis/RegisterAgentTool/RegisterAg
ent -a https://cloud.company.com -t cloud -u maxmustermann -p maxmustermannskennwort
-o register
```

Registrierung mit einem Token.

```
sudo
/Library/Application\ Support/BackupClient/Acronis/RegisterAgentTool/RegisterAg
ent -a https://eu2-cloud company.com -t cloud o -register --token D91D-DC46-4F0B
```

***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 den Agenten für Mac deinstallieren

Führen Sie folgenden Befehl aus:

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

Führen Sie folgenden Befehl aus, um alle Protokolle, Tasks und Konfigurationseinstellungen während der Deinstallation zu entfernen:

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

8.6 Maschinen manuell registrieren

Neben der Möglichkeit, eine Maschine direkt während der Agenten-Installation im Cyber Protection Service zu registrieren, können Sie dies auch über die Befehlszeilenschnittstelle tun. Dies kann angebracht sein, wenn Sie den Agenten installiert haben, die automatische Registrierung jedoch fehlgeschlagen ist – oder, wenn Sie eine vorhandene Maschine unter einem neuen Konto registrieren wollen.

So können Sie eine Maschine registrieren

Führen Sie folgenden Befehl aus, um eine Maschine mithilfe von Anmeldedaten (Benutzername, Kennwort) zu registrieren:

Unter Windows:

Befehl, um eine Maschine unter dem aktuellen Konto zu registrieren:

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -s mms
-t cloud --update
```

Befehlsvorlage, um eine Maschine unter einem anderen Konto zu registrieren:

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

Befehlsbeispiel:

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

Unter Linux:

Befehl, um eine Maschine unter dem aktuellen Konto zu registrieren:

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -s mms -t cloud
--update
```

Befehlsvorlage, um eine Maschine unter einem anderen Konto zu registrieren:

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

Befehlsbeispiel:

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

Unter macOS:

Befehl, um eine Maschine unter dem aktuellen Konto zu registrieren:

```
sudo "/Library/Application
Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent" -o register -s mms -t
cloud --update
```

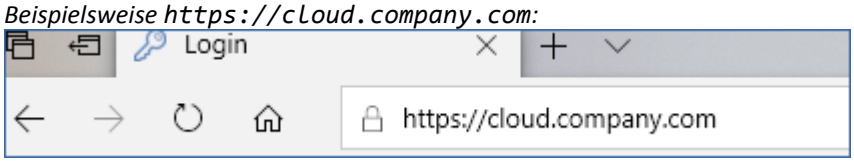
Befehlsvorlage, um eine Maschine unter einem anderen Konto zu registrieren:

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

Befehlsbeispiel:

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

***Hinweis**: Verwenden Sie die Anmeldedaten (Benutzername, Kennwort) für das spezielle Konto, unter dem der Agent registriert wird. Dies darf kein Partner-Administrator-Konto sein.*
*Die Service-Adresse ist die URL, die Sie verwenden, um sich am Cyber Protection Service **anzumelden**.*
Beispielsweise `https://cloud.company.com`:



Alternativ können Sie eine Maschine auch mithilfe eines Registrierungstokens registrieren. Führen Sie dafür folgenden Befehl aus:

Unter Windows:

Befehlsvorlage:

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

Befehlsbeispiel:

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

Unter Linux:

Befehlsvorlage:

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

Befehlsbeispiel:

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

Unter macOS:

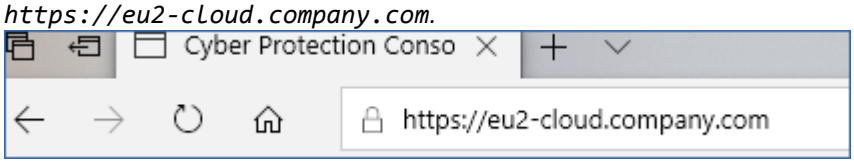
Befehlsvorlage:

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

Befehlsbeispiel:

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

***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 darüber, wie Sie dieses generieren können, finden Sie im Abschnitt 'Agenten per Gruppenrichtlinie bereitstellen (S. 84)'.

So können Sie die Registrierung einer Maschine aufheben

Führen Sie folgenden Befehl aus:

Unter Windows:

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

Unter Linux:

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

Unter macOS:

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

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:

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

Wenn Sie weiterhin eine Fehlermeldung erhalten:

- Codieren Sie Ihr Kennwort im Base64-Format unter https://www.base64encode.org/ (https://www.base64encode.org - https://www.base64encode.org).
- Spezifizieren Sie 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:

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

8.7 Automatische Erkennung von Maschinen

Mit der Funktionalität zur Erkennung von Maschinen können Sie Folgendes tun:

- Den Prozess der Installation des Protection Agenten und der Maschinenregistrierung zu automatisieren, indem Sie die Maschinen in Ihrer Active Directory (AD)-Domain oder im lokalen Netzwerk automatisch ermitteln lassen.
- Den Protection Agenten auf einer ganzen Reihe von Maschinen zu installieren oder zu aktualisieren.
- Verwenden Sie die Synchronisierung mit dem Active Directory, um den Aufwand und die Kosten für die Ressourcen-Bereitstellung und die Maschinen-Verwaltung in einer großen AD-Umgebung zu senken.

***Wichtig**: Die Erkennung von Maschinen kann nur von Agenten durchgeführt werden, die auf Windows-Maschinen installiert sind. Derzeit ist nicht nur die Erkennung durch den Discovery Agenten auf Windows-Maschinen beschränkt, sondern auch die Remote-Installation von Software ist nur auf Windows-Maschinen möglich.*
*Wenn es keine Maschine mit installiertem Agenten gibt, wird die automatische Erkennungsfunktion ausgeblendet – der Bereich **Mehrere Geräte** wird im Assistenten 'Neues Laufwerk hinzufügen' also verborgen.*

Nachdem Maschinen zur Service-Konsole hinzugefügt wurden, werden diese folgendermaßen kategorisiert:

- **Erkannt** – Maschinen, die erkannt wurden, auf denen jedoch noch kein Protection Agent installiert ist.
- **Verwaltet** – Maschinen, auf denen der 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 der Schutzplan angewendet wurde.

Und so funktioniert es

Beim Scannen des lokalen Netzwerks verwendet der Discovery Agent folgende Technologien: NetBIOS-Erkennung, WSD (Web Service Discovery) und die ARP-Tabelle (Address Resolution Protocol). Der Agent versucht, folgende Parameter von jeder Maschine abzurufen:

- 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)

Wenn das AD-Scanning durchgeführt wird, versucht der Agent, fast die gleichen Parameter wie oben aufgelistet von jeder Maschine abzurufen. Der Unterschied besteht darin, dass es zusätzlich den Parameter für die Organisationseinheit (OE) sowie umfassendere Informationen über den Namen und das Betriebssystem abruft, aber keine Informationen über die IP- und MAC-Adresse.

Voraussetzungen

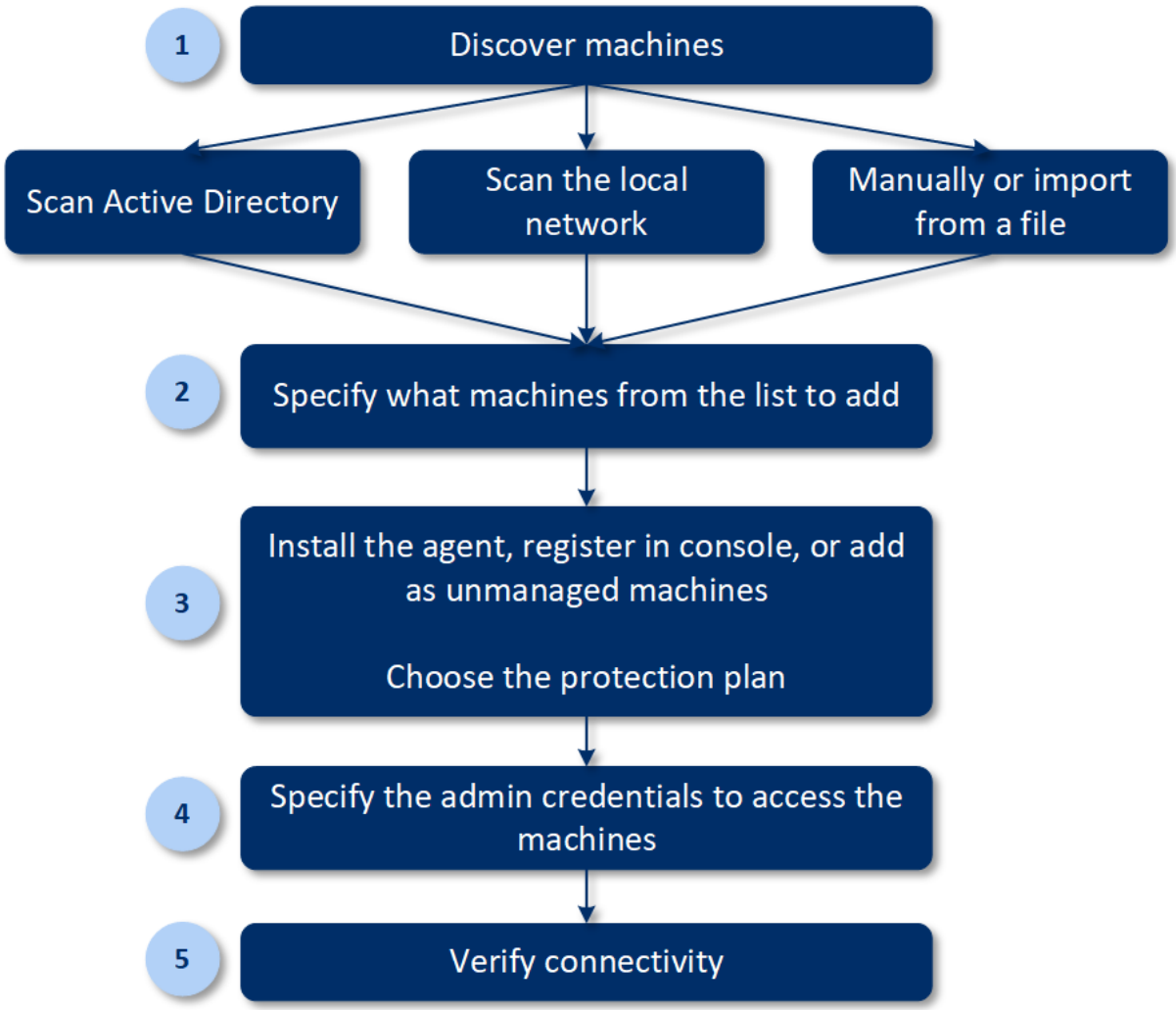
Sie müssen vor der Erkennung der Maschinen den Protection Agenten auf mindestens einer Maschine in ihrem lokalen Netzwerk installiert haben, um ihn als Discovery Agenten verwenden zu können.

Wenn Sie Maschinen in der Active Directory-Domain erkennen wollen, müssen Sie den Agenten auf mindestens einer Maschine in der AD-Domain installiert haben. Dieser Agent wird dann als Discovery Agent zum Scannen des Active Directorys verwendet.

Auf einer Maschine mit Windows Server 2012 R2 muss das Udpate KB2999226 installiert sein, damit ein Protection Agent remote installiert werden kann.

Der Prozess der Maschinen-Erkennung

Das folgende Schema verdeutlicht die Hauptschritte des Maschinen-Erkennungsprozesses:



Der komplette Prozess der automatischen Erkennung besteht grundsätzlich aus den folgenden Schritten:

1. Die Methode zur Erkennung der Maschinen auswählen:
   - Durch Scannen des Active Directorys
   - Durch Scannen des lokalen Netzwerks
   - Manuell – eine Maschine wird anhand der IP-Adresse oder des Host-Namens hinzugefügt oder eine Liste der Maschinen wird aus einer Datei importiert
2. Wählen Sie die hinzuzufügenden Maschinen aus der Liste aus, die Sie als Ergebnis des vorherigen Schrittes erhalten haben.
3. Bestimmen Sie, wie die Maschinen hinzugefügt werden sollen:
   - Der Protection Agent und weitere Komponenten werden auf den Maschinen installiert und diese werden außerdem in der Service-Konsole registriert.
   - Die Maschinen werden in der Service-Konsole registriert (falls der Agent bereits auf ihnen installiert ist).
   - Die Maschinen werden der Service-Konsole als **Unverwaltete Maschinen** hinzugefügt, ohne die Installation eines Agenten oder einer Komponente.

   Wenn Sie eine der ersten beiden Methoden zum Hinzufügen einer Maschine ausgewählt haben, können Sie auch den Schutzplan aus den vorhandenen auswählen und auf die entsprechenden Maschinen anwenden.
4. Geben Sie die Anmeldedaten eines Benutzers an, der über administrative Berechtigungen zur Verwaltung der Maschinen verfügt.
5. Überprüfen Sie mithilfe der bereitgestellten Anmeldedaten, dass eine Verbindung mit den Maschinen möglich ist.

In den nächsten Abschnitten erhalten Sie genauere Informationen über die Erkennungsprozedur.

8.7.1 Automatische und manuelle Erkennung

Stellen Sie vor dem Start der Erkennung sicher, dass die Voraussetzungen (S. 62) erfüllt sind.

So können Sie Maschinen erkennen

1. Gehen Sie in der Service-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. [Wenn die Erkennungsmethode 'Active Directory' oder 'Lokales Netzwerk' ausgewählt wurde] Verwenden Sie eine Liste, um die Maschinen auszuwählen, die Sie hinzufügen wollen.

   [Wenn die manuelle Erkennungsmethode ausgewählt wurde] 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:

   - **Agenten installieren und Maschinen registrieren**. Wenn Sie auf den Befehl **Komponenten auswählen** klicken, können Sie festlegen, welche Komponenten auf den Maschinen installiert werden sollen. Weitere Informationen dazu finden Sie im Abschnitt 'Zu installierende Komponenten auswählen'.

     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.

     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**. Diese Option wird verwendet, 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 die Maschinen mit der Kennzeichnung **Nicht verwaltet** hinzugefügt.

- **Als nicht verwaltete Maschinen hinzufügen**. Der Agent wird nicht auf den Maschinen installiert. Sie können sich die Maschinen in der Konsole anzeigen lassen und den Agenten später installieren oder registrieren.

[Wenn als 'Aktion nach Erkennung' die Option **Agenten installieren und Maschinen registrieren** ausgewählt wurde] **Maschine bei Bedarf neu starten** – wenn diese Option aktiviert ist, wird die Maschine (so oft wie notwendig) neu gestartet, um die Installation abzuschließen.

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.

[Wenn die Option **Maschine bei Bedarf neu starten** ausgewählt wurde] **Nicht neu starten, wenn Benutzer angemeldet ist** – wenn diese Option aktiviert ist, wird die Maschine nicht automatisch neu gestartet, wenn der Benutzer am System angemeldet ist. Wenn ein Benutzer auf der Maschine arbeitet, während die Installation einen Neustart einfordert, wird das System nicht neu gestartet.

Wenn die Vorgaben installiert wurden und kein Neustart durchgeführt wurde, weil ein Benutzer angemeldet war, müssen Sie die Maschine manuell neu starten und die Installation erneut starten, damit die Installation des Agenten fertiggestellt werden kann.

Wenn der Agent installiert wurde, aber anschließend kein Neustart erfolgte, müssen Sie die Maschine manuell neu starten.

[Wenn es Einheiten/Abteilungen in Ihrer Organisation gibt] **Benutzer, für den die Maschinen registriert werden sollen** – wählen Sie den Benutzer Ihrer Einheit oder Untereinheit aus, für den die Maschinen registriert werden sollen.

Wenn Sie eine der ersten beiden 'Aktionen nach der Entdeckung' ausgewählt haben, gibt es außerdem die Möglichkeit, einen Schutzplan auf die Maschinen anzuwenden. Wenn Sie mehrere Schutzpläne haben, können Sie auswählen, welchen Sie verwenden wollen.

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 die Anmeldedaten eines benutzerdefinierte Administrators definieren wollen, müssen Sie zusätzliche manuelle Vorbereitungen durchführen (wie im unteren Abschnitt 'Remote-Installation eines Agenten für einen benutzerdefinierten Administrator ermöglichen' beschrieben).*

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 **Dashboard** –> **Aktivitäten** –> **Maschinen erkennen** finden.

Remote-Installation eines Agenten für einen benutzerdefinierten Administrator ermöglichen

Wenn Sie die Anmeldedaten eines benutzerdefinierte Administrators definieren wollen, um einen Agenten remote installieren zu können, müssen Sie zusätzliche manuelle Vorbereitungen durchführen:

1. Damit die Installation auf einer Remote-Maschine mit Windows XP erfolgreich ist, muss die Option **Systemsteuerung –> Ordneroptionen –> Ansicht –> Einfache Dateifreigabe verwenden** auf dieser Maschine *deaktiviert* sein.

   Damit die Installation auf einer Remote-Maschine mit Windows Vista (oder höher) erfolgreich ist, muss die Option **Systemsteuerung –> Ordneroptionen –> Ansicht –> Freigabe-Assistent verwenden (empfohlen)** auf dieser Maschine *deaktiviert* sein.
2. Zur erfolgreichen Installation auf einer Remote-Maschine, die *kein* Mitglied einer Active Directory-Domain ist, muss die Benutzerkontensteuerung (UAC) *deaktiviert sein*.
3. Auf der Remote-Maschine muss die Datei- und Druckerfreigabe *aktiviert* sein. So erhalten Sie Zugriff auf diese Option:
   - Auf einer Maschine, die unter Windows XP oder Windows 2003 Server läuft: gehen Sie zu **Systemsteuerung –> Windows-Firewall –> Ausnahmen –> Datei- und Druckerfreigabe**.
   - Auf einer Maschine, die unter Windows Vista, Windows Server 2008, Windows 7 oder neuer läuft: gehen Sie zu **Systemsteuerung –> Windows-Firewall –> Netzwerk- und Freigabecenter –> Erweiterte Freigabeeinstellungen ändern**.
4. 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.

ODER

Nehmen Sie folgenden Eintrag in den Registry-Schlüssel HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System auf: ein DWORD-Wert (32 Bit) mit 'LocalAccountTokenFilterPolicy = 1'

8.7.1.1 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 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 Office 365	Dieser Agent sichert Microsoft Office 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.
Befehlszeilenwerkzeug	Cyber Protection bietet eine Befehlszeilenschnittstelle über das Utility 'acrocmd'. acrocmd enthält jedoch keine Tools, die die Befehle physisch selbst ausführen würden. Es stellt lediglich eine Befehlszeilenschnittstelle zu den entsprechenden Komponenten von Cyber Protection bereit – den Agenten und dem Management Server. Er wird installiert, sofern er ausgewählt wurde.

8.7.2 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.

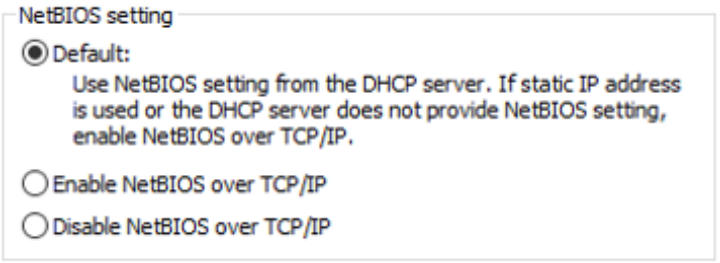
Diese Maschinen werden nach der Installation des Protection Agenten im Bereich **Geräte** –> **Maschinen mit Agenten** angezeigt.

Um Ihren Status zu überprüfen, gehen Sie zu **Dashboard** –> **Überblick** und fügen Sie dann das Widget **Sicherungsstatus** (S. 417) oder das Widget **Erkannte Maschinen** (S. 417) hinzu.

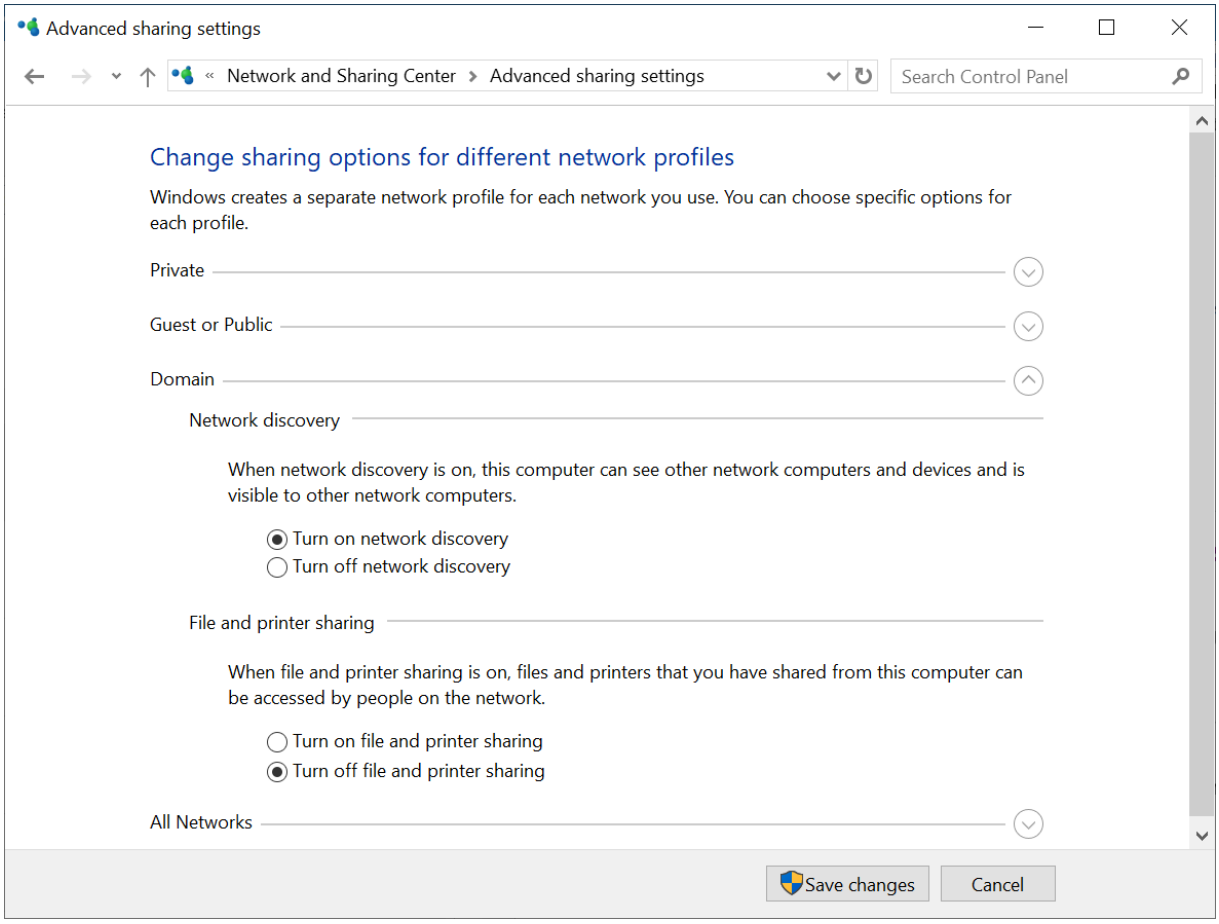
8.7.3 Problembehebung (Troubleshooting)

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.

8.8 Den Agenten für VMware (Virtuelle Appliance) von einer OVF-Vorlage aus bereitstellen

8.8.1 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. Wir empfehlen, diese Ressourcen auf 8 GB RAM und 4 vCPUs zu erhöhen, wenn die Bandbreite der Backup-Übertragungen voraussichtlich 100 MB/Sek. übersteigt (z.B. in 10-Gigabit-Netzwerken), um die Backup-Performance zu verbessern.

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'.

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**.

8.8.2 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.

8.8.3 Die virtuelle Appliance konfigurieren

1. **Die virtuelle Appliance starten**

   Lassen Sie im vSphere-Client die **Bestandsliste** (Inventory) anzeigen, klicken Sie mit der rechten Maustaste auf den Namen der virtuellen Appliance und wählen Sie dann **Einschalten** (Power on). Wählen Sie die Registerlasche '**Konsole**'.
2. **Proxy-Server**

   Falls in Ihrem Netzwerk ein Proxy-Server verwendet wird:

a. Drücken Sie zum Starten der Eingabeaufforderung die Tastenkombination Strg+Umschalt+F2, während Sie sich in der Benutzeroberfläche der virtuellen Appliance befinden.
b. Öffnen Sie die Datei **/etc/Acronis/Global.config** in einem Text-Editor.
c. Suchen Sie den folgenden Abschnitt:

```
<key name="HttpProxy">
    <value name="Enabled" type="Tdword">"0"</value>
    <value name="Host" type="TString">"ADRESSE"</value>
    <value name="Port" type="Tdword">"PORT"</value>
    <value name="Login" type="TString">"ANMELDENAME"</value>
    <value name="Password" type="TString">"KENNWORT"</value>
</key>
```

d. Ersetzen Sie **0** durch **1**.
e. Ersetzen Sie ADRESSE mit dem Host-Namen/der IP-Adresse des neuen Proxy-Servers – und PORT mit dem Dezimalwert der dazugehörigen Port-Nummer.
f. Wenn Ihr Proxy-Server eine Authentifizierung benötigt, ersetzen Sie ANMELDENAME und KENNWORT mit den entsprechenden Anmeldedaten des Proxy-Servers. Anderenfalls können Sie diese Zeilen aus der Datei löschen.
g. Speichern Sie die Datei.
h. Führen Sie den Befehl **reboot** aus.

Ansonsten können Sie diesen Schritt überspringen.

3. **Netzwerkeinstellungen**

   Die Netzwerkverbindung des Agenten wird automatisch per DHCP (Dynamic Host Configuration Protocol) konfiguriert. Zur Änderung der Standardkonfiguration klicken Sie unter **Agentenoptionen** bei **eth0** auf **Ändern** und spezifizieren die gewünschten Netzwerkeinstellungen.

4. **vCenter/ESX(i)**

   Klicken Sie unter **Agentenoptionen**, in **vCenter/ESX(i)**, auf **Ändern** und spezifizieren Sie den Namen oder die IP-Adresse des vCenter-Servers. Der Agent kann daraufhin Backup- und Recovery-Aktionen mit jeder vom vCenter-Server verwalteten virtuellen Maschine durchführen.

   Falls Sie keinen vCenter-Server verwenden, dann spezifizieren Sie den Namen oder die IP-Adresse desjenigen ESXi-Hosts, dessen virtuelle Maschinen Sie sichern und wiederherstellen wollen. Normalerweise laufen Backups schneller ab, wenn der Agent solche virtuelle Maschinen sichert, die von seinem eigenen Host gehostet werden.

   Spezifizieren Sie die Anmeldedaten, die der Agent verwendet, um sich mit dem vCenter-Server oder ESXi zu verbinden. Wir empfehlen, dass Sie ein Konto verwenden, dem die Rolle **Administrator** zugewiesen ist. Alternativ können Sie auch ein Konto angeben, welches über die notwendigen Berechtigungen (S. 312) auf dem vCenter Server oder ESXi-Host verfügt.

   Sie können auf **Verbindung prüfen** klicken, um sicherzustellen, dass die Anmeldedaten korrekt sind.

5. **Management Server**
   a. Klicken Sie bei **Agent-Optionen** im **Management Server** auf den Befehl **Ändern**.
   b. Wählen Sie bei **Server-Name/IP** die Option **Cloud**. Die Software zeigt die Adresse des Cyber Protection Service an. Ändern Sie diese Adresse nicht, solange es keine anderslautenden Anweisungen gibt.
   c. Spezifizieren Sie unter **Benutzername** und **Kennwort** die Anmeldedaten für den Cyber Protection Service. Der Agent und die virtuellen Maschinen, die der Agent verwaltet, werden unter diesem Konto registriert.

6. **Zeitzone**

   Klicken Sie im Bereich **Zeitzone** unter **Virtuelle Maschine** auf **Ändern**. Stellen Sie durch die Auswahl Ihres Standortes sicher, dass alle geplanten Aktionen zur korrekten Zeit ausgeführt werden.

7. **[Optional] Lokale Storages**

   Sie können an die virtuelle Appliance ein zusätzliches Laufwerk anschließen, sodass der Agent für VMware seine Backups zu diesem lokal angeschlossenen Storage durchführen kann.

   Fügen Sie das Laufwerk hinzu, indem Sie die Einstellungen der virtuellen Maschine bearbeiten und dann auf '**Aktualisieren** klicken. Darauf wird der Link **Storage erstellen** verfügbar. Klicken Sie auf den Link, wählen Sie das Laufwerk und spezifizieren Sie eine Bezeichnung für dieses.

8.9 Den Agenten für die Virtuozzo Infrastructure Platform (Virtuelle Appliance) aus einer QCOW2-Vorlage bereitstellen

8.9.1 Bevor Sie beginnen

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

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. Wir empfehlen, diese Ressourcen auf 4 vCPUs und 8 GB RAM zu erhöhen, wenn die Bandbreite des Backup-Datenverkehrs voraussichtlich 100 MB/Sek. übersteigt (z.B. in 10-Gigabit-Netzwerken), um die Backup-Performance zu verbessern.

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 gleiche 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 beispielsweise kommen, wenn eine Maschine oder ein Agent hinzugefügt oder entfernt wird. 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 verteilt. Dies geschieht jedoch nicht, wenn ein Agent beschädigt wird oder manuell aus dem Virtuozzo Infrastructure Platform-Knoten gelöscht wird. Eine Neuverteilung wird in

diesem Fall nur dann gestartet, wenn Sie einen solchen Agenten über die Cyber Protection-Weboberfläche entfernen.

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 über **Einstellungen** –> **Agenten** ausgewählt wurde

Einschränkungen

- Die Virtuozzo Infrastructure Platform-Appliance kann nicht remote bereitgestellt werden.
- Applikationskonforme Backups von virtuellen Maschinen werden nicht unterstützt.

8.9.2 Netzwerke in Virtuozzo Infrastructure Platform konfigurieren

Bevor Sie die virtuelle Appliance bereitstellen und konfigurieren können, müssen Sie Ihre Netzwerke in Virtuozzo Infrastructure Platform konfiguriert haben. Es gibt zwei Arten von Netzwerken: die physischen (im Bereich **Infrastruktur** –> **Netzwerke**) und die virtuellen (im Bereich **Compute** –> **Netzwerke**).

Die Grundkonfiguration besteht aus nur einem physischen Netzwerk. Empfohlene Konfigurationen bestehen aus zwei oder mehr physischen Netzwerken und, daraus folgend, zwei oder mehr virtuellen Netzwerken.

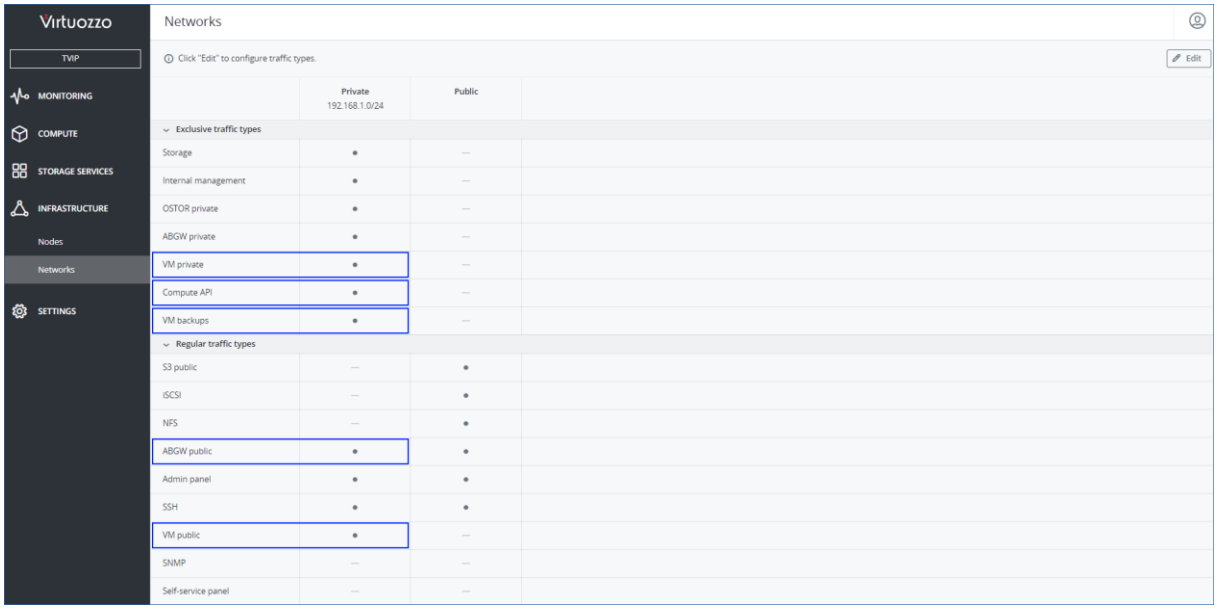
Grundkonfiguration

1. Physisches Netzwerk

   Sie haben standardmäßig im Bereich **Infrastruktur** –> **Netzwerke** zwei automatisch erstellte Netzwerkvorlagen: **Privat** und **Öffentlich**. Das Netzwerk **Privat** ist darauf ausgelegt, ein sicheres oder isoliertes Netzwerk zu sein, welches sich hinter einer Firewall befindet und auf das kein direkter Zugriff aus dem Internet möglich ist.

   Für diese Grundkonfiguration müssen Sie sicherstellen, dass diesem Netzwerk die Traffic-Typen **VM privat**, **Compute-API**, **VM-Backups, ABGW öffentlich** und **VM öffentlich** zugewiesen wurden.

Weitere Informationen über die Netzwerke finden Sie unter 'Managing Networks and Traffic Types' in der (englischsprachigen) Virtuozzo Infrastructure Platform-Dokumentation.

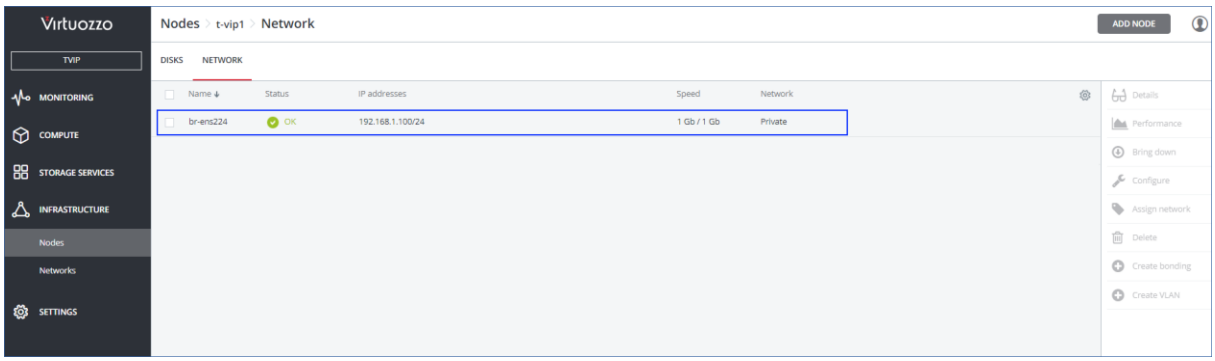


2. Netzwerkschnittstellen der Knoten

   Stellen Sie sicher, dass den Netzwerkschnittstellen aller Knoten im Cluster eine IP-Adresse zugewiesen wurde. Diese Adressen hängen von Ihrer gegenwärtigen Netzwerkinfrastruktur ab.

   Stellen Sie dann sicher, dass das physische Netzwerk, welches Sie in Schritt 1 konfiguriert haben, ebenfalls den Netzwerkschnittstellen zugewiesen wurde.

   Weitere Informationen über die Netzwerkschnittstellen finden Sie unter 'Configuring Node Network Interfaces' in der (englischsprachigen) Virtuozzo Infrastructure Platform-Dokumentation.



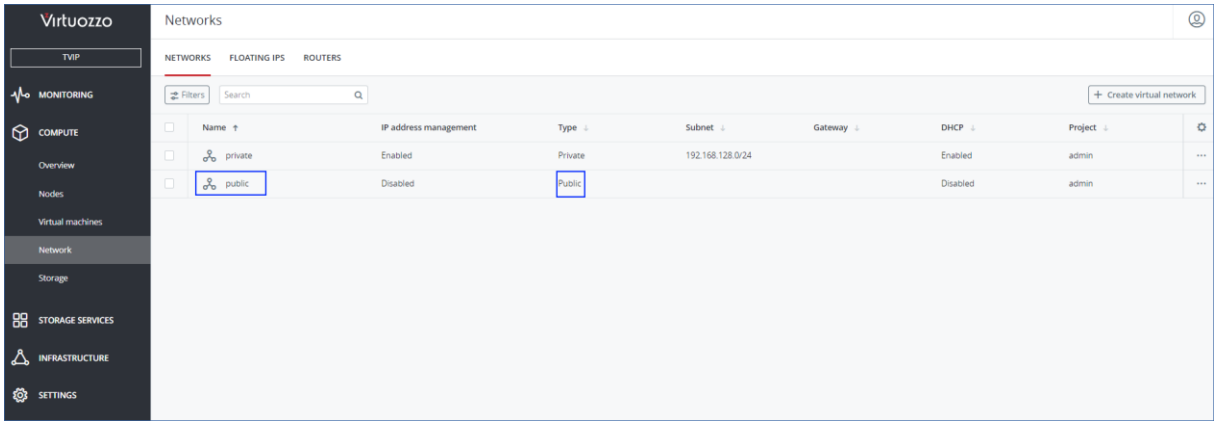
3. Virtuelles Netzwerk

   Sie haben standardmäßig im Bereich **Compute** –> **Netzwerke** zwei automatisch erstellte Netzwerke namens **privat** und **öffentlich**. Diese haben den Typ *privat* bzw. *öffentlich*. Sie können diese verwenden oder Ihre eigenen virtuellen Netzwerke erstellen.

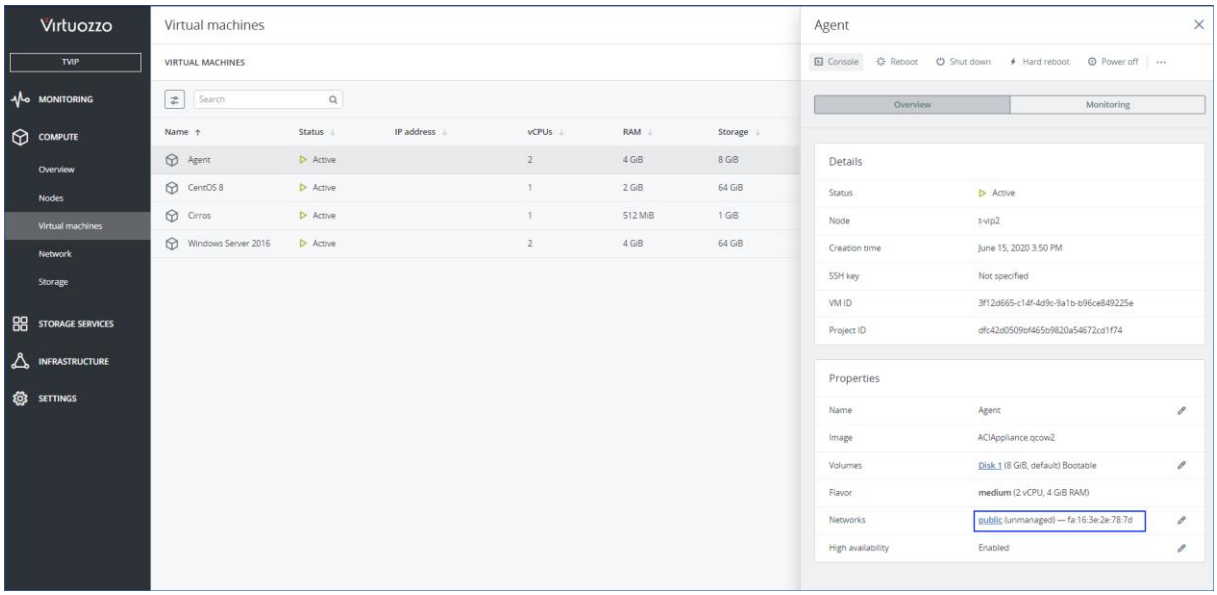
   Für diese Konfiguration benötigen Sie ein virtuelles Netzwerk vom Typ *öffentlich*. Es muss über (im Sinne von 'oberhalb') dem physischen Netzwerk erstellt werden, das Sie in Schritt 1 konfiguriert haben.

***Hinweis**: Nur virtuelle Netzwerke vom Typ 'öffentlich' können über ein physischen Netzwerken erstellt werden. Physischen Netzwerken muss der Traffic-Typ 'VM öffentlich' zugewiesen werden.*

Weitere Informationen darüber, wie Sie ein virtuelles Netzwerk erstellen und konfigurieren können, finden Sie im Abschnitt 'Managing Compute Network' der (englischsprachigen) Virtuozzo Infrastructure Platform-Dokumentation.



Wenn Sie die virtuelle Maschine der Appliance bereitstellen, müssen Sie dieses virtuelle Netzwerk auswählen.



Empfohlene Konfiguration mit zwei oder mehr physischen Netzwerken

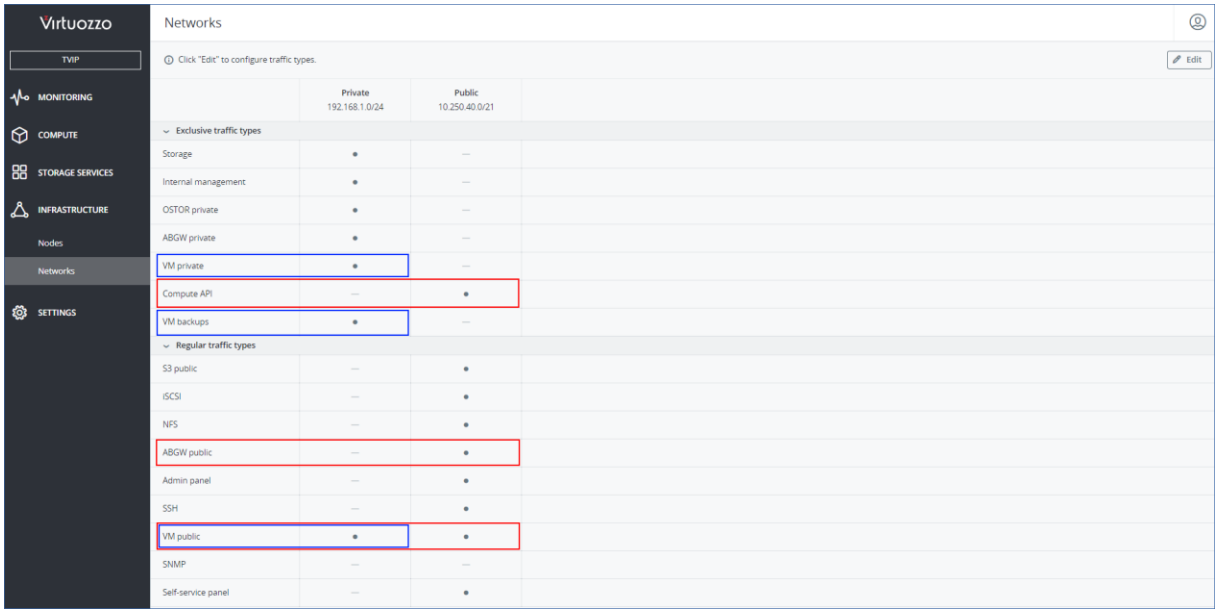
1. Physische Netzwerke

   Bei dieser Konfiguration benötigen Sie zwei oder mehr Netzwerke. Sie haben standardmäßig im Bereich **Infrastruktur** –> **Netzwerke** zwei automatisch erstellte Netzwerke: **Privat** und **Öffentlich**. Sie können diese verwenden oder Ihre eigenen Netzwerke erstellen. Beispielsweise können Sie ein drittes Netzwerk nur für den Storage-Traffic verwenden. Das Netzwerk **Privat** ist darauf ausgelegt, ein sicheres oder isoliertes Netzwerk zu sein, welches sich hinter einer Firewall befindet und auf das kein direkter Zugriff aus dem Internet möglich ist.

   Folgende Voraussetzungen müssen erfüllt sein:

   - Die Traffic-Typen **VM privat, VM-Backups** und **VM öffentlich** wurden dem Netzwerk **Privat** zugewiesen.
   - Die Traffic-Typen **Compute-API**, **ABGW öffentlich** und **VM öffentlich** wurden dem Netzwerk **Öffentlich** zugewiesen.
   - Die anderen Traffic-Typen können je nach Ihren Bedürfnissen verteilt sein.

Weitere Informationen über die Netzwerke finden Sie unter 'Managing Networks and Traffic Types' in der (englischsprachigen) Virtuozzo Infrastructure Platform-Dokumentation.

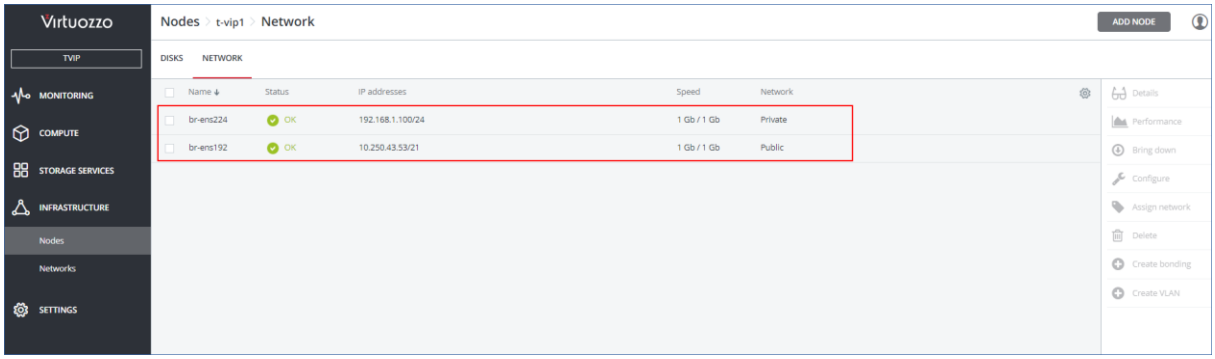


2. Netzwerkschnittstellen der Knoten

   Stellen Sie sicher, dass den Netzwerkschnittstellen aller Knoten im Cluster IP-Adressen zugewiesen wurden. Diese Adressen hängen von Ihrer gegenwärtigen Netzwerkinfrastruktur ab. Sie können die Netzwerkschnittstellen im Bereich **Infrastruktur** –> **Knoten** –> **Netzwerk** konfigurieren.

   Stellen Sie dann sicher, dass die physischen Netzwerke, welche Sie in Schritt 1 konfiguriert haben, ebenfalls den Netzwerkschnittstellen zugewiesen wurden. Sie können einer Schnittstelle nur je ein (1) Netzwerk zuweisen. Daher hängt die Anzahl der erforderlichen Schnittstellen für jeden Knoten von der Anzahl der von Ihnen verwendeten Netzwerke ab.

   Weitere Informationen über die Netzwerkschnittstellen finden Sie unter 'Configuring Node Network Interfaces' in der (englischsprachigen) Virtuozzo Infrastructure Platform-Dokumentation.



3. Virtuelle Netzwerke

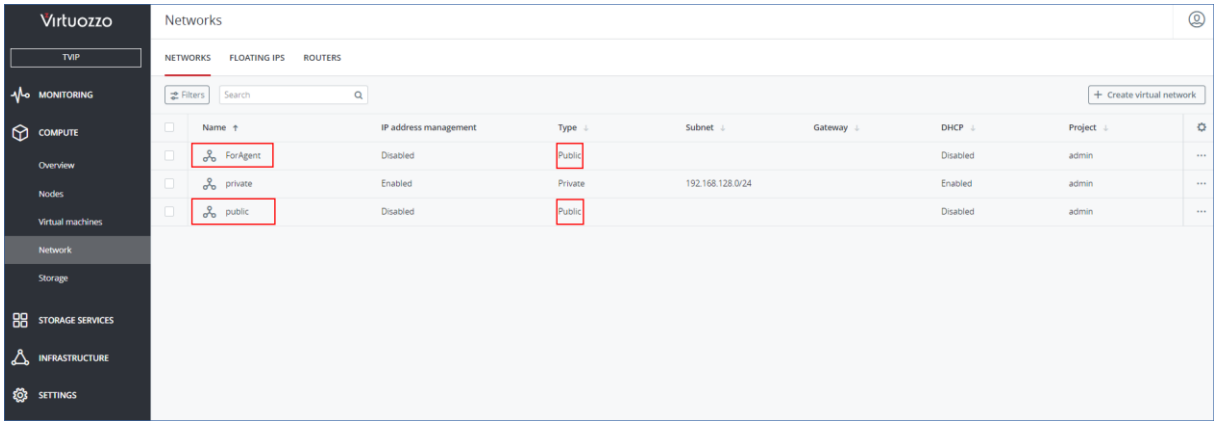
   Sie haben standardmäßig im Bereich **Compute** –> **Netzwerke** zwei automatisch erstellte Netzwerke namens **privat** und **öffentlich**. Diese haben den Typ *privat* bzw. *öffentlich*. Sie können diese verwenden oder Ihre eigenen virtuellen Netzwerke erstellen.

   Für diese Konfiguration benötigen Sie zwei virtuelle Netzwerke vom Typ *öffentlich*.

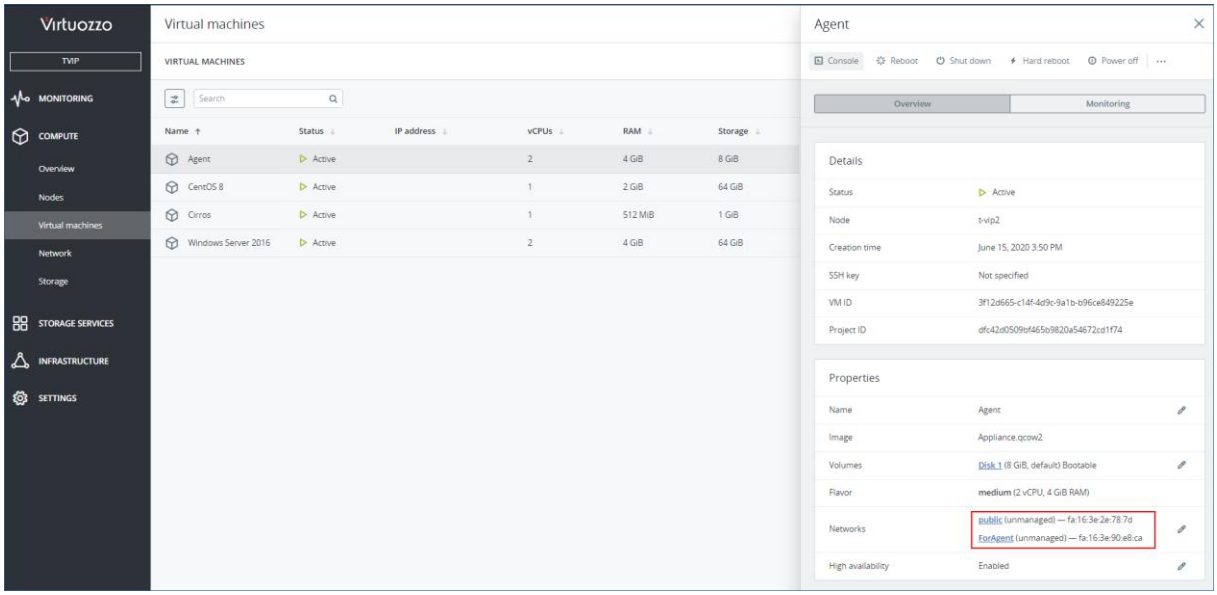
   Stellen Sie sicher, dass die beiden virtuellen Netzwerke vom Typ *öffentlich* über (im Sinne von 'oberhalb') den physischen Netzwerken, die Sie in Schritt 1 erstellt haben, erstellt werden. Wenn Sie weitere physische Netzwerke in Ihrer Konfiguration haben, erstellen Sie entsprechend weitere virtuelle Netzwerke vom Typ *öffentlich*.

***Hinweis**: Nur virtuelle Netzwerke vom Typ 'öffentlich' können über ein physischen Netzwerken erstellt werden. Physischen Netzwerken muss der Traffic-Typ 'VM öffentlich' zugewiesen werden.*

Weitere Informationen darüber, wie Sie ein virtuelles Netzwerk erstellen und konfigurieren können, finden Sie im Abschnitt 'Managing Compute Network' der (englischsprachigen) Virtuozzo Infrastructure Platform-Dokumentation.



Wenn Sie die virtuelle Maschine der Appliance bereitstellen, müssen Sie diese virtuellen Netzwerke auswählen.



8.9.3 Benutzerkonten in Virtuozzo Infrastructure Platform konfigurieren

Um die virtuelle Appliance konfigurieren zu können, benötigen Sie ein Virtuozzo Infrastructure Platform-Benutzerkonto. Dieses Konto muss über die Rolle **Administrator** in der Domain **Default** (Standard) verfügen. Weitere Informationen über Benutzer finden Sie im Abschnitt 'Managing Domain Users' in der englischsprachigen Virtuozzo Infrastructure Platform-Dokumentation. Stellen Sie sicher, dass Sie diesem Konto Zugriff auf alle Projekte in der Domain **Standard** (Default) gewährt haben.

So können Sie Zugriff auf alle Projekte in der Domain 'Default' (Standard) gewähren

Führen Sie das nachfolgende Skript im Virtuozzo Infrastructure Platform-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' der englischsprachigen Virtuozzo Infrastructure Platform-Dokumentation.

```
su - vstoradmin
kolla-ansible post-deploy
exit
. /etc/kolla/admin-openrc.sh
openstack --insecure user set --project admin --project-domain Default --domain Default
<Benutzername>
openstack --insecure role add --domain Default --user <Benutzername> --user-domain
Default compute --inherited
```

Wobei <Benutzername> das Virtuozzo Infrastructure Platform-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 das nachfolgende Skript ausführen.

So können Sie Zugriff auf alle Projekte in einer anderen Domain gewähren

```
su - vstoradmin
kolla-ansible post-deploy
exit
. /etc/kolla/admin-openrc.shopenstack --insecure role add --domain <Domain-Name>
--inherited --user <Benutzername> --user-domain Default admin
```

Wobei <domain name> die Domain für die Projekte ist, in denen das Konto <Benutzername> Zugriff haben wird.

Beispiel

```
su - vstoradmin
kolla-ansible post-deploy
exit. /etc/kolla/admin-openrc.sh
openstack --insecure role add --domain MyNewDomain --inherited --user johndoe
--user-domain Default admin
```

8.9.4 Die QCOW2-Vorlage bereitstellen

1. Melden Sie sich an Ihrem Cyber Protection-Konto an.
2. Klicken Sie auf **Geräte** –> **Alle Geräte** –> **Hinzufügen** –> **Virtuozzo Infrastructure Platform**.
   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 Infrastructure Platform-Konto an.
5. Fügen Sie die .qcow2-Image-Datei folgendermaßen dem Virtuozzo Infrastructure Platform-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. Ein Beispiel für eine mögliche Netzwerkkonfiguration finden Sie hier dokumentiert (englischsprachig): Network configuration in Virtuozzo Infrastructure Platform.
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.

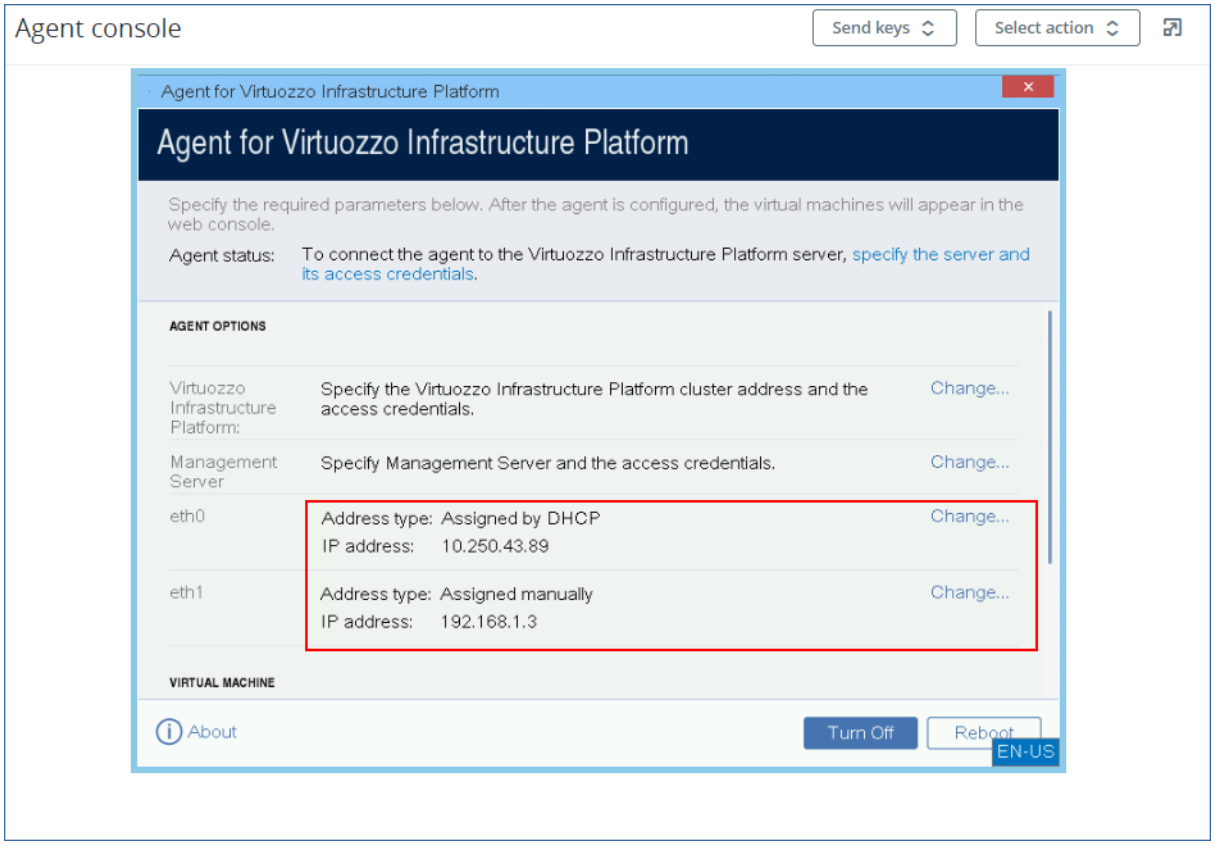
8.9.5 Die virtuelle Appliance konfigurieren

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

So konfigurieren Sie die virtuelle Appliance

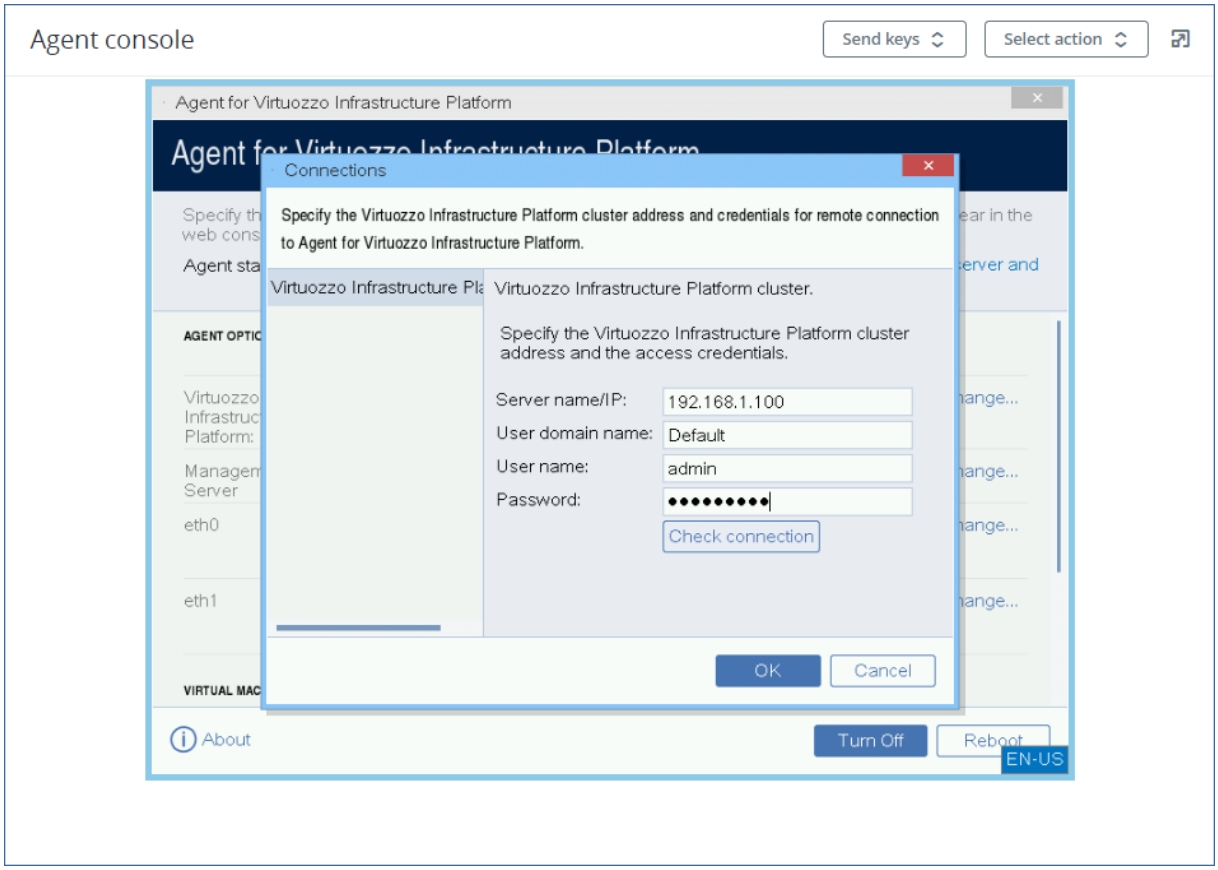
1. Melden Sie sich an Ihrem Virtuozzo Infrastructure Platform-Konto an.
2. Wählen Sie in der Registerkarte **Compute** –> **Virtuelle Maschinen** –> **Virtuelle Maschinen** die von Ihnen erstellte virtuelle Maschine aus. Klicken Sie dann auf **Konsole**.

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.

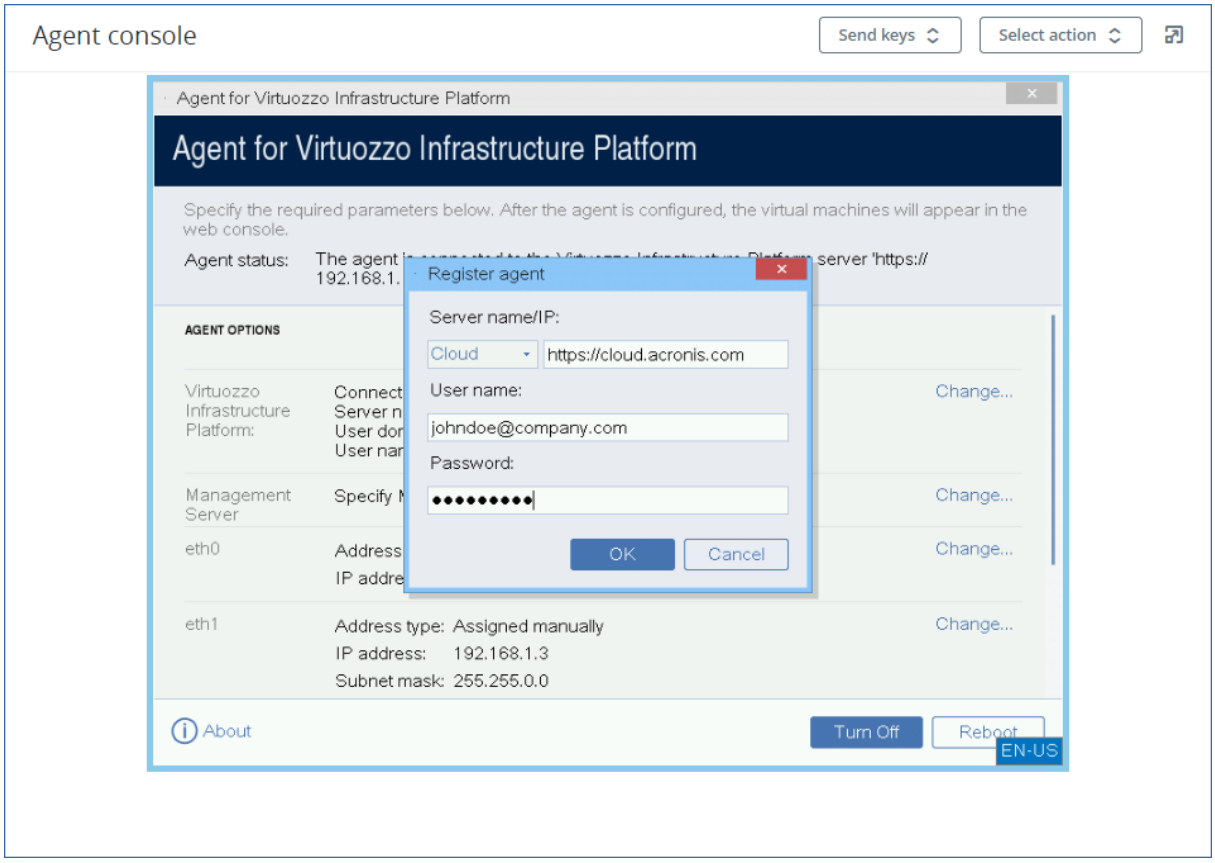


4. Spezifizieren Sie die Adresse und Anmeldedaten des Virtuozzo-Clusters:
   - DNS-Name oder IP-Adresse des Virtuozzo Infrastructure Platform-Clusters – dies ist die Adresse des Management-Knotens des Clusters. Der Standard-Port 5000 wird automatisch festgelegt. Wenn Sie einen anderen Port verwenden wollen, müssen Sie diesen manuell spezifizieren.
   - Spezifizieren Sie im Feld **Benutzer-Domain-Name** Ihre Domain in Virtuozzo Infrastructure Platform. Beispiel: **Standard** (Default).

- Geben Sie in den Feldern **Benutzername** und **Kennwort** die Anmeldedaten eines Virtuozzo Infrastructure Platform-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 Infrastructure Platform konfigurieren (p. 78)'.

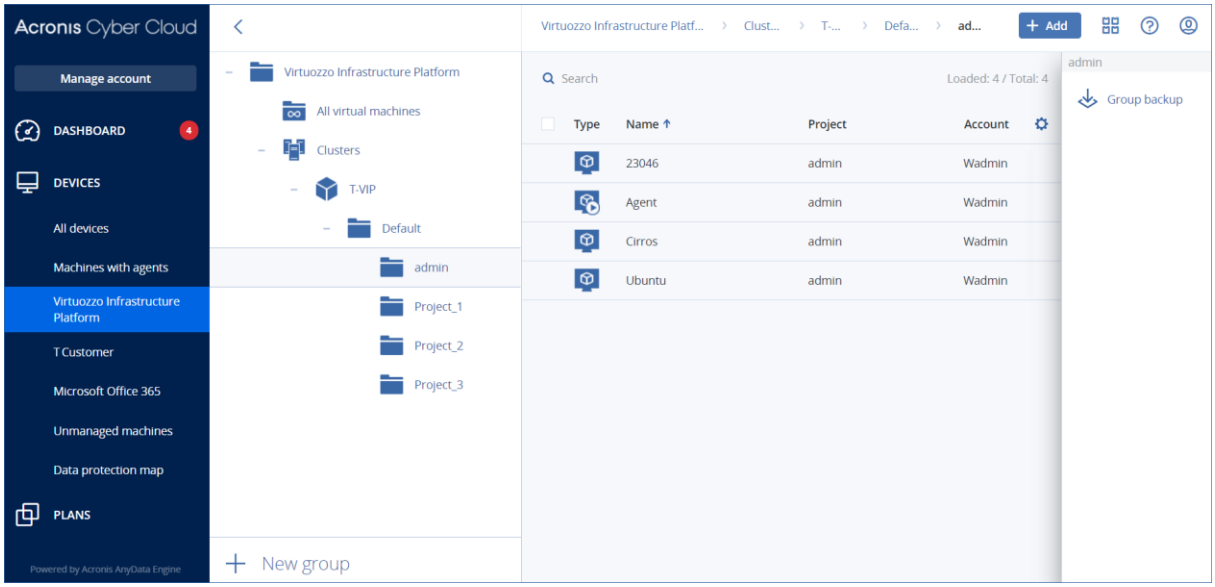


5. Spezifizieren Sie die Adresse und Anmeldedaten des Cyber Protection Management Servers, um auf diese zugreifen zu können.



So können Sie die virtuellen Maschinen im Virtuozzo Infrastructure Platform-Cluster schützen

1. Melden Sie sich an Ihrem Cyber Protection-Konto an.
2. Gehen Sie zu **Geräte** –> **Virtuozo Infrastructure Platform** –> <Ihr Cluster> –> **Standardprojekt** –> **admin** – oder suchen Sie Ihre Maschinen in **Geräte** –> **Alle Geräte**.
3. Wählen Sie die gewünschten Maschinen aus und wenden Sie einen Schutzplan auf diese an.



8.10 Agenten per Gruppenrichtlinie bereitstellen

Sie können den Agenten für Windows durch Verwendung einer 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

Bevor Sie mit dem Deployment des Agenten fortfahren, sollten Sie sicherstellen, dass:

- Sie eine Active Directory-Domain mit einem Domain Controller haben, die unter Microsoft Windows Server 2003 oder später laufen.
- Sie innerhalb der Domain ein Mitglied der Gruppe **Domänen-Admins** Domain sind.
- Sie das Setup-Programm **Alle Agenten für Windows** heruntergeladen haben. Auf der Seite **Geräte hinzufügen** in der Service-Konsole der Download-Link verfügbar ist.

Schritt 1: Ein Registrierungstoken generieren

Ein Registrierungstoken übermittelt Ihre Identität an das Setup-Programm, ohne dass dabei Ihre Anmeldedaten (Anmeldename, Kennwort) für die Service-Konsole gespeichert werden. Dadurch können Sie eine beliebige Anzahl von Maschinen unter Ihrem Konto registrieren. Um mehr Sicherheit zu erreichen, hat ein Token eine begrenzte Lebensdauer.

So können Sie ein Registrierungstoken generieren

1. Melden Sie sich an der Service-Konsole mit den Anmeldedaten desjenigen Kontos an, dem die Maschinen zugewiesen werden sollen.
2. Klicken Sie auf **Alle Geräte** –> **Hinzufügen**.
3. Scrollen Sie bis zu **Registrierungstoken** runter und klicken Sie dann auf **Generieren**.
4. Spezifizieren Sie die Token-Lebensdauer und klicken Sie anschließend auf **Token generieren**.
5. Kopieren Sie das Token oder notieren Sie es auf einem Zettel. Achten Sie darauf, dass Sie das Token speichern, falls Sie es zukünftig vielleicht noch benötigen.

   Wenn Sie auf **Aktive Tokens verwalten** klicken, können Sie alle bereits generierten Tokens einsehen und verwalten. Beachten Sie, dass in dieser Tabelle aus Sicherheitsgründen keine vollständigen Token-Werte angezeigt werden.

Schritt 2: Die .mst-Transform-Datei erstellen und das Installationspaket erstellen

1. Melden Sie sich als Administrator an einer beliebigen Maschine in der 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. Starten Sie das Setup-Programm.
4. Klicken Sie auf **.mst- und .msi-Dateien für eine unbeaufsichtigte Installation erstellen**.
5. Klicken Sie neben **Registrierungseinstellungen** auf **Spezifizieren** und geben Sie dann das von Ihnen generierte Token ein.

   Sie können die Methode zur Registrierung der Maschine im Cyber Protection Service von **Registrierungstoken verwenden** (Standard) auf **Anmeldedaten verwenden** oder **Registrierung**

überspringen ändern. Bei der Option **Registrierung überspringen** wird angenommen, dass Sie die Maschine zu einem späteren Zeitpunkt registrieren werden.

6. Überprüfen oder ändern Sie die Installationseinstellungen, die der .mst-Datei hinzugefügt werden, und klicken Sie dann auf **Fortsetzen**.
7. Spezifizieren Sie bei **Speicherziel für die Dateien** den Pfad zu dem von Ihnen erstellten Ordner.
8. Klicken Sie auf **Generieren**.

Anschließend wird die .mst-Transform-Datei erstellt und werden die .msi- und .cab-Installationspakete in dem von Ihnen erstellten Ordner extrahiert.

Schritt 3: Die Gruppenrichtlinienobjekte aufsetzen

1. Melden Sie sich am Domain Controller als Domain-Administrator an. Sollte die Domain mehr als einen Domain Controller haben, so melden Sie sich an irgendeinem von diesen als Domain-Administrator an.
2. Falls Sie planen, den Agenten in einer Organisationseinheit bereitzustellen, stellen Sie sicher, dass diese Organisationseinheit in der Domain existiert. Ansonsten können Sie diesen Schritt überspringen.
3. Gehen Sie im **Startmenü** zu **Verwaltung** und klicken Sie auf **Active Directory-Benutzer und -Computer** (im Windows Server 2003) oder **Gruppenrichtlinienverwaltung** (im Windows Server 2008 oder höher).
4. Im 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**.

   In 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. Bezeichnen Sie das neue Gruppenrichtlinienobjekt als **Agent für Windows**.
6. Öffnen Sie das Gruppenrichtlinienobjekt **Agent für Windows** folgendermaßen, um es bearbeiten zu können:
   - Klicken Sie im Windows Server 2003 auf das Gruppenrichtlinienobjekt und dann auf den Befehl **Bearbeiten**.
   - Klicken Sie im Windows Server 2008 oder höher unter **Gruppenrichtlinienobjekte** mit der rechten Maustaste auf das Gruppenrichtlinienobjekt und dann auf den Befehl **Bearbeiten**.
7. Erweitern Sie im Snap-In 'Gruppenrichtlinienobjekt-Editor' den Eintrag **Computerkonfiguration**.
8. Im Windows Server 2003 und Windows Server 2008:
   - Erweitern Sie den Eintrag **Softwareeinstellungen**.

   In Windows Server 2012 oder höher:
   - Erweitern Sie **Richtlinien** –> **Softwareeinstellungen**.
9. Klicken Sie mit der rechten Maustaste auf **Softwareinstallation**, wählen Sie dort **Neu** und klicken Sie auf **Paket**.
10. Wählen Sie das .mis-Installationspaket des Agenten in dem eben von Ihnen erstellten, freigegebenen Ordner und klicken Sie dann auf **Öffnen**.
11. Klicken Sie im Dialogfenster **Software bereitstellen** auf **Erweitert** und bestätigen Sie dann mit **OK**.
12. Klicken Sie in der Registerkarte **Modifikationen** auf **Hinzufügen** und wählen Sie das .mst-Transform, welches Sie zuvor erstellt haben.

13. Klicken Sie auf **OK** und schließen Sie das Dialogfenster **Software bereitstellen**.

8.11 Update der Agenten

Agenten mit/ab folgenden Versionen können über die Weboberfläche aktualisiert werden:

- Agent für Windows, Agent für VMware (Windows), Agent für Hyper-V: Version 11.9.191 (und höher)
- Agent für VMware (Virtuelle Appliance): Version 12.5.23094 und höher
- Agent für Virtuozzo Infrastructure Platform (Virtuelle Appliance): Version 12.5.23094 und höher
- Agent für Linux: Version 11.9.191 (und höher)
- Andere Agenten: jede Version kann aktualisiert werden

Sie können die Version des Agenten ermitteln, wenn Sie die betreffende Maschine auswählen und dann auf den Befehl **Details** klicken.

Wenn Sie ältere Agenten-Versionen aktualisieren wollen, müssen Sie die neueste Agenten-Version 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. Sie sollten überprüfen, dass dieses bereits auf Ihrer Maschine installiert ist – oder es anderenfalls vor dem Update des Agenten installieren. Nach der Installation ist möglicherweise ein Neustart der Maschine erforderlich. Das Microsoft Visual C++ Redistributable-Paket kann unter dieser Adresse gefunden werden: https://support.microsoft.com/help/2999226/update-for-universal-c-runtime-in-windows.

So können Sie das Update eines Agenten über die Weboberfläche 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 (S. 87)'. 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 (S. 71)' bereit.
4. Konfigurieren Sie den Agenten für VMware (Virtuelle Appliance) gemäß der Beschreibung im Abschnitt 'Agenten deinstallieren (S. 71)'.

   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 (S. 308)' 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 (S. 89) zuweisen wollen, klicken Sie auf **Details**, dann in den Bereich **Cyber Protection-Definitionen** und aktivieren Sie dann die Option **Diesen Agenten verwenden, um Patches und Updates herunterzuladen und zu verteilen**.

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**.

8.12 Agenten deinstallieren

Unter Windows:

Wenn Sie einzelne Produktkomponenten (z.B. einen der Agenten oder den Cyber Protection Monitor) entfernen wollen, führen Sie das Setup-Programm '**Alle Agenten für Windows**' aus, wählen Sie die Option zur Änderung des Produktes und deaktivieren Sie dann das Kontrollkästchen derjenigen Komponente, die Sie entfernen wollen. Den Link für das Setup-Programm finden Sie auf

der Seite **Downloads** (klicken Sie in der oberen rechten Ecke auf das Symbol für das Konto und dann auf **Downloads**).

Wenn Sie alle Produktkomponenten entfernen wollen, befolgen Sie die nachfolgend beschriebenen Schritte.

1. Melden Sie sich als Administrator an.
2. Gehen Sie zur **Systemsteuerung** und wählen Sie **Programme und Funktionen** (oder **Software** bei Windows XP) –> **Acronis Cyber Protection Agent** –> **Deinstallieren**.
3. [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, wird die Maschine möglicherweise in der Service-Konsole dupliziert – und die Backups der alten Maschine werden nicht mehr mit der neuen Maschine assoziiert sein.
4. Bestätigen Sie Ihre Entscheidung.
5. Überspringen Sie diesen Schritt, falls Sie vorhaben, den Agenten später noch einmal erneut zu installieren. Klicken Sie anderenfalls in der Service-Konsole auf **Einstellungen** –> **Agenten**, wählen Sie die Maschine aus, auf welcher der Agent installiert war und klicken Sie dann auf **Löschen**.

Unter Linux:

1. Führen Sie als Benutzer 'root' die Datei '**/usr/lib/Acronis/BackupAndRecovery/uninstall/uninstall**' 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, wird die Maschine möglicherweise in der Service-Konsole dupliziert – und die Backups der alten Maschine werden nicht mehr mit der neuen Maschine assoziiert sein.
3. Bestätigen Sie Ihre Entscheidung.
4. Überspringen Sie diesen Schritt, falls Sie vorhaben, den Agenten später noch einmal erneut zu installieren. Klicken Sie anderenfalls in der Service-Konsole auf **Einstellungen** –> **Agenten**, wählen Sie die Maschine aus, auf welcher der Agent installiert war und klicken Sie dann auf **Löschen**.

Unter macOS:

1. Klicken Sie doppelt auf die Installationsdatei (.dmg).
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.
6. Überspringen Sie diesen Schritt, falls Sie vorhaben, den Agenten später noch einmal erneut zu installieren. Klicken Sie anderenfalls in der Service-Konsole auf **Einstellungen** –> **Agenten**, wählen Sie die Maschine aus, auf welcher der Agent installiert war und klicken Sie dann auf **Löschen**.

Den Agenten für VMware (Virtuelle Appliance) entfernen

1. Starten Sie den vSphere Client und melden Sie sich am vCenter Server an.
2. Sollte die virtuelle Appliance (VA) eingeschaltet sein, dann klicken Sie mit der rechten Maustaste auf die VA. Klicken Sie anschließend auf die Befehle **Betrieb** –> **Ausschalten**. Bestätigen Sie Ihre Entscheidung.

3. Sollte die VA einen lokal angeschlossenen Storage auf einem virtuellen Festplattenlaufwerk verwenden und Sie die Daten diesem Laufwerk bewahren wollen, dann gehen Sie folgendermaßen vor:
   a. Klicken Sie mit der rechten Maustaste auf die VA und wählen Sie **Einstellungen bearbeiten**.
   b. Wählen Sie die virtuelle Festplatte mit dem Storage und klicken Sie auf **Entfernen**. Klicken Sie unter **Optionen beim Entfernen** auf **Von der virtuellen Maschine entfernen**.
   c. Klicken Sie auf **OK**.

   Die Festplatte verbleibt als Ergebnis im Datenspeicher. Sie können die virtuelle Festplatte an eine andere VA anschließen.
4. Klicken Sie mit der rechten Maustaste auf die VA und wählen Sie **Von Festplatte löschen**. Bestätigen Sie Ihre Entscheidung.
5. Überspringen Sie diesen Schritt, falls Sie vorhaben, den Agenten später noch einmal erneut zu installieren. Alternativ können Sie in der Service-Konsole auch Folgendes tun:
   a. Klicken Sie auf **Einstellungen** –> **Agenten**, wählen Sie die virtuelle Appliance aus und klicken Sie dann auf **Löschen**.
   b. Klicken Sie auf **Backup Storage** –> **Speicherorte** und löschen Sie dann den Speicherort, der dem lokal angeschlossenen Storage entspricht.

8.13 Sicherheitseinstellungen

Wenn Sie die allgemeinen Schutzeinstellungen für Cyber Protection konfigurieren wollen, gehen Sie in der Service-Konsole zu **Einstellungen** –> **Schutz**.

Automatische Updates für Komponenten

Cyber Protection verwendet eine Peer-zu-Peer-Technologie für Komponenten-Updates, um die Bandbreite des Netzwerkverkehrs zu minimieren. Sie können einen oder mehrere dedizierte Agenten bestimmen, die Updates aus dem Internet herunterladen und als Peer-zu-Peer-Agenten für die anderen Agenten im Netzwerk bereitstellen sollen.

Die Option **Diesen Agenten verwenden, um Patches und Updates herunterzuladen und zu verteilen** ist standardmäßig für die Agenten deaktiviert. Dies bedeutet, dass alle registrierten Agenten selbst nach den neuesten Updates suchen und diese verteilen. Wenn ein Benutzer für einen bestimmten Agenten die Option **Diesen Agenten verwenden, um Patches und Updates herunterzuladen und zu verteilen** aktiviert, wird diesem Agenten die Rolle 'Updater' zugewiesen und werden anschließend alle übrigen Agenten diesen speziellen Agenten verwenden, um nach Upates zu suchen und diese dann zu verteilen. Sie müssen sicherstellen, dass die Agenten mit der Updater-Rolle ausreichend leistungsfähig sind, einen stabilen und schnellen Internetzugang sowie genügend freien Speicherplatz haben.

Der Update-Workflow sieht folgendermaßen aus:

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.

So können Sie einem Protection Agenten die Rolle 'Updater' zuweisen

1. Gehen Sie in der Service-Konsole in den Bereich **Einstellungen** –> **Agenten**.
2. Wählen Sie die Maschine aus, der Sie die Updater-Rolle zuweisen wollen.

3. Klicken Sie auf **Details** und aktivieren Sie dann die Option **Diesen Agenten verwenden, um Patches und Updates herunterzuladen und zu verteilen**.

Die Cyber Protection-Definitionen per Planung aktualisieren

Sie können in der Registerkarte **Planung** für jede der Komponenten festlegen, ob die Cyber Protection-Definitionen automatisch per Zeitplanung aktualisiert werden sollen.

- Antimalware
- Schwachstellenbewertung
- Patch-Verwaltung

Planungstyp:

- **Täglich** – definiert, an welchen Wochentagen die Definitionen aktualisiert werden sollen.

  Starten um – Sie können auswählen, zu welchem Zeitpunkt die Definitionen aktualisiert werden sollen.
- **Stündlich** – definiert eine genauere stündliche Planung für die Aktualisierung der Definitionen.

  Ausführen alle/jede(n) – definieren die Periodizität für die Ausführung von Definitions-Updates.

  Von ... **Bis** – definiert einen bestimmten Zeitraum, in dem das automatische Update der Definition durchgeführt wird.

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 Service-Konsole in den Bereich **Einstellungen** –> **Agenten**.
2. Wählen Sie die Maschinen aus, auf denen Sie die Cyber Protection-Definitionen aktualisieren wollen, und klicken Sie dann auf **Definitionen aktualisieren**.

Cache Storage

Der Speicherort der gechachten Daten:

- 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`**

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** – definiert den Speicherplatz, der dem Cache auf der Maschine/den Maschinen mit der Rolle 'Updater' zugewiesen wird.
- **Andere Rollen** – definiert den Speicherplatz, der dem Cache auf anderen Maschinen zugewiesen wird.

Remote-Verbindung

Klicken Sie auf **Remote-Desktop-Verbindung**, um Remote-Verbindungen zu den Maschinen über einen RDP- oder HTML5-Client zu ermöglichen. Wenn dieser Punkt deaktiviert ist, werden die Optionen **Über RDP-Client verbinden** / **Über HTML5-Client verbinden** in der Service-Konsole

ausgeblendet, sodass die Benutzer keine Remote-Verbindung mit anderen Maschinen aufbauen können. Diese Option wirkt sich auf alle Benutzer in Ihrer Organisation aus.

Klicken Sie auf **Remote-Desktop-Verbindung freigeben**, um die Freigabe der Remote-Verbindung für andere Benutzer zu aktivieren. Dadurch erscheint, wenn Sie eine Maschine auswählen, die neue Option **Remote-Verbindung freigeben** im rechten Menü – und Sie können einen Link für den Zugriff auf die Remote-Maschine generieren, den Sie mit anderen Benutzern teilen können.

8.14 Die Quota für ein Gerät ändern

Der Cyber Protection Service gleicht Quotas (Kontingente) und Geräte automatisch ab. Wenn Sie ermitteln wollen, welcher Quota ein bestimmtes Gerät zugewiesen wurde, können Sie den Bereich **Service-Quota** in den **Details** des Gerätes einsehen.

In seltenen Fällen kann es notwendig sein, diese Konfiguration manuell zu ändern. Beispielsweise, wenn die Quota **Workstations** einer virtuellen Maschine zugewiesen wurde. Wenn Sie die Quota **Virtuelle Maschine** erwerben, können Sie dann die Maschine dieser günstigeren Quota zuweisen.

So können Sie die Quota für ein Gerät ändern

1. Wählen Sie das Gerät aus.
2. Klicken Sie auf **Details**.
3. Klicken Sie im Bereich **Service-Quota** auf **Ändern**.
4. Wählen Sie die neue Quota oder **Keine Quota** aus. **Keine Quota** bedeutet, dass die aktuell verwendete Quota freigegeben wird und Sie ein anderes Gerät dieser Quota zuweisen können.
5. Bestätigen Sie Ihre Entscheidung.

8.15 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

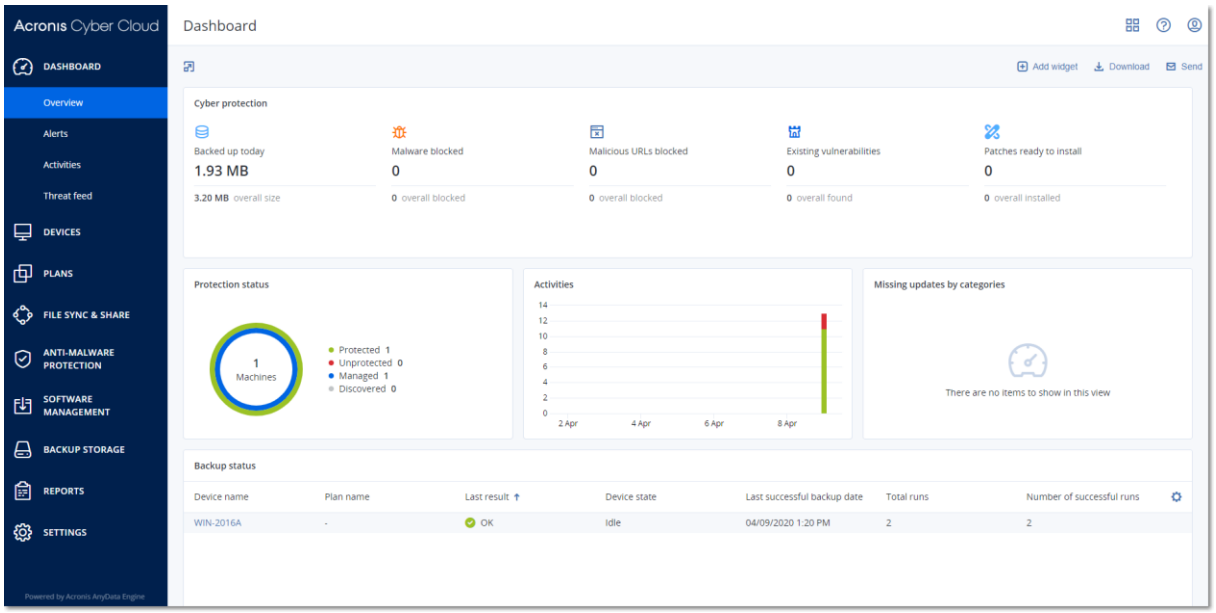
Service-Name und -Speicherort	Zweck
/Library/LaunchDaemons/com.acronis.aakore.plist	Ermöglicht die Kommunikation zwischen dem Agenten und den Verwaltungskomponenten
/Library/LaunchDaemons/com.acronis.cyber-protect-service.plist	Ermöglicht die Erkennung von Malware

Service-Name und -Speicherort	Zweck
/Library/LaunchDaemons/com.acronis.mms.plist	Stellt die Backup- und Recovery-Funktionalität bereit
/Library/LaunchDaemons/com.acronis.schedule.plist	Führt geplante Tasks aus

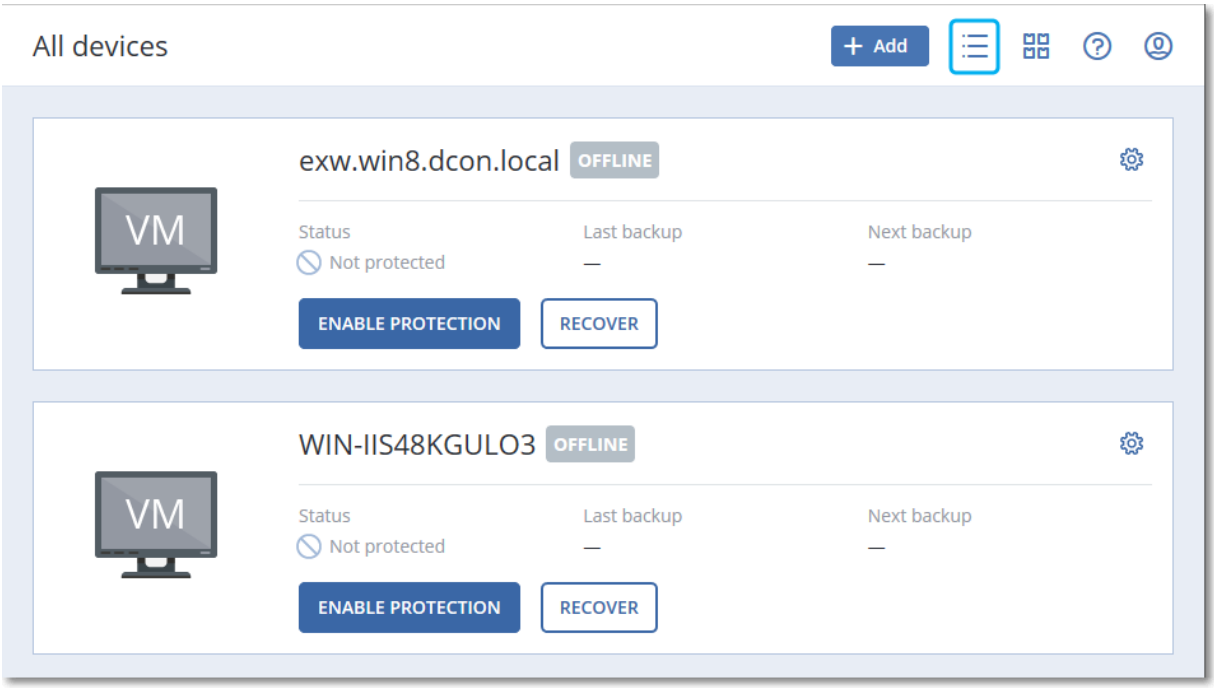
9 Service-Konsole

Die Service-Konsole ermöglicht Ihnen, Ihre Geräte und Schutzpläne zu verwalten, und stellt Ihnen ein praktisches Dashboard bereit, wo Sie die wichtigsten Informationen über Ihre Cyber Protection finden können.

Sie können in der Service-Konsole Ihre Einstellungen ändern, Ihre Berichte konfigurieren oder Ihren Backup-Storage überprüfen. Die Konsole bietet Ihnen außerdem Zugriff auf zusätzliche Services oder Funktionen von Cyber Protection – wie etwa File Sync & Share-Funktionen, Antivirus & Antimalware Protection, Patch-Verwaltung und Schwachstellenbewertung. Je nach vorliegender Cyber Protection Edition kann deren Typ und Anzahl unterschiedlich sein.

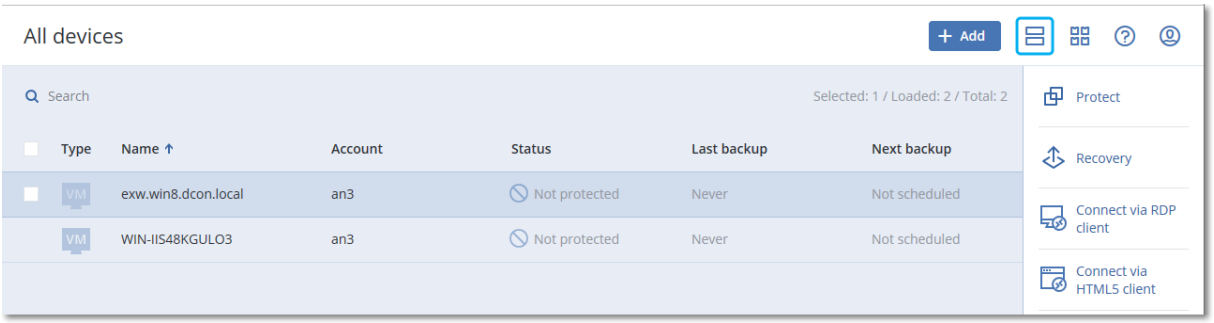


Für den Bereich **Geräte** können Sie zwischen einer einfachen Ansicht und einer Tabellenansicht wählen. Sie können zwischen diesen wechseln, wenn Sie in der oberen rechten Ecke auf das entsprechende Symbol klicken.



In der einfachen Ansicht werden nur einige wenige Maschinen angezeigt.

Die Tabellenansicht wird automatisch aktiviert, wenn die Anzahl der Maschinen 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.

So können Sie eine Maschine aus der Service-Konsole entfernen

1. Aktivieren Sie das Kontrollkästchen neben der gewünschten Maschine.
2. Klicken Sie auf **Löschen** und bestätigen Sie Ihre Wahl.

***Wichtig**: Wenn Sie eine Maschine aus der Service-Konsole entfernen, wird dadurch nicht der Protection Agent auf der Maschine deinstalliert und werden auch nicht die auf diese Maschine angewendeten Schutzpläne gelöscht. Und auch die Backups der gelöschten Maschine werden weiter aufbewahrt.*

Virtuelle VMware- oder Hyper-V-Maschinen sowie ESXi-Hosts können durch einen Agenten gesichert werden, der nicht auf den betreffenden Maschinen/Hosts installiert ist. Sie können solche Maschinen nicht einzeln löschen. Wenn Sie diese löschen wollen, müssen Sie diejenige Maschine finden und löschen, auf welcher der entsprechende Agent für VMware bzw. der Agent für Hyper-V installiert ist.

So können Sie eine virtuelle Maschine oder einen ESXi-Host ohne Agenten löschen

1. Wählen Sie unter **Geräte** den Befehl **Alle Geräte**.
2. Klicken Sie in der rechten oberen Ecke auf das Zahnrad-Symbol und aktivieren Sie die Spalte **Agent**.

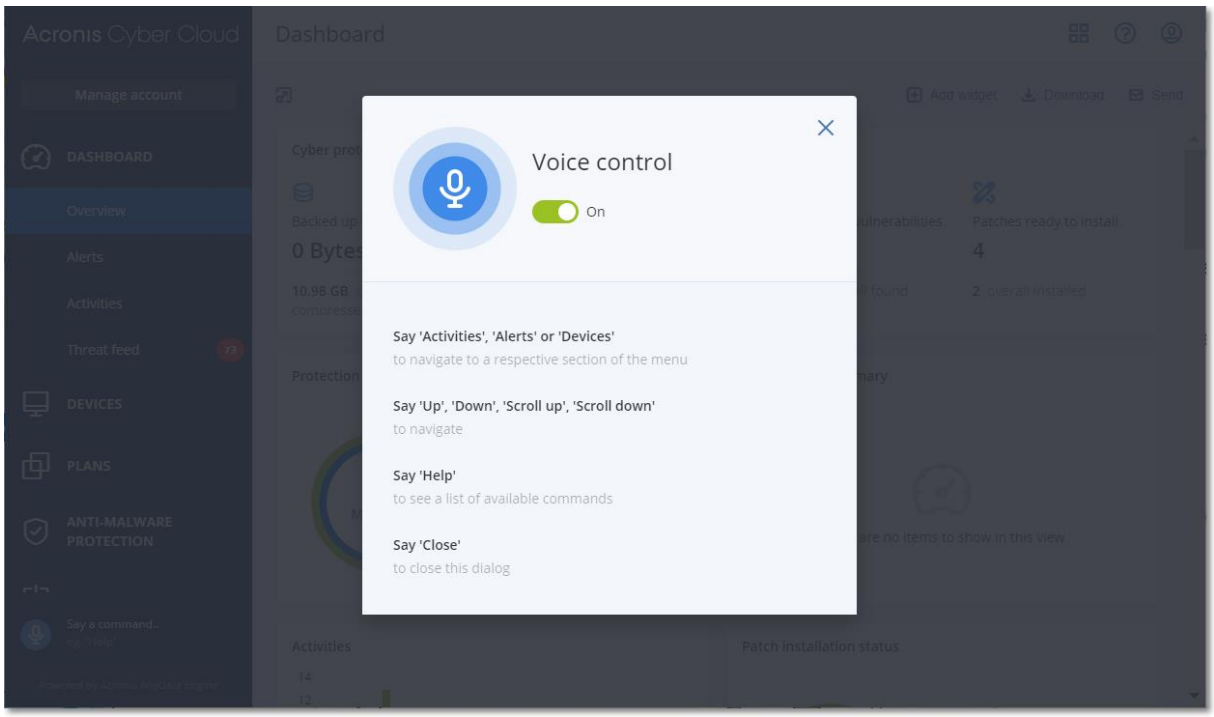
3. Aktivieren Sie in der Spalte **Agent** das Kontrollkästchen für den Namen der Maschine, auf welcher der entsprechende Agent installiert ist.
4. Löschen Sie diese Maschine aus der Service-Konsole. Dadurch werden auch alle Maschinen entfernt, die von diesem entsprechenden Agenten gesichert werden.
5. Deinstallieren Sie den Agenten von der gelöschten Maschine, wie es im Abschnitt 'Agenten deinstallieren (S. 87)' erläutert ist.

10 Sprachsteuerung für Aktionen in der Konsole

Sie können die Sprachsteuerung aktivieren, um verschiedene Aktionen in der Service-Konsole mithilfe Ihrer Stimme auszuführen. Diese Funktionalität ist jedoch nur in den Cyber Protect-Editionen verfügbar.

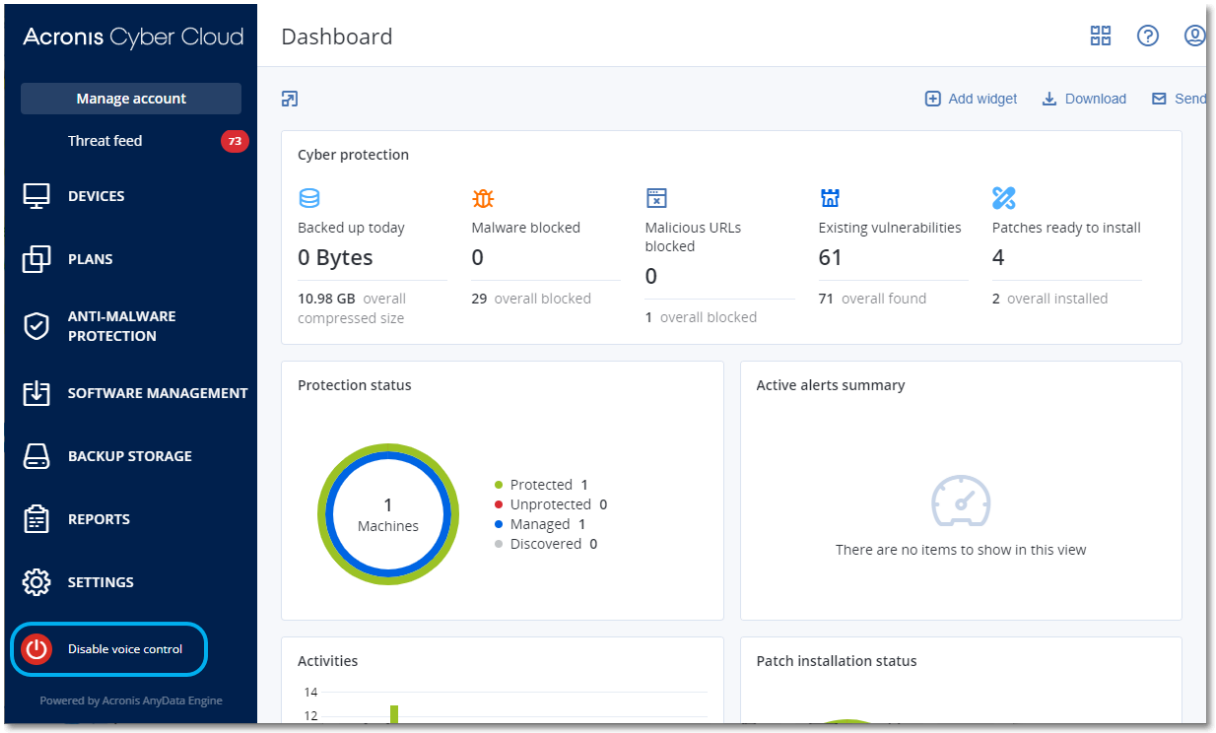
Stellen Sie vor dem Einschalten der Sprachsteuerung sicher, dass der Zugriff auf das entsprechende Mikrofon aktiviert ist.

Um die Sprachsteuerung zu aktivieren, müssen Sie in der rechten oberen Ecke der Service-Konsole auf das Benutzersymbol klicken, dort dann auf den Befehl **Sprachsteuerung** klicken und anschließend den Schalter einschalten. Anschließend sehen Sie jedes Mal, wenn Sie einen Befehl aussprechen, den erkannten Text in der linken unteren Ecke der Service-Konsole.



Wenn Sie die Sprachsteuerung wieder ausschalten wollen, können Sie den Mauszeiger über das Mikrofonsymbol in der linken unteren Ecke bewegen und dort dann auf die rote Schaltfläche klicken. Alternativ können Sie auch auf das Benutzersymbol in der rechten oberen Ecke der Service-Konsole

klicken, dann auf den Befehl **Sprachsteuerung** und anschließend den Schalter auf ausgeschaltet stellen.



Einschränkungen:

- Die Sprachsteuerungsfunktionalität wird nur für Englisch unterstützt. Diese Option ist für andere Sprachen nicht verfügbar.
- Die Sprachsteuerungsfunktionalität wird nur im Google Chrome-Webbrowser für Desktop-PCs unterstützt. Webbrowser für Mobilgeräte werden nicht unterstützt.
- Die Sprachsteuerungsfunktionalität funktioniert nur mit dem HTTPS-Protokoll. Wenn ein Anwender versucht, über das HTTP-Protokoll auf die Service-Konsole zuzugreifen, wird er das Mikrofon nicht aktivieren und die Option **Sprachsteuerung** nicht einschalten können.

Wenn Sie die Hilfe öffnen und alle verfügbaren Sprachbefehle angezeigt bekommen wollen, müssen Sie in der rechten oberen Ecke auf das Fragezeichen-Symbol klicken und anschließend den Befehl **Sprachsteuerungshilfe** auswählen.

Sprachbefehl	Beschreibung
Allgemein	
Hilfe	Ein modales Hilfefenster öffnen
Nach oben scrollen	Um die Seite nach oben zu scrollen
Nach unten scrollen	Um die Seite nach unten zu scrollen
Nach oben (oder Zurück)	Zur oberen Zeile in einer Tabelle wechseln
Nach unten (oder Weiter)	Zur unteren Zeile in einer Tabelle wechseln
Schließen	Ein modales Fenster schließen
Dashboard > Überblick	
Überblick	Zum Bereich 'Überblick' gehen

[Statusname]	Im Widget 'Schutzstatus' nach dem Maschinenstatus auflisten
Dashboard > Alarmmeldungen	
Alarmmeldungen	Zum Bereich 'Alarmmeldungen' gehen
[Name des Alarms]	Filtern Sie nach dem Alarmtyp, indem Sie den entsprechenden Namen des Alarms sagen. Beispielsweise 'Backup ist fehlgeschlagen', 'Lizenz ist abgelaufen', 'Maschine ist offline'
Alle löschen	Alle Alarmmeldungen bereinigen
Dashboard > Aktivitäten	
Aktivitäten	Zum Bereich 'Aktivitäten' gehen
Dashboard > Bedrohungsfeed	
Bedrohungsfeed	Zum Bereich 'Bedrohungsfeed' gehen
Geräte > Alle Geräte	
Geräte	Zum Bereich 'Alle Geräte' gehen
Schützen	Die Liste der Schutzpläne für ein Gerät öffnen
[Plan-Name]	Wählen Sie den Plan-Namen für ein Gerät. Beispielsweise 'Komplette Maschine in die Cloud', 'Cloud-zu-Cloud-Backup'
Anwenden	Einen bestimmten Schutzplan auf ein Gerät anwenden
Backup abbrechen	Die Ausführung eines Backups für ein bestimmtes Gerät stoppen
Backup jetzt	Das Backup für ein bestimmtes Gerät ausführen
Recovery	Die Recovery-Punkte ein Gerät öffnen
Details	Die Details zu einem Gerät anzeigen
Aktivitäten	Die Aktivitäten für ein Gerät öffnen
Alarmmeldungen	Die Alarmmeldungen für ein Gerät öffnen
Antivirus & Antimalware Protection	
Quarantäne	Zum Bereich 'Quarantäne' gehen
Positivliste	Zum Bereich 'Positivliste' gehen
Software-Verwaltung	
Patches	Zum Bereich 'Patches' gehen
Schwachstellen	Zum Bereich 'Schwachstellen' gehen

Typische Szenarien:

- Wenn Sie einen Schutzplan für ein Gerät auswählen, sagen Sie: Schützen > <Plan-Name>
- Wenn Sie einem Gerät einen bestimmten Schutzplan zuweisen wollen, sagen Sie: Schützen > <Plan-Name> > Anwenden
- Wenn Sie ein Backup auf einem bestimmten Gerät ausführen wollen, sagen Sie: Schützen > <Plan-Name> > Backup jetzt
- Wenn Sie ein Backup auf einem bestimmten Gerät abbrechen wollen, sagen Sie: Schützen > <Plan-Name> > Backup abbrechen

11 Gerätegruppen

***Hinweis**: Diese Funktionalität ist in den Standard Editionen des Cyber Protection Service nicht verfügbar.*

Gerätegruppen wurden entworfen, um eine größere Anzahl von registrierten Geräten bequem verwalten zu können.

Sie können einen Schutzplan auf eine Gruppe anwenden. Sobald ein neues Gerät in der Gruppe erscheint, wird das Gerät automatisch durch diesen Plan geschützt. Wenn ein Gerät aus einer Gruppe entfernt wird, so wird es auch nicht mehr länger durch den Plan geschützt. Ein Plan, der auf eine Gruppe angewendet wird, kann nur von der kompletten Gruppe wieder entfernt werden – jedoch nicht von einem einzelnen Mitglied in der Gruppe.

Einer Gruppe können nur Geräte hinzugefügt werden, die denselben Typ haben. Beispiel: Sie können unter **Hyper-V** eine Gruppe für virtuelle Hyper-V-Maschinen erstellen. Unter **Maschinen mit Agenten** können Sie eine Gruppe mit Maschinen erstellen, auf denen Agenten installiert sind. Unter **Alle Geräte** können Sie keine Gruppe erstellen.

Ein einzelnes Gerät kann Mitglied in mehr als einer Gruppe sein.

Vorgegebene Gruppen

Sobald ein Gerät registriert wird, erscheint es in einer der vorgegebenen Stammgruppen in der Registerkarte **Geräte**.

Stammgruppen können nicht bearbeitet oder gelöscht werden. Sie können keine Pläne auf Stammgruppen anwenden.

Einige der Stammgruppen enthalten vorgegebene Unterstammgruppen. Diese Gruppen können nicht bearbeitet oder gelöscht werden. Sie können jedoch Pläne auf vorgegebene Unterstammgruppen anwenden.

Benutzerdefinierte Gruppen

Alle Geräte über eine vorgegebene Gruppe mit nur einem Schutzplan zu sichern, ist jedoch nicht zufriedenstellend, da die Maschinen üblicherweise unterschiedliche Aufgaben haben. Die zu sichernden Daten sind spezifisch für jede Abteilung, manche Daten müssen häufig erfasst werden, bei anderen erfolgt das Backup nur zweimal im Jahr. Von daher werden Sie vermutlich verschiedene Schutzpläne für diverse Arten von Maschinen erstellen. In diesem Fall sollten Sie die Erstellung benutzerdefinierter Gruppen erwägen.

Eine benutzerdefinierte Gruppe kann eine oder mehrere verschachtelte Gruppen enthalten. Jede benutzerdefinierte Gruppe kann bearbeitet oder gelöscht werden. Es gibt folgende Typen von benutzerdefinierten Gruppen:

- **Statische Gruppen**

  Statische Gruppen enthalten nur Maschinen, die der Gruppe manuell hinzugefügt wurden. Der Inhalt einer statischen Gruppe ändert sich solange nicht, bis Sie eine Maschine hinzufügen oder löschen.

  Beispiel: Sie erstellen eine benutzerdefinierte Gruppe für die Buchhaltung und fügen die Maschinen der entsprechenden Mitarbeiter der Gruppe manuell hinzu. Diese Maschinen aus der Buchhaltungsmitarbeiter sind geschützt, sobald Sie der Gruppe einen Schutzplan zuweisen. Wird ein neuer Buchhalter eingestellt, so müssen Sie dessen neue Maschine der Gruppe einfach nur manuell hinzufügen.

- **Dynamische Gruppen**

  Die Maschinen in einer dynamischen Gruppe werden dieser automatisch hinzugefügt – und zwar auf Basis von Suchkriterien, die bei Erstellung einer Gruppe spezifiziert wurden. Der Inhalt einer dynamischen Gruppe ändert sich automatisch. Eine Maschine verbleibt solange in der Gruppe, wie sie die spezifizierten Kriterien erfüllt.

  Beispiel 1: Die Host-Namen der Maschinen, die zur Buchhaltungsabteilung gehören, enthalten alle den Begriff 'Buchhaltung'. Sie verwenden diesen Teil des Maschinennamens als Kriterium für die Gruppenmitgliedschaft – und wenden dann einen Schutzplan auf die Gruppe an. Wenn ein neuer Buchhaltungsmitarbeiter eingestellt wird, so wird dessen neue Maschine in die Gruppe aufgenommen (und damit automatisch gesichert), sobald die Maschine registriert wird.

  Beispiel 2: Die Buchhaltungsabteilung bildet eine eigene Active Directory-Organisationseinheit (Organizational Unit, OU). Sie verwenden die Buchhaltungs-Organisationseinheit als Kriterium für die Gruppenmitgliedschaft – und wenden dann einen Schutzplan auf die Gruppe an. Wenn ein neuer Buchhaltungsmitarbeiter eingestellt wird, so wird dessen neue Maschine in die Gruppe aufgenommen (und damit automatisch gesichert), sobald die Maschine registriert und der Organisationseinheit hinzugefügt wird (unabhängig davon, was zuerst passiert).

11.1 Eine statische Gruppe erstellen

1. Klicken Sie auf **Geräte** und wählen Sie die vorgegebene Gruppe (Standardgruppe) aus, welche die Geräte enthält, für die Sie eine statische Gruppe erstellen wollen.
2. Klicken Sie auf das Zahnradsymbol, welches neben derjenigen Gruppe liegt, in der Sie eine neue Gruppe erstellen wollen.
3. Klicken Sie auf **Neue Gruppe**.
4. Spezifizieren Sie einen Namen für die Gruppe und klicken Sie dann auf **OK**.

   Die neue Gruppe erscheint im Gruppen-Verzeichnisbaum.

11.2 Geräte zu statischen Gruppen hinzufügen

1. Klicken Sie auf **Geräte** und wählen Sie dann ein oder mehrere Gerät(e) aus, welche(s) Sie einer Gruppe hinzufügen wollen.
2. Klicken Sie auf **Zur Gruppe hinzufügen**.

   Die Software zeigt eine Verzeichnisbaum mit allen Gruppen an, denen das ausgewählte Gerät hinzugefügt werden kann.
3. Wenn Sie eine neue Gruppe erstellen wollen, gehen Sie wie nachfolgend beschrieben vor. Wenn Sie dies nicht wollen, können Sie diesen Schritt überspringen.
   a. Wählen Sie die Gruppe, in der Sie eine Gruppe erstellen wollen.
   b. Klicken Sie auf **Neue Gruppe**.
   c. Spezifizieren Sie einen Namen für die Gruppe und klicken Sie dann auf **OK**.
4. Bestimmen Sie die Gruppe, der Sie das Gerät hinzufügen wollen, und klicken Sie anschließend auf **Fertig**.

Eine weitere Möglichkeit, Geräte zu einer statischen Gruppe hinzuzufügen, besteht darin, die Gruppe auszuwählen und dann auf die Schaltfläche **Geräte hinzufügen** zu klicken.

11.3 Eine dynamische Gruppe erstellen

1. Klicken Sie auf **Geräte** und wählen Sie die Gruppe aus, die die Geräte enthält, für die Sie eine dynamische Gruppe erstellen wollen.

2. Suchen Sie nach den Geräten über das Feld 'Suchen'. Sie können mehrere Suchkriterien und Operatoren verwenden (wie unten beschrieben).
3. Klicken Sie neben dem Suchfeld auf **Speichern unter**.

   ***Hinweis**: Bei der Gruppenerstellung werden einige Suchkriterien nicht unterstützt. Siehe die Tabelle im unteren Abschnitt zu den Suchkritierien.*

4. Spezifizieren Sie einen Namen für die Gruppe und klicken Sie dann auf **OK**.

Suchkriterien

Die nachfolgende Tabelle fasst alle unterstützten Suchkritieren zusammen.

Kriterium	Bedeutung	Beispiele für Suchanfragen	Für Gr
name	▪ Host-Name für physische Maschinen ▪ Name für virtuelle Maschinen ▪ Datenbankname ▪ E-Mail-Adresse für Postfächer	**name = 'en-00'**	Ja

comment	Kommentar für ein Gerät.
	Standardwert:
	▪ Für physische Computer unter Windows wird die Computer-Beschreibung aus den Computer-Eigenschaften in Windows übernommen. Dieser Wert wird automatisch alle 15 Minuten aktualisiert.
	▪ Leer für andere Geräte.
	Wenn Sie den Kommentar einsehen wollen, wählen Sie unter **Geräte** das entsprechende Geräte, 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 **Bearbeiten**. In diesem Fall wird das automatische Update nicht mehr funktionieren. Wenn Sie die automatischen Updates wieder zulassen wollen, müssen Sie den von Ihnen hinzugefügten Kommentar löschen.
	Um das Kommentarfeld für Ihre Geräte 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`
		comment = 'important machine'
		comment = '' (alle Maschinen ohne Kommentar).
			Ja

ip	IP-Adresse (nur für physische Maschinen)	**ip RANGE ('10.250.176.1','10.250.176.50')**	Ja

Kriterium	Bedeutung	Beispiele für Suchanfragen	Für Gr
memorySize	RAM-Größe in Megabyte (MiB)	**memorySize < 1024**	Ja
insideVm	Virtuelle Maschine, die einen Agenten enthält. Mögliche Werte: ▪ **true** ▪ **false**	**insideVm = true**	Ja
osName	Betriebssystemname.	**osName LIKE '%Windows XP%'**	Ja
osType	Betriebssystemtyp. Mögliche Werte: ▪ **'windows'** ▪ **'linux'** ▪ **'macosx'**	**osType IN ('linux', 'macosx')**	Ja
osProductType	Der Betriebssystemprodukttyp. Mögliche Werte: ▪ **'dc'** Steht für Domain Controller. ▪ **'server'** ▪ **'workstation'**	**osProductType = 'server'**	Ja
tenant	Der Name der Abteilung, zu welcher das Gerät gehört.	**tenant = 'Unit 1'**	Ja
tenantId	Die ID der Abteilung, zu welcher das Gerät gehört. So können Sie die Abteilungs-ID abrufen: 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

Kriterium	Bedeutung	Beispiele für Suchanfragen	Für Gr
state	Gerätestadium. Mögliche Werte: ▪ **'idle'** ▪ **'interactionRequired'** ▪ **'canceling'** ▪ **'backup'** ▪ **'recover'** ▪ **'install'** ▪ **'reboot'** ▪ **'failback'** ▪ **'testReplica'** ▪ **'run_from_image'** ▪ **'finalize'** ▪ **'failover'** ▪ **'replicate'** ▪ **'createAsz'** ▪ **'deleteAsz'** ▪ **'resizeAsz'**	**state = 'backup'**	Nein
protectedByPlan	Geräte, die durch einen Schutzplan mit einer bestimmten ID gesichert werden. So können Sie die Plan-ID abrufen: Klicken Sie auf **Pläne** –> **Backup** und wählen Sie den gewünschten Plan aus. Klicken Sie auf das Diagramm in der Spalte **Status** und dann auf einen Status. Es wird eine neue Suche mit der Plan-ID erstellt.	**protectedByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'**	Nein
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

Kriterium	Bedeutung	Beispiele für Suchanfragen	Für Gr
ou	Maschinen, die zu der spezifizierten Active Directory-Organisationseinheit gehören.	**ou IN ('RnD', 'Computers')**	Ja
id	Geräte-ID. So können Sie die Geräte-ID abrufen: 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
lastBackupTime*	Datum und Zeitpunkt des letzten erfolgrechen Backups. Das Format ist `'YYYY-MM-DD HH:MM'`.	**lastBackupTime > '2016-03-11'** **lastBackupTime <= '2016-03-11 00:15'** **lastBackupTime is null**	Nein
lastBackupTryTime*	Zeitpunkt des letzten Backup-Versuchs. Das Format ist `'YYYY-MM-DD HH:MM'`.	**lastBackupTryTime >= '2016-03-11'**	Nein
nextBackupTime*	Zeitpunkt des nächsten Backups. Das Format ist `'YYYY-MM-DD HH:MM'`.	**nextBackupTime >= '2016-03-11'**	Nein
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 abrufen: Wählen Sie bei **Geräte** die gewünschte Maschine aus und klicken Sie dann auf **Details** –> **Alle Eigenschaften**. Verwenden Sie den Wert **"id"** der Eigenschaft **agent**.	**hostId = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'**	Ja
resourceType	Ressourcentyp. Mögliche Werte: ▪ **'machine'** ▪ **'virtual_machine.vmwesx'** ▪ **'virtual_machine.mshyperv'** ▪ **'virtual_machine.rhev'** ▪ **'virtual_machine.kvm'** ▪ **'virtual_machine.xen'**	**resourceType = 'machine'** **resourceType in ('mssql_aag_database', 'mssql_database')**	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 = 2020-02-20' bedeutet, dass die Suchergebnisse alle Backups aus dem Zeitraum 'lastBackupTime >= 2020-02-20 00:00' und 'lastBackup time <= 2020-02-20 23:59:59' enthalten werden.*

Operatoren

Die nachfolgende Tabelle fasst alle unterstützten Operatoren zusammen.

Operator	Bedeutung	Beispiele
AND	Operator für logische Konjunktion.	**name like 'en-00' AND tenant = 'Unit 1'**
OR	Operator für logische Disjunktion.	**state = 'backup' OR state = 'interactionRequired'**
NOT	Operator für logische Negation.	**NOT(osProductType = 'workstation')**
LIKE 'Platzhalter-Muster'	Dieser Operator wird verwendet, um zu testen, ob ein Ausdruck mit dem Platzhalter-Muster übereinstimmt. Bei diesem Operator wird Groß-/Kleinschreibung unterschieden. Die folgenden Platzhalteroperatoren können verwendet werden: ▪ * oder %. Der Asterisk und das Prozentzeichen stehen für kein, ein oder oder mehrere Zeichen. ▪ _. Das Unterstrichzeichen repräsentiert ein einzelnes Zeichen	**name LIKE 'en-00'** **name LIKE '*en-00'** **name LIKE '*en-00*'** **name LIKE 'en-00_'**
IN (<Wert1>,... <WertN>**)**	Dieser Operator wird verwendet, um zu testen, ob ein Ausdruck mit irgendeinem Wert in einer Liste von Werten übereinstimmt. Bei diesem Operator wird Groß-/Kleinschreibung unterschieden.	**osType IN ('windows', 'linux')**
RANGE(<Startwert>, <Endwert>**)**	Dieser Operator wird verwendet, um zu testen, ob sich ein Ausdruck innerhalb eines Wertebereichs befindet.	**ip RANGE('10.250.176.1','10.250.176.50')**

11.4 Einen Schutzplan auf eine Gruppe anwenden

1. Klicken Sie auf **Geräte** und wählen Sie dann die vorgegebene Gruppe (Standardgruppe), welche diejenige Gruppe enthält, auf welche der Schutzplan angewendet werden soll.

   Die Software zeigt eine Liste mit Untergruppen an.
2. Wählen Sie die Gruppe aus, auf welche der Schutzplan angewendet werden soll.
3. Klicken Sie auf **Gruppen-Backup**.

   Die Software zeigt die Liste der Schutzpläne an, die auf die Gruppe angewendet werden können.
4. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Erweitern Sie einen vorhandenen Schutzplan und klicken Sie auf **Anwenden**.
   - Klicken Sie auf **Neu erstellen** und erstellen Sie dann – wie im Abschnitt 'Schutzplan (S. 412)' beschrieben – einen neuen Schutzplan.

12 Unterstützung für mehrere Mandanten

Cyber Protection verfügt über Mandantenfähigkeit (Multitenancy). Das bedeutet, dass ein Mandantenadministrator/Benutzer Objekte verwalten kann, die mit seinem Mandanten oder deren Untermandanten (Abteilungen/Einheiten) zusammenhängen. Ein Administrator/Benutzer von einer Abteilung kann keine Objekte eines übergeordneten Mandanten verwalten.

Beispiel: ein Kundenadministrator hat einen Schutzplan erstellt und diesen auf eine Maschine angewendet. Ein Kundenadministrator kann außerdem Schutzpläne verwalten, die von einem

Abteilungsadministrator erstellt wurden. Ein Abteilungsadministrator wiederum, kann keinen Schutzplan verwalten, der von einem Kundenadministrator erstellt wurde. Ein Abteilungsadministrator kann seinen eigenen Schutzplan erstellen, der nicht mit dem Plan des Kundenadministrators in Konflikt steht.

Mandantenfähigkeit bedeutet auch, dass ein Mandantenadministrator/Benutzer alle Objekte sehen kann, die mit diesem Mandanten oder dessen Untermandanten (Abteilungen) zusammenhängen. Ein Administrator/Benutzer von einer Abteilung kann keine Objekte eines übergeordneten Mandanten sehen.

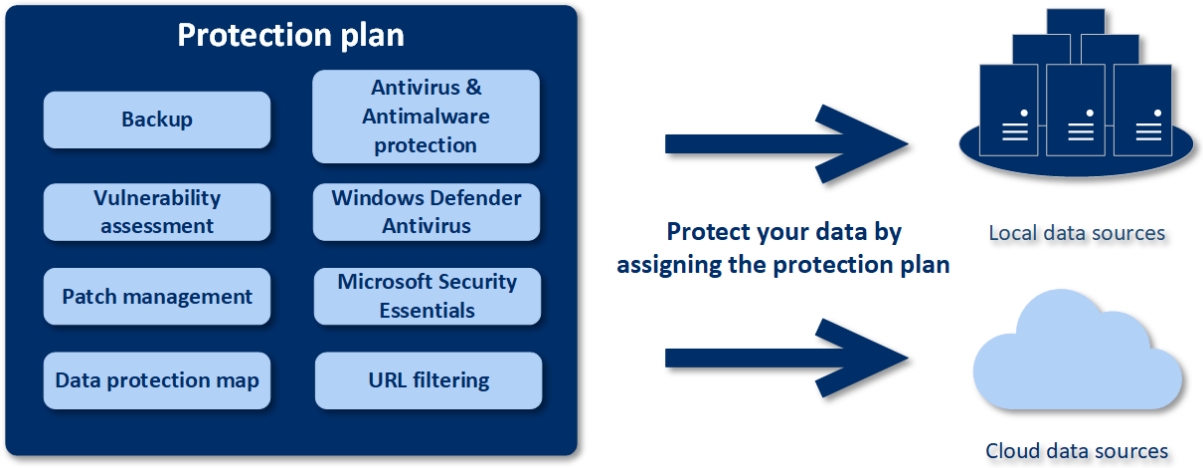
Beispielsweise werden die Daten in der Patch-Liste, der Quarantäne, im Bedrohungsfeed, den Warnmeldungen und den Aktivitäten nur für den aktuellen Mandanten und dessen Untermandanten angezeigt. Daten, die zum übergeordneten Mandanten gehören, werden dagegen nicht angezeigt.

13 Schutzplan und Module

Ein Schutzplan ist ein Plan, der mehrere Data Protection-Module kombiniert. Dazu gehören:

- Backup (S. 121) – ermöglicht Ihnen, Ihre Datenquellen zu einem lokalen Storage oder Cloud Storage zu sichern.
- Antivirus & Antimalware Protection (S. 359) – ermöglicht Ihnen, Ihre Maschinen mit der integrierten Antimalware-Lösung zu überprüfen.
- URL-Filterung (S. 371) – ermöglicht Ihnen, Ihre Maschinen vor Bedrohungen aus dem Internet zu schützen, indem der Zugriff auf bösartige URLs und der Download bestimmter Inhalte blockiert wird.
- Windows Defender Antivirus (S. 368) – ermöglicht Ihnen, die Einstellungen des Windows Defenders zu verwalten, um Ihre Umgebung zu schützen.
- Microsoft Security Essentials (S. 371) – ermöglicht Ihnen, die Einstellungen der Microsoft Security Essentials zu verwalten, um Ihre Umgebung zu schützen.
- Schwachstellenbewertung (S. 385) – überprüft bestimmte Microsoft- und Drittthersteller-Produkte, die auf Ihren Maschinen installiert sind, auf Schwachstellen (Verwundbarkeiten, Sicherheitslücken) und benachrichtigt Sie, sofern welche gefunden werden.
- Patch-Verwaltung (S. 389) – ermöglicht Ihnen, für die Microsoft- und Drittthersteller-Produkte, die auf Ihren Maschinen installiert sind, Patches und Updates zu installieren, um die gefundenen Schwachstellen zu beheben.
- Data Protection-Karte (S. 409) – ermöglicht es Ihnen, bestimmte Daten zu ermitteln, um den Sicherungsstatus wichtiger Dateien zu überwachen.

Mit einem Schutzplan können Sie Ihre Datenquellen umfassend vor externen und internen Bedrohungen absichern. Indem Sie unterschiedliche Module (de)aktivieren und deren Modul-Einstellungen konfigurieren, können Sie flexible Pläne erstellen, die unterschiedliche Geschäftsanforderungen erfüllen.



13.1 Einen Schutzplan erstellen

Ein Schutzplan kann zum Zeitpunkt seiner Erstellung (oder später) auf mehrere Maschinen angewendet werden. Wenn Sie einen Plan erstellen, überprüft das System das Betriebssystem und

den Gerätetyp (z.B. Workstation, virtuelle Maschine etc.) und zeigt dann nur die Plan-Module an, die auf diese Geräte anwendbar sind.

Ein Schutzplan kann auf zwei Arten erstellt werden:

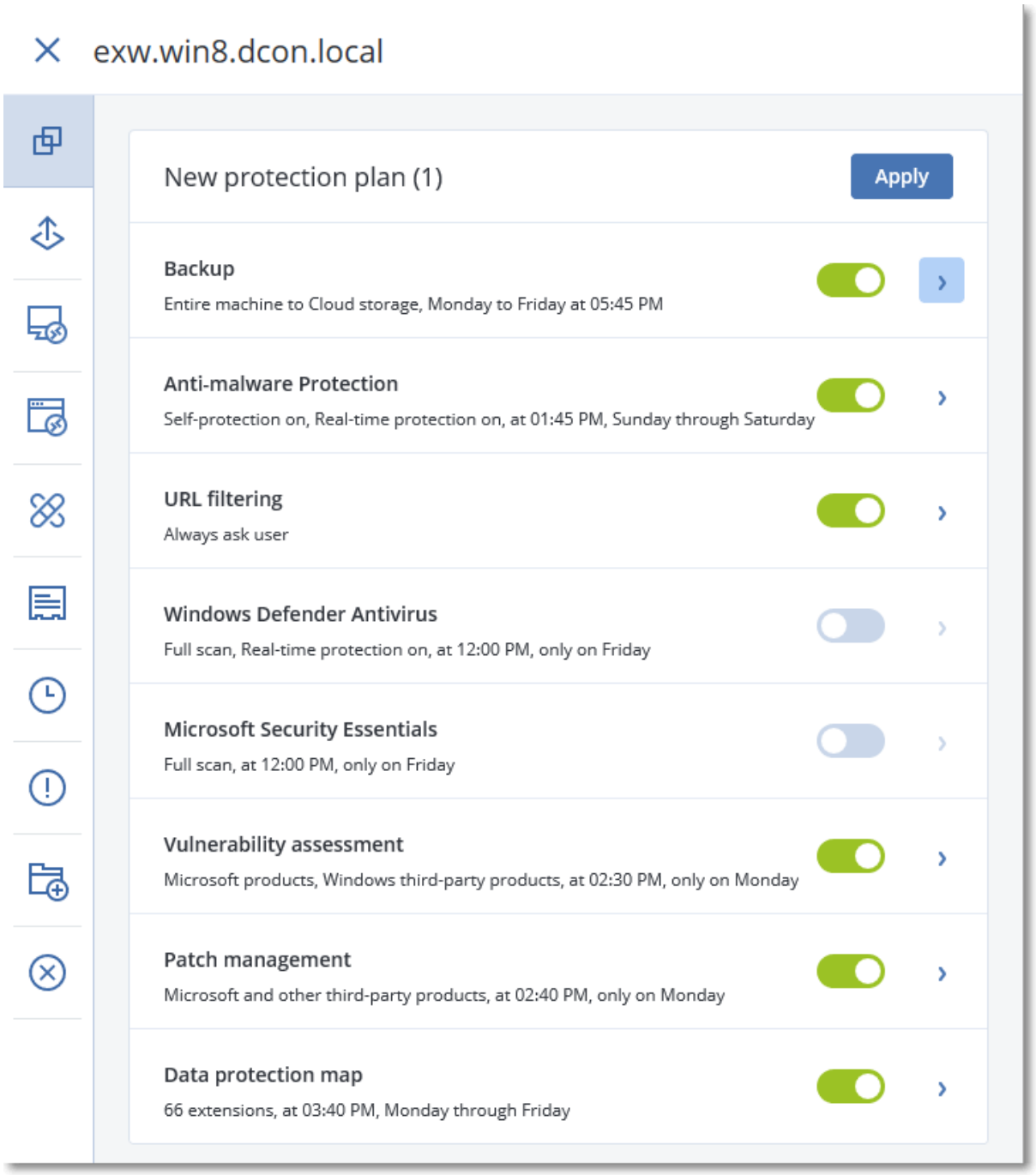
- Im Bereich **Geräte** – wenn Sie (ein) zu schützende(n) Gerät(e) auswählen und dann einen Plan für diese(s) erstellen.
- Im Bereich **Pläne** – wenn Sie einen Plan erstellen und dann die Maschinen auswählen, auf die er angewendet werden soll (S. 412).

Betrachten wir die erste Möglichkeit.

So können Sie den ersten Schutzplan erstellen

1. Gehen Sie in der Service-Konsole zu **Geräte** –> **Alle Geräte**.
2. Wählen Sie die Maschinen aus, die Sie sichern wollen.

3. Klicken Sie auf **Schützen** und dann auf **Plan erstellen**. Ihnen wird der Schutzplan mit den Standardeinstellungen angezeigt.



4. [Optional] Wenn Sie den Namen des Schutzplans ändern wollen, müssen Sie auf das Stiftsymbol neben dem Namen klicken.
5. [Optional] Wenn Sie das Plan-Modul (de)aktivieren wollen, müssen Sie auf den Schalter neben dem Namen des Moduls klicken.
6. [Optional] Wenn Sie die Modul-Parameter konfigurieren wollen, müssen Sie in den entsprechenden Bereich des Schutzplans klicken.
7. Klicken Sie, wenn Sie fertig sind, auf **Erstellen**.

Die Module für Backup, Antivirus & Antimalware Protection, Schwachstellenbewertung, Patch-Verwaltung und die Data Protection-Karte können bei Bedarf ausgeführt werden, indem Sie auf **Jetzt ausführen** klicken.

13.2 Standard-Schutzpläne

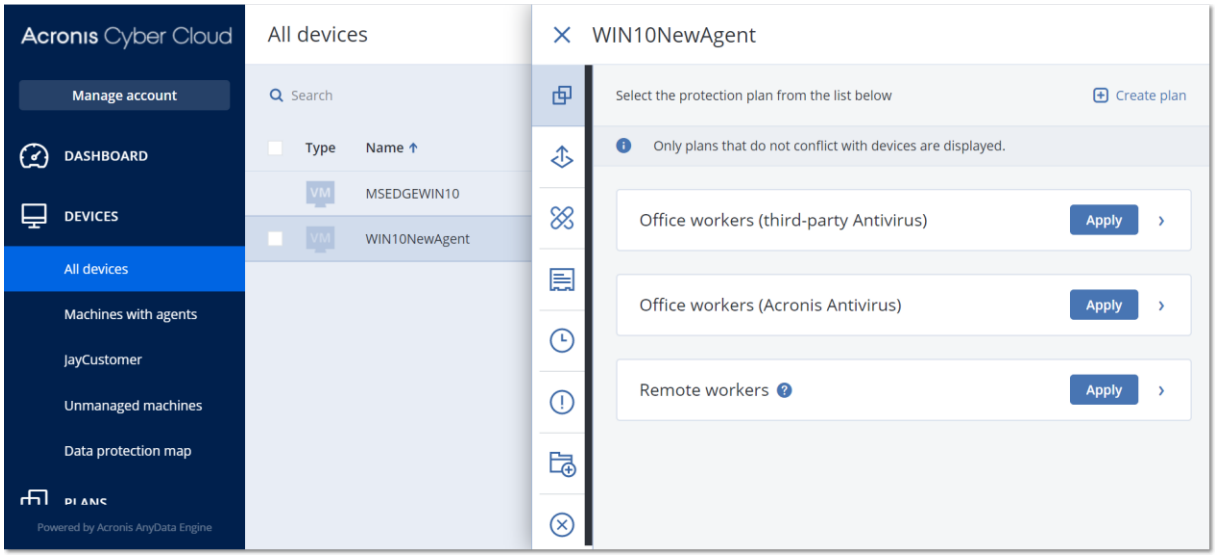
Drei vorkonfigurierte Pläne, die standardmäßig verfügbar sind, gewährleisten, dass Sie bestimmte Workloads schnell schützen können:

- Büro-Arbeiter (Acronis Antivirus)

  Dieser Plan ist für Benutzer optimiert, die im Büro arbeiten und bevorzugt die Acronis Antivirus-Software verwenden wollen.
- Büro-Arbeiter (Drittthersteller-Antivirus)

  Dieser Plan ist für Benutzer optimiert, die im Büro arbeiten und bevorzugt die Antivirus-Software eines Drittherstellers verwenden wollen. Der wesentliche Unterschied besteht darin, dass bei diesem Plan das **Antivirus & Antimalware Protection**-Modul und die **Active Protection**-Funktion deaktiviert sind.
- Remote-Arbeiter

  Dieser Plan ist speziell für Benutzer optimiert, die aus der Ferne (remote) arbeiten wollen. Er bietet häufigere Tasks (wie Backup, Antimalware Protection, Schwachstellenbewertung) , strengere Schutzaktionen sowie optimierte Performance- und Energieoptionen.



So können Sie einen Standard-Schutzplan anwenden

1. Gehen Sie in der Service-Konsole zu **Geräte** –> **Alle Geräte**.
2. Wählen Sie die Maschinen aus, die Sie sichern wollen.
3. Klicken Sie auf den Befehl **Schützen**.
4. Wählen Sie einen der Standardpläne aus und klicken Sie dann auf **Anwenden**.

   ***Tipp**: Sie können auch Ihren eigenen Schutzplan (S. 105) konfigurieren, indem Sie auf **Plan erstellen** klicken.*

So können Sie einen angewendeten Standard-Schutzplan modifizieren

1. Gehen Sie in der Service-Konsole zu **Pläne** –> **Schutz**.
2. Wählen Sie den zu ändernden 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 Einstellungen eines vorhandenen Schutzplans können nicht geändert werden.*

Standard-Plan-Optionen

Die vorkonfigurierten Pläne verwenden die Standardoptionen für jedes Module* – mit folgenden Modifikationen:

Module und Optionen/Plan	Büro-Arbeiter (Acronis Antivirus)	Büro-Arbeiter (Dritthersteller-Antivirus)	Remote-Arbeiter
Backup (S. 121)			
Backup-Quelle	Komplette Maschine	Komplette Maschine	Komplette Maschine
Kontinuierliche Datensicherung (CDP)	Deaktiviert	Deaktiviert	Aktiviert
Backup-Ziel	Cloud Storage	Cloud Storage	Cloud Storage
Backup-Schema	Nur inkrementell (Einzeldatei)	Nur inkrementell (Einzeldatei)	Nur inkrementell (Einzeldatei)
Planung	Standardmäßige tägliche Planung	Standardmäßige tägliche Planung	Täglich: Montag bis Freitag um 12:00 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
Aufbewahrungsdauer	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	Standardoptionen, plus: Performance und Backup-Fenster (der grüne Satz): ▪ CPU-Priorität: Niedrig ▪ Ausgabegeschwindigkeit: 50%
Antivirus & Antimalware Protection			
Scan planen	Scan-Typ: Schnell	n/a	Scan-Typ: Vollständig 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
URL-Filterung (S. 371)			
Zugriff auf schädliche Websites	Immer den Benutzer fragen	Immer den Benutzer fragen	Blockieren
Schwachstellenbewertung (S. 385)			
	Standard	Standard	Standard
Patch-Verwaltung (S. 389)			
Planung	Standard	Standard	Täglich: Montag bis Freitag um 14:20 Uhr
Vor-Update-Backup	Aus	Aus	An
Data Protection-Karte (S. 409)			

Erweiterungen	Standardoptionen	Standardoptionen	Standardoptionen, plus: **Bilder:** ▪ .bmp ▪ .png ▪ .ico ▪ .wbmp ▪ .gif ▪ .bmp ▪ .xcf ▪ .psd ▪ .tiff ▪ .jpeg, .jpg ▪ .dwg **Audio:** ▪ .wav ▪ .aif, .aifc, .aiff ▪ .au, .snd ▪ .mid, .midi ▪ .mid ▪ .mpga, .mp3 ▪ .oga ▪ .flac ▪ .oga ▪ .oga ▪ .opus ▪ .oga ▪ .spx ▪ .oga ▪ .ogg ▪ .ogx ▪ .ogx ▪ .mp4

* Die Anzahl der Module im Standard-Schutzplan kann zwischen den verschiedenen Editionen des Cyber Protection Service variieren.

13.3 Plan-Konflikte lösen

Ein Schutzplan kann sich in einem der folgenden Statuszustände befinden:

- **Aktiv** – ein Plan, der Geräten zugewiesen wurde und auf diesen ausgeführt wird.
- **Inaktiv** – ein Plan, der Geräten zugewiesen wurde, aber deaktiviert ist und nicht auf diesen ausgeführt wird.

Mehrere Pläne auf ein Gerät anwenden

Sie können mehrere Schutzpläne auf ein einzelnes Gerät anwenden. Als Ergebnis erhalten Sie eine Kombination aus verschiedenen Schutzplänen, die einem einzigen Gerät zugewiesen wurden. Sie können beispielsweise einen Plan anwenden, in dem nur das Antivirus & Antimalware Protection-Modul aktiviert ist, und einen weiteren Plan, der nur das Backup-Modul enthält. Die Schutzpläne können nur dann kombiniert werden, wenn Sie Module haben, deren Funktionalitäten sich nicht überschneiden. Wenn in den angewendeten Schutzplänen Module mit ähnlicher Funktionalität aktiviert sind, müssen Sie die entstehenden Konflikte zwischen diesen Modulen lösen.

Plan-Konflikte lösen

Plan-Konflikte mit bereits angewendeten Plänen

Wenn Sie einen neuen Plan auf einem oder mehreren Geräten mit bereits angewendeten Plänen erstellen, die mit dem neu erstellten Plan in Konflikt stehen, können Sie den Konflikt auf eine der folgenden Arten lösen:

- Erstellen Sie einen neuen Plan, wenden Sie diesen an und deaktivieren Sie alle bereits angewendeten Pläne, die einen Konflikt verursachen.
- Erstellen Sie einen neuen Plan und deaktivieren Sie diesen.

Wenn Sie einen Plan auf einem oder mehreren Geräten mit bereits angewendeten Plänen bearbeiten, die mit den gemachten Änderungen zu einem Konflikt führen, können Sie den Konflikt auf eine der folgenden Arten lösen:

- Speichern Sie die Änderungen am Plan und deaktivieren Sie alle bereits angewendeten Pläne mit Konflikten.
- Speichern Sie die Änderungen am Plan und deaktivieren Sie ihn.

Ein Geräteplan steht im Konflikt mit einem Gruppenplan

Wenn ein Gerät zu einer Gerätegruppe mit zugewiesenem Gruppenplan gehört und Sie versuchen, einem Gerät einen neuen Plan zuzuweisen, wird Sie das System auffordern, den Konflikt auf eine der folgenden Arten zu lösen:

- Entfernen Sie ein Gerät aus der Gruppe und wenden Sie einen neuen Plan auf das Gerät an.
- Wenden Sie einen neuen Plan auf die komplette Gruppe an oder bearbeiten Sie den aktuellen Gruppenplan.

Lizenzproblem

Die auf einem Gerät zugewiesene Quota muss passend für den Schutzplan sein, damit dieser ausgeführt, aktualisiert oder angewendet werden kann. Führen Sie einen der folgenden Schritte aus, um das Lizenzproblem zu beheben:

- Deaktivieren Sie die Module, die von der zugewiesenen Quota nicht unterstützt werden, und verwenden Sie dann den Schutzplan weiter.
- Ändern Sie die zugewiesene Quota manuell: gehen Sie zu **Geräte** –> **<bestimmtes_Gerät>** –> **Details** –> **Service-Quota**, widerrufen Sie die vorhandene Quota und weisen Sie dann eine neue zu.

13.4 Aktionen mit Schutzplänen

Verfügbare Aktionen für einen Schutzplan

Sie können die folgenden Aktionen mit einem Schutzplan durchführen:

- Einen Plan umbenennen
- Module (de)aktivieren und die einzelnen Modul-Einstellungen bearbeiten
- Einen Plan (de)aktivieren
- Geräten oder einer Gruppe von Geräten einen Plan zuweisen
- Einen Plan von Geräten widerrufen
- Einen Plan importieren/exportieren

  ***Hinweis**: Sie können nur Schutzpläne importieren, die in Cyber Protection 9.0 erstellt wurden. Pläne, die in früheren Produkversionen erstellt wurden, sind mit Version 9.0 nicht kompatibel.*

- Einen Plan löschen

So können Sie einen vorhandenen Schutzplan anwenden

1. Wählen Sie die Maschinen aus, die Sie sichern wollen.
2. Klicken Sie auf den Befehl **Schützen**. Sollte auf die ausgewählten Maschinen bereits ein Schutzplan angewendet worden sein, dann klicken Sie auf **Plan hinzufügen**.
3. Die Software zeigt die bisher erstellten Schutzpläne an.
4. Wählen Sie einen Schutzplan aus, der angewendet werden soll, und klicken Sie dann auf **Anwenden**.

So können Sie einen Schutzplan bearbeiten

1. Wenn Sie den Schutzplan für alle Maschinen (auf die er angewendet wird) bearbeiten wollen, wählen Sie eine dieser Maschinen aus. Alternativ können Sie auch die Maschinen auswählen, für die Sie den Schutzplan bearbeiten wollen.
2. Klicken Sie auf den Befehl **Schützen**.
3. Wählen Sie den Schutzplan aus, den Sie bearbeiten wollen.
4. Klicken Sie neben dem Namen des Schutzplans auf das Drei-Punkte-Symbol und anschließend auf den Befehl **Bearbeiten**.
5. Wenn Sie die Plan-Parameter ändern wollen, klicken Sie auf den entsprechenden Schutzplan-Fensterbereich.
6. Klicken Sie auf **Änderungen speichern**.
7. Wenn Sie den Schutzplan für alle Maschinen (auf die er angewendet wird) ändern wollen, klicken Sie auf **Änderungen auf diesen Schutzplan anwenden**. Klicken Sie alternativ auf **Einen neuen Schutzplan nur für die ausgewählten Geräte erstellen**.

So widerrufen Sie die Anwendung einen Schutzplans auf bestimmte Maschinen

1. Wählen Sie die Maschinen aus, für die Sie die Anwendung des Schutzplans widerrufen wollen.
2. Klicken Sie auf den Befehl **Schützen**.

3. Falls mehrere Schutzpläne auf die Maschinen angewendet werden, wählen Sie denjenigen Schutzplan aus, dessen Anwendung Sie widerrufen wollen.
4. Klicken Sie neben dem Namen des Schutzplans auf das Drei-Punkte-Symbol und anschließend auf den Befehl **Widerrufen**.

So können Sie einen Schutzplan löschen

1. Wählen Sie irgendeine Maschine aus, auf die der zu löschende Schutzplan angewendet wird.
2. Klicken Sie auf den Befehl **Schützen**.
3. Falls mehrere Schutzpläne auf die Maschine angewendet werden, wählen Sie denjenigen Schutzplan aus, den Sie löschen wollen.
4. Klicken Sie neben dem Namen des Schutzplans auf das Drei-Punkte-Symbol und anschließend auf den Befehl **Löschen**.

   Der Schutzplan wird daraufhin zuerst auf allen Maschinen widerrufen und dann vollständig von der Weboberfläche gelöscht.

14 #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 drei 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 AV-Test oder AV-Comparatives zurückgreifen, wenn Sie eine Liste von empfohlenen Antimalware-Lösungen einsehen wollen.	275 – auf einer Maschine ist eine Antimalware-Software installiert 0 – auf einer Maschine ist keine Antimalware-Software installiert
Backup	Der Agent überprüft, ob auf der 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: Ihnen wird empfohlen, Ihre Daten regelmäßig per Backup zu 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. 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.	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) ▪ 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: Es wird empfohlen, 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	100 – die öffentliche Windows-Firewall ist aktiviert 75 – die private Windows-Firewall ist aktiviert 175 – die öffentliche und 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 Drittherstellers 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: Es wird empfohlen, 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 ▪ VyprVPN ▪ IPVanish VPN ▪ Hotspot Shield VPN ▪ Fortigate VPN ▪ ZYXEL VPN ▪ SonicWall GVPN ▪ LANCOM VPN	75 – ein VPN ist aktiviert und wird ausgeführt 0 – kein VPN ist aktiviert

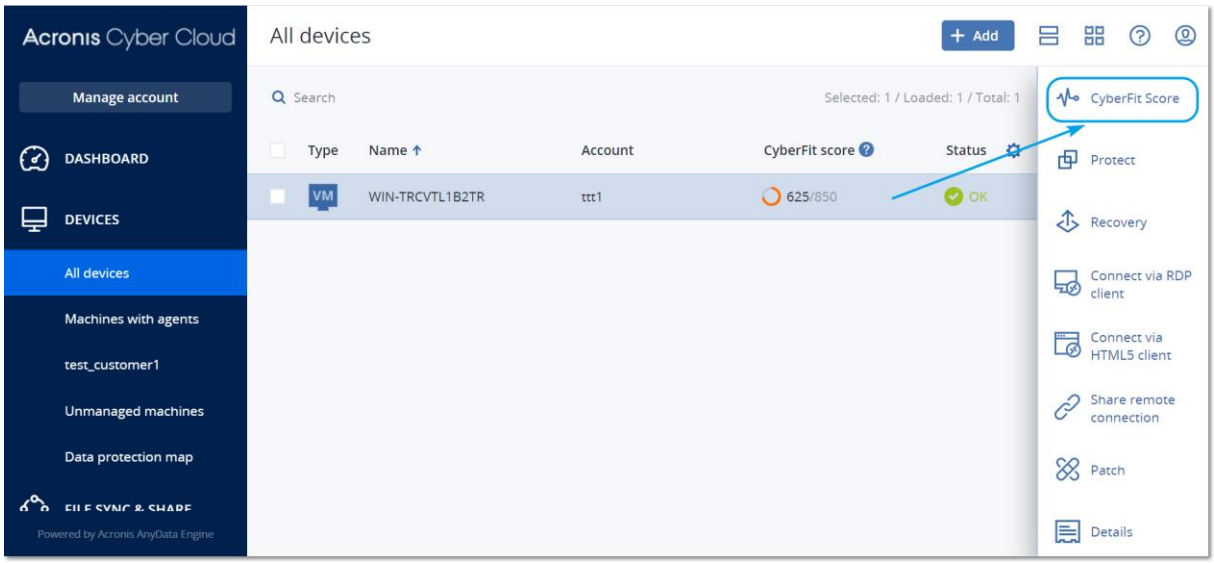
Laufwerksverschlüsselung	Der Agent überprüft, ob für Ihre Maschine eine Laufwerksverschlüsselung aktiviert ist. Der Agent überprüft, ob Windows BitLocker eingeschaltet ist.	Ergebnisse: ▪ Sie haben eine vollständige Laufwerksverschlüsselung aktiviert, Ihre Maschine ist vor physischen Manipulationen geschützt (+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: Es wird empfohlen, 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 eingeschränkt hat.	Ergebnisse: ▪ Ausgehender NTLM-Traffic zu Remote-Servern wird verweigert; Ihre 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: Es wird empfohlen, den ausgehenden NTLM-Traffic zu Remote-Servern zu verweigern, um einen besseren Sicherheitsschutz zu erreichen. 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	25 – der ausgehende NTML-Traffic ist auf 'Alle verweigern' 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 Service-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.



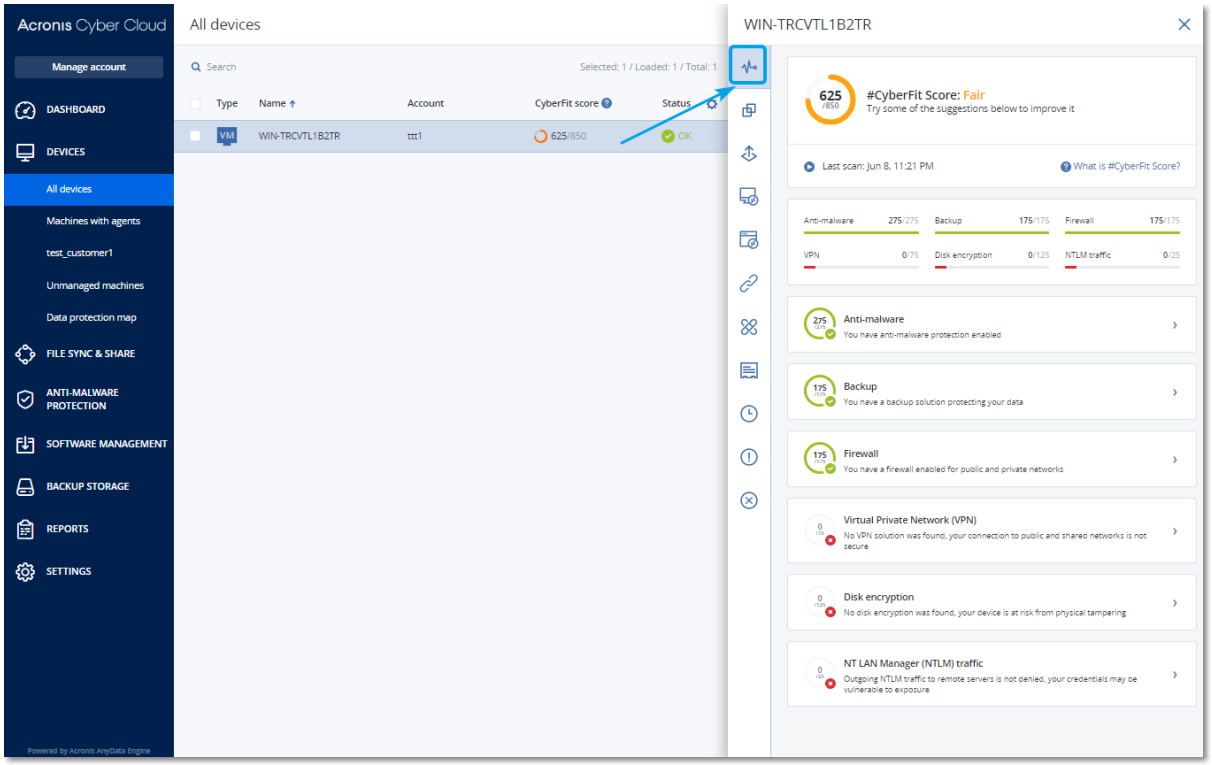
Außerdem können Sie Informationen über den #CyberFit-Score auf den entsprechenden Seiten 'Widget (p. 418)' und/oder 'Bericht (p. 430)' erhalten.

14.1 Einen #CyberFit-Score-Scan ausführen

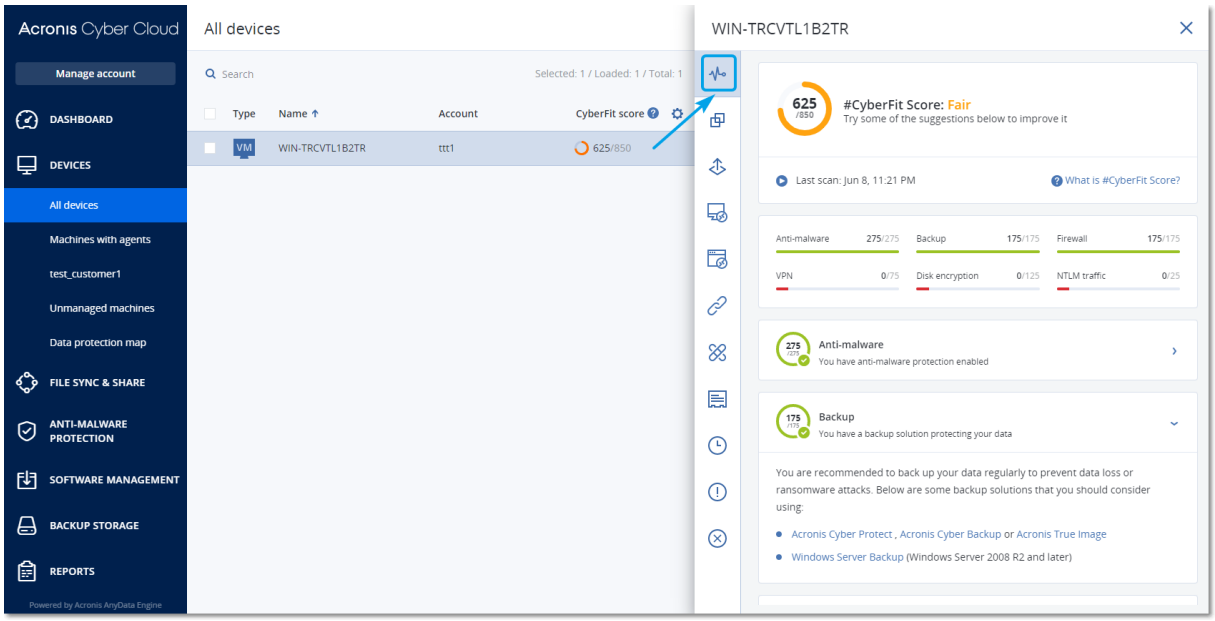
So können Sie einen #CyberFit-Score-Scan ausführen

1. Gehen Sie in der Service-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 ausführen**.

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.

15 Backup und Recovery

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.

15.1 Backup

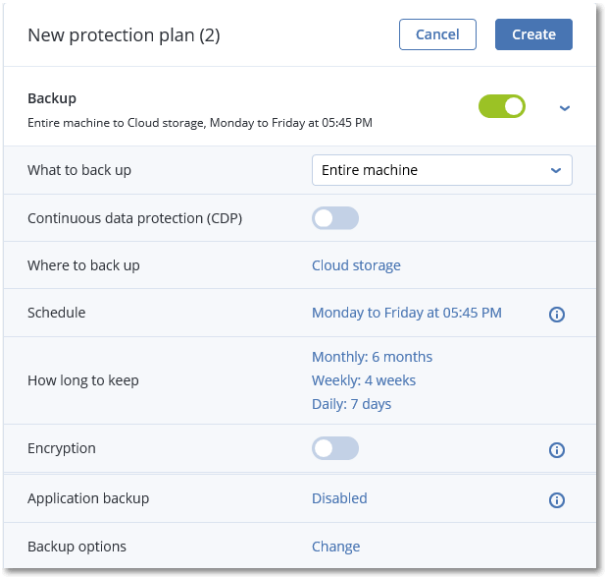
Ein Schutzplan mit einem aktivierten Backup-Modul ist ein Satz von Regeln, die spezifizieren, wie bestimmte Daten auf einer bestimmten Maschine gesichert werden sollen.

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**.

   Die Software zeigt die Schutzpläne an, die auf die Maschine angewendet werden. 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.

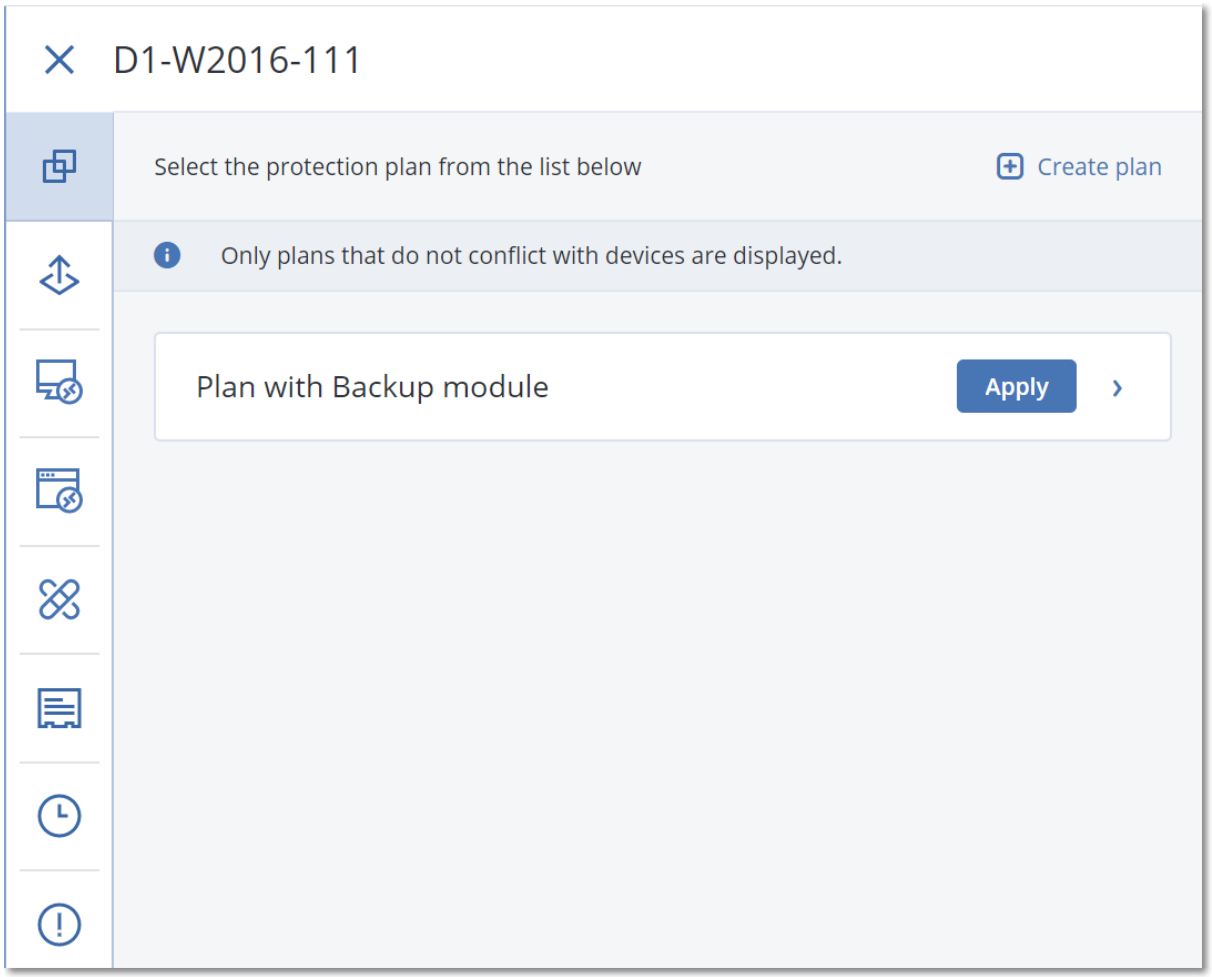


4. [Optional] Wenn Sie den Namen des Schutzplans ändern wollen, klicken Sie auf den vorgegebenen Standardnamen.
5. [Optional] Wenn Sie Parameter des Backup-Moduls ändern wollen, klicken Sie im Fensterbereich des Schutzplans auf die gewünschte Einstellung.
6. [Optional] Wenn Sie die Backup-Optionen ändern 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**.

15.2 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 (S. 436))	Direkte Auswahl Richtlinienregeln Dateifilter (S. 168)	Cloud (S. 136) Lokaler Ordner (S. 136) Netzwerkordner (S. 136) NFS (S. 136)* Secure Zone (S. 136)**	Nur inkrementell (Einzeldatei) (S. 140) Nur vollständig (S. 140) Wöchentlich vollständig, täglich inkrementell (S. 140) Monatlich vollständig,	Nach Backup-Alter (einzelne Regel/per Backup-Set) (S. 150) Nach Backup-Anzahl (S. 150) Nach der

<table>
<tr><th colspan="2">BACKUP-QUELLE</th><th>Elemente für das Backup
Auswahlmethoden</th><th>Backup-Ziel</th><th>Planung
Backup-Schemata</th><th>Aufbewahrungsdauer</th></tr>
<tr><td colspan="2">Laufwerke/Volumes (virtuelle Maschinen (S. 437))</td><td>Richtlinienregeln
Dateifilter (S. 168)</td><td>Cloud (S. 136)
Lokaler Ordner (S. 136)
Netzwerkordner (S. 136)
NFS (S. 136)*</td><td>wöchentlich differentiell, täglich inkrementell (GVS) (S. 140)
Benutzerdefiniert (V-D-I) (S. 140)</td><td rowspan="13">Gesamtgröße der Backups (S. 150)***
Unbegrenzt aufbewahren (S. 150)</td></tr>
<tr><td colspan="2">Dateien (nur physische Maschinen (S. 436))</td><td>Direkte Auswahl
Richtlinienregeln
Dateifilter (S. 168)</td><td>Cloud (S. 136)
Lokaler Ordner (S. 136)
Netzwerkordner (S. 136)
NFS (S. 136)*
Secure Zone (S. 136)**</td><td rowspan="3">Nur inkrementell (Einzeldatei) (S. 140)
Nur vollständig (S. 140)
Wöchentlich vollständig, täglich inkrementell (S. 140)
Monatlich vollständig, wöchentlich differentiell, täglich inkrementell (GVS) (S. 140)
Benutzerdefiniert (V-D-I) (S. 140)</td></tr>
<tr><td colspan="2">ESXi-Konfiguration</td><td>Direkte Auswahl</td><td>Lokaler Ordner (S. 136)
Netzwerkordner (S. 136)
NFS (S. 136)*</td></tr>
<tr><td colspan="2">Websites (Dateien und MySQL-Datenbanken)</td><td>Direkte Auswahl (S. 292)</td><td>Cloud (S. 136)</td><td>—</td></tr>
<tr><td colspan="2">Systemzustand</td><td>Direkte Auswahl (S. 129)</td><td rowspan="3">Cloud (S. 136)
Lokaler Ordner (S. 136)
Netzwerkordner (S. 136)</td><td rowspan="3">Nur vollständig (S. 140)
Wöchentlich vollständig, täglich inkrementell (S. 140)
Benutzerdefiniert (V-I) (S. 140)</td></tr>
<tr><td colspan="2">SQL-Datenbanken</td><td>Direkte Auswahl</td></tr>
<tr><td colspan="2">Exchange-Datenbanken</td><td>Direkte Auswahl (S. 227)</td></tr>
<tr><td rowspan="5">Microsoft Office 365</td><td>Postfächer (lokaler Agent für Office 365)</td><td>Direkte Auswahl</td><td>Cloud (S. 136)
Lokaler Ordner (S. 136)
Netzwerkordner (S. 136)</td><td>Nur inkrementell (Einzeldatei) (S. 140)</td></tr>
<tr><td>Postfächer (lokaler Agent für Office 365)</td><td>Direkte Auswahl (S. 258)</td><td rowspan="4">Cloud (S. 136)</td><td rowspan="4">—</td></tr>
<tr><td>Öffentliche Ordner</td><td>Direkte Auswahl (S. 258)</td></tr>
<tr><td>OneDrive-Dateien</td><td>Direkte Auswahl (S. 263)
Richtlinienregeln (S. 263)</td></tr>
<tr><td>SharePoint Online-Daten</td><td>Direkte Auswahl (S. 267)
Richtlinienregeln (S. 267)</td></tr>
</table>

BACKUP-QUELLE		Elemente für das Backup Auswahlmethoden	Backup-Ziel	Planung Backup-Schemata	Aufbewahrungsdauer
	Teams	Direkte Auswahl (S. 270)			
G Suite	Gmail-Postfächer	Direkte Auswahl (S. 280)	Cloud (S. 136)	—	
	Google Drive-Dateien	Direkte Auswahl (S. 284) Richtlinienregeln (S. 284)			
	Shared Drive-Dateien	Direkte Auswahl (S. 288) Richtlinienregeln (S. 288)			

* 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.

15.3 Daten für ein Backup auswählen

15.3.1 Laufwerke/Volumes auswählen

Ein Backup auf Laufwerksebene (kurz 'Laufwerk-Backup') enthält eine Kopie der Daten eines Laufwerks/Volumes – und zwar in 'gepackter' Form. Sie können aus einem solchen Laufwerk-Backup sowohl einzelne Laufwerke/Volumes wie auch einzelne Dateien/Ordner wiederherstellen. Unter dem 'Backup einer kompletten Maschine' versteht man ein Backup, das alle festeingebauten Laufwerke (interne „Nicht-Wechsellaufwerke“) der betreffenden Maschine umfasst.

Laufwerke, die über das iSCSI-Protokoll mit einer physischen Maschine verbunden sind, können ebenfalls per Backup gesichert werden. Es gibt jedoch Einschränkungen (S. 22), wenn Sie den Agenten für VMware oder den Agenten für Hyper-V verwenden, um per iSCSI verbundene Laufwerke zu sichern.

Es gibt zwei Möglichkeiten, wie Sie Laufwerke/Volumes auswählen können: direkt (manuell) auf jeder Maschine oder mithilfe von Richtlinienregeln. Es besteht die Möglichkeit, bestimmte Dateien durch die Festlegung von Dateifiltern (S. 168) von einem Laufwerk-Backup auszuschließen.

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 jede der im Schutzplan enthaltenen Maschinen die entsprechenden Kontrollkästchen neben den zu sichernden Laufwerken/Volumes.
5. Klicken Sie auf **Fertig**.

Richtlinienregeln verwenden

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).

   Die Richtlinienregeln werden auf alle Maschinen angewendet, die im Schutzplan enthalten sind. Wenn (beim Start des Backups) auf einer Maschine keine Daten gefunden werden, die den definierten Regeln entsprechen, so wird das Backup auf dieser Maschine fehlschlagen.
5. Klicken Sie auf **Fertig**.

Regeln für Windows, Linux und macOS

- Der Parameter **[All Volumes]** wählt bei Maschinen, die unter Windows laufen, alle Volumes aus – und bei Maschinen, die unter Linux oder macOS laufen, alle gemounteten Volumes.

Regeln für Windows

- Ein Laufwerksbuchstabe (beispielsweise **C:**) wählt das Volume mit eben diesem Laufwerksbuchstaben aus.
- **[Fixed Volumes (physical machines)]** wählt bei physischen Maschinen 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. Diese Kombination entspricht dem minimalen Datensatz, der für die Wiederherstellbarkeit eines Betriebssystems aus einem Backup notwendig ist.
- Der Parameter **[Disk 1]** wählt das erste Laufwerk der betreffenden Maschine aus (einschließlich aller Volumes auf diesem Laufwerk). Um ein anderes Laufwerk auszuwählen, müssen Sie nur die entsprechende Laufwerksnummer eingeben.

Regeln für Linux

- Der Parameter **/dev/hda1** wählt das erste Volume auf dem ersten IDE-Laufwerk aus.
- Der Parameter **/dev/sda1** wählt das erste Volume auf dem ersten SCSI-Laufwerk aus.
- Der Parameter **/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. Geben Sie Folgendes ein, um diese Volumes per Backup zu sichern:

/dev/mapper/vg_1-lv1
/dev/mapper/vg-l-lv2

Regeln für macOS

- **[Disk 1]** wählt das erste Laufwerk der betreffenden Maschine aus (einschließlich aller Volumes auf diesem Laufwerk). Um ein anderes Laufwerk auszuwählen, müssen Sie nur die entsprechende Laufwerksnummer eingeben.

15.3.1.1 Was speichert das Backup eines Laufwerks oder Volumes?

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 (S. 188) '**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 (S. 190) **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.

15.3.2 Dateien/Verzeichnisse auswählen

Datei-Backups sind für physische und virtuelle Maschinen verfügbar, die von einem Agenten gesichert werden, der im Gastbetriebssystem installiert ist. Dateien und Ordner, die sich auf Laufwerken befinden, die über das iSCSI-Protokoll mit einer physischen Maschine verbunden sind, können ebenfalls per Backup gesichert werden. Es gibt jedoch Einschränkungen (S. 22), wenn Sie den Agenten für VMware oder den Agenten für Hyper-V verwenden, um Daten auf Laufwerken zu sichern, die per iSCSI angeschlossen sind.

Ein dateibasiertes Backup ist zur Wiederherstellung eines Betriebssystems nicht ausreichend geeignet. Verwenden Sie ein Datei-Backup, wenn Sie nur bestimmte Daten (beispielsweise ein aktuelles Projekt) sichern wollen. Sie können so die Backup-Größe verringern bzw. Speicherplatz sparen.

Es gibt zwei Möglichkeiten, wie Sie Dateien auswählen können: direkt (manuell) auf jeder Maschine oder mithilfe von Richtlinienregeln. Bei beiden Methoden können Sie die Auswahl durch die Festlegung von Dateifiltern (S. 168) noch verfeinern.

Direkte Auswahl

1. Wählen Sie bei **Backup-Quelle** die Option **Dateien/Ordner**.
2. Spezifizieren Sie die **Elemente für das Backup**.
3. Wählen Sie bei **Elemente für das Backup auswählen** die Option **Direkt**.
4. Für jede der im Schutzplan enthaltenen Maschinen:
   a. Klicken Sie auf **Dateien und Ordner auswählen**.
   b. Klicken Sie auf **Lokaler Ordner** oder **Netzwerkordner**.
      Die Freigabe muss von der ausgewählten Maschine aus zugreifbar sein.
   c. Bestimmen Sie (über 'Durchsuchen') die gewünschten Dateien/Ordner oder geben Sie den Pfad manuell ein – und klicken Sie dann auf die Schaltfläche mit dem Pfeil. Spezifizieren Sie bei Aufforderung die Anmeldedaten (Benutzernamen, Kennwort), um auf den freigegebenen Ordner zugreifen zu können.
      Ein Backup von Ordnern mit anonymem Zugriff wird nicht unterstützt.
   d. Wählen Sie die gewünschten Dateien/Ordner aus.
   e. Klicken Sie auf **Fertig**.

Richtlinienregeln verwenden

1. Wählen Sie bei **Backup-Quelle** die Option **Dateien/Ordner**.
2. Spezifizieren Sie die **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).

   Die Richtlinienregeln werden auf alle Maschinen angewendet, die im Schutzplan enthalten sind. Wenn (beim Start des Backups) auf einer Maschine keine Daten gefunden werden, die den definierten Regeln entsprechen, so wird das Backup auf dieser Maschine fehlschlagen.
5. Klicken Sie auf **Fertig**.

Auswahlregeln für Windows

- Vollständiger Pfad zu einer Datei oder einem Ordner, beispielsweise **D:\Arbeit\Text.doc** oder **C:\Windows**.
- Templates:
  - Der Parameter **[All Files]** wählt alle Dateien auf allen Volumes der betreffenden Maschine aus.
  - Der Parameter **[All Profiles Folder]** wählt die Benutzerordner aller Benutzerprofile aus (üblicherweise **C:\Benutzer** (evtl. 'C:\Users' direkt im Dateisystem) oder **C:\Dokumente und Einstellungen**).
- Umgebungsvariablen:
  - Der Parameter **%ALLUSERSPROFILE%** wählt die Ordner der 'Gemeinsamen Daten' aller Benutzerprofile aus (üblicherweise **C:\ProgramData** oder **C:\Dokumente und Einstellungen\All Users**).
  - Der Parameter **%PROGRAMFILES%** wählt den Systemordner 'Programme' aus (beispielsweise **C:\Programme**).
  - Der Parameter **%WINDIR%** wählt den Systemordner von Windows aus (beispielsweise **C:\Windows**).

  Sie können auch andere Umgebungsvariablen oder eine Kombination von Umgebungsvariablen und Text verwenden. Geben Sie beispielsweise Folgendes ein, wenn Sie den Ordner 'Java' im Systemordner 'Programme' auswählen wollen: **%PROGRAMFILES%\Java**.

Auswahlregeln für Linux

- Vollständiger Pfad für eine Datei oder ein Verzeichnis. Beispiel: um **datei.txt** auf dem Volume **/dev/hda3** zu sichern, welches wiederum unter **/home/usr/docs** gemountet ist, können Sie entweder die Befehlszeile **/dev/hda3/datei.txt** oder **/home/usr/docs/datei.txt** spezifizieren.
  - **/home** wählt das Home-Verzeichnis der allgemeinen Benutzer aus.
  - **/root** wählt das Home-Verzeichnis des Benutzers 'root' aus.
  - Der Parameter **/usr** wählt das Verzeichnis für alle benutzerbezogenen Programme aus.
  - **/etc** wählt das Verzeichnis der Systemkonfigurationsdateien aus.
- Templates:
  - **[All Profiles Folder]** wählt **/home** aus Dies ist der Ordner, in dem sich standardmäßig alle Benutzerprofile befinden.

Auswahlregeln für macOS

- Vollständiger Pfad für eine Datei oder ein Verzeichnis.
- Templates:

- **`[All Profiles Folder]`** wählt **/Users** aus Dies ist der Ordner, in dem sich standardmäßig alle Benutzerprofile befinden.

Beispiele:

- Um **datei.txt** auf Ihrem Desktop zu sichern, müssen Sie die Befehlszeile **/Users/<Benutzername>/Desktop/datei.txt** spezifizieren, wobei <Benutzername> für Ihren eigenen Benutzernamen steht.
- Spezifizieren Sie **/Users**, wenn Sie die Home-Verzeichnisse aller Benutzer sichern wollen.
- Spezifizieren Sie **/Applications**, wenn Sie das Verzeichnis sichern wollen, in dem alle Programme installiert sind.

15.3.3 Einen Systemzustand auswählen

Ein Backup des Systemzustands ist für Maschinen verfügbar, die unter Windows Vista oder einer neuere Windows-Version laufen.

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

15.3.4 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 VMware vSphere 6.7 unterstützt.
- 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.

15.4 Kontinuierliche Datensicherung (CDP)

Backups werden üblicherweise mit regelmäßigen, aber – aus Performance-Gründen – recht langen Zeitintervallen durchgeführt. Wenn das System plötzlich beschädigt wird, gehen die Daten, die in dem Zeitraum zwischen dem letzten (neuesten) Backup und dem Systemausfall geändert wurden, verloren.

Die Funktion **Kontinuierliche Datensicherung (CDP)** (CDP für die ebenfalls übliche englische Bezeichnung 'Continuous Data Protection') ermöglicht Ihnen, ausgewählte Daten zwischen den geplanten Backups auf kontinuierlicher Basis zu sichern.

- Indem spezifizierte Dateien/Ordner auf Änderungen überwacht werden
- Indem die Dateien von spezifizierten Applikationen auf Änderungen überwacht werden

Wenn Sie Daten für ein Backup ausgewählt haben, können Sie aus diesen dann bestimmte Dateien festlegen, die kontinuierlich gesichert werden sollen. Das System wird dann jede Änderung an diesen Dateien per Backup sichern. Sie können diese Dateien dann auf den Zeitpunkt ihrer letzten Änderung zurückzusetzen/wiederherstellen.

Derzeit wird die **Kontinuierliche Datensicherung (CDP)** für folgende Betriebssysteme unterstützt:

- Windows 7 und höher
- Windows Server 2008 R2 und höher

Das unterstützte Dateisystem: nur NTFS , nur lokale Ordner (freigegebene Netzwerkordner werden nicht unterstützt).

Die Option **Kontinuierliche Datensicherung (CDP)** ist nicht mit der Option **Applikations-Backup** kompatibel.

Und so funktioniert es

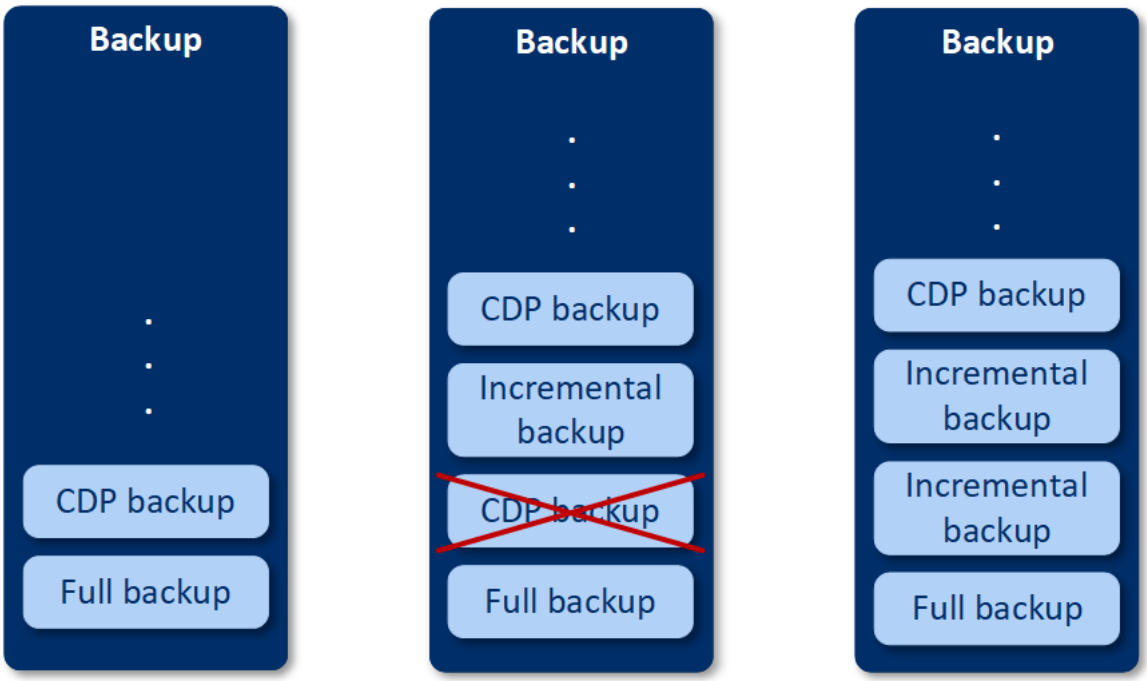
Wir bezeichnen ein solches, auf kontinuierlicher Basis erstelltes Backup ein CDP-Backup. Damit ein CDP-Backup erstellt werden kann, muss zuvor bereits ein vollständiges oder inkrementelles Backup erstellt worden sein.

Wenn Sie den Schutzplan mit dem Backup-Modul zum ersten Mal ausführen und die Option **Kontinuierliche Datensicherung (CDP)** aktiviert ist, wird zuerst ein Voll-Backup erstellt. Direkt anschließend wird das CDP-Backup für die ausgewählten oder geänderten Dateien/Ordner erstellt.

Die von Ihnen ausgewählten Daten sind im CDP-Backup immer im letzten (jüngsten) Zustand enthalten. Wenn Sie Änderungen an den ausgewählten Dateien/Ordnern vornehmen, wird kein neues CDP-Backup erstellt, sondern werden alle Änderungen im selben CDP-Backup aufgezeichnet.

Wenn der Zeitpunkt für das geplante inkrementelle Backup kommt, wird das bisher erstellte CDP-Backup verworfen und – nachdem das inkrementelle Backup durchgeführt wurde – ein neues CDP-Backup erstellt.

Auf diese Weise bleibt das CDP-Backup immer die letzte Sicherung in der Backup-Kette und enthält jeweils den aktuellsten Stand der geschützten Dateien/Ordner.



Wenn Sie bereits einen Schutzplan mit aktiviertem Backup-Modul haben und Sie beschließen, die **Kontinuierliche Datensicherung (CDP)** zu aktivieren, wird das CDP-Backup direkt nach Aktivierung dieser Option erstellt, weil die vorhandene Backup-Kette ja bereits Voll-Backups hat.

Datenquellen und Backup-Ziele, die für die kontinuierliche Datensicherung (CDP) unterstützt werden

Damit die kontinuierliche Datensicherung (CDP) richtig funktionieren kann, müssen Sie die folgenden Elemente für die folgenden Datenquellen spezifizieren:

Backup-Quelle	Elemente für das Backup
Komplette Maschine	Entweder Dateien/Ordner oder Applikationen müssen spezifiziert werden
Laufwerke/Volumes	Laufwerke/Volumes und entweder Dateien/Ordner oder Applikationen müssen spezifiziert werden
Dateien/Ordner	Dateien/Ordner müssen spezifiziert werden Applikationen können spezifiziert werden (nicht obligatorisch)

Folgende Backup-Ziele werden für die kontinuierliche Datensicherung (CDP) unterstützt:

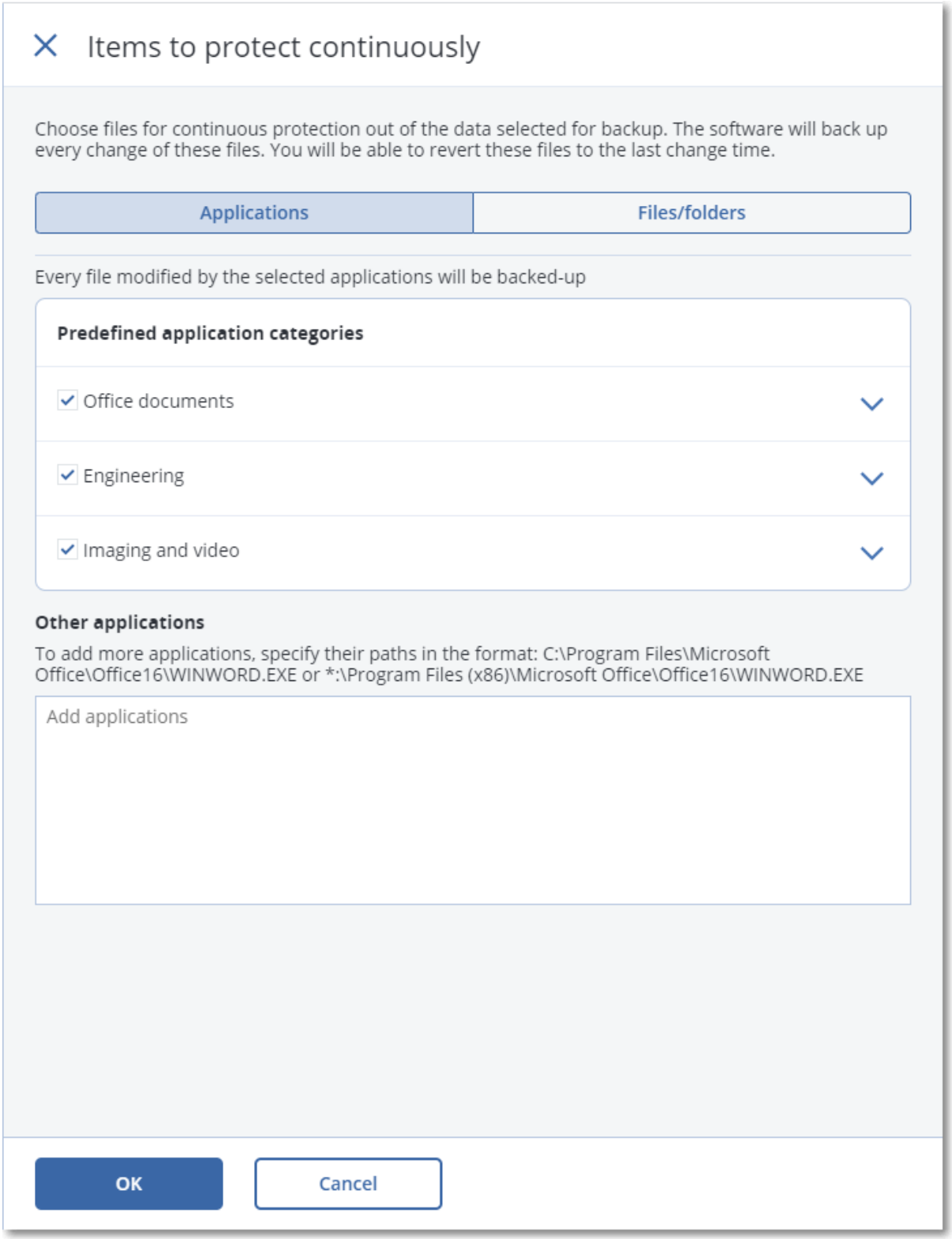
- Lokaler Ordner
- Netzwerkordner

- Per Skript festgelegter Speicherort
- Cloud Storage
- Acronis Cyber Infrastructure

So können Sie Geräte mit der kontinuierlichen Datensicherung (CDP) schützen

1. Erstellen Sie in der Service-Konsole einen Schutzplan (S. 105) mit aktiviertem **Backup**-Modul.
2. Aktivieren Sie die Option **Kontinuierliche Datensicherung (CDP)**.
3. Spezifizieren Sie die **Elemente, die kontinuierlich geschützt werden sollen**:

- **Applikationen** (jede Datei, die von den ausgewählten Applikationen geändert wird, wird gesichert). Wir empfehlen diese Option, wenn Sie Ihre Office-Dokumente per CDP-Backup schützen wollen.



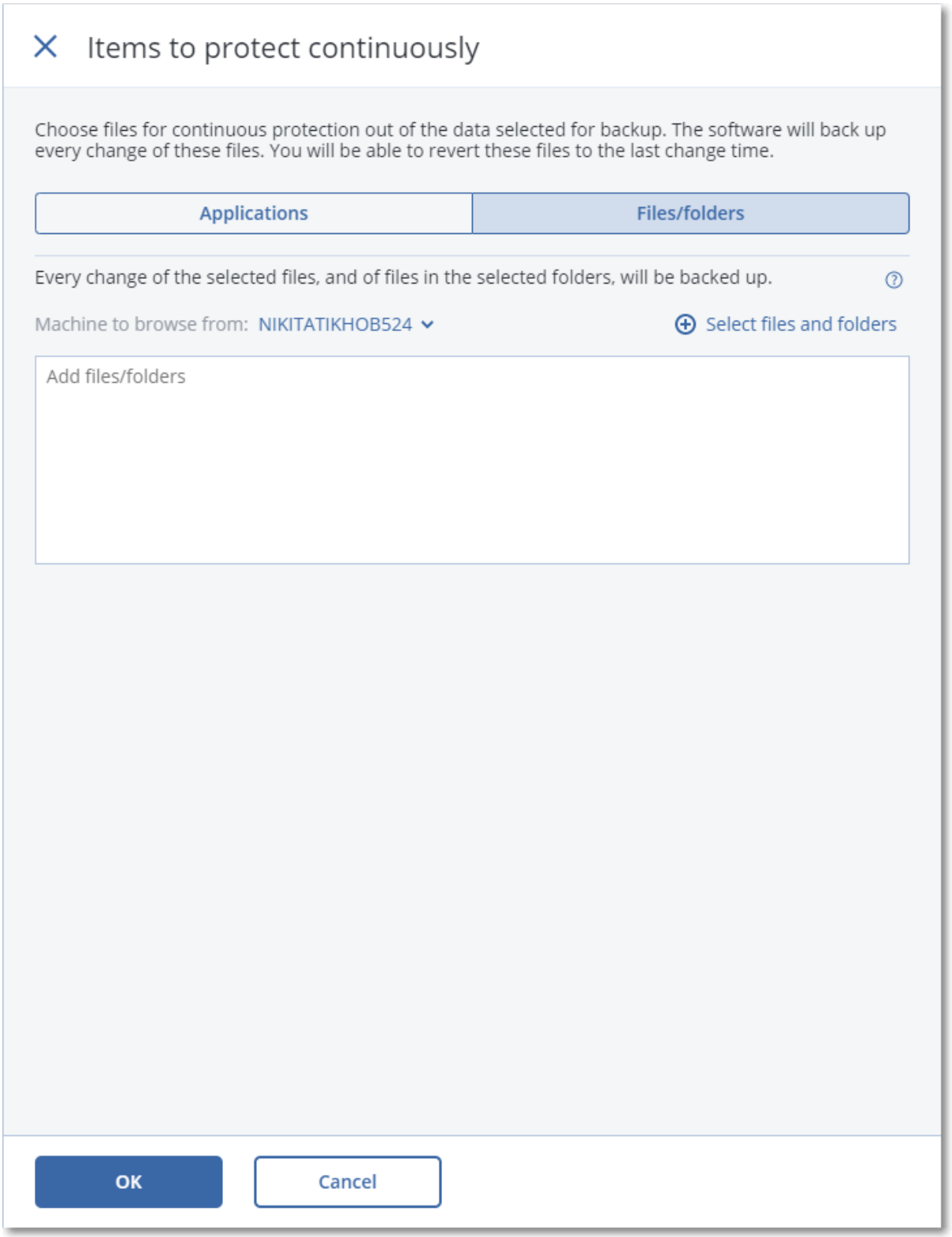
Sie können die Applikationen aus den vordefinierten Kategorien auswählen oder andere Applikationen spezifizieren, indem Sie den Pfad zu der ausführbaren Datei der Applikation festlegen. Verwenden Sie eines der nachfolgenden Formate:

C:\Program Files\Microsoft Office\Office16\WINWORD.EXE

ODER

***:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE**

- **Dateien/Ordner** (jede Datei, die sich am/an den spezifizierten Speicherort(en) befindet, wird gesichert). Wir empfehlen diese Option, wenn Sie bestimmte Dateien und Ordner schützen wollen, die häufig geändert werden.



Von dieser Maschine aus durchsuchen – spezifizieren Sie die Maschine, deren Dateien/Ordner Sie für die kontinuierliche Datensicherung (CDP) auswählen wollen.

Klicken Sie auf den Befehl **Dateien und Ordner auswählen**, um die gewünschten Dateien/Ordner auf der spezifizierten Maschine auszuwählen.

***Wichtig**: Wenn Sie einen kompletten Ordner manuell spezifizieren wollen, um dessen Dateien kontinuierlich zu sichern, können Sie eine Maske verwenden. Beispiel:*
*Korrekt spezifizierter Pfad: D:\Daten**
Falsch spezifizierter Pfad: D:\Daten

Sie können in dem Textfeld auch Regeln spezifizieren, um die zu sichernden Dateien/Ordner auszuwählen. Weitere Informationen über die Definierung von Regeln finden Sie im Abschnitt 'Dateien/Ordner auswählen'. Wenn Sie dies abgeschlossen haben, klicken Sie auf **Fertig**.

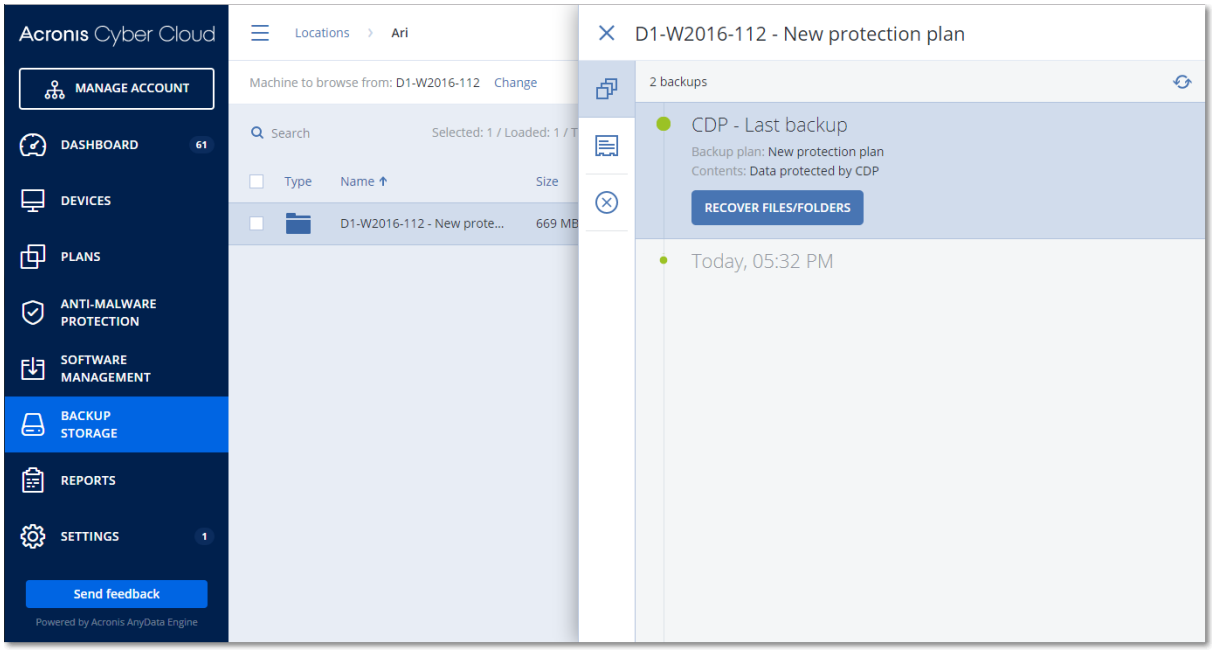
4. Klicken Sie auf **Erstellen**.

Als Ergebnis wird der Schutzplan mit aktivierter kontinuierliche Datensicherung (CDP) der ausgewählten Maschine zugewiesen. Nach dem ersten regelmäßigen Backup werden Backups mit der neuesten Kopie der per CDP gesicherten Daten auf regelmäßiger Basis erstellt. Es werden beide Arten von Daten (die, die über Applikationen ausgewählt wurden und die, die über Dateien/Ordner ausgewählt wurden) gesichert.

Die kontinuierlich gesicherten Daten werden entsprechend der für das Backup-Modul definierten Aufbewahrungsrichtlinie vorgehalten.

So können Sie auf kontinuierlicher Basis erstellte Backups unterscheiden

Backups, die auf kontinuierlicher Basis erstellt wurden, haben das Präfix 'CDP'.



So können Sie Ihre komplette Maschine auf ihren letzten (neuesten) Zustand zurücksetzen

Wenn Sie in der Lage sein wollen, den letzten (neuesten) Zustand einer Maschine wiederherzustellen, können Sie die Option **Kontinuierliche Datensicherung (CDP)** im Backup-Modul eines Schutzplans verwenden.

Sie können entweder die komplette Maschine oder einzelne Dateien/Ordner aus einem CDP-Backup wiederherstellen. Im ersten Fall erhalten Sie eine komplette Maschine, die sich wieder in ihrem

zuletzt gesicherten Zustand befindet. Im zweiten Fall erhalten Sie die entsprechenden Dateien/Ordner in ihrem zuletzt gesicherten Zustand.

15.5 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.

- **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 Secure Zone 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, ihrer Vorteile und Beschränkungen finden Sie im Abschnitt 'Über die Secure Zone''.

Erweiterte Storage-Option

***Hinweis**: Diese Funktionalität ist in den Standard-Editionen des Cyber Protection Service nicht 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.

  Beispiel: 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.

15.5.1 Über die 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 einer Secure Zone sinnvoll?

Die 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

- Unter Mac OS X ist die Verwendung einer Secure Zone nicht möglich.

- Die Secure Zone kann nur als normale Partition 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.
- Das Backup-Format 'Einzeldatei' (S. 434) wird von der Secure Zone nicht unterstützt. Wenn Sie einen Schutzplan mit dem Backup-Schema '**Nur inkrementell (Einzeldatei)**' haben/erstellen und dort die Secure Zone als Backup-Ziel auswählen, wird das Backup-Schema automatisch auf **Wöchentlich vollständig, täglich inkrementell** geändert.

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.*

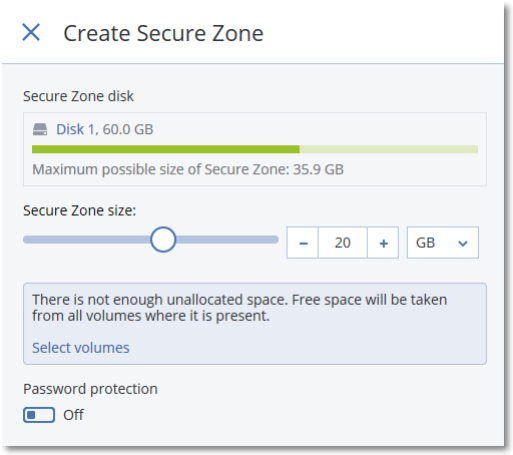
So können Sie eine Secure Zone erstellen

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.

15.6 Planung

Planungen verwenden die Zeiteinstellungen (einschließlich der Zeitzone) des Betriebssystems, auf welchem der Agent installiert ist. Die Zeitzone des Agenten für VMware (Virtuelle Appliance) kann in der Benutzeroberfläche des Agenten (S. 71) konfiguriert werden.

Wenn beispielsweise in einem Schutzplan eine Ausführung für 21:00 Uhr geplant ist und auf mehrere Maschinen in verschiedenen Zeitzonen angewendet wird, wird auf jeder Maschine das Backup um 21:00 Uhr der jeweiligen Ortszeit gestartet.

Backup-Schemata

Sie können eines der vordefinierten Backup-Schemata verwenden oder ein benutzerdefiniertes Schema erstellen. Ein Backup-Schema ist derjenige Teil eines Schutzplans, der die Backup-Planung und die Backup-Methode enthält.

Wählen Sie bei **Backup-Schema** eine der folgenden Möglichkeiten:

- **Nur inkrementell (Einzeldatei)**

  Die standardmäßig Planung für die Durchführung von Backups ist 'täglich' und zwar von Montag bis Freitag. Sie können den Zeitpunkt bestimmen, an dem das Backup ausgeführt werden soll.

  Wenn Sie die Backup-Häufigkeit ändern wollen, bewegen Sie einfach den entsprechenden grafischen Schieber – und spezifizieren Sie dann die gewünschte Backup-Planung.

  Die Backups verwenden das Backup-Format 'Einzeldatei' (S. 434).

  Das erst Backup ist vom Typ 'vollständig' – was bedeutet, dass es die meiste Zeit benötigt. Alle nachfolgenden Backups sind inkrementell und benötigen deutlich weniger Zeit.

  Dieses Schema wird dringend empfohlen, wenn der Cloud-Storage als Backup-Speicherort verwendet wird. Andere Backup-Schemata können mehrere Voll-Backups beinhalten, die viel Zeit und Netzwerkverkehr benötigen.

  Dieses Schema ist nicht verfügbar, wenn Sie die Secure Zone als Backup-Ziel verwenden.

- **Nur vollständig**

  Die standardmäßig Planung für die Durchführung von Backups ist 'täglich' und zwar von Montag bis Freitag. Sie können den Zeitpunkt bestimmen, an dem das Backup ausgeführt werden soll.

  Wenn Sie die Backup-Häufigkeit ändern wollen, bewegen Sie einfach den entsprechenden grafischen Schieber – und spezifizieren Sie dann die gewünschte Backup-Planung.

  Alle Backups sind vom Typ 'vollständig'.

- **Wöchentlich vollständig, täglich inkrementell**

  Die standardmäßig Planung für die Durchführung von Backups ist 'täglich' und zwar von Montag bis Freitag. Sie können die Wochentage sowie den Zeitpunkt der Backup-Ausführung ändern.

  Einmal pro Woche wird ein Voll-Backup erstellt. Alle anderen Backups sind inkrementell. Der genaue Tag, an dem das Voll-Backup erstellt wird, wird durch die Option **Wöchentliches Backup** definiert (klicken Sie auf das Zahnradsymbol und dann auf die Befehle **Backup-Optionen** –> **Wöchentliches Backup**).

- **Monatlich vollständig, wöchentlich differentiell, täglich inkrementell (GVS)**

  Die standardmäßige Backup-Planung ist: inkrementelle Backups werden täglich von Montag bis Freitag ausgeführt, differentielle Backups jeden Samstag, Voll-Backups am ersten Tag eines jeden Monats. Sie können diese Planungen und den Zeitpunkt der Backup-Ausführung ändern.

  Dieses Backup-Schema wird im Fensterbereich des Schutzplans als '**Benutzerdefiniertes**' Schema angezeigt.

- **Benutzerdefiniert**

  Spezifizieren Sie die Planungen für die vollständigen, differentiellen und inkrementellen Backups.

  Beim Backup von SQL- und Exchange-Daten sowie eines Systemzustands ist die Option 'Differentielles Backup' nicht verfügbar.

Sie können jede Backup-Planung so konfigurieren, dass die Ausführung nicht nach Zeit, sondern auf bestimmte Ereignisse hin erfolgt. Wählen Sie dazu in den Planungseinstellungen den gewünschten Ereignistyp aus. Weitere Informationen finden Sie im Abschnitt 'Planung nach Ereignissen'.

Zusätzliche Planungsoptionen

Für jedes Ziel haben Sie folgende Einstellungsmöglichkeiten:

- Spezifizieren Sie die Backup-Startbedingungen, damit das geplante Backup nur ausgeführt wird, wenn bestimmte Bedingungen erfüllt sind. Weitere Informationen finden Sie im Abschnitt 'Startbedingungen'.
- 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. Solange die Planung deaktiviert ist, werden die Aufbewahrungsregeln nicht angewendet – außer ein Backup wird manuell gestartet.
- Eine Verzögerung für den Ausführungszeitpunkt einführen. 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.

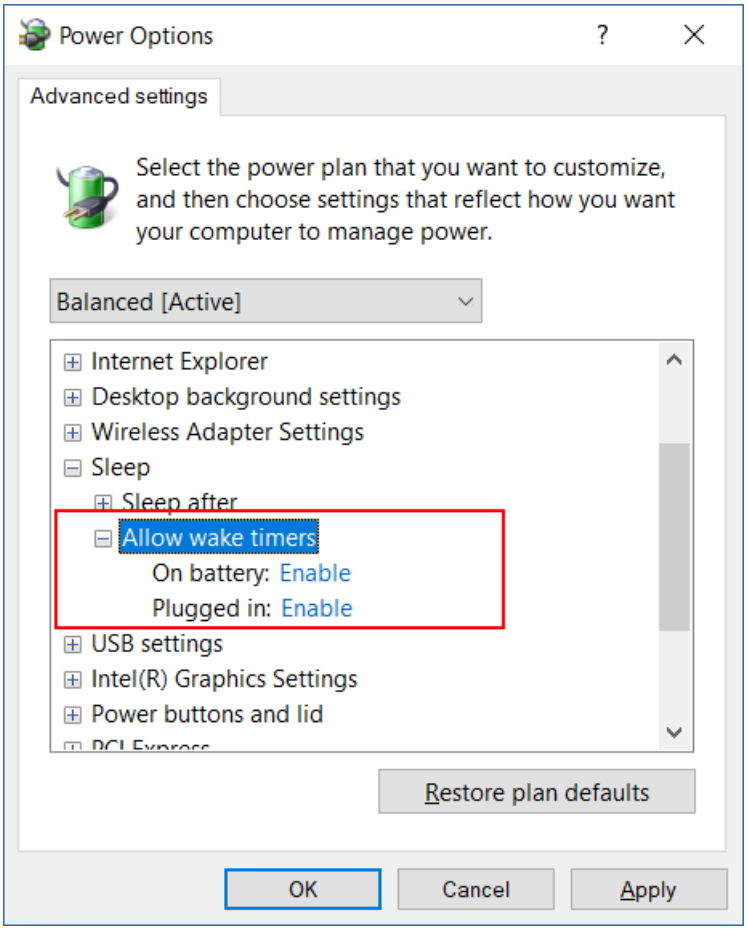
  Gehen Sie in den Backup-Modul-Einstellungen des Schutzplans zu **Backup-Optionen** –> **Planung**. Wählen Sie die Option **Backup-Startzeiten in einem Zeitfenster verteilen** und spezifizieren Sie dann den maximalen Verzögerungswert. Der Verzögerungswert für jede Maschinen wird bestimmt, wenn der Schutzplan auf die Maschine angewendet wird – und er bleibt so lange gleich, bis Sie den Schutzplan erneut bearbeiten und den maximalen Verzögerungswert ändern.

  ***Hinweis**: Diese Option ist standardmäßig aktiviert und der vorgegebene maximale Verzögerungswert beträgt 30 Minuten.*

- Klicken Sie auf **Mehr anzeigen**, um auf die folgenden Optionen zugreifen zu können.
  - **Task bei Neustart der Maschine ausführen, wenn die Maschine zur geplanten Zeit ausgeschaltet war** (standardmäßig deaktiviert)
  - **Standby- oder Ruhezustandsmodus während des Backups verhindern** standardmäßig aktiviert)

    Diese Option gilt nur für Maschinen, die unter Windows laufen.
  - **Aus Standby- oder Ruhezustandsmodus aufwecken, um ein geplantes Backup zu starten** (standardmäßig deaktiviert)

Diese Option gilt nur für unter Windows laufende Maschinen, bei denen im Energiesparplan die Einstellung **Zeitgeber zur Aktivierung zulassen** aktiviert ist.



Diese Option ist nicht wirksam, wenn das Gerät ausgeschaltet ist, d.h. die Option macht keinen Gebrauch von der Wake-on-LAN-Funktionalität.

15.6.1 Planung nach Ereignissen

Wenn Sie eine Planung für das Backup-Modul eines Schutzplans konfigurieren, können Sie in den entsprechenden Planungseinstellungen einen Ereignistyp festlegen. Das Backup wird gestartet, sobald das festgelegte Ereignisse eintritt.

Sie können eines der folgenden Ereignisse wählen:

- **Zeit seit letztem Backup**

  Dies ist die verstrichene Zeit seit Abschluss des letzten erfolgreichen Backups innerhalb desselben Schutzplans. Sie können einen bestimmten Zeitraum definieren.

- **Wenn sich ein Benutzer am System anmeldet**

  Standardmäßig führt die Anmeldung eines beliebigen Benutzers dazu, dass das Backup ausgelöst wird. Sie können aber von 'Jeder Benutzer' zu einem bestimmten Benutzerkonto wechseln.

- **Wenn sich ein Benutzer vom System abmeldet**

  Standardmäßig führt die Abmeldung eines beliebigen Benutzers dazu, dass das Backup ausgelöst wird. Sie können aber von 'Jeder Benutzer' zu einem bestimmten Benutzerkonto wechseln.

Hinweis: *Das Backup wird nicht ausgeführt, wenn das System herunterfährt, weil 'Herunterfahren' nicht dasselbe wie 'Abmelden' ist.*

- **Beim Systemstart**
- **Beim Herunterfahren des Systems**
- **Bei Ereignis im Windows-Ereignisprotokoll**

  Sie müssen die Ereigniseigenschaften spezifizieren.

Die untere Tabelle zeigt die Ereignisse an, die für verschiedene Daten unter Windows, Linux und macOS verfügbar sind.

Backup-Quelle	Zeit seit letztem Backup	Wenn sich ein Benutzer am System anmeldet	Wenn sich ein Benutzer vom System abmeldet	Beim Systemstart	Beim Herunterfahren des Systems	Bei Ereignis im Windows-Ereignisprotokoll
Laufwerke/Volumes oder Dateien (physische Maschinen)	Windows, Linux, macOS	Windows	Windows	Windows, Linux, macOS	Windows	Windows
Laufwerke/Volumes (virtuelle Maschinen)	Windows, Linux	–	–	–	–	–
ESXi-Konfiguration	Windows, Linux	–	–	–	–	–
Office 365-Postfächer	Windows	–	–	–	–	Windows
Exchange-Datenbanken und -Postfächer	Windows	–	–	–	–	Windows
SQL-Datenbanken	Windows	–	–	–	–	Windows

15.6.1.1 Bei Ereignis im Windows-Ereignisprotokoll

Sie können ein Backup so planen, dass es automatisch gestartet wird, wenn ein bestimmtes Windows-Ereignis in eine der Protokolllisten **Anwendung**, **Sicherheit** oder **System** aufgenommen wird.

Angenommen, Sie wollen einen Schutzplan aufstellen, der automatisch ein vollständiges Notfall-Backup Ihrer Daten durchführt, sobald Windows entdeckt, dass die Festplatte vor einem Ausfall steht.

Sie können die Ereignisse durchsuchen und Ereigniseigenschaften einsehen, wenn Sie das Snap-In **Ereignisanzeige** verwenden (welches auch über die **Computerverwaltung** verfügbar ist). Um die Windows-Protokolle für **Sicherheit** öffnen zu können, müssen Sie Mitglied in der Gruppe der **Administratoren** sein.

Ereigniseigenschaften

Protokollname

Spezifizieren Sie den Namen eines Protokolls. Wählen Sie den Namen einer Standard-Protokollliste (**Anwendung**, **Sicherheit** oder **System**) oder geben Sie den Namen einer Protokollliste ein – beispielsweise: **Microsoft Office Sitzungen**

Ereignisquelle

Spezifizieren Sie die Quelle des Ereignisses, welche typischerweise das Programm oder die Systemkomponente angibt, die das Ereignis verursachte – beispielsweise: **Laufwerk**.

Jede Ereignisquelle, die die spezifizierte Zeichenfolge 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

Geben Sie den Typ des Ereignisses an: **Fehler**, **Warnung**, **Informationen**, **Überwachung erfolgreich** oder **Überwachung fehlgeschlagen**.

Ereignis-ID

Bezeichnet die Ereignis-Nummer, die üblicherweise die spezielle Art der Ereignisse unter Ereignissen derselben Quelle identifiziert.

So tritt z.B. ein **Fehler**-Ereignis mit der Ereignisquelle **disk** und der Ereignis-Kennung **7** auf, wenn Windows einen fehlerhaften Block auf einem Festplattenlaufwerk entdeckt – während ein **Fehler**-Ereignis mit der Ereignisquelle **disk** und der Ereignis-Kennung **15** stattfindet, wenn ein Laufwerk noch nicht zugriffsbereit ist.

Beispiel: 'Fehlerhafte Blöcke'-Notfall-Backup

Treten ein oder mehrere fehlerhafte Blöcke plötzlich auf einer Festplatte auf, so deutet das üblicherweise auf einen baldigen Ausfall der Festplatte hin. Angenommen, Sie wollen einen Schutzplan erstellen, der die Daten eines Laufwerks sichert, sobald eine solche Situation eintritt.

Wenn Windows einen fehlerhaften Block auf einer Festplatte entdeckt, nimmt es ein Ereignis mit der Ereignis-Quelle **disk** und der Ereignis-Kennung **7** in die Protokollliste **System** auf; der Typ des Ereignisses ist **Fehler**.

Wenn Sie den Plan erstellen, geben Sie Folgendes im Bereich **Planung** ein bzw. wählen es aus:

- **Protokollname**: **System**
- **Ereignis-Quelle**: **Laufwerk**
- **Ereignis-Typ**: **Fehler**
- **Ereignis-Kennung**: **7**

Wichtig: *Um sicherzustellen, dass ein Backup trotz Vorhandensein von fehlerhaften Blöcken fertiggestellt wird, müssen Sie festlegen, dass das Backup die fehlerhaften Blöcke ignorieren soll. Zur Umsetzung gehen Sie in den* ***Backup-Optionen*** *zum Unterpunkt* ***Fehlerbehandlung*** *und aktivieren das Kontrollkästchen* ***Fehlerhafte Sektoren ignorieren****.*

15.6.2 Startbedingungen

Diese Einstellungen geben dem Scheduler mehr Flexibilität und ermöglichen es, ein Backup in Abhängigkeit von gewissen Bedingungen auszuführen. Bei mehreren Bedingungen müssen diese alle gleichzeitig erfüllt sein, damit das Backup starten kann. Startbedingungen gelten nicht, wenn ein Backup-Plan manuell gestartet wird.

Wenn Sie auf diese Einstellungen zugreifen wollen, klicken Sie auf **Mehr anzeigen**, wenn Sie die Planungseinstellungen für einen Schutzplan konfigurieren.

Wie sich der Scheduler verhalten soll, wenn die Bedingung (oder eine von mehreren Bedingungen) nicht erfüllt ist, kann über die Backup-Option Backup-Startbedingungen (S. 189) definiert werden. Wenn die Bedingung(en) über einen zu langen Zeitraum nicht erfüllt wurde(n), könnte ein weiteres Aufschieben des Backups zu kritisch werden. Um zu bestimmen, was in so einem Fall passieren soll,

können Sie ein Zeitintervall festlegen, nach dessen Ablauf des Backups auf jeden Fall ausgeführt wird – egal ob die Bedingung(en) erfüllt wurde(n) oder nicht.

Die untere Tabelle zeigt die Startbedingungen an, die für verschiedene Daten unter Windows, Linux und macOS verfügbar sind.

Backup-Quelle	Laufwerke/Volumes oder Dateien (physische Maschinen)	Laufwerke/Volumes (virtuelle Maschinen)	ESXi-Konfiguration	Office 365-Postfächer	Exchange-Datenbanken und -Postfächer	SQL-Datenbanken
Benutzer ist inaktiv (S. 145)	Windows	–	–	–	–	–
Der Host des Backup-Speicherorts ist verfügbar (S. 146)	Windows, Linux, macOS	Windows, Linux	Windows, Linux	Windows	Windows	Windows
Benutzer sind abgemeldet (S. 146)	Windows	–	–	–	–	–
Entspricht dem Zeitintervall (S. 147)	Windows, Linux, macOS	Windows, Linux	–	–	–	–
Akkubelastung senken (S. 147)	Windows	–	–	–	–	–
Nicht starten, wenn eine getaktete Verbindung besteht (S. 148)	Windows	–	–	–	–	–
Nicht starten, wenn eine Verbindung mit folgenden WLANs besteht: (S. 149)	Windows	–	–	–	–	–
IP-Adresse des Gerätes überprüfen (S. 149)	Windows	–	–	–	–	–

15.6.2.1 Benutzer ist inaktiv

'Benutzer ist inaktiv' bedeutet, dass auf der Maschine ein Bildschirmschoner läuft oder die Maschine gesperrt ist.

Beispiel

Starte das Backup auf der Maschine 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. Start um: **21:00**.
- Bedingung: **Benutzer ist inaktiv**.
- Backup-Startbedingungen: **Warten, bis die Bedingungen erfüllt sind**, **Backup trotzdem ausführen nach 2** Stunde(n).

Ergebnis:

(1) Wenn der Benutzer vor 21:00 Uhr inaktiv wird, so wird das Backup um 21:00 Uhr ausgeführt.

(2) Wenn der Benutzer zwischen 21:00 und 23:00 Uhr inaktiv wird, so wird das Backup sofort gestartet, nachdem der Benutzer inaktiv wurde.

(3) Wenn der Benutzer um 23 Uhr immer noch aktiv ist, wird das Backup um 23:00 Uhr gestartet.

15.6.2.2 Der Host des Backup-Speicherorts ist verfügbar

'Der Host des Backup-Speicherorts ist verfügbar' bedeutet, dass die Maschine, die den Backup-Zielspeicherort hostet, über das Netzwerk verfügbar ist.

Diese Bedinung 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

Bestimmte Daten werden an jedem Arbeitstag um 21 Uhr zu einem Netzwerkordner gesichert. Wenn die Maschine, die den Ordner hostet, gerade nicht verfügbar ist (z.B. wegen Wartungsarbeiten), können Sie das Backup überspringen und bis zum nächsten geplanten Start am nächsten Werktag warten lassen.

- Planung: Täglich, Montag bis Freitag ausführen Start um: **21:00**.
- Bedingung: **Der Host des Backup-Speicherorts ist verfügbar**.
- Backup-Startbedingungen: **Das geplante Backup überspringen**.

Ergebnis:

(1) Wenn es 21:00 Uhr wird und der Host verfügbar ist, wird das Backup sofort ausgeführt.

(2) Wenn es 21 Uhr wird, aber der Host nicht verfügbar ist, wird das Backup am nächsten Arbeitstag starten, sofern der Host dann verfügbar ist.

(3) Wenn der Host niemals an Werktagen um 21 Uhr verfügbar ist, wird das Backup niemals starten.

15.6.2.3 Benutzer sind abgemeldet

Ermöglicht Ihnen, ein Backup auf Warteposition zu setzen, bis sich alle Benutzer von Windows abgemeldet haben.

Beispiel

Starte das 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. Start um: **20:00**.
- Bedingung: **Benutzer sind abgemeldet**.
- Backup-Startbedingungen: **Warten, bis die Bedingungen erfüllt sind**, **Backup trotzdem ausführen nach 3** Stunde(n).

Ergebnis:

(1) Wenn alle Benutzer um 20:00 Uhr abgemeldet sind, wird das Backup um 20:00 Uhr gestartet.

(2) Wenn sich der letzte Benutzer zwischen 20:00 und 23:00 Uhr abmeldet, wird das Backup sofort ausgeführt, nachdem sich der Benutzer abgemeldet hat.

(3) Wenn ein Benutzer um 23 Uhr immer noch angemeldet ist, wird das Backup um 23:00 Uhr gestartet.

15.6.2.4 Entspricht dem Zeitintervall

Beschränkt die Startzeit für ein Backup auf ein bestimmtes Zeitintervall.

Beispiel

Eine Firma verwendet unterschiedliche Speicherorte auf demselben NAS-Gerät (Network Attached Storage), um Benutzerdaten und Server zu sichern. Ein Arbeitstag beginnt um 8:00 und endet um 17:00 Uhr. Benutzerdaten sollen jeweils gesichert werden, sobald ein Benutzer sich abmeldet – jedoch nicht vor 16:30 Uhr. Das Backup der Unternehmensserver erfolgt täglich um 23:00 Uhr. Die Benutzerdaten sollten daher alle möglichst vor diesem Zeitpunkt gesichert sein, damit genügend freie Netzwerkbandbreite verfügbar ist. Zur Kalkulation wird angenommen, dass das Backup der Daten eines Benutzers nicht mehr als je eine Stunde benötigt. Das letzte Benutzer-Backup sollte also spätestens um 22 Uhr starten. Daraus ergibt sich folgende Anweisung: Wenn ein Benutzer im vorgegebenen Zeitintervall noch angemeldet ist oder sich zu einer anderen Zeit abmeldet, werden die Daten des Benutzers nicht gesichert – also die Backup-Ausführung übersprungen.

- Ereignis: **Wenn sich ein Benutzer vom System abmeldet**. Spezifizieren Sie das Benutzerkonto: **Jeder Benutzer**.
- Bedingung: **Entspricht dem Zeitintervall**: von **16:30 Uhr** bis **22:00 Uhr**.
- Backup-Startbedingungen: **Das geplante Backup überspringen**.

Ergebnis:

(1) Wenn sich der Benutzer zwischen 16:30 Uhr und 22:00 Uhr abmeldet, wird das Backup unmittelbar nach seiner Abmeldung gestartet.

(2) Wenn sich der Benutzer zu einem anderen Zeitpunkt abmeldet, wird das Backup übersprungen.

15.6.2.5 Akkubelastung senken

Verhindert ein Backup, wenn das Gerät (Notebook oder Tablet) nicht an eine externe Stromquelle angeschlossen ist (sondern im Akkubetrieb läuft). In Abhängigkeit vom Wert der Option Backup-Startbedingungen (S. 189), wird das übersprungene Backup (nicht) gestartet, wenn das Gerät wieder an eine externe Stromquelle angeschlossen wird. Folgende Optionen sind verfügbar:

- **Nicht starten, wenn im Akkubetrieb**

  Ein Backup wird nur gestartet, wenn das Gerät mit einer externen Stromquelle verbunden ist.
- **Im Akkubetrieb starten, wenn Akkustand höher ist als:**

Ein Backup wird gestartet, wenn das Gerät mit einer externen Stromquelle verbunden ist oder der Akkustand über dem spezifizierten Wert liegt.

Beispiel

Das Backup erfolgt normalerweise immer werktags um 21:00 Uhr. Wenn das Gerät nicht mit einer externen Stromquelle verbunden ist (beispielsweise, weil der Benutzer an einem späten Meeting teilnimmt), können Sie das Backup überspringen lassen, um Akkuladung zu sparen, und stattdessen darauf warten lassen, dass der Benutzer das Gerät wieder an eine externe Stromquelle anschließt.

- Planung: Täglich, Montag bis Freitag ausführen Start um: 21:00.
- Bedingung: **Akkubelastung senken**, **Nicht starten, wenn im Akkubetrieb**.
- Backup-Startbedingungen: **Warten, bis die Bedingungen erfüllt sind**.

Ergebnis:

(1) Wenn es 21:00 Uhr wird und das Gerät mit einer externen Stromquelle verbunden ist, wird das Backup sofort gestartet.

(2) Wenn es 21:00 Uhr wird und das Gerät im Akkubetrieb läuft, wird das Backup gestartet, sobald das Gerät wieder mit einer externen Stromquelle verbunden ist.

15.6.2.6 Nicht starten, wenn eine getaktete Verbindung besteht

Verhindert ein Backup (auch ein Backup zu einem lokalen Laufwerk), wenn das Gerät 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.

Es gibt eine zusätzliche Maßnahme, um Backups über WLAN- bzw. Mobile Hotspots zu verhindern: Wenn Sie die Option **Nicht starten, wenn eine getaktete Verbindung besteht** aktivieren, wird automatisch auch die Option **Nicht starten, wenn eine Verbindung mit folgenden WLANs besteht** aktiviert. Folgende Netzwerknamen sind standardmäßig eingetragen: 'android', 'phone', 'mobile' und 'modem'. Sie können diese Namen aus der Liste löschen, wenn Sie auf das X-Zeichen klicken.

Beispiel

Das Backup erfolgt normalerweise immer werktags um 21:00 Uhr. Wenn das Gerät eine getaktete Internetverbindung verwendet (beispielsweise, weil der Benutzer auf einer Geschäftsreise ist), können Sie das Backup überspringen lassen, um Netzwerkverkehr/Gebühren zu sparen, und stattdessen auf den geplanten Start am nächsten Werktag warten lassen.

- Planung: Täglich, Montag bis Freitag ausführen Start um: 21:00.
- Bedingung: **Nicht starten, wenn eine getaktete Verbindung besteht**.
- Backup-Startbedingungen: **Das geplante Backup überspringen**.

Ergebnis:

(1) Wenn es 21:00 Uhr wird und das Gerät keine getaktete (aber eine andere) Internetverbindung verwendet, wird das Backup sofort gestartet.

(2) Wenn es 21:00 Uhr wird und das Gerät eine getaktete Internetverbindung verwendet, wird das Backup am nächsten Werktag gestartet.

(3) Wenn das Gerät werktags um 21:00 Uhr immer eine getaktete Internetverbindung verwendet, wird das Backup niemals gestartet.

15.6.2.7 Nicht starten, wenn eine Verbindung mit folgenden WLANs besteht:

Verhindert ein Backup (auch ein Backup zu einem lokalen Laufwerk), wenn das Gerät mit einem der spezifizierten WLANs verbunden ist. 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 SSID enthalten (unabhängig von Groß-/Kleinschreibung). Beispiel: wenn Sie 'phone' als Netzwerkname spezifizieren, wird das Backup nicht gestartet, wenn das Gerät mit einem WLAN mit einer der folgenden SSIDs verbunden ist: 'Peters iPhone', 'phone_wlan' oder 'mein_PHONE_wlan'.

Diese Bedingung ist nützlich, um Backups zu verhindern, wenn ein Gerät per WLAN-/Mobile Hotspot mit dem Internet verbunden ist.

Es gibt eine zusätzliche Maßnahme, um Backups über WLAN- bzw. Mobile Hotspots zu verhindern: Wenn Sie die Option **Nicht starten, wenn eine getaktete Verbindung besteht** aktivieren, wird automatisch auch die Option **Nicht starten, wenn eine Verbindung mit folgenden WLANs besteht** aktiviert. Folgende Netzwerknamen sind standardmäßig eingetragen: 'android', 'phone', 'mobile' und 'modem'. Sie können diese Namen aus der Liste löschen, wenn Sie auf das X-Zeichen klicken.

Beispiel

Das Backup erfolgt normalerweise immer werktags um 21:00 Uhr. Wenn das Gerät über einen WLAN-/Mobile Hotspot mit dem Internet verbunden ist (beispielsweise, weil das betreffende Notebook per Tethering-Modus mit einem Smartphone verbunden ist), können Sie das Backup überspringen lassen, um Netzwerkverkehr/Gebühren zu sparen, und stattdessen auf den geplanten Start am nächsten Werktag warten lassen.

- Planung: Täglich, Montag bis Freitag ausführen Start um: 21:00.
- Bedingung: **Nicht starten, wenn eine Verbindung mit folgenden WLANs besteht**, **Netzwerkname**: `<SSID des Hotspot-Netzwerks>`.
- Backup-Startbedingungen: **Das geplante Backup überspringen**.

Ergebnis:

(1) Wenn es 21:00 Uhr wird und die Maschine nicht mit dem spezifizierten Netzwerk verbunden ist, wird das Backup sofort gestartet.

(2) Wenn es 21:00 Uhr wird und die Maschine mit dem spezifizierten Netzwerk verbunden ist, wird das Backup am nächsten Werktag gestartet.

(3) Wenn die Maschine werktags um 21:00 Uhr immer mit dem spezifizierten Netzwerk verbunden ist, wird das Backup niemals gestartet.

15.6.2.8 IP-Adresse des Gerätes überprüfen

Verhindert ein Backup (auch ein Backup zu einem lokalen Laufwerk), wenn eine der Geräte-IP-Adressen innerhalb oder außerhalb des angegebenen IP-Adressbereichs liegt. 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.

Diese Bedingung ist nützlich, wenn sich ein Benutzer im Ausland befindet, um hohe Datenübertragungsgebühren zu vermeiden. Außerdem kann es helfen, Backups über eine VPN-Verbindung (Virtual Private Network) zu verhindern.

Beispiel

Das Backup erfolgt normalerweise immer werktags um 21:00 Uhr. Wenn sich ein Gerät per VPN-Tunnel mit dem Firmennetzwerk verbindet (z.B., weil der Benutzer von zu Hause aus arbeitet), können Sie das Backup überspringen lassen und darauf warten, bis der Benutzer mit seinem Gerät wieder im Büro ist.

- Planung: Täglich, Montag bis Freitag ausführen Start um: 21:00.
- 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:

(1) Wenn es 21:00 Uhr wird und die IP-Adresse der Maschine nicht im spezifizierten Bereich liegt, wird das Backup sofort gestartet.

(2) Wenn es 21:00 Uhr wird und die IP-Adresse der Maschine im spezifizierten Bereich liegt, wird das Backup gestartet, sobald das Gerät eine 'nicht-VPN'-IP-Adresse erhält.

(3) Wenn die IP-Adresse der Maschine werktags um 21:00 Uhr immer im spezifizierten Bereich liegt, wird das Backup niemals gestartet.

15.7 Aufbewahrungsregeln

1. Klicken Sie auf **Aufbewahrungsdauer**.
2. Wählen Sie bei **Bereinigung** eine der folgenden Möglichkeiten:
   - **Nach Backup-Alter** (Standardeinstellung)

     Spezifizieren Sie, wie lange Backups, die von diesem Schutzplan erstellt wurden, aufbewahrt werden sollen. Die Aufbewahrungsregeln werden standardmäßig für jedes Backup-Set (S. 434) separat spezifiziert. Um für alle Backups eine gemeinsame Regel verwenden zu können, müssen Sie auf **Auf einzelne Regel für alle Backup-Sets umschalten** klicken.
   - **Nach Backup-Anzahl**

     Spezifizieren Sie ein Maximum für die Anzahl an Backups, die aufbewahrt werden sollen.
   - **Nach der Gesamtgröße der Backups**

     Spezifizieren Sie eine maximale Gesamtgröße für die Backups, die aufbewahrt werden sollen.

     Diese Einstellung ist nicht verfügbar, wenn das Backup-Schema **Nur inkrementell (Einzeldatei)** verwendet wird oder wenn der Cloud Storage als Backup-Ziel dient.
   - **Backups unbegrenzt aufbewahren**
3. Bestimmen Sie, wann die Bereinigung beginnen soll:
   - **Nach dem Backup** (Standardvorgabe)

     Die Aufbewahrungsregeln werden angewendet, nachdem ein neues Backup erstellt wurde.

- **Vor dem Backup**

  Die Aufbewahrungsregeln werden angewendet, bevor ein neues Backup erstellt wird.

  Diese Einstellung ist beim Backup von Microsoft SQL Server-Clustern oder Microsoft Exchange Server-Clustern nicht verfügbar.

Was Sie zudem noch wissen sollten

- Wenn laut Backup-Schema und Backup-Format jedes Backup als separate Datei gespeichert wird, kann diese Datei solange nicht gelöscht werden, bis die 'Lebensdauer' aller von dieser Datei abhängigen (inkrementellen und differentiellen) Backups abgelaufen ist. Dies erfordert eine gewisse Menge an extra Speicherplatz, um solche Backups aufbewahren zu können, deren Löschung zurückgestellt wurde. Es kann daher auch vorkommen, dass die von Ihnen spezifizierten Werte für Backup-Alter, Backup-Größe und Backup-Anzahl überschritten werden.

  Diese Verhalten kann durch Verwendung der Backup-Option 'Backup-Konsolidierung (S. 159)' geändert werden.
- Aufbewahrungsregeln sind Bestandteil eines Schutzplans. Sie werden nicht mehr auf die Backups einer Maschine angewendet, sobald der entsprechende Schutzplan von dieser Maschine widerrufen oder gelöscht wird – oder die Maschine selbst aus dem Cyber Protection Service gelöscht wird. Wenn Sie die vom Backup-Plan erstellten Backups nicht mehr benötigen, können Sie diese löschen (wie im Abschnitt 'Backups löschen (S. 222)' beschrieben).

15.8 Replikation

Wenn Sie die Backup-Replikation aktivieren, wird jedes Backup direkt nach seiner Erstellung zu einem anderen Speicherort kopiert. Falls frühere Backups nicht repliziert wurden (weil beispielsweise die Netzwerkverbindung verloren ging), wird die Software auch alle Backups replizieren, die nach der letzten erfolgreichen Replikation erschienen sind. Wenn die Backup-Replikation mitten in einem Prozess unterbrochen wird, werden beim nächsten Replikationsstart die bereits replizierten Daten nicht erneut repliziert, wodurch der Zeitverlust klein gehalten wird.

Replizierte Backups sind unabhängig von den Backups, die am ursprünglichen Speicherort verbleiben (und umgekehrt). Sie können Daten von jedem dieser Backups wiederherstellen, ohne Zugriff auf andere Speicherorte zu haben.

Anwendungsbeispiele

- **Verlässliches Disaster Recovery**

  Speichern Sie Ihre Backups sowohl 'on-site' (zur sofortigen Wiederherstellung) wie auch 'off-site' (um die Backups vor Ausfall des lokalen Speichers oder natürlichen Desastern zu schützen).
- **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**

  Löschen Sie ältere Backups mithilfe von Aufbewahrungsregeln von einem schnellen Speicher, um den teuren Speicherplatz nicht übermäßig zu beanspruchen.

Unterstützte Speicherorte

Sie können ein Backup *von* jedem der nachfolgenden Speicherorte aus (als Quelle) replizieren:

- Einem lokalen Ordner
- Einem Netzwerkordner
- Einer Secure Zone

Sie können ein Backup *zu* jedem der nachfolgenden Speicherorte (als Ziel) replizieren:

- Einem lokalen Ordner
- Einem Netzwerkordner
- Dem Cloud Storage

So können Sie die Replikation von Backups aktivieren

1. Klicken Sie im Fensterbereich des Schutzplans auf **Speicherort hinzufügen**.

   Das Steuerelement **Speicherort hinzufügen** wird nur dann angezeigt, wenn eine Replikation *von* dem zuletzt ausgewählten Speicherort unterstützt wird.
2. Spezifizieren Sie den Speicherort, wohin die Backups repliziert werden sollen.
3. [Optional] Ändern Sie bei **Aufbewahrungsdauer** die Aufbewahrungsregeln für den gewählten Speicherort (wie im Abschnitt 'Aufbewahrungsregeln (S. 150)' beschrieben).
4. [Optional] Klicken Sie auf das Zahnradsymbol –> **Performance und Backup-Fenster** und konfigurieren Sie dann das Backup-Fenster für den gewählten Speicherort (wie im Abschnitt 'Performance und Backup-Fenster (S. 181)' beschrieben Diese Einstellung bestimmt die Replikations-Performance.
5. [Optional] Wiederholen Sie die Schritte 1-4 für alle weiteren Speicherorte, zu denen die Backups repliziert werden sollen. Es werden bis zu fünf aufeinanderfolgende Speicherorte unterstützt (der erste eingeschlossen).

15.9 Verschlüsselung

Wir empfehlen Ihnen, alle Backups zu verschlüsseln, die im Cloud Storage gespeichert werden – insbesondere, wenn Ihr Unternehmen gesetzlichen Bestimmungen (zum Datenschutz u. Ä.) unterliegt.

Wichtig: *Falls Sie Ihr Kennwort verlieren, gibt es keine Möglichkeit, Ihre verschlüsselten Backups wiederherzustellen!*

Verschlüsselung in einem Schutzplan

Die Verschlüsselung wird aktiviert, wenn Sie beim Erstellen eines Schutzplans die entsprechenden Verschlüsselungseinstellungen spezifizieren. Nachdem ein Schutzplan angewendet wurde, können die Verschlüsselungseinstellungen nicht mehr geändert werden. Erstellen Sie einen neuen Schutzplan, wenn Sie andere Verschlüsselungseinstellungen verwenden wollen.

So können Sie die Verschlüsselungseinstellungen in einem Schutzplan spezifizieren

1. Aktivieren Sie im Fensterbereich des Schutzplans in den Einstellungen des Backup-Moduls den Schalter **Verschlüsselung**.
2. Spezifizieren und bestätigen Sie das Verschlüsselungskennwort.
3. Wählen Sie einen der folgenden Verschlüsselungsalgorithmen:
   - **AES 128** – die Backups werden nach dem Advanced Encryption Standard (AES) und mit einer Tiefe von 128 Bit verschlüsselt.
   - **AES 192** – die Backups werden mit dem AES-Algorithmus und einer Tiefe von 192-Bit verschlüsselt.
   - **AES 256** – die Backups werden mit dem AES-Algorithmus und einer Tiefe von 256-Bit verschlüsselt.
4. Klicken Sie auf **OK**.

Verschlüsselung als Eigenschaft einer Maschine

Diese Option ist für Administratoren gedacht, die die Backups vieler Maschinen handhaben müssen. Falls Sie ein einzigartiges Verschlüsselungskennwort für jede Maschine benötigen oder die Verschlüsselung von Backups unabhängig von den Verschlüsselungseinstellungen des Schutzplans erzwingen wollen, müssen Sie die Verschlüsselungseinstellungen individuell auf jeder Maschine speichern. Die Backups werden mit dem AES-Algorithmus und einer Tiefe von 256-Bit verschlüsselt.

Das Speichern von Verschlüsselungseinstellungen auf einer Maschine beeinflusst die Schutzpläne folgendermaßen:

- **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 einer Maschine gespeicherten Verschlüsselungseinstellungen überschreiben die Verschlüsselungseinstellungen eines Schutzplans. Jedes Backup wird verschlüsselt – selbst dann, wenn die Verschlüsselung in den Backup-Modul-Einstellungen deaktiviert ist.

Diese Option kann auf einer Maschine verwendet werden, auf welcher der Agent für VMware läuft. Sie sollten jedoch vorsichtig sein, wenn Sie mehr als einen Agenten für VMware mit demselben vCenter Server verbunden haben. Sie müssen dieselben Verschlüsselungseinstellungen für alle Agenten verwenden, weil es eine Art Lastverteilung (Load Balancing) zwischen ihnen gibt.

Nachdem die Verschlüsselungseinstellungen gespeichert wurden, können diese wie unten beschrieben geändert oder zurückgesetzt werden.

Wichtig: *Sollte ein Schutzplan, der auf dieser Maschine ausgeführt wird, bereits Backups erstellt haben, so wird eine Änderung der Verschlüsselungseinstellungen bewirken, dass dieser Plan fehlschlagen wird. Wenn Sie weiterhin Backups erstellen wollen, müssen Sie daher einen neuen Backup-Plan erstellen.*

So können Sie die Verschlüsselungseinstellungen auf einer Maschine speichern

1. Melden Sie sich als Administrator (unter Windows) oder als Benutzer 'root' (unter Linux) an.
2. Führen Sie folgendes Skript aus:
   - Unter Windows: `<Installationspfad>`**\PyShell\bin\acropsh.exe -m manage_creds --set-password** `<Verschlüsselungskennwort>`

     Wobei `<Installationspfad>` für den Installationspfad des Protection Agenten steht. Standardmäßig ist dies der Ordner '**%ProgramFiles%\BackupClient**'.
   - Unter Linux: **/usr/sbin/acropsh -m manage_creds --set-password** `<Verschlüsselungskennwort>`

So können Sie die Verschlüsselungseinstellungen auf einer Maschine zurücksetzen

1. Melden Sie sich als Administrator (unter Windows) oder als Benutzer 'root' (unter Linux) an.
2. Führen Sie folgendes Skript aus:
   - Unter Windows: `<Installationspfad>`**\PyShell\bin\acropsh.exe -m manage_creds --reset**

     Wobei `<Installationspfad>` für den Installationspfad des Protection Agenten steht. Standardmäßig ist dies der Ordner '**%ProgramFiles%\BackupClient**'.
   - Unter Linux: **/usr/sbin/acropsh -m manage_creds --reset**

So können Sie die Verschlüsselungseinstellungen über den Cyber Protection Monitor ändern

1. Melden Sie sich bei Windows oder macOS als Administrator an.
2. Klicken Sie im Infobereich der Taskleiste (Windows) oder in der Menüleiste (macOS) auf das Symbol für den Cyber Protection Monitor.

3. Klicken Sie auf das Zahnradsymbol.
4. Klicken Sie auf die Option **Verschlüsselung**.
5. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Wählen Sie den Befehl **Spezifisches Kennwort für diese Maschine festlegen**. Spezifizieren und bestätigen Sie das Verschlüsselungskennwort.
   - Wählen Sie den Befehl **Verschlüsselungseinstellungen des Schutzplans verwenden**.
6. Klicken Sie auf **OK**.

Wie die Verschlüsselung arbeitet

Der kryptografische AES-Algorithmus arbeitet im 'Cipher Block Chaining Mode' (CBC) und verwendet einen zufällig erstellten Schlüssel mit einer benutzerdefinierten Größe von 128, 192 oder 256 Bit. Je größer der Schlüssel, desto länger wird das Programm zur Verschlüsselung der Backups benötigen, aber desto sicherer sind auch die Daten.

Der Codierungsschlüssel ist dann per AES-256 verschlüsselt, wobei ein SHA-256-Hash-Wert 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.

15.10 Beglaubigung (Notarization)

***Hinweis**: Diese Funktionalität ist in den Standard-Editionen des Cyber Protection Service nicht 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 (S. 208) können.

Und so funktioniert es

Der Agent berechnet während eines Backups die Hash-Werte der zu sichernden Dateien, baut einen Hash-Baum auf (basierend auf der Ordnerstruktur), speichert diesen Hash-Baum mit im Backup und sendet dann das Wurzelverzeichnis (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 garantiert.

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.

15.11 Ein Backup manuell starten

1. Wählen Sie eine Maschine aus, die über mindestens einen auf sie angewendeten Schutzplan verfügt.
2. Klicken Sie auf den Befehl **Schützen**.
3. Sollten mehr als ein Schutzplan auf die Maschine angewendet werden, dann wählen Sie den gewünschten Schutzplan aus.
4. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Klicken Sie auf **Jetzt ausführen**. Es wird ein inkrementelles Backup erstellt.
   - Wenn das Backup-Schema mehrere Backup-Methoden beinhaltet, können Sie die zu verwendende Methode auswählen. Klicken Sie auf den Pfeil auf der Schaltfläche **Jetzt ausführen** und wählen Sie dann **Vollständig, Inkrementell** oder **Differentiell**.

Das erste Backup, welches ein Schutzplan erstellt, ist immer ein Voll-Backup.

Der Backup-Fortschritt für die Maschine wird in der Spalte **Status** angezeigt.

15.12 Standardoptionen für Backup

Die Standardwerte der Backup-Optionen (S. 156) 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 Service-Konsole an.
   - Um den Standardwert für eine Abteilung zu ändern, melden Sie sich als ein Administrator für die Abteilung an der Service-Konsole an.

- Um den Standardwert für Sie selbst zu ändern, melden Sie sich an der Service-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**.

15.13 Backup-Optionen

Wenn Sie die Backup-Optionen ändern wollen, müssen Sie im Backup-Modul des Schutzplans neben den **Backup-Optionen** auf den Befehl **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 (S. 159)	+	+	+	+	+	+	+	+	+	+
Backup-Konsolidierung (S. 159)	+	+	+	+	+	+	+	+	+	-
Backup-Dateiname (S. 160)	+	+	+	+	+	+	+	+	+	+
Backup-Format (S. 163)	+	+	+	+	+	+	+	+	+	+
Backup-Validierung (S. 164)	+	+	+	+	+	+	+	+	+	+
CBT (Changed Block Tracking) (S. 165)	+	-	-	-	-	-	+	+	-	-
Cluster-Backup-Modus (S. 165)	-	-	-	-	-	-	-	-	-	+
Komprimierungsgrad (S. 167)	+	+	+	+	+	+	+	+	+	+

	Backup auf Laufwerksebene			Backup auf Dateiebene			Virtuelle Maschinen			SQL und Exchange
	Windows	Linux	macOS	Windows	Linux	macOS	ESXi	Hyper-V	Virtuozzo	Windows
Fehlerbehandlung (S. 167)										
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 (S. 168)	+	+	+	-	-	-	-	-	-	-
Snapshot für Datei-Backups (S. 170)	-	-	-	+	+	+	-	-	-	-
Dateifilter (S. 168)	+	+	+	+	+	+	+	+	+	-
Forensische Daten (S. 171)	+	-	-	-	-	-	-	-	-	-
Protokollabschneidung (S. 179)	-	-	-	-	-	-	+	+	-	Nur SQL
LVM-Snapshot-Erfassung (S. 179)	-	+	-	-	-	-	-	-	-	-
Mount-Punkte (S. 179)	-	-	-	+	-	-	-	-	-	-

	Backup auf Laufwerksebene			Backup auf Dateiebene			Virtuelle Maschinen			SQL und Exchange
	Windows	Linux	macOS	Windows	Linux	macOS	ESXi	Hyper-V	Virtuozzo	Windows
Multi-Volume-Snapshot (S. 180)	+	+	-	+	+	-	-	-	-	-
Performance und Backup-Fenster (S. 181)	+	+	+	+	+	+	+	+	+	+
Physischer Datenversand (S. 183)	+	+	+	+	+	+	+	+	+	-
Vor-/Nach-Befehle (S. 184)	+	+	+	+	+	+	+	+	+	+
Befehle vor/nach der Datenerfassung (S. 186)	+	+	+	+	+	+	-	-	-	+
Planung (S. 188)										
Startzeiten in einem Zeitfenster verteilen	+	+	+	+	+	+	+	+	+	+
Die Anzahl gleichzeitig ausgeführter Backups begrenzen	-	-	-	-	-	-	+	+	+	-
Sektor-für-Sektor-Backup (S. 188)	+	+	-	-	-	-	+	+	+	-
Aufteilen (S. 189)	+	+	+	+	+	+	+	+	+	+
Task-Fehlerbehandlung (S. 189)	+	+	+	+	+	+	+	+	+	+
Task-Startbedingungen (S. 189)	+	+	-	+	+	-	+	+	+	+
VSS (Volume Shadow Copy Service) (S. 190)	+	-	-	+	-	-	-	+	-	+

	Backup auf Laufwerksebene			Backup auf Dateiebene			Virtuelle Maschinen			SQL und Exchange
	Windows	Linux	macOS	Windows	Linux	macOS	ESXi	Hyper-V	Virtuozzo	Windows
VSS (Volume Shadow Copy Service) für virtuelle Maschinen (S. 191)	-	-	-	-	-	-	+	+	-	-
Wöchentliche Backups (S. 192)	+	+	+	+	+	+	+	+	+	+
Windows-Ereignisprotokoll (S. 192)	+	-	-	+	-	-	+	+	-	+

15.13.1 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.

15.13.2 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 (S. 163) 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.

15.13.3 Backup-Dateiname

Die Option bestimmt die Namen der Backup-Dateien, die vom Schutzplan erstellt werden.

Diese Namen werden beispielsweise in einem Datei-Manager angezeigt, wenn der Backup-Speicherort durchsucht wird.

Was ist ein Backup-Datei?

Jeder Schutzplan erstellt eine oder mehrere Dateien am Backup-Speicherort – abhängig davon, welches Backup-Schema und welches Backup-Format (S. 163) 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) beim Erstellen oder Bearbeiten eines Schutzplans festlegen.

***Hinweis**: Der Zeitstempel wird nur beim Backup-Format **Version 11** dem Backup-Dateinamen hinzugefügt.*

Nachdem Sie einen Backup-Dateinamen geändert haben, wird das nächste Backup als Voll-Backup erstellt – außer Sie spezifizieren den Dateinamen eines bereits vorhandenen Backups auf derselben Maschine. Im letzteren Fall wird dann – gemäß der vorliegenden Schutzplanung – ein vollständiges, differentielles oder inkrementelles Backup erstellt.

Beachten Sie, dass es möglich ist, Backup-Dateinamen auch für Speicherorte festzulegen, die nicht von einem Datei-Manager durchsucht werden können (wie etwa der Cloud Storage). Dies macht dennoch Sinn, falls Sie sich die benutzerdefinierten Namen über die Registerkarte **Backup Storage** anzeigen lassen wollen.

Wo kann ich Backup-Dateinamen einsehen?

Gehen Sie zur Registerkarte **Backup Storage** und wählen die Gruppe der Backups 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**).

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**).

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 Office 365-Postfächern, die von einem lokalen Agenten für Office 365 erstellt wurden, lautet: **`[Mailbox ID]_mailbox_[Plan ID]A`**.

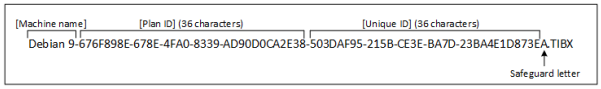
Der Standardname für Backups von Cloud-Applikationen, die von Cloud Agenten erstellt wurden, lautet: **`[Resource Name]_[Resource Type]_[Resource Id]_[Plan Id]A`**.

Der Standardname setzt sich aus folgenden Variablen zusammen:

- **`[Machine Name]`** – Diese Variable wird mit dem Namen der Maschine ersetzt (derselbe Name, der in der Service-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 Office 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]** enthalten.

Anwendungsbeispiele

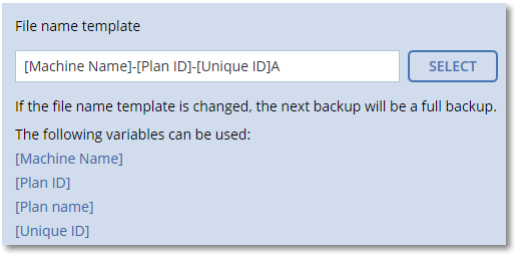
- **Benutzerfreundliche Dateinamen anzeigen**

  Sie möchten, dass Backups leicht unterscheidbar sind, wenn Sie den Backup-Speicherort mit einem Datei-Manager durchsuchen.

- **Eine vorhandene Sequenz von Backups fortsetzen**

  Nehmen wir an, ein Schutzplan wird auf eine einzelne Maschine angewendet und Sie müssen diese Maschine aus der Service-Konsole entfernen oder den Agenten inkl. seiner Konfigurationseinstellungen deinstallieren. Wenn die Maschine erneut hinzugefügt oder der Agent erneut installiert wird, können Sie den Schutzplan zwingen, für weitere Datensicherungen das bisherige Backup bzw. dieselbe Backup-Sequenz fortzusetzen. Nehmen Sie einfach diese Option, klicken Sie auf **Auswahl** und bestimmten Sie das gewünschte Backup.

  Die Schaltfläche **Auswahl** zeigt die Backups des Speicherorts an, der im Abschnitt **Backup-Ziel** des Schutzplan-Fensterbereichs ausgewählt wurde. Es kann nur dieser Speicherort durchsucht werden (und keine außerhalb davon liegenden Bereiche/Orte).

***Hinweis**: Die Schaltfläche **Auswahl** ist nur bei Schutzplänen verfügbar, die für ein einzelnes Gerät erstellt oder auf ein solches angewendet werden.*

15.13.4 Backup-Format

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

Die Option **Backup-Format** bestimmt das Format der Backups, die vom Schutzplan erstellt werden. Es gibt zwei Formate:

- **Version 11**

  Das herkömmliche Format (Legacy-Format), welches aus Gründen der Abwärtskompatibilität beibehalten wurde.

- **Version 12**

  Das neue Format, welches für schnelleres Backup und Recovery entwickelt 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 Sie jedoch 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 Backup-Format 'Version 12' unterstützt eine innerhalb des Archives erfolgende Deduplizierung (Archiv-interne Deduplizierung), die folgende Vorteile bietet:

- Reduzierte Backup-Größe im zigfachen Umfang durch integrierte Deduplizierung auf Block-Ebene mit jeder 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.*

15.13.5 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 direkt nach seiner Erstellung validiert.

Die Voreinstellung ist: **Deaktiviert**.

Bei einer Validierung wird für jeden Datenblock, der aus dem entsprechenden Backup wiederhergestellt werden kann, eine Prüfsumme berechnet. 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 ist ein zeitaufwendiger Prozess (auch bei inkrementellen oder differentiellen Backups, die normalerweise kleiner sind). Hintergrund ist, dass die Aktion nicht einfach nur die tatsächlich in dem betreffenden Backup enthaltenen Daten validiert, sondern alle Daten, die ausgehend von diesem Backup wiederherstellbar sind. Dies erfordert unter Umständen auch einen Zugriff auf zuvor erstellte (abhängige) Backups.

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. Wenn Sie ein Betriebssystem per Backup gesichert haben und dieses zusätzlich testen wollen, empfehlen wir Ihnen, dass Sie mit einem Boot-Medium eine Testwiederherstellung auf ein freies, überzähliges Laufwerk durchführen. In einer ESXi- oder Hyper-V-Umgebungen können Sie eine entsprechende virtuelle Maschine auch direkt aus dem Backup heraus ausführen (S. 296).

***Hinweis**: Eine Validierung ist bei einem Cloud Storage möglich, der sich entweder in einem Acronis Datacenter befindet oder von einem Acronis Partner bereitgestellt wird.*

15.13.6 CBT (Changed Block Tracking)

Diese Option gilt nur für Laufwerk-Backups von virtuellen Maschinen und von physischen Maschinen, die unter Windows laufen. Sie gilt außerdem auch für Backups von Microsoft SQL Server- und 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.

15.13.7 Cluster-Backup-Modus

***Hinweis**: Diese Funktionalität ist in den Standard-Editionen des Cyber Protection Service nicht 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.

15.13.8 Komprimierungsgrad

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 den Backup-Prozess, verkleinert aber den benötigten Backup-Speicherplatz. Derzeit funktionieren die hohen und maximalen Grade 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.

15.13.9 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: 30. Abstand 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 der Speicherort des Backups im Netzwerk nicht verfügbar/erreichbar ist, wird das Programm 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.

Cloud Storage

Wenn Sie den Cloud Storage als Backup-Ziel auswählen, wird der Optionswert automatisch auf **Aktiviert** gesetzt. **Anzahl der Versuche: 300**. **Abstand zwischen den Versuchen: 30 Sekunden.**

Die tatsächliche Anzahl der Versuche ist in diesem Fall unbegrenzt. Die Zeitüberschreitung (Timeout), bevor das Backup als fehlgeschlagen gilt, wird dagegen folgendermaßen berechnet: (300 Sekunden + **Abstand zwischen den Versuchen**) * (**Anzahl der Versuche** + 1).

Beispiele:

- Mit den Standardwerten wird das Backup nach folgender Zeit fehlschlagen: 99330 Sekunden bzw. ca. 27,6 Stunden = (300 Sekunden + 30 Sekunden) * (300 + 1).

- Wenn Sie die **Anzahl der Versuche** auf 1 und den **Abstand zwischen den Versuchen** auf 1 Sekunde festlegen, wird das Backup nach folgender Zeit fehlschlagen: 602 Sekunden bzw. ca. 10 Minuten = (300 Sekunden + 1 Sekunde) * (1 + 1).

Wenn der berechnete Timeout-Wert 30 Minuten überschreitet und die Datenübertragung noch nicht gestartet wurde, wird die tatsächliche Zeitüberschreitung auf 30 Minuten gesetzt.

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.

Erneut versuchen, wenn bei der VM-Snapshot-Erstellung ein Fehler auftritt

Die Voreinstellung ist: **Aktiviert. Anzahl der Versuche: 3. Abstand 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.

15.13.10 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.

15.13.11 Dateifilter

Dateifilter definieren, welche Dateien und Ordner während des Backup-Prozesses übersprungen werden sollen.

Dateifilter stehen, sofern nicht anders angegeben, für Backups auf Laufwerk- und Dateiebene zur Verfügung.

So können Sie Dateifilter aktivieren

1. Wählen Sie die Daten für das Backup aus.
2. Klicken Sie neben **Backup-Optionen** auf **Ändern**.
3. Wählen Sie **Dateifilter**.
4. Verwenden Sie eine der nachfolgend beschriebenen Optionen.

Dateien ausschließen, die bestimmte Kriterien erfüllen

Es gibt zwei Optionen, die auf gegensätzliche Weise funktionieren.

- **Nur Dateien ins Backup einschließen, die folgende Kriterien erfüllen**

  Beispiel: Falls Sie festlegen, dass die komplette Maschine gesichert werden soll, und dann den Eintrag '**C:\Datei.exe**' in den Filterkriterien spezifizieren, wird nur diese Datei im Backup gesichert.

  Hinweis: *Dieser Filter wirkt sich nicht auf Datei-Backups aus, wenn* ***Version 11*** *beim* ***Backup-Format*** *(S. 163) ausgewählt ist und das Backup-Ziel NICHT der Cloud Storage ist.*

- **Dateien vom Backup ausschließen, die folgende Kriterien erfüllen**

  Beispiel: Falls Sie festlegen, dass die komplette Maschine gesichert werden soll, und dann den Eintrag '**C:\Datei.exe**' in den Filterkriterien spezifizieren, wird genau diese (und nur diese) Datei beim Backup übersprungen.

Es ist auch möglich, beide Optionen gemeinsam zu verwenden. Die letzte Option überschreibt die vorhergehende, was bedeutet: falls Sie '**C:\Datei.exe**' in beiden Feldern spezifizieren, wird die Datei beim Backup übersprungen.

Kriterien

- **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.

  Sowohl unter Windows wie auch unter Linux/macOS können Sie in den Datei- bzw. Ordnerpfaden einen normalen Schrägstrich (Slash) verwenden (Beispiel: **C:/Temp/Datei.tmp**). Unter Windows können Sie zudem den herkömmlichen, nach links geneigten Schrägstrich (Backslash) verwenden (Beispiel: **C:\Temp\Datei.tmp**).

- **Name**

  Spezifizieren Sie den Namen der Datei oder des Ordners (Beispiel: **Dokument.txt**). Es werden alle Dateien und Ordner mit diesem Namen ausgewählt.

Bei den Kriterien wird die Groß-/Kleinschreibung *nicht* beachtet. Wenn Sie beispielsweise **C:\Temp** spezifizieren, wird **C:\TEMP**, **C:\temp** usw. ausgewählt.

Sie können ein oder mehrere Platzhalterzeichen (*, ** und ?) in dem Kriterium verwenden. Diese Zeichen können innerhalb des vollständigen Pfades und im Namen der Datei oder des Ordners verwendet werden.

Der Asterisk (*) ersetzt null bis mehrere Zeichen in einem Dateinamen. So beinhaltet beispielsweise das Kriterium **Dok*.txt** Dateien wie **Dok.txt** und **Dokument.txt**.

[Nur für Backups im Format **Version 12**] Der doppelte Asterisk (**) ersetzt null bis mehrere Zeichen in einem Dateinamen und Pfad (Schrägstriche eingeschlossen). Beispielweise schließt das Kriterium ****/Docs/**.txt** alle txt-Dateien in allen Unterordnern von allen Ordnern mit der Bezeichnung **Docs** ein.

Das Fragezeichen (?) steht für exakt ein Zeichen in einem Dateinamen. Beispielsweise schließt das Kriterium **Dok?.txt** Dateien wie **Dok1.txt** und **Doks.txt** ein – während Dateien wie **Dok.txt** oder **Dok11.txt** ausgeschlossen werden.

Versteckte Dateien und Ordner ausschließen

Aktivieren Sie dieses Kontrollkästchen, um Dateien und Ordner zu überspringen, die mit dem Attribut **Versteckt** gekennzeichnet sind (bei Windows-typischen Dateisystemen) – oder die mit einem Punkt (.) beginnen (bei Linux-typischen Dateisystemen wie Ext2 und Ext3). Bei Ordnern mit dem Attribut 'Versteckt' wird der gesamte Inhalt ausgeschlossen (einschließlich solcher Dateien, die nicht versteckt sind).

Systemdateien und Systemordner ausschließen

Diese Option ist nur für Dateisysteme wirksam, die von Windows unterstützt werden. Aktivieren Sie dieses Kontrollkästchen, um alle Dateien und Ordner mit dem Attribut **System** zu überspringen. Bei Ordnern mit dem Attribut **System** wird der gesamte Inhalt ausgeschlossen (einschließlich solcher Dateien, die nicht mit dem Attribut **System** gekennzeichnet sind).

Tipp: *Sie können die Attribute von Dateien oder Ordnern über ihre Datei- bzw. Ordner-Eigenschaften oder den Kommandozeilenbefehl 'attrib' überprüfen. Weitere Informationen finden Sie im Hilfe und Support-Center von Windows.*

15.13.12 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.

15.13.13 Forensische Daten

Schadprogramme wie Viren, Malware oder Ransomware können auf einer Maschine bösartige bzw. schädliche Aktivitäten ausführen. Ein anderes Beispiel, bei dem Untersuchungen angebracht sein können, wäre es, wenn Daten auf einer Maschine durch Fremdprogramme unberechtigt geändert oder gestohlen werden. Bei all diesen Aktivitäten können Untersuchungen sinnvoll sein. Diese sind jedoch nur vernünftig möglich, wenn Sie auf der zu untersuchenden Maschine digitale Beweise erfassen. Solche Beweise (wie beispielsweise bestimmte Dateien oder andere Datenspuren) können jedoch leicht gelöscht werden bzw. verloren gehen oder die komplette Maschine fällt so aus, dass sie nicht mehr verfügbar ist.

Die Backup-Option **Forensische Daten** ermöglicht Ihnen, solche digitalen Beweismittel zu sammeln. Diese können dann für forensische Untersuchungen (z.B. durch Kriminalermittler) verwendet werden. Folgende Datenelemente können als digitale Beweismittel verwendet werden: ein Snapshot des nicht verwendeten Speicherplatzes auf dem Laufwerk, ein Speicherabbild (Memory Dump) des Arbeitsspeichers sowie ein Snapshot der laufenden Prozesse. Die Funktion **Forensische Daten** ist nur bei Erstellung eines 'Backups der kompletten Maschine' verfügbar.

Derzeit ist die Option **Forensische Daten** außerdem nur für Windows-Maschinen mit folgenden Betriebssystemversionen verfügbar:

- Windows 8.1, Windows 10
- Windows Server 2012 R2 – Windows Server 2019

***Hinweis**:*
• Wenn ein Schutzplan mit aktiviertem Backup-Modul auf eine Maschine angewendet wurde, können die 'Forensische Daten'-Einstellungen nicht nachträglich geändert werden. Erstellen Sie einen neuen Schutzplan, wenn Sie andere 'Forensische Daten'-Einstellungen verwenden wollen.
• Bei Maschinen, die über ein VPN mit Ihrem Netzwerk verbunden sind und keinen direkten Internetzugang haben, werden keine Forensik-Backups unterstützt.

Folgende Speicherorte für Backups mit forensischen Daten werden unterstützt:

- Cloud Storage
- Lokaler Ordner

  ***Hinweise**:*
  1. Ein lokaler Ordner als Speicherort wird nur unterstützt, wenn sich dieser auf einer per USB angeschlossenen Festplatte befindet.
  2. Lokale dynamische Datenträger werden nicht als Speicherort für Forensik-Backups unterstützt.

- Netzwerkordner

Backups mit forensischen Daten werden automatisch digital beglaubigt. Durch ein Forensik-Backup können Ermittler auch solche Laufwerksbereiche untersuchen, die normalerweise in einem herkömmlichen Laufwerk-Backup nicht enthalten sind.

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 Service-Konsole zu **Geräte** –> **Alle Geräte**. Alternativ können Sie den Schutzplan auch über die Registerkarte **Pläne** 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.

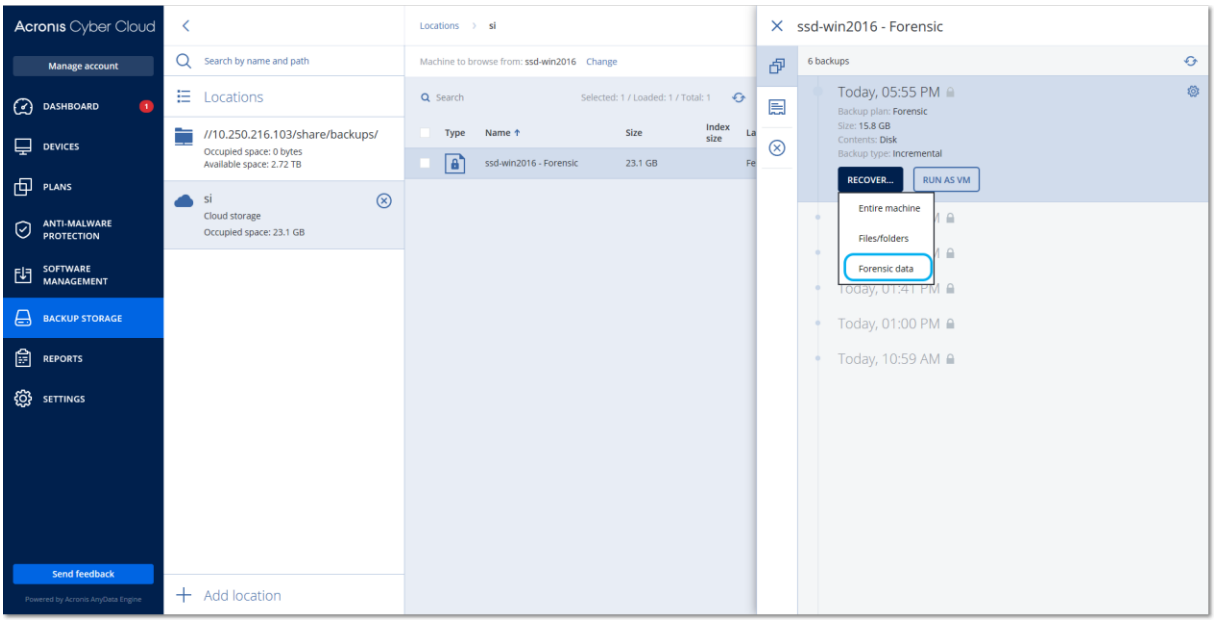
   ***Hinweis**: Ein vollständiges Speicherabbild kann auch sensible Daten wie Kennwörter enthalten.*
8. Spezifizieren Sie den Speicherort.
9. Klicken Sie auf **Jetzt ausführen**, wenn Sie wollen, dass das Forensik-Backup direkt erstellt wird – oder warten Sie, bis das Backup gemäß seiner Planung ausgeführt wird.
10. Gehen Sie zu **Dashboard** –> **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.

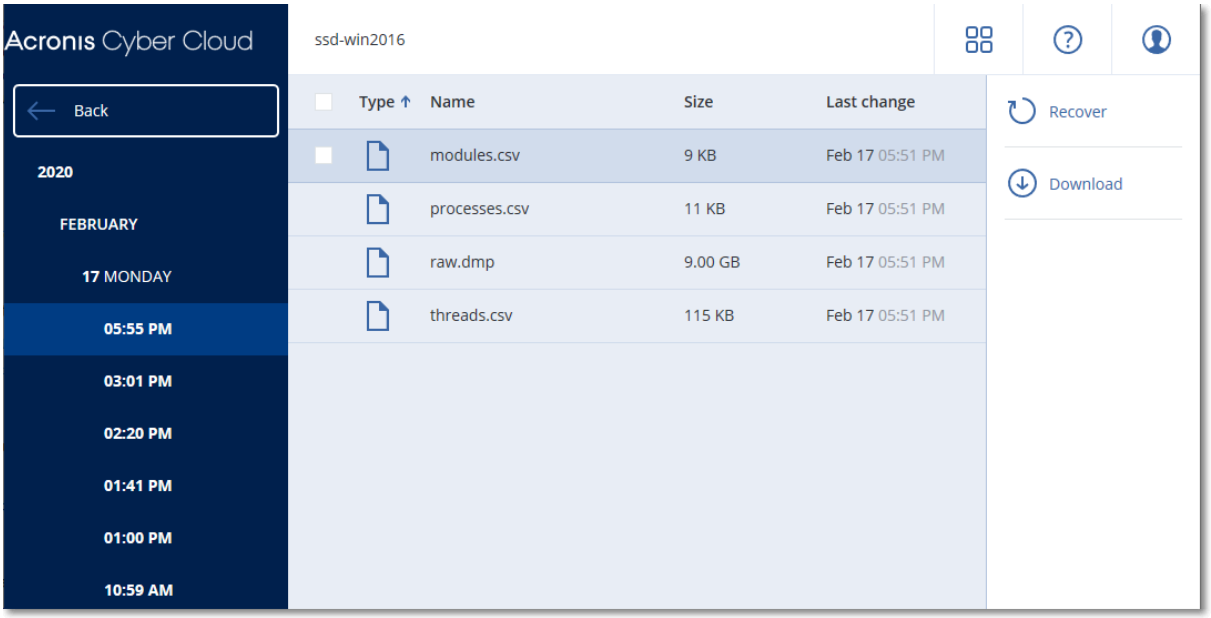
Wie können Sie die forensischen Daten aus einem Backup abrufen?

1. Gehen Sie in der Service-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 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.

15.13.13.1 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

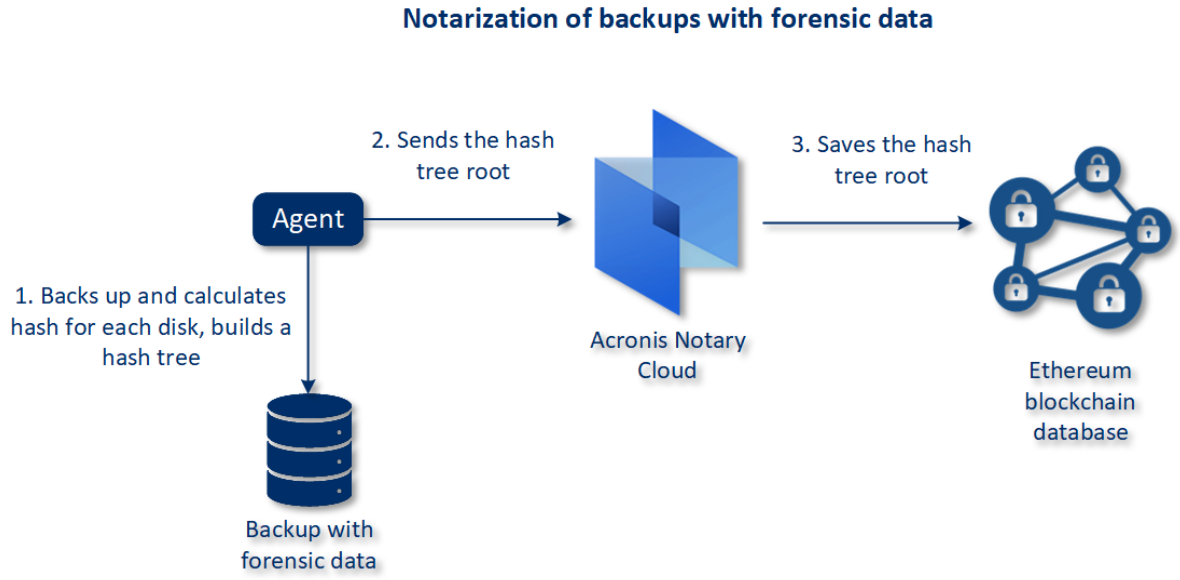
Mit der Beglaubigungsfunktion können Sie überprüfen und belegen, dass ein Laufwerk mit forensischen Daten authentisch ist und die entsprechenden Daten seit der ursprünglichen Backup-Erfassung nicht geändert wurden.

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 (S. 175)).

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.

15.13.13.2 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:\Program Files\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\Default\<tenant_login>\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
```

Output template:

```
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-256-Algorithmus 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 Webkonsole 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\folder** ▪ Cloud Storage **--loc=<IP_address>:443 --cert=<path_to_certificate> [--storage_path=/1]** **<IP_address>** – kann unter Windows im folgenden Registry-Schlüssel gefunden werden: HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\BackupAndRecovery\Settings\OnlineBackup\FesAddressCache\Default\<Mandanten-Anmeldename>\FesUri **<path_to_certificate>** – der Pfad zur Zertifikatsdatei, um auf Cyber Cloud zugreifen zu können. Unter Windows befindet sich dieses Zertifikat beispielsweise im Ordner **C:\ProgramData\Acronis\BackupAndRecovery\OnlineBackup\Default\<username>.crt** – wobei <username> Ihrem Kontonamen entspricht, den Sie für den Zugriff auf Cyber 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=KENNWORT	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%

15.13.14 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-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).

15.13.15 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 daher nur zu ändern, falls es ansonsten 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.

15.13.16 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 (S. 217) 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** (S. 217) wiederhergestellt werden.

Die Voreinstellung ist: **Deaktiviert**.

Tipp: *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 (S. 217) 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**.

15.13.17 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 (S. 170) 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.

15.13.18 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.

Sie können diese Option für jeden im Schutzplan angegebenen Speicherort separat konfigurieren. Wenn Sie diese Option für einen Replikationsspeicherort konfigurieren wollen, klicken Sie auf das Zahnradsymbol neben dem Speicherortnamen und anschließend auf **Performance und Backup-Fenster**.

Diese Option gilt nur für Backup- und Backup-Replikationsprozesse. 'Nach-Backup'-Befehle und andere Aktionen, die in einem Schutzplan enthalten sind (wie Validierung oder Konvertierung zu einer virtuellen Maschine), 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 **Niedriger als normal**).
- Ausgabegeschwindigkeit: **Unbegrenzt.**

Wenn diese Option aktiviert ist, werden geplante Backups gemäß den für die aktuelle Stunde angegebenen Performance-Parametern zugelassen oder blockiert. Zu Beginn einer Stunde, in welcher Backups blockiert werden, wird ein Backup-Prozess automatisch gestoppt und ein entsprechender Alarm generiert.

Auch wenn geplante Backups blockiert werden, kann ein Backup immer noch manuell gestartet werden. Es werden die Performance-Parameter der letzten Stunde verwendet, zu der Backups erlaubt waren.

Backup-Fenster

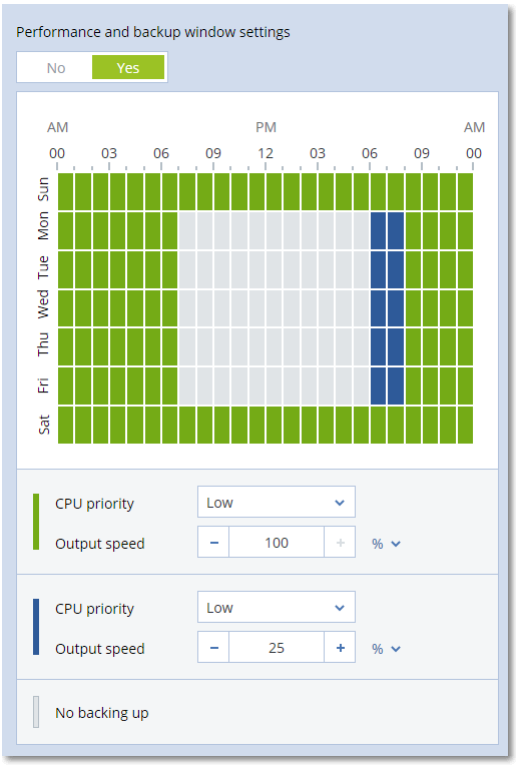
Jedes Rechteck repräsentiert eine Stunde innerhalb eines Wochentages. Klicken Sie auf ein Rechteck, um zwischen folgenden Zustände zu wechseln:

- **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.



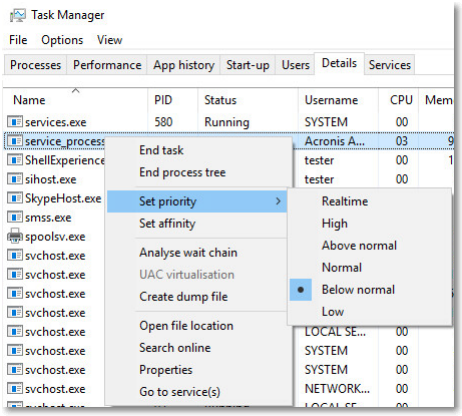
CPU-Priorität

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 OS X.



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).

15.13.19 Physischer Datenversand

Diese Option gilt, wenn als Backup-Ziel der Cloud Storage verwendet wird und das Backup-Format (S. 163) mit **Version 12** festgelegt 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.

Diese Option bestimmt, ob das erste Voll-Backup, welches durch einen entsprechenden Schutzplan erstellt wurde, auf einem Festplattenlaufwerk gespeichert und dann über den Service 'Physische Datenversand' (Physical Data Shipping) in den Cloud Storage übertragen wird. Alle dazugehörigen, nachfolgenden inkrementellen Backups können dann über das Netzwerk/Internet durchgeführt werden.

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. Erstellen Sie einen neuen Schutzplan. Aktivieren Sie in diesem Plan die Backup-Option **Physischer Datenversand**.

   Sie können das Backup direkt auf dem für den Versand verwendeten Laufwerk erstellen lassen – oder zuerst in einen lokalen Ordner oder Netzwerkordner speichern und das Backup anschließend auf das Laufwerk kopieren.

   ***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.*

2. 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**.

3. 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.*

4. 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.

15.13.20 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'.

15.13.20.1 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.

15.13.20.2 Befehlsausführung nach dem Backup

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 ausgeführt werden soll.
4. Geben bei Bedarf im Feld **Argumente** eventuell benötigte Parameter für die Befehlsausführung ein.

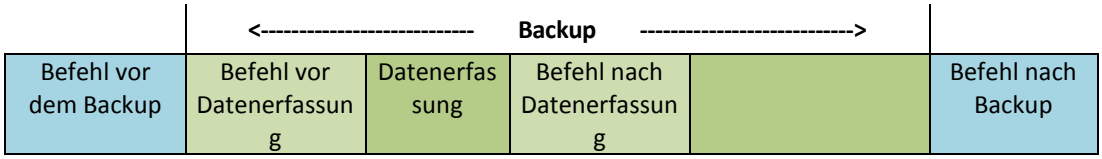
5. Aktivieren Sie das Kontrollkästchen **Backup scheitern lassen, wenn die Befehlsausführung fehlschlägt**, sofern eine erfolgreiche Ausführung des Befehls besonders wichtig für Sie ist. Ein Befehl wird als 'fehlgeschlagen' betrachtet, wenn sein Exit-Code ungleich Null ist. Sollte die Befehlsausführung 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**.

15.13.21 Befehle vor/nach der Datenerfassung

Diese Option ermöglicht die Definition von Befehlen, die automatisch vor oder nach der Datenerfassung (also Erstellung des Daten-Snapshots) durchgeführt werden. Die Datenerfassung wird zu Beginn der Backup-Prozedur durchgeführt.

Das folgende Schema zeigt, wann diese Befehle ausgeführt werden.



Wenn die Option Volume Shadow Copy Service (VSS) (S. 190) aktiviert ist, werden die Ausführung der Befehle und die Aktionen von Microsofts VSS folgendermaßen eingeordnet:

Befehle „vor Datenerfassung“ -> VSS Suspend -> Datenerfassung -> VSS Resume -> 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.

15.13.21.1 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	Ausgewählt	Deaktiviert	Ausgewählt	Deaktiviert

fehlschlägt*				
Datenerfassung erst ausführen, wenn die Befehlsausführung abgeschlossen ist	Ausgewählt	Ausgewählt	Deaktiviert	Deaktiviert
Ergebnis				
	Voreinstellung Datenerfassung nur ausführen, nachdem der Befehl erfolgreich durchgeführt wurde. Backup scheitern lassen, wenn die Befehlsausführung fehlschlägt.	Datenerfassung nach Befehlsausführung fortsetzen, unabhängig vom Erfolg oder Misserfolg der Ausführung.	Nicht verfügbar	Datenerfassung gleichzeitig mit Befehlsausführung durchführen, unabhängig vom Ergebnis der Befehlssausführung.

* Ein Befehl wird als 'fehlgeschlagen' betrachtet, wenn sein Exit-Code ungleich Null ist.

15.13.21.2 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.

15.13.22 Planung

Mit dieser Option können Sie festlegen, ob Backups nach Planung oder mit einer Verzögerung starten sollen – und wie viele virtuelle Maschinen gleichzeitig gesichert werden.

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**

  Diese Option ist nur dann verfügbar, wenn ein Schutzplan auf mehrere virtuelle Maschinen angewendet wird. Diese Option definiert, wie viele virtuelle Maschinen ein Agent gleichzeitig sichern kann, wenn er den gegebenen Schutzplan ausführt.

  Falls ein Agent gemäß eines Schutzplans ein gleichzeitiges Backup mehrerer Maschinen starten muss, wird dieser zwei Maschinen auswählen. (Zur Optimierung der Backup-Performance versucht der Agent Maschinen zuzuweisen, die auf verschiedenen Storages gespeichert sind). Sobald eines der beiden Backups abgeschlossen ist, wählt der Agent eine dritte Maschine und so weiter.

  Sie können die Anzahl der virtuellen Maschinen ändern, die ein Agent gleichzeitig sichern soll. Der maximale Wert ist 10. Wenn der Agent jedoch mehrere Schutzpläne ausführt, die sich zeitlich überlappen, werden die in deren Optionen angegebenen Zahlen addiert. Sie können die Gesamtzahl der virtuellen Maschinen (S. 316), die ein Agent gleichzeitig sichern kann, begrenzen – unabhängig davon, wie viele Schutzpläne ausgeführt werden.

  Die Backups von physischen Maschinen werden wie im Plan definiert gestartet.

15.13.23 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 (S. 167)' 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.

***Anmerkung**: Es wird unmöglich sein, eine Wiederherstellung der Anwendungsdaten aus den Backups durchzuführen, die im Sektor-für-Sektor-Modus erstellt wurden.*

15.13.24 Aufteilen

Mit dieser Option können Sie festlegen, ob und wie große Backups in kleinere Dateien aufgeteilt werden sollen.

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.

15.13.25 Task-Fehlerbehandlung

Diese Option bestimmt, wie sich das Programm verhalten soll, wenn die geplante Ausführung eines Schutzplans fehlschlägt. 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).

Die Voreinstellung ist: **Deaktiviert**.

15.13.26 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 dazu finden Sie im Abschnitt 'Startbedingungen'.

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.

15.13.27 VSS (Volume Shadow Copy Service)

Diese Option gilt nur für Windows-Betriebssysteme.

Diese Option definiert, ob ein VSS-Provider (Volume Shadow Copy Service) die VSS-konforme Applikationen benachrichtigen muss, dass ein Backup startet. Dies 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.

Die Voreinstellung ist: **Aktiviert**. **Snapshot Provider automatisch auswählen**.

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, diese Option beim Backup von Applikationsservern (Microsoft Exchange Server, Microsoft SQL Server, Microsoft SharePoint oder Active Directory) zu verwenden.

Deaktivieren Sie diese Option, wenn Ihre Datenbank nicht VSS-kompatibel ist. Snapshots werden zwar schneller erfasst, aber die Datenkonsistenz von Applikationen, deren Transaktionen zum Zeitpunkt des Snapshots nicht vollendet sind, kann nicht garantiert werden. Mit definierbaren Befehlen vor/nach der Datenerfassung (S. 186) können Sie sicherstellen, dass die Daten in einem konsistenten Zustand gesichert wurden. Spezifizieren Sie z.B. einen Befehl vor der Datenerfassung, der diese Datenbank anhält und alle Cache-Speicher leert, um zu sichern, dass alle Transaktionen vollendet sind – und ergänzen Sie Befehle nach der Datenerfassung, damit die Datenbank nach der Snapshot-Erstellung den Betrieb wieder aufnimmt.

Hinweis: *Wenn diese Option aktiviert ist, werden alle Dateien, die im Registry-Schlüssel '**HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToSnapshot**' spezifiziert sind, nicht per Backup gesichert. Es werden insbesondere keine offline Outlook-Datendateien (.ost) gesichert, da diese im Wert '**OutlookOST**' dieses Schlüssels spezifiziert sind.*

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 Dritthersteller-Software zum Backup von Exchange Server-Daten verwenden. Hintergrund ist, dass die Protokollabschneidung die aufeinanderfolgenden Transaktionsprotokoll-Backups beeinträchtigt.
- Falls Sie eine Dritthersteller-Software zum Backup der SQL Server-Daten verwenden. Hintergrund ist, dass die Dritthersteller-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 Dritthersteller-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.

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 (S. 179) aktivieren.

15.13.28 VSS (Volume Shadow Copy Service) für virtuelle Maschinen

Diese Option definiert, ob die virtuellen Maschinen mit stillgelegten (quiesced) Snapshots erfasst werden sollen. 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 oder der Virtuozzo Guest Tools.

Die Voreinstellung ist: **Aktiviert**.

Eine Aktivierung dieser Option bewirkt, dass die Transaktionen aller VSS-konformen Applikationen einer virtuellen Maschine abgeschlossen werden, bevor der Snapshot erfasst wird. Falls ein stillgelegter Snapshot (nach einer in der Option 'Fehlerbehandlung (S. 167)' spezifizierten Anzahl von Neuversuchen) fehlschlägt und die Option 'Applikations-Backup' deaktiviert ist, wird ein 'nicht stillgelegter' (non-quiesced) Snapshot erstellt. Sollte die Option 'Applikations-Backup' aktiviert sein, wird das Backup fehlschlagen.

Wenn diese Option deaktiviert ist, wird ein 'nicht stillgelegter' (non-quiesced) Snapshot erstellt. Die Maschine wird dann in einem 'crash-konsistenten' Zustand gesichert.

15.13.29 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**.

15.13.30 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**.

15.14 Recovery

15.14.1 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.

Recovery-Quelle		Recovery-Methode
Physische Maschine (Windows oder Linux)		Weboberfläche verwenden (S. 197) Boot-Medium verwenden (S. 201)
Physische Maschine (Mac)		Boot-Medium verwenden (S. 201)
Virtuelle Maschine (VMware oder Hyper-V)		Weboberfläche verwenden (S. 200) Boot-Medium verwenden (S. 201)
Virtuelle Maschine oder Container (Virtuozzo)		Weboberfläche verwenden (S. 200)
ESXi-Konfiguration		Boot-Medium verwenden (S. 211)
Dateien/Ordner		Weboberfläche verwenden (S. 206) Dateien aus dem Cloud Storage herunterladen (S. 207) Boot-Medium verwenden (S. 209) Dateien aus lokalen Backups extrahieren (S. 210)
Systemzustand		Weboberfläche verwenden (S. 211)
SQL-Datenbanken		Weboberfläche verwenden (S. 235)
Exchange-Datenbanken		Weboberfläche verwenden (S. 238)
Exchange-Postfächer		Weboberfläche verwenden (S. 241)
Websites		Weboberfläche verwenden (S. 294)
Microsoft Office 365	Postfächer (lokaler Agent für Office 365)	Weboberfläche verwenden (S. 254)
	Postfächer (lokaler Agent für Office 365)	Weboberfläche verwenden (S. 259)
	Öffentliche Ordner	Weboberfläche verwenden (S. 261)
	OneDrive-Dateien	Weboberfläche verwenden (S. 264)
	SharePoint Online-Daten	Weboberfläche verwenden (S. 268)
G Suite	Postfächer	Weboberfläche verwenden (S. 281)

Recovery-Quelle		Recovery-Methode
	Google Drive-Dateien	Weboberfläche verwenden (S. 285)
	Shared Drive-Dateien	Weboberfläche verwenden (S. 289)

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.

15.14.2 Safe Recovery

Ein per Backup-Image gesichertes Betriebssystem kann Malware enthalten, durch die eine Maschine nach der Wiederherstellung erneut infiziert werden kann.

Mit der Funktion 'Safe Recovery' (sichere Wiederherstellung) können Sie verhindern, dass Infektionen erneut auftreten, indem Sie während eines Wiederherstellungsprozesses das integrierte Anti-Malware-Scanning (S. 381) sowie die Malware-Erkennung verwenden.

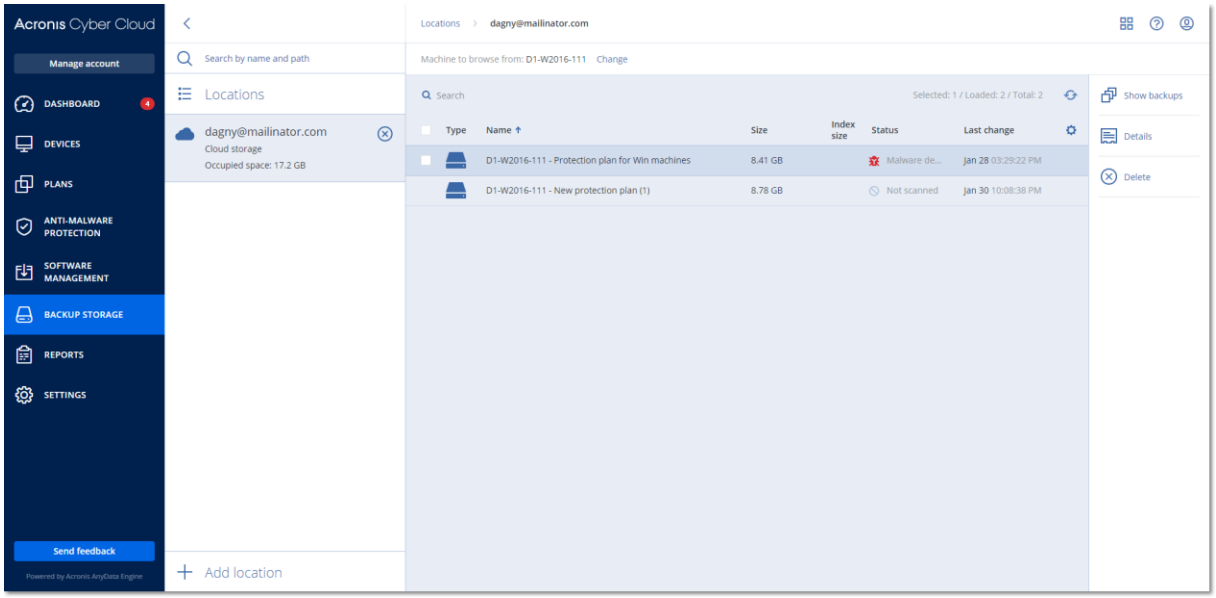
Einschränkungen:

- Die Safe Recovery-Funktion wird nur für physische oder virtuelle Windows-Maschinen unterstützt, auf denen zudem der Agent für Windows installiert ist.
- Bei den Backup-Typen werden nur die Backup-Quellen 'Komplette Maschine' oder 'Laufwerke/Volumes' unterstützt.
- Safe Recovery wird nur für Volumes mit dem Dateisystem 'NTFS' unterstützt. Nicht-NTFS-Volumes werden wiederhergestellt, ohne dass das Anti-Malware-Scanning ausgeführt wird.
- Safe Recovery wird nicht für CDP-Backups (S. 130) unterstützt. Die Maschine wird auf der Grundlage des letzten regelmäßigen Backups wiederhergestellt – ohne die Daten des CDP-Backups. Wenn Sie die CDP-Daten wiederherstellen wollen, müssen Sie eine Wiederherstellung von **Dateien/Ordnern** starten.

Und so funktioniert es

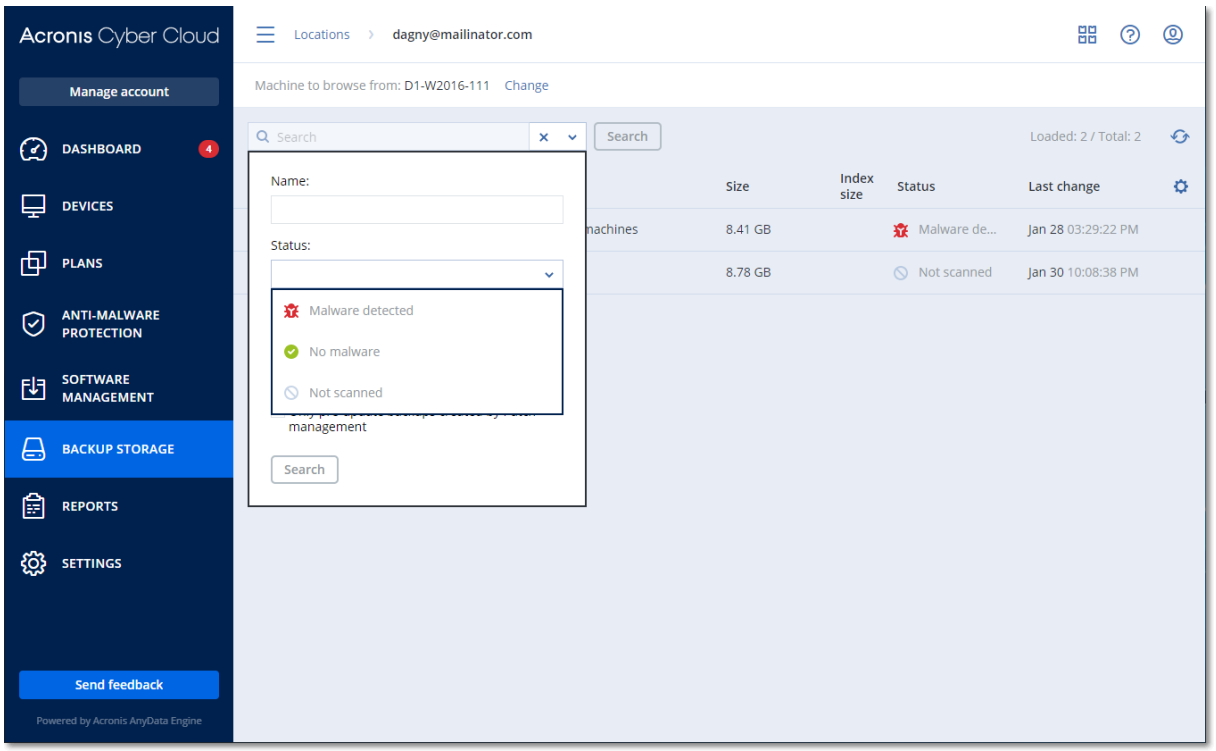
Wenn Sie während des Wiederherstellungsprozesses die Safe Recovery-Option aktivieren, wird das System folgende Aktionen durchführen:

1. Das Image-Backup wird nach Malware gescannt und die infizierte Dateien werden gekennzeichnet. Dem Backup wird einer der folgenden Statuszustände zugewiesen:
   - **Keine Malware** – beim Scannen wurde keine Malware im Backup gefunden.
   - **Malware erkannt** – beim Scannen wurde Malware im Backup gefunden.
   - **Nicht gescannt** – das Backup wurde nicht nach Malware gescannt.



2. Das Backup wird zu der ausgewählten Maschine wiederhergestellt.
3. Die erkannte Malware wird gelöscht.

Sie können Backups über den Parameter **Status** filtern.



15.14.3 Ein Boot-Medium erstellen

Ein Boot-Medium ist eine CD, eine DVD, ein USB-Stick oder ein anderes Wechselmedium, welches Ihnen ermöglicht, den Agenten ohne die Hilfe des eigentlichen Betriebssystems auszuführen. Der Haupteinsatzzweck eines Boot-Mediums besteht in der Möglichkeit, ein System wiederherzustellen, welches nicht mehr starten (booten) kann.

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 Boot-Medium unter Windows oder Linux erstellen

1. Laden Sie die ISO-Datei des Boot-Mediums herunter. Wählen Sie zum Herunterladen der Datei eine Maschine aus – und klicken Sie dann auf **Wiederherstellen** > **Weitere Wiederherstellungsmöglichkeiten...** > **ISO-Image herunterladen**.
2. [Optional] Kopieren, drucken oder notieren Sie sich das Registrierungstoken, das von der Service-Konsole angezeigt wird.

   Mit diesem Token können Sie von einem Boot-Medium aus direkt auf den Cloud Storage zugreifen, ohne Ihre Anmeldedaten eingeben zu müssen. Dies ist notwendig, wenn Sie sich nicht selbst direkt an der Cloud anmelden können, sondern stattdessen eine Drittanbieter-Authentifizierung verwenden.
3. Gehen Sie nach einer der folgenden Möglichkeiten vor:
   - 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.
   - Mounten Sie die ISO-Datei als CD-/DVD-Laufwerk für diejenige virtuelle Maschine, die Sie wiederherstellen wollen.

So können Sie ein Boot-Medium unter macOS erstellen

1. Klicken Sie auf einer Maschine, auf welcher der Agent für Mac installiert ist, im Menü **Programme** 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 diesem Laufwerk werden gelöscht.*
3. Klicken Sie auf **Erstellen**.
4. Warten Sie, bis die Software das Boot-Medium erstellt hat.

15.14.4 Startup Recovery Manager

Der Startup Recovery Manager ist eine spezielle bootfähige Komponente, die sich auf dem Systemlaufwerk (bei Windows) oder auf der '/boot'-Partition (bei Linux) befindet und so konfiguriert ist, dass sie gestartet wird, wenn während des Boot-Vorgangs des Computers die F11-Taste gedrückt

wird. Diese Komponente ist eine alternative und bequeme Möglichkeit, das bootfähige Notfallwerkzeug starten zu können, ohne (wie sonst) ein separates Boot-Medium (in Form eines physischen Datenträgers oder per Netzwerkverbindung zu einem PXE Server) starten zu müssen.

Startup Recovery Manager ist besonders nützlich für Benutzer, die häufig auf Reisen sind. Wenn ein Fehler auftritt, booten Sie die Maschine einfach neu und drücken dann die F11-Taste, sobald die Meldung „Druecken Sie F11 zum Ausfuehren des Acronis Startup Recovery Manager…“ erscheint. Das Programm wird daraufhin gestartet und Sie können mit einer Wiederherstellung beginnen.

Sie können mit dem Startup Recovery Manager natürlich auch Backups erstellen (wenn Sie unterwegs sind).

Auf Maschinen, auf denen ein GRUB-Boot-Loader installiert ist, müssen Sie den Startup Recovery Manager aus dem GRUB-Boot-Menü auswählen, statt (wie sonst) die F11-Taste zu drücken.

Eine Maschine, die mit dem Startup Recovery Manager gebootet wird, kann genauso auf dem Management Server registriert werden, wie eine Maschine, die mit einem normalen Boot-Medium gestartet wurde. Klicken Sie dazu auf die Befehlsfolge **Extras** –> **Medium auf dem Management Server registrieren** und befolgen Sie dann die im Abschnitt 'Medien auf dem Management Server registrieren' beschriebene Schritt-für-Schritt-Prozedur.

Den Startup Recovery Manager aktivieren

Auf einer Maschine, auf welcher der Agent für Windows oder der Agent für Linux ausgeführt wird, kann der Startup Recovery Manager über die Service-Konsole aktiviert werden.

So können Sie den Startup Recovery Manager in der Service-Konsole aktivieren

1. Wählen Sie die Maschine aus, auf welcher Sie den Startup Recovery Manager aktivieren wollen.
2. Klicken Sie auf **Details**.
3. Aktivieren Sie den Schalter für den **Startup Recovery Manager**.
4. Warten Sie, bis die Software den Startup Recovery Manager aktiviert hat.

So können Sie den Startup Recovery Manager auf einer Maschine ohne Agenten aktivieren

1. Booten Sie die Maschine mithilfe eines Boot-Mediums.
2. Klicken Sie auf **Extras** –> **Startup Recovery Manager aktivieren**.
3. Warten Sie, bis die Software den Startup Recovery Manager aktiviert hat.

Was passiert, wenn Sie den Startup Recovery Manager aktivieren

Die Aktivierung bewirkt, dass beim Booten der Maschine die Meldung 'Druecken Sie F11 zum Ausfuehren des Acronis Startup Recovery Manager…' angezeigt wird (sofern bei Ihnen kein GRUB Boot-Loader vorhanden ist) – oder fügt Menü dem Boot-Menü von GRUB das Element 'Startup Recovery Manager' hinzu (sofern bei Ihnen GRUB vorhanden ist).

Auf dem Systemlaufwerk (unter Linux: der '/boot'-Partition) sollten mindestens 100 MB freier Speicherplatz verfügbar sein, damit der Startup Recovery Manager aktiviert werden kann.

Bei der Aktivierung überschreibt der Startup Recovery Manager den Boot-Code des vorhandenen MBR (Master Boot Record), der vom Betriebssystem installiert wurde, komplett mit seinem eigenen Boot-Code. Wenn GRUB als Boot-Loader im MBR installiert ist, wird GRUB und dessen Boot-Menü entsprechend angepasst. Falls Sie andere Boot-Loader (von Drittherstellern) installiert haben, müssen Sie diese möglicherweise reaktivieren.

Wenn Sie unter Linux einen anderen Boot-Loader als GRUB verwenden (z.B. LILO), sollten Sie erwägen, diesen statt in den MBR in den Boot-Record einer Linux-root- oder Boot-Partition zu

installieren, bevor Sie den Startup Recovery Manager aktivieren. Rekonfigurieren Sie anderenfalls den Boot-Loader nach der Aktivierung manuell.

Den Startup Recovery Manager deaktivieren

Die Deaktivierung wird ähnlich durchgeführt wie die Aktivierung

Mit der Deaktivierung wird die Boot-Meldung 'Druecken Sie F11 zum Ausfuehren des Acronis Startup Recovery Manager...' (oder der entsprechende Menü-Eintrag von GRUB) wieder ausgeschaltet. Wenn kein Startup Recovery Manager aktiviert ist, müssen Sie eine der folgenden Möglichkeiten verwenden, um ein System wiederherzustellen, wenn eine Maschine ihre Bootfähigkeit verliert:

- Starten Sie die Maschine mithilfe eines eigenständigen Boot-Mediums
- Booten Sie die Maschine über das Netzwerk, indem Sie einen PXE Server oder die Microsoft Remote Installation Services (RIS) verwenden

15.14.5 Recovery einer Maschine

15.14.5.1 Physische Maschinen

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:

- macOS
- 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.

Die Wiederherstellung eines Betriebssystems erfordert immer einen Neustart (Reboot) des Systems. 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.

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.

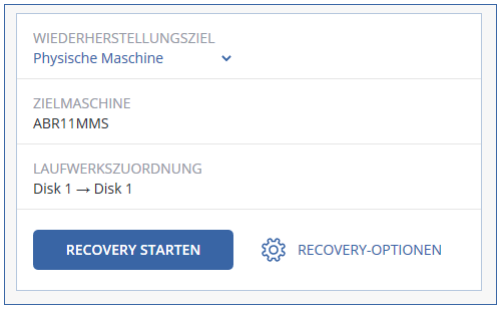
   Falls die Maschine offline ist, werden keine Recovery-Punkte angezeigt. Gehen Sie nach einer der folgenden Möglichkeiten vor:

   - 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' (S. 220).
   - Stellen Sie die Maschine so wieder her, wie es im Abschnitt 'Laufwerke mithilfe eines Boot-Mediums wiederherstellen (S. 201)' beschrieben ist.

4. Klicken Sie auf **Recovery** –> **Komplette Maschine**.

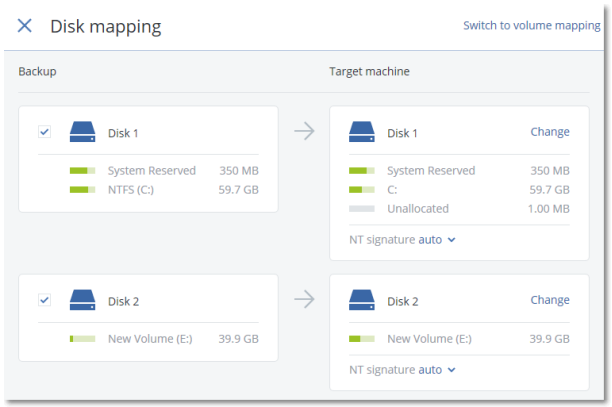
   Die Software weist die Laufwerke im Backup automatisch den Laufwerken der Zielmaschine zu.

   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. [Optional] Aktivieren Sie **Safe Recovery**, damit das Backup nach Malware gescannt wird. Wenn eine Malware gefunden wurde, wird diese im Backup gekennzeichnet und direkt gelöscht, wenn der Wiederherstellungsprozesses abgeschlossen ist.
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.

15.14.5.2 Physische Maschinen als virtuelle Maschinen wiederherstellen

Dieser Abschnitt erläutert, wie Sie eine physische Maschine über die Weboberfläche als virtuelle Maschine wiederherstellen können. Damit Sie diese Aktion ausführen können, muss mindestens ein Agent für VMware oder ein Agent für Hyper-V installiert und registriert sein.

Weiter Informationen zu P2V-Migrationen finden Sie im Abschnitt 'Migration von Maschinen (S. 317)'.

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:

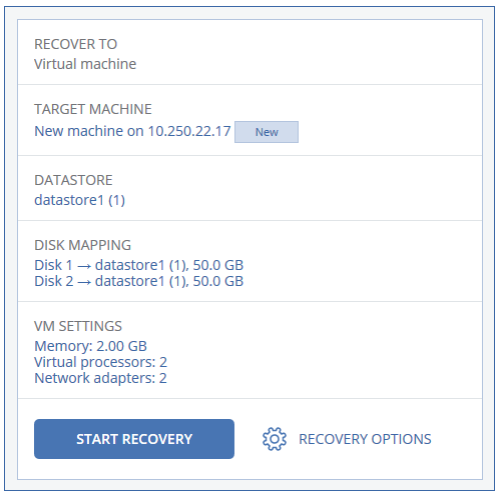
   - Sollte sich das Backup im Cloud Storage oder einem freigegebenen Storage befinden (d.h., dass andere Agenten auf diesen zugreifen können), dann klicken Sie zuerst auf den Befehl **Maschine auswählen**. Wählen Sie anschließend eine Maschine aus, die online ist, und dann den gewünschten Recovery-Punkt.
   - Wählen Sie einen Recovery-Punkt auf der Registerkarte 'Backup Storage' (S. 220).
   - Stellen Sie die Maschine so wieder her, wie es im Abschnitt 'Laufwerke mithilfe eines Boot-Mediums wiederherstellen (S. 201)' beschrieben ist.
4. Klicken Sie auf **Recovery** –> **Komplette Maschine**.
5. Wählen Sie unter **Wiederherstellungsziel** die Option **Virtuelle Maschine**.
6. Klicken Sie auf **Zielmaschine**.
   a. Bestimmen Sie den Hypervisor (**VMware ESXi** oder **Hyper-V**).

      Für die Aktion muss mindestens ein Agent für VMware oder ein Agent für Hyper-V installiert 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. [Optional] Wenn Sie eine neue Maschine als Recovery-Ziel verwenden, können Sie außerdem noch Folgendes tun:
   - 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.
   - Klicken Sie auf **VM-Einstellungen**, um die Größe des Arbeitsspeichers, die Anzahl der Prozessoren und die Netzwerkverbindungen für die virtuelle Maschine zu ändern.



8. [Optional] Aktivieren Sie **Safe Recovery**, damit das Backup nach Malware gescannt wird. Wenn eine Malware gefunden wurde, wird diese im Backup gekennzeichnet und direkt gelöscht, wenn der Wiederherstellungsprozesses abgeschlossen ist.
9. Klicken Sie auf **Recovery starten**.
10. 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.

15.14.5.3 Virtuelle Maschine

Eine virtuelle Maschine, die als Recovery-Ziel dient, muss während der Wiederherstellung gestoppt werden. Die Software stoppt die entsprechende Maschine ohne weitere Benutzeraufforderung. Wenn die Wiederherstellung abgeschlossen wurde, müssen Sie die Maschine manuell wieder starten.

Dieses Verhalten kann durch die Verwendung der Recovery-Option für die VM-Energieverwaltung geändert werden (klicken Sie dazu auf **Recovery-Optionen** –> **VM-Energieverwaltung**).

So können Sie eine virtuelle Maschine wiederherstellen

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' (S. 220).
2. Klicken Sie auf **Recovery** –> **Komplette Maschine**.
3. Wenn Sie die Wiederherstellung zu einer physischen Maschine durchführen wollen, wählen Sie bei **Wiederherstellungsziel** 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 (S. 197)' fort. Falls dies nicht zutrifft, empfehlen wir Ihnen, eine V2P-Migration mithilfe eines Boot-Mediums (S. 201) durchzuführen.
4. Die Software wählt 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** oder **Virtuozzo Infrastructure Platform**).

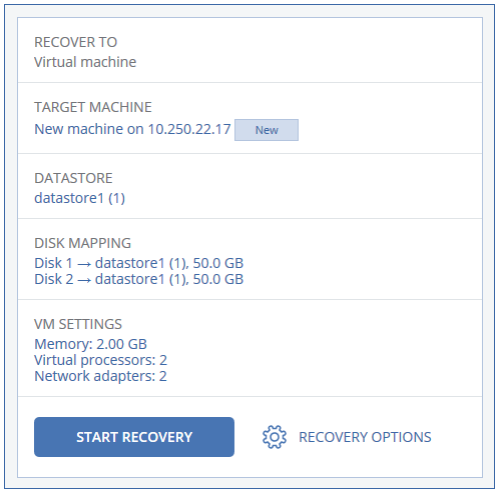
      Nur virtuelle Virtuozzo-Maschinen können zu Virtuozzo wiederhergestellt werden. Weiter Informationen zu V2V-Migrationen finden Sie im Abschnitt 'Migration von Maschinen (S. 317)'.
   b. Bestimmen Sie, ob eine neue oder eine vorhandene Maschine als Recovery-Ziel verwendet werden soll.
   c. Wählen Sie 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. Wenn Sie eine neue Maschine als Recovery-Ziel verwenden, können Sie außerdem noch Folgendes tun:

- [Optional, nicht verfügbar für die Virtuozzo Infrastructure Platform] Klicken Sie auf **Datenspeicher** für ESXi oder **Pfad** für Hyper-V und Virtuozzo – und bestimmten Sie dann den Datenspeicher (Storage) für die neue virtuelle Maschine.
- [Optional] Klicken Sie auf **Laufwerkszuordnung**, um den Datenspeicher (Storage), die Oberfläche 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 die Virtuozzo Infrastructure Platform wieder her.

  Für die Virtuozzo Infrastructure Platform 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] Klicken Sie auf **VM-Einstellungen**, um die Größe des Arbeitsspeichers, die Anzahl der Prozessoren (für die Virtuozzo Infrastructure Platform: wählen Sie die **Variante**) und/oder die Netzwerkeinstellungen für die virtuelle Maschine zu ändern.

  Hinweis: *Für die Virtuozzo Infrastructure Platform ist die Auswahl des Variante (Englisch: Flavor) ein erforderlicher Schritt.*



6. [Optional] Aktivieren Sie **Safe Recovery**, damit das Backup nach Malware gescannt wird. Wenn eine Malware gefunden wurde, wird diese im Backup gekennzeichnet und direkt gelöscht, wenn der Wiederherstellungsprozesses abgeschlossen ist.
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.

15.14.5.4 Laufwerke mithilfe eines Boot-Mediums wiederherstellen

Genau Informationen über die Erstellung eines Boot-Mediums finden Sie im Abschnitt 'Ein Boot-Medium erstellen (S. 195)'.

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. Stellen Sie die ursprüngliche Laufwerkskonfiguration wieder her. Anweisungen dazu finden Sie unter https://support.apple.com/guide/disk-utility/welcome.
   c. 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 **Extras** –> **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, das 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.

   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.

    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.

15.14.5.5 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' (S. 203).
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 den 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.

15.14.6 Dateien wiederherstellen

15.14.6.1 Dateien über die Weboberfläche wiederherstellen

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' (S. 220).
   - Laden Sie die Dateien aus dem Cloud Storage herunter (S. 207).
   - Verwenden Sie ein Boot-Medium (S. 209).
4. Klicken Sie auf **Wiederherstellen** –> **Dateien/Ordner**.
5. Wechseln Sie zum benötigten Ordner oder verwenden Sie die Suchfunktion, um eine Liste der erforderlichen Dateien und Ordner abzurufen.

   Sie können ein oder mehrere Platzhalterzeichen (* und ?) verwenden. Ausführlichere Informationen über die Verwendung von Platzhalterzeichen finden Sie im Abschnitt 'Dateifilter (S. 168)'.

   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. Wenn Sie dies nicht wollen, 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.
8. Klicken Sie auf **Recovery**.

   Wählen Sie bei **Recovery zu** eine der folgenden Möglichkeiten:

   - Die ursprüngliche Maschine, auf der sich die Dateien im Backup befunden haben, die Sie wiederherstellen wollen (sofern auf der Maschine ein Agent installiert ist).
   - Die Maschine, auf welcher ein Agent für VMware, ein Agent für Hyper-V oder ein Agent für Virtuozzo installiert ist (sofern die Dateien von einer virtuellen ESXi-, Hyper-V- oder Virtuozzo-Maschine stammen).

   Dies ist die Zielmaschine für die Wiederherstellung. Sie können bei Bedarf auch eine andere Maschine auswählen.
9. Wählen Sie bei **Pfad** das gewünschte Ziel für die Wiederherstellung. Sie können eine der folgenden Optionen wählen:

   - Der ursprüngliche Speicherort (bei Wiederherstellung zur ursprünglichen Maschine)
   - Ein lokaler Ordner auf der Zielmaschine

***Hinweis**: Symbolische Links werden nicht unterstützt.*

- Ein Netzwerkordner, auf von der Zielmaschine aus verfügbar ist.

1. Klicken Sie auf **Recovery starten**.
2. 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.

15.14.6.2 Dateien aus dem Cloud Storage herunterladen

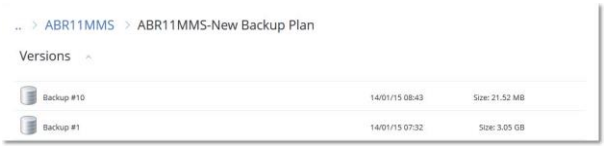
Sie können den Cloud Storage durchsuchen, die Inhalte von Backups einsehen und benötigte Dateien herunterladen.

Einschränkungen

- Die Backups von SQL-Datenbanken, Exchange-Datenbanken und eines Systemzustands können nicht durchsucht werden.
- Für ein optimales Download-Erlebnis sollten Sie nicht mehr als 100 MB gleichzeitig herunterladen. Um größere Datenmengen schnell aus der Cloud abzurufen, verwenden Sie die Prozedur zur Wiederherstellung von Dateien (S. 206).

So laden Sie Dateien aus dem Cloud Storage herunter

1. Wählen Sie eine Maschine, die per Backup gesichert wurde.
2. Klicken Sie auf **Recovery** –> **Weitere Wiederherstellungsmöglichkeiten...** –> **Dateien herunterladen**.
3. Geben Sie die Anmeldedaten des Kontos ein, dem die gesicherte Maschine zugewiesen wird.
4. [Beim Durchsuchen von Laufwerk-Backups] Klicken Sie unter **Versionen** auf dasjenige Backup, dessen Dateien Sie wiederherstellen wollen.

   [Beim Durchsuchen von Datei-Backups] Sie können den Backup-Zeitpunkt im nächsten Schritt auswählen (unter dem Zahnradsymbol, das rechts neben der ausgewählten Datei liegt). Standardmäßig werden die Dateien des letzten (jüngsten) Backups wiederhergestellt.
5. Wechseln Sie zum benötigten Ordner oder verwenden Sie die Suchfunktion, um eine Liste der erforderlichen Dateien abzurufen.

6. Aktivieren Sie die Kontrollkästchen derjenigen Elemente, die Sie wiederherstellen müssen – und klicken Sie dann auf **Download**.

Falls Sie eine einzelne Datei auswählen, wird diese 'wie vorliegend' heruntergeladen. Anderenfalls werden die ausgewählten Daten in eine .zip-Datei archiviert.

7. Wählen Sie den Ort, wo die Daten abgelegt werden sollen und klicken Sie auf **Speichern**.

15.14.6.3 Die Authentizität von Dateien mit dem Notary Service überprüfen

Falls die Beglaubigungsfunktion (Notarization) während eines Backups (S. 154) 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 (S. 206)' oder in den Schritten 1-5 des Abschnitts 'Dateien aus dem Cloud Storage herunterladen (S. 207)' 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.

15.14.6.4 Eine Datei mit ASign signieren

***Hinweis**: Diese Funktionalität ist in den Standard-Editionen des Cyber Protection Service nicht 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 (S. 206)' oder in den Schritten 1-5 des Abschnitts 'Dateien aus dem Cloud Storage herunterladen (S. 207)' 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.

15.14.6.5 Dateien mit einem Boot-Medium wiederherstellen

Genau Informationen über die Erstellung eines Boot-Mediums finden Sie im Abschnitt 'Ein Boot-Medium erstellen (S. 195)'.

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 **Extras** –> **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, das 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.

   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.

15.14.6.6 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.
- Auf der Maschine, von der aus Sie ein Backup durchsuchen wollen, muss ein Protection Agent installiert sein.
- Folgende, im Backup gesicherte Dateisysteme werden dabei unterstützt: FAT16, FAT32, NTFS, ReFS, Ext2, Ext3, Ext4, XFS oder HFS+.
- 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.

15.14.7 Einen Systemzustand wiederherstellen

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 Speicherort 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.

15.14.8 Eine ESXi-Konfiguration wiederherstellen

Um eine ESXi-Konfiguration wiederherstellen zu können, benötigen Sie ein Linux-basiertes Boot-Medium. Genau Informationen über die Erstellung eines bootfähigen Mediums finden Sie im Abschnitt 'Ein Boot-Medium erstellen (S. 195)'.

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.

15.14.9 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 (S. 213)	+	+	+	+	+	+	+	+	+
Boot-Modus (S. 214)	+	-	-	-	-	-	-	+	-
Zeitstempel für Dateien (S. 215)	-	-	-	+	+	+	+	-	-
Fehlerbehandlung (S. 215)	+	+	+	+	+	+	+	+	+

	Laufwerke			Dateien				Virtuelle Maschinen	SQL und Exchange
	Windows	Linux	Boot-Medium	Windows	Linux	macOS	Boot-Medium	ESXi, Hyper-V und Virtuozzo	Windows
Dateifilter (Ausschluss) (S. 216)	-	-	-	+	+	+	+	-	-
Dateisicherheitseinstellungen (S. 216)	-	-	-	+	-	-	-	-	-
Flashback (S. 216)	+	+	+	-	-	-	-	+	-
Wiederherstellung mit vollständigem Pfad (S. 217)	-	-	-	+	+	+	+	-	-
Mount-Punkte (S. 217)	-	-	-	+	-	-	-	-	-
Performance (S. 217)	+	+	-	+	+	+	-	+	+
Vor-/Nach-Befehle (S. 217)	+	+	-	+	+	+	-	+	+
SID ändern (S. 219)	+	-	-	-	-	-	-	-	-
VM-Energieverwaltung (S. 219)	-	-	-	-	-	-	-	+	-
Windows-Ereignisprotokoll (S. 220)	+	-	-	+	-	-	-	Nur Hyper-V	+

15.14.9.1 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.

Die Voreinstellung ist: **Deaktiviert**.

Die Validierung berechnet eine Prüfsumme für jeden Datenblock, der im Backup gespeichert ist. 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 ist ein zeitaufwendiger Prozess (auch bei inkrementellen oder differentiellen Backups, die normalerweise kleiner sind). Hintergrund ist, dass die Aktion nicht einfach nur die tatsächlich in dem betreffenden Backup enthaltenen Daten validiert, sondern alle Daten, die ausgehend von diesem Backup wiederherstellbar sind. Dies erfordert unter Umständen auch einen Zugriff auf zuvor erstellte (abhängige) Backups.

***Hinweis**: Eine Validierung ist bei einem Cloud Storage möglich, der sich entweder in einem Acronis Datacenter befindet oder von einem Acronis Partner bereitgestellt wird.*

15.14.9.2 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 Vista SP1
  - 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.

15.14.9.3 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**.

15.14.9.4 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. Abstand 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.

15.14.9.5 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.*

15.14.9.6 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.

15.14.9.7 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**.

Wenn Sie eine virtuelle Maschine wiederherstellen, ist die Voreinstellung: **Aktiviert**.

15.14.9.8 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**.

15.14.9.9 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 (S. 179)' 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.*

15.14.9.10 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.

15.14.9.11 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.*

15.14.9.12SID ändern

Diese Option ist gültig, wenn Sie Windows 8.1/Windows Server 2012 R2 (oder früher) wiederherstellen.

Diese Option gilt nicht, wenn eine Wiederherstellung zu einer virtuellen Maschine (als Ziel) mit einem Agenten für VMware oder einem Agenten für Hyper-V durchgeführt 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 Dritthersteller-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.

15.14.9.13VM-Energieverwaltung

Diese Optionen gelten nur, wenn eine Wiederherstellung zu einer virtuellen Maschine (als Ziel) durchgeführt wird und dafür ein Agent für VMware, ein Agent für Hyper-V oder ein Agent für Virtuozzo 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.

15.14.9.14 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**.

15.15 Aktionen mit Backups

15.15.1 Die Registerkarte 'Backup Storage'

Die Registerkarte **Backup Storage** ermöglicht den Zugriff auf alle Backups – inklusive der Backups von Offline-Maschinen und solchen Maschinen, die nicht mehr für den Cyber Protection Service registriert sind.

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.

Im Cloud Storage haben Benutzer jedoch immer nur Zugriff auf Ihre jeweils eigenen Backups. Ein Administrator kann die Backups eines jeden Kontos einsehen, welches zu einer gegebenen Abteilung oder einer Firma und deren Untergruppen gehört. Dieses Konto wird indirekt über den Befehl **Von dieser Maschine aus durchsuchen** ausgewählt. Die Registerkarte **Backup Storage** zeigt die Backups all derjenigen Maschinen an, die jemals für dasselbe Konto registriert wurden, da diese Maschine registriert ist.

Backups, die vom *Cloud* Agenten für Office 365 erstellt wurden, sowie Backups von G Suite-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**.

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 (S. 171) 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 (S. 391).

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.

15.15.2 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. Volumes werden im 'Nur Lesen'-Modus gemountet.

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.

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.

   ***Tipp**: 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 klicken Sie dann auf **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**.
   Das Mounten des ausgewählten Volumes wird von der Software aufgehoben und das entsprechende Laufwerk vom Dateisystem getrennt.

15.15.3 Backups löschen

***Warnung**: Wenn ein Backup gelöscht wird, werden damit auch all seine Daten dauerhaft gelöscht. Gelöschte Daten können nicht wiederhergestellt werden.*

So können Sie die Backups einer Maschine löschen, die online und in der Service-Konsole aufgeführt sind

1. Wählen Sie auf der Registerkarte **Alle Geräte** eine Maschine aus, deren Backups Sie löschen wollen.
2. Klicken Sie auf **Recovery**.
3. Wählen Sie den Speicherort aus, an dem sich die zu löschen Backups befinden.
4. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Zum Löschen eines einzelnen Backups müssen Sie das entsprechende Backup auswählen und dann auf das X-Symbol klicken.
   - Um alle Backups am ausgewählten Speicherort zu löschen, klicken Sie auf **Alle löschen**.
5. Bestätigen Sie Ihre Entscheidung.

So können Sie die Backups einer bestimmten Maschine löschen

1. Wählen Sie auf der Registerkarte **Backup Storage** den Speicherort aus, an dem Sie die Backups löschen wollen.

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 aus.
3. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Wenn Sie ein einzelnes Backup löschen wollen, klicken Sie auf **Backups anzeigen**, wählen Sie anschließend das zu löschende Backup aus und klicken Sie dann auf das X-Symbol.
   - Um die ausgewählte Gruppe zu löschen: klicken Sie auf **Löschen**.
4. Bestätigen Sie Ihre Entscheidung.

So können Sie Backups direkt aus dem Cloud Storage löschen

1. Melden Sie sich, wie im Abschnitt 'Dateien aus dem Cloud Storage herunterladen (S. 207)' beschrieben, am Cloud Storage an.
2. Klicken Sie auf den Namen der Maschine, deren Backups Sie löschen wollen.

   Die Software zeigt eine oder mehrere Backup-Gruppen an.
3. Klicken Sie auf das Zahnradsymbol, das zu der Backup-Gruppe gehört, die Sie löschen möchten.
4. Klicken Sie auf **Entfernen**.
5. Bestätigen Sie die Aktion.

Vorgehensweise, wenn Sie lokale Backups mit einem Datei-Manager gelöscht haben

Wir empfehlen, dass Sie Backups nach Möglichkeit nur über die Service-Konsole löschen. Wenn Sie lokale Backups dennoch mit einem Datei-Manager (wie dem Windows Explorer) gelöscht haben, gehen Sie folgendermaßen vor:

1. Klicken Sie auf der Registerkarte **Backup Storage** auf das Zahnradsymbol neben dem Speicherortsnamen.
2. Klicken Sie auf **Aktualisieren**.

Auf diese Weise teilen Sie dem Cyber Protection Service mit, dass die lokale Storage-Nutzung geringer geworden ist.

15.16 Microsoft-Applikationen sichern

Microsoft SQL Server und Microsoft Exchange Server sichern

Es gibt zwei Methoden, wie Sie diese Applikationen per Backup 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 Office 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 (S. 235) Datenbanken als Dateien (S. 235)	Komplette Maschine (S. 197) Datenbanken zu einer aktiven SQL Server-Instanz (S. 235) Datenbanken als Dateien (S. 235)	Komplette Maschine (S. 197)
Microsoft Exchange Server	Datenbanken zu einem aktiven Exchange Server (S. 238) Datenbanken als Dateien (S. 238) Granulares Recovery zu einem aktiven Exchange Server oder zu Office 365* (S. 241)	Komplette Maschine (S. 197) Datenbanken zu einem aktiven Exchange Server (S. 238) Datenbanken als Dateien (S. 238) Granulares Recovery zu einem aktiven Exchange Server oder zu Office 365* (S. 241)	Komplette Maschine (S. 197)

Microsoft SharePoint-Datenbank-Server	Datenbanken zu einer aktiven SQL Server-Instanz (S. 235) Datenbanken als Dateien (S. 235) Granulares Recovery mithilfe des SharePoint Explorers	Komplette Maschine (S. 197) Datenbanken zu einer aktiven SQL Server-Instanz (S. 235) Datenbanken als Dateien (S. 235) Granulares Recovery mithilfe des SharePoint Explorers	Komplette Maschine (S. 197)
Microsoft SharePoint-Front-End-Webserver	-	-	Komplette Maschine (S. 197)
Active Directory-Domänendienste	-	Komplette Maschine (S. 197)	-

* Granulares Recovery ist auch für Postfach-Backups möglich. Die Wiederherstellung von Exchange-Datenelementen zu Office 365 (und umgekehrt) wird nur unter der Bedingung unterstützt, dass der Agent für Office 365 lokal installiert ist.

15.16.1 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.

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) (S. 190)' aktiviert.
- Für virtuelle Maschinen ist die Backup-Option 'VSS (Volume Shadow Copy Service) für virtuelle Maschinen (S. 191)' 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 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 eines integrierten Domain-Administrators (DOMAIN\Administrator) bereitstellen, wenn Sie das Applikations-Backup aktivieren.

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 eines integrierten Domain-Administrators (DOMAIN\Administrator) bereitstellen, wenn Sie das Applikations-Backup aktivieren.
- 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**).

15.16.2 Datenbank-Backup

Bevor Sie ein Datenbank-Backup durchführen, sollten Sie sicherstellen, dass die unter 'Voraussetzungen (S. 225)' aufgeführten Anforderungen erfüllt sind.

Wählen Sie die Datenbanken wie nachfolgend beschrieben aus – und spezifizieren Sie die anderen Einstellungen des Schutzplans je nach Bedarf (S. 122).

15.16.2.1 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 (S. 179) 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 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. Das Konto muss 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.

15.16.2.2 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 im Abschnitt 'Postfach-Backup (S. 233)' 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 das Backup von Datenbankverfügbarkeitsgruppen finden Sie im Abschnitt 'Datenbankverfügbarkeitsgruppen (DAG) sichern'.
   - 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 im Abschnitt 'Postfach-Backup (S. 233)' beschrieben ist, können Sie auch Postfächer zur Sicherung auswählen.
4. Geben Sie bei Aufforderung die Anmeldedaten an, die für den Datenzugriff notwendig sind.
5. Klicken Sie auf den Befehl **Schützen**.

15.16.2.3 AlwaysOn-Verfügbarkeitsgruppen (AAG) sichern

***Hinweis**: Diese Funktionalität ist in den Standard Editionen des Cyber Protection Service nicht 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.

   Tipp: *Nachdem Sie den Agenten auf einem der Knoten installiert haben, zeigt die Software die AAG und deren Knoten unter* ***Geräte*** *–>* ***Microsoft SQL*** *–>* ***Datenbanken*** *an. Um die Agenten für SQL auf den restlichen Knoten zu installieren, müssen Sie die AAG auswählen, dann auf* ***Details*** *klicken und abschließend neben jedem Knoten auf* ***Agent installieren****.*

2. Wählen Sie die zu sichernde AAG aus wie im Abschnitt 'SQL-Datenbanken auswählen' beschrieben.

   Wichtig: *Sie müssen die AAG selbst auswählen und nicht die einzelnen Knoten oder Datenbanken in ihr. Wenn Sie einzelne Elemente innerhalb der AAG auswählen, wird das Backup nicht Cluster-konform sein und es werden nur die ausgewählten Kopien der Elemente gesichert.*

3. Konfigurieren Sie die Backup-Option 'Cluster-Backup-Modus (S. 165)'.

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' (S. 220) 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 (S. 235)' 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.*

15.16.2.4 Datenbankverfügbarkeitsgruppen (DAG) sichern

Hinweis*: Diese Funktionalität ist in den Standard Editionen des Cyber Protection Service nicht 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.

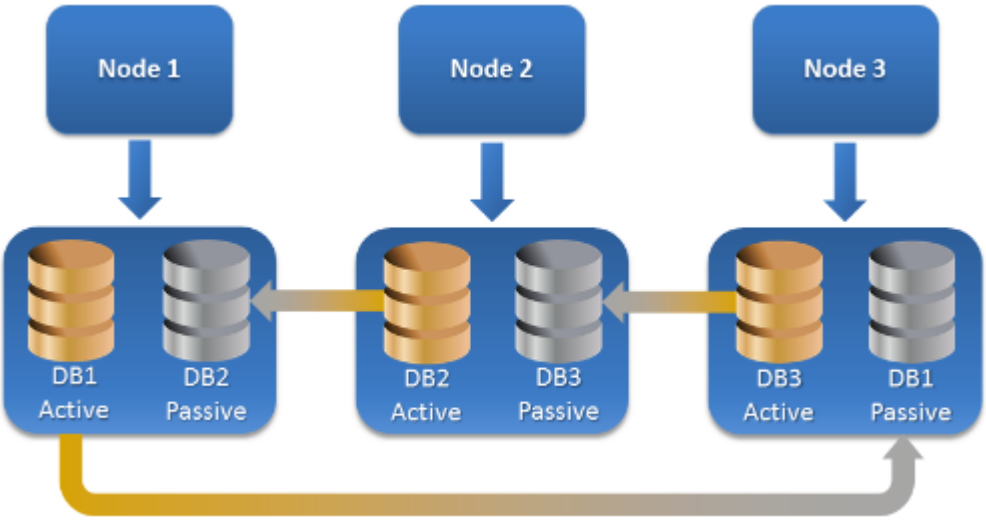
Cluster-konformes Backup

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.

Tipp: *Nachdem Sie den Agenten auf einem der Knoten installiert haben, zeigt die Service-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. 227)' beschrieben ist.
2. Konfigurieren Sie die Backup-Option 'Cluster-Backup-Modus (S. 165)'.
3. Spezifizieren Sie bei Bedarf (S. 122) 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' (S. 220) auszuwählen.
2. Befolgen Sie die im Abschnitt 'Exchange-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.

15.16.3 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:

1. Die Applikationen werden in einem konsistenten Zustand gesichert und sind daher nach der Wiederherstellung der Maschine auch direkt verfügbar.
2. Sie können SQL- und Exchange-Datenbanken, Exchange-Postfächer und Exchange-Postfachelemente wiederherstellen, ohne die komplette Maschine wiederherstellen zu müssen.
3. Die SQL-Transaktionsprotokolle werden nach jedem erfolgreichen Backup abgeschnitten. Die SQL-Protokollabschneidung kann in den Schutzplan-Optionen (S. 179) deaktiviert werden. Die Exchange-Transaktionsprotokolle werden nur auf virtuellen Maschinen abgeschnitten. Sie können die Option 'VSS-Voll-Backup' (S. 190) aktivieren, falls Sie wollen, dass die Exchange-Transaktionsprotokolle auf einer physischen Maschine abgeschnitten werden.
4. 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.

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 (S. 225)' und 'Erforderliche Benutzerrechte (S. 233)'.

15.16.3.1 Erforderliche Benutzerrechte

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 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.
- 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 eines integrierten Domain-Administrators (DOMAIN\Administrator) bereitstellen, wenn Sie das Applikations-Backup aktivieren.

15.16.4 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.

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 (S. 234)' aufgeführt.
10. Klicken Sie auf **Hinzufügen**.

Als Ergebnis erscheinen die Postfächer anschließend unter **Geräte** –> **Microsoft Exchange** –> **Postfächer**.

15.16.4.1 Exchange Server-Postfächer auswählen

Wählen Sie die Postfächer wie nachfolgend beschrieben aus – und spezifizieren Sie dann die anderen Einstellungen des Schutzplans nach Bedarf (S. 122).

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**.

15.16.4.2 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.

15.16.5 SQL-Datenbanken wiederherstellen

Dieser Abschnitt beschreibt die Wiederherstellung von Datenbank-Backups und applikationskonformen Backups.

Sie können SQL-Datenbanken zu einer SQL Server-Instanz wiederherstellen, sofern der Agent für SQL auf derjenigen Maschine installiert ist, auf welcher die Instanz läuft. Sie müssen außerdem 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.

Sie können die Datenbanken alternativ auch als Dateien wiederherstellen. Das kann nützlich sein, falls Sie Daten zur Überwachung oder weiteren Verarbeitung durch Dritthersteller-Tools extrahieren müssen. Wie Sie SQL-Datenbankdateien an eine SQL Server-Instanz anfügen, ist im Abschnitt 'SQL Server-Datenbanken anfügen (S. 238)' erläutert.

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.

Systemdatenbanken werden grundsätzlich auf die gleiche Weise wie Benutzerdatenbanken wiederhergestellt. Die Besonderheiten bei der Wiederherstellung einer Systemdatenbank sind im Abschnitt 'Systemdatenbanken wiederherstellen (S. 237)' beschrieben.

So können Sie SQL-Datenbanken zu einer SQL Server-Instanz 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 SQL** – 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 SQL installiert ist, und dann den gewünschten Recovery-Punkt.
   - Wählen Sie einen Recovery-Punkt auf der Registerkarte 'Backup Storage' (S. 220).

   Die in einer der oberen Aktionen zum Durchsuchen ausgewählte Maschine wird als Zielmaschine für die Wiederherstellung der SQL-Datenbanken verwendet.

4. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Wenn Sie eine Wiederherstellung aus einem applikationskonformen Backup durchführen, klicken Sie auf **Recovery** –> **SQL-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 einer Instanz**.
5. Die Datenbanken werden standardmäßig zu den ursprünglichen Datenbanken wiederhergestellt. Falls die ursprüngliche Datenbank nicht existiert, wird sie automatisch neu erstellt. Sie können auch eine andere SQL Server-Instanz (die auf derselben Maschine läuft) auswählen, auf welcher die Datenbanken wiederhergestellt werden sollen.

   So können Sie eine Datenbank als eine andere Datenbank auf derselben Instanz 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. [Optional] [Nicht verfügbar für eine Datenbank, die als neue Datenbank zu ihrer ursprünglichen Instanz wiederhergestellt wurde] Um das Datenbankstadium nach der Wiederherstellung zu ändern, müssen Sie auf den Datenbanknamen klicken und dann einen der folgenden Stadien auswählen:
   - **Verwendungsbereit (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.
7. Klicken Sie auf **Recovery starten**.

Der Recovery-Fortschritt wird auf der Registerkarte 'Aktivitäten' angezeigt.

So können Sie SQL-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 SQL** – 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 SQL oder der Agent für VMware installiert ist, und dann den gewünschten Recovery-Punkt.
   - Wählen Sie einen Recovery-Punkt auf der Registerkarte 'Backup Storage' (S. 220).

   Die in einer der oberen Aktionen zum Durchsuchen ausgewählte Maschine wird als Zielmaschine für die Wiederherstellung der SQL-Datenbanken verwendet.
4. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Wenn Sie eine Wiederherstellung aus einem applikationskonformen Backup durchführen, klicken Sie auf **Recovery** –> **SQL-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.

15.16.5.1 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 'Verwendungsbereit' (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.

15.16.5.2 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**.

15.16.6 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 (S. 241).

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' (S. 220).

   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' (S. 220).

   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.

15.16.6.1 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 das Protokolldatei-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

15.16.7 Exchange-Postfächer und Postfachelemente wiederherstellen

Dieser Abschnitt beschreibt die Wiederherstellung von Exchange-Postfächern und Postfachelementen aus Datenbank-Backups, applikationskonformen Backups und Postfach-Backups. Die Postfächer oder auch einzelne Postfachelemente können zu einem aktiv laufenden Exchange Server oder zu Microsoft Office 365 wiederhergestellt werden.

Folgende Elemente können wiederhergestellt werden:

- Postfächer (ausgenommen archivierte Postfächer)
- Öffentliche Ordner
- Öffentlicher Ordner-Elemente
- E-Mail-Ordner
- E-Mail-Nachrichten
- Kalenderereignisse
- Aufgaben
- Kontakte
- Journal-Einträge
- Hinweise

Sie können eine Suchfunktion verwenden, um bestimmte Elemente zu finden.

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 für 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 Office 365

Die Wiederherstellung von Exchange-Datenelementen zu Office 365 (und umgekehrt) wird nur unter der Bedingung unterstützt, dass der Agent für Office 365 lokal installiert ist.

Wiederherstellungen können aus Backups von Microsoft Exchange Server 2010 (oder höher) durchgeführt werden.

Wenn ein Postfach zu einem vorhandenen Office 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 Office 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 die Wiederherstellung von Office 365 finden Sie im Abschnitt 'Office 365-Postfächer sichern (S. 251)'.

15.16.7.1 Postfächer wiederherstellen

So können Sie Postfächer aus einem applikationskonformen Backup oder einem Datenbank-Backup wiederherstellen

1. [Nur bei Wiederherstellung eines Datenbank-Backups zu Office 365] Wenn der Agent für Office 365 auf der Maschine, die den Exchange Server ausführt und per Backup gesichert wurde, nicht installiert ist, gehen Sie folgendermaßen vor:

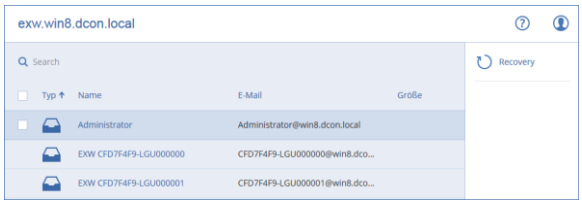
- Falls Sie keinen Agenten für Office 365 in Ihrem Unternehmen haben, dann installieren Sie den Agenten für Office 365 auf der Maschine, die per Backup gesichert wurde (oder auf einer anderen Maschine mit derselben Microsoft Exchange Server-Version).
- Falls Sie einen Agenten für Office 365 in Ihrem 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 Office 365. Eine entsprechende Beschreibung dazu finden Sie im Abschnitt 'Microsoft Exchange-Bibliotheken kopieren (S. 247)'.

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' (S. 220).

   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 Office 365]:
   a. Wählen Sie bei **Recovery zu** den Eintrag **Microsoft Office 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.

9. 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.

   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 (S. 234)' 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' (S. 220) 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.

15.16.7.2 Postfachelemente wiederherstellen

So können Sie Postfachelemente aus einem applikationskonformen Backup oder einem Datenbank-Backup wiederherstellen

1. [Nur bei Wiederherstellung eines Datenbank-Backups zu Office 365] Wenn der Agent für Office 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 Office 365 in Ihrem Unternehmen haben, dann installieren Sie den Agenten für Office 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 Office 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 Office 365. Eine entsprechende Beschreibung dazu finden Sie im Abschnitt 'Microsoft Exchange-Bibliotheken kopieren (S. 247)'.
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' (S. 220).

   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.

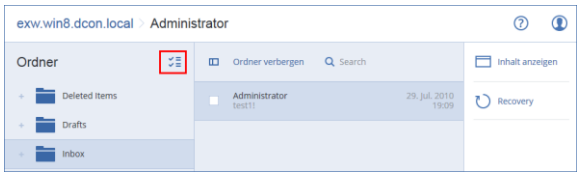
   Folgende Suchoptionen sind verfügbar. Platzhalterzeichen (Wildcards) werden nicht unterstützt.

   - 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.

   Tipp: *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 Office 365 wiederherstellen wollen, wählen Sie bei **Recovery zu** den Eintrag **Microsoft Office 365**.

   Wenn Sie zu einem Exchange Server wiederherstellen wollen, übernehmen Sie bei **Recovery zu** den Standardwert **Microsoft Exchange**.
10. [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.

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 (S. 234)' 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 Kalenderereignisse, 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' (S. 220) 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.

   Tipp: *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.

15.16.7.3 Microsoft Exchange-Bibliotheken kopieren

Wenn Sie Exchange-Postfächer oder Postfach-Elemente zu Office 365 wiederherstellen wollen (S. 241), 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 Agenten für Office 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.

15.16.8 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**.

15.17 Mobilgeräte sichern

Mit der Backup-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 Backup-App auf einem Mobilgerät installieren, das mit einem der folgenden Betriebssysteme läuft:

- iOS 10.3 und höher (iPhone, iPod und iPads)
- Android 5.0 und höher

Was Sie per Backup sichern können

- Kontakte
- Fotos
- 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:
  - Bei Android 7.0 oder höher erkennt die Backup-App neue Daten automatisch „on-the-fly“ und lädt diese dann in die Cloud hoch,
  - Bei Android 5 und 6 werden die Änderungen von der App alle drei Stunden überprüft. Sie können das kontinuierliche Backup in den Einstellungen der App ausschalten.
- Die Option **Nur WLAN verwenden** ist in den Einstellungen der App standardmäßig aktiviert. Wenn diese Einstellung aktiviert ist, wird die Backup-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.
- Sie haben zwei Möglichkeiten, Energie zu sparen:
  - Mit der Funktionalität **Backup beim Aufladen** – die standardmäßig deaktiviert ist. Wenn diese Einstellung aktiviert ist, wird die Backup-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 Backup-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. Diese Option ist für Android 8 oder höher verfügbar.

- 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 Service-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 Backup-App können Sie immer nur jeweils die letzten (neuesten) Datenversionen wiederherstellen. Wenn Sie Daten aus einer spezifischen Backup-Version wiederherstellen wollen, müssen Sie die Service-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 Backup-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:
   1. Ein Verschlüsselungskennwort zweimal eingeben.

      Stellen Sie sicher, dass Sie sich das Kennwort merken, weil ein vergessenes Kennwort weder wiederhergestellt noch geändert werden kann.

   2. 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

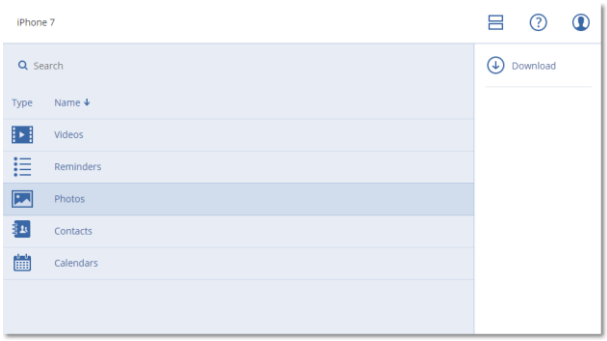
1. Öffnen Sie die Backup-App.
2. Tippen Sie auf den Befehl **Durchsuchen**.
3. Tippen Sie auf den Gerätenamen.
4. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:

- 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.

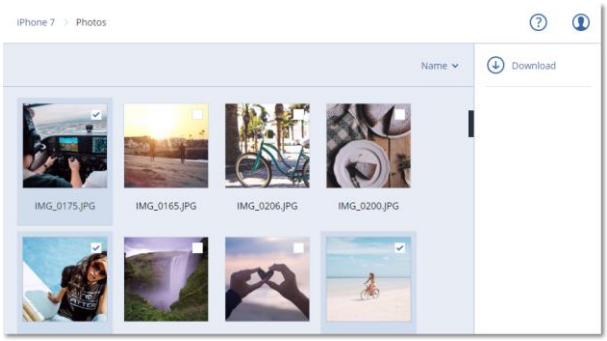
5. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Wenn Sie ein einzelnes Datenelement wiederherstellen wollen, müssen Sie dieses antippen.
   - Wenn Sie mehrere Datenelemente wiederherstellen wollen, müssen Sie auf **Auswahl** tippen und dann die Kontrollkästchen der gewünschten Elemente aktivieren.
6. Tippen Sie auf den Befehl **Recovery**.

So können Sie Daten über die Service-Konsole überprüfen

1. Öffnen Sie auf einem Computer einen Webbrowser und geben Sie die URL der Service-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.

15.18 Office 365-Daten sichern

Warum sollten Sie Office 365-Daten per Backup sichern?

Microsoft Office 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 Office 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.

Agent für Office 365

Abhängig von der gewünschten Funktionalität können Sie den Agenten für Office 365 lokal installieren, den in der Cloud installieren Agenten verwenden – oder beides. Die nachfolgende Tabelle fasst die Funktionalität des lokalen und Cloud-basierten Agenten zusammen.

	Lokaler Agent für Office 365	**Cloud Agent für Office 365**
Datenelemente, die per Backup gesichert werden können	**Exchange Online:** Benutzer und freigegebene Postfächer	▪ **Exchange Online**: Benutzerpostfächer, freigegebene Postfächer und Gruppenpostfächer; öffentliche Ordner ▪ **OneDrive**: Benutzer-Dateien und -Ordner ▪ **SharePoint Online**: klassische Website-Sammlungen, Gruppen-(Team)-Websites, Kommunikations-Websites, einzelne Datenelemente
Backup von Archivpostfächern (**In-Situ-Archiv**)	Nein	Ja
Backup-Planung	Benutzerdefiniert (S. 140)	Kann nicht geändert werden. Jeder Schutzplan wird täglich zur gleichen Tageszeit ausgeführt.*
Backup-Speicherorte	Cloud Storage, lokaler Ordner, Netzwerkordner	Nur Cloud Storage
Automatischer Schutz für neue Office 365-Benutzer, -Gruppen, -Websites	Nein	Ja, indem Sie einen Schutzplan auf die Gruppen **Alle Benutzer**, **Alle Gruppen**, **Alle Websites** anwenden.
Mehr als eine Office 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

	Lokaler Agent für Office 365	Cloud Agent für Office 365
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 (S. 415)
Maximale Anzahl von gleichzeitigen Recovery-Aktionen	Nein	10 Aktionen, einschließlich G Suite-Recovery-Aktionen

* Da ein 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.

***Hinweis**: Die Planung für den Schutz kann durch Aktionen und Einstellungen von Dritthersteller-Diensten beeinflusst werden – beispielsweise die Verfügbarkeit von Microsoft Office 365-Servern, den Drosselungseinstellungen auf den Microsoft-Servern und ähnlichem. Zu weiteren Informationen siehe https://docs.microsoft.com/de-de/graph/throttling https://docs.microsoft.com/en-us/graph/throttling.*

** Es wird 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.

Einschränkungen

- 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.

Erforderliche Benutzerrechte

Im Cyber Protection Service

Jeder Agent für Office 365, ob lokal oder Cloud-basiert, muss unter dem Konto eines Firmenadministrators registriert sein und auf einer Kunden-Mandanten-Ebene verwendet werden. Firmenadministratoren, die auf Abteilungsebene agieren, Abteilungsadministratoren und Benutzer können keine Backups oder Wiederherstellungen von Office 365-Daten durchführen.

In Microsoft Office 365

Ihrem Konto muss die Rolle 'globaler Administrator' in Microsoft Office 365 zugewiesen sein.

Um öffentliche Office 365-Ordner sichern und wiederherstellen zu können, muss mindestens eines Ihrer Office 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 Office 365 anmelden. Damit der Agent auf die Inhalte aller Postfächer zugreifen kann, wird diesem Konto die Verwaltungsrolle **ApplicationImpersonation** zugewiesen. Wenn Sie das Kontokennwort ändern, müssen Sie auch das Kennwort in der Service-Konsole aktualisieren (wie unter 'Die Office 365-Zugriffsanmeldedaten ändern (S. 255)' beschrieben).
- Der Cloud Agent meldet sich nicht bei Office 365 an. Der Agent erhält die notwendigen Berechtigungen direkt von Microsoft Office 365. Sie müssen die Gewährung dieser Berechtigungen nur einmal bestätigen, wenn Sie als globaler Administrator angemeldet sind. Der Agent speichert Ihre Kontoanmeldedaten nicht und verwendet diese beim Durchführen von Backups und Wiederherstellungen nicht. Eine Änderung des Kontokennworts oder Deaktivierung dieses Kontos oder Löschen dieses Kontos in Office 365 hat keinen Einfluss auf den Betrieb des Agenten.

15.18.1 Den lokal installierten Agenten für Office 365 verwenden

15.18.1.1 Eine Microsoft Office 365-Organisation hinzufügen

So können Sie eine Microsoft Office 365-Organisation hinzufügen

1. Melden Sie sich als Firmenadministrator an der Service-Konsole an.
2. Klicken Sie in der rechten oberen Ecke auf das Symbol für 'Konto' und anschließend auf die Befehle **Downloads** –> **Agent fü Office 365**.
3. Laden Sie den Agenten herunter und installieren Sie ihn auf einer Windows-Maschine, die mit dem Internet verbunden ist.
4. Klicken Sie nach Abschluss der Installation auf **Geräte** –> **Microsoft Office 365** – und geben Sie dann die Anmeldedaten des globalen Office 365-Administrators ein.

   ***Wichtig:**: Innerhalb einer Organisation (Firmen-Gruppe) darf es nur einen lokal installierten Agenten für Office 365 geben.*

Als Ergebnis erscheinen die Datenelemente Ihrer Organisation in der Service-Konsole auf der Seite **Microsoft Office 365**.

15.18.1.2 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
- Anmerkungen

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.

Postfächer auswählen

Wählen Sie die Postfächer wie nachfolgend beschrieben aus – und spezifizieren Sie dann die anderen Einstellungen des Schutzplans nach Bedarf (S. 122).

So können Sie Postfächer auswählen

1. Klicken Sie auf **Microsoft Office 365**.
2. Melden Sie sich bei Aufforderung als globaler Administrator an Microsoft Office 365 an.
3. Wählen Sie die Postfächer aus, die Sie per Backup sichern wollen.
4. Klicken Sie auf **Backup**.

Postfächer und Postfachelemente wiederherstellen

Postfächer wiederherstellen

1. Klicken Sie auf **Microsoft Office 365**.
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' (S. 220) 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**.
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' (S. 220) 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.

   Tipp: *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. 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.

Die Office 365-Zugriffsanmeldedaten ändern

Sie können die Zugriffsanmeldedaten für Office 365 ändern, ohne den Agenten neu installieren zu müssen.

So ändern Sie die Anmeldedaten für Office 365

1. Klicken Sie auf **Geräte** –> **Microsoft Office 365**.
2. Klicken Sie auf **Anmeldedaten spezifizieren**.
3. Geben Sie die Anmeldedaten des globalen Office 365-Administrators ein und klicken Sie dann auf **OK**.

   Der Agent wird sich mit diesem Konto bei Office 365 anmelden. Damit der Agent auf die Inhalte aller Postfächer zugreifen kann, wird diesem Konto die Verwaltungsrolle **ApplicationImpersonation** zugewiesen.

15.18.2 Den Cloud Agenten für Office 365 verwenden

15.18.2.1 Eine Microsoft Office 365-Organisation hinzufügen

So können Sie eine Microsoft Office 365-Organisation hinzufügen

1. Melden Sie sich als Firmenadministrator an der Service-Konsole an.
2. Klicken Sie auf **Geräte** –> **Hinzufügen** –> **Microsoft Office 365 Business**.
3. Wählen Sie das von Ihrer Organisation/Firma verwendete Microsoft Datacenter aus.

   Die Software leitet Sie zur Microsoft Office 365-Anmeldeseite weiter.
4. Melden Sie sich mit den Anmeldedaten des globalen Office 365-Administrators an.

   Microsoft Office 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 erscheinen die Datenelemente Ihres Unternehmens in der Service-Konsole auf der Seite **Microsoft Office 365**.

Tipps zur weiteren Nutzung

- Der Cloud Agent führt die Synchronisierung mit Office 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 Service-Konsole angezeigt. Wenn Sie die Synchronisierung des Cloud Agenten mit Office 365 erzwingen wollen, wählen Sie die entsprechende Organisation auf der **Microsoft Office 365**-Seite aus und klicken Sie dann auf **Aktualisieren**.
- 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, nachdem diese aus der Office 365-Benutzeroberfläche entfernt wurden, noch für einige weitere Tage per API verfügbar. Während dieser Tage wird das entfernte Element in der Service-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 Service-Konsole. Dessen Backups können (sofern vorhanden) unter **Backups** –> **Cloud-Applikationen-Backups** gefunden werden.

15.18.2.2 Eine Microsoft Office 365-Organisation löschen

So können Sie eine Microsoft Office 365-Organisation löschen

1. Melden Sie sich als Firmenadministrator an der Service-Konsole an.
2. Gehen Sie zu **Geräte** –> **Microsoft Office 365**.
3. Wählen Sie die Organisation aus und klicken Sie 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 Office 365-Organisationsdaten manuell entziehen.

So können Sie die Zugriffsrechte widerrufen

1. Melden Sie sich als globaler Administrator an Office 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 im Aktionsbereich auf den Befehl **Löschen**.
5. Bestätigen Sie die Löschaktion.

Als Ergebnis werden der Backup Service-Applikation die Zugriffsrechte auf die Daten der Office 365-Organisation entzogen.

15.18.2.3 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 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. Sie dürfen die Organisation nicht löschen. Wiederholen Sie stattdessen einfach die im Abschnitt 'Eine Microsoft Office 365-Organisation hinzufügen (S. 256)' 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
- Kalendereregnisse
- 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 (S. 122).

So können Sie Exchange Online-Postfächer auswählen

1. Klicken Sie auf **Microsoft Office 365**.
2. Wenn dem Cyber Protection Service mehrere Office 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 Office 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 Office 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 **Office 365-Postfächer** bei **Backup-Quelle** ausgewählt ist.
   - 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 (S. 122).

So können Sie öffentliche Ordner von Exchange Online auswählen

1. Klicken Sie auf **Microsoft Office 365**.
2. Wenn dem Cyber Protection Service mehrere Office 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-Backp**.
- 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 **Office 365-Postfächer** bei **Backup-Quelle** ausgewählt ist.

Postfächer und Postfachelemente wiederherstellen

Postfächer wiederherstellen

1. Klicken Sie auf **Microsoft Office 365**.
2. Wenn dem Cyber Protection Service mehrere Office 365-Organisationen hinzugefügt wurden, wählen Sie diejenige Organisation aus, deren Backup-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' (S. 220) 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.

   ***Tipp**: 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 Office 365-Organisationen hinzugefügt werden, klicken Sie auf **Office 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.
8. Klicken Sie auf **Recovery starten**.
9. Wählen Sie eine dieser Überschreiben-Optionen:
   - **Vorhandene Elemente überschreiben**

- **Vorhandene Elemente nicht überschreiben**

10. Klicken Sie auf **Fertig stellen**, um Ihre Entscheidung zu bestätigen.

Postfachelemente wiederherstellen

1. Klicken Sie auf **Microsoft Office 365**.
2. Wenn dem Cyber Protection Service mehrere Office 365-Organisationen hinzugefügt wurden, wählen Sie diejenige Organisation aus, deren Backup-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' (S. 220) 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.

   Tipp: *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 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 Office 365-Organisationen hinzugefügt wurden, klicken Sie auf **Office 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 **Fertig stellen**, um Ihre Entscheidung zu bestätigen.

Öffentliche Ordner und Ordnerelemente wiederherstellen

Um einen öffentlichen Ordner oder einzelne Elemente eines öffentlichen Ordners wiederherzustellen, muss mindestens ein Administrator der Office 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 Service-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 Office 365**.
2. Wenn dem Cyber Protection Service mehrere Office 365-Organisationen hinzugefügt werden, 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' (S. 220) 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.
   - Klicken Sie bei der Auswahl einer E-Mail-Nachricht oder eines Postings auf **Als E-Mail senden**, wenn Sie das Element an spezifizierte E-Mail-Adressen 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 Office 365-Organisationen hinzugefügt wurden, klicken Sie auf **Office 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.
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:
    - **Vorhandene Elemente überschreiben**
    - **Vorhandene Elemente nicht überschreiben**
14. Klicken Sie auf **Fertig stellen**, um Ihre Entscheidung zu bestätigen.

15.18.2.4 OneDrive-Dateien sichern

Welche Elemente können per Backup gesichert werden?

Sie können ein komplettes OneDrive sichern – oder auch nur einzelne Dateien und Ordner.

Dateien werden inklusive ihrer Freigabeberechtigungen gesichert. Erweiterte Berechtigungsstufen (**Entwerfen**, **Vollzugriff**, **Mitwirken**) werden nicht mitgesichert.

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 Freigabeberechtigungen 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 (S. 122).

So können Sie OneDrive-Dateien auswählen

1. Klicken Sie auf **Microsoft Office 365**.
2. Wenn dem Cyber Protection Service mehrere Office 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.
   - 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 (S. 168)'.
     - 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.

OneDrive und OneDrive-Dateien wiederherstellen

Ein komplettes OneDrive wiederherstellen

1. Klicken Sie auf **Microsoft Office 365**.
2. Wenn dem Cyber Protection Service mehrere Office 365-Organisationen hinzugefügt wurden, wählen Sie diejenige Organisation aus, deren Backup-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' (S. 220) 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.

   Tipp: *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 Office 365-Organisationen hinzugefügt wurden, klicken Sie auf **Office 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 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 Freigabeberechtigungen der Dateien mit wiederherstellen wollen.
9. Klicken Sie auf **Recovery starten**.
10. Wählen Sie eine dieser Überschreiben-Optionen:
    - **Vorhandene Dateien überschreiben**
    - **Vorhandene Datei überschreiben, wenn diese älter ist**
    - **Vorhandene Dateien nicht überschreiben**
11. Klicken Sie auf **Fertig stellen**, um Ihre Entscheidung zu bestätigen.

OneDrive-Dateien wiederherstellen

1. Klicken Sie auf **Microsoft Office 365**.

2. Wenn dem Cyber Protection Service mehrere Office 365-Organisationen hinzugefügt wurden, wählen Sie diejenige Organisation aus, deren Backup-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' (S. 220) 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.

   Tipp: *Wenn Sie nur Recovery-Punkte sehen wollen, die OneDrive-Dateien enthalten, wählen Sie* ***OneDrive*** *bei* ***Nach Inhalt filtern****.*
5. Klicken Sie auf **Wiederherstellen** –> **Dateien/Ordner**.
6. Wechseln Sie zum benötigten Ordner oder verwenden Sie die Suchfunktion, um eine Liste der erforderlichen Dateien und Ordner abzurufen.

   Die Suchfunktion ist nicht verfügbar, wenn das Backup verschlüsselt ist.
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 Office 365-Organisationen hinzugefügt wurden, klicken Sie auf **Office 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 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:
    - **Vorhandene Dateien überschreiben**
    - **Vorhandene Datei überschreiben, wenn diese älter ist**
    - **Vorhandene Dateien nicht überschreiben**

16. Klicken Sie auf **Fertig stellen**, um Ihre Entscheidung zu bestätigen.

15.18.2.5 SharePoint Online-Websites sichern

Welche Elemente können per Backup gesichert werden?

Sie können klassische SharePoint Website-Sammlungen, Gruppen-(Team)-Websites und Kommunikations-Websites sichern. Sie können außerdem einzelne Unterwebsites, Listen und Bibliotheken für ein Backup auswählen.

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.
- OneNote-Dateien (aufgrund von Beschränkungen der SharePoint Online API).
- 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.
- Sie können keine Websites sichern, die mit der Business Productivity Online Suite (BPOS), dem Vorgänger von Microsoft Office 365, erstellt wurden.
- Sie können keine Einstellungen von Websites sichern, die den verwalteten Pfad '**`/portals`**' verwenden (Beispiel: **`https://<tenant>.sharepoint.com/portals/...`**).

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 (S. 122).

So können Sie SharePoint Online-Daten auswählen

1. Klicken Sie auf **Microsoft Office 365**.
2. Wenn dem Cyber Protection Service mehrere Office 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), erweitern Sie den Knoten **Website-Sammlung**, wählen Sie **Alle Website-Sammlungen** und klicken Sie dann auf **Gruppen-Backup**.
   - 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 zu sichern (einschließlich der Websites, die erst in der Zukunft erstellt werden), erweitern Sie den Knoten **Gruppen**, wählen Sie **Alle Gruppen** und klicken Sie dann auf **Gruppen-Backup**.
   - Wenn Sie einzelne Gruppen-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.

SharePoint Online-Daten wiederherstellen

1. Klicken Sie auf **Microsoft Office 365**.
2. Wenn dem Cyber Protection Service mehrere Office 365-Organisationen hinzugefügt wurden, wählen Sie diejenige Organisation aus, deren Backup-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 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' (S. 220) 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.

   Tipp: *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.

   Die Suchfunktion ist nicht verfügbar, wenn das Backup verschlüsselt ist.
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. Wenn Sie ein Element herunterladen wollen, müssen Sie dieses auswählen, auf **Download** klicken, den Zielspeicherort für das Element bestimmen und schließlich auf **Speichern** klicken. Ansonsten können Sie diesen Schritt überspringen.
9. Klicken Sie auf **Recovery**.
10. Wenn dem Cyber Protection Service mehrere Office 365-Organisationen hinzugefügt wurden, klicken Sie auf **Office 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.

    Standardmäßig ist die ursprüngliche Website vorausgewählt. Wenn diese Website nicht mehr existiert oder Sie eine andere als die ursprüngliche Organisation als Ziel ausgewählt haben, müssen Sie die Ziel-Website 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 Dateien überschreiben**
    - **Vorhandene Datei überschreiben, wenn diese älter ist**
    - **Vorhandene Dateien nicht überschreiben**
15. Klicken Sie auf **Fertig stellen**, um Ihre Entscheidung zu bestätigen.

15.18.2.6 Office 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.

Welche Elemente können wiederhergestellt werden?

- Das komplette Team
- 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, Chats.
- Aufkleber und Lobs.

Backup und Recovery werden für folgende Kanal-Registerkarten unterstützt:

- Word
- Excel
- PowerPoint
- PDF
- Dokumentbibliothek

Dateien, die in privaten Kanälen freigegeben sind, werden zwar gesichert, aber aufgrund einer API-Beschränkung nicht wiederhergestellt.

***Hinweis**: Diese Dateien werden an bestimmten Orten gespeichert, getrennt von den Dateien, die in öffentlichen Kanälen freigegeben werden.*

Teams auswählen

Wählen Sie Teams wie nachfolgend beschrieben aus – und spezifizieren Sie dann die anderen Einstellungen des Schutzplans nach Bedarf (S. 122).

So können Sie Teams auswählen

1. Klicken Sie auf **Microsoft Office 365**.
2. Wenn dem Cyber Protection Service mehrere Office 365-Organisationen hinzugefügt wurden, müssen Sie die Organisation auswählen, 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.

Ein komplettes Team wiederherstellen

1. Klicken Sie auf **Microsoft Office 365**.
2. Wenn dem Cyber Protection Service mehrere Office 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 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 Office 365-Organisationen hinzugefügt wurden, klicken Sie auf **Office 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 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.
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**
9. Klicken Sie auf **Fertig stellen** , 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`.

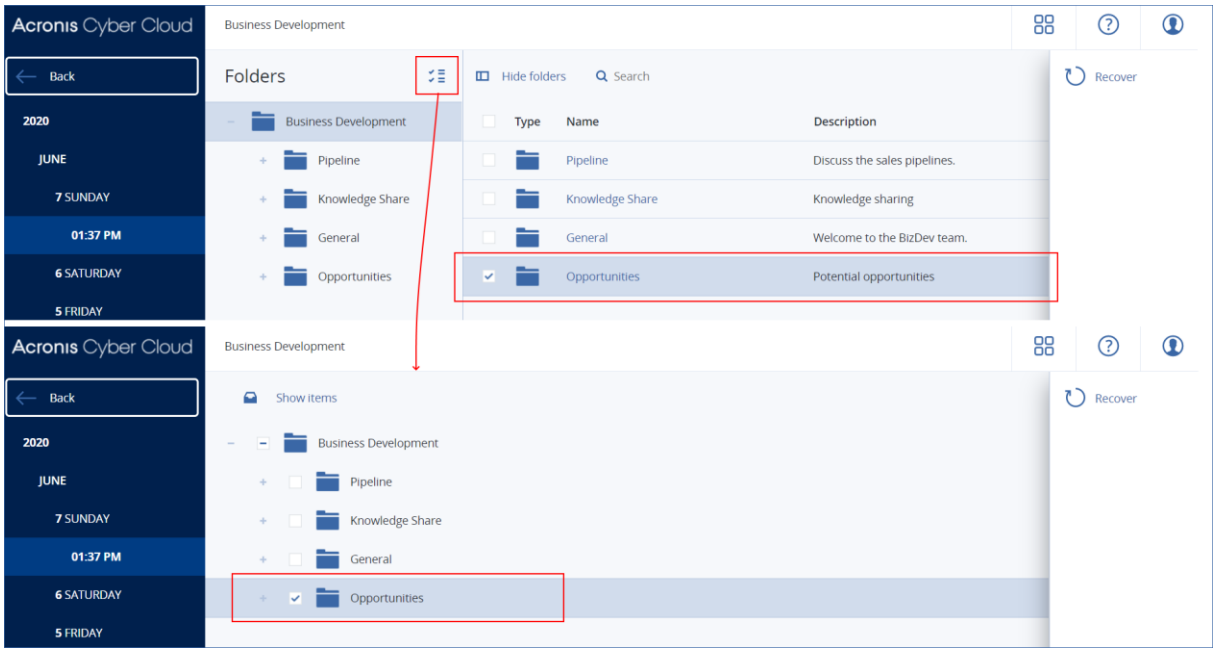
***Hinweis**: Nachdem Sie ein Team oder Team-Kanäle wiederhergestellt haben, gehen Sie zu Microsoft Teams, wählen Sie die wiederhergestellten Kanäle aus und klicken Sie dann auf deren Registerkarte **Dateien**. Anderenfalls werden die nachfolgenden Backups dieser Kanäle die Inhalte dieser Registerkarte 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 Office 365**.
2. Wenn dem Cyber Protection Service mehrere Office 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. Alternativ können Sie auch auf das Symbol 'Ordner wiederherstellen' klicken und den gewünschten Kanal im Bereich **Ordner** auswählen.



Folgende Suchoptionen sind verfügbar:

- Für **Unterhaltungen**: Absender, Inhalt, Sprache, Name der Anlage, Datum oder Datumsbereich.
- Für **Dateien**: Dateiname oder Ordnername, Dateityp, Größe, Datum oder Datumsbereich der letzten Änderung.

7. Wenn dem Cyber Protection Service mehrere Office 365-Organisationen hinzugefügt wurden, klicken Sie auf **Office 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**

12. Klicken Sie auf **Fertig stellen**, 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 Office 365**.
2. Wenn dem Cyber Protection Service mehrere Office 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. Wählen Sie die wiederherzustellenden Elemente aus und klicken Sie dann auf **Recovery**.
8. Wenn dem Cyber Protection Service mehrere Office 365-Organisationen hinzugefügt wurden, klicken Sie auf 'Office 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 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.
10. Bei **Zu Kanal wiederherstellen** können Sie den gewünschte Zielkanal anzeigen lassen, ändern oder 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**
14. Klicken Sie auf **Fertig stellen**, 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 der Anlage
- Datum

Team-Postfächer wiederherstellen

1. Klicken Sie auf **Microsoft Office 365**.
2. Wenn dem Cyber Protection Service mehrere Office 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 Office 365-Organisationen hinzugefügt wurden, klicken Sie auf **Office 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 **Fertig stellen** , um Ihre Entscheidung zu bestätigen.

E-Mail-Nachrichten und Besprechungen wiederherstellen

1. Klicken Sie auf **Microsoft Office 365**.

2. Wenn dem Cyber Protection Service mehrere Office 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 Office 365-Organisationen hinzugefügt wurden, klicken Sie auf **Office 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 **Fertig stellen** , um Ihre Entscheidung zu bestätigen.

Eine Team-Website oder bestimmte Elemente einer Website wiederherstellen

1. Klicken Sie auf **Microsoft Office 365**.

2. Wenn dem Cyber Protection Service mehrere Office 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.

   Die Suchfunktion ist nicht verfügbar, wenn das Backup verschlüsselt ist.
7. Wählen Sie die wiederherzustellenden Elemente aus und klicken Sie dann auf **Recovery**.
8. Wenn dem Cyber Protection Service mehrere Office 365-Organisationen hinzugefügt wurden, klicken Sie auf **Office 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.
9. 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.
10. Bestimmen Sie, ob Sie auch die Freigabe-Berechtigungen der wiederhergestellten Elemente mit wiederherstellen wollen.
11. Klicken Sie auf **Recovery starten**.
12. Wählen Sie eine dieser Überschreiben-Optionen:
    - **Vorhandene Inhalte überschreiben, wenn diese älter sind**
    - **Vorhandene Inhalte überschreiben**
    - **Vorhandene Inhalte nicht überschreiben**
13. Klicken Sie auf **Fertig stellen** , um Ihre Entscheidung zu bestätigen.

15.18.2.7 Upgrade des Cloud Agenten

In diesem Abschnitt wird beschrieben, wie Sie ein Upgrade auf die aktuelle Version der Backup-Lösung für Microsoft Office 365 durchführen können. Diese Version unterstützt OneDrive- und SharePoint Online-Backups und bietet eine verbesserte Performance bei Backups und Wiederherstellungen. Ab der Version 8.0 des Cyber Protection Service werden folgende Funktionen von der alten Lösung nicht mehr unterstützt: einen Schutzplan bearbeiten, löschen, anwenden und widerrufen.

Die Upgrade-Verfügbarkeit hängt davon ab, welches Datacenter verfügbar ist und welche Einstellungen Ihr Service-Provider vorgenommen hat. Wenn das Upgrade verfügbar ist, wird in der Service-Konsole oben auf der Registerkarte **Microsoft Office 365 (v1)** eine Benachrichtigung angezeigt.

Der Upgrade-Prozess

Während des Upgrades werden die Benutzer Ihrer Office 365-Organisation der neuen Backup-Lösung hinzugefügt. Die Schutzpläne werden migriert und auf die entsprechenden Benutzer angewendet.

Früher erstellte Backups werden von einem Speicherort in der Cloud zu einem anderen kopiert. Die kopierten Backups werden auf der Registerkarte **Backup Storage** in einem separaten Bereich namens **Cloud-Applikationen-Backups** angezeigt, während die ursprünglichen Backups im Speicherort **Cloud Storage** verbleiben. Nach Abschluss des Upgrade-Prozesses werden die ursprünglichen Backups aus dem Speicherort **Cloud Storage** gelöscht.

Das Upgrade kann mehrere Stunden oder sogar Tage dauern – in Abhängigkeit von der Anzahl der Benutzer im Unternehmen, der Anzahl der Backups und der Zugriffsgeschwindigkeit auf Office 365. Während des Upgrades können aber weiterhin Wiederherstellungen aus früher erstellten Backups durchgeführt werden. Jedoch gehen alle Backups und Schutzpläne, die während des Upgrades erstellt werden, verloren.

Für den unwahrscheinlichen Fall, dass es zu einem Upgrade-Fehler kommt, bleibt die Backup-Lösung voll funktionsfähig. Das Upgrade kann dann vom Fehlerzeitpunkt aus neu gestartet werden.

So können Sie den Upgrade-Prozess starten

1. Klicken Sie auf **Microsoft Office 365 (v1)**.
2. Klicken Sie in der Benachrichtigung im oberen Fensterbereich auf den Befehl **Upgrade**.
3. Bestätigen Sie, dass Sie den Upgrade-Prozess wirklich starten wollen.
4. Wählen Sie das von Ihrer Organisation/Firma verwendete Microsoft Datacenter aus.

   Die Software leitet Sie zur Microsoft Office 365-Anmeldeseite weiter.
5. Melden Sie sich mit den Anmeldedaten des globalen Office 365-Administrators an.

   Microsoft Office 365 zeigt eine Liste der Berechtigungen an, die erforderlich sind, um die Daten Ihres Unternehmens sichern und wiederherstellen zu können.
6. Bestätigen Sie, dass Sie dem Cyber Protection Service diese Berechtigungen gewähren wollen.

   Sie werden zur Service-Konsole umgeleitet und der Upgrade-Prozess wird gestartet. Der Verlauf des Upgrades wird im Fensterbereich **Microsoft Office 365** –> **Aktivitäten** angezeigt.

15.19 G Suite-Daten sichern

Was bedeutet die Sicherung von G Suite?

- Cloud-zu-Cloud-basiertes Backup & Recovery von G Suite-Benutzerdaten (Gmail-Postfächer, Kalender, Kontakte, Google Drives) und G Suite Shared Drives.
- Granulares Recovery von E-Mails, Dateien, Kontakten und anderen Datenelementen.
- Unterstützung für mehrere G Suite-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.

Unterstützte G Suite-Editionen

- G Suite Basic. Nur Gmail-, Drive-, Kalender- und Kontakte-Services.
- G Suite Business. Nur Gmail-, Drive- (inkl. Shared Drives), Kalender- und Kontakte-Services.
- G Suite Enterprise. Nur Gmail-, Drive- (inkl. Shared Drives), Kalender- und Kontakte-Services.
- G Suite for Education. Nur Gmail-, Drive- (inkl. Shared Drives), Kalender- und Kontakte-Services. Der Classroom-Service wird nicht unterstützt

Erforderliche Benutzerrechte

Im Cyber Protection Service

Im Cyber Protection Service müssen Sie ein Firmenadministrator sein, der auf einer Kunden-Mandanten-Ebene agiert. Firmenadministratoren, die auf Abteilungsebene agieren, Abteilungsadministratoren und Benutzer können keine Backups oder Wiederherstellungen von G Suite-Daten durchführen.

In G Suite

Wenn Sie Ihre G-Suite-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 G Suite ändern, hat dies keinen Einfluss auf die Cyber Protection Service-Operationen.

Wenn der Super Admin, der die G Suite-Organisation hinzugefügt hat, aus G Suite gelöscht wird oder eine Admin-Rolle mit weniger Rechten erhält, werden die Backups mit einer Fehlermeldung wie 'Zugriff verweigert' fehlschlagen. In diesem Fall müssen Sie die im Abschnitt 'Eine G Suite-Organisation hinzufügen (S. 279)' erläuterte Prozedur wiederholen und gültige Super Admin-Anmeldedaten spezifizieren. Zur Vermeidung dieser Situation 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.

Einschränkungen

- Eine Suche in verschlüsselten Backups wird nicht unterstützt.
- Nicht mehr als 10 manuelle Backup-Ausführungen in einer Stunde (S. 415).
- Nicht mehr als 10 gleichzeitige Recovery-Aktionen (diese Anzahl beinhaltet sowohl Office 365- als auch G Suite-Wiederherstellungen).

15.19.1 Eine G Suite-Organisation hinzufügen

Eine G Suite-Organisation hinzufügen

1. Melden Sie sich als Firmenadministrator an der Service-Konsole an.
2. Klicken Sie auf **Geräte** –> **Hinzufügen** –> **G Suite**.
3. Befolgen Sie die von der Software angezeigten Instruktionen:
   a. Klicken Sie auf **Marketplace öffnen**.
   b. Melden Sie sich mit den Anmeldedaten des Super Admins an.
   c. Klicken Sie auf **Domain installieren**.
   d. Bestätigen Sie die Domain-weite Installation.

      G Suite zeigt eine Liste der Berechtigungen an, die erforderlich sind, um die Daten Ihrer Organisation sichern und wiederherstellen zu können.
   e. Bestätigen Sie, dass Sie dem Cyber Protection Service diese Berechtigungen gewähren wollen.
   f. Schließen Sie die Installationsprozedur ab.
   g. Gehen Sie zum App Launcher-Symbol, suchen Sie die Cyber Protection Service-Applikation in der Liste und klicken Sie dann auf diese.

Sie werden zurück zur Service-Konsole geleitet. Die Datenelemente Ihrer Organisation werden in der Service-Konsole auf der Seite **G Suite** angezeigt.

Tipps zur weiteren Nutzung

- Nach dem Hinzufügen einer G-Suite-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 G Suite 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 Service-Konsole angezeigt. Wenn Sie die Synchronisierung des Cloud Agenten mit G Suite erzwingen wollen, wählen Sie die entsprechende Organisation auf der **G Suite**-Seite aus und klicken Sie dann auf **Aktualisieren**.
- 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, nachdem dieser/dieses aus der G Suite-Benutzeroberfläche entfernt wurde, noch für einige weitere Tage per API verfügbar. Während dieser Tage wird das entfernte Element in der Service-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 Service-Konsole. Dessen Backups können (sofern vorhanden) unter **Backups** –> **Cloud-Applikationen-Backups** gefunden werden.

15.19.2 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 Kalendereereignisse 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
- Kalendereereignisse
- Kontakte

Sie können die Suchfunktion verwenden, um bestimmte Elemente in einem Backup zu finden – außer das Backup ist verschlüsselt. Eine Suche in verschlüsselten Backups wird nicht unterstützt.

Sie können bei der Wiederherstellung von Postfächern und Postfachelementen 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 Kalendereereignis wiederhergestellt.

15.19.2.1 Postfächer auswählen

Wählen Sie die Postfächer wie nachfolgend beschrieben aus – und spezifizieren Sie dann die anderen Einstellungen des Schutzplans nach Bedarf (S. 122).

So können Sie Gmail-Postfächer auswählen

1. Klicken Sie auf **G Suite**.

2. Wenn dem Cyber Protection Service mehrere G Suite-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 (S. 281) durchsuchen wollen. Sie finden diese Option, wenn Sie zuerst auf das Zahnradsymbol klicken – und dann auf **Backup-Optionen** –> **Volltextsuche**.

Volltextsuche

Diese Option bestimmt, ob die Inhalte von E-Mail-Nachrichten vom Cloud-Agenten indiziert werden.

Die Voreinstellung ist: **Aktiviert**.

Wenn diese Option aktiviert ist, werden die Nachrichteninhalte indiziert und Sie können Nachrichten nach ihrem Inhalten durchsuchen. Ansonsten können Sie die Nachrichten nur nach Betreff, Absender, Empfänger oder Datum durchsuchen.

***Hinweis**: Eine Suche in verschlüsselten Backups wird nicht unterstützt.*

Der Indizierungsprozess hat keinen Einfluss auf die Backup-Performance, da diese Prozesse jeweils von unterschiedlichen Software-Komponenten durchgeführt werden. Die Indizierung des ersten (vollständigen) Backups kann einige Zeit benötigen, daher kann es zu einer Verzögerung zwischen der Backup-Fertigstellung und der anschließenden Anzeige der Inhalt in den Suchergebnissen kommen.

Der Index belegt 10-30 Prozent des Speicherplatzes, der für die Postfach-Backups belegt wird. Wenn Sie den exakten Wert erfahren wollen, klicken Sie auf **Backup Storage** –> **Cloud-Applikationen-Backups** und sehen Sie sich die Spalte **Indexgröße** an. Wenn Sie Speicherplatz sparen wollen, können Sie die Volltextsuche deaktivieren. Der Wert in der Spalte **Indexgröße** wird dann nach dem nächsten Backup auf eine wenige Megabyte reduziert. Diese minimale Menge an Metadaten ist notwendig, um nach Betreff, Absender, Empfänger oder Datum suchen zu können.

Wenn Sie die Volltextsuche wieder aktivieren, indiziert die Software alle Backups, die zuvor durch den Schutzplan erstellt wurden. Dies wird ebenfalls einige Zeit benötigen.

15.19.2.2 Postfächer und Postfachelemente wiederherstellen

Postfächer wiederherstellen

1. Klicken Sie auf **G Suite**.

2. Wenn dem Cyber Protection Service mehrere G Suite-Organisationen hinzugefügt wurden, wählen Sie diejenige Organisation aus, deren Backup-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 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' (S. 220) 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.

   Tipp: *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 G Suite-Organisationen hinzugefügt werden, klicken Sie auf **G Suite-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 **Fertig stellen**, um Ihre Entscheidung zu bestätigen.

Postfachelemente wiederherstellen

1. Klicken Sie auf **G Suite**.
2. Wenn dem Cyber Protection Service mehrere G Suite-Organisationen hinzugefügt wurden, wählen Sie diejenige Organisation aus, deren Backup-Daten Sie wiederherstellen wollen. 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' (S. 220) 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.

   Tipp: *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. Die letzten beiden Optionen sind nur dann verfügbar, wenn die Option **Volltextsuche** während des Backups aktiviert war. Die Sprache eines zu durchsuchenden Nachrichtenfragments kann als weiterer Parameter angegeben werden.
   - 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 G Suite-Organisationen hinzugefügt wurden, klicken Sie auf **G Suite-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. 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 **Fertig stellen**, um Ihre Entscheidung zu bestätigen.

15.19.3 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. Optional können Sie auch Dateien sichern, die für Google Drive-Benutzer freigegeben wurden.

Dateien werden inklusive ihrer Freigabeberechtigungen gesichert.

Folgende Elemente werden bei einem Backup *übersprungen*:

- Eine freigegebene Datei – wenn der Benutzer Zugriff als Kommentator oder Betrachter auf die Datei hat und der Dateibesitzer die Optionen zum Herunterladen, Drucken und Kopieren für Kommentatoren und Betrachter deaktiviert hat.
- Der Ordner **Computer** (vom Backup & Sync-Client erstellt)

Einschränkungen

- Von den Google-spezifischen Dateiformaten werden nur Google Docs, Google Tabellen, Google Präsentationen und Google Zeichnungen gesichert.

Welche Elemente können wiederhergestellt werden?

Sie können ein komplettes Google Drive wiederherstellen oder beliebige einzelne Dateien/Ordner, die gesichert wurden.

Sie können die Suchfunktion verwenden, um bestimmte Elemente in einem Backup zu finden – außer das Backup ist verschlüsselt. Eine Suche in verschlüsselten Backups wird nicht unterstützt.

Sie können wählen, ob die Dateien bei der Wiederherstellung ihre ursprünglichen Freigabeberechtigungen 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.

15.19.3.1 Google Drive-Dateien auswählen

Wählen Sie die Dateien wie nachfolgend beschrieben aus – und spezifizieren Sie dann die anderen Einstellungen des Schutzplans nach Bedarf (S. 122).

So können Sie Google Drive-Dateien auswählen

1. Klicken Sie auf **G Suite**.
2. Wenn dem Cyber Protection Service mehrere G Suite-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 ist.
   - 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 (S. 168)'.
     - 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 die Dateien sichern möchten, die für die ausgewählten Benutzer freigegeben wurden, aktivieren Sie den Schalter **Freigegebene Dateien einbeziehen**.
   - 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) (S. 291)'.

15.19.3.2 Google Drive und Google Drive-Dateien wiederherstellen

Ein komplettes Google Drive wiederherstellen

1. Klicken Sie auf **G Suite**.
2. Wenn dem Cyber Protection Service mehrere G Suite-Organisationen hinzugefügt wurden, wählen Sie diejenige Organisation aus, deren Backup-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 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' (S. 220) 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.

   Tipp: *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 G Suite-Organisationen hinzugefügt wurden, klicken Sie auf **G Suite-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 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 Freigabeberechtigungen der Dateien mit wiederherstellen wollen.
9. Klicken Sie auf **Recovery starten**.
10. Wählen Sie eine dieser Überschreiben-Optionen:
    - **Vorhandene Dateien überschreiben**
    - **Vorhandene Datei überschreiben, wenn diese älter ist**
    - **Vorhandene Dateien nicht überschreiben**
11. Klicken Sie auf **Fertig stellen**, um Ihre Entscheidung zu bestätigen.

Google Drive-Dateien wiederherstellen

1. Klicken Sie auf **G Suite**.
2. Wenn dem Cyber Protection Service mehrere G Suite-Organisationen hinzugefügt wurden, wählen Sie diejenige Organisation aus, deren Backup-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 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' (S. 220) 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.

   Tipp: *Wenn Sie nur Recovery-Punkte sehen wollen, die Google Drive-Dateien enthalten, wählen Sie* ***Google Drive*** *bei* ***Nach Inhalt filtern****.*
5. Klicken Sie auf **Wiederherstellen** –> **Dateien/Ordner**.
6. Wechseln Sie zum benötigten Ordner oder verwenden Sie die Suchfunktion, um eine Liste der erforderlichen Dateien und Ordner abzurufen.

   Die Suchfunktion ist nicht verfügbar, wenn das Backup verschlüsselt ist.
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 G Suite-Organisationen hinzugefügt wurden, klicken Sie auf **G Suite-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 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:
    - **Vorhandene Dateien überschreiben**
    - **Vorhandene Datei überschreiben, wenn diese älter ist**
    - **Vorhandene Dateien nicht überschreiben**
16. Klicken Sie auf **Fertig stellen**, um Ihre Entscheidung zu bestätigen.

15.19.4 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 Freigabeberechtigungen gesichert.

Einschränkungen

- Ein Shared Drive ohne Mitglieder kann aufgrund von Beschränkungen der Google Drive API nicht gesichert werden.
- Von den Google-spezifischen Dateiformaten werden nur Google Docs, Google Tabellen, Google Präsentationen und Google Zeichnungen gesichert.

Welche Elemente können wiederhergestellt werden?

Sie können ein komplettes Shared Drive wiederherstellen oder beliebige einzelne Dateien/Ordner, die gesichert wurden.

Sie können die Suchfunktion verwenden, um bestimmte Elemente in einem Backup zu finden – außer das Backup ist verschlüsselt. Eine Suche in verschlüsselten Backups wird nicht unterstützt.

Sie können wählen, ob die Dateien bei der Wiederherstellung ihre ursprünglichen Freigabeberechtigungen aus dem Backup beibehalten sollen – oder ob sie die Berechtigungen desjenigen Ordner übernehmen sollen, in dem sie wiederhergestellt werden.

Folgende Elemente werden nicht wiederhergestellt:

- Freigabeberechtigungen 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.
- Freigabeberechtigungen 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.

15.19.4.1 Shared Drive-Dateien auswählen

Wählen Sie die Dateien wie nachfolgend beschrieben aus – und spezifizieren Sie dann die anderen Einstellungen des Schutzplans nach Bedarf (S. 122).

So können Sie Shared Drive-Dateien auswählen

1. Klicken Sie auf **G Suite**.
2. Wenn dem Cyber Protection Service mehrere G Suite-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 (S. 168)'.
     - 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) (S. 291)'.

15.19.4.2 Ein Shared Drive und Shared Drive-Dateien wiederherstellen

Ein komplettes Shared Drive wiederherstellen

1. Klicken Sie auf **G Suite**.
2. Wenn dem Cyber Protection Service mehrere G Suite-Organisationen hinzugefügt wurden, wählen Sie diejenige Organisation aus, deren Backup-Daten Sie wiederherstellen wollen. 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' (S. 220) 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 G Suite-Organisationen hinzugefügt wurden, klicken Sie auf **G Suite-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 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 Freigabeberechtigungen der Dateien mit wiederherstellen wollen.
9. Klicken Sie auf **Recovery starten**.
10. Wählen Sie eine dieser Überschreiben-Optionen:
    - **Vorhandene Dateien überschreiben**
    - **Vorhandene Datei überschreiben, wenn diese älter ist**
    - **Vorhandene Dateien nicht überschreiben**
11. Klicken Sie auf **Fertig stellen**, um Ihre Entscheidung zu bestätigen.

Shared Drive-Dateien wiederherstellen

1. Klicken Sie auf **G Suite**.
2. Wenn dem Cyber Protection Service mehrere G Suite-Organisationen hinzugefügt wurden, wählen Sie diejenige Organisation aus, deren Backup-Daten Sie wiederherstellen wollen. 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' (S. 220) 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 **Wiederherstellen** –> **Dateien/Ordner**.
6. Wechseln Sie zum benötigten Ordner oder verwenden Sie die Suchfunktion, um eine Liste der erforderlichen Dateien und Ordner abzurufen.

   Die Suchfunktion ist nicht verfügbar, wenn das Backup verschlüsselt ist.
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 G Suite-Organisationen hinzugefügt wurden, klicken Sie auf **G Suite-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 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:
    - **Vorhandene Dateien überschreiben**
    - **Vorhandene Datei überschreiben, wenn diese älter ist**
    - **Vorhandene Dateien nicht überschreiben**
16. Klicken Sie auf **Fertig stellen**, um Ihre Entscheidung zu bestätigen.

15.19.5 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 G Suite 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 (S. 208) können.

Und so funktioniert es

Der Agent berechnet während eines Backups die Hash-Werte der zu sichernden Dateien, baut einen Hash-Baum auf (basierend auf der Ordnerstruktur), speichert diesen Hash-Baum mit im Backup und sendet dann das Wurzelverzeichnis (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 garantiert.

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.

15.19.5.1 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 (S. 286)' beschrieben auswählen.
   - Wenn Sie die Authentizität einer G Suite Shared Drive-Datei überprüfen wollen, müssen Sie die Datei wie in Schritt 1-7 des Abschnitts 'Shared Drive-Dateien wiederherstellen (S. 289)' 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.

15.20 Oracle Database sichern

Das Backup von Oracle Database wird in einem separaten Dokument erläutert, welches hier verfügbar ist: https://dl.managed-protection.com/u/pdf/OracleBackup_whitepaper.pdf

***Hinweis**: Diese Funktionalität ist in den Standard-Editionen des Cyber Protection Service nicht verfügbar.*

15.21 SAP HANA sichern

Die Sicherung von SAP HANA wird in einem separaten Dokument erläutert, welches hier verfügbar ist: https://dl.managed-protection.com/u/pdf/SAP%20HANA_backup_whitepaper.pdf

***Hinweis**: Diese Funktionalität ist in den Standard-Editionen des Cyber Protection Service nicht verfügbar.*

15.22 Websites und Webhosting-Server schützen

15.22.1 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 (S. 160)'.
- Die Website-Schutzpläne werden nicht auf der Registerkarte **Pläne** –> **Schutz** angezeigt.

15.22.1.1 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 Service-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 **Verbindungsart**, 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 Service-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 (S. 150).
5. [Optional] Aktivieren Sie die Verschlüsselung von Backups (S. 152).
6. [Optional] Klicken Sie auf das Zahnradsymbol, wenn Sie die **Backup-Dateiname** (S. 160) 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.

15.22.1.2 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' (S. 220) 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 Freigabeberechtigungen 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. Wenn Sie dies nicht wollen, 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. Wenn Sie dies nicht wollen, 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 Freigabeberechtigungen der wiederhergestellten Elemente mit wiederherstellen wollen.
6. Klicken Sie auf **Recovery starten** und bestätigen Sie dann die Aktion.

15.22.2 Webhosting-Server sichern

Webhosting-Administratoren, die die Plattformen Plesk oder cPanel verwenden, können diese Plattformen in den Cyber Protection Service integrieren.

Nach der Integration kann ein Administrator Folgendes tun:

- Einen kompletten Plesk- oder cPanel-Server per Laufwerk-Backup zum Cloud Storage sichern
- Den kompletten Server (inkl. aller Websites) wiederherstellen
- Für Plesk: granulare Wiederherstellungen von Websites, einzelnen Dateien, Postfächern oder Datenbanken durchführen
- Für cPanel: granulare Wiederherstellungen von Websites, einzelnen Dateien, Postfächern, E-Mail-Filtern, E-Mail-Weiterleitungen, Datenbanken und Konten durchführen
- Self-Service-Recovery für Plesk- und cPanel-Kunden aktivieren

Die Integration erfolgt über die Cyber Protection Service-Erweiterung. Wenn Sie die Erweiterung für Plesk oder cPanel benötigen, wenden Sie sich an den Anbieter des Cyber Protection Service.

Unterstützte Plesk- und cPanel-Versionen

- Plesk für Linux 17.0 und höher

- Jede cPanel-Version mit PHP 5.6 und höher

Quotas

Jeder per Backup gesicherte Plesk- oder cPanel-Server wird auf die Quota **Webhosting-Server** angerechnet. Wenn diese Quota deaktiviert ist oder die Überschreitungsgrenze für diese Quota erreicht ist, passiert Folgendes:

- 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.

15.23 Spezielle Aktionen mit virtuellen Maschinen

15.23.1 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 Recovery' 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, eine solche temporäre virtuelle Maschine für einen Zeitraum von bis zu drei Tagen auszuführen. 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

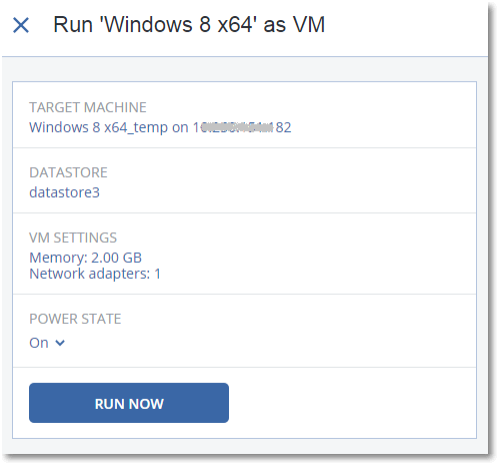
werden, welches im Cloud Storage gespeichert ist. Dies ist jedoch langsamer, weil für diese Aktion intensive wahlfreie Lesezugriffe auf das Backup notwendig sind.

- 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.

15.23.1.1 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' (S. 220).
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 (S. 298) 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.

15.23.1.2 Eine Maschine löschen

Wir raten davon ab, eine temporäre virtuelle Maschine direkt in vSphere/Hyper-V zu löschen. 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.

15.23.1.3 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.

15.23.2 Mit VMware vSphere arbeiten

Dieser Abschnitt beschreibt Aktionen, die spezifisch für VMware vSphere-Umgebungen sind.

15.23.2.1 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)' (S. 303) 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** (S. 301)

  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** (S. 301)

  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.

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 Replikationsfrequenz 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 (S. 303) 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 ein Failover von einer Maschine auf ein Replikat durch

1. Wählen Sie ein Replikat aus, auf welches das Failover erfolgen soll.
2. Klicken Sie auf **Replikat-Aktionen**.

3. Klicken Sie auf **Failover**.
4. Bestimmen Sie, ob das eingeschaltete Replikat mit einem 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** (S. 302)

  Stoppen Sie das Failover, wenn die ursprüngliche Maschine repariert wurde. Das Replikat wird ausgeschaltet. Die Replikation wird fortgesetzt.
- **Permanentes Failover auf das Replikat durchführen** (S. 302)

  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** (S. 302)

  Führen Sie ein Failback aus, falls Sie ein 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.

Ein Failover stoppen

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.

Ein permanentes Failover durchführen

So führen Sie ein permanentes Failover durch

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 ein 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 das 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 (S. 303) 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) (S. 165)'.

Laufwerk-Provisioning

Diese Option definiert die Laufwerk-Provisioning-Einstellungen 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 (S. 167)'.

Vor-/Nach-Befehle

Diese Option entspricht im Wesentlichen der Backup-Option 'Vor-/Nach-Befehle (S. 184)'.

VSS (Volume Shadow Copy Service) für virtuelle Maschinen

Diese Option entspricht im Wesentlichen der Backup-Option 'VSS (Volume Shadow Copy Service) für virtuelle Maschinen (S. 191)'.

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 (S. 215)'.

Performance

Diese Option entspricht im Wesentlichen der Recovery-Option 'Performance (S. 217)'.

Vor-/Nach-Befehle

Diese Option entspricht im Wesentlichen der Recovery-Option 'Vor-/Nach-Befehle (S. 217)'.

VM-Energieverwaltung

Diese Option entspricht im Wesentlichen der Recovery-Option 'VM-Energieverwaltung (S. 219)'.

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 (S. 300).

   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.

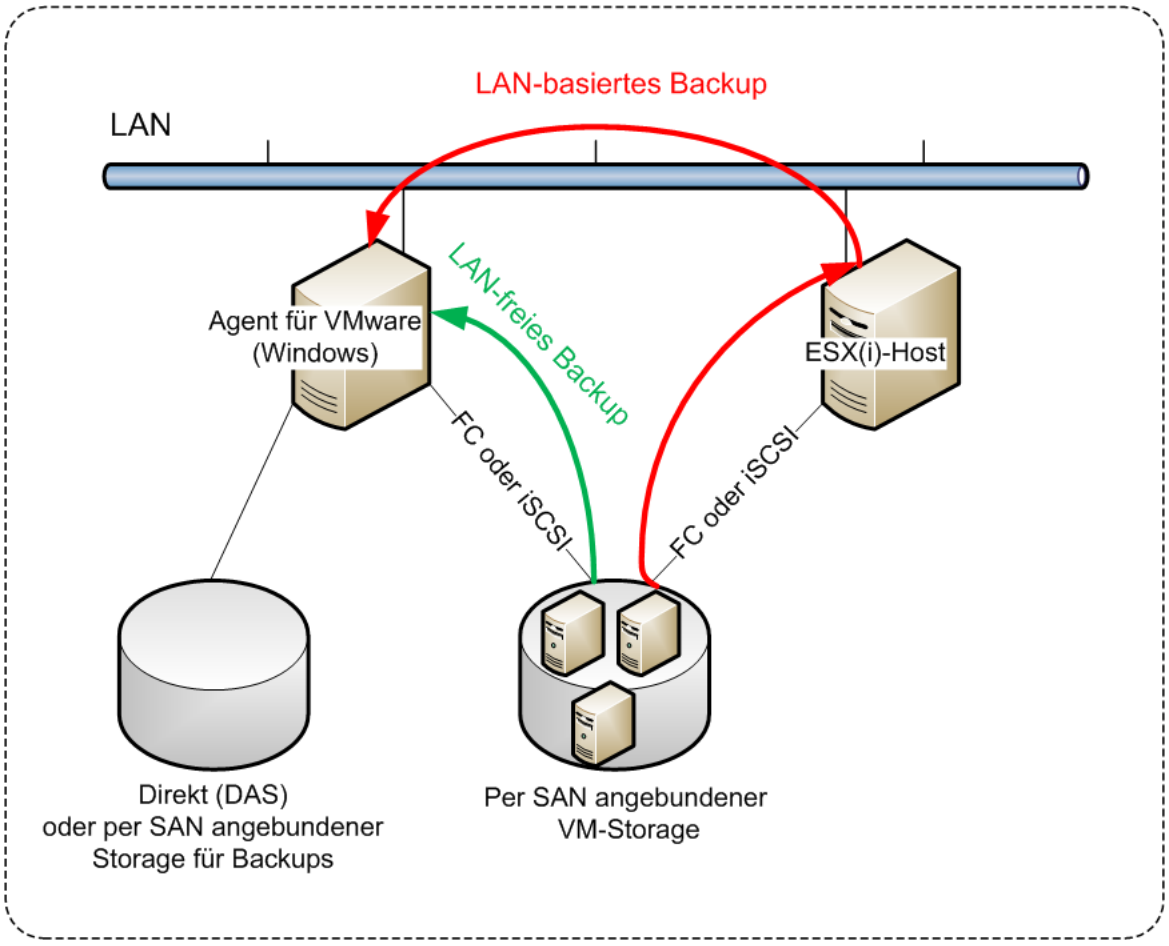
7. Bearbeiten Sie den Replikationsplan, den Sie in Schritt 2 erstellt haben. Wählen Sie bei **Zielmaschine** die Option **Vorhandenes Replikat** und wählen Sie dann das importierte Replikat aus.

Die Software wird daraufhin die Aktualisierung des Replikats fortsetzen. Alle Replikationen werden inkrementell sein.

15.23.2.2 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 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 den Befehl **`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**.

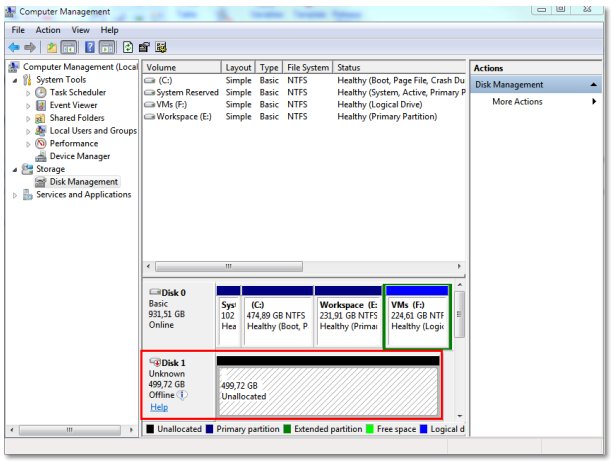
   Tipp: *Wenn Sie das Systemsteuerungsmodul **Verwaltung** nicht finden können, müssen Sie evtl. die Ansicht der **Systemsteuerung** von **Start** oder **Kategorie** auf eine andere Ansicht umstellen – oder die Suchfunktion verwenden.*

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.



15.23.2.3 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 (S. 308), 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 (S. 71) 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 (S. 121) unter **Backup-Ziel** die Option **Lokale Ordner** – Sie dann den mit dem lokal angeschlossenen Storage korrespondierenden Laufwerksbuchstaben an, beispielsweise **D:**.

15.23.2.4 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

Zu einer Neuverteilung kommt es immer dann, wenn eine etablierte Balance zusammenbricht – oder, wenn das Ungleichgewicht bei der Auslastung der Agenten 20 Prozent übersteigt. 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. Die Neuverteilung startet nur, wenn Sie einen solchen Agenten von der 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 wird

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.

15.23.2.5 Unterstützung für VM-Migration

In diesem Abschnitt erfahren Sie, was Sie bei der Migration virtueller Maschinen innerhalb einer vSphere-Umgebung zu beachten haben – einschließlich der Migration zwischen ESXi-Hosts, die Teil eines vSphere-Clusters sind.

vMotion

vMotion verschiebt Status und Konfiguration einer virtuellen Maschine zu einem anderen Host, während die Laufwerke der Maschine am selben Speicherort des freigegebenen Storages verbleiben.

- vMotion für den Agenten für VMware (Virtuelle Appliance) wird nicht unterstützt und ist deaktiviert.
- vMotion für eine virtuelle Maschine ist während eines Backups deaktiviert. Backups werden weiter ausgeführt, nachdem die Migration abgeschlossen wurde.

Storage vMotion

Storage vMotion verschiebt die Laufwerke von virtuellen Maschinen von einem Datenspeicher zu einem anderen.

- Storage vMotion für den Agenten für VMware (Virtuelle Appliance) wird nicht unterstützt und ist deaktiviert.
- Storage vMotion für eine virtuelle Maschine ist während eines Backups deaktiviert. Backups werden nach der Migration weiter ausgeführt.

15.23.2.6 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.

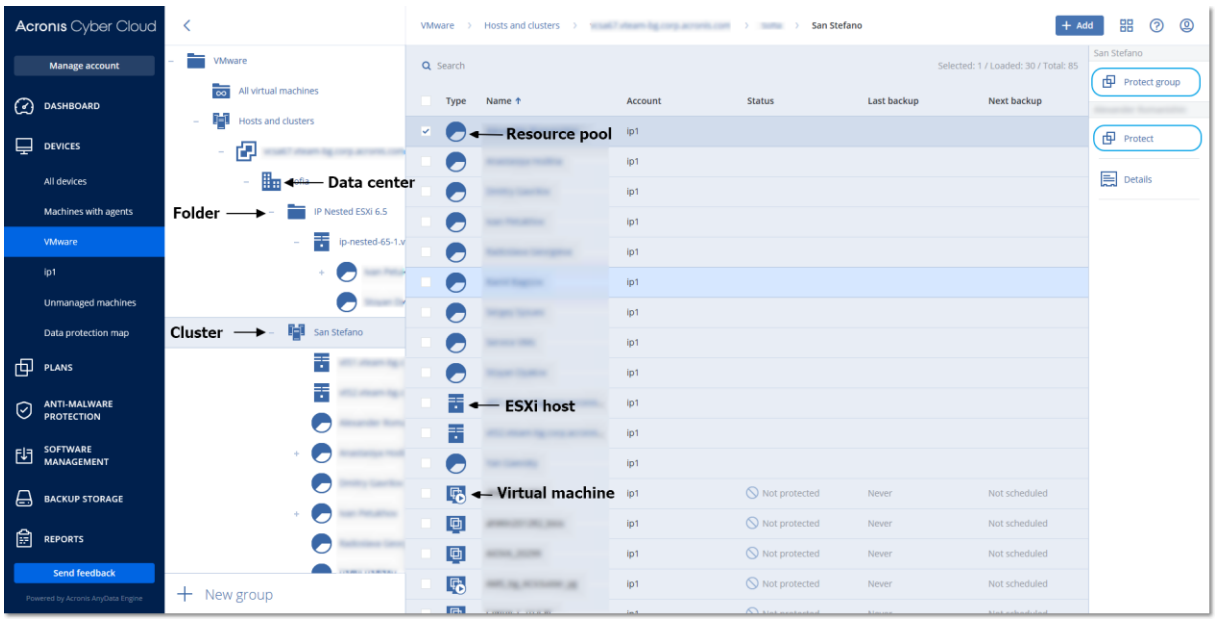
Sie können in der Registerkarte **VMware** die folgenden vSphere-Infrastrukturobjekte per Backup sichern:

- 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 'San 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 'San 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**.

15.23.2.7 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 (S. 312)' beschriebenen Berechtigungen noch über folgende Berechtigungen verfügen:

- **Global** –> **Benutzerdefinierte Attribute verwalten**
- **Global** –> **Benutzerdefinierte Attribute festlegen**

15.23.2.8 Agent für VMware – notwendige Berechtigungen

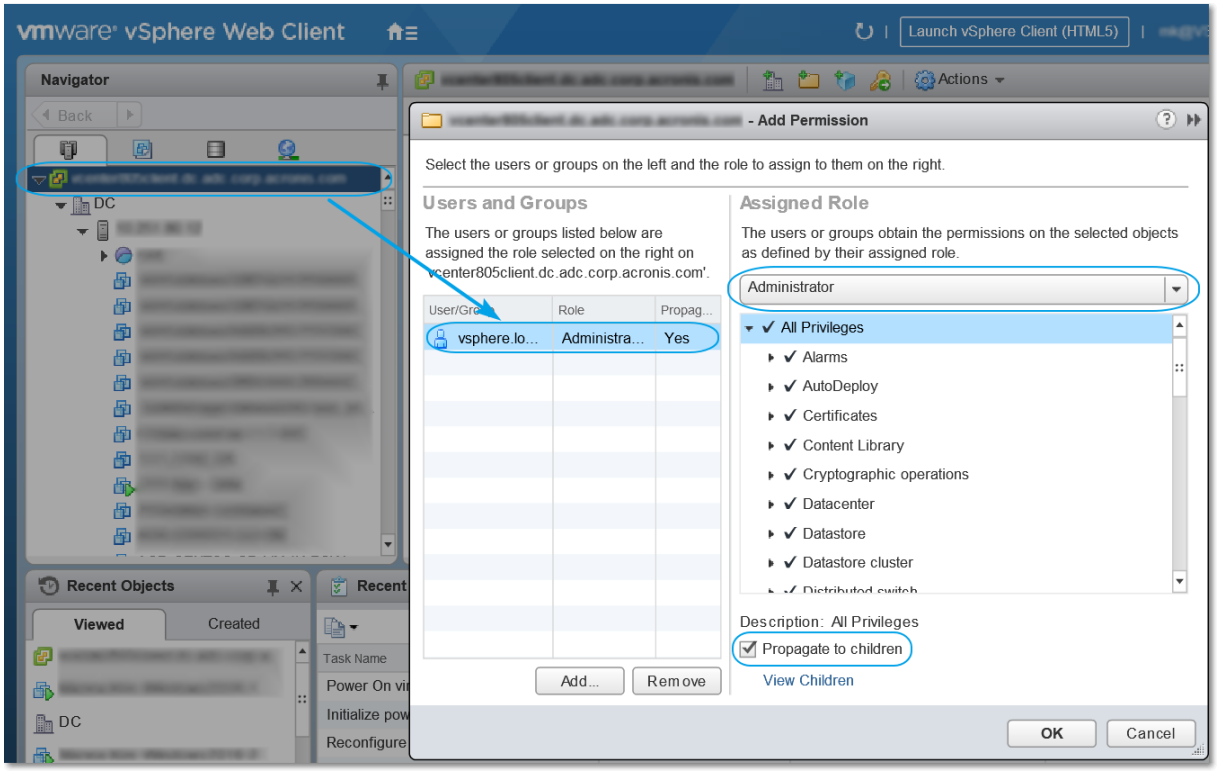
Um Aktionen mit vCenter-Objekten (wie z.B. virtuelle Maschinen, ESXi-Hosts, Cluster, vCenter und mehr) durchführen zu können, muss sich der Agent für VMware auf dem vCenter- oder ESXi-Host mithilfe der von einem Benutzer bereitgestellten vSphere-Anmeldedaten authentifizieren. Das vSphere-Konto, welches 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. 310)'.

Gehen Sie folgendermaßen vor, um einem vSphere-Benutzer auf der vCenter-Ebene die Berechtigungen zuzuweisen:

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**.



		Aktion			
Objekt	**Recht**	**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	+	+	+	

		Aktion			
Objekt	**Recht**	**Backup einer VM**	**Recovery zu einer neuen VM**	**Recovery zu einer existierenden VM**	**VM von Backup ausführen**
	Benutzerdefinierte Attribute festlegen	+	+	+	
Host –> Konfiguration	**Konfiguration für 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	+**			

		Aktion			
Objekt	**Recht**	**Backup einer VM**	**Recovery zu einer neuen VM**	**Recovery zu einer existierenden VM**	**VM von Backup ausführen**
Virtuelle Maschine –> Interaktion	**Ticket zur Steuerung durch Gast abrufen** (in vSphere 4.1 und 5.0)				+
	CD-Medien konfigurieren		+	+	
	Gastbetriebssystem-Verwaltung über VIX API (in vSphere 5.1 und höher)				+
	Ausschalten			+	+
	Einschalten		+	+	+
Virtuelle Maschine –> Bestandsliste	**Aus vorhandener erstellen**		+	+	+
	Neu erstellen		+	+	+
	Registrieren				+
	Entfernen		+	+	+
	Registrierung aufheben				+
Virtuelle Maschine –> Provisioning	**Laufwerkszugriff zulassen**		+	+	+
	Lesezugriff auf Festplatte zulassen	+		+	
	Download virtueller Maschine zulassen	+	+	+	+
Virtuelle Maschine –> Status	**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.

15.23.3 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.

15.23.4 Die Gesamtzahl der gleichzeitig gesicherten virtuellen Maschinen begrenzen

Die Backup-Option **Planung** (S. 188) bestimmt, wie viele virtuelle Maschinen ein Agent gleichzeitig sichern kann, wenn er den gegebenen Schutzplan ausführt.

Wenn sich mehrere Schutzpläne zeitlich überschneiden, werden die Zahlen, die in deren Backup-Optionen spezifiziert wurden, addiert. Auch wenn die resultierende Gesamtzahl vom Programm auf 10 begrenzt ist, können überlappende Pläne die Backup-Performance beeinträchtigen und sowohl den Host als auch den Storage für die virtuellen Maschinen überlasten.

Sie können die Gesamtzahl der virtuellen Maschinen, die ein Agent für VMware oder Agent für Hyper-V gleichzeitig sichern kann, noch weiter reduzieren.

So können Sie die Gesamtzahl der virtuellen Maschinen begrenzen, die ein Agent für VMware (Windows) oder Agent für Hyper-V gleichzeitig sichern kann

1. Erstellen Sie auf der Maschine, die den Agenten ausführt, 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\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 '**proxy.reg**'.
5. Führen Sie die Datei 'als Administrator' aus.
6. Bestätigen Sie, dass Sie die Änderung der Windows Registry wirklich ausführen wollen.
7. Gehen Sie dann folgendermaßen vor, um den Agenten neu zu starten:
   a. Klicken Sie im **Start**-Menü auf **Ausführen** und geben Sie ein: **cmd**

b. Klicken Sie auf **OK**.

c. Führen Sie folgende Befehle aus:

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

So können Sie die Gesamtzahl der virtuellen Maschinen begrenzen, die der Agent für VMware (Virtuelle Appliance) sichern kann

1. Drücken Sie zum Starten der Eingabeaufforderung die Tastenkombination Strg+Umschalt+F2, während Sie sich in der Benutzeroberfläche der virtuellen Appliance befinden.
2. Öffnen Sie die Datei **/etc/Acronis/MMS.config** in einem Text-Editor (wie **vi**).
3. Suchen Sie den folgenden Abschnitt:

```
<key name="SimultaneousBackupsLimits">
    <value name="MaxNumberOfSimultaneousBackups" type="Tdword">"10"</value>
</key>
```

4. Ersetzen Sie `10` mit dem Dezimalwert der Begrenzung, die Sie festlegen wollen.
5. Speichern Sie die Datei.
6. Führen Sie den Befehl **`reboot`** aus, um den Agenten neu zu starten.

15.23.5 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	Virtuelle Virtuozzo-Maschine	Virtuozzo-Container
Physische Maschine	+	+	+	-	-
Virtuelle VMware ESXi-Maschine	+	+	+	-	-
Virtuelle Hyper-V-Maschine	+	+	+	-	-
Virtuelle Virtuozzo-Maschine	+	+	+	+	-
Virtuozzo-Container	-	-	-	-	+

Anleitungen zur Durchführung von Migrationen finden Sie in folgenden Abschnitten:

- Physisch-zu-virtuell (P2V) – 'Physische Maschinen als virtuelle Maschinen wiederherstellen'
- Virtuell-zu-virtuell (V2V) – 'Virtuelle Maschine (S. 200)'
- Virtuell-zu-physisch (V2P) – 'Virtuelle Maschine (S. 200)' oder 'Laufwerke mithilfe eines Boot-Mediums wiederherstellen (S. 201)'

Obwohl es möglich ist, V2P-Migrationen von der Weboberfläche aus durchzuführen, empfehlen wir für bestimmte Fälle die Verwendung eines Boot-Mediums. Sie können das Boot-Medium auch für eine Migration zu ESXi oder Hyper-V verwenden.

Mit dem Boot-Medium können Sie Folgendes tun:

- P2V-, V2P- oder V2P-Migrationen (von Virtuozzo) von einer Linux-Maschine durchführen, die logischen Volumes (LVMs) enthält. Den Agenten für Linux oder Boot-Medien verwenden, um Backups und Boot-Medien für Wiederherstellungen zu erstellen.
- Treiber für bestimmte Hardware bereitstellen, die für die Bootfähigkeit des Systems notwendig sind.

15.23.6 Virtuelle Windows Azure- und Amazon EC2-Maschinen

Um eine virtuelle Windows 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 Windows Azure- und Amazon EC2-Maschinen nicht mit einem Boot-Medium gebootet werden können. Wenn Sie bei einer Wiederherstellung eine neue virtuelle Windows Azure- und Amazon EC2-Maschine als Ziel verwenden wollen, gehen Sie wie nachfolgend beschrieben vor.

So können Sie eine Maschine als virtuelle Windows Azure- oder Amazon EC2-Maschine wiederherstellen

1. Erstellen Sie in Windows 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 (S. 197)' wieder her. Wählen Sie die neue Maschine als Zielmaschine aus, wenn Sie die Wiederherstellung konfigurieren.

16 Disaster Recovery

***Hinweis**: Diese Funktionalität ist nur in den Disaster Recovery Editionen des Cyber Protection Service verfügbar.*

17 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 und sich hauptsächlich an kleine und mittlere Unternehmen (KMUs) richtet. 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).

Die Kernfunktionalität

- Verwalten Sie den Cyber Disaster Recovery Cloud Service über eine einzelne, zentrale Konsole
- Erweitern Sie bis zu fünf lokale Netzwerke über einen sicheren VPN-Tunnel in die Cloud
- Bauen Sie eine Verbindung zur Cloud-Site auf, ohne dass eine VPN-Appliance-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

18 Software-Anforderungen

Unterstützte Betriebssysteme

Der Schutz mit einem Recovery-Server wurde mit folgenden Betriebssystemen getestet:

- CentOS 6.6, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6
- Debian 9
- Ubuntu 16.04, 18.04
- Windows Server 2008/2008 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-Desktop-Betriebssysteme werden aufgrund von Microsoft-Produktbedingungen nicht unterstützt.

Eine korrekte Funktion der Software mit anderen Windows-Betriebssystemen und Linux-Distributionen ist möglich, wird jedoch nicht garantiert.

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
- Windows Server 2008 R2 mit Hyper-V
- Windows Server 2012/2012 R2 mit Hyper-V
- Windows Server 2016 mit Hyper-V – alle Installationsoptionen, mit Ausname des Nano Servers
- Windows Server 2019 mit Hyper-V – alle Installationsoptionen, mit Ausname des Nano Servers
- Microsoft Hyper-V Server 2012/2012 R2
- Microsoft Hyper-V Server 2016
- Kernel-based Virtual Machines (KVM)
- 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 Ausname des Nano Servers
- Windows Server 2019 mit Hyper-V – alle Installationsoptionen, mit Ausname 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
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:
   - Linux-Maschinen mit logischen Volumes (LVM) oder Volumes, die mit dem XFS-Dateisystem formatiert sind
   - Dateisysteme ohne Partitionstabelle
3. Nicht unterstützte Backup-Typen:
   - Recovery-Punkte aus einer kontinuierlichen Datensicherung (CDP) (S. 130) 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 (S. 171) 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.

19 Die Disaster Recovery-Funktionalität einrichten

So können Sie die Disaster Recovery-Funktionalität einrichten

1. Konfigurieren Sie den Verbindungstyp mit der Cloud-Site:
   - Point-to-Site-Verbindung (S. 331)
   - Site-to-Site-Verbindung (S. 333)
   - 'Nur Cloud'-Modus (S. 335)
2. Erstellen Sie einen Schutzplan (S. 105) 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 (S. 344) für jeden Ihrer lokalen Server, den Sie schützen wollen.
5. Führen Sie einen Test-Failover aus (S. 346), um zu überprüfen, wie dieser funktioniert.
6. [Optional] Erstellen Sie die primären Server (S. 352) 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 (S. 347) 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 (S. 349).

20 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.

20.1.1 Netzwerkkonzepte

Cyber Disaster Recovery Cloud ermöglicht Ihnen, den Verbindungstyp zur Cloud-Site zu definieren:

- **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.

- **Site-to-Site-Verbindung**

  Diese Verbindungstyp erfordert eine Bereitstellung der VPN-Appliance am lokalen Standort.

  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.

- **'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.

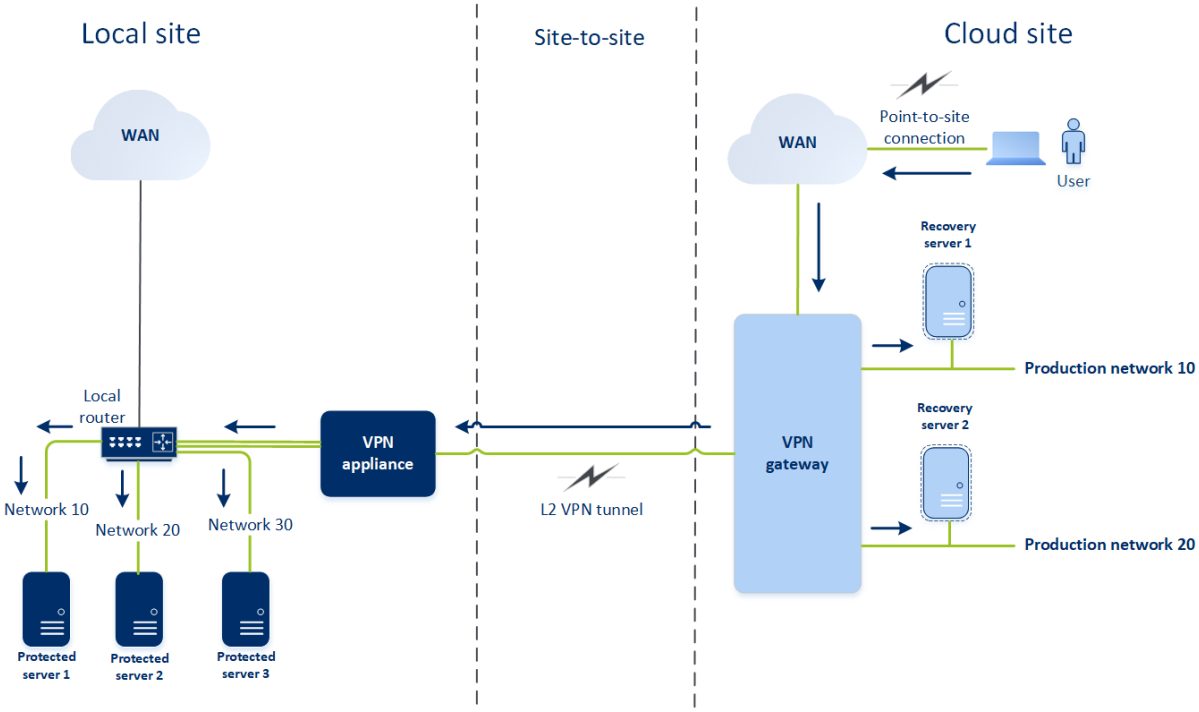
20.1.1.1 Point-to-Site-VPN-Remote-Zugriff

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. Dieser Verbindungstyp kann für folgende Szenarien verwendet werden:

- In vielen Unternehmen sind die Unternehmensdienste und Webressourcen nur über das Unternehmensnetzwerk verfügbar. Eine Point-to-Site-Verbindung ermöglicht Ihnen, sich sicher mit dem entsprechenden 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 eine 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:

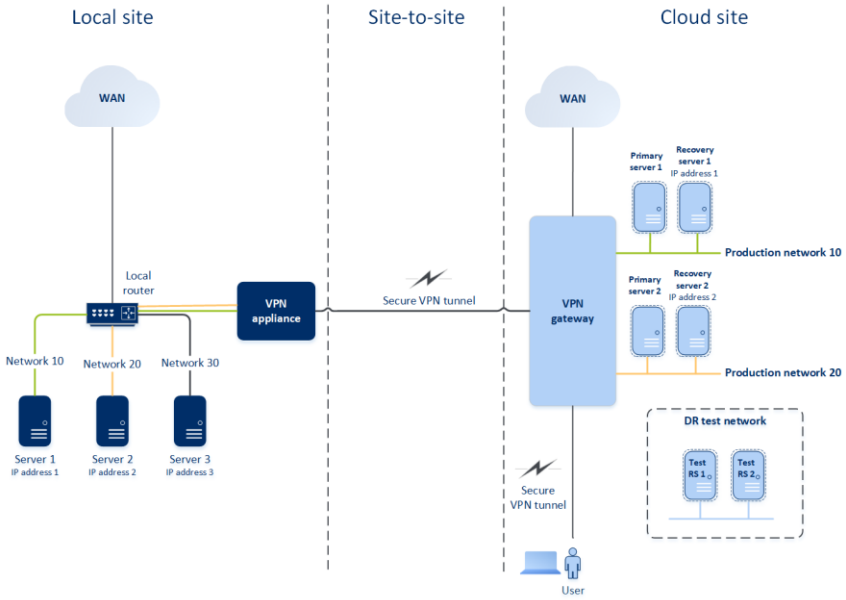
- Die Benutzer sollten Ihre Cyber Cloud-Anmeldedaten verwenden, um sich im VPN-Client zu authentifizieren. Sie müssen entweder die Rolle 'Firmenadministrator' oder 'Cyber Protection' haben.
- Wenn Sie die OpenVPN-Konfiguration neu generieren (S. 340), müssen Sie die aktualisierte Konfiguration allen Benutzern zur Verfügung stellen, die die Point-to-Site-Verbindung zur Cloud-Site verwenden.

20.1.1.2 Site-to-Site-Verbindung

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. Mit Cyber Disaster Recovery Cloud können maximal fünf Netzwerke geschützt werden.



Um eine Site-to-Site-Kommunikation zwischen dem lokalen Standort und der Cloud-Site aufzubauen, werden die **VPN-Appliance** und das **VPN-Gateway** verwendet. Wenn Sie als Erstes mit der Konfiguration der Site-to-Site-Verbindung in der Service-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 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.

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 der 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 stellt folgende Funktionen bereit:

- 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 Kommunikationen zwischen dem lokalen Standort und der Cloud-Site.

Recovery-Server

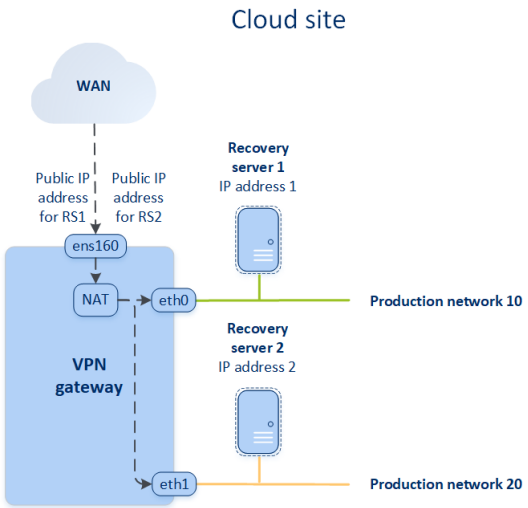
Ein **Recovery-Server** – ist das VM-Replikat einer ursprünglichen Maschine, das auf den (in der Cloud gespeicherten) Backups eines geschützten Servers basiert. Recovery-Server werden verwendet, um bei einem Desaster die Workloads der ursprünglichen Server in die Cloud umschalten zu können.

Wenn Sie einen Recovery-Server erstellen, müssen Sie folgende Netzwerkparameter spezifizieren:

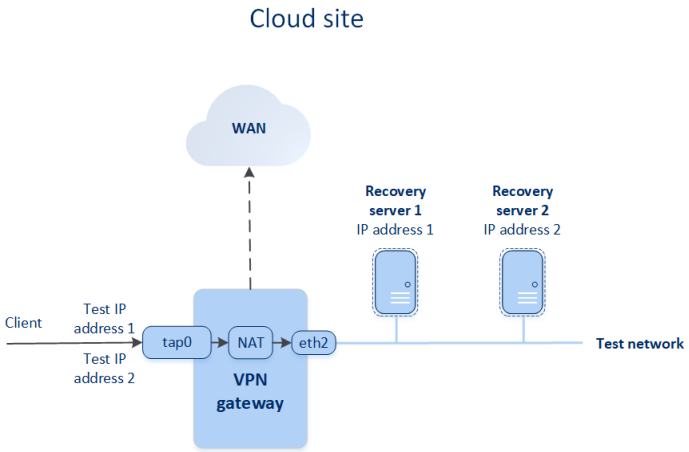
- **Cloud-Netzwerk** (erforderlich): das Cloud-Netzwerk, mit dem der Recovery-Server verbunden wird.
- **IP-Adresse im Produktionsnetzwerk** (erforderlich): die IP-Adresse, mit der die virtuelle Maschine des Recovery-Servers gestartet wird. Diese Adresse wird in den Produktions- und Testnetzwerken verwendet. Die virtuelle Maschine wird vor dem Starten so konfiguriert, dass sie ihre IP-Adresse per DHCP erhält.
- **Test-IP-Adresse** (optional): diese IP-Adresse wird benötigt, um beim Test-Failover vom Client-Produktionsnetzwerk aus auf den Recovery-Server zuzugreifen. 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): die IP-Adresse, die verwendet wird, um aus dem Internet auf den Recovery-Server zuzugreifen. 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 über diese IP-Adresse im Testnetzwerk 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.



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 (per 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 der dazugehörigen 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, 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): die IP-Adresse, die verwendet wird, um aus dem Internet auf den primären Server zuzugreifen. Wenn ein Server keine öffentliche IP-Adresse hat, ist er nur aus dem lokalen Netzwerk und nicht dem Internet erreichbar.

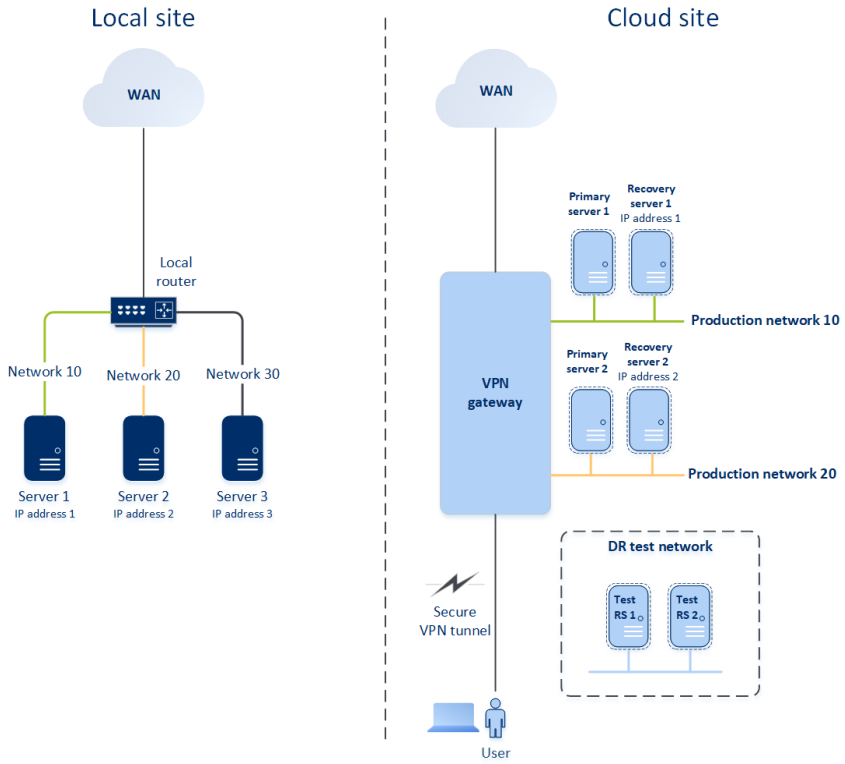
- **Internetzugriff** (optional): diese Option ermöglicht es einem primären Server, auf das Internet zuzugreifen.

20.1.1.3 '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.

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.



20.1.1.4 Automatisches Löschen einer ungenutzten Kundenumgebung auf einer Cloud-Site

Der Disaster Recovery Service überwacht die Nutzung einer Kundenumgebung, die für Disaster Recovery-Zwecke erstellt wurde, und löscht diese automatisch, wenn sie nicht verwendet wird.

Folgende Kriterien werden verwendet, um zu definieren, dass 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-VPN-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 daher folgende Aktionen aus:

- Das VPN-Gateway wird gelöscht und alle Cloud-Ressourcen, die zu dem entsprechenden Mandanten gehören, werden ebenfalls gelöscht.
- Die Registrierung der VPN-Appliance wird aufgehoben

Solche Mandants werden auf das Stadium zurückversetzt, in dem noch keine Verbindungsart konfiguriert war.

20.1.2 Grundsätzliche Verbindungskonfiguration

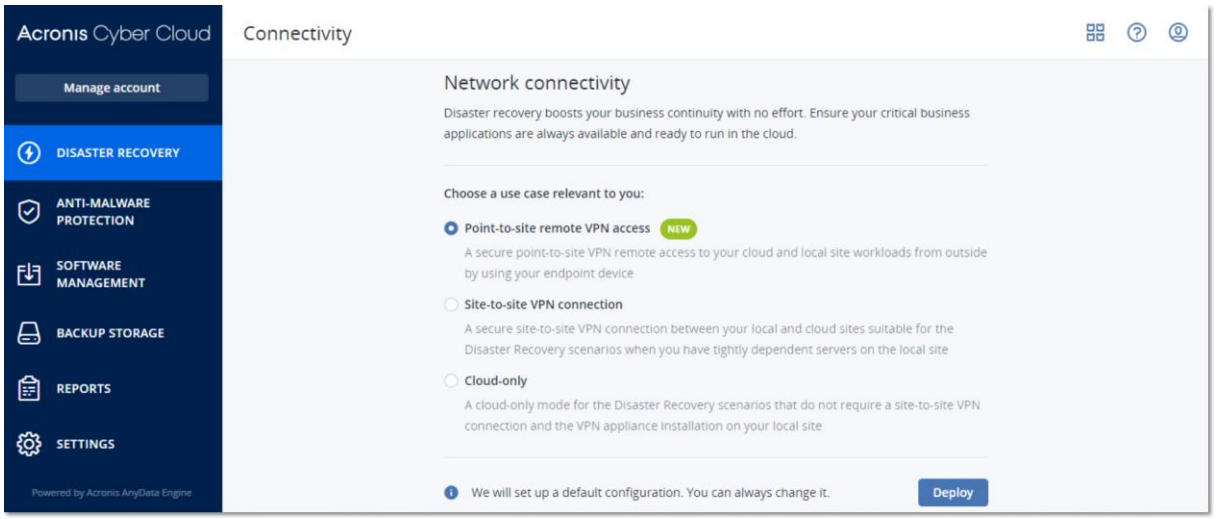
In diesem Abschnitt werden verschiedene Szenarien für die Verbindungskonfiguration beschrieben.

20.1.2.1 Point-to-Site-VPN-Remote-Zugriff

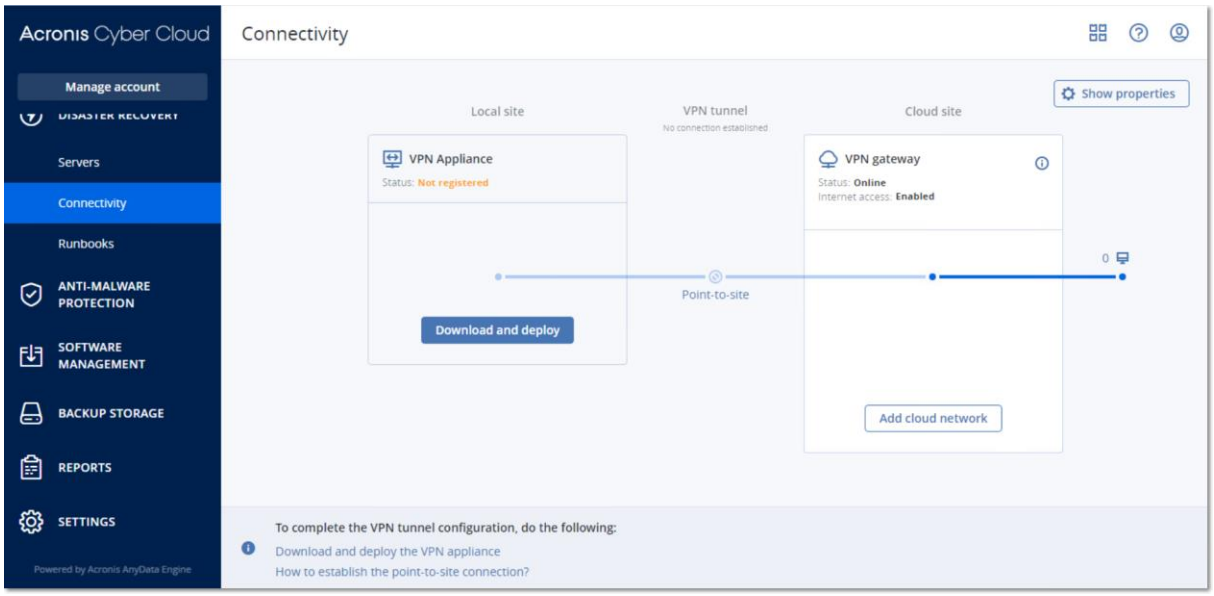
Wenn Sie eine Remote-Verbindung zu Ihrem lokalen Standort aufbauen müssen, können Sie die Point-to-Site-Verbindung zum lokalen Standort verwenden. Sie können die nachfolgende Prozedur befolgen oder sich das Video-Tutorial ansehen.

So können Sie eine Point-to-Site-Verbindung zum lokalen Standort konfigurieren

1. Gehen Sie in der Service-Konsole zu **Disaster Recovery** –> **Verbindung**.
2. Wählen Sie den Anwendungsfall **Point-to-Site-Remote-VPN-Zugriff** aus und klicken Sie dann auf **Bereitstellen**. Das System wird automatisch die Site-to-Site-Verbindung zwischen dem lokalen Standort und der Cloud-Site aktivieren und den Point-to-Site-Zugriff zum lokalen Standort ermöglichen.



3. Sie können die VPN-Appliance bereitstellen, indem Sie im VPN-Appliance-Block auf den Befehl **Herunterladen und bereitstellen** klicken.



4. Stellen Sie sicher, dass Ihr Benutzer, der die Point-to-Site-Verbindung zum lokalen Standort aufbauen muss, ein Benutzerkonto in Cyber Cloud hat. Diese Anmeldedaten werden für die Authentifizierung im VPN-Client verwendet. Ansonsten müssen Sie ein Benutzerkonto in Cyber Cloud erstellen. Stellen Sie sicher, dass ein Benutzer die Rolle 'Firmenadministrator' oder 'Cyber Protection' hat.
5. Den OpenVPN-Client konfigurieren:
    1. Sie können den OpenVPN-Client von dieser Adresse herunterladen: https://openvpn.net/community-downloads/ https://openvpn.net/community-downloads/. Folgende OpenVPN-Client-Versionen werden unterstützt: 2.4.0 und höher.
    2. Installieren Sie den OpenVPN-Client auf derjenigen Maschine, von der aus Sie sich mit dem lokalen Standort verbinden wollen.
    3. Klicken Sie auf **Konfiguration für OpenVPN herunterladen**. Die Konfigurationsdatei ist auf Benutzer in Ihrer Organisation anwendbar, die die Benutzerrolle 'Firmenadministrator' oder 'Cyber Protection' haben.
    4. Importieren Sie die heruntergeladene Konfiguration in die OpenVPN-Einstellungen.
    5. Melden Sie sich mithilfe der Benutzeranmeldedaten von Cyber Cloud (siehe Schritt 4 weiter oben) am OpenVPN-Client an.
    6. [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 Cloud anmelden, um die Zwei-Faktor-Authentifizierung für ihre Konten einzurichten.*

Anschließend kann sich Ihr Benutzer mit Maschinen am lokalen Standort verbinden.

20.1.2.2 Site-to-Site-Verbindung

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 (S. 339)

Stellen Sie sicher, dass Ihre Firewalls und anderen Komponenten des Netzwerk-Sicherheitssystems Verbindungen zu allen IP-Adressen über diese Ports zulassen.

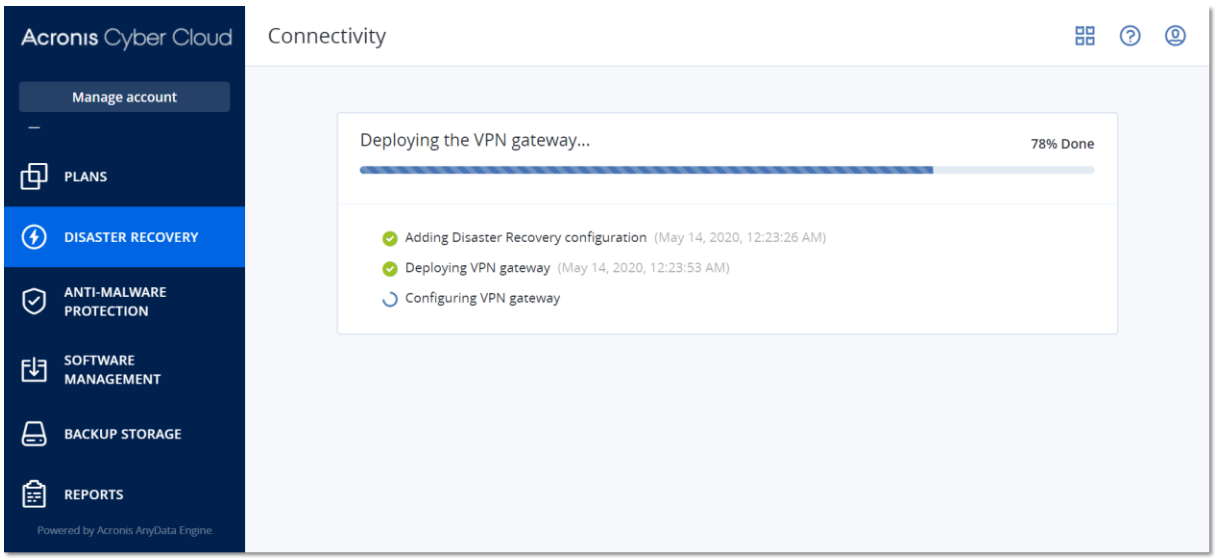
Site-to-Site-Verbindung konfigurieren

Die VPN-Appliance erweitert Ihr lokales Netzwerk (LAN) über einen sicheren VPN-Tunnel in die Cloud. Eine solche Verbindung wird oft auch als S2S-Verbindung (Site-to-Site) bezeichnet. Sie können die nachfolgende Prozedur befolgen oder sich das Video-Tutorial ansehen.

So können Sie eine Verbindung über die VPN-Appliance einrichten

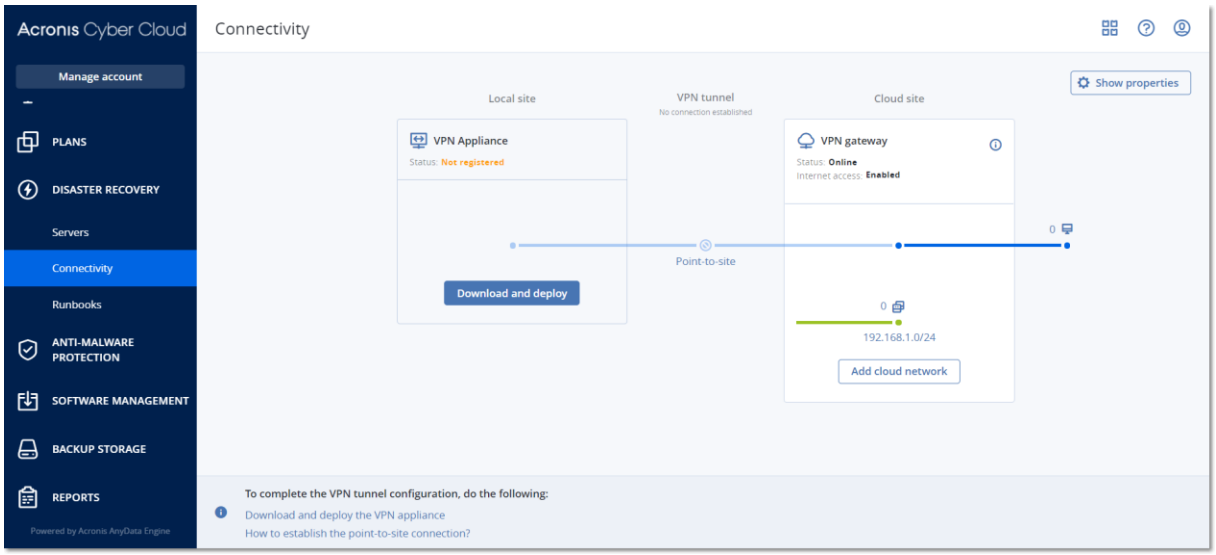
1. Gehen Sie in der Service-Konsole zu **Disaster Recovery** –> **Verbindung**.
2. Wählen Sie **Site-to-Site-VPN-Verbindung** aus und klicken Sie dann auf **Bereitstellen**.

   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**.

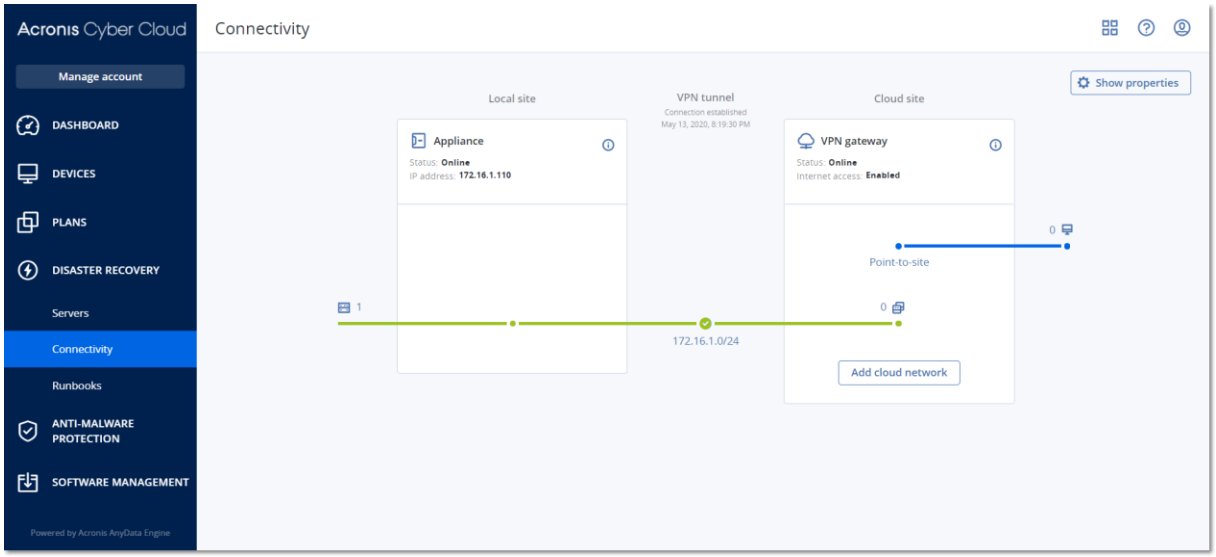
   Erstellen Sie in Hyper-V eine virtuelle Maschine der **Generation 1** mit 1,024 MB Arbeitsspeicher. Wir empfehlen außerdem, dass Sie für diese Maschine die Option **Dynamischer Arbeitsspeicher** aktivieren. Gehen Sie, sobald die Maschine erstellt wurde, zu **Einstellungen** –> **Hardware** –> **Netzwerkkarte** –> **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 Service-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

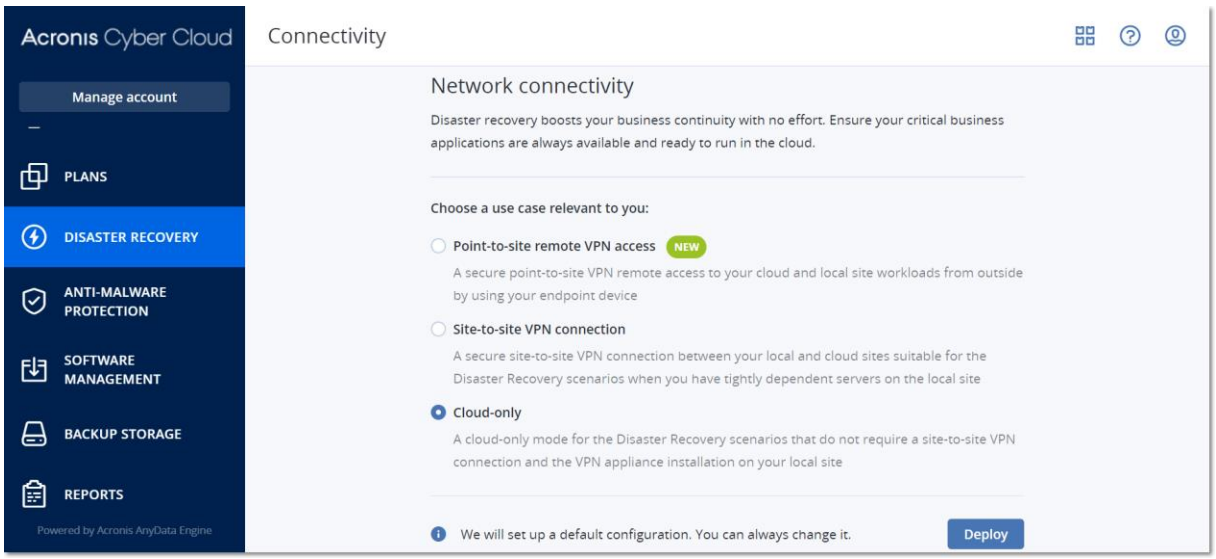
allen aktiven Schnittstellen an den Cyber Disaster Recovery Cloud Service zu melden. Die Service-Konsole zeigt die Schnittstellen basierend auf den Informationen der VPN-Appliance an.



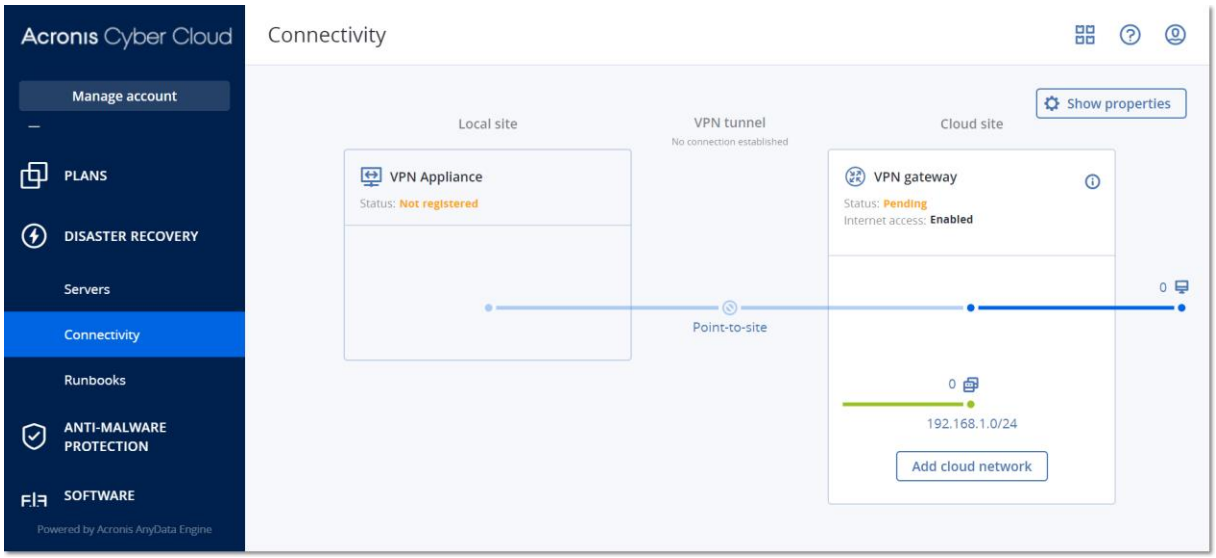
20.1.2.3 'Nur Cloud'-Modus

So können Sie eine Verbindung im 'Nur Cloud'-Modus einrichten

1. Gehen Sie in der Service-Konsole zu **Disaster Recovery** –> **Verbindung**.
2. Wählen Sie die Option **Nur Cloud** aus und klicken Sie dann auf den Befehl **Bereitstellen**.



3. Anschließend 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 (S. 336)'.

20.1.3 Netzwerkverwaltung

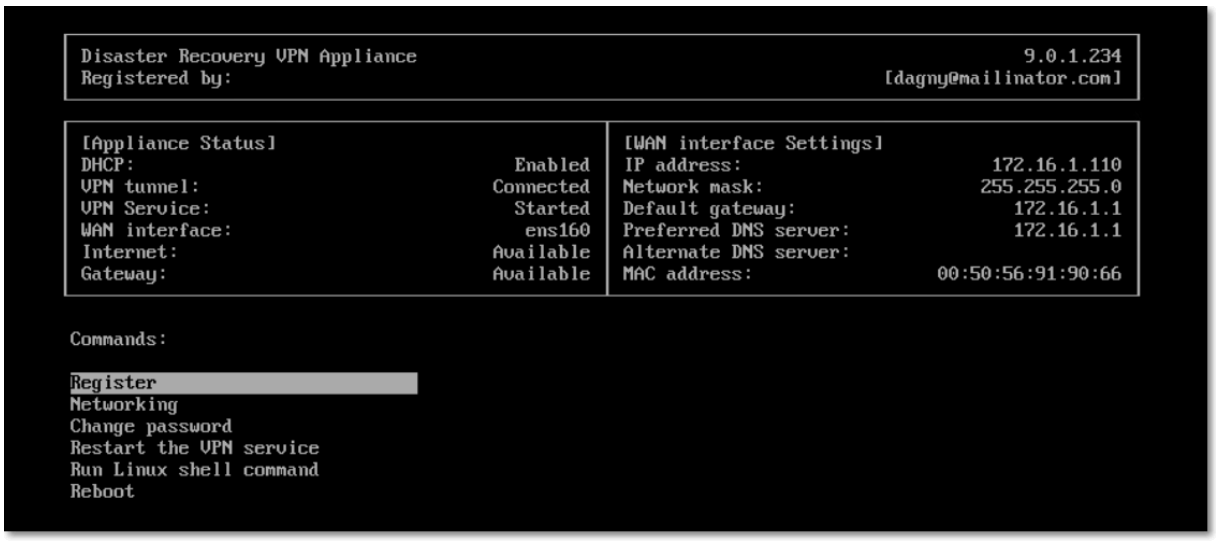
In diesem Abschnitt werden verschiedene Szenarien für die Netzwerkverwaltung beschrieben.

20.1.3.1 Netzwerke verwalten

Site-to-Site-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 Service-Konsole zeigt die Schnittstellen basierend auf den Informationen der VPN-Appliance an.

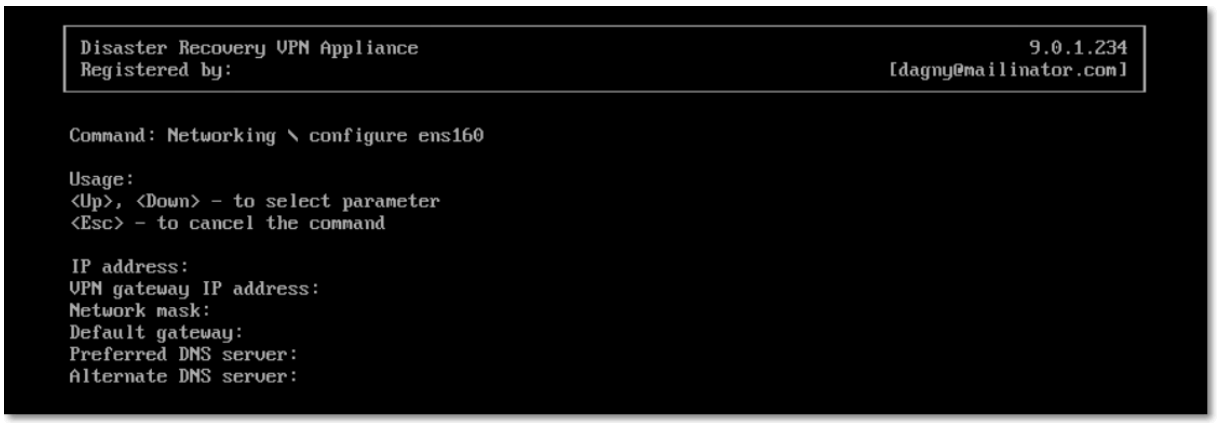
So können Sie ein Netzwerk, das in die Cloud erweitert ist, löschen

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 fünf 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 solange nicht löschen, wie in diesem wenigstens noch ein Cloud Server vorliegt. 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 auf eine 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. 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 neu konfiguriert 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**.

20.1.3.2 Die Einstellungen der VPN-Appliance verwalten

In der Service-Konsole (**Disaster Recovery** –> **Verbindung**) können Sie:

- 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)

20.1.3.3 Die Site-to-Site-Verbindung (de)aktivieren

In folgenden Fällen können Sie die Site-zu-Site-Verbindung (wieder) 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 auf **Eigenschaften anzeigen** und deaktivieren Sie die Option **Site-to-Site-Verbindung**.

Als Ergebnis wird die Verbindung vom lokalen Standort zur Cloud-Site getrennt.

20.1.3.4 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.

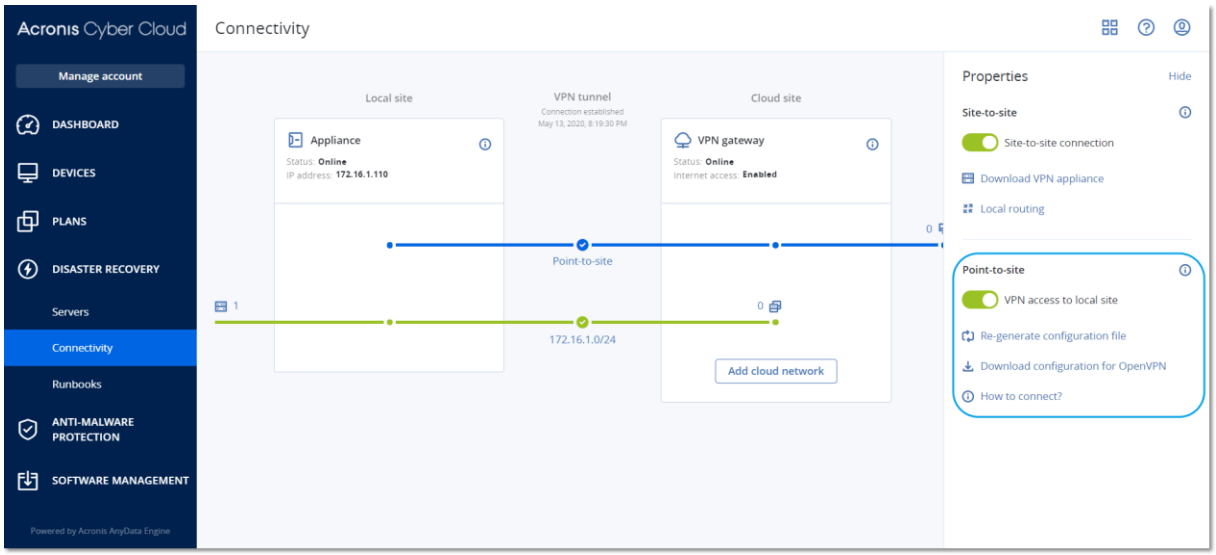
So können Sie ein lokales Routing konfigurieren

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. Wenn Sie fertig sind, klicken Sie auf **Speichern**.

Als Ergebnis können die Server aus den spezifizierten lokalen Netzwerken mit den Cloud Servern kommunizieren.

20.1.3.5 Einstellungen der Point-to-Site-Verbindung verwalten

Gehen Sie in der Service-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.

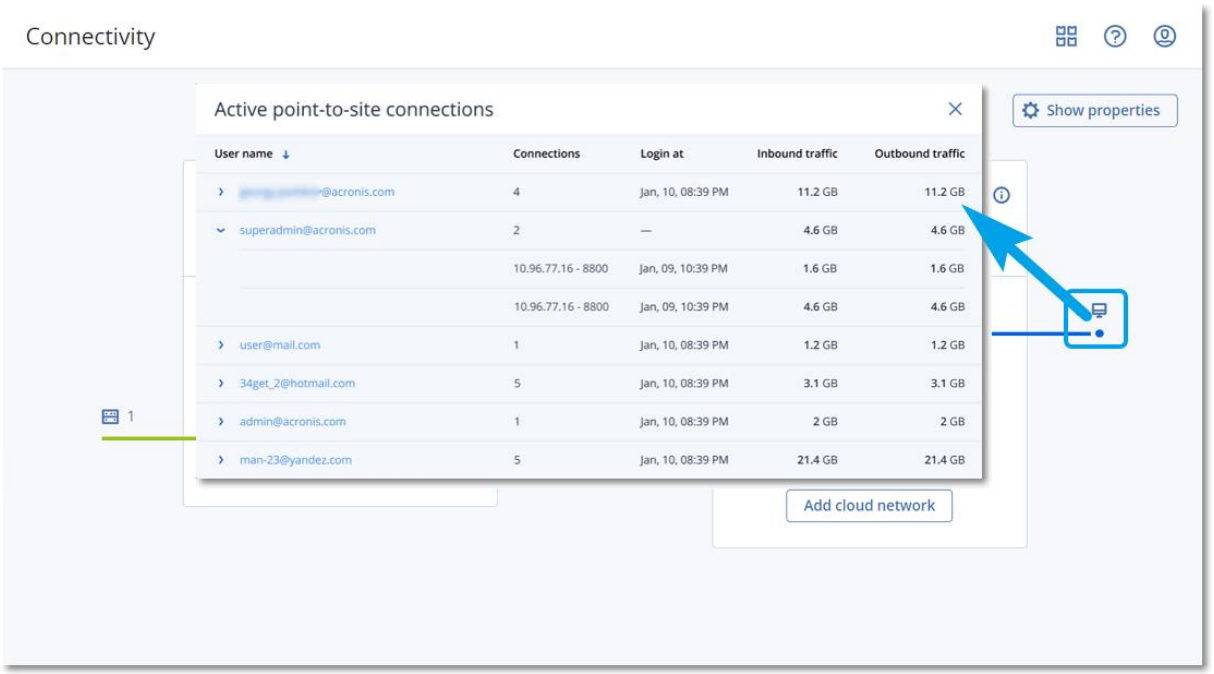
Dies ist in folgenden Fällen erforderlich:

- 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.

20.1.3.6 Aktive Point-to-Site-Verbindungen

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.



21 Recovery-Server einrichten

Dieser Abschnitt beschreibt die Konzepte von Failover und Failback, einen Recovery-Server-Lebenszyklus, die Erstellung eines Recovery-Servers und die entsprechenden Disaster-Recovery-Operationen.

21.1.1 Wie funktionieren Failover und Failback?

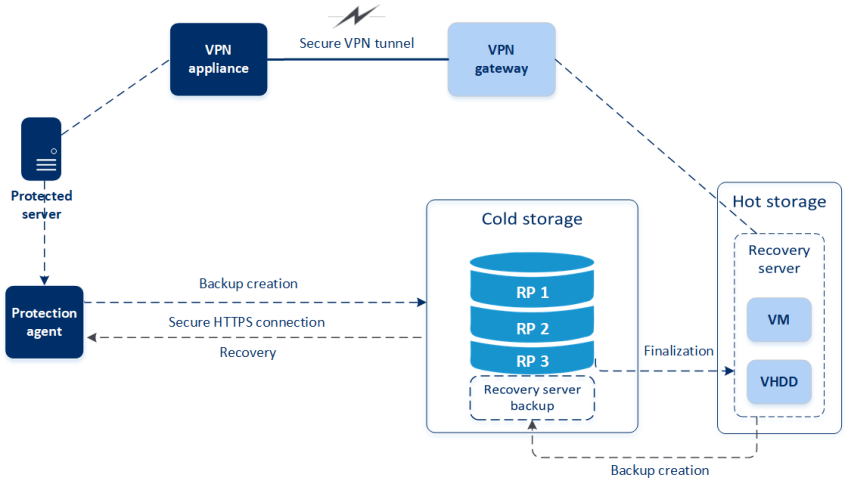
Failover und Failback

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 den Failover-Prozess starten, müssen Sie mindestens ein Disk-Image-Backup (mit bootfähigem Volume) Ihrer ursprünglichen Maschine erstellen.

Wenn Sie den Failover-Prozess starten, wählen Sie den Recovery-Punkt 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“). Der Server bleibt während der Finalisierung verfügbar und betriebsbereit. Die Performance ist gegenüber dem Normalzustand jedoch herabgesetzt. 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.

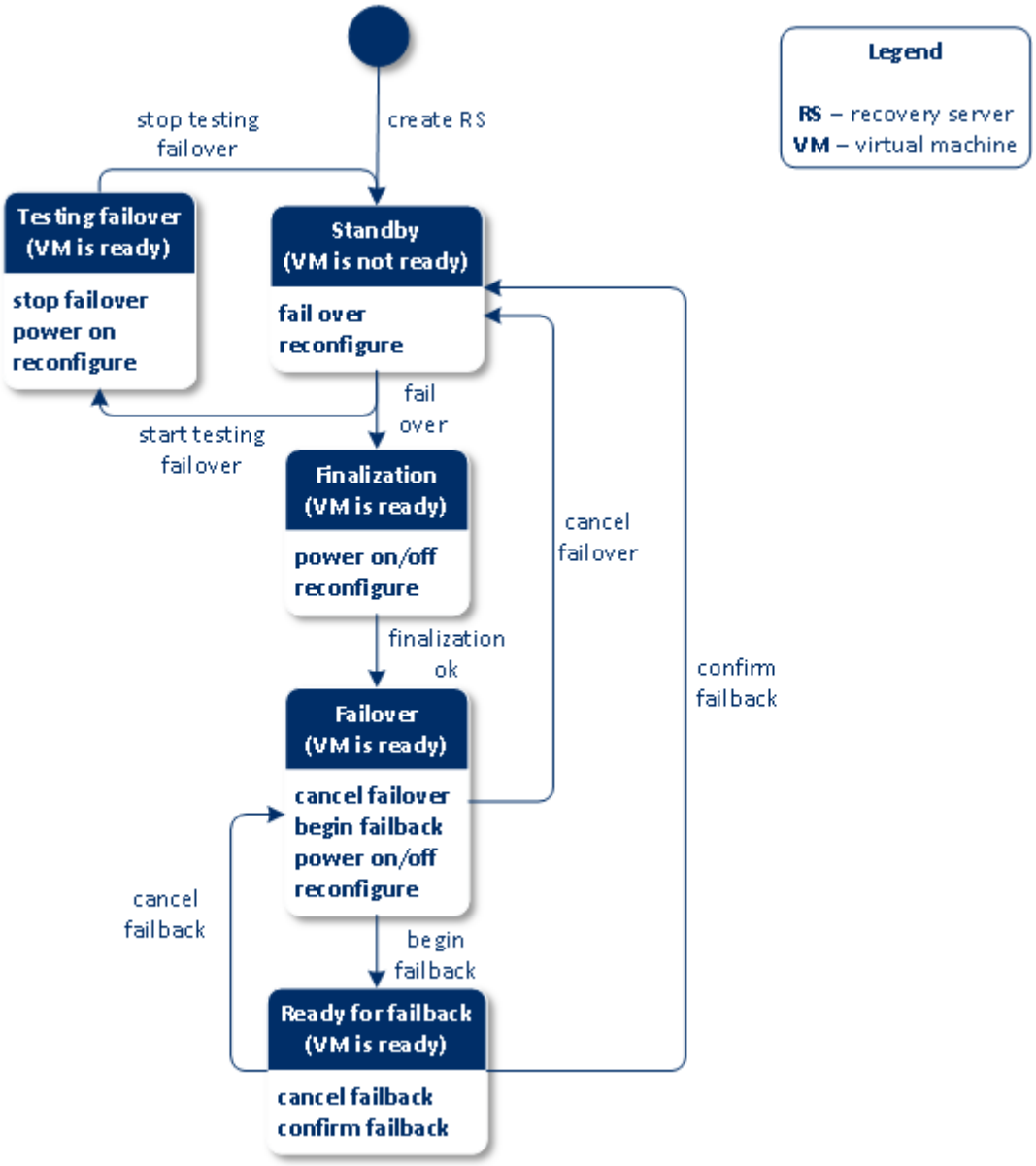


Failover testen

Bei einem **Test-Failover** wird eine 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.

21.1.2 Recovery-Server-Lebenszyklus

In der nachfolgenden Abbildung können Sie einen Recovery-Server-Lebenszyklus sehen, der dauerhafte und vorübergehende Server-Stadien verdeutlicht. Jeder Block zeigt ein Recovery-Server-Stadium, ein Stadium der entsprechenden virtuellen Maschine sowie die Aktionen an, die einem Benutzer in dieser Phase zur Verfügung stehen. Jeder Pfeil ist ein Ereignis oder eine Benutzeraktion, die zum nächsten Stadium führt.



Failover- und Failback-Workflow

1. Benutzeraktion: Erstellen Sie einen Recovery-Server für die ausgewählte Maschine, die geschützt werden soll.
2. **Standby**-Stadium. Die Konfiguration des Recovery-Servers ist definiert, aber die entsprechende virtuelle Maschine ist nicht fertig.
3. Benutzeraktion: Der Failover wird im Produktionsmodus eingeleitet und der Recovery-Server wird auf Basis des ausgewählten Recovery-Punkts erstellt.

4. **Finalisierung**-Stadium Die Laufwerke der virtuellen Maschine werden aus dem gemounteten Recovery-Punkt in den High-Performance-Storage finalisiert. Der Recovery-Server ist betriebsbereit, obwohl seine Performance bis zum Abschluss der Finalisierung gegenüber dem Normalzustand herabgesetzt ist.
5. Ereignis: Die Finalisierung ist erfolgreich.
6. **Failover**-Stadium. Der Workload wird von der ursprünglichen Maschine zum Recovery-Server umgeschaltet.
7. Benutzeraktionen:
   - Initiieren Sie einen Failback. Als Ergebnis wird der Recovery-Server ausgeschaltet und per Backup in den Cloud Storage gesichert.

     ODER
   - Wenn ein Benutzer den Failover-Prozess abbricht, wird der Workload wieder zur ursprünglichen Maschine zurückgeschaltet und der Recovery-Server kehrt in den **Standby**-Modus zurück.
8. **Bereit für Failback**-Stadium. Das Backup des Recovery-Servers wird erstellt. Sie müssen Ihren lokalen Server aus diesem Backup wiederherstellen, indem Sie den üblichen Recovery-Prozess verwenden.
9. Benutzeraktionen:
   - Bestätigen Sie den Failback. Als Ergebnis werden die Cloud-Ressourcen, die dem Recovery-Server zugewiesen wurden, wieder freigegeben.

     ODER
   - Brechen Sie den Failback-Prozess ab. Der Failback-Prozess wird auf Ihre Anforderung hin abgebrochen. Der Recovery-Server kehrt in das **Failover**-Stadium zurück.

Test-Failover-Workflow

1. Benutzeraktion: Erstellen Sie einen Recovery-Server für die ausgewählte Maschine, die geschützt werden soll.
2. **Standby**-Stadium. Die Konfiguration des Recovery-Servers ist definiert, aber die entsprechende virtuelle Maschine ist nicht fertig.
3. Benutzeraktion: Starten Sie mit dem Test des Failovers.
4. **Failover wird getestet**-Stadium. In diesem Zustand wird eine temporäre virtuelle Maschine zu Testzwecken erstellt.
5. Benutzeraktion: Stoppen Sie den Test des Failovers.

21.1.3 Einen Recovery-Server erstellen

Sie können die nachfolgenden Anleitungen befolgen oder sich das Video-Tutorial ansehen.

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 Maschinen** 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.

Beachten Sie die Berechnungspunkte neben jeder Option. Die Anzahl der Berechnungspunkte spiegelt wieder, wie viel die Ausführung des Recovery-Servers pro Stunde kostet.

4. Spezifizieren Sie das Cloud-Netzwerk, mit dem der Server verbunden werden soll.
5. 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.*

6. [Optional] Aktivieren Sie das Kontrollkästchen **IP-Adresse testen** 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.
7. [Optional] Aktivieren Sie das Kontrollkästchen **Internetzugriff**.

   Dies ermöglicht es dem Recovery-Server, sich während eines Failovers (auch im Testmodus) mit dem Internet zu verbinden.
8. [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.
9. [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. Für eingehende Verbindungen zu den öffentlichen IP-Adressen sind folgende offene Ports verfügbar:

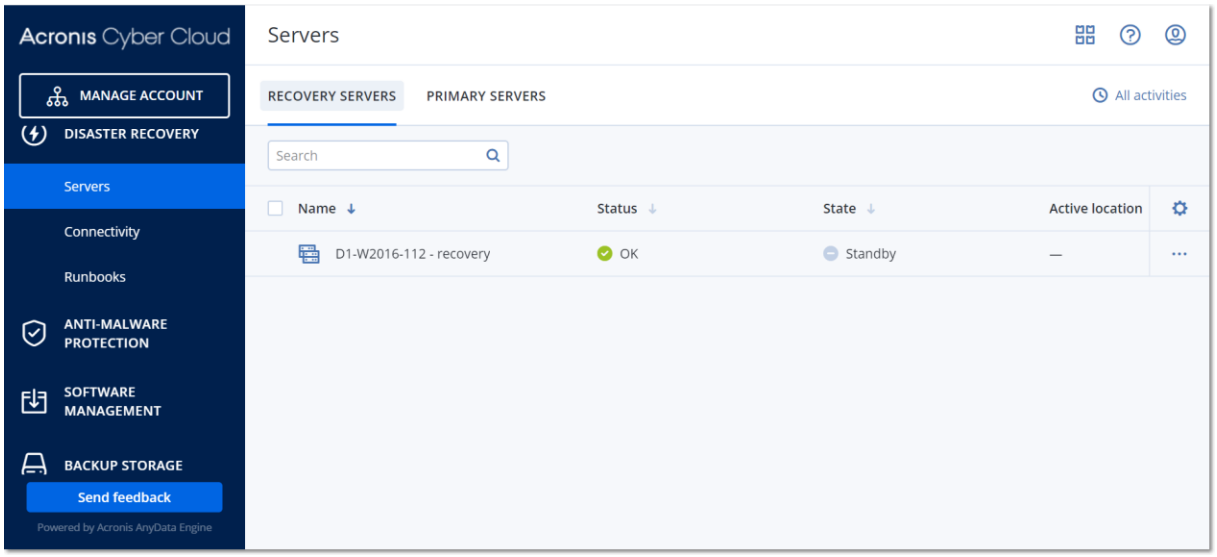
   TCP: 80, 443, 8088, 8443

   UDP: 1194

   Wenn Sie andere offene Ports benötigen, kontaktieren Sie den Support.
10. [Optional] Wenn die Backups für die ausgewählte Maschine verschlüsselt sind, können Sie das Kennwort spezifizieren. Dieses wird dann automatisch verwendet, wenn eine virtuelle Maschine für den Recovery-Server aus dem verschlüsselten Backup erstellt wird. Klicken Sie auf **Spezifizieren** und definieren Sie die Anmeldedaten (Benutzername und Kennwort). Standardmäßig wird Ihnen das neueste Backup in der Liste angezeigt. Wenn Sie alle Backups sehen wollen, müssen Sie auf **Alle Backups anzeigen** klicken.
11. [Optional] Ändern Sie den Namen des Recovery-Servers.
12. [Optional] Geben Sie eine Beschreibung für den Recovery-Server ein.

13. Klicken Sie auf **Erstellen**.

Der Recovery-Server wird in der Service-Konsole in der Registerkarte **Disaster Recovery** –> **Server** –> **Recovery-Server** angezeigt. Sie können dessen Einstellungen auch einsehen, wenn Sie die ursprüngliche Maschine auswählen und dann auf **Disaster Recovery** klicken.



21.1.4 Einen Test-Failover durchführen

Einen Failover zu testen bedeutet, einen Recovery-Server in einem Test-VLAN zu starten, welches von Ihrem Produktionsnetzwerk isoliert ist. Sie können mehrere Recovery-Server gleichzeitig testen, um deren Interaktion zu überprüfen. Innerhalb des Testnetzwerks kommunizieren die Server über ihre Produktions-IP-Adressen. Die Server können jedoch keine TCP- oder UDP-Verbindungen zu den Maschinen in Ihrem lokalen Netzwerk (LAN) aufbauen.

Obwohl Failover-Tests optional sind, empfehlen wir Ihnen, diese 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.

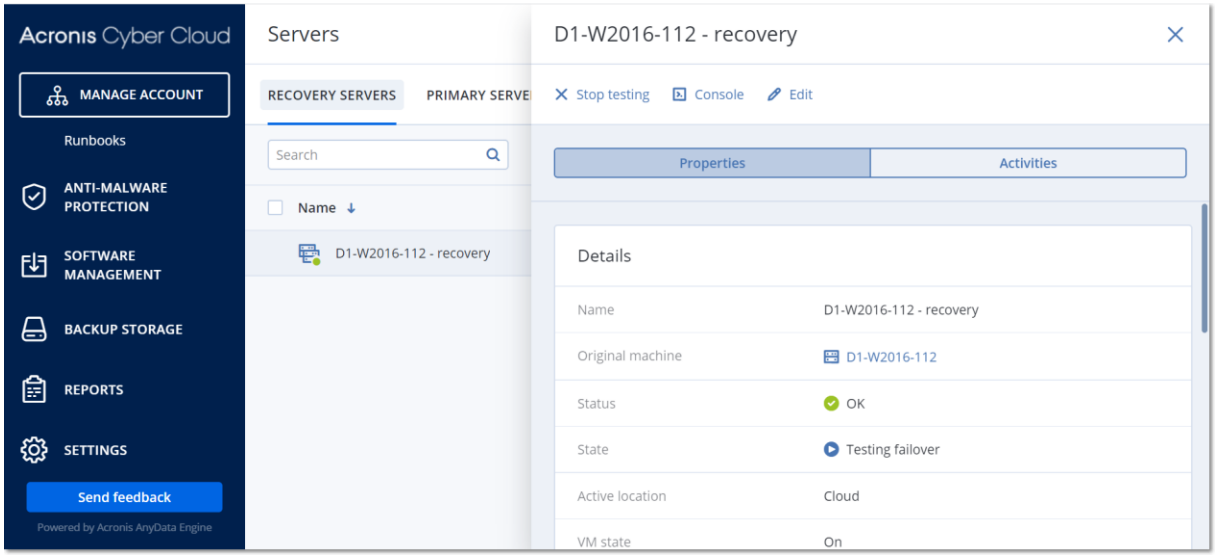
Es wird empfohlen, bereits im Voraus einen Recovery-Server zu erstellen (S. 344), um Ihre Geräte vor einem möglicherweise auftretenden Desaster zu schützen. Sie können dann einen Test-Failover von jedem Recovery-Punkt aus durchführen, der zu einem Zeitpunkt generiert wurde, nachdem der Recovery-Server für das entsprechende Gerät erstellt wurde.

So können Sie einen Test-Failover ausführen

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 und klicken Sie dann auf **Failover testen**.

Wenn der Recovery-Server gestartet ist, ändert sich dessen Stadium auf '**Failover wird getestet**'.



6. 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.
7. 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.

21.1.5 Einen Failover durchführen

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 initiieren, startet der Recovery-Server im Produktionsnetzwerk. Alle Schutzpläne werden von der ursprünglichen Maschine widerrufen. Es wird automatisch ein neuer Schutzplan erstellt und dem Recovery-Server zugewiesen.

Es muss mindestens ein Recovery-Punkt erstellt worden sein, bevor ein Failover-Prozess zu einem Recovery-Server durchgeführt werden kann.

Es wird empfohlen, bereits im Voraus einen Recovery-Server zu erstellen (S. 344), um Ihre Geräte vor einem möglicherweise auftretenden Desaster zu schützen. Sie können dann einen

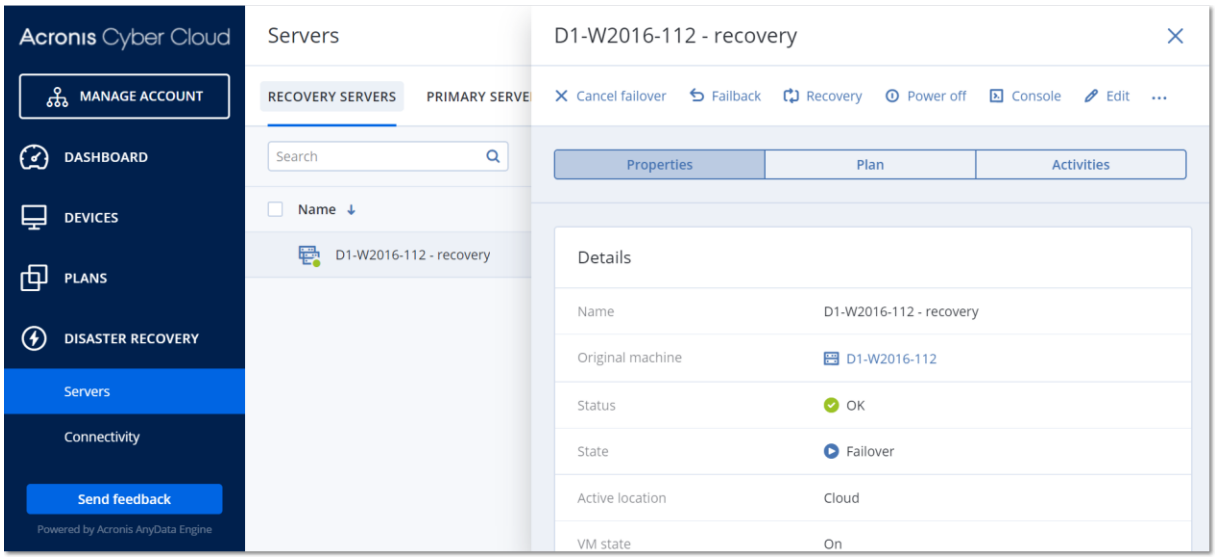
Produktions-Failover von jedem Recovery-Punkt aus durchführen, der zu einem Zeitpunkt generiert wurde, nachdem der Recovery-Server für das entsprechende Gerät erstellt wurde.

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 Service-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 und klicken Sie dann auf **Produktions-Failover starten**.

   Wenn der Recovery-Server gestartet ist, ändert sich dessen Stadium auf **Finalisierung** und nach einer gewissen Zeit auf **Failover.** Es ist wichtig zu verstehen, dass der Server in beiden Stadien verfügbar ist, trotz der rotierenden Fortschrittsanzeige. Ausführlichere Informationen finden Sie im Abschnitt 'Wie funktionieren Failover und Failback? (S. 342)'.



6. 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**.
7. 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 (S. 355)'.

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 durchführen (S. 349) wollen, müssen Sie 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.

21.1.6 Einen Failback durchführen

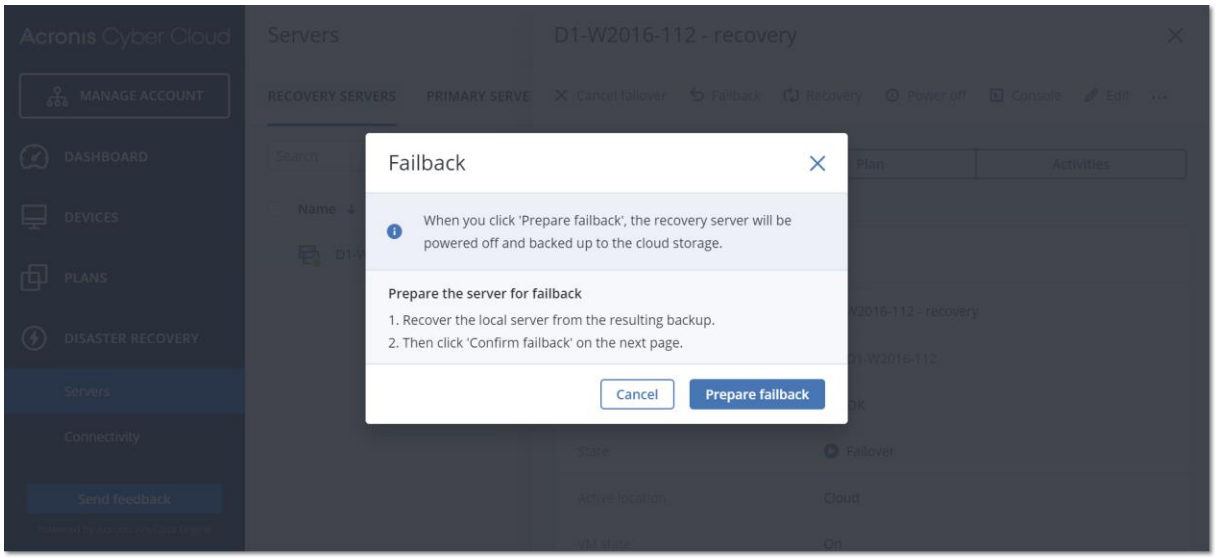
Ein Failback ist ein Prozess, bei dem ein Workload aus der Cloud zurück zu Ihren lokalen Systemen verschoben wird.

Während der Prozess läuft, ist der Server, der verschoben wird, nicht verfügbar. Die Länge dieses Wartungsfensters entspricht in etwa der Dauer einer Backup-Ausführung und einer sich daran anschließenden Wiederherstellung des Servers.

So können Sie einen Failback durchführen

1. Wählen Sie den Recovery-Server aus, der sich im **Failover**-Stadium befindet.

2. Klicken Sie auf **Failback**.



3. Klicken Sie auf **Failback vorbereiten**.

   Der Recovery-Server wird gestoppt und als Backup zum Cloud Storage gesichert. Warten Sie, bis das Backup erfolgreich abgeschlossen wurde.

   Anschließend sind zwei Aktionen verfügbar: **Failback abbrechen** und **Failback bestätigen**. Wenn Sie auf **Failback abbrechen** klicken, wird der Recovery-Server wieder gestartet und der Failover fortgesetzt.
4. Stellen Sie den Server aus diesem Backup auf einer physischen oder virtuellen Maschine in Ihrer lokalen Infrastruktur (on-premise) wieder her.
   - Wenn Sie ein Boot-Medium verwenden, sollten Sie die Anleitung im Abschnitt 'Laufwerke mithilfe eines Boot-Mediums wiederherstellen (S. 201)' der Cyber Protection-Benutzeranleitung befolgen. Stellen Sie sicher, dass Sie sich mit dem Konto in der Cloud anmelden, für welches der Server registriert ist – und dass Sie dann das neueste Backup auswählen.
   - Wenn die Zielmaschine online ist oder es sich um eine virtuelle Maschine (VM) handelt, können Sie die Service-Konsole verwenden. Wählen Sie in der Registerkarte **Backup Storage** den Cloud Storage aus. Wählen Sie bei der Option **Von dieser Maschine aus durchsuchen** die physische Zielmaschine aus oder die Maschine, auf welcher der Agent läuft (wenn die Zielmaschine eine VM ist). Die ausgewählte Maschine muss für dasselbe Konto registriert sein, für welches auch der Server registriert ist. Suchen Sie das neueste Backup des Servers, klicken Sie auf die Option **Komplette Maschine wiederherstellen** – und konfigurieren Sie dann die Recovery-Parameter. Ausführliche Informationen dazu finden Sie im Abschnitt 'Eine Maschine wiederherstellen (S. 197)' der Cyber Protection-Benutzeranleitung.

   Überprüfen Sie, dass die Wiederherstellung abgeschlossen wurde und die wiederhergestellte Maschine korrekt funktioniert.
5. Gehen Sie in der Service-Konsole wieder zurück zum Recovery-Server und klicken Sie auf **Failback bestätigen**.

   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.

21.1.7 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 (S. 344). 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.

22 Primäre Server einrichten

In diesem Abschnitt wird beschrieben, wie Sie Ihre primären Server erstellen und verwalten können.

22.1.1 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 Anzahl der virtuellen CPU-Kerne und die Größe des Arbeitsspeichers.

   Beachten Sie die Berechnungspunkte neben jeder Option. Die Anzahl der Berechnungspunkte spiegelt wieder, wie viel die Ausführung des primären Servers pro Stunde kostet.
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. 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.*
8. [Optional] Aktivieren Sie das Kontrollkästchen **Internetzugriff**.

   Dadurch wird dem primären Server ermöglicht, auf das Internet zuzugreifen.
9. [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. Für eingehende Verbindungen zu den öffentlichen IP-Adressen sind folgende offene Ports verfügbar:

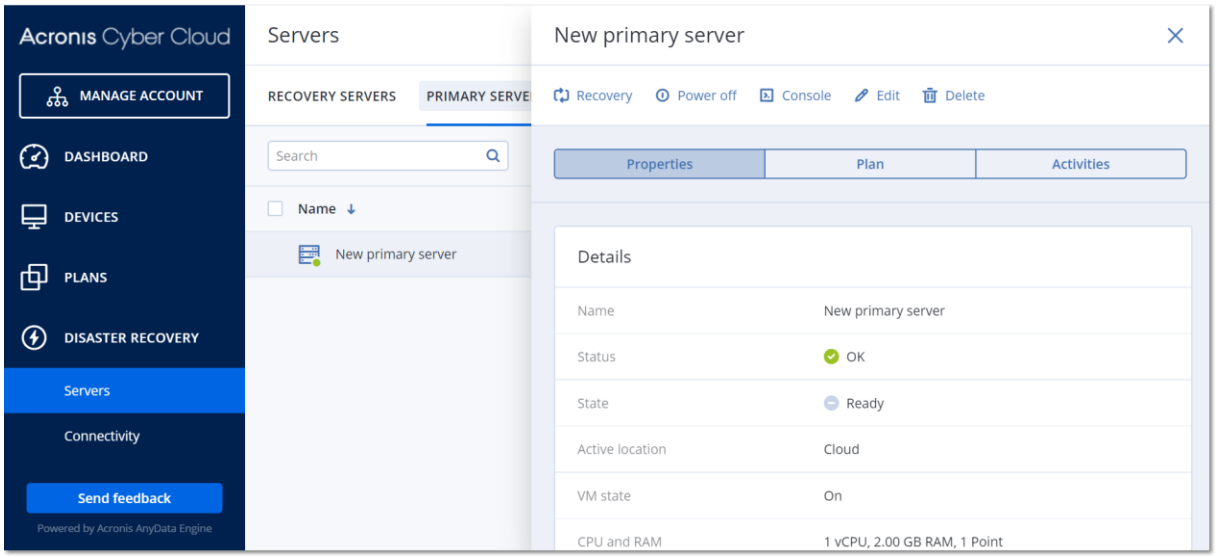
   TCP: 80, 443, 8088, 8443

   UDP: 1194

   Wenn Sie andere offene Ports benötigen, kontaktieren Sie den Support.
10. [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.
11. Definieren Sie einen Namen für den primären Server.
12. [Optional] Spezifizieren Sie eine Beschreibung für den primären Server.
13. 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.



22.1.2 Aktionen mit einem primären Server

Der primäre Server wird in der Service-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 (S. 355)'.

23 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, gemäß seinem Lebenszyklus (S. 343)
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.

23.1 Backup der Cloud Server

Primäre Server und Recovery-Server werden von dem Agenten für VMware gesichert, der auf der Cloud-Site installiert ist. In der ersten Version ist dieses Backup funktionell noch beschnitten, wenn man es gegen ein Backup vergleicht, das vom lokalen Agenten ausgeführt wird. Diese Beschränkungen sind aber nur temporär und werden mit zukünftigen Versionen aufgehoben.

- Der einzig mögliche Backup-Speicherort ist der Cloud Storage.
- Ein Schutzplan kann nicht auf mehrere Server gleichzeitig angewendet werden. Jeder Server muss seinen eigenen Schutzplan haben, auch wenn alle Schutzpläne ansonsten die gleichen Einstellungen haben.
- Auf einen Server kann nur je ein Schutzplan 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 Schutzpläne für Cloud Server werden nach UTC-Zeit durchgeführt.*

24 Orchestrierung (Runbooks)

Ein Runbook ist eine Zusammenstellung von Anweisungen, die beschreibt, wie die Produktionsumgebung in die Cloud übertragen wird. Sie können Runbooks in der Service-Konsole erstellen. Wenn Sie auf die Registerkarte **Runbooks** zugreifen wollen, wählen Sie die Befehle **Disaster Recovery** –> **Runbooks**.

Warum sollte ich Runbooks verwenden?

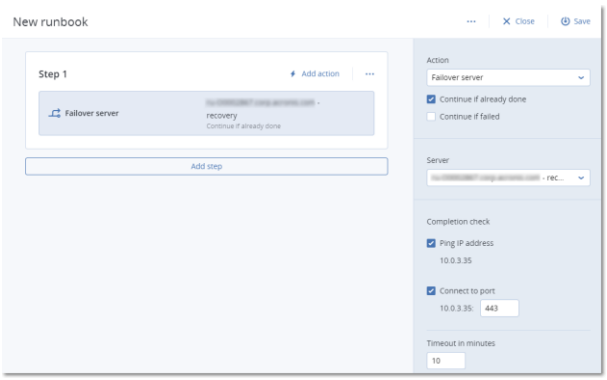
Mit Runbooks können Sie:

- 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

24.1.1 Ein Runbook erstellen

Sie können die nachfolgende Anleitung befolgen oder sich das Video-Tutorial ansehen.

Klicken Sie zum Erstellen eines Runbooks auf **Runbook erstellen** –> **Schritt hinzufügen** –> **Aktion hinzufügen**. Sie können die Aktionen und Schritte per Drag&Drop verschieben. Vergessen Sie nicht, dem Runbook einen eindeutigen Namen zu geben. Wenn Sie ein längeres Runbook erstellen, sollten Sie zwischenzeitlich immer mal wieder auf **Speichern** klicken. Klicken Sie auf **Schließen**, wenn Sie fertig sind.



Schritte und Aktionen

Ein Runbook besteht aus Schritten, die nacheinander ausgeführt werden. Ein Schritt besteht aus Aktionen, die gleichzeitig gestartet werden. Eine Aktion kann bestehen aus:

- Eine Operation kann mit einem Cloud Server durchgeführt werden (**Server-Failover ausführen**, **Server starten**, **Server stoppen**, **Server-Failback ausführen**). Hinweis: normalerweise wird der Begriff 'Aktion(en)' in der Benutzerdokumentation und Bernutzeroberfläche für den hier verwendeten Begriff 'Operation(en)' verwendet bzw. zwischen diesen beiden nicht unterschieden. Für diesen Abschnitt über Runbooks wird zwischen den beiden Begriffen unterschieden. Im übrigen Verlauf der Dokumentation werden die hier genannten

'Operation(en)' ansonsten als Aktionen bezeichnet. Um diese Operation zu definieren, müssen Sie zuerst die Operation auswählen, dann den Cloud Server und dann die Parameter für die Operation.

- Eine manuelle Operation, die Sie verbal beschreiben müssen. Sobald die Operation abgeschlossen wurde, muss ein Benutzer auf die Bestätigungsschaltfläche klicken, damit das Runbook fortgesetzt werden kann.
- Die Ausführung eines anderen Runbooks. Um diese Operation zu definieren, müssen Sie das entsprechende 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'.

***Hinweis**: In dieser Produktversion muss ein Benutzer einen Failback manuell durchführen. Ein Runbook zeigt die Eingabeaufforderung an, wenn dies erforderlich ist.*

Aktionsparameter

Alle Operationen mit Cloud Servern haben folgende Parameter:

- **Fortsetzen, wenn bereits durchgeführt** (standardmäßig aktiviert)

  Dieser Parameter definiert das Runbook-Verhalten, wenn die erforderliche Operation bereits 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 Operation und damit dann auch das Runbook fehl.
- **Fortsetzen, wenn fehlgeschlagen** (standardmäßig deaktiviert)

  Dieser Parameter definiert das Runbook-Verhalten, wenn die erforderliche Operation 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 Operation und damit dann auch das Runbook fehl.

Fertigstellungsprüfung

Sie können für die Aktionen **Server-Failover ausführen** und **Server Starten** eine Fertigstellungsprüfung hinzufügen, um sicherzustellen, dass der entsprechende Server verfügbar ist und die benötigen Services bereitgestellt sind. Wenn eine dieser Prüfungen scheitert, wird die Aktion als fehlgeschlagen betrachtet.

- **IP-Adresse anpingen**

  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)

  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 angegebenen Port lauscht, auch ausgeführt wird.

Der vorgegebene Timeout-Wert beträgt 10 Minuten. Sie können diesen bei Bedarf ändern.

24.1.2 Aktionen mit Runbooks

Um auf die Liste der Aktionen zuzugreifen, bewegen Sie den Mauszeiger auf ein Runbook und klicken Sie auf das Symbol mit den drei Punkten. 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**

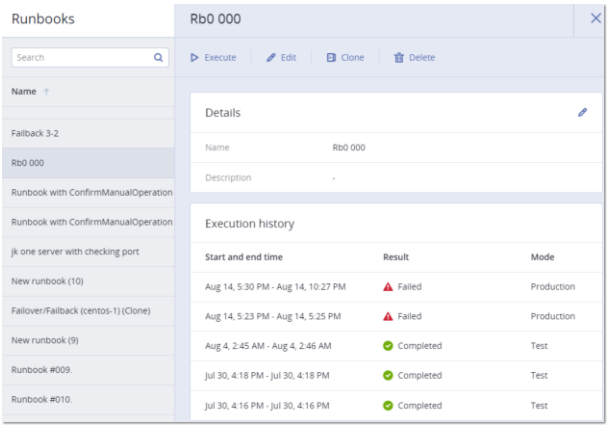
  Wählen Sie den neuesten Recovery-Punkt (Standardvorgabe) oder wählen Sie einen bestimmten Zeitpunkt in der Vergangenheit. Bei letzterem werden für jeden Server diejenigen Recovery-Punkte ausgewählt, die dem spezifizierten Zeitpunkt am nächsten liegen.

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.



25 Antimalware Protection und Web Protection

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 Windows Defender Antivirus.

25.1 Antivirus & Antimalware Protection

Mit dem Antivirus & Antimalware Protection-Modul können Sie Ihre Windows- und macOS-Maschinen gegen alle aktuellen Malware-Bedrohungen absichern. Beachten Sie, dass die Active Protection-Funktionalität, die Teil der Antimalware Protection ist, auf macOS-Maschinen nicht unterstützt wird. Hier finden Sie die vollständige Liste der unterstützten Antimalware-Funktionen: Unterstützte Funktionen, nach Betriebssystem (S. 15).

Die Antivirus & Antimalware Protection wird vom Windows-Sicherheitscenter unterstützt und in diesem registriert.

Folgende Antimalware-Fähigkeiten stehen Ihnen zur Verfügung:

- Erkennen von Malware in Dateien (für Windows oder macOS) – 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 bösartige URLs (für Windows)
- Verschieben von gefährlichen Dateien in eine Quarantäne
- Verwalten einer Positivliste mit vertrauenswürdigen Unternehmensapplikationen

Das Antivirus & Antimalware Protection-Modul bietet Ihnen zwei verschiedene Scanning-Methoden:

- Echtzeitschutz-Scan
- On-Demand-Antimalware-Scan

Echtzeitschutz-Scan

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.

Der Echtzeitschutz kann nicht parallel mit anderen Antivirus-Lösungen arbeiten, die ebenfalls Echtzeitschutzfunktionen verwenden, um mögliche Kompatibilitäts- und Performance-Probleme zu verhindern. Die Statuszustände anderer installierter Antivirus-Lösungen werden über das Windows-Sicherheitscenter bestimmt. Wenn die Windows-Maschine bereits von einer anderen Antivirus-Lösung geschützt ist, wird der Echtzeitschutz nach dem Neustart der Maschine automatisch ausgeschaltet.

Wenn Sie den Echtzeitschutz aktivieren wollen, müssen Sie die andere Antivirus-Lösung deaktivieren oder deinstallieren. Unser Echtzeitschutz kann den Echtzeitschutz von Windows Defender automatisch ersetzen.

Für Sie können folgende Scanning-Varianten wählen:

- Eine Erkennung bei Bedarf (On-Access Detection) bedeutet, dass das Antimalware-Programm 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/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.

On-Demand-Antimalware-Scan

Das Antimalware-Scanning wird auf Basis eines Zeitplans durchgeführt.

Sie können die Ergebnisse des Antimalware-Scannings im Widget **Dashboard** –> **Überblick** –> Kürzlich betroffen (S. 428) überwachen.

25.1.1 Einstellungen für die Antivirus & Antimalware Protection

Eine Anleitung zum Erstellen eines Schutzplans mit aktiviertem Antivirus & Antimalware Protection-Modul finden Sie im Abschnitt 'Einen Schutzplan erstellen (S. 105)'.

Für das Antivirus & Antimalware Protection-Modul können folgende Einstellungen spezifiziert werden:

Active Protection

Active Protection kann ein System vor Ransomware und Cryptomining-Malware schützen. Ransomware verschlüsselt Dateien und verlangt ein Lösegeld für die Bereitstellung des Codierungsschlüssels. Cryptomining-Malware führt mathematische Berechnungen im Hintergrund durch, um digitale Crypto-Währungen zu 'schürfen', und stiehlt auf diese Weise Rechenleistung und Netzwerkressourcen vom betroffenen System.

Active Protection ist derzeit nur für Maschinen verfügbar, die unter Windows (Version 7 und höher) oder Windows Server (Version 2008 R2 und höher) laufen. Auf der zu schützenden Maschine muss der Agent für Windows laufen.

Active Protection ist für Agenten ab Version 12.0.4290 verfügbar. Die Aktualisierung von Agenten wird im Abschnitt 'Update der Agenten (S. 86)' erläutert.

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, sofern diese zuvor über eine entsprechende Konfiguration spezifiziert wurden.

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.

Standardeinstellung: **Aktiviert**.

Active Protection-Einstellungen

Wählen Sie bei **Aktion bei Erkennung** diejenige Aktion aus, die die Software durchführen soll, wenn eine Ransomware-Aktivität erkannt wurde. Klicken Sie anschließend auf **Fertig**.

Sie können eine der folgenden Optionen wählen:

- **Nur benachrichtigen**
  Die Software erstellt eine Alarmmeldung über den Prozess.
- **Den Prozess stoppen**
  Die Software erstellt eine Alarmmeldung und hält den Prozess an.
- **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**.

Verhaltenserkennung und Exploit-Prävention

Um schädliche Prozesse identifizieren zu können, vergleicht die Software die von einem Prozess ausgeführten Aktionsketten (z.B. Ereignisse im Dateisystem) mit Aktionsketten, die in einer Referenzdatenbank mit bekannten schädlichen Verhaltensmustern gespeichert sind. Dadurch kann neue Malware anhand typischer Verhaltensmuster erkannt werden.

Verhaltenserkennung

Die Behavior Engine schützt ein System vor Malware.

Standardeinstellung: **Aktiviert**.

Verhaltenserkennungseinstellungen

Wählen Sie bei **Aktion bei Erkennung** diejenige Aktion aus, die die Software durchführen soll, wenn eine Malware-Aktivität erkannt wurde. Klicken Sie anschließend auf **Fertig**.

Sie können eine der folgenden Optionen wählen:

- **Nur benachrichtigen**
  Die Software wird einen Alarm generieren, wenn ein Prozess eine mögliche Malware-Aktivität zeigt.
- **Den Prozess stoppen**
  Die Software wird einen Alarm generieren und den Prozess stoppen, der eine mögliche Malware-Aktivität zeigt.
- **Quarantäne**
  Die Software wird einen Alarm generieren, den Prozess stoppen und die entsprechende ausführbare Datei in den Quarantäne-Ordner verschieben.

Standardeinstellung: **Quarantäne**.

Exploit-Prävention

Die Exploit-Prävention erkennt und verhindert, dass sich infizierte Prozesse ausbreiten und vorhandene Software-Schwachstellen in einem Windows-System ausnutzen. Wenn ein Exploit erkannt wird, generiert die Software eine Alarmmeldung und stoppt den Prozess, der mögliche Exploit-Aktivitäten zeigt.

Die Exploit-Prävention ist nur mit Agenten ab Build 23130 verfügbar.

Standardeinstellung: **Aktiviert** für neu erstellte Schutzpläne – und **Deaktiviert** für bereits vorhandene Schutzpläne, die mit früheren Versionen des Protection Agenten erstellt wurden.

***Hinweis**: Sie müssen die Verhaltenserkennung aktivieren, um die Exploit-Prävention aktivieren zu können.*

Einstellungen für die Exploit-Prävention

Sie können auswählen, welche Methoden der Exploit-Prävention vom Programm angewendet werden.

Aktivieren oder deaktivieren Sie unter **Aktivierte Exploit-Präventionstechniken** die Methoden, die angewendet werden sollen, und klicken Sie dann auf **Fertig**.

Sie können eine der folgenden Optionen wählen:

- 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.
- 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.

***Hinweis**: Prozesse, die in der Ausschlussliste als vertrauenswürdige Prozesse aufgeführt sind, werden nicht nach Exploits gescannt.*

Selbstschutz

Der **Selbstschutz** (Self-Protection) verhindert, dass die Prozesse, Registry-Einträge, ausführbaren Dateien und Konfigurationsdateien der Backup-Software selbst sowie Backups, die in lokalen Ordnern gespeichert sind, verändert werden können. Wir raten davon ab, diese Funktion zu deaktivieren.

Standardeinstellung: **Aktiviert**.

Prozessen erlauben, Backups zu modifizieren

Die Option **Bestimmten Prozessen erlauben, Backups zu modifizieren** ist wirksam, wenn der **Selbstschutz** (Self-Protection) aktiviert ist.

Er gilt für Dateien mit den Endungen .tibx, .tib sowie .tia und die in lokalen Ordnern vorliegen.

Mit dieser Option 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 Option 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 Option 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**.

Netzwerkordnerschutz

Die Option **Als lokale Laufwerke zugeordnete Netzwerkordner schützen** bestimmt, ob auch Netzwerkordner durch die Antivirus & Antimalware Protection vor lokalen Schadprozessen geschützt werden sollen, die als lokale Laufwerke zugeordnet (gemountet) sind.

Diese Option gilt für Ordner, die per SMB oder NFS 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 Caceh in demjenigen Ordner wiederhergestellt, der in den Einstellungen der Option spezifiziert wurde. Der vorgegebene Ordner ist: **C:\ProgramData\Acronis\Restored Network Files**. Falls es diesen Ordner nicht gibt, wird er automatisch erstellt. Wenn Sie diesen Pfad ändern wollen, dürfen Sie nur einen lokalen Ordner spezifizieren. Netzwerkordner werden nicht unterstützt (gilt auch für Ordner von Netzwerklaufwerken)

Standardeinstellung: **Aktiviert**.

Serverseitiger Schutz

Diese Option schützt Netzwerkordner, die Sie freigegeben haben, per Antivirus & Antimalware Protection vor potentiellen Bedrohungen, die über externe Verbindungen (also von anderen Servern im Netzwerk) hereinkommen können.

Standardeinstellung: **Deaktiviert**.

Vertrauenswürde und blockierte Verbindungen einrichten

Auf der Registerkarte **Vertrauenswürdig** können Sie Verbindungen spezifizieren, die Daten modifizieren dürfen. Sie sollten den Benutzernamen und die IP-Adressen spezifizieren.

Auf der Registerkarte **Blockiert** können Sie Verbindungen spezifizieren, die keine Daten modifizieren dürfen. Sie sollten den Benutzernamen und die IP-Adressen spezifizieren.

Erkennung von Cryptomining-Prozessen

Diese Option bestimmt, ob Antivirus & Antimalware Protection auch mögliche Cryptomining-Malware erkennen soll.

Cryptomining-Malware kann die Performance nützlicher Applikationen beeinträchtigen, die Stromrechnung erhöhen, Systemabstürze oder sogar Hardware-Schäden (durch übermäßige Nutzung) verursachen. Wir empfehlen, Cryptomining-Malware zur Liste der **Schädlichen Prozesse** hinzuzufügen, um deren Ausführung zu unterbinden.

Standardeinstellung: **Aktiviert**.

Einstellungen für die Erkennung von Cryptomining-Prozessen

Wählen Sie bei **Aktion bei Erkennung** diejenige Aktion aus, die die Software durchführen soll, wenn eine Cryptomining-Aktivität erkannt wurde. Klicken Sie anschließend auf **Fertig**.

Sie können eine der folgenden Optionen wählen:

- **Nur benachrichtigen**

  Die Software generiert einen Alarm, wenn ein Prozess eine mögliche Cryptomining-Aktivität zeigt.
- **Den Prozess stoppen**

  Die Software generiert einen Alarm und stoppt den Prozess, der eine mögliche Cryptomining-Aktivität zeigt.

Standardeinstellung: **Den Prozess stoppen**.

Echtzeitschutz-Scan

Der **Echtzeitschutz-Scan** überprüft das System Ihrer Maschine kontinuierlich auf Viren und andere bösartige Bedrohungen. Dies erfolgt während der gesamten Betriebszeit Ihres Systems – außer, der Echtzeitschutz wird vom Benutzer des Computers pausiert.

Standardeinstellung: **Aktiviert**.

Die Aktion bei Erkennung für den Echtzeitschutz konfigurieren

Wählen Sie bei **Aktion bei Erkennung** diejenige Aktion aus, die die Software durchführen soll, wenn ein Virus oder eine andere bösartige Bedrohung erkannt wurde. Klicken Sie anschließend auf **Fertig**.

Sie können eine der folgenden Optionen wählen:

- **Blockieren und benachrichtigen**

  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 entsprechende ausführbare Datei in den Quarantäne-Ordner

Standardeinstellung: **Quarantäne**.

Den Scan-Modus für den Echtzeitschutz konfigurieren

Wählen Sie bei **Scan-Modus** diejenige Aktion aus, die die Software durchführen soll, wenn ein Virus oder eine andere bösartige Bedrohung erkannt wurde. Klicken Sie anschließend auf **Fertig**.

Sie können eine der folgenden Optionen wählen:

- **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.

Standardeinstellung: **Bei Zugriff (intelligent)**.

Scan planen

Sie können einen Zeitplan definieren, auf dessen Basis das System Ihrer Maschine nach Malware überprüft wird. Aktivieren Sie die Option **Scan planen**.

Standardeinstellung: **Aktiviert**.

Aktion bei Erkennung:

- **Quarantäne**

  Die Software generiert einen Alarm, stoppt den Prozess und verschiebt die entsprechende ausführbare Datei in den Quarantäne-Ordner
- **Nur benachrichtigen**

  Die Software generiert einen Alarm, wenn ein Prozess eine mögliche Malware-Aktivität zeigt.

Standardeinstellung: **Quarantäne**.

Scan-Modus:

- **Vollständig**

  Dauert im Vergleich zum Schnellscan deutlich länger, weil jede Datei überprüft werden muss.
- **Schnell**

  Beim Schnellscan werden nur allgemeine Bereiche überprüft, wo Malware normalerweise auf einer Maschine zu finden ist.

Standardeinstellung: **Schnell**.

Die Task-Ausführung auf Basis folgender Ereignisse planen

- **Planung nach Zeit** – der Task wird zum spezifizierten Zeitpunkt ausgeführt.
- **Wenn sich ein Benutzer am System anmeldet** – die Task-Ausführung wird standardmäßig durch die Anmeldung eines jeden Benutzers ausgelöst. Sie können aber von 'Jeder Benutzer' zu einem bestimmten Benutzerkonto wechseln.
- **Wenn sich ein Benutzer vom System abmeldet** – die Task-Ausführung wird standardmäßig durch die Abmeldung eines jeden Benutzers ausgelöst. Sie können aber von 'Jeder Benutzer' zu einem bestimmten Benutzerkonto wechseln.

  Hinweis: *Der Task wird nicht beim Herunterfahren eines Systems ausgeführt, weil 'Herunterfahren' nicht dasselbe wie 'Abmelden' ist.*
- **Beim Systemstart** – der Task wird ausgeführt, wenn das Betriebssystem startet.

- **Beim Herunterfahren des Systems** – der Task wird ausgeführt, wenn das Betriebssystem herunterfährt.

Standardeinstellung: **Planung nach Zeit**.

Planungstyp:

- **Monatlich** – bestimmen Sie, an welchen Tagen in welchem Monat der Task ausgeführt werden soll.
- **Täglich** – bestimmen Sie, an welchen Wochentagen der Task ausgeführt werden soll.
- **Stündlich** – bestimmen Sie, an welchen Wochentagen und wie oft ein Task in einer Stunde ausgeführt werden soll.

Standardeinstellung: **Täglich**.

Starten um – bestimmen sie, zu welchem Zeitpunkt der Task ausgeführt werden soll.

Standardeinstellung: **14:00 Uhr** (auf der Maschine, auf welcher die Software installiert ist).

Innerhalb eines Zeitraums ausführen – bestimmten Sie einen Datumsbereich, wann die Planung gültig ist.

Startbedingungen – definieren Sie Bedingungen, die gleichzeitig zutreffen müssen, damit der Task gestartet werden kann. Sie ähneln den Startbedingungen für das Backup-Modul, die im Abschnitt 'Startbedingungen (S. 144)' beschrieben sind.

Folgende zusätzliche Startbedingungen können definiert werden:

- **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 (in Stunden), nachdem der Task dennoch gestartet werden soll.

Archivdateien scannen

Standardeinstellung: **Aktiviert**.

- **Max. Rekursionstiefe**

  Wie viele Ebenen von eingebetteten Archiven gescannt werden können. Beispiel: MIME-Dokument –> ZIP-Archiv –> Office-Archiv –> Dokumenteninhalt.

  Standardeinstellung: **16**.
- **Maximale Größe**

  Die maximale Größe einer zu scannenden Archivdatei.

  Standardeinstellung: **Unbegrenzt**.

Wechsellaufwerke scannen

Standardeinstellung: **Deaktiviert**.

- **Zugeordnetes Netzlaufwerk (Remote-Laufwerk)**
- **USB-Speichergeräte** (wie etwa USB-Sticks und externe Festplatten)
- **CDs/DVDs**

Nur neue und geänderte Dateien scannen – es werden nur neu erstellte und/oder geänderte Dateien überprüft.

Standardeinstellung: **Aktiviert**.

Quarantäne

Die Quarantäne (S. 379) ein spezieller Ordner, um verdächtige (möglicherweise infizierte) oder potenziell gefährliche Dateien isolieren zu können.

Dateien aus der Quarantäne entfernen nach: – definiert einen Zeitraum in Tagen, nach dessen Ablauf die entsprechenden Dateien aus der Quarantäne gelöscht werden.

Standardeinstellung: **30 Tage**.

Ausschlusskriterien

Sie können Ausnahmen für die von Ihnen festgelegten Schutzregeln festlegen.

Auf der Registerkarte **Vertrauenswürdig** können Sie Folgendes spezifizieren:

- Prozesse, die niemals als Malware eingestuft werden
- Ordner, die nicht auf Dateiänderungen überwacht werden
- Dateien und Ordner, in denen kein geplantes Scanning ausgeführt wird.

Auf der Registerkarte **Blockiert** können Sie Folgendes spezifizieren:

- Prozesse, die immer geblockt werden
- Ordner, wo jeder Prozess geblockt wird

Standardeinstellung: standardmäßig sind keine Ausnahmen definiert.

25.2 Active Protection

Active Protection wird als Modul eines Schutzplans dargestellt, wenn Sie eine der folgenden Editionen haben:

- Cyber Backup Standard
- Cyber Backup Advanced
- Cyber Backup Disaster Recovery

Da Active Protection ein Bestandteil eines Schutzplans ist, kann es individuell konfiguriert und auf verschiedene Geräte oder Gerätegruppen angewendet werden.

Bei allen anderen Editionen des Cyber Protection Service ist die Active Protection-Funktionalität Bestandteil des Antivirus & Antimalware Protection-Moduls.

Active Protection kann ein System vor Ransomware und Cryptomining-Malware schützen. Ransomware verschlüsselt Dateien und verlangt ein Lösegeld für die Bereitstellung des Codierungsschlüssels. Cryptomining-Malware führt mathematische Berechnungen im Hintergrund durch, um digitale Crypto-Währungen zu 'schürfen', und stiehlt auf diese Weise Rechenleistung und Netzwerkressourcen vom betroffenen System.

Active Protection ist derzeit nur für Maschinen verfügbar, die unter Windows (Version 7 und höher) oder Windows Server (Version 2008 R2 und höher) laufen. Auf der zu schützenden Maschine muss der Agent für Windows laufen.

Active Protection ist für Agenten ab Version 12.0.4290 verfügbar. Die Aktualisierung von Agenten wird im Abschnitt 'Update der Agenten (S. 86)' erläutert.

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, sofern diese zuvor über eine entsprechende Konfiguration spezifiziert wurden.

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

Das Active Protection-Modul hat folgende Einstellungen:

- Aktion bei Erkennung
- Selbstschutz
- Netzwerkordnerschutz
- Serverseitiger Schutz
- Erkennung von Cryptomining-Prozessen
- Ausschlusskriterien

Weitere Informationen über die Active Protection-Einstellungen finden Sie im Abschnitt 'Antivirus & Antimalware Protection-Einstellungen (S. 360)'.

25.3 Windows Defender Antivirus

Windows Defender Antivirus ist eine integrierte Antimalware -Komponente von Microsoft Windows, die seit Windows 8 mit dem Betriebssystem ausgeliefert wird.

Das Windows Defender Antivirus (WDA)-Modul ermöglicht Ihnen, eine Windows Defender Antivirus-Sicherheitsrichtlinie zu konfigurieren und deren Status über die Cyber Protection Service-Konsole zu verfolgen.

Dieses Modul ist auf Maschinen anwendbar, auf denen Windows Defender Antivirus installiert ist.

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 entsprechenden WDA-Einstellungen finden Sie unter der Adresse https://docs.microsoft.com/de-de/configmgr/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 einer Maschine erkannte Malware wird entfernt.
- **Quarantäne** – die erkannte Malware wird nicht vollständig entfernt, sondern in den Quarantäne-Ordner verschoben.
- **Entfernen** – die auf einer Maschine erkannte Malware wird gelöscht.
- **Zulassen** – 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 entsprechenden WDA-Einstellungen finden Sie unter der Adresse https://docs.microsoft.com/de-de/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 Maschinen installiert oder ausgeführt wird.

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 entsprechenden WDA-Einstellungen finden Sie unter der Adresse https://docs.microsoft.com/de-de/configmgr/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 Protection Service-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 entsprechenden WDA-Einstellungen finden Sie unter der Adresse https://docs.microsoft.com/de-de/configmgr/protect/deploy-use/endpoint-antimalware-policies#advanced-settings.

Ausschlusskriterien

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 entsprechenden WDA-Einstellungen finden Sie unter der Adresse https://docs.microsoft.com/de-de/configmgr/protect/deploy-use/endpoint-antimalware-policies#exclusion-settings.

25.4 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 Protection Service-Konsole zu verfolgen.

Dieses Modul ist auf Maschinen anwendbar, auf denen Microsoft Security Essentials installiert ist.

Die Einstellungen von Microsoft Security Essentials sind fast identisch zu denen von Microsoft Windows Defender Antivirus – mit Ausnahme fehlender Echtzeitschutz-Einstellungen und der fehlenden Möglichkeit, Ausschlusskriterien über die Cyber Protection Service-Konsole definieren zu können.

25.5 URL-Filterung

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 Inhalte haben können. Die URL-Filterungsdatenbank enthält auch Daten über Websites mit strittigen Informationen über COVID-19, Scam- und Phishing-URLs. Solche Websites werden daher automatisch vom System geblockt, wenn ein Benutzer versucht, diese zu öffnen.

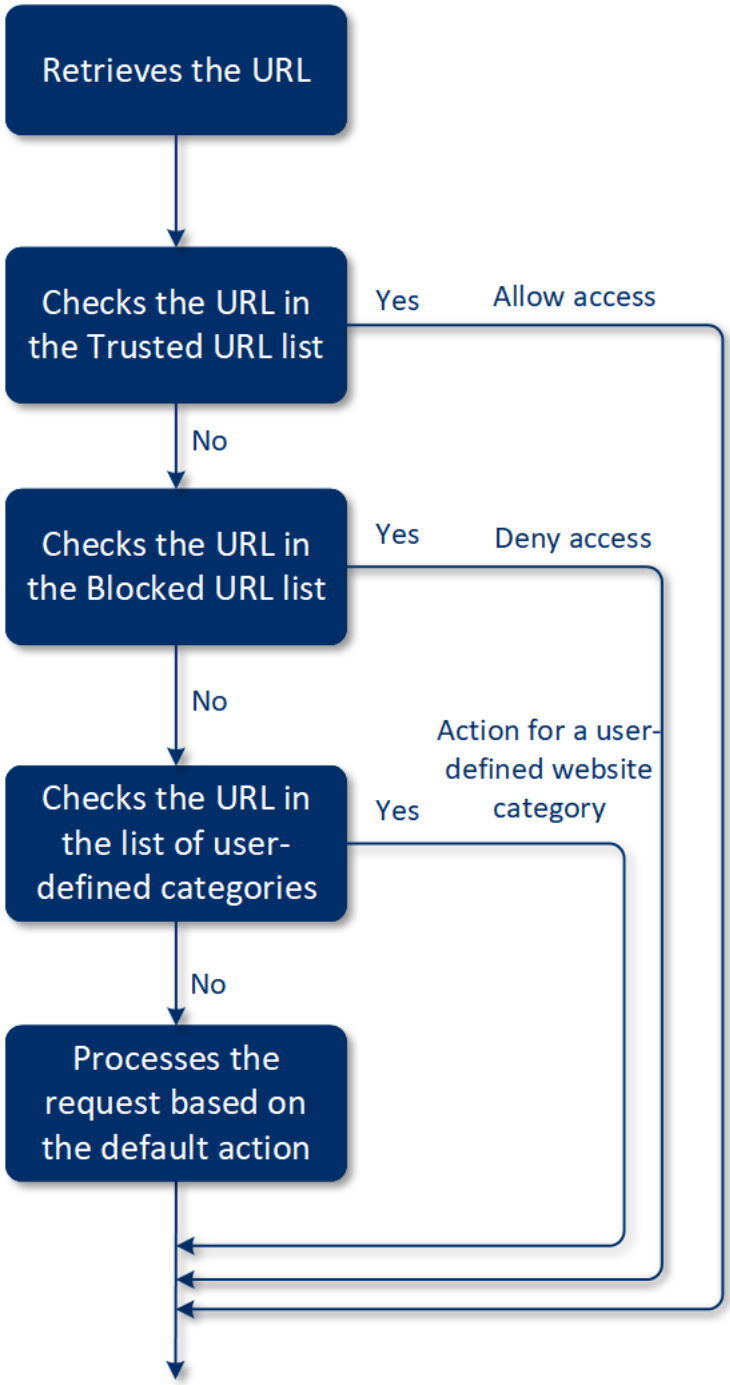
Sie können mit der URL-Filterung auch die Nutzung des Webs (WWWs) kontrollieren, um beispielsweise externe Vorschriften (wie gesetzliche Bestimmungen) oder interne Unternehmensrichtlinien einzuhalten. Sie können den Zugriff auf die Websites nach Kategorien konfigurieren, in die sich die Websiten einordnen 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.

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.

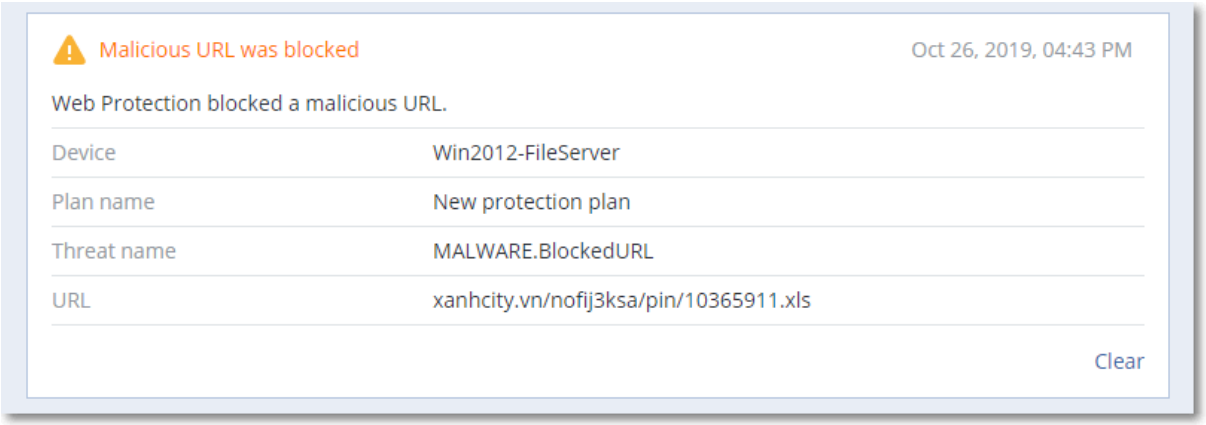


Die Konfiguration der URL-Filterung

Die Konfiguration der URL-Filterung besteht grundsätzlich aus den folgenden Schritten:

1. Sie erstellen einen Schutzplan (S. 105), 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 **Dashboard** –> **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:

- **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	**Nachrichten**	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. Es wird empfohlen, diese Kategorie zusammen mit der Kategorie 'Soziale Netzwerke' zu 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.

Ausschlusskriterien

Webadressen, von denen bekannt ist, dass sie sicher sind, können in eine Liste von vertrauenswürdigen URLs aufgenommen werden. Webadressen, die eine Bedrohung darstellen, können in eine Liste von blockierten URLs aufgenommen werden.

Wenn Sie eine Domain zur Liste der vertrauenswürdigen URLs aufnehmen wollen, müssen Sie in der Registerkarte **Vertrauenswürdig** auf den Befehl **Hinzufügen** klicken und dann die URL spezifizieren, indem Sie einen bestimmten Domain-Namen oder eine IP-Adresse verwenden.

Wenn Sie eine Domain zur Liste der blockierten URLs aufnehmen wollen, müssen Sie in der Registerkarte **Blockiert** auf den Befehl **Hinzufügen** klicken und dann die URL spezifizieren, indem Sie einen bestimmten Domain-Namen oder eine IP-Adresse verwenden.

***Hinweis**: Alle Adressen aus der Domain, die Sie eingegeben haben, werden als vertrauenswürdig oder blockiert (gesperrt) behandelt. Wenn Sie z.B. 'xyz.com' als vertrauenswürdige Domain eingegeben haben, werden auch alle Pfade bzw. Subdomains unterhalb von xyz.com als vertrauenswürdig behandelt.*

25.6 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

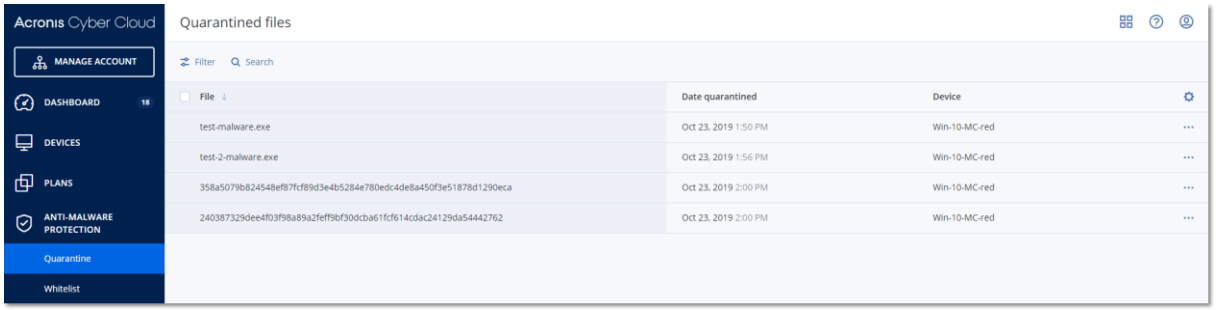
Wenn Sie die unter Quarantäne stehenden Dateien verwalten wollen, gehen Sie zu **Antimalware Protection** –> **Quarantäne**. Sie sehen eine Liste mit allen unter Quarantäne stehenden Dateien von allen Maschinen.

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.

- **Wiederherstellen** – die entsprechende, unter Quarantäne stehende Datei wird ohne Modifikationen zurück zu ihrem ursprünglichen Speicherort verschoben. Sollte sich am ursprünglichen Speicherort eine Datei mit gleichem Namen befinden, dann wird diese durch die wiederhergestellte Datei überschrieben. Beachten sie, dass die wiederhergestellte Datei der Positivliste hinzugefügt wird und daher bei weiteren Antimalware-Scans übersprungen wird.



Quarantäne-Speicherort auf den Maschinen

Der Standardspeicherort für die Quarantäne von verdächtigen Dateien ist:

Bei Windows-Maschinen: **`%ProgramData%\%product_name%\Quarantine`**

Bei Mac-/Linux-Maschinen: **`/usr/local/share/%product_name%/quarantine`**

Der Quarantäne-Speicherort wird durch die Selbstschutzfunktion (Self-Protection) des Service-Providers geschützt.

25.7 Positivliste für Unternehmensapplikationen

Firmen haben normalerweise unternehmensspezifische Applikationen, die von Antivirus-Lösungen als falsch-positiv erkannt und eingestuft werden können. Es kann außerdem zeitaufwendig sein, die vertrauenswürdigen Applikationen manuell in eine Positivliste aufzunehmen.

Cyber Protection kann den Prozess des Hinzufügens solcher Applikationen zu einer entsprechenden Positivliste automatisieren. Backups werden vom Antivirus & Antimalware Protection-Modul gescannt und die gescannten Daten werden analysiert, um solche Applikationen in eine Positivliste aufzunehmen und Falsch-Positiv-Erkennungen zu verhindern.

Wenn Sie vertrauenswürdige Applikationen in eine Positivliste auf unternehmensweiter Ebene aufnehmen, können Sie die weitere Scan-Performance verbessern. Die Positivliste wird für jeden Kunden allein auf Grundlage seiner Daten erstellt.

Automatisches Hinzufügen zur Positivliste

1. Zuerst sollten Sie ein Cloud-Scanning von Backups auf mindestens zwei Maschinen durchführen. Dies kann mithilfe von Backup-Scanning-Plänen (S. 414) durchgeführt werden.
2. Dann sollten Sie in den Einstellungen für die Positivliste die Option **Positivliste automatisch generieren** aktivieren.

Manuelles Hinzufügen zur Positivliste

Das manuelle Hinzufügen von Applikationen zur Positivliste ist nur verfügbar, wenn die Option **Positivliste automatisch generieren** aktiviert wurde.

1. Gehen Sie in der Service-Konsole zu **Antimalware Protection** –> **Positivliste**.
2. Klicken Sie auf **Datei hinzufügen**.

3. Spezifizieren Sie den Pfad zur Datei und klicken Sie auf **Hinzufügen**.

Einstellungen für die Positivliste

Sie können die Option **Positivliste automatisch generieren** aktivieren.

Dann können Sie eine der drei vertrauenswürdigen Regelstufen spezifizieren, die das Aggressionslevel der Heuristik definieren:

- **Niedrig** – Unternehmensapplikationen werden erst nach längerer Zeit und Überprüfung in die Positivliste aufgenommen. Solche Applikationen sind vertrauenswürdiger. Dieser Ansatz erhöht jedoch die Möglichkeit von falsch-positiven Erkennungen. Die Kriterien, nach denen eine Datei als sauber und vertrauenswürdig eingestuft wird, sind hoch.
- **Standard** – Unternehmensapplikationen werden der Positivliste entsprechend der empfohlenen Schutzstufe hinzugefügt, um mögliche falsch-positive Erkennungen zu reduzieren. Die Kriterien, nach denen eine Datei als sauber und vertrauenswürdig eingestuft wird, sind mittelstark.
- **Hoch** – Unternehmensapplikationen werden der Positivliste schneller hinzugefügt, um mögliche falsch-positive Erkennungen zu reduzieren. 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.

25.8 Antimalware-Scan von Backups

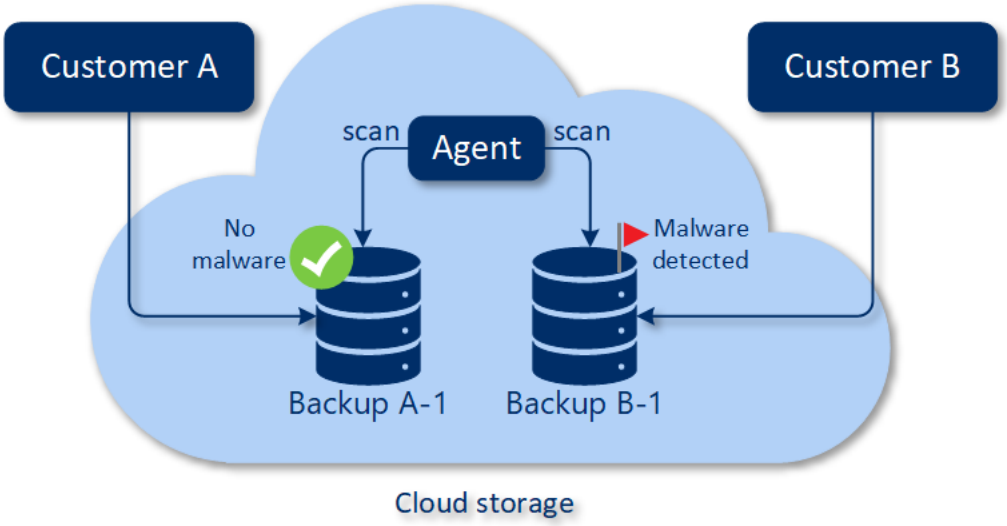
Durch die Backup-Scanning-Funktionalität können Sie verhindern, dass infizierte Dateien aus Backups wiederhergestellt werden. Durch Verwendung dieser Funktionalität können Sie überprüfen, ob Ihre Backups sauber sind (also nicht mit Malware infiziert). Die Backup-Scanning-Funktionalität wird nur für Windows-Betriebssysteme unterstützt.

Das Backup-Scanning wird vom Cloud Agenten in einer Umgebung außerhalb der entsprechenden Endbenutzer-Maschine durchgeführt, nämlich in der Acronis Cloud. Jeder neue Backup-Scanning-Plan erstellt einen neuen Scanning-Task. Dieser Task wird dann in eine gemeinsame Warteschlange für das aktuelle Datacenter gestellt und gemäß seiner Position in dieser Warteschlange ausgeführt. Die Dauer des jeweiligen Scan-Vorgangs hängt von der Backup-Größe ab. Daher kann es nach der Erstellung eines Backup-Scanning-Plans und dessen Ausführung zu gewissen Verzögerungen kommen.

Wenn kein Backup-Scanning durchgeführt wird, behalten die Backups den Status **Nicht gescannt**. Nachdem ein Backup-Scanning durchgeführt wurde, erhalten die Backups einen der folgenden Statuszustände:

- **Keine Malware**

- **Malware erkannt**



Das Backup-Scanning kann mithilfe eines Backup-Scanning-Plans konfiguriert werden.

So können Sie das Backup-Scanning in der Cloud konfigurieren

Beachten Sie Folgendes:

- Bei den Backup-Typen werden nur die Backup-Quellen 'Komplette Maschine' oder 'Laufwerke/Volumes' unterstützt.
- Es werden nur Volumes mit NTFS-Dateisystem und GPT- oder MBR-Partitionierung gescannt.
- Als Backup-Speicherort wird nur der Cloud Storage unterstützt (derzeit nur in der Konfiguration 'gehostet von Acronis').
- Backups, die CDP-Recovery-Punkte (S. 130) enthalten, können zwar zum Scannen ausgewählt werden, aber es werden nur reguläre Recovery-Punkte gescannt (die CDP-Recovery-Punkte werden also vom Scannen ausgeschlossen).
- Wenn ein CDP-Backup für die sichere Wiederherstellung (Safe Recovery) einer kompletten Maschine ausgewählt wurde, wird die Maschine ohne die Daten im CDP-Recovery-Punkt sicher wiederhergestellt. Wenn Sie die CDP-Daten wiederherstellen wollen, müssen Sie eine Wiederherstellung von Dateien/Ordnern starten.

Erstellen Sie einen Backup-Scanning-Plan (S. 414), um die Ausführung des Backup-Scannings in der Cloud zu konfigurieren.

Sie können Ergebnisse des Backup-Scannings auf dem Dashboard im Widget 'Backup-Scanning-Details (S. 427)' einsehen.

26 Schutz von Applikationen für Zusammenarbeit und Kommunikation

Zoom, Cisco Webex Meetings 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 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 Service-Konsole an und wenden Sie einen Schutzplan an (p. 113), für den eines der folgenden Module aktiviert ist:
   - **Antivirus & Antimalware Protection** (S. 360) (mit der **Active Protection**-Einstellung aktiviert) – wenn Sie eine der Cyber Protect-Editionen haben:
   - **Active Protection** (S. 367) – wenn Sie eine der Cyber Backup-Editionen haben.
1. [Optional] Konfigurieren das Modul **Patch-Verwaltung** (S. 389) 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

27 Schwachstellenbewertung und Patch-Verwaltung

27.1 Unterstützte Microsoft- und Dritthersteller-Produkte

Unterstützte Microsoft-Produkte

Windows-Betriebssysteme

- Windows 7 (Enterprise, Professional, Ultimate)
- Windows 8
- Windows 8.1
- Windows 10

Windows Server-Betriebssysteme

- 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 Sharepoint Server 2016
- Microsoft Sharepoint Server 2016

Unterstützte Dritthersteller-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

- MS Teams
- Zoom
- Skype
- Slack
- WebEx
- NordVPN
- TeamViewer

Weitere Informationen über unterstützte Dritthersteller-Produkte für Windows-Betriebssysteme finden Sie unter https://kb.acronis.com/content/62853.

27.2 Schwachstellenbewertung

Die **Schwachstellenbewertung** (SB, Englisch auch Vulnerability Assessment oder kurz VA) ist ein Prozess zum Identifizieren, Quantifizieren und Priorisieren Schwachstellen, die in einem untersuchten System gefunden werden. Mit dem Schwachstellenbewertungsmodul können Sie Ihre Maschinen nach Schwachstellen/Verwundbarkeiten (wie Sicherheitslücken) scannen lassen und sicherstellen, dass alle installierten Applikationen und die verwendeten Betriebssysteme aktuell sind und korrekt arbeiten.

Derzeit wird das Scannen nach Schwachstellen nur für Windows-Maschinen und Linux-Maschinen (CentOS 7/Virtuozzo/Acronis Cyber Infrastucture) unterstützt. Weitere Informationen über die Konfigurationen für Linux-Rechner finden Sie unter 'Schwachstellenbewertung für Linux-Maschinen (p. 388)'.

Und so funktioniert es

1. Sie erstellen einen Schutzplan (S. 105) mit aktiviertem Schwachstellenbewertungsmodul, spezifizieren die SB-Einstellungen (S. 386) und weisen den Plan den gewünschten Maschinen zu (S. 105).
2. Das System sendet (per Planung oder manuell ausgelöst) einen Befehl zur Ausführung des Scans nach Schwachstellen 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 das Scannen nach Schwachstellen 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 (S. 424) an und listet die gefundenen Schwachstellen auf.
6. Wenn Sie eine Liste von gefundenen Schwachstellen (S. 387) abrufen, können Sie diese verarbeiten und entscheiden, welche der gefundenen Schwachstellen behoben werden sollten.

Sie können die Ergebnisse des Scannens nach Schwachstellen im Widget **Dashboard** –> **Überblick** –> **Schwachstellen / Gefundene Schwachstellen** (S. 424) überwachen.

27.2.1 Einstellungen für die Schwachstellenbewertung

Eine Anleitung zum Erstellen eines Schutzplans mit aktiviertem Schwachstellenbewertungsmodul finden Sie im Abschnitt 'Einen Schutzplan erstellen (S. 105)'. Das Scannen nach Schwachstellen kann auf Basis einer Planung oder bei Bedarf/manuell (mithilfe der Aktion **Jetzt ausführen** in einem Schutzplan) ausgelöst werden

Für das Schwachstellenbewertungsmodul können folgende Einstellungen spezifiziert werden:

Scan-Umfang

Definieren Sie, welche Software-Produkte nach Schwachstellen gescannt werden sollen:

- Windows-Maschinen:
  - **Microsoft-Produkte**
  - **Windows-Produkte von Drittherstellern** (weitere Informationen über unterstützte Dritthersteller-Produkte für Windows-Betriebssysteme finden Sie unter https://kb.acronis.com/content/62853).
- Linux-Maschinen:
  - **Linux-Pakete scannen**

Planung

Definieren Sie eine Planung, auf deren Basis das Scannen nach Schwachstellen auf den ausgewählten Maschinen durchgeführt werden soll.

Die Task-Ausführung auf Basis folgender Ereignisse planen

- **Planung nach Zeit** – der Task wird zum spezifizierten Zeitpunkt ausgeführt.
- **Wenn sich ein Benutzer am System anmeldet** – die Task-Ausführung wird standardmäßig durch die Anmeldung eines jeden Benutzers ausgelöst. Sie können aber von 'Jeder Benutzer' zu einem bestimmten Benutzerkonto wechseln.
- **Wenn sich ein Benutzer vom System abmeldet** – die Task-Ausführung wird standardmäßig durch die Abmeldung eines jeden Benutzers ausgelöst. Sie können aber von 'Jeder Benutzer' zu einem bestimmten Benutzerkonto wechseln.

  Hinweis: *Der Task wird nicht beim Herunterfahren eines Systems ausgeführt, weil 'Herunterfahren' nicht dasselbe wie 'Abmelden' ist.*
- **Beim Systemstart** – der Task wird ausgeführt, wenn das Betriebssystem startet.
- **Beim Herunterfahren des Systems** – der Task wird ausgeführt, wenn das Betriebssystem herunterfährt.

Standardeinstellung: **Planung nach Zeit**.

Planungstyp:

- **Monatlich** – bestimmen Sie, an welchen Tagen in welchem Monat der Task ausgeführt werden soll.
- **Täglich** – bestimmen Sie, an welchen Wochentagen der Task ausgeführt werden soll.
- **Stündlich** – bestimmen Sie, an welchen Wochentagen und wie oft ein Task in einer Stunde ausgeführt werden soll.

Standardeinstellung: **Täglich**.

Starten um – bestimmen sie, zu welchem Zeitpunkt der Task ausgeführt werden soll.

Standardeinstellung: **14:00 Uhr** (auf der Maschine, auf welcher die Software installiert ist).

Innerhalb eines Zeitraums ausführen – bestimmten Sie einen Datumsbereich, wann die Planung gültig ist.

Startbedingungen – definieren Sie Bedingungen, die gleichzeitig zutreffen müssen, damit der Task gestartet werden kann. Sie ähneln den Startbedingungen für das Backup-Modul, die im Abschnitt 'Startbedingungen (S. 144)' beschrieben sind.

Folgende zusätzliche Startbedingungen können definiert werden:

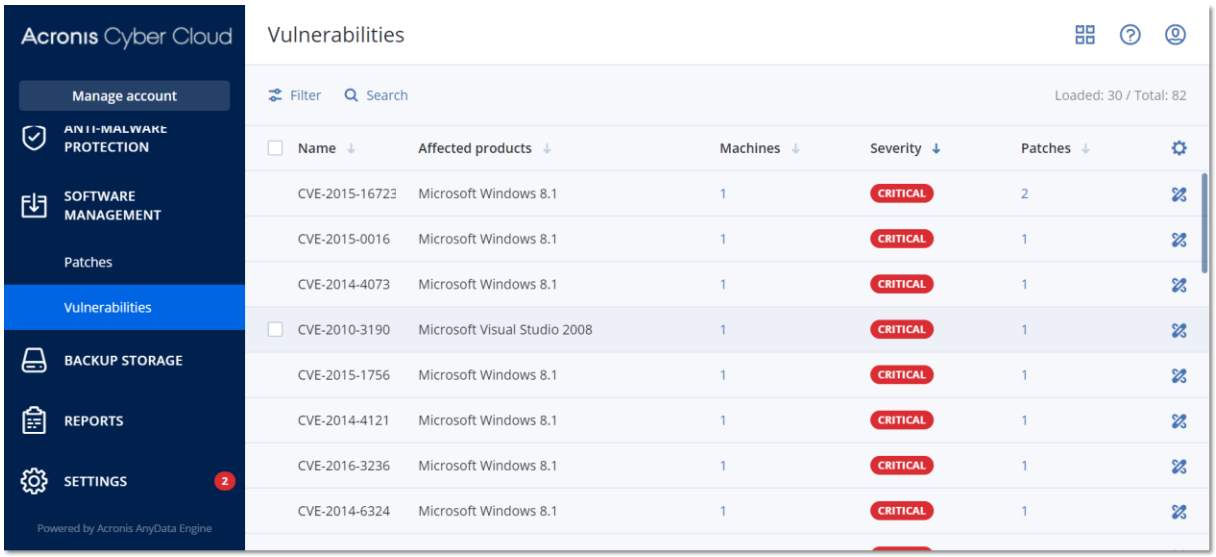
- **Task bei Neustart der Maschine ausführen, wenn die Maschine zur geplanten Zeit ausgeschaltet war**
- **Standby- oder Ruhezustandsmodus während der Task-Ausführung verhindern** – diese Option gilt nur für Maschinen, die unter Windows laufen.
- **Wenn die Startbedingungen nicht erfüllt sind, Task trotzdem ausführen nach:** – spezifizieren Sie einen Zeitraum (in Stunden), nachdem der Task dennoch gestartet werden soll.

27.2.2 Gefundene Schwachstellen verwalten

Wenn die Schwachstellenbewertung mindestens einmal durchgeführt wurde und Schwachstellen gefunden wurden, werden Ihnen diese unter **Software-Verwaltung** –> **Schwachstellen** angezeigt. 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 Service-Konsole in den Bereich **Software-Verwaltung** –> **Schwachstellen**.
2. Wählen Sie die Schwachstelle aus der Liste aus und klicken Sie auf **Patches installieren**. Der Assistent zur Schwachstellenbehebung wird geöffnet.
3. Wählen Sie die Patches aus, die auf den ausgewählten Maschinen installiert werden sollen. Klicken Sie auf **Weiter**.
4. Wählen Sie Maschinen aus, für die Sie Patches installieren wollen.
5. Bestimmen Sie, ob nach der Patch-Installation ein Maschinen-Neustart durchgeführt werden soll.
   - **Nein** – es wird kein Neustart nach der Update-Installation initiiert.
   - **Bei Bedarf** – es wird nur dann ein Neustart durchgeführt, wenn dies für die Anwendung der Updates erforderlich ist.
   - **Ja** – es wird immer ein Neustart nach der Update-Installation initiiert. Sie können in allen Fällen eine Verzögerung für den Neustart spezifizieren.

   Nicht neu starten, bevor das Backup abgeschlossen wurde – wenn der Backup-Prozess läuft, wird der Neustart der Maschine solange verzögert, bis das Backup abgeschlossen wurde.

   Klicken Sie, wenn Sie fertig sind, auf **Patches installieren**.

Als Ergebnis werden die ausgewählten Patches auf den ausgewählten Maschinen installiert.

27.2.3 Schwachstellenbewertung für Linux-Maschinen

Die Schwachstellenbewertung wird auch für Linux-Maschinen unterstützt. Sie können Linux-Maschinen nach Schwachstellen auf Applikations- und Kernel-Ebene scannen lassen.

Folgende Linux-Distributionen/-Versionen werden unterstützt:

- Virtuozzo 7.0.11
- Virtuozzo 7.0.10 (320)
- Virtuozzo 7.0.9 (539)
- Virtuozzo 7.0.8 (524)
- CentOS 7.x
- Acronis Cyber Infrastructure 3.x

- Acronis Storage 2.4.0
- Acronis Storage 2.2.0

So können Sie die Schwachstellenbewertung für Linux-Maschinen konfigurieren

1. Installieren Sie den Agenten für Linux auf dem Host von Acronis Cyber Infrastructure (oder Virtuozzo) oder in einer virtuellen Maschine mit CentOS.
2. Erstellen Sie in der Service-Konsole einen Schutzplan (S. 105) und aktivieren Sie das Modul für die **Schwachstellenbewertung**.
3. 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.
4. Weisen Sie den Maschinen den Plan zu (S. 105).

Als Ergebnis der Schwachstellenbewertung wird Ihnen eine Liste mit gefundenen Schwachstellen angezeigt (S. 387). Sie können diese bearbeiten und entscheiden, welche der gefundenen Schwachstellen behoben werden sollen.

Sie können die Ergebnisse der Schwachstellenbewertung im Widget **Dashboard** –> **Überblick** –> **Schwachstellen / Gefundene Schwachstellen** (S. 424) überwachen.

27.3 Patch-Verwaltung

Mithilfe der **Patch-Verwaltung** (PV) können Sie Patches/Updates für die Betriebssysteme und Applikationen verwalten, die auf Ihren Maschinen installiert sind, um Ihre Systeme so auf dem neuesten Stand zu halten. Das Patch-Verwaltungsmodul ermöglicht Ihnen, automatisch oder manuell zu genehmigen, welche Updates auf Ihren Maschinen installiert werden. Die Patch-Verwaltungsfunktionalität wird derzeit nur für Windows-Maschinen unterstützt.

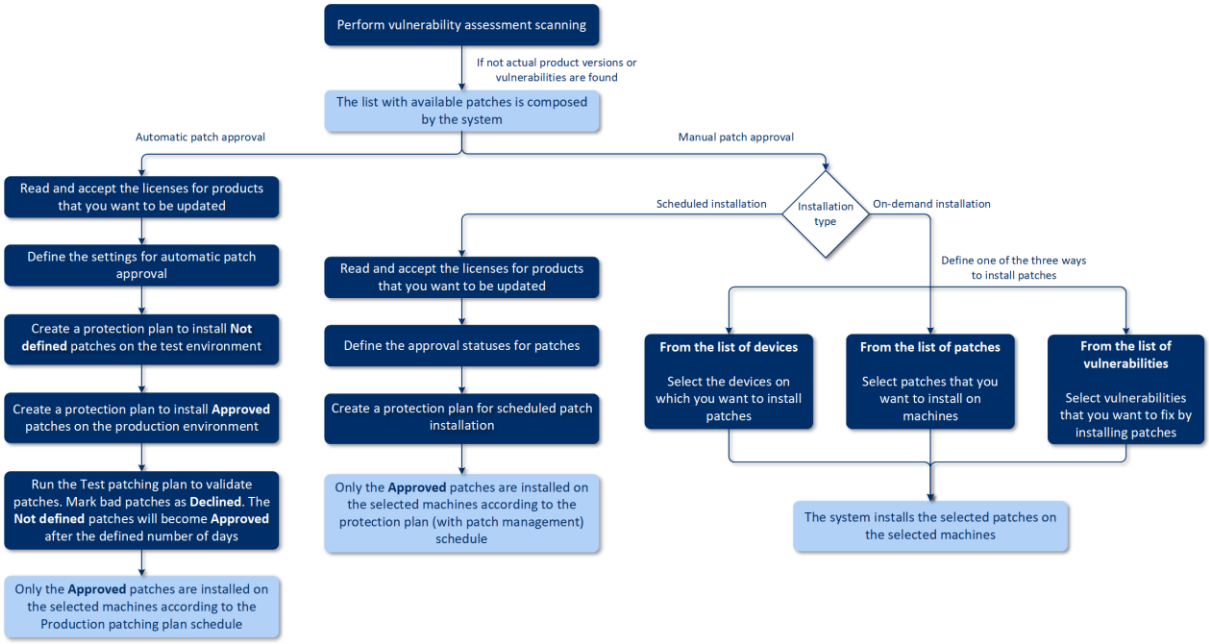
Die Patch-Verwaltungsfunktionalität ermöglicht Ihnen:

- So können Sie Updates auf Betriebssystem- und Applikationsebene installieren
- So können Sie Patches manuell oder automatisch genehmigen
- So können Sie Patches bei Bedarf (manuell) oder per Planung installieren
- So können Sie präzise nach verschiedenen Kriterien definieren, welche Patches angewendet werden: Schweregrad, Kategorie und Genehmigungsstatus
- So können Sie Backups vor den Updates durchführen, um möglichweise erfolglose Updates zu verhindern
- So können Sie die Neustart-Option definieren, die nach der Patch-Installation angewendet werden soll

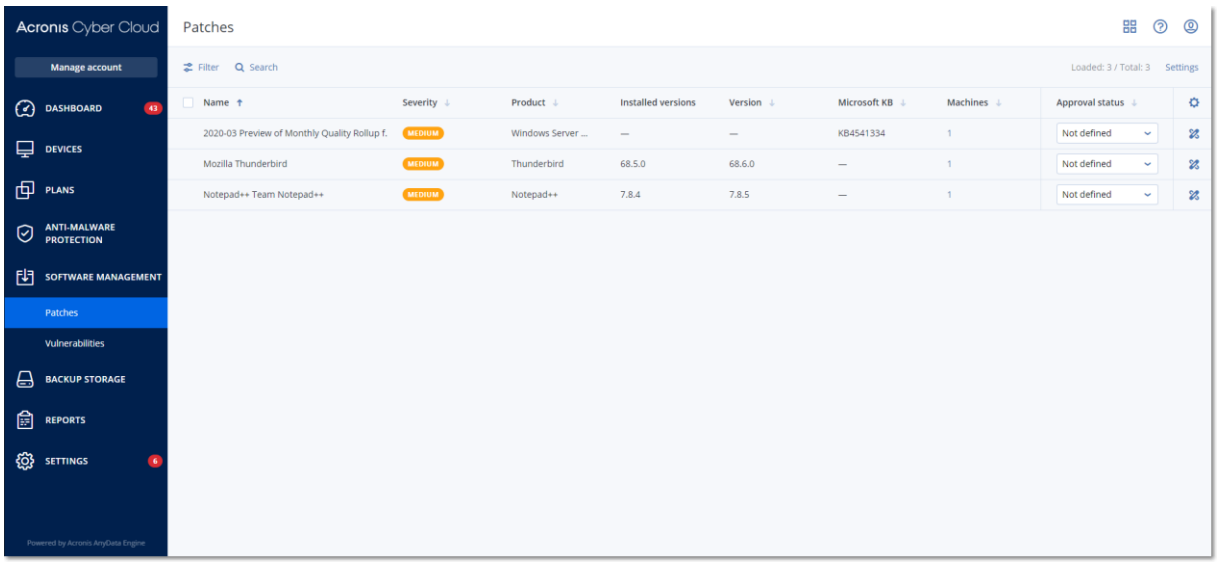
Mit Cyber Protection wurde eine Peer-zu-Peer-Technologie für Komponenten-Updates eingeführt, um die Bandbreite des Netzwerkverkehrs zu minimieren. Sie können einen oder mehrere dedizierte Agenten bestimmen, die Updates aus dem Internet herunterladen und für die anderen Agenten im Netzwerk bereitstellen sollen. Alle Agenten werden außerdem die Updates als Peer-zu-Peer-Agenten mit den anderen teilen.

Und so funktioniert es

Sie können entweder eine automatische oder manuelle Patch-Genehmigung konfigurieren. Das nachfolgende Schema verdeutlicht Ihnen sowohl automatische als auch manuelle Patch-Genehmigungs-Workflows.



1. Als erstes müssen Sie mindestens einen Schwachstellenbewertungsscan (S. 385) mithilfe eines Schutzplans durchführen, bei dem das Modul **Schwachstellenbewertung** aktiviert wurde. Nach erfolgtem Scan stellt das System die Listen der gefundenen Schwachstellen (S. 387) und der verfügbaren Patches zusammen.
2. Anschließend können Sie die automatische Patch-Genehmigung (S. 395) konfigurieren oder die manuelle Patch-Genehmigung (S. 398) verwenden.
3. Definieren Sie, wie die Patches installiert werden sollen – nach Planung oder bei Bedarf. Eine Patch-Installation bei Bedarf kann je nach Ihren Anforderungen auf drei Arten erfolgen:
   - Gehen Sie zur Liste der Patches (**Software-Verwaltung** –> **Patches**) und installieren Sie die erforderlichen Patches.



- Gehen Sie zur Liste der Schwachstellen (**Software-Verwaltung** –> **Schwachstellen**) und starten Sie den Prozess zur Schwachstellenbehebung, der auch die Installation der Patches umfasst.
- Gehen Sie zur Liste der Geräte (**Geräte** –> **Alle Geräte**), wählen Sie die zu aktualisierenden Maschinen aus und installieren Sie die Patches auf diesen.

Sie können die Ergebnisse der Patch-Installation im Widget **Dashboard** –> **Überblick** –> **Verlauf der Patch-Installation** überwachen.

27.3.1 Einstellungen für die Patch-Verwaltung

Eine Anleitung zum Erstellen eines Schutzplans mit aktiviertem Patch-Verwaltungsmodul finden Sie im Abschnitt 'Einen Schutzplan erstellen (S. 105)'. Sie können über den Schutzplan spezifizieren, welche Updates für Microsoft- und andere Drittthersteller-Produkte für Windows-Betriebssysteme auf den festgelegten Maschinen automatisch installiert werden sollen.

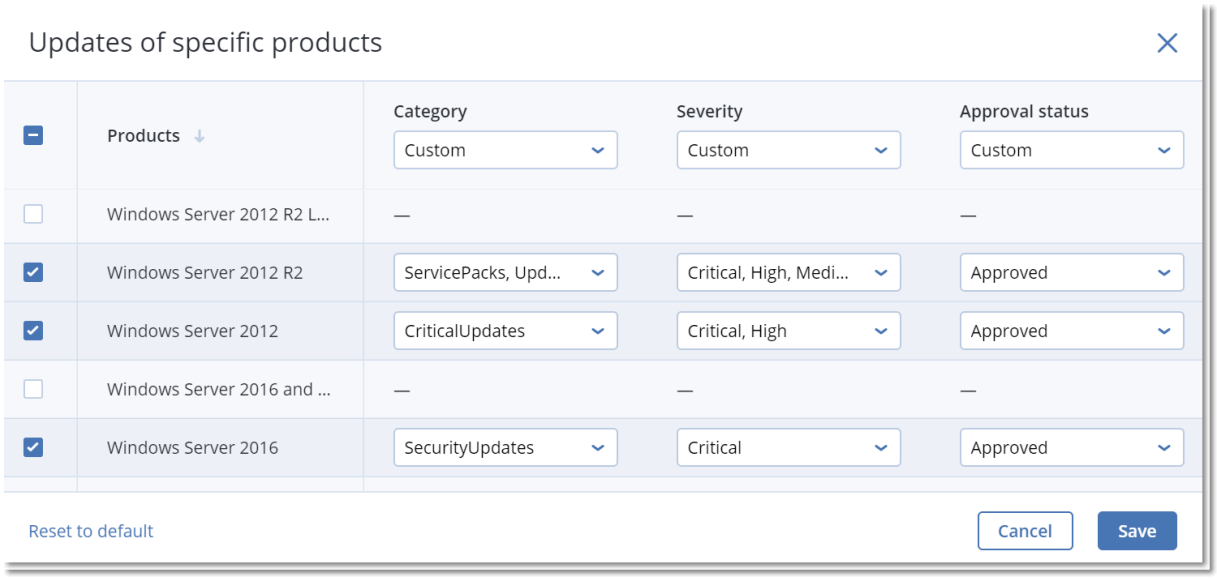
Für das Patch-Verwaltungsmodul können folgende Einstellungen spezifiziert werden:

Microsoft-Produkte

Wenn Sie Microsoft-Updates auf den ausgewählten Maschinen installieren lassen wollen, aktivieren Sie die Option **Microsoft-Produkte aktualisieren**.

Bestimmen Sie, welche Updates installiert werden sollen:

- **Alle Updates**
- **Nur kritische und Sicherheits-Updates**
- **Updates bestimmter Produkte**: Sie können benutzerdefinierte Einstellungen für verschiedene Produkte definieren. 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.

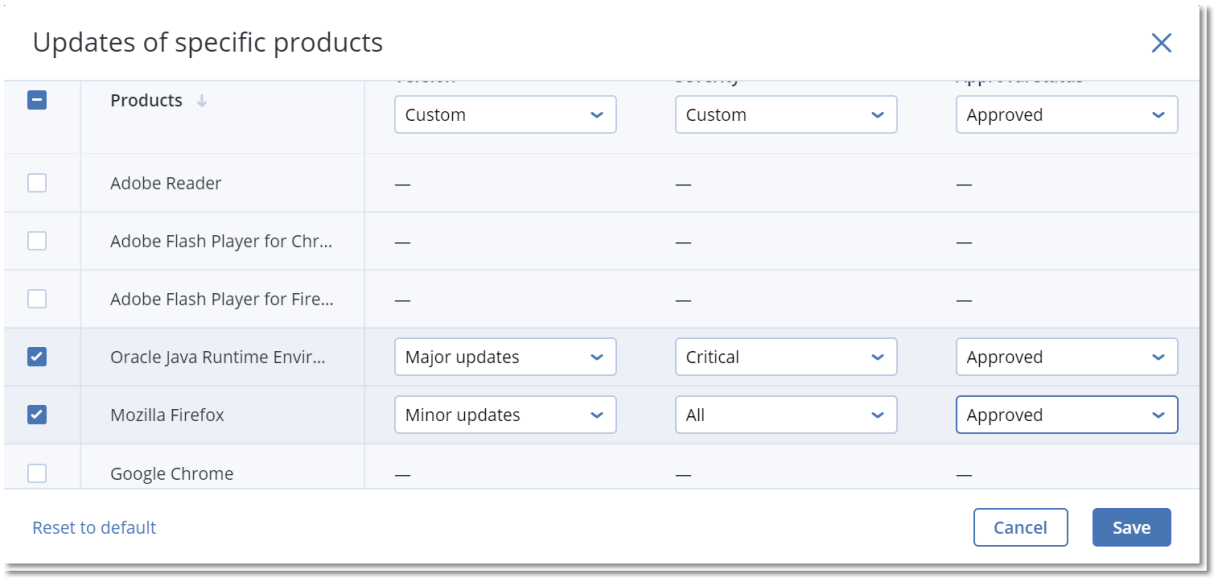


Windows-Produkte von Drittherstellern

Wenn Sie Drittthersteller-Updates für Windows-Betriebssysteme auf den ausgewählten Maschinen installieren lassen wollen, aktivieren Sie die Option **Windows-Produkte von Drittherstellern**.

Bestimmen Sie, welche Updates installiert werden sollen:

- **Nur letzte größere Updates** – ermöglicht Ihnen, die letzte (jüngste) verfügbare Version eines Updates zu installieren.
- **Nur letzte kleinere Updates** – ermöglicht Ihnen, die kleinere Version eines Updates zu installieren.
- **Updates bestimmter Produkte**: Sie können benutzerdefinierte Einstellungen für verschiedene Produkte definieren. 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.



Planung

Definieren Sie eine Planung, auf deren Basis die Updates auf den ausgewählten Maschinen installiert werden sollen.

Die Task-Ausführung auf Basis folgender Ereignisse planen

- **Planung nach Zeit** – der Task wird zum spezifizierten Zeitpunkt ausgeführt.
- **Wenn sich ein Benutzer am System anmeldet** – die Task-Ausführung wird standardmäßig durch die Anmeldung eines jeden Benutzers ausgelöst. Sie können aber von 'Jeder Benutzer' zu einem bestimmten Benutzerkonto wechseln.
- **Wenn sich ein Benutzer vom System abmeldet** – die Task-Ausführung wird standardmäßig durch die Abmeldung eines jeden Benutzers ausgelöst. Sie können aber von 'Jeder Benutzer' zu einem bestimmten Benutzerkonto wechseln.

  Hinweis: *Der Task wird nicht beim Herunterfahren eines Systems ausgeführt, weil 'Herunterfahren' nicht dasselbe wie 'Abmelden' ist.*

- **Beim Systemstart** – der Task wird ausgeführt, wenn das Betriebssystem startet.
- **Beim Herunterfahren des Systems** – der Task wird ausgeführt, wenn das Betriebssystem herunterfährt.

Standardeinstellung: **Planung nach Zeit**.

Planungstyp:

- **Monatlich** – bestimmen Sie, an welchen Tagen in welchem Monat der Task ausgeführt werden soll.
- **Täglich** – bestimmen Sie, an welchen Wochentagen der Task ausgeführt werden soll.
- **Stündlich** – bestimmen Sie, an welchen Wochentagen und wie oft ein Task in einer Stunde ausgeführt werden soll.

Standardeinstellung: **Täglich**.

Starten um – bestimmen sie, zu welchem Zeitpunkt der Task ausgeführt werden soll.

Standardeinstellung: **14:00 Uhr** (auf der Maschine, auf welcher die Software installiert ist).

Innerhalb eines Zeitraums ausführen – bestimmten Sie einen Datumsbereich, wann die Planung gültig ist.

Startbedingungen – definieren Sie Bedingungen, die gleichzeitig zutreffen müssen, damit der Task gestartet werden kann. Sie ähneln den Startbedingungen für das Backup-Modul, die im Abschnitt 'Startbedingungen (S. 144)' beschrieben sind.

Folgende zusätzliche Startbedingungen können definiert werden:

- **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 (in Stunden), nachdem der Task dennoch gestartet werden soll.

Nach dem Update neu starten – definiert, ob/wie ein Neustart nach der Installation der Updates initiiert wird:

- **Niemals** – es wird kein Neustart nach der Update-Installation initiiert.
- **Bei Bedarf** – es wird nur dann ein Neustart durchgeführt, wenn dies für die Anwendung der Updates erforderlich ist.
- **Immer** – es wird immer ein Neustart nach der Update-Installation initiiert. Sie können in allen Fällen eine Verzögerung für den Neustart spezifizieren.

Nicht neu starten, bevor das Backup abgeschlossen wurde – wenn der Backup-Prozess läuft, wird 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.

27.3.2 Die Liste der Patches verwalten

Nachdem ein Schwachstellenbewertungsscan durchgeführt wurde, können Sie die gefundenen verfügbaren Patches im Bereich **Software-Verwaltung** –> **Patches** finden.

Name	Beschreibung
Name	Der Name des Patches
Schweregrad	Der Schweregrad des Patches: ▪ **Kritisch** ▪ **Hoch** ▪ **Mittel** ▪ **Niedrig** ▪ **Ohne**
Anbieter	Der Anbieter oder Hersteller des Patches
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.
Microsoft KB	Wenn der Patch für ein Microsoft-Produkt ist, wird die entsprechende ID des dazugehörigen KB-Artikels angegeben

Veröffentlichungsdatum	Das Datum, an dem der Patch veröffentlicht wurde
Maschinen	Anzahl der betroffenen Maschinen
Genehmigungsstatus	Der Genehmigungsstatus wird hauptsächlich für das Szenario 'Automatische Genehmigung' benötigt und um im Schutzplan definieren zu können, welche Updates auf Basis ihres Status installiert werden sollen. 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 ▪ **Nicht definiert** – der Patch-Status ist unklar und sollte validiert werden
Lizenzvereinbarung	▪ Lesen und akzeptieren ▪ Keine Zustimmung. Wenn Sie der Lizenzvereinbarung nicht zustimmen, wird als Patch-Status **Abgelehnt** festgelegt und der Patch wird nicht installiert.
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

27.3.3 Automatische Patch-Genehmigung

Die automatische Patch-Genehmigung ermöglicht Ihnen, den Prozess der Update-Installation auf den Maschinen zu vereinfachen. Betrachten wir ein Beispiel.

Und so funktioniert es

Sie sollten zwei Umgebungen haben: Test und Produktion. Die Testumgebung dient dazu, die Patch-Installation zu testen und sicherzustellen, dass die Patches keine Schäden verursachen. Nachdem Sie die Patch-Installation in der Testumgebung ausprobiert haben, können Sie diese sicheren Patches in der Produktionsumgebung automatisch installieren lassen.

Konfiguration der automatischen Patch-Genehmigung

So können Sie die automatische Patch-Genehmigung konfigurieren

1. Sie müssen für jeden Anbieter/Hersteller, dessen Produkte Sie aktualisieren wollen, die Lizenzvereinbarungen lesen und akzeptieren. Ansonsten kann keine automatische Patch-Installation durchgeführt werden.
2. Konfigurieren Sie die Einstellungen für die automatische Genehmigung.
3. Erstellen Sie einen entsprechenden Schutzplan (S. 105) (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 **Nicht definiert** sein. Dieser Schritt ist erforderlich, um die Patches zu validieren und zu überprüfen, ob die Maschinen nach der Patch-Installation noch ordnungsgemäß funktionieren.

4. Erstellen Sie einen entsprechenden Schutzplan (S. 105) (beispielsweise mit der Bezeichnung 'Produktion patchen'), in dem das Modul **Patch-Verwaltung** aktiviert ist, und wenden Sie den Schutzplan auf die Maschinen in der Produktionsumgebung an. Spezifizieren Sie folgende Bedingung für die Patch-Installation: der Patch-Status muss **Genehmigt** sein.
5. Führen Sie den Schutzplan 'Patch-Test' aus und überprüfen Sie die Ergebnisse. Der Genehmigungsstatus für diejenigen Maschinen, die keine Probleme haben, kann mit **Nicht definiert** beibehalten werden – während der Status derjenigen Maschinen, die fehlerhaft arbeiten, mit **Abgelehnt** festgelegt werden sollte.
6. Entsprechend der Anzahl der Tage, die über die Option **Automatische Genehmigung** festgelegt wurden, werden diejenigen Patches, die bis dahin **Nicht definiert** waren, auf den Status **Genehmigt** geändert.
7. Wenn der Schutzplan 'Produktion patchen' gestartet wird, werden nur Patches mit dem Status **Genehmigt** auf den Produktionsmaschinen installiert.

Die manuellen Schritte werden nachfolgend aufgeführt.

Schritt 1: Lesen und akzeptieren Sie die Lizenzvereinbarungen für die Produkte, die Sie aktualisieren wollen

1. Gehen Sie in der Service-Konsole in den Bereich **Software-Verwaltung** –> **Patches**.
2. Wählen Sie den gewünschten Patch und lesen und akzeptieren Sie dann die Lizenzvereinbarung.

Schritt 2: Konfigurieren Sie die Einstellungen für die automatische Genehmigung

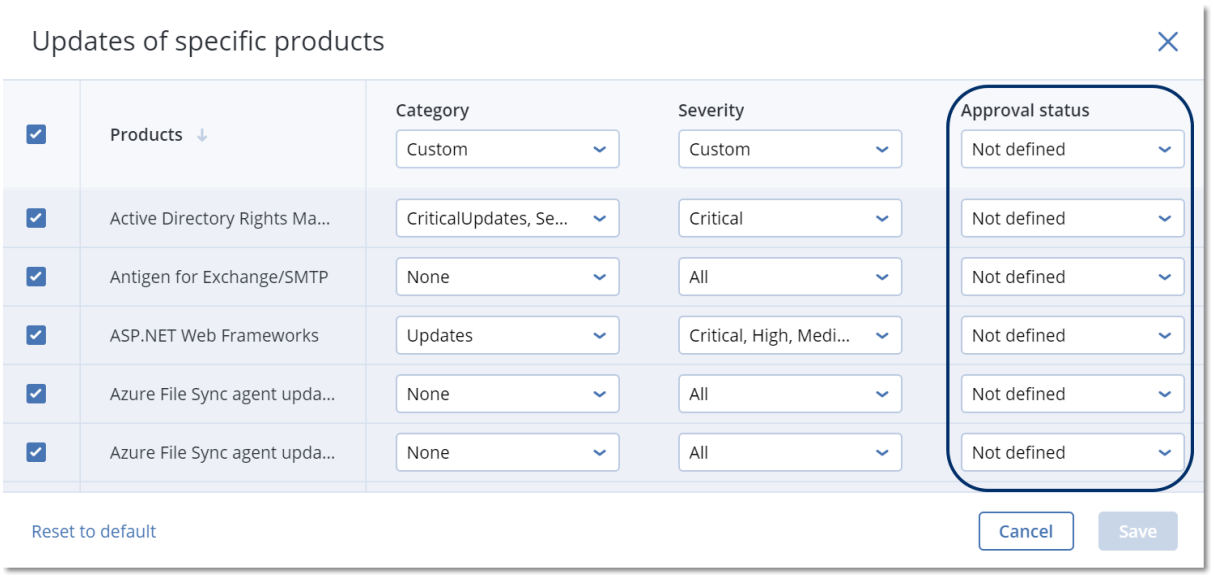
1. Gehen Sie in der Service-Konsole in den Bereich **Software-Verwaltung** –> **Patches**.
2. Klicken Sie auf **Einstellungen**.
3. Aktivieren Sie die Option **Automatische Genehmigung** und spezifizieren Sie die Anzahl der Tage. Das bedeutet, dass nach der spezifizierten Anzahl von Tagen (ab dem ersten Versuch der Patch-Installation) die Patches mit dem Status **Nicht definiert** automatisch auf **Genehmigt** geändert werden.

   Nehmen wir beispielsweise an, Sie spezifizieren 10 Tage. Sie haben den Schutzplan 'Patch-Test' für die Testmaschinen durchgeführt und die Patches wurden installiert. Diejenigen Patches, die die Maschinen offensichtlich beschädigt haben, wurden von Ihnen mit **Abgelehnt** gekennzeichnet, während die übrigen Patches den Status **Nicht definiert** behalten. Nachdem 10 Tage verstrichen sind, werden die Patches mit dem Status **Nicht definiert** automatisch auf den Status **Genehmigt** umgeschaltet.
4. Aktivieren Sie die Option **Lizenzvereinbarungen automatisch akzeptieren**. Dies ist erforderlich, um während der Patch-Installation die Lizenzvereinbarung automatisch akzeptieren zu können, damit der jeweilige Benutzer diese nicht manuell bestätigen muss.

Schritt 3: Erstellen Sie den Schutzplan zum Testen der Patches

1. Gehen Sie in der Service-Konsole zu **Pläne** –> **Schutz**.
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 über diese Einstellungen finden Sie im Abschnitt 'Einstellungen für die Patch-Verwaltung (S. 391)'.

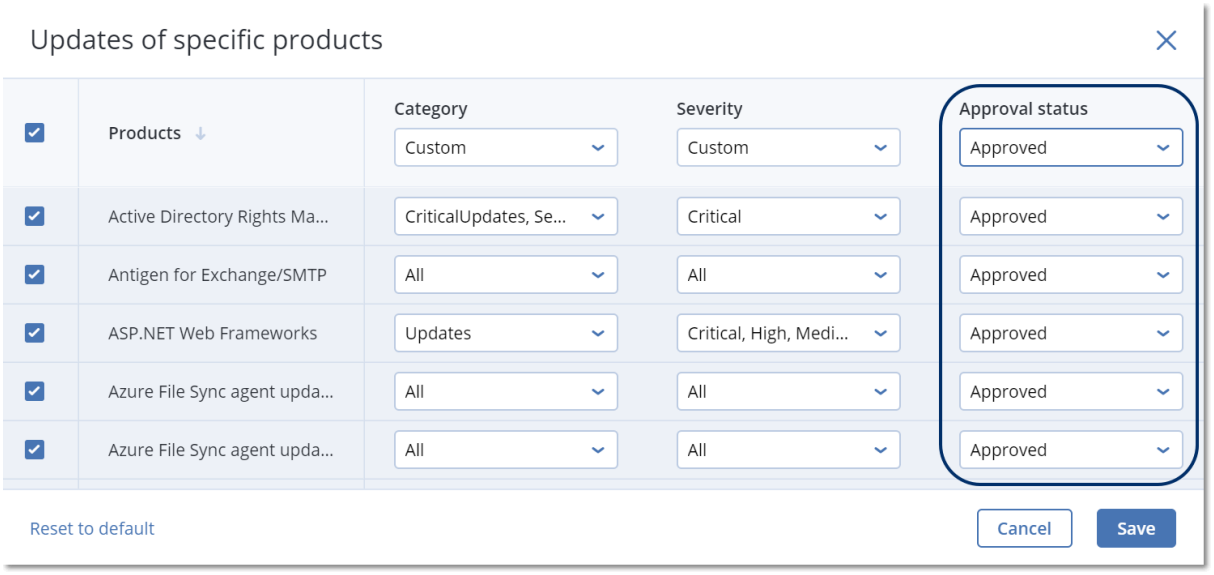
***Wichtig**: Definieren Sie für alle zu aktualisierenden Produkte den **Genehmigungsstatus** als **Nicht definiert**. Wenn der Zeitpunkt zur Aktualisierung gekommen ist, wird der Agent nur Patches mit dem Status **Nicht definiert** auf den ausgewählten Maschinen in der Testumgebung installieren.*



Schritt 4: Erstellen Sie den Schutzplan zum Patchen der Produktionsumgebung

1. Gehen Sie in der Service-Konsole zu **Pläne** –> **Schutz**.
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 über diese Einstellungen finden Sie im Abschnitt 'Einstellungen für die Patch-Verwaltung (S. 391)'.

***Wichtig**: Definieren Sie für alle zu aktualisierenden Produkte den **Genehmigungsstatus** als **Genehmigt**. Wenn der Zeitpunkt zur Aktualisierung gekommen ist, wird der Agent nur Patches mit dem Status **Genehmigt** auf den ausgewählten Maschinen in der Produktionsumgebung installieren.*



Schritt 5: Führen Sie den Schutzplan 'Patch-Test' aus und überprüfen Sie die Ergebnisse

1. Führen Sie den Schutzplan zum Patchen der Testumgebung aus (nach Planung oder bei Bedarf/manuell).
2. Überprüfen Sie anschließend, welche der installierten Patches sicher sind und welche nicht.
3. Gehen Sie zu **Software-Verwaltung** –> **Patches** und legen Sie den **Genehmigungsstatus** der nicht sicheren Patches als **Abgelehnt** fest.

27.3.4 Manuelle Patch-Genehmigung

Der Prozess einer manuellen Patch-Genehmigung verläuft folgendermaßen:

1. Gehen Sie in der Service-Konsole in den Bereich **Software-Verwaltung** –> **Patches**.
2. Wählen Sie die zu installierenden Patches aus und lesen und akzeptieren Sie dann die Lizenzvereinbarungen.
3. Legen Sie den **Genehmigungsstatus** für diejenigen Patches, deren Installation Sie erlauben wollen, als **Genehmigt** fest.
4. Erstellen Sie einen Schutzplan mit aktiviertem Patch-Verwaltungsmodul (S. 391). Sie können entweder eine Planung konfigurieren oder den Plan bei Bedarf/manuell starten, indem Sie in den Einstellungen des Patch-Verwaltungsmoduls auf **Jetzt ausführen klicken**.

Als Ergebnis werden nur die genehmigten Patches auf den ausgewählten Maschinen installiert.

27.3.5 Patch-Installation bei Bedarf

Eine Patch-Installation bei Bedarf kann je nach Ihren Anforderungen auf drei Arten erfolgen:

- Gehen Sie zur Liste der Patches (**Software-Verwaltung** –> **Patches**) und installieren Sie die erforderlichen Patches.
- Gehen Sie zur Liste der Schwachstellen (**Software-Verwaltung** –> **Schwachstellen**) und starten Sie den Prozess zur Schwachstellenbehebung, der auch die Installation der Patches umfasst.
- Gehen Sie zur Liste der Geräte (**Geräte** –> **Alle Geräte**), wählen Sie die zu aktualisierenden Maschinen aus und installieren Sie die Patches auf diesen.

Betrachten wir die Patch-Installation aus der Liste der Patches:

1. Gehen Sie in der Service-Konsole in den Bereich **Software-Verwaltung** –> **Patches**.
2. Akzeptieren Sie die Lizenzvereinbarungen derjenigen Patches, die Sie installieren wollen.
3. Wählen Sie die zu installierenden Patches aus und klicken Sie dann auf den Befehl **Installieren**.
4. Bestimmen Sie die Maschinen, auf denen die Patches installiert werden sollen.

   Wenn Sie für den Fall, dass die Patch-Installation das System beschädigt, eine Rollback-Funktion haben wollen, dann aktivieren Sie die Option **Backup vor der Installation von Software-Updates ausführen**. Das System überprüft daraufhin direkt, ob es einen Schutzplan mit aktiviertem Backup-Modul gibt (wobei als Backup-Quelle 'Komplette Maschine' festgelegt sein muss). Wenn der entsprechenden Maschine kein solcher Schutzplan zugewiesen wurde, wird sie mit einem roten Symbol gekennzeichnet. Sie können dann die Auswahl dieser Maschinen aufheben und fortfahren.
5. Definieren Sie, ob/wie nach der Installation der Patches ein Neustart initiiert werden soll:
   - **Niemals** – es wird kein Neustart nach der Patch-Installation initiiert.

- **Bei Bedarf** – es wird nur dann ein Neustart durchgeführt, wenn dies für die Anwendung der Patches erforderlich ist.
- **Immer** – es wird immer ein Neustart nach der Patch-Installation initiiert. Sie können in allen Fällen eine Verzögerung für den Neustart spezifizieren.

Nicht neu starten, bevor das Backup abgeschlossen wurde – wenn der Backup-Prozess läuft, wird der Neustart der Maschine solange verzögert, bis das Backup abgeschlossen wurde.

6. Klicken Sie auf **Patches installieren**.

Die ausgewählten Patches werden auf den ausgewählten Maschinen installiert.

27.3.6 Patch-Lebensdauer in der Liste

Wenn Sie die Liste der Patches aktuell halten wollen, gehen Sie zu **Software-Verwaltung** –> **Patches** –> **Einstellungen** und spezifizieren Sie die Option **Lebensdauer in der Liste**.

Die Option **Lebensdauer in der Liste** definiert, wie lange ein erkannter verfügbarer Patch in der Patch-Liste vorgehalten wird. Normalerweise wird ein Patch aus der Liste entfernt, wenn dieser erfolgreich auf allen Maschinen installiert wurde, auf denen seine Abwesenheit festgestellt wurde oder die festgelegte Zeit verstrichen ist.

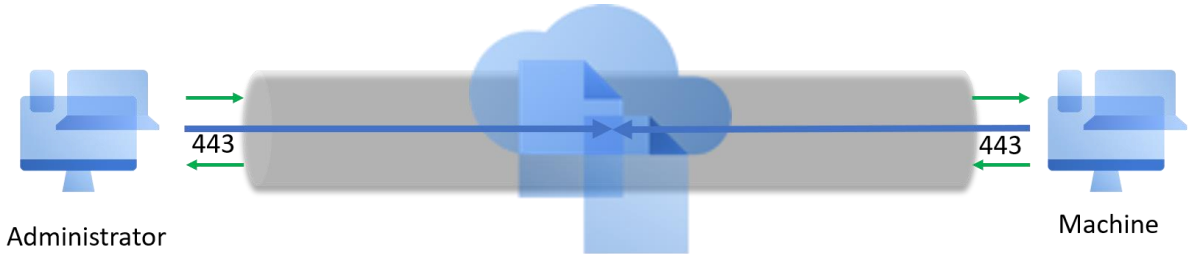
- **Unbegrenzt** – der Patch wird nie aus der Liste entfernt.
- **7 Tage** – der Patch wird entfernt, wenn sieben Tage nach der ersten Installation verstrichen sind.

  Beispiel: Sie haben zwei Maschinen, auf denen Patches installiert werden müssen. Eine davon ist online, die andere jedoch 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 entfernt, wenn dreißig Tage nach der ersten Installation verstrichen sind.

28 Remote-Desktop-Zugriff

28.1 Remote-Zugriff (RDP- und HTML5-Clients)

Cyber Protection ermöglicht Ihnen Remote-Zugriffe auf Maschinen. Sie können sich remote (aus der Ferne) mit Ihren Endbenutzer-Maschinen verbinden und diese verwalten. Mit dem HTML5-Client können Sie in beiden Richtungen Texte über die Zwischenablage mit der Remote-Maschine austauschen (kopieren und einfügen). Mit dem RDP-Client können Sie neben Texten auch Dateien über die Zwischenablage austauschen (kopieren und einfügen). Dies ermöglicht Ihnen, Ihren Endbenutzern bei der Lösung von Problemen auf deren Maschinen zu helfen.

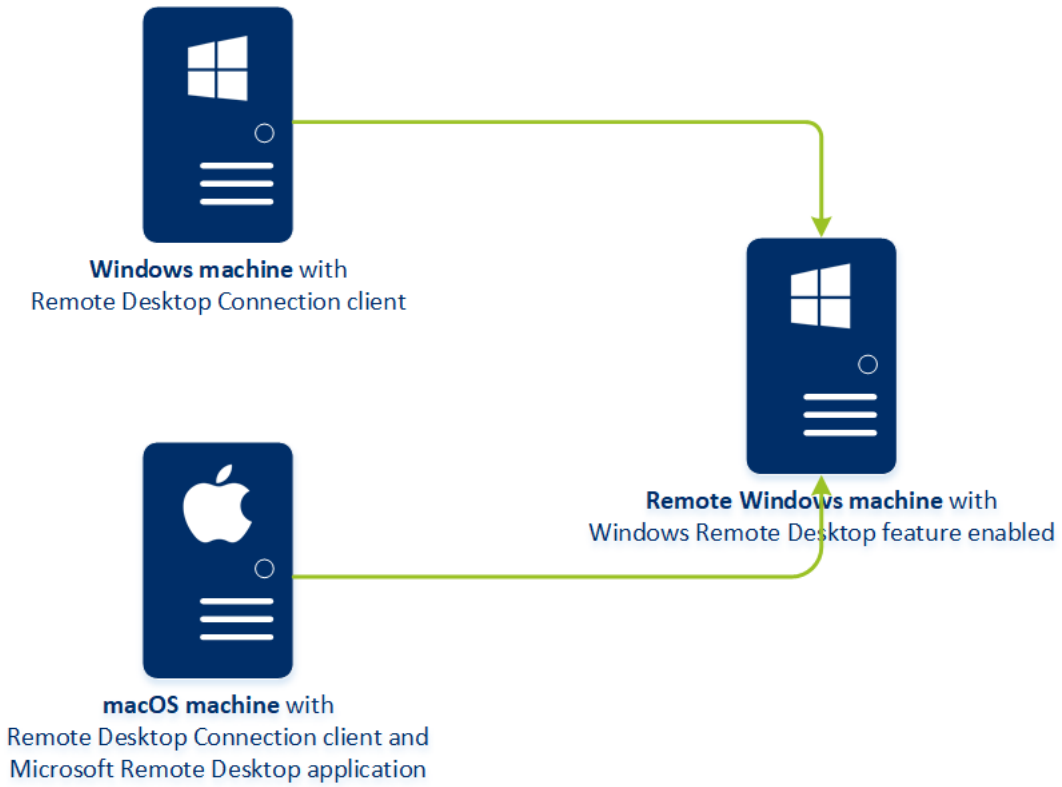


Cloud Connection broker

Voraussetzungen:

- Eine Remote-Maschine ist in Cyber Protection registriert und der Protection Agent ist auf der Maschine installiert.
- Die Cyber Protect-Quota ist vorhanden oder wurde bereits für eine Maschine übernommen.
- Bei RDP-Verbindungen wird der Remote-Desktop-Verbindungsclient auf einer Maschine installiert, von der aus die Verbindung gestartet wird.

Eine RDP-Sitzung kann von Windows- und macOS-Maschinen aus hergestellt werden. Eine HTML5-Remote-Verbindungssitzung kann über jeden Browser mit HTML5-Unterstützung hergestellt werden.



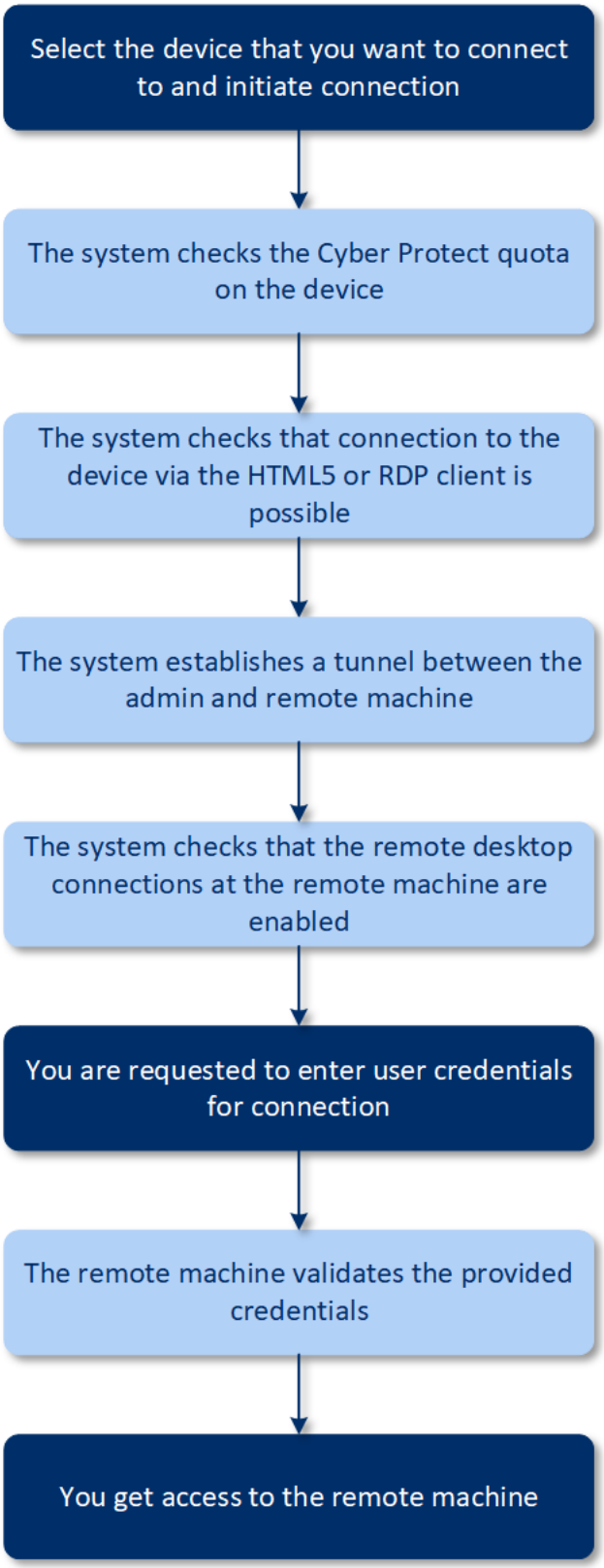
Die Remote-Zugriffsfunktionalität kann nur für Verbindungen mit Windows-Maschinen verwendet werden, auf denen die Windows-Remote-Desktop-Unterstützung aktiviert ist. Daher ist beispielsweise kein Remote-Zugriff auf Systeme mit Windows 10 Home oder macOS möglich.

Wenn Sie eine Verbindung von einer macOS-Maschine aus zu einer Remote-Maschine aufbauen wollen, sollten Sie sicherstellen, dass auf der macOS-Maschine folgende Applikationen installiert sind:

- Der Remote-Desktop-Verbindungsclient
- Die Microsoft Remote-Desktop-Applikation

Und so funktioniert es

Wenn Sie eine Remote-Verbindung zu einer Maschine aufbauen wollen, prüft das System zuerst, ob diese Maschine über die Cyber Protect-Quota verfügt. Danach überprüft das System, ob eine Verbindung per HTML5- oder RDP-Client möglich ist. Sie initiieren eine Verbindung über den RDP- oder HTML5-Client. Das System baut einen Tunnel zur Remote-Maschine auf und überprüft, ob die Remote-Desktop-Unterstützung auf der Remote-Maschine aktiviert ist. Anschließend geben Sie die entsprechenden Anmeldedaten ein und erhalten, sofern die Anmeldedaten korrekt waren, Zugriff auf die Maschine.



So können Sie sich mit einer Remote-Maschine verbinden

Gehen Sie folgendermaßen vor, um eine Remote-Verbindung mit einer Maschine herzustellen:

1. Gehen Sie in der Service-Konsole zu **Geräte** –> **Alle Geräte**.

2. Klicken Sie auf die Maschine, auf die Sie aus der Ferne zugreifen wollen, und klicken Sie dann auf **Über RDP-Client verbinden** / **Über HTML5-Client verbinden**.
3. [Optional, nur für Verbindungen über den RDP-Client] Laden Sie den Remotedesktopverbindungs-Client von Microsoft herunterladen und installieren Sie diesen. Initiieren Sie die Verbindung mit der Remote-Maschine.
4. Spezifzieren Sie die Anmeldedaten (Benutzername, Kennwort), um auf die Maschine zugreifen zu können, und klicken Sie dann auf den Befehl **Verbinden**.

Als Ergebnis erhalten Sie Fernzugriff auf die Remote-Maschine und können Sie diese verwalten.

So können Sie eine Remote-Unterstützungssitzung ausführen

Eine Remote-Unterstützung ermöglicht den gleichzeitigen Zugriff auf dieselbe Remote-Desktop-Sitzung. Wenn Sie beispielsweise ein Problem auf dem Computer eines Remote-Benutzers beheben müssen, können Sie die Verbindung mit diesem Computer über die Remote-Unterstützung aufbauen. Der Benutzer und der Remote-Administrator teilen sich eine Sitzung und der Benutzer kann sein Problem vermitteln und demonstrieren.

1. Gehen Sie in der Service-Konsole zu **Geräte** –> **Alle Geräte**.
2. Klicken Sie auf diejenige Maschine, mit der Sie sich remote verbinden wollen, und klicken Sie dann auf **Remote-Unterstützung ausführen**.
3. Kopieren Sie das Kennwort für die Remote-Unterstützungssitzung und klicken Sie dann auf **Verbinden**. Wenn die Sitzung nicht gestartet wird, laden Sie den Connectivity Agent auf der Remote-Maschine herunter, installieren Sie ihn und versuchen Sie dann, die Verbindung erneut aufzubauen.
4. Wenn es laufende interaktive Sitzungen gibt, klicken Sie auf **Mit Sitzung verbinden**.
5. Geben Sie das Kennwort für die Remote-Unterstützungssitzung ein.

Als Ergebnis erhalten Sie Remote-Desktop-Zugriff auf die entfernte Maschine und können den entsprechenden Benutzer dann unterstützen.

28.2 Remote-Verbindungen für Endbenutzer freigeben

Mitarbeiter, die im Home-Office arbeiten, benötigen manchmal Zugriff auf ihren Arbeitscomputer. Es kann jedoch vorkommen, dass Ihr Unternehmen kein konfiguriertes VPN oder andere Tools für Remote-Verbindungen hat.

Der Cyber Protection Service bietet Ihnen die Möglichkeit, eine RDP-Link für Endbenutzer freizugeben und diesen so den Remote-Zugriff auf ihre Maschinen zu ermöglichen.

So können Sie die Funktionalität zur Freigabe von Remote-Verbindungen aktivieren

Gehen Sie folgendermaßen vor, um die Funktionalität zur Freigabe von Remote-Verbindungen zu aktivieren:

1. Gehen Sie in der Service-Konsole zum Bereich **Einstellungen** –> **Schutz** –> **Remote-Verbindung**.
2. Aktivieren Sie die Option **Remote-Desktop-Verbindung freigeben**.

Als Ergebnis erscheint im rechten Menü die neue Option **Remote-Verbindung freigeben**, wenn Sie ein Gerät auswählen.

So können Sie eine Remote-Verbindung für Ihre Benutzer freigeben

Gehen Sie folgendermaßen vor, um eine Remote-Verbindung für einen Benutzer freizugeben:

1. Gehen Sie in der Service-Konsole zu **Geräte** –> **Alle Geräte**.
2. Wählen Sie das Gerät aus, zu dem Sie eine Remote-Verbindung bereitstellen wollen.
3. Klicken Sie im geöffneten rechten Menü auf den Befehl **Remote-Verbindung freigeben**.
4. Klicken Sie auf **Link abrufen**. Kopieren Sie im geöffneten Fenster den generierten Link. Dieser Link kann einem Benutzer bereitgestellt werden, der einen Remote-Zugriff auf dieses Gerät benötigt. Der Link ist 10 Stunden lang gültig.

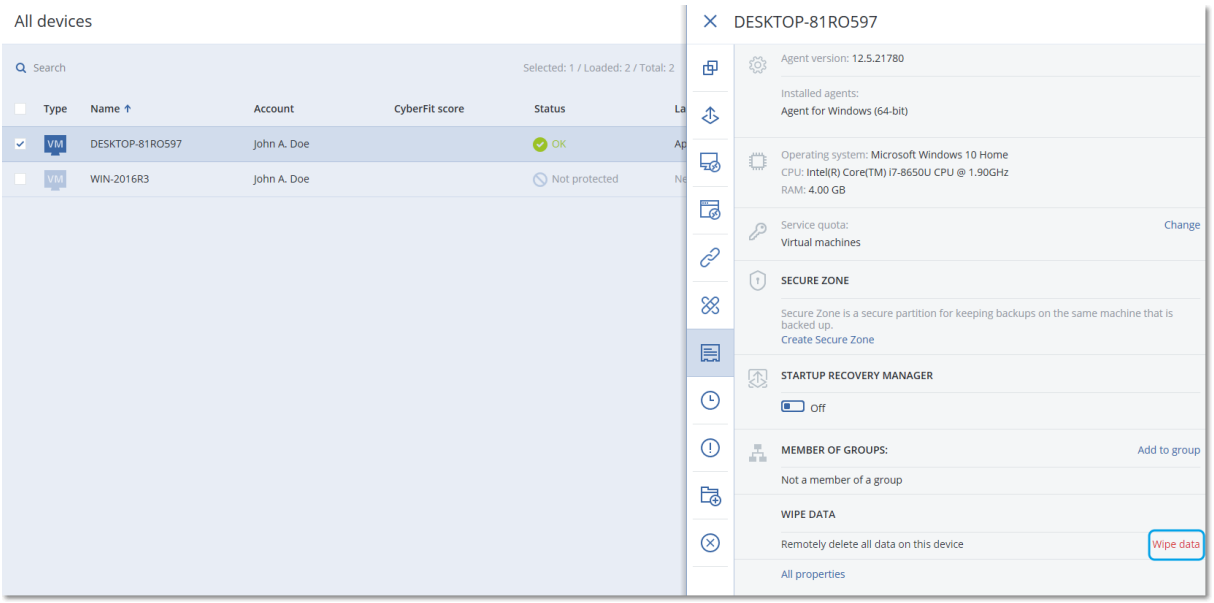
Nachdem Sie den Link abgerufen haben, können Sie diesen per E-Mail oder über andere Kommunikationsmittel mit Ihrem Benutzer teilen. Wenn dieser Benutzer auf den Link klickt, wird er auf eine Seite weitergeleitet, wo er den Verbindungstyp auswählen muss:

- Über RDP-Client verbinden. Bei diesem Verbindungstyp wird der Benutzer aufgefordert, den Remotedesktopverbindungs-Client herunterzuladen und zu installieren.
- Über HTML5-Client verbinden. Bei diesem Verbindungstyp ist es nicht notwendig, einen RDP-Client auf der Maschine des Benutzers zu installieren. Der Benutzer wird zu einem Anmeldefenster weitergeleitet, wo er die Anmeldedaten für die Remote-Maschine eingeben muss.

29 Remote-Löschung

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 10 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 Service-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**.

***Tipp**: Über **Dashboard** –> **Aktivitäten** können Sie Details zum Löschvorgang und wer diesen gestartet einsehen.*

30 Smart Protection

30.1 Bedrohungsfeed

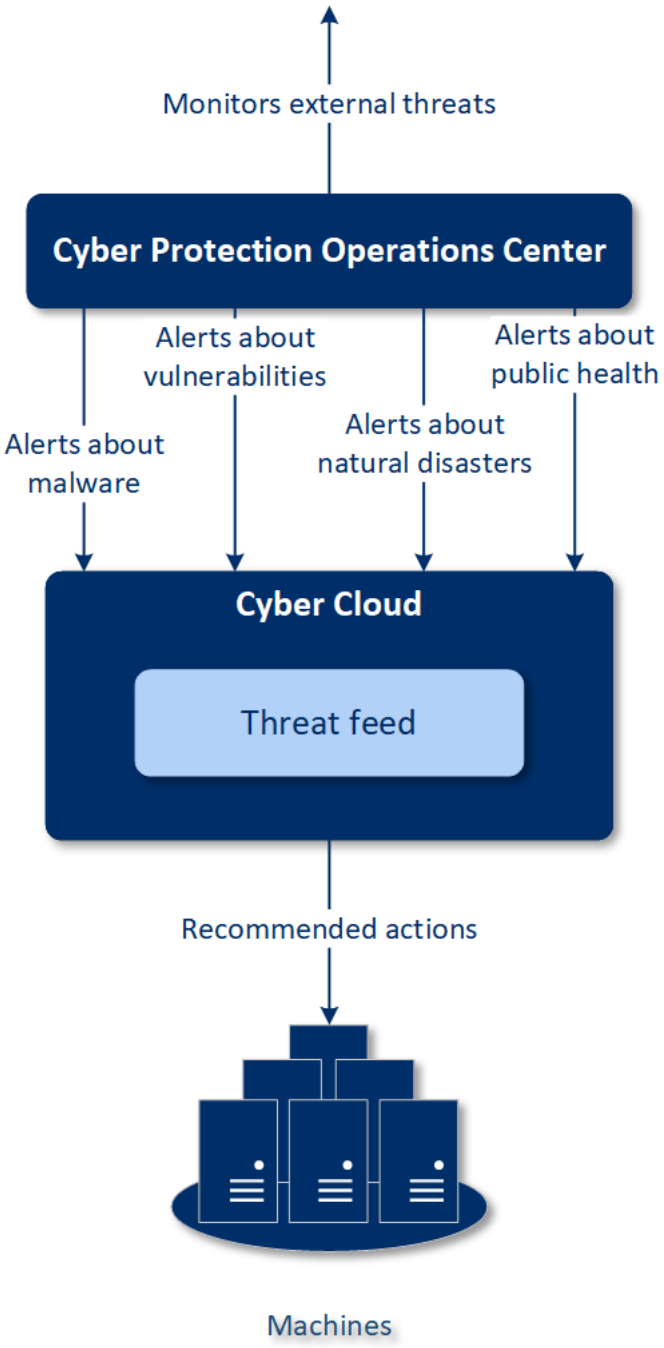
Das Acronis Cyber Protection Operations Center (CPOC) generiert Sicherheitsalarmmeldungen, die nur zu entsprechenden geographischen Regionen gesendet werden. Diese Sicherheitsmeldungen liefern Informationen über Malware, Schwachstellen, Naturkatastrophen, zu relevanten Aspekten der öffentlichen Gesundheit 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.

Ein Sicherheitsalarm kann über eine Anzahl spezifischer Aktionen gelöst werden, die von entsprechenden Sicherheitsexperten bereitgestellt werden. Es gibt einige Alarmmeldungen, die nur dazu dienen, Sie über die bevorstehenden Bedrohungen zu informieren, ohne dass empfohlene Aktionen verfügbar sind.

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 Service-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 Service-Konsole zu **Dashboard** –> **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.

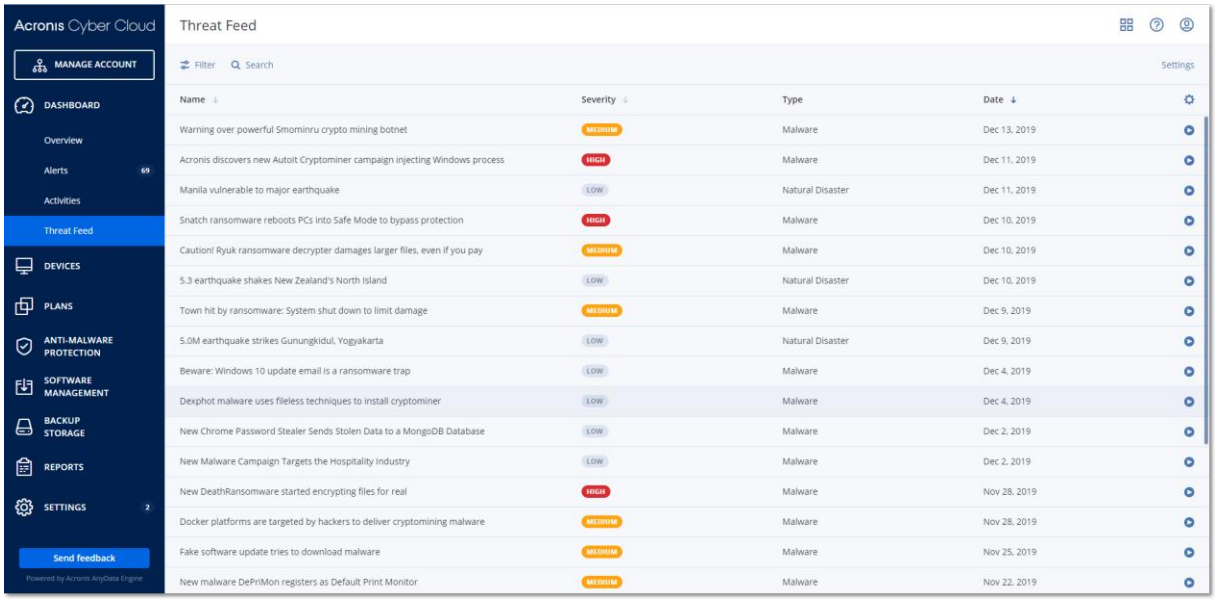
3. Klicken Sie auf **Start**, um den Assistenten zu starten.

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
- **Backup von geschützten oder ungeschützten Maschinen** – um geschützte/ungeschützte Maschinen per Backup zu sichern

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

30.2 Data Protection-Karte

Die Funktionalität 'Data Protection-Karte' bietet Ihnen folgende Möglichkeiten:

- Ausführliche Informationen über die auf Ihren Maschinen gespeicherten Daten (Klassifizierung, Speicherorte, Schutzstatus 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 (S. 410) aktiviert ist.

2. Nachdem dieser Plan ausgeführt wurde und Ihre Daten erkannt und analysiert wurden, erhalten Sie im Widget Data Protection-Karte (S. 423) 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 Service-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 die Anzahl der ungeschützten Dateien (aufgeschlüsselt nach Erweiterungen) und deren Speicherort angezeigt. 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.

30.2.1 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 (S. 105)'.

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.

Die Task-Ausführung auf Basis folgender Ereignisse planen

- **Planung nach Zeit** – der Task wird zum spezifizierten Zeitpunkt ausgeführt.
- **Wenn sich ein Benutzer am System anmeldet** – die Task-Ausführung wird standardmäßig durch die Anmeldung eines jeden Benutzers ausgelöst. Sie können aber von 'Jeder Benutzer' zu einem bestimmten Benutzerkonto wechseln.

- **Wenn sich ein Benutzer vom System abmeldet** – die Task-Ausführung wird standardmäßig durch die Abmeldung eines jeden Benutzers ausgelöst. Sie können aber von 'Jeder Benutzer' zu einem bestimmten Benutzerkonto wechseln.

  Hinweis: *Der Task wird nicht beim Herunterfahren eines Systems ausgeführt, weil 'Herunterfahren' nicht dasselbe wie 'Abmelden' ist.*

- **Beim Systemstart** – der Task wird ausgeführt, wenn das Betriebssystem startet.
- **Beim Herunterfahren des Systems** – der Task wird ausgeführt, wenn das Betriebssystem herunterfährt.

Standardeinstellung: **Planung nach Zeit**.

Planungstyp:

- **Monatlich** – bestimmen Sie, an welchen Tagen in welchem Monat der Task ausgeführt werden soll.
- **Täglich** – bestimmen Sie, an welchen Wochentagen der Task ausgeführt werden soll.
- **Stündlich** – bestimmen Sie, an welchen Wochentagen und wie oft ein Task in einer Stunde ausgeführt werden soll.

Standardeinstellung: **Täglich**.

Starten um – bestimmen sie, zu welchem Zeitpunkt der Task ausgeführt werden soll.

Standardeinstellung: **14:00 Uhr** (auf der Maschine, auf welcher die Software installiert ist).

Innerhalb eines Zeitraums ausführen – bestimmten Sie einen Datumsbereich, wann die Planung gültig ist.

Startbedingungen – definieren Sie Bedingungen, die gleichzeitig zutreffen müssen, damit der Task gestartet werden kann. Sie ähneln den Startbedingungen für das Backup-Modul, die im Abschnitt 'Startbedingungen (S. 144)' beschrieben sind.

Folgende zusätzliche Startbedingungen können definiert werden:

- **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 (in Stunden), nachdem der Task dennoch gestartet werden soll.

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 Schutzstatus 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.

31 Die Registerkarte 'Pläne'

***Hinweis**: Diese Funktionalität ist in den Standard-Editionen des Cyber Protection Service nicht verfügbar.*

Über die Registerkarte **Pläne** können Sie Schutzpläne und andere Pläne verwalten.

Jeder Bereich der Registerkarte **Pläne** enthält alle Pläne eines bestimmten Typs. Folgende Bereiche sind verfügbar:

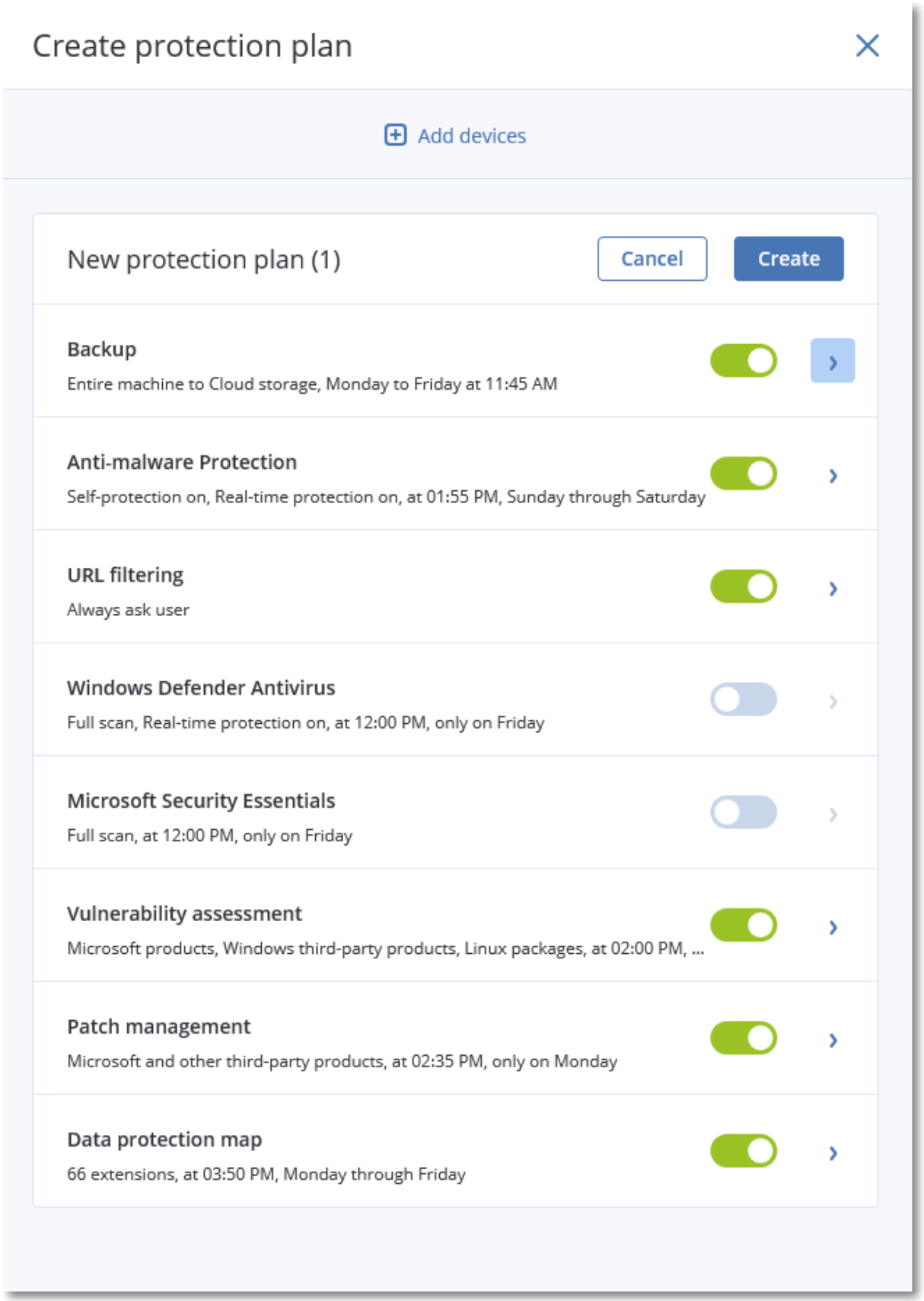
- **Schutz** (S. 412)
- **Backup-Scanning** (S. 414)
- **Cloud-Applikationen-Backup** (S. 415)
- **VM-Replikation** (S. 299)

31.1 Schutzplan

So können Sie einen Schutzplan erstellen

1. Gehen Sie in der Service-Konsole zu **Pläne** –> **Schutz**.
2. Klicken Sie auf **Plan erstellen**.
3. Wählen Sie die Maschinen aus, die Sie sichern wollen.

4. Klicken Sie auf den Befehl **Schützen**. Sie sehen den Schutzplan mit den Standardeinstellungen.



5. [Optional] Wenn Sie den Namen des Schutzplans ändern wollen, müssen Sie auf das Stiftsymbol neben dem Namen klicken.

6. [Optional] Wenn Sie das Plan-Modul (de)aktivieren wollen, müssen Sie auf den Schalter neben dem Namen des Moduls klicken.
7. [Optional] Wenn Sie die Modul-Parameter konfigurieren wollen, müssen Sie in den entsprechenden Bereich des Schutzplans klicken.
8. Klicken Sie auf **Geräte hinzufügen**, um diejenigen Maschinen auszuwählen, auf die Sie den Plan anwenden wollen.
9. Klicken Sie, wenn Sie fertig sind, auf **Erstellen**.

Als Ergebnis werden die ausgewählten Geräte mit dem Schutzplan gesichert.

Sie können die folgenden Aktionen mit einem Schutzplan durchführen:

- Einen Schutzplan erstellen, anzeigen, ausführen, stoppen, bearbeiten und löschen
- Aktivitäten anzeigen, die mit einem betreffenden Schutzplan verbunden sind
- Alarmmeldungen anzeigen, die mit einem betreffenden Schutzplan verbunden sind
- Einen Plan in eine Datei exportieren
- Einen zuvor exportierten Plan importieren

31.2 Backup-Scanning-Plan

Wenn Sie Backups nach Malware durchsuchen wollen, können Sie einen Backup-Scanning-Plan erstellen.

Beachten Sie Folgendes:

- Backups, die CDP-Recovery-Punkte (S. 130) enthalten, können zwar zum Scannen ausgewählt werden, aber es werden nur reguläre Recovery-Punkte gescannt (die CDP-Recovery-Punkte werden also vom Scannen ausgeschlossen).
- Wenn ein CDP-Backup für die sichere Wiederherstellung (Safe Recovery) einer kompletten Maschine ausgewählt wurde, wird die Maschine ohne die Daten im CDP-Recovery-Punkt sicher wiederhergestellt. Wenn Sie die CDP-Daten wiederherstellen wollen, müssen Sie eine Wiederherstellung von Dateien/Ordnern starten.

So können Sie einen Backup-Scanning-Plan erstellen

1. Gehen Sie in der Service-Konsole zu **Pläne** –> **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 neu definiert werden. Die Backups werden vom Cloud Agenten im Cloud Datacenter gescannt. Der Cloud Agent, der das Scannen durchführt, wird vom System automatisch ausgewählt.
   - **Zu scannende Backups**:
     - **Speicherorte** – wählen Sie Speicherorte mit Backups aus, die Sie scannen wollen.
     - **Backups** – wählen Sie Backups aus, die Sie scannen wollen.
   - **Scannen nach**:
     - **Malware** – diese Option kann nicht neu definiert werden. Sie überprüft Backups auf das Vorhandensein von Malware.
   - **Verschlüsselung** – stellen Sie ein entsprechendes Kennwort bereit, um verschlüsselte Backups scannen zu können. Wenn ein Depot oder mehrere Backups ausgewählt wurden,

können Sie ein einzelnes Kennwort für alle Backups spezifizieren. Wenn ein Kennwort für ein bestimmtes Backup nicht funktioniert, wird das System einen Alarm erstellen.

- **Planung** – diese Option kann nicht neu definiert werden. Die Scan-Aktivität im Cloud Storage wird automatisch gestartet.

4. Klicken Sie, wenn Sie fertig sind, auf **Erstellen**.

Als Ergebnis wird der Backup-Scanning-Plan erstellt. Die spezifizierten Backup-Speicherorte werden vom Cloud Agenten automatisch gescannt.

31.3 Backup-Pläne für Cloud-Applikationen

Der Bereich **Pläne** –> **Cloud-Applikationen-Backup** zeigt Cloud-zu-Cloud-Backup-Pläne an. 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:

- Office 365-Daten sichern (S. 251)
- G Suite-Daten sichern (S. 277)

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 Office 365- oder G Suite-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.

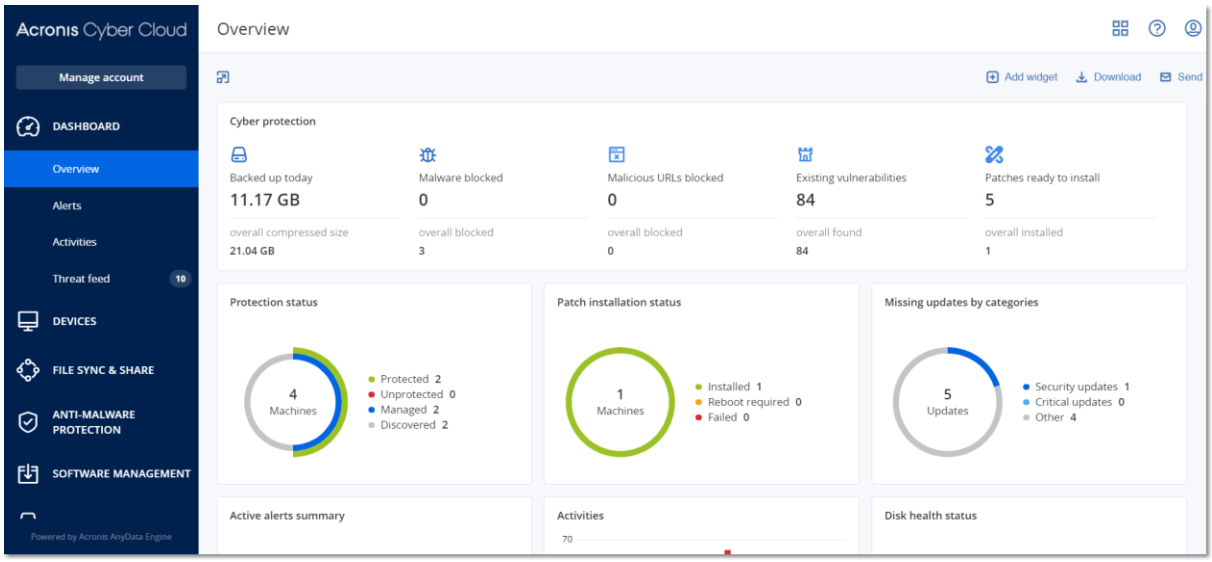
32 Monitoring

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 **Dashboard** –> **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:

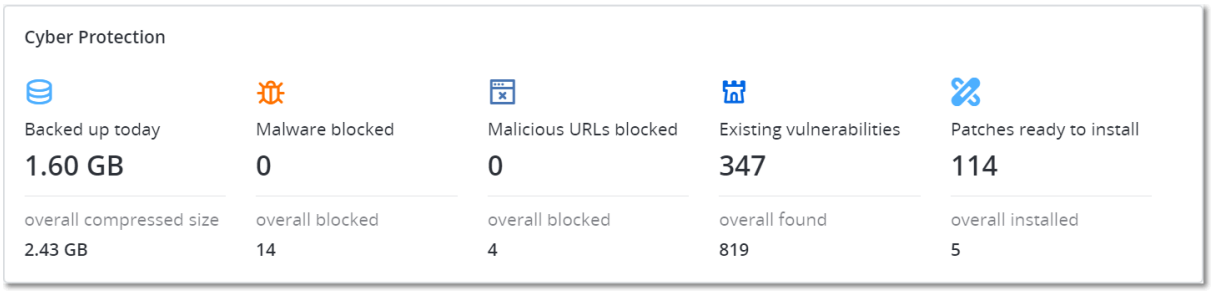
- Klicken Sie auf das hinzuzufügende Widget. Das Widget wird daraufhin mit den Standardeinstellungen hinzugefügt.
- Wenn Sie das Widgeht vor dem Hinzufügen bearbeiten wollen, dann klicken Sie nach der Auswahl des Widgets auf das Stiftsymbol. Klicken Sie, nachdem Sie das Widget bearbeitet haben, auf **Fertig**.

So können Sie ein Widget entfernen

Klicken Sie neben dem Widget-Namen auf das X-Symbol.

32.1 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

32.2 Schutzstatus

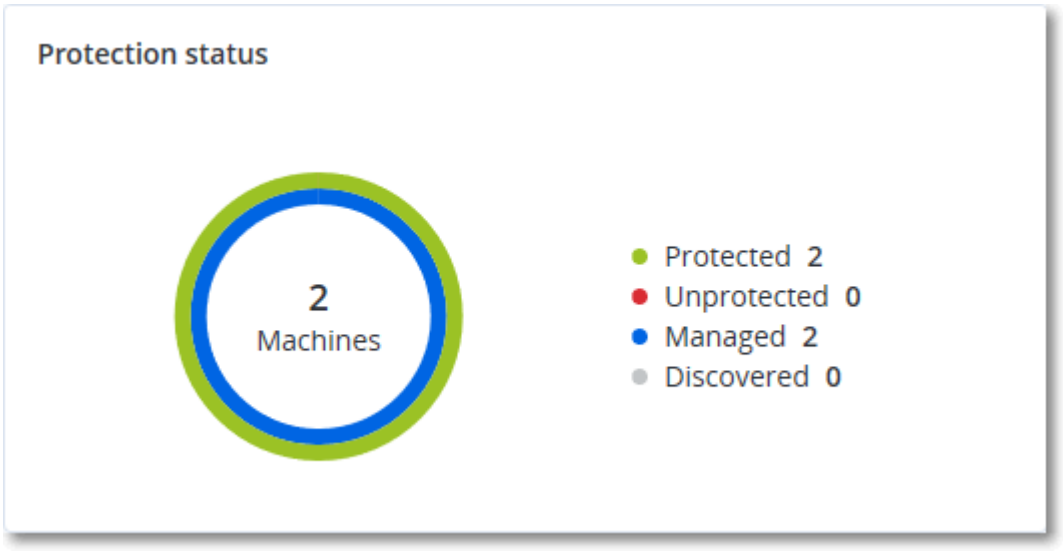
Schutzstatus

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

32.3 #CyberFit-Score pro Maschine

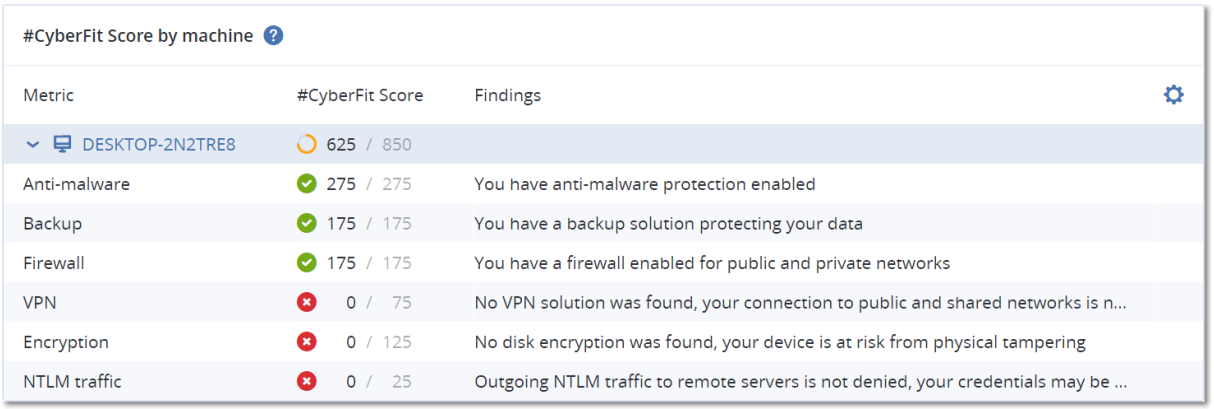
Dieses Widget zeigt für jede Maschine den #CyberFit-Gesamt-Score und die Einzel-Scores an, aus denen sich dieser Gesamtwert zusammensetzt – sowie die Ergebnisse für jede der bewerteten Metriken:

- 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 (p. 114)'.



32.4 Vorhersage zur Laufwerksintegrität

Mit der Funktion zur Kontrolle der Laufwerksintegrität können Sie den aktuellen Zustand Ihrer Festplatten überwachen und eine Vorhersage zu deren Integrität erhalten. Diese Informationen ermöglichen es Ihnen, Datenverluste zu vermeiden, die durch Laufwerksausfälle entstehen können. Es werden sowohl Laufwerke vom Typ HDD (klassische Festplatten) als auch SSD (Flash-Speicher basierte Laufwerke) unterstützt.

Einschränkungen:
1. Die Vorhersage zur Laufwerksintegrität wird nur für Windows-Maschinen unterstützt.
2. Es können nur die Laufwerke von physischen Maschinen überwacht werden. Die Laufwerke von virtuellen Maschinen können nicht überwacht werden und werden nicht im Widget angezeigt.

Die Laufwerksintegrität kann sich in einem der folgenden Statuszustände befinden:

- **OK** – die Laufwerksintegrität beträgt 70-100%
- **Warnung** – die Laufwerksintegrität beträgt 30-70%
- **Kritisch** – die Laufwerksintegrität beträgt 0-30%
- **Laufwerksdaten werden berechnet** – der aktuelle Laufwerksstatus und die Vorhersage werden ermittelt

Und so funktioniert es

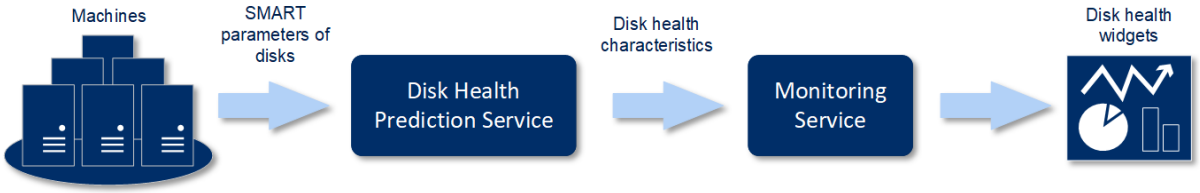
Der Disk Health Prediction Service verwendet ein auf künstlicher Intelligenz (KI) basierendes Vorhersagemodell.

1. Der 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 folgende Laufwerksintegritätsmerkmale bereit:
   - Aktueller Zustand der Laufwerksintegrität: OK, Warnung, Kritisch.
   - Vorhersage zur Laufwerksintegrität: negativ, stabil, positiv.
   - Vorhersage-Wahrscheinlichkeit der Laufwerksintegrität in Prozent:

   Der Vorhersagezeitraum beträgt immer ein Monat.
3. Der Monitoring Service erhält die Laufwerksintegritätsmerkmale und verwendet diese Daten in den Laufwerksintegrität-Widgets, die einem Benutzer in der Konsole angezeigt werden.



Laufwerksintegrität-Widgets

Die Ergebnisse der Laufwerksintegritätsüberwachung können auf dem Dashboard in den Widgets mit Bezug zur Laufwerksintegrität gefunden werden:

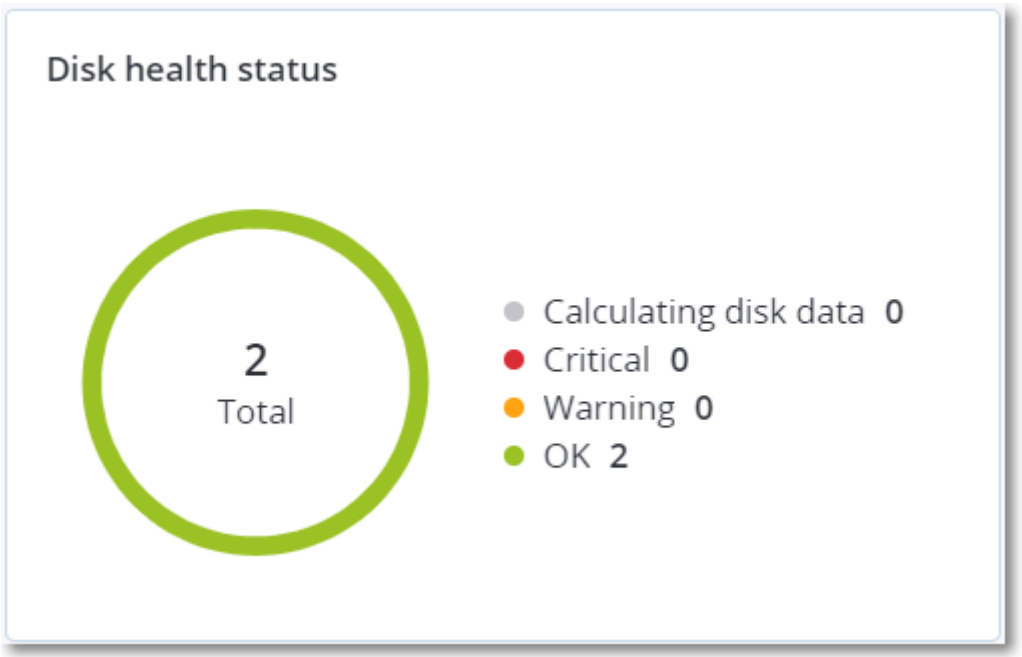
- **Überblick der Laufwerksintegrität** – ein Treemap-Diagramm (Kacheldiagramm mit Baumstruktur) hat zwei Detailebenen, zwischen denen umgeschaltet werden kann.

- Maschinenebene – zeigt zusammengefasste Informationen über den Laufwerkstatus für die ausgewählten Kundenmaschinen an. Das Widget zeigt die kritischsten Laufwerksstatusdaten an. Andere Statusmeldungen werden im Tooltip angezeigt, wenn Sie mit dem Mauszeiger über den jeweiligen 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 Laufwerksstatus aller Laufwerke für die ausgewählte Maschine an. Jeder Laufwerksblock zeigt eine Vorhersage für die Änderung des Laufwerksstatus an:
  - Wird heruntergestuft (Vorhersage-Wahrscheinlichkeit der Laufwerksintegrität in %)
  - Wird stabil bleiben (Vorhersage-Wahrscheinlichkeit der Laufwerksintegrität in %)

- Wird verbessert (Vorhersage-Wahrscheinlichkeit der Laufwerksintegrität in %)

- **Laufwerksintegritätsstatus** – ein Kuchendiagramm-Widget, welches die Anzahl der Laufwerke für jeden Status anzeigt.



Alarmmeldungen zum Laufwerksintegritätsstatus

Eine Laufwerksintegritätsprüfung wird alle 30 Minuten durchgeführt, während die entsprechende Alarmmeldung nur einmal täglich generiert wird. Wenn sich der Status der Laufwerksintegrität von 'Warnung' auf 'Kritisch' ändert, werden Sie auch dann alarmiert, wenn Sie an dem Tag bereits eine Alarmmeldung erhalten haben.

Alarmbezeichnung	Schweregrad	Laufwerksintegritätsstatus	Beschreibung
Laufwerksausfall ist möglich	Warnung	[30;70)	Das Laufwerk [Laufwerksname] auf der Maschine [Maschinenname] 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 der Maschine [Maschinenname] befindet sich in einem kritischen Zustand und wird höchstwahrscheinlich sehr bald ausfallen. Es ist nicht empfehlenswert, 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.

32.5 Data Protection-Karte

Die Funktion 'Data Protection-Karte' ermöglicht es Ihnen, alle für Sie wichtigen Daten zu ermitteln sowie ausführliche Informationen über Anzahl, Größe, Speicherort und Schutzstatus aller wichtigen Dateien in Form einer skalierbaren Treemap-Anzeige (Kacheldiagramm mit Baumstruktur) zu erhalten.

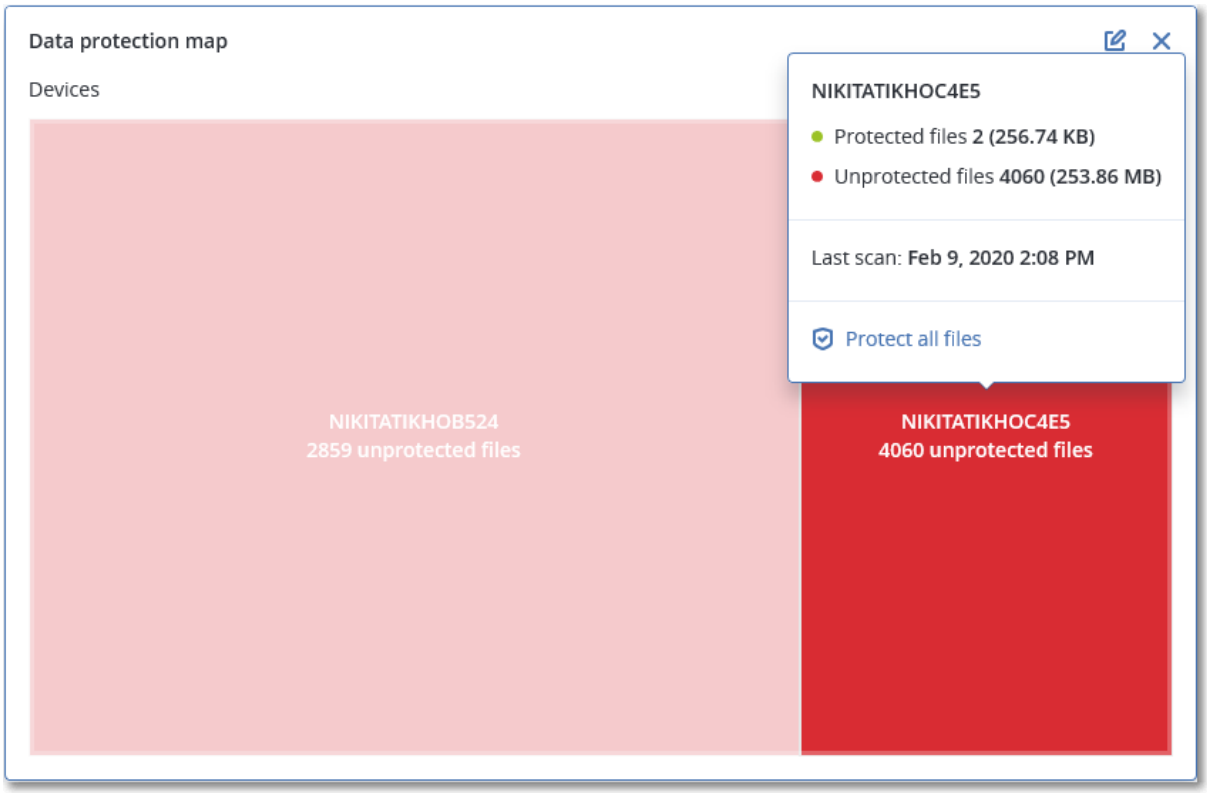
Jede Blockgröße hängt von der Gesamtzahl/Größe aller wichtigen Dateien ab, die zu einem Kunden/einer Maschine gehören.

Dateien können einen der folgenden Statuszustände 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 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.

32.6 Widget für Schwachstellenbewertung

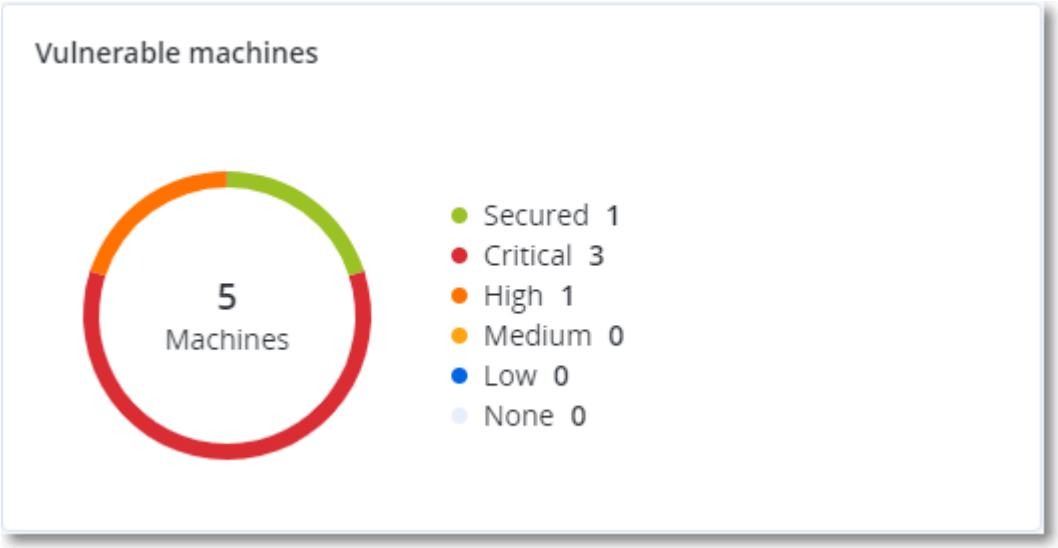
Verwundbare Maschinen

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

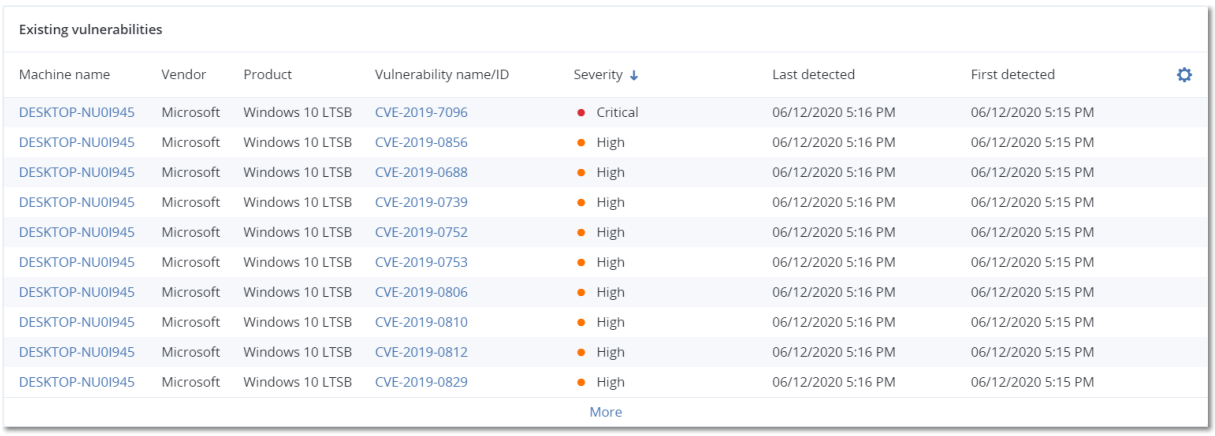
- Ohne: 0.0 CVSS



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.



32.7 Widgets für Patch-Installation

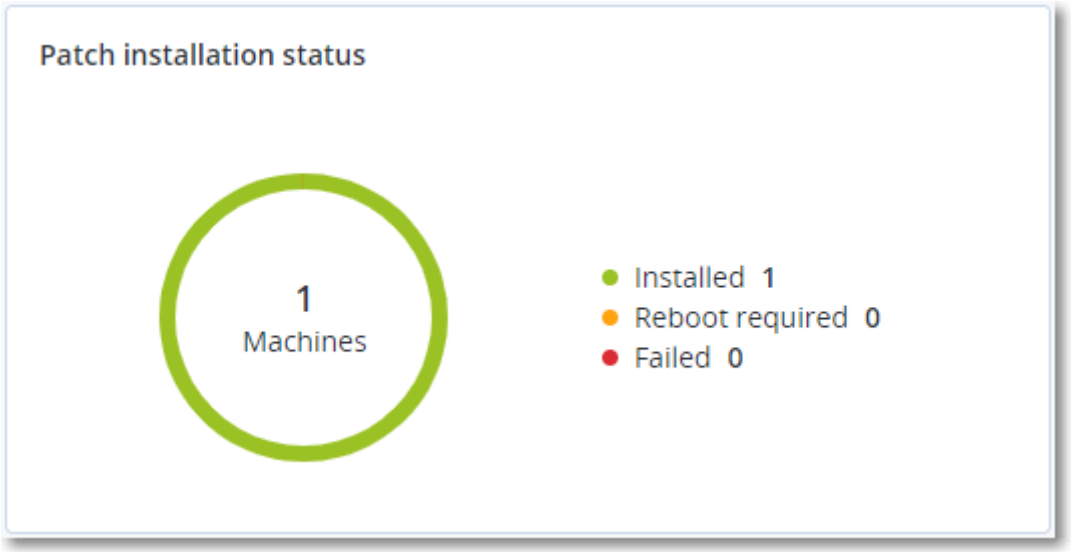
Es gibt vier Widgets im Zusammenhang mit der Patch-Verwaltungsfunktionalität.

Status der Patch-Installation

Dieses Widget zeigt die Anzahl der Maschinen gruppiert nach dem Status des Patch-Installation an.

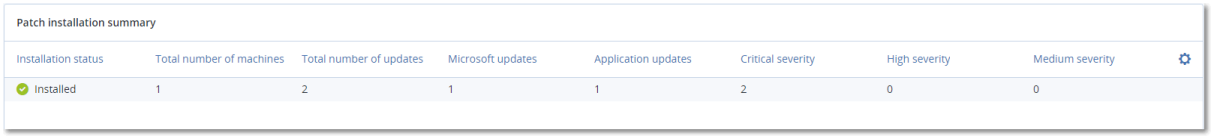
- **Installiert** – alle verfügbaren Patches sind auf einer Maschine installiert
- **Neustart erforderlich** – nach einer Patch-Installation muss eine Maschine neu gestartet werden

- **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.



Patch installation summary

Installation status	Total number of machines	Total number of updates	Microsoft updates	Application updates	Critical severity	High severity	Medium severity
Installed	1	2	1	1	2	0	0

Verlauf der Patch-Installation

Dieses Widget zeigt ausführliche Informationen über die Patches auf den Maschinen an.

Patch installation history

Machine name	Update name	Version	Severity	Approval status	Installation status	Installation date
NIKITATIKHOC4E5	FastStone Soft FastStone I...	5.9	Medium	New	Installed	02/05/2020
NIKITATIKHOB524	Mozilla Firefox	72.0.1	Critical	Approved	Failed	02/04/2020
NIKITATIKHOB524	Mozilla Firefox	72.0.1	Critical	Approved	Installed	02/04/2020
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	Failed	02/04/2020
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	Installed	02/04/2020
NIKITATIKHOC4E5	Oracle Java Runtime Envir...	8.0.2410.7	High	New	Failed	02/04/2020
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	Installed	02/04/2020
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	Installed	02/04/2020
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	Failed	02/04/2020
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	Failed	02/04/2020

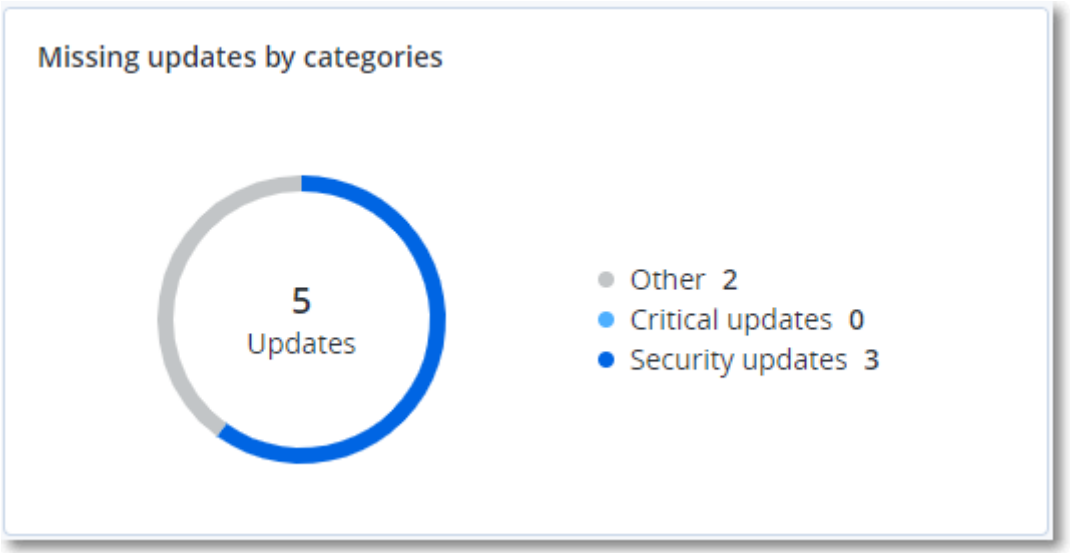
More

Fehlende Updates nach Kategorie

Dieses Widget zeigt die Anzahl der fehlenden Updates nach Kategorie an. Folgende Kategorien werden angezeigt:

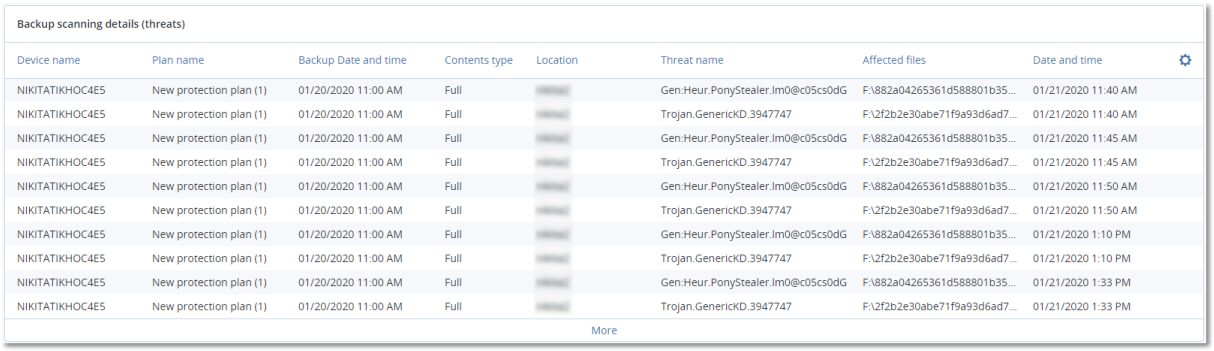
- Sicherheitsupdates
- Kritische Updates

- Andere



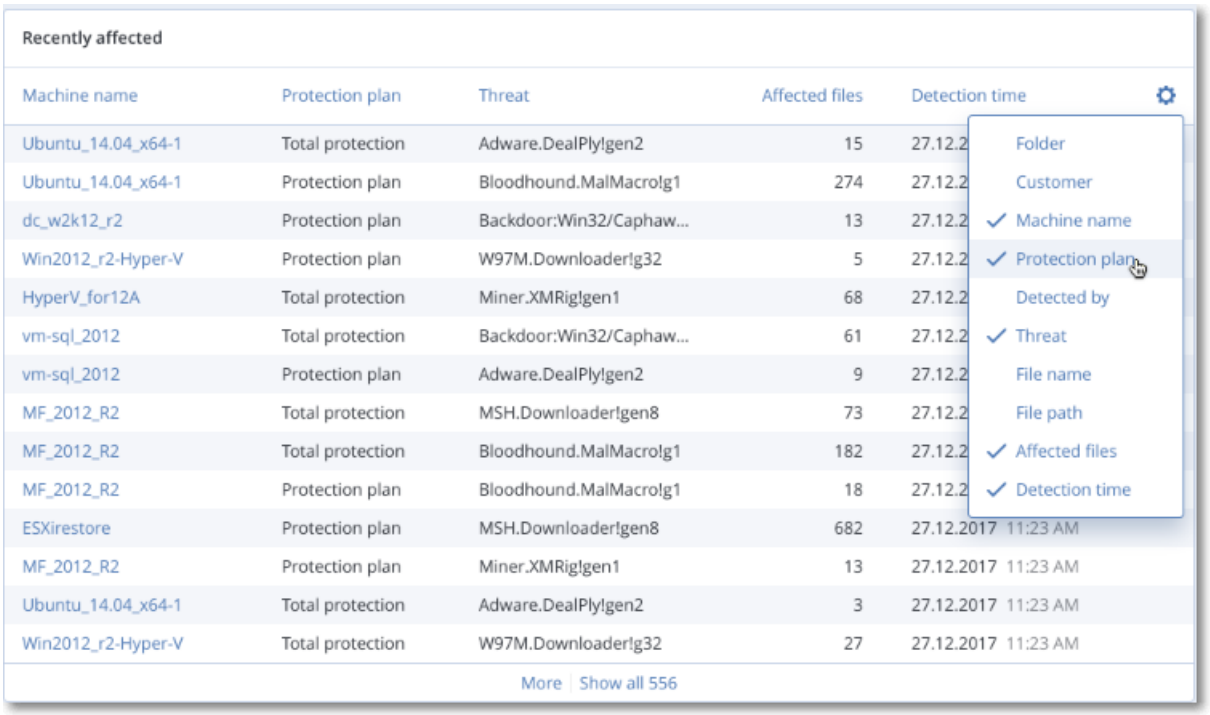
32.8 Details zu 'Backup scannen'

Dieses Widget zeigt ausführliche Informationen über erkannte Bedrohungen in den Backups an.



32.9 Kürzlich betroffen

Dieses Widget zeigt ausführliche Informationen über kürzlich infizierte Maschinen an. Sie können Informationen darüber finden, welche Bedrohung erkannt wurde und wie viele Dateien infiziert wurden.

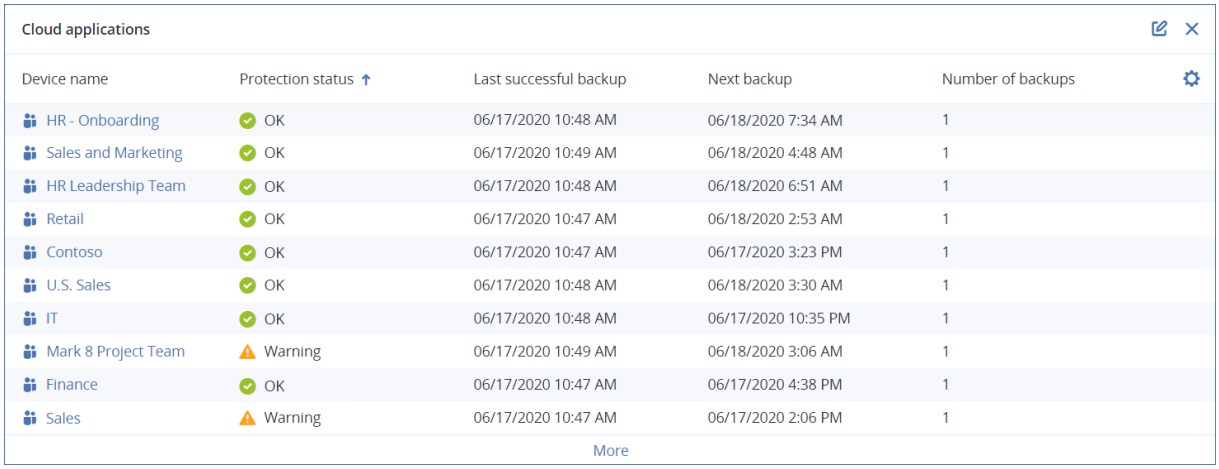


32.10 Cloud-Applikationen

Dieses Widget zeigt ausführliche Informationen über Cloud-zu-Cloud-Ressourcen an:

- Office 365-Benutzer (Postfach, OneDrive)
- Office 365-Gruppen (Postfach, Gruppen-Website)
- Öffentliche Office 365-Ordner
- Office 365-Website-Sammlungen
- Office 365-Teams
- G Suite-Benutzer (Gmail, GDrive)

- G Suite Shared Drives



Weitere Informationen über Cloud-zu-Cloud-Ressourcen sind auch in folgenden Widgets verfügbar:

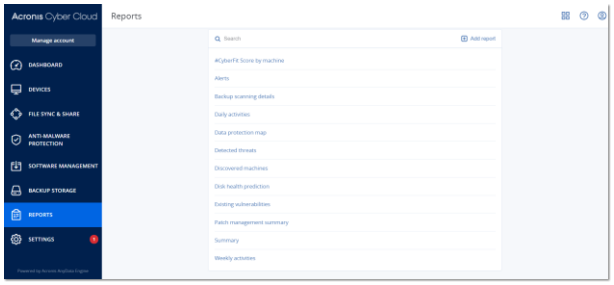
- Aktivitäten
- Aktivitätsliste
- 5 neueste Alarmmeldungen
- Alarmverlauf
- Aktive Alarmmeldungen – Übersicht
- Übersicht der historischen Alarmmeldungen
- Details 'Aktiver Alarm'
- Speicherorteübersicht

33 Berichte

***Hinweis**: Diese Funktionalität ist in den Standard-Editionen des Cyber Protection Service nicht verfügbar.*

Ein Bericht über Aktionen kann einen beliebigen Satz von Dashboard-Widgets (S. 416) enthalten. Alle Widgets zeigen zusammengefasste Informationen für die komplette Firma an. Alle Widgets zeigen die Parameter für denselben Zeitraum an. Sie können diesen Zeitbereich in den Berichtseinstellungen ändern.

Sie können vorgegebene Berichte (Standardberichte) verwenden oder einen benutzerdefinierten Bericht erstellen.



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.
Details zu 'Backup scannen'	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 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.
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.

Wenn Sie einen Bericht einsehen wollen, klicken Sie auf dessen Namen.

Wenn Sie mit einem Bericht auf Aktionen zugreifen wollen, müssen Sie in der Berichtszeile auf das Drei-Punkte-Symbol klicken. Dieselben Aktionen sind aus dem Bericht heraus verfügbar.

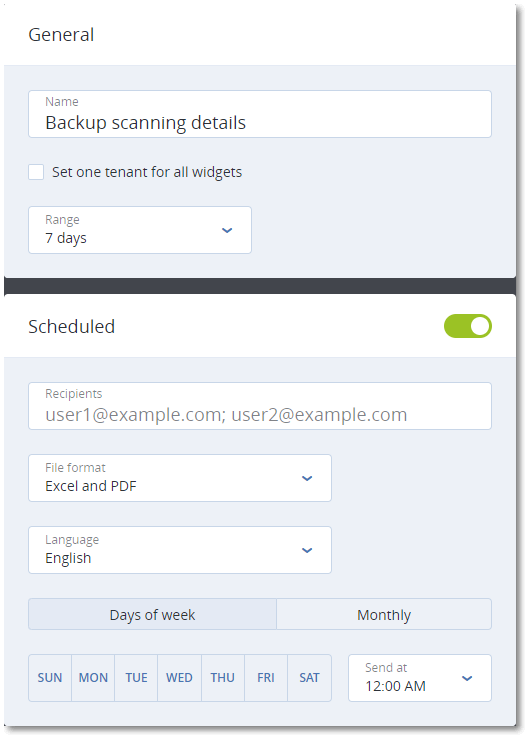
Einen Bericht hinzufügen

1. Klicken Sie auf **Bericht hinzufügen**.
2. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Wenn Sie einen vordefinierten Bericht hinzufügen wollen, klicken Sie auf dessen Namen.
   - Wenn Sie einen benutzerdefinierten Bericht hinzufügen wollen, klicken Sie zuerst auf **Benutzerdefiniert**, dann auf den Berichtsnamen (die automatisch zugewiesenen Namen sehen folgendermaßen aus: **Benutzerdefiniert(1)**) und fügen Sie dann die Widgehts dem Bericht hinzu.
3. [Optional] Ordnen Sie die Widgets per Drag & Drop nach Ihren Vorstellungen neu an.
4. [Optional] Bearbeiten Sie den Bericht wie nachfolgend beschrieben.

Einen Bericht bearbeiten

Wenn Sie einen Bericht bearbeiten wollen, müssen Sie zuerst auf dessen Namen klicken und dann auf **Einstellungen**. Durch Bearbeitung eines Berichts können Sie:

- Den Bericht umbenennen
- Den Zeitraum für alle im Report enthaltenen Widgets ändern
- Eine Planung für das Versenden des Bericht im .pdf- und/oder .xlsx-Format per E-Mail festlegen



Einen Bericht planen

1. Klicken Sie auf den Berichtsnamen und dann auf **Einstellungen**.
2. Aktivieren Sie den Schalter **Geplant**.
3. Spezifizieren Sie die E-Mail-Adresse(n) des/der Empfänger.
4. Bestimmen Sie das Format für den Bericht: .pdf, .xlsx oder beides.
5. Bestimmen Sie die Tage und den genauen Zeitpunkt, an dem der Bericht versendet werden soll.
6. Klicken Sie in der oberen rechten Ecke auf **Speichern**.

***Hinweis**: Die maximale Anzahl von Elementen, die in eine .pdf- oder .xlsx-Datei exportiert werden können, beträgt 1000.*

Die Berichtsstruktur exportieren und importieren

Sie können die Berichtsstruktur (die Zusammenstellung der Widgets und die Berichtseinstellungen) als .json-Datei exportieren oder importieren.

Wenn Sie die Berichtsstruktur exportieren wollen, müssen Sie zuerst auf den Berichtsnamen klicken, dann in der rechten oberen Ecke auf das Drei-Punkte-Symbol und abschließend auf den Befehl **Exportieren**.

Wenn Sie die Berichtsstruktur importieren wollen, müssen Sie zuerst auf **Bericht hinzufügen** klicken und anschließend auf **Importieren**.

Einen Bericht herunterladen

Wenn Sie einen Bericht herunterladen wollen, klicken Sie auf **Download** und wählen Sie das gewünschte Format aus:

- Excel oder PDF
- Excel
- PDF

Die Berichtsdaten sichern

Sie können eine Abbild (Dump) der Berichtsdaten (als .csv-Datei) per E-Mail versenden. Die Abbildsicherung enthält alle Berichtsdaten (ungefiltert) für einen bestimmten Zeitraum. Die Zeitstempel in CSV-Berichten verwenden das UTC-Format, während die Zeitstempel in Excel- und PDF-Berichten die aktuelle Zeitzone des Systems verwenden.

Die Software generiert die Sicherungsdaten „on the fly“. Wenn Sie einen langen Zeitraum definieren, kann die Aktion jedoch einige Zeit benötigen.

So können Sie die Berichtsdaten sichern

1. Klicken Sie auf den Berichtsnamen.
2. Klicken Sie in der rechten oberen Ecke auf das Drei-Punkte-Symbol und anschließend auf **Sicherungsdaten**.
3. Spezifizieren Sie die E-Mail-Adresse(n) des/der Empfänger.
4. Spezifizieren Sie bei **Zeitraum** den gewünschten Zeitrahmen.
5. Klicken Sie auf **Senden**.

***Hinweis**: Die maximale Anzahl von Elementen, die in eine .csv-Datei exportiert werden können, beträgt 150.000.*

34 Problembehebung (Troubleshooting)

Dieser Abschnitt beschreibt, wie Sie ein Agenten-Protokoll (Log) als .zip-Datei speichern können. Falls ein Backup aus unbekannten Gründen fehlschlägt, hilft diese Datei den Mitarbeitern des technischen Supports, das Problem zu identifizieren.

So stellen Sie Logs zusammen

1. Wählen Sie die Maschine aus, deren Protokolle (Logs) Sie sammeln wollen.
2. Klicken Sie auf **Aktivitäten**.
3. Klicken Sie auf **Systeminformationen sammeln**.
4. Spezifizieren Sie bei Aufforderung durch Ihren Webbrowser, wo die Datei gespeichert werden soll.

35 Glossar

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 Ressourcenbeanspruchung.

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 seit 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 seit Anbruch einer Stunde erstellt wird – es sei denn, dieses Backup fällt unter die Definition eines 'monatlichen', 'wöchentlichen' oder 'täglichen' Backups.

C

Cloud Server

[Disaster Recovery] Allgemeiner Begriff für eine primären Server oder Recovery-Server (auch Wiederherstellungsserver genannt).

Cloud-Site (oder DR-Site)

[Disaster Recovery] Ein in der Cloud gehosteter Remote-Standort, der dazu verwendet wird, im Desasterfall eine Recovery-Infrastruktur auszuführen.

D

Differentielles Backup

Ein differentielles Backup speichert Änderungen an den Daten im Vergleich zum letzten vorangegangenen Voll-Backup (S. 438). Sie benötigen den Zugriff auf das entsprechende Voll-Backup, um die Daten aus einem differentiellen Backup wiederherzustellen.

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.

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

Lokale Site

[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
- Microsoft Security Essentials
- Schwachstellenbewertung
- Patch-Verwaltung
- Data Protection-Karte

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.

V

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

Selbstständiges Backup, das alle Daten enthält, die für die Sicherung gewählt wurden. 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 Verbindungsgateway wird in der Cloud-Site bereitgestellt.