Acronis

acronis.com

# Acronis Cyber Protect 15

## Update 6

Benutzeranleitung

REVISION: 15.06.2023

# Inhaltsverzeichnis

# Urheberrechtserklärung



# Von Acronis patentierte Technologien

Die in diesem Produkt verwendeten Technologien werden durch einzelne oder mehrere U.S.-Patentnummern abgedeckt und geschützt: 7,047,380; 7,246,211; 7,275,139; 7,281,104; 7,318,135; 7,353,355; 7,366,859; 7,383,327; 7,475,282; 7,603,533; 7,636,824; 7,650,473; 7,721,138; 7,779,221; 7,831,789; 7,836,053; 7,886,120; 7,895,403; 7,934,064; 7,937,612; 7,941,510; 7,949,635; 7,953,948; 7,979,690; 8,005,797; 8,051,044; 8,069,320; 8,073,815; 8,074,035; 8,074,276; 8,145,607; 8,180,984; 8,225,133; 8,261,035; 8,296,264; 8,312,259; 8,347,137; 8,484,427; 8,645,748; 8,732,121; 8,850,060; 8,856,927; 8,996,830; 9,213,697; 9,400,886; 9,424,678; 9,436,558; 9,471,441; 9,501,234 sowie weitere, schwebende Patentanmeldungen.

# Acronis Cyber Protect 15-Editionen

Acronis Cyber Protect 15 ist in Form folgender Editionen verfügbar:

- Cyber Protect Essentials
- Cyber Protect Standard
- Cyber Protect Advanced
- Cyber Backup Standard
- Cyber Backup Advanced

Ausführliche Informationen über die in jeder Edition enthaltenen Funktionen finden Sie im Abschnitt 'Acronis Cyber Protect 15 – Vergleich der Editionen (inkl. Cloud-Bereitstellung)'.

Alle Editionen von Acronis Cyber Protect 15 werden nach der Anzahl der geschützten Workloads und deren Typ (Workstation, Server und virtueller Host) lizenziert. Die Cyber Protect-Editionen sind nur als Abonnementlizenzen erhältlich. Die Cyber Backup-Editionen sind sowohl mit Abonnement- als auch mit Dauerlizenzen erhältlich. Weitere Informationen über die verfügbaren Optionen finden Sie im Abschnitt '"Lizenzierung" (S. 22)'.

Dauerlizenzschlüssel für Version 15 können nicht mit den Backup Agenten von Acronis Cyber Backup 12.5 verwendet werden. Diese Agenten können jedoch weiter mit ihren alten Lizenzschlüsseln arbeiten – selbst wenn deren Management Server auf Version 15 aktualisiert wurde.

Backup-Abonnementlizenzen können mit den Agenten der Version 12.5 verwendet werden, auch wenn die Agenten auf Version 15 aktualisiert werden. Die Cyber Protect-Abonnementlizenzen können jeodch nur von den Agenten der Version 15 verwendet werden.

Backup Agenten der Version 12.5, die auf einem Management Server der Version 15 registriert sind, können keine Off-Host Data Processing-Operationen (wie Backup-Replikationen, Backup-Validierungen, Backup-Bereinigung oder Konvertierungen zu einer virtuellen Maschine) durchführen.

**Hinweis**
Die Funktionen variieren zwischen den verschiedenen Editionen. Einige der in dieser Dokumentation beschriebenen Funktionen sind daher möglicherweise mit Ihrer Lizenz nicht verfügbar. Ausführliche Informationen über die in jeder Edition enthaltenen Funktionen finden Sie im Abschnitt 'Acronis Cyber Protect 15 – Vergleich der Editionen (inkl. Cloud-Bereitstellung)'.

## Unterstützte Cyber Protect-Funktionen, nach Betriebssystem

Die Cyber Protect-Funktionen werden auf folgenden Betriebssystemen unterstützt:

- Windows: Windows 7 und höher, Windows Server 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 unterstützten die Cyber Protect-Funktionen möglicherweise ebenfalls. Sie wurden aber nicht ausdrücklich darauf 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 Scale Computing) wird nur die Backup-Funktionalität unterstützt.

| Cyber Protect-Funktionen | Windows | Linux | macOS |
|---|---|---|---|
| **Forensik-Backup** | 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 |
| **Acronis Antimalware Protection** | | | |
| Erkennung von Ransomware aufgrund von Prozessverhalten (KI-basiert) | Ja | Nein | Nein |
| Erkennung von Cryptomining-Prozessen | Ja | Nein | Nein |
| Antimalware Protection in Echtzeit | Ja | Nein | Ja |
| Automatisches Recovery von betroffenen Dateien aus lokalem Cache | Ja | Nein | Nein |
| Selbstschutzfunktion für Acronis Backup-Dateien | Ja | Nein | Nein |

| | | | |
|---|---|---|---|
| Selbstschutzfunktion für die Acronis Software | Ja | Nein | Nein |
| Statische Analyse für übertragbare ausführbare Dateien | Ja | Nein | Ja* |
| Schutz von externen Laufwerken (HDD, USB-Sticks, SD-Karten) | Ja | Nein | Nein |
| Netzwerkordnerschutz | Ja | Nein | Nein |
| Serverseitiger Schutz | Ja | Nein | Nein |
| Schutz für Zoom, WebEx und Microsoft Teams sowie weitere Remote Work Protection-Funktionen | Ja | Nein | Nein |
| On-Demand-Antimalware-Scanning | Ja | Nein | Ja |
| Archivdateien scannen | Ja | Nein | Ja |
| Ausschluss von Dateien/Ordnern | Ja | Nein | Ja** |
| Ausschluss von Prozessen | Ja | Nein | Nein |
| Unternehmensweite Positivliste | Ja | Nein | Ja |
| Verhaltenserkennung | Ja | Nein | Nein |
| Quarantäne | Ja | Nein | Ja |
| URL-Filterung (http/https) | Ja | Nein | Nein |
| Windows Defender Antivirus-Verwaltung | Ja | Nein | Nein |
| Microsoft Security Essentials-Management | Ja | Nein | Nein |
| **Schwachstellenbewertung** | | | |
| Schwachstellenbewertung des Betriebssystems und seiner nativen Applikationen | Ja | Ja*** | Nein |
| Schwachstellenbewertung für Drittanbieter-Applikationen | Ja | Nein | Nein |
| **Patch-Verwaltung** | | | |
| Automatische Patch-Genehmigung | Ja | Nein | Nein |
| Manuelle Patch-Installation | Ja | Nein | Nein |
| Planung der automatischen Patch-Installation | Ja | Nein | Nein |

| | | | |
|---|---|---|---|
| Ausfallsicheres Patching: Backup einer Maschine vor der Patch-Installation als Bestandteil eines Schutzplans | Ja | Nein | Nein |
| Maschinen-Neustarts während Backup-Ausführungen verhindern | Ja | Nein | Nein |
| **Data Protection-Karte** | | | |
| Maschinen scannen, um ungeschützte Dateien zu finden | Ja | Nein | Nein |
| Überblick über ungeschützte Speicherorte | Ja | Nein | Nein |
| Schutzaktionen in der Data Protection-Karte ausführen | 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** | | | |
| Scannen von verschlüsselten Backups | Ja | Nein | Nein |
| Scannen von Laufwerk-Backups in lokalen Storages, Netzwerkfreigaben und dem Acronis Cloud Storage | Ja | Nein | Nein |
| **Safe Recovery** | | | |
| Antimalware-Scanning mit Acronis Antivirus & Antimalware Protection bei Wiederherstellungsprozessen | Ja | Nein | Nein |
| **Remote-Desktop** | | | |
| Verbindung über HTML5-Client | Ja | Nein | Nein |
| Verbindung über Windows-eigenen RDP-Client | Ja | Nein | Nein |
| **Remote-Löschung** | Ja**** | Nein | Nein |
| **Cyber Protect Monitor** | Ja | Nein | Ja |

* Bei macOS wird die statische Analyse von übertragbaren ausführbaren Dateien nur für geplante Scans unterstützt.

** Bei macOS wird der Ausschluss von Dateien/Ordnern nur dann unterstützt, wenn Sie Dateien/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-cr-announce/ und andere.

**** Die Funktion zur Remote-Löschung ist nur für Maschinen verfügbar, die unter Windows 10 oder höher laufen

# Lizenzierung

Um einen Workload mit Acronis Cyber Protect schützen zu können, benötigen Sie eine Lizenz. Es ist jedoch keine Lizenz erforderlich, um Acronis Cyber Protect zu installieren.

## Lizenztypen

Acronis Cyber Protect ist über Abonnementlizenzen erhältlich. Innerhalb des Gültigkeitszeitraums, der mit dem Kaufdatum beginnt, sind unbegrenzte Updates und ein kostenloser technischer Support verfügbar. Wenn der Gültigkeitszeitraum abgelaufen ist, werden vorhandene Schutzpläne nicht mehr funktionieren und können keine neuen Schutzpläne mehr erstellt werden.

Lizenzerneuerungen für ältere Dauerlizenzen sind möglich. Einige Funktionen (z.B. eine Cloud-Bereitstellung oder Cloud-zu-Cloud-Backups) sind mit einer Dauerlizenz nicht verfügbar.

Eine Testlizenz ist ebenfalls verfügbar. Sie bietet Ihnen für 30 Tage (ab Lizenzaktivierung) Zugriff auf alle Produktfunktionen.

Weitere Informationen über die unterschiedlichen Lizenzierungsoptionen finden Sie im folgenden englischsprachigen Knowledge Base-Artikel: Acronis Cyber Protect 15: licensing and upgrade/downgrade FAQ. Die Acronis Lizenzierungsrichtlinie ist unter dieser Adresse verfügbar: https://www.acronis.com/company/licensing.html.

**Wichtig**
Mit Acronis Cyber Protect 15 Update 3 wurde ein neues Lizenzierungsmodell eingeführt. Es erfordert eine Lizenzregistrierung und die Aktivierung von lokalen Management Servern.

## Die Lizenzierung in Acronis Cyber Protect 15 Update 3 und höheren Versionen

In Acronis Cyber Protect 15 Update 3 und nachfolgenden Versionen werden keine Lizenzschlüssel in der lokalen Konsole des Management Servers (`https://<IP-Adresse Ihres Management Servers>:<Port>`) hinzugefügt.

Stattdessen fügen Sie die Lizenzen zu Ihrem Konto im Acronis Support-Portal (`https://account.acronis.com`) hinzu und verwalten Ihre Lizenzen dann in der Acronis Cyber Protect Cloud-Konsole (`https://cloud.acronis.com`).

Die Lizenzverwaltung von Offline Management Servern erfordert, dass Sie bestimmte Aktionen sowohl in der lokalen Konsole als auch in der Cloud-Konsole durchführen.

Weitere Informationen über die lokale und Cloud-Konsole finden Sie im Abschnitt '"Acronis Konto, lokale und Cloud-Konsolen" (S. 24)'.

***So beginnen Sie mit der Verwendung eines Management Servers mit Acronis Cyber Protect 15 Update 3 und höher***

1. Fügen Sie eine oder mehrere Lizenzen zu Ihrem Konto im Acronis Support-Portal (https://account.acronis.com) hinzu.
   Lizenzen, die Sie online erworben haben, werden diesem Konto automatisch hinzugefügt.
2. [Für den On-Premise-Bereitstellungsmodus) Aktivieren Sie Ihren Management Server.
3. Ordnen Sie dem Management Server eine Lizenz zu.

## Verschiedene Typen von Management Server

Je nach Bereitstellungsmodus, den Sie verwenden, können Sie folgende Typen von Management Servern verwenden:

- Cloud Management Server
- Lokaler Management Server
  - Online Management Server
  - Offline Management Server

Sie können mehr als einen Management Server in Ihrem Acronis Konto haben. Sie können auch einen gemischten Bereitstellungsmodus verwenden, bei dem ein Cloud Management Server und ein lokal bereitgestellter Management Server verwendet werden.

Wenn Sie mit mehreren Management Servern arbeiten, können Sie eine Lizenz-Quota auch zwischen diesen aufteilen. Weitere Informationen über die entsprechende Durchführung finden Sie im Abschnitt '"Lizenz-Quotas zu einem anderen Management Server übertragen" (S. 34)'.

### Cloud Management Server

Bei einer Cloud-Bereitstellung wird kein Management Server in Ihrem Netzwerk installiert bzw. gewartet. Sie verwenden einen Management Server, der bereits in einem Acronis Datacenter bereitgestellt wurde, und müssen nur noch die jeweiligen Protection Agenten für Ihre Workloads installieren.

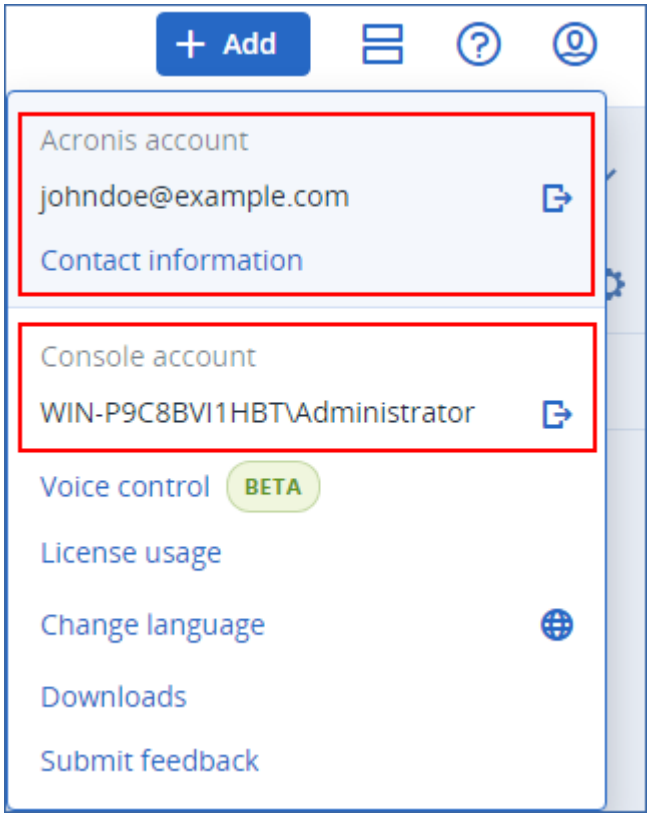
Der Cloud Management Server muss nicht aktiviert werden. Er ist immer online und die Lizenzierungsinformationen werden automatisch zwischen dem Server und Ihrem Acronis Konto synchronisiert.

### Lokaler Management Server

Bei einer lokalen Bereitstellung (On-Premise-Bereitstellung) müssen Sie sowohl den Management Server als auch die entsprechenden Protection Agenten in Ihrem Netzwerk installieren. Sie können auch einen Offline Management Server verwenden, der nicht mit dem Internet verbunden ist, oder einen Online Management Server, der wiederum Zugriff auf das Internet hat.

Management Server, die on-premise bereitgestellt wurden, müssen aktiviert werden. Weitere Informationen zur Aktivierung finden Sie im Abschnitt '"Einen Management Server aktivieren" (S. 28)'.

**Hinweis**
In der lokalen Konsole eines aktivierten On-Premise-Management-Servers werden zwei verschiedene Konten angezeigt: das Acronis Konto, welches für die Synchronisierung der Lizenzierungsinformationen verwendet wird, und das Konsolen-Konto, welches für den Zugriff auf die lokale Konsole selbst verwendet wird.




### Ein lokaler Online Management Server

Sie aktivieren einen Online Management Server über das Internet, indem Sie sich an Ihrem Acronis Konto anmelden, wenn Sie zum ersten Mal auf die lokale Konsole zugreifen.

### Ein lokaler Offline Management Server

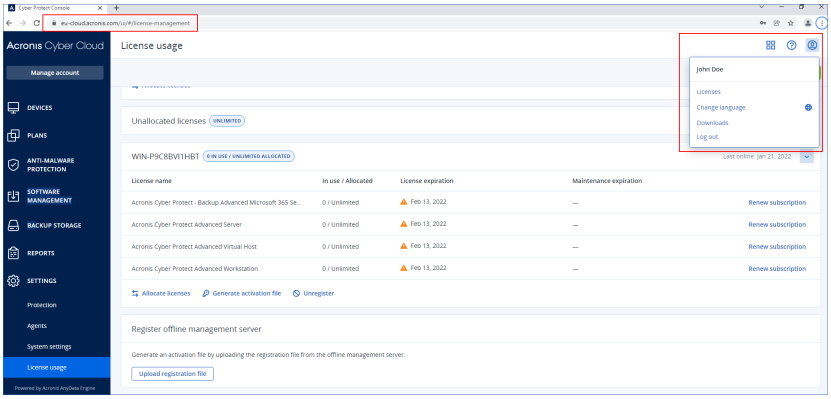
Die Aktivierung eines Offline Management Servers und die Synchronisierung von dessen Lizenzierungsinformationen mit Ihrem Acronis Konto erfolgt manuell über eine entsprechende Datei.

## Acronis Konto, lokale und Cloud-Konsolen

Um Acronis Cyber Protect nutzen und Ihre Lizenzen sowie deren Nutzung verwalten zu können, benötigen Sie ein Acronis Konto. All Ihre Lizenzen und Management Server werden unter diesem Konto registriert.

Mit diesem Konto können Sie auf folgende Konsolen zugreifen:

- Die Cloud-Konsole (`https://cloud.acronis.com`)

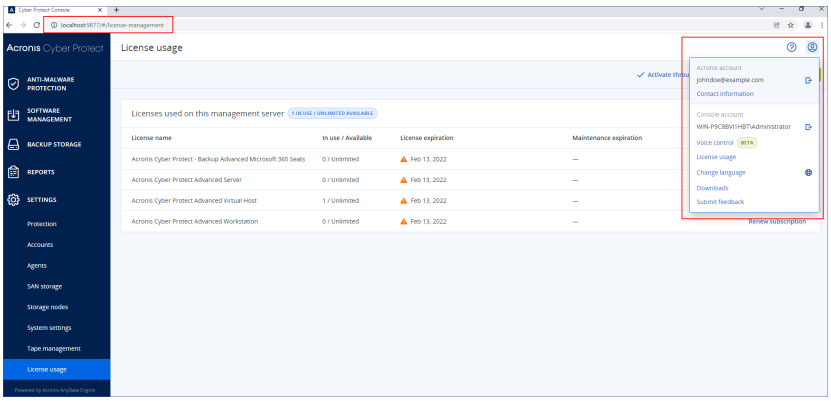



**Hinweis**

Wenn Sie sich an der Cloud-Konsole anmelden, ändert sich deren URL und zeigt das entsprechende Datacenter an, zu dem Ihr Konto gehört. Beispielsweise `https://eu-cloud.acronis.com` oder `https://jp-cloud.acronis.com`.

Die Cloud-Konsole ist der Hauptort, wo Sie Ihre Lizenzen verwalten. Hier können Sie auf der Registerkarte **Einstellungen** –> **Lizenznutzung** verfügbare Lizenzen und Lizenz-Quotas einem bestimmten Management Server zuordnen, Lizenz-Quotas einem anderen Management Server neu zuordnen oder die Registrierung eines Offline Management Servers finalisieren.

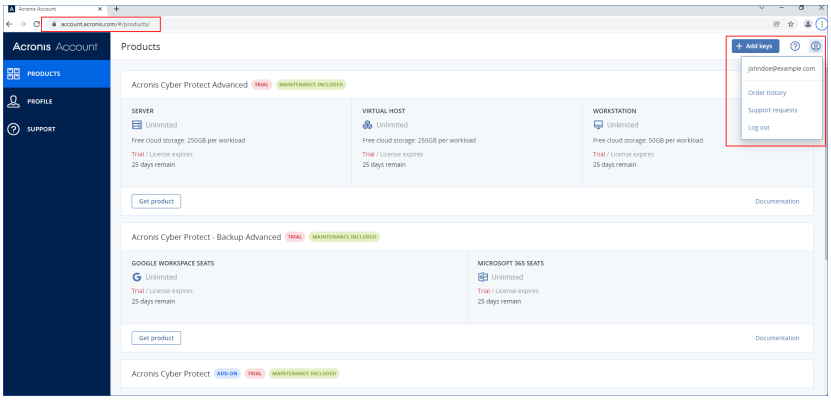
- Die lokale Konsole eines Management Servers in Ihrer lokalen Umgebung bei einer On-Premise-Bereitstellung (`https://<IP-Adresse Ihres Management Servers>:<Port>`)




Hier können Sie die zugeordneten Lizenzen, deren Quota und Nutzung sowie deren Ablaufdatum überprüfen.

Sie verwenden die lokale Konsole zusammen mit der Cloud-Konsole, wenn Sie einen Offline Management Server aktivieren oder diesem Lizenzen zuordnen.

- Acronis Kundenservice- und Support-Portal (Customer Portal) (`https://account.acronis.com`)




Im Acronis Kundenservice- und Support-Portal können Sie Ihre erworbenen Produkte verwalten – beispielsweise das Ablaufdatum Ihrer Abonnements überprüfen, neue Lizenzschlüssel hinzufügen, Lizenzerneuerungen registrieren oder ein Upgrade beantragen. Sie können außerdem das Support-Team kontaktieren, die Produktinstallationsdateien herunterladen oder auf die Produktdokumentation zugreifen.

## Lizenzen verwalten

Die nachfolgende Tabelle gibt einen Überblick über die verfügbaren Aktionen und zeigt, wo sie durchgeführt werden können.

| Aktion | Ort |
|---|---|
| Lizenzen zu Ihrem Konto hinzufügen | Sie fügen die Lizenzen im Acronis Support-Portal (`https://account.acronis.com`) hinzu. Lizenzen, die Sie online erworben haben, werden diesem Konto automatisch hinzugefügt. |
| Einen Management Server aktivieren | Sie können einen Management Server aktivieren, indem Sie ihn in Ihrem Konto registrieren.<br><br>Sie aktivieren die Online Management Server in deren lokalen Konsole (`https://<IP-Adresse Ihres Management Servers>:<Port>`), indem Sie sich an Ihrem Acronis Konto anmelden.<br><br>Die Aktivierung eines Offline Management Servers erfordert, dass Sie bestimmte Aktionen sowohl in der lokalen Konsole als auch in der Cloud-Konsole durchführen. |
| Lizenzen einem Management Server zuordnen<br><br>Eine vorhandene Lizenz-Zuordnung ändern | Auf Online Management Servern werden Lizenzen über die Cloud-Konsole (`https://cloud.acronis.com`) zugeordnet. Die zugeordneten Lizenzen werden automatisch mit dem Management Server synchronisiert.<br><br>Bei Offline Management Servern erfolgt die Zuordnung der Lizenzen über eine Aktivierungsdatei. Für diese Prozedur müssen Sie sowohl die lokale Konsole des Management Servers (`https://<IP-Adresse Ihres Management Servers>:<Port>`) als auch die Cloud-Konsole (`https://cloud.acronis.com`) verwenden. |
| Lizenzen zu Workloads zuweisen | Diese Aktion wird automatisch durchgeführt. |

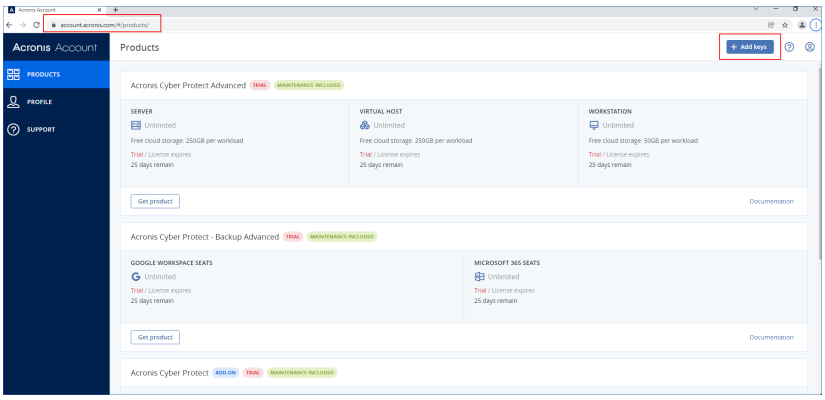
| Aktion | Ort |
| --- | --- |
| Die Registrierung eines Management Servers in Ihrem Konto aufheben | Sie heben die Registerierung eines Online Management Servern mithilfe der Cloud-Konsole (`https://cloud.acronis.com`) auf.<br><br>Sie heben die Registrierung von Offline Management Servern durch eine Deaktivierungsdatei auf. Für diese Prozedur müssen Sie sowohl die lokale Konsole des Offline Management Servers (`https://<IP-Adresse Ihres Management Servers>:<Port>`) als auch die Cloud-Konsole (`https://cloud.acronis.com`) verwenden.<br><br>Um die Registrierung eines Offline Management Servers, auf den Sie keinen Zugriff haben, aufzuheben, verwenden Sie nur die Cloud-Konsole. |

## Lizenzen zu Ihrem Acronis Konto hinzufügen

Wenn Sie eine Lizenz verwenden wollen, müssen Sie diese zuerst Ihrem Acronis Konto hinzufügen. Lizenzen, die Sie online erworben haben, werden automatisch zu Ihrem Konto hinzugefügt. Lizenzen, die Sie offline erworben haben, müssen Sie manuell hinzufügen.

***So können Sie eine Lizenz zu Ihrem Acronis Konto hinzufügen***

1. Melden Sie sich mit den Anmeldedaten Ihres Kontos am Acronis Support-Portal an (`https://account.acronis.com`).
2. Klicken Sie im Navigationsmenü **Produkte**.
3. Klicken Sie auf **Schlüssel hinzufügen**.




4. Geben Sie einen oder mehrere Lizenzschlüssel ein (einen pro Zeile) und klicken Sie dann auf **Hinzufügen**.

> **Hinweis**
> Sie können bis zu 100 Lizenzschlüssel gleichzeitig eingeben.

Die Lizenzen werden nun zu Ihrem Konto hinzugefügt und Sie können deren Verwendung in der Cloud-Konsole (`https://cloud.acronis.com`) verwalten.

**Wichtig**
Bevor Sie auf Acronis Cyber Protect 15 Update 3 upgraden, sollten Sie Ihre lokal gespeicherten Dauerlizenzen in eine Datei exportieren und die Lizenzen dann zu Ihrem Acronis Konto hinzufügen.

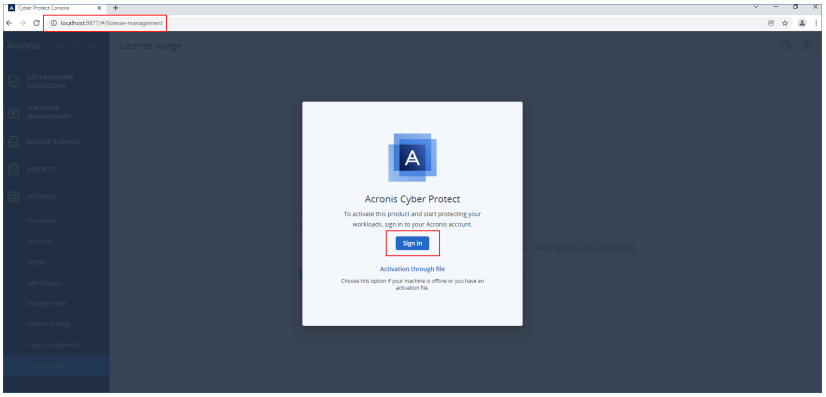
Wenn Sie die Lizenzschlüssel überprüfen wollen, die Sie auf einem Management Server lokal eingegeben haben, gehen Sie zu `https://<IP-Adresse Ihres Management Servers>:<Port>/api/account_server/v2/licensing/legacy/license_keys`.

## Einen Management Server aktivieren

Sie können einen Management Server aktivieren, indem Sie ihn in Ihrem Acronis Konto registrieren.

***So können Sie einen Online Management Server aktivieren***

1. Öffnen Sie nach der Installation des Acronis Cyber Protect Management Servers dessen lokale Konsole (`https://<IP-Adresse Ihres Management Servers>:<Port>`).
2. Klicken Sie in dem sich öffnenden Dialogfenster auf **Anmelden**.




3. Melden Sie sich an Ihrem Acronis Konto an.

Der Management Server wird daraufhin automatisch registriert und aktiviert.

Wenn Sie mit dem Schutz Ihrer Workloads beginnen wollen, müssen Sie diesem Server mindestens eine Lizenz zuordnen. Weitere Informationen über die Zuordnung einer Lizenz finden Sie im Abschnitt '"Lizenzen einem Management Server zuordnen" (S. 31)'.

**Hinweis**
Online Management Server benötigen einen Internetzugriff, um die Lizenzierungsinformationen mit Ihrem Acronis Konto synchronisieren zu können. Wenn ein solcher Server länger als 30 Tage offline bleibt, werden seine Schutzpläne ihre Funktion einstellen und Ihre Workloads dadurch ungeschützt.

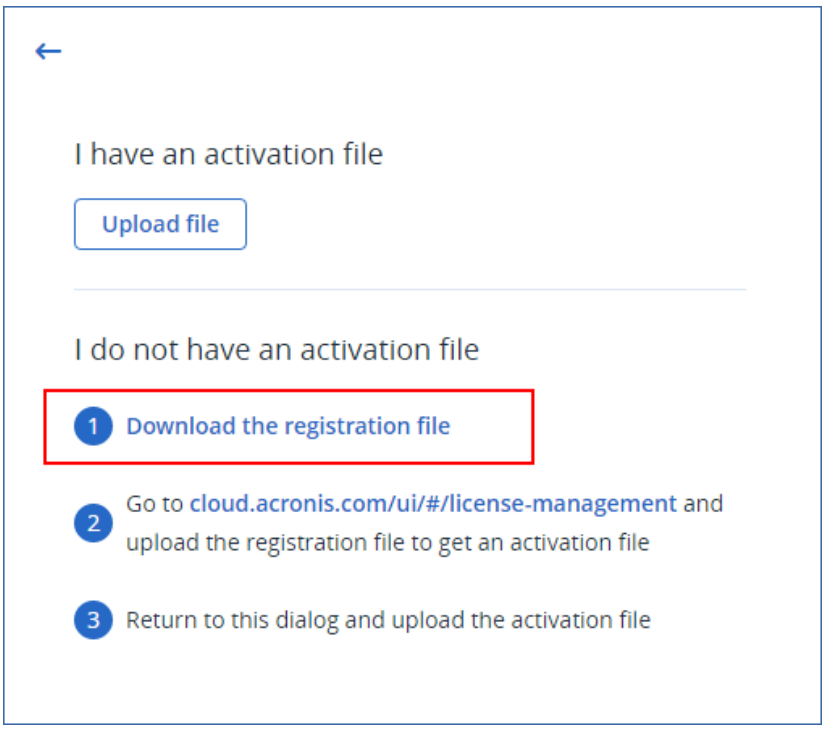
Wenn Sie sich von Ihrem Acronis Konto in der lokalen Konsole abmelden, können keine Lizenzinformationen mehr synchronisiert werden. Wenn Sie sich nicht innerhalb von 30 Tagen erneut anmelden, werden die entsprechenden Schutzpläne außer Kraft gesetzt und Ihre Workloads dadurch ungeschützt.

***So können Sie einen Offline Management Server aktivieren***

Die Aktivierung eines Offline Management Servers erfordert, dass Sie bestimmte Aktionen sowohl in der lokalen Konsole als auch in der Cloud-Konsole durchführen.

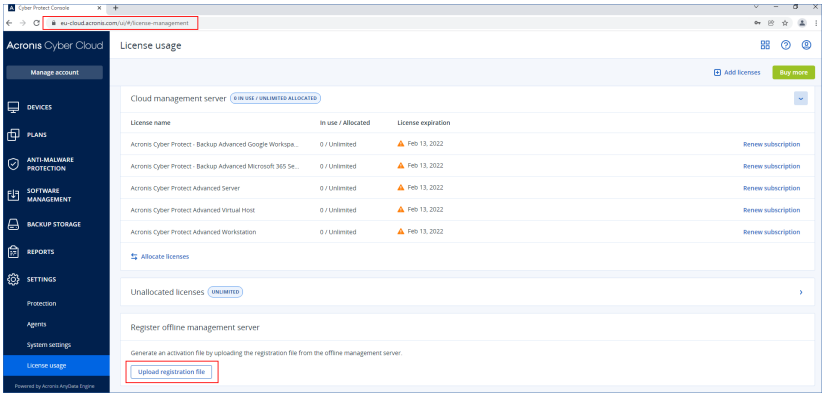
Um auf die Cloud-Konsole zugreifen zu können, benötigen Sie eine zweite Maschine, die über eine Internetverbindung verfügt.

1. Öffnen Sie nach der Installation des Acronis Cyber Protect Management Servers dessen lokale Konsole (`https://<IP-Adresse Ihres Management Servers>:<Port>`).
2. Klicken Sie in dem sich öffnenden Dialogfenster auf **Aktivierung über Datei**.
3. Klicken Sie unter **Ich habe keine Aktivierungsdatei** auf den Befehl **Die Registrierungsdatei herunterladen**.




Die Registrierungsdatei wird auf Ihrer Maschine heruntergeladen.

4. Melden Sie sich auf einer Maschine mit Internetzugriff an der Cloud-Konsole (`https://cloud.acronis.com`) an und gehen Sie dort zu **Einstellungen** –> **Lizenznutzung**.
5. Klicken Sie im Bereich **Offline Management Server registrieren** auf den Befehl **Registrierungsdatei hochladen**.



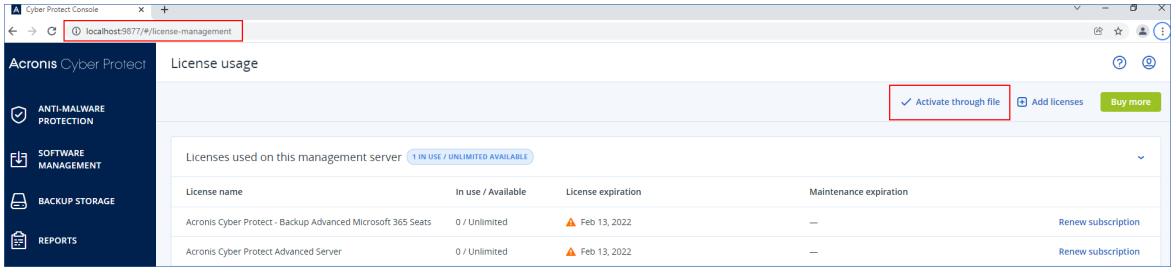
6. Klicken Sie in dem sich öffnenden Dialogfeld auf **Durchsuchen** und wählen Sie dann die Registrierungsdatei, die Sie von Ihrem Offline Management Server heruntergeladen haben.
7. Klicken Sie in dem sich öffnenden Dialogfenster auf **Datei herunterladen**.
   Eine Aktivierungsdatei wird auf Ihrer Maschine heruntergeladen.

**Wichtig**
Wenn dieser Offline Management Server der einzige Management Server in Ihrer Umgebung ist, werden die Lizenzen in Ihrem Acronis Konto diesem Server automatisch zugewiesen. Die Aktivierungsdatei enthält diese Informationen bereits, sodass keine weitere Zuordnung erforderlich ist.

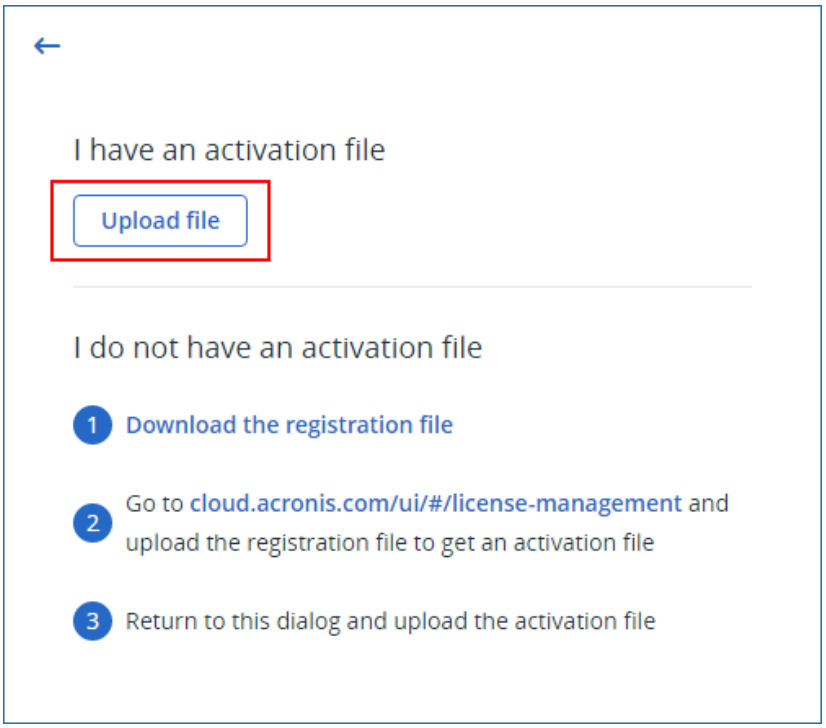
Wenn dies nicht der einzige Management Server in Ihrer Umgebung ist, müssen Sie diesen nach der Aktivierung die vorhandenen Lizenzen zuordnen, indem Sie die Prozedur in Abschnitt '"Lizenzen einem Management Server zuordnen" (S. 31)' befolgen.

8. Wechseln Sie in der lokalen Konsole des Offline Management Servers (`https://<IP-Adresse Ihres Management Servers>:<Port>`) zum Dialogfenster **Aktivierung über Datei**.

**Hinweis**
Wenn die Dialogbox **Aktivierung durch Datei** nicht geöffnet sein sollte, müssen Sie zu **Einstellungen** –> **Lizenznutzung** gehen und dann auf den Befehl **Aktivierung durch Datei** klicken.




9. Klicken Sie unter **Ich habe eine Aktivierungsdatei** auf **Datei hochladen** und wählen Sie dann die Aktivierungsdatei aus, die Sie von der Cloud-Konsole heruntergeladen haben.




Dadurch wird der Offline Management Server in Ihrem Acronis Konto registriert und aktiviert.

**Hinweis**
Ein Management Server, der auf einer virtuellen Maschine läuft, deren UUID nicht eindeutig ist, kann möglicherweise nicht aktiviert werden. Beispielsweise kann es vorkommen, dass die UUID einer virtuellen Maschine dupliziert wird, wenn diese geklont oder mit dem VMware vCenter Converter konvertiert wird. Wenn bei Ihnen ein ähnliches Problem auftritt, kontaktieren Sie den Support.

Weitere Informationen darüber, wie die Duplizierung von UUIDs auf virtuellen VMware-Maschinen verhindert werden kann, finden Sie im (englischsprachigen) Knowledge Base-Artikel Editing a virtual machine with a duplicate UUID.bios (1002403).

## Lizenzen einem Management Server zuordnen

Um eine Lizenz verwenden zu können, müssen Sie deren Quota oder einen Anteil ihrer Quota einem Management Server zuordnen. Sie können einem Management Server mehr als eine Lizenz zuordnen. Außerdem können Sie die Lizenz-Quota aufteilen und verschiedene Anteile der Quota unterschiedlichen Management Servern zuordnen.

**Hinweis**
Wenn es in Ihrem Acronis Konto nur einen einzigen Management Server gibt, werden alle Ihre Lizenzen automatisch diesem Server zugeordnet. Wie Sie Lizenzen einem anderen Management Server zuordnen können, erfahren Sie in Abschnitt '"Lizenz-Quotas zu einem anderen Management Server übertragen" (S. 34)'.

Wenn Sie mehr als einen Management Server in Ihrem Acronis Konto haben, werden die neuen Lizenzen in der Cloud-Konsole (https://cloud.acronis.com) unter **Nicht zugeordnete Lizenzen** angezeigt. Sie müssen diese Lizenzen manuell zuordnen.

Alle Aktionen mit Lizenzen werden automatisch mit den Online Management Servern synchronisiert. Wenn Sie eine Zuordnungsänderung mit einem Offline Management Server synchronisieren wollen, müssen Sie eine neue Aktivierungsdatei erstellen und dann die Zuordnungsprozedur wiederholen. Weitere Informationen über die unterschiedlichen Management Server finden im Abschnitt '"Verschiedene Typen von Management Server" (S. 23)'.

***So können Sie einem Online Management Server Lizenzen zuordnen***

1. Klicken Sie in der Cloud-Konsole (https://cloud.acronis.com) auf **Einstellungen** –> **Lizenznutzung**.
2. Wechseln Sie zu dem Management Server, dem Sie eine Lizenz zuordnen wollen.
3. Klicken Sie auf **Lizenzen zuordnen**.
4. Spezifizieren Sie in dem sich öffnenden Dialogfenster die Lizenz und Lizenz-Quota, die Sie diesem Server zuordnen wollen.
5. Klicken Sie auf **Speichern**.

Dadurch werden die Lizenzierungsinformationen automatisch mit dem Management Server synchronisiert und Sie können die zugeordnete Lizenz verwenden, um Ihre Workloads zu schützen.

Wenn Sie die Zuordnung ändern wollen, müssen Sie die obere Prozedur wiederholen.

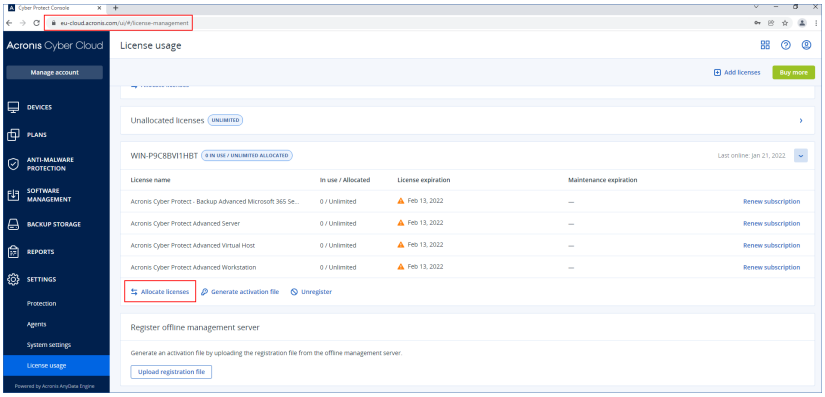
**Wichtig**
Wenn die geänderte Lizenz-Quota kleiner ist als die Anzahl der Protection Agenten, werden die am wenigsten ausgelasteten Agenten ihre Arbeit einstellen. Diese Auswahl erfolgt automatisch. Wenn dies nicht Ihren Anforderungen entspricht, können Sie die verfügbaren Lizenzen manuell neu zuweisen.

***So können Sie einem Offline Management Server Lizenzen zuordnen***

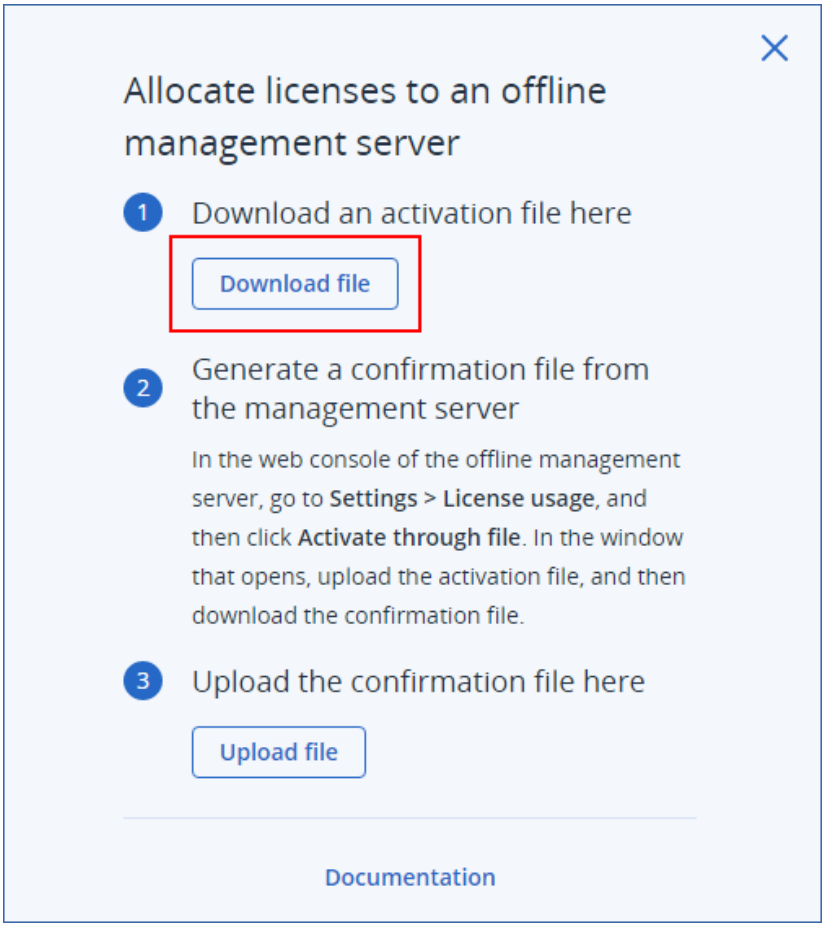
Wenn Sie einem Offline Management Server Lizenzen zuordnen wollen, müssen Sie sowohl die Cloud- als auch die lokalen Konsole verwenden. Um auf die Cloud-Konsole zugreifen zu können, benötigen Sie eine zweite Maschine, die über eine Internetverbindung verfügt.

1. Melden Sie sich auf einer Maschine mit Internetzugriff an der Cloud-Konsole (https://cloud.acronis.com) an und klicken Sie dort auf **Einstellungen** –> **Lizenznutzung**.
2. Wechseln Sie zu dem Management Server, dem Sie eine Lizenz zuordnen wollen.

3. Klicken Sie auf **Lizenzen zuordnen**.



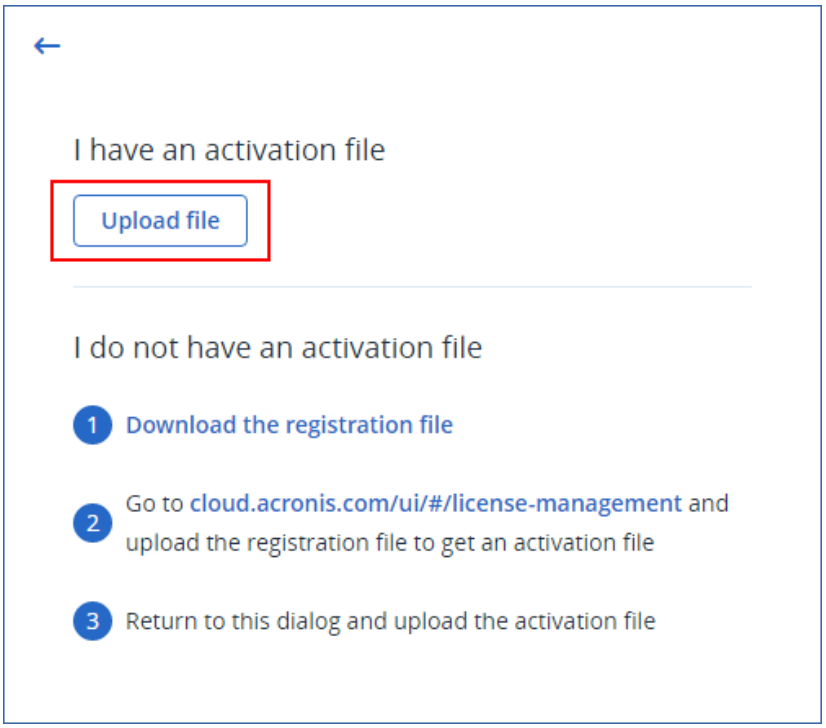

4. Spezifizieren Sie in dem sich öffnenden Dialogfenster die Lizenz und Lizenz-Quota, die Sie diesem Server zuordnen wollen.
5. Klicken Sie auf **Speichern**.
6. Klicken Sie im Dialogfenster **Lizenzen einem Offline Management Server zuordnen** auf den Befehl **Datei herunterladen**.




Die Aktivierungsdatei wird auf Ihrer Maschine heruntergeladen.

7. Gehen Sie in der lokalen Konsole des Offline Management Servers (`https://<IP-Adresse Ihres Management Servers>:<Port>`) zu **Einstellungen** –> **Lizenznutzung** und klicken Sie dann auf den Befehl **Über Datei aktivieren**.

8. Klicken Sie in dem geöffneten Dialogfenster unter **Ich habe eine Aktivierungsdatei** auf **Datei hochladen** – und wählen Sie dann die Aktivierungsdatei aus, die Sie von der Cloud-Konsole heruntergeladen haben.




Als Ergebnis werden die Lizenzierungsinformationen zwischen Ihrem Acronis Konto und dem Offline Management Server synchronisiert.

Wenn Sie die zugeordnete Lizenz-Quota erhöhen wollen, müssen Sie die obere Prozedur wiederholen.

Wie Sie die zugeordnete Lizenz-Quota verringern können, ist in Abschnitt '"Die einem Offline Management Server zugeordnete Lizenz-Quota verringern" (S. 35)' beschrieben.

## Lizenz-Quotas zu einem anderen Management Server übertragen

Sie können eine Lizenz-Quota von einem Management Server zu einem anderen übertragen. Diese Option kann nützlich sein, wenn Lizenzen, die einem bestimmten Management Server zugeordnet wurden, von keinem Workload verwendet werden. Und wenn Sie mehr Lizenzen für einen anderen Management Server benötigen.

**Hinweis**
Wenn es in Ihrem Acronis Konto nur einen einzigen Management Server gibt, werden alle Ihre Lizenzen automatisch diesem Server zugeordnet.

Wenn Sie mehr als einen Management Server in Ihrem Acronis Konto haben, werden die neuen Lizenzen in der Cloud-Konsole (`https://cloud.acronis.com`) unter **Nicht zugeordnete Lizenzen** angezeigt. Sie müssen diese Lizenzen manuell zuordnen.

***So können Sie eine Lizenz-Quota zu einem anderen Management Server übertragen***

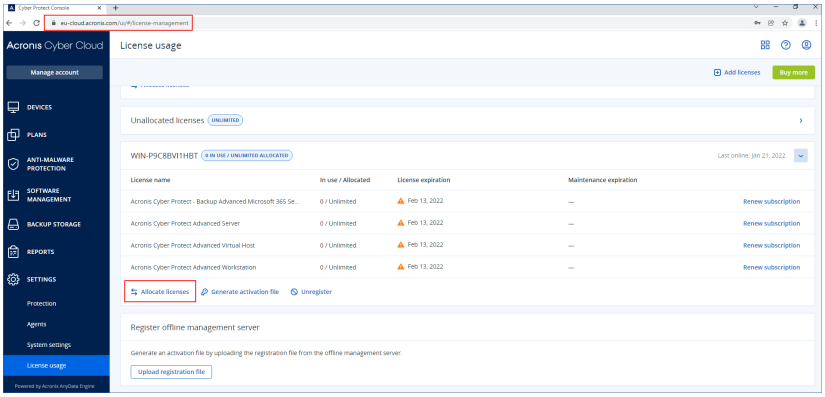
1. Verringern Sie die Lizenz-Quota, die dem ursprünglichen Management Server zugeordnet wurde, indem Sie die Prozedur in Abschnitt '"Lizenzen einem Management Server zuordnen" (S. 31)' befolgen.

   Die freigegebene Lizenz-Quota wird in der Cloud-Konsole im Bereich **Nicht zugeordnete Lizenzen** angezeigt.
2. Ordnen Sie die Lizenz-Quota dem zweiten Management Server zu, indem Sie die Prozedur in Abschnitt '"Lizenzen einem Management Server zuordnen" (S. 31)' befolgen.

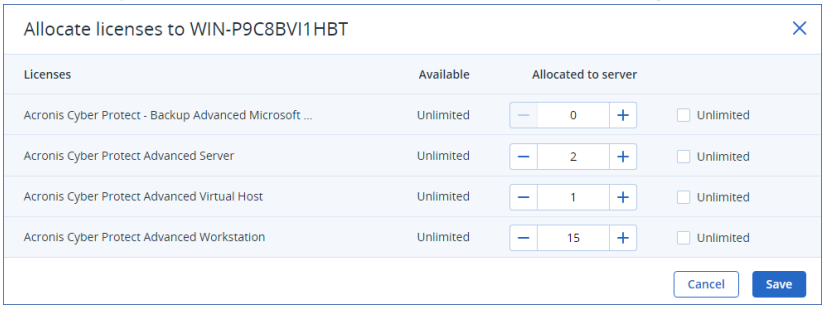
## Die einem Offline Management Server zugeordnete Lizenz-Quota verringern

Wenn Sie die Lizenz-Quota, die einem Offline Management Server zugeordnet ist, verringern wollen, müssen Sie sowohl die Cloud- als auch die lokale Konsole verwenden. Um auf die Cloud-Konsole zugreifen zu können, benötigen Sie eine zweite Maschine, die über eine Internetverbindung verfügt.

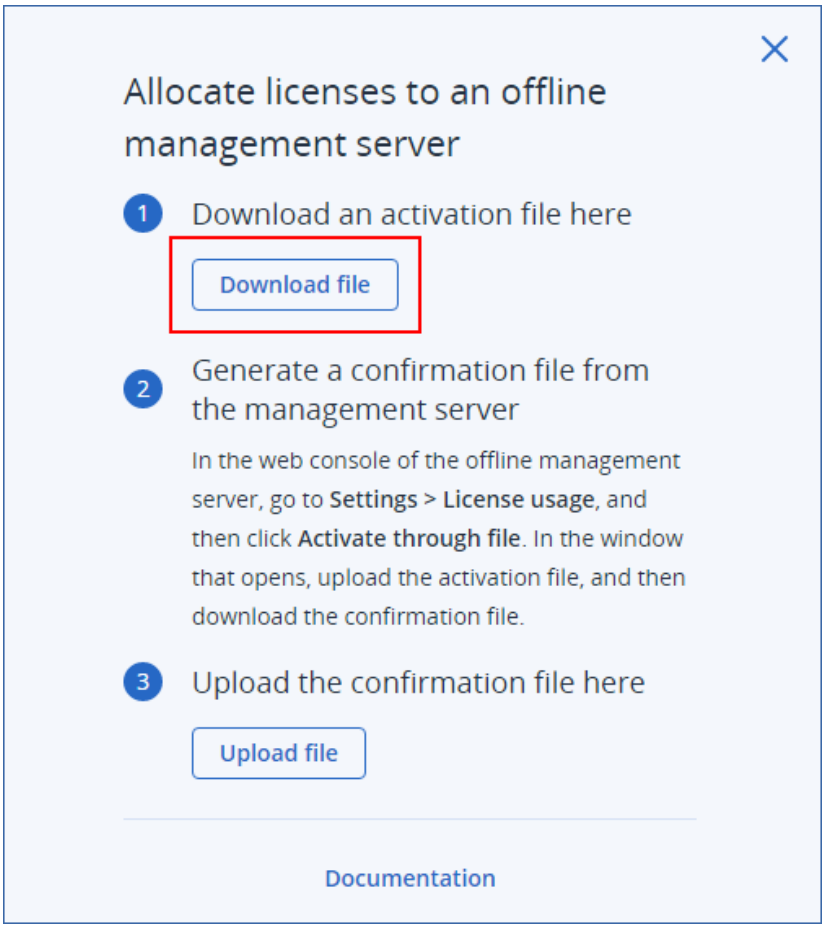
1. Melden Sie sich auf einer Maschine mit Internetzugriff an der Cloud-Konsole (`https://cloud.acronis.com`) an und klicken Sie dort auf **Einstellungen** –> **Lizenznutzung**.
2. Wechseln Sie zu dem Management Server, dem Sie eine Lizenz zuordnen wollen, und klicken Sie dann auf **Lizenzen zuordnen**.




3. Ändern Sie in dem sich öffnenden Dialogfenster die Lizenzen und die Lizenz-Quota, die diesem Server zugeordnet wurden, und klicken Sie dann auf **Speichern**.

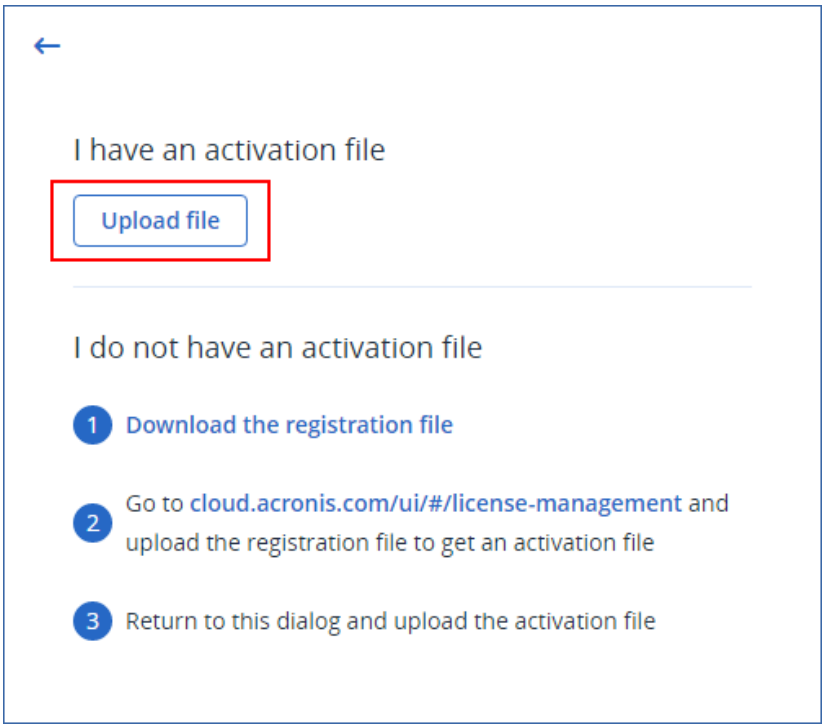



   Die neue Zuordnung ist jetzt noch ausstehend. Wenn Sie diese abbrechen wollen, können Sie auf **Diese Zuordnung entfernen** klicken.
4. Klicken Sie im Dialogfenster **Lizenzen einem Offline Management Server zuordnen** auf den Befehl **Datei herunterladen**.

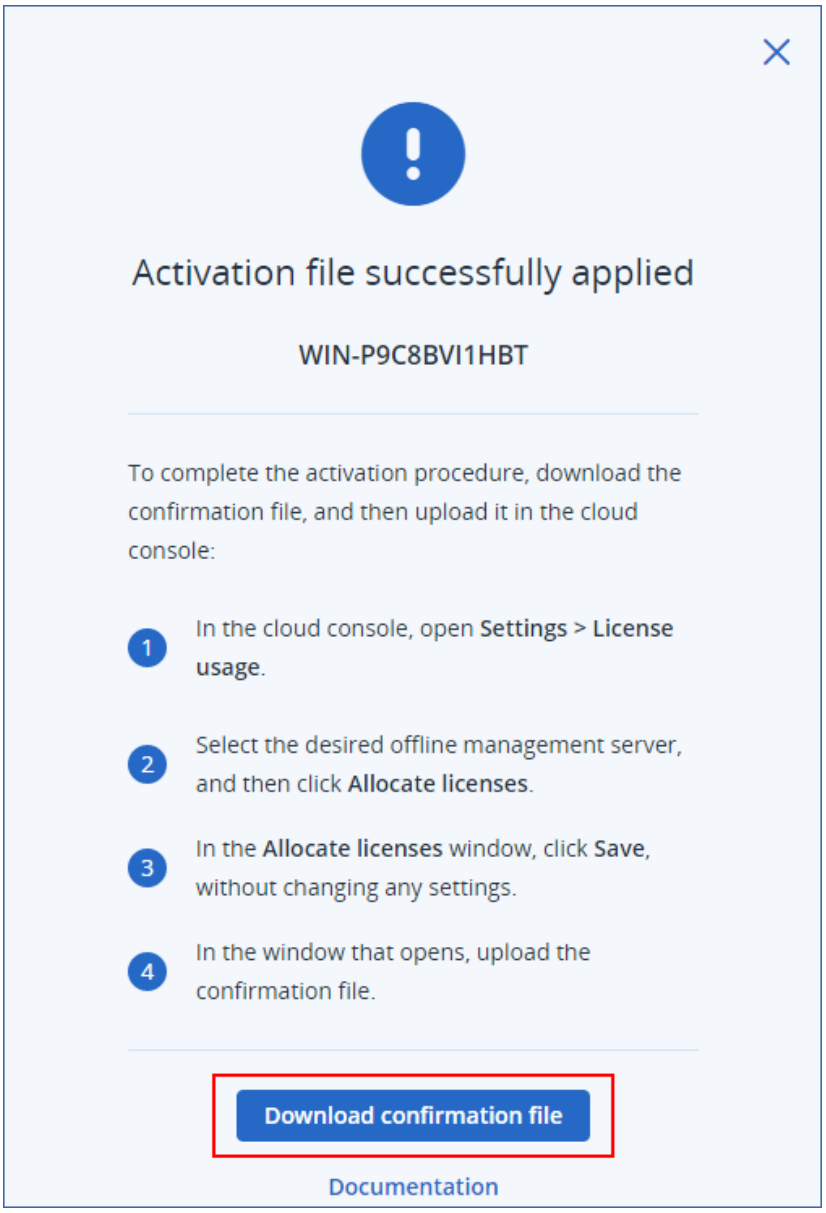



Die Aktivierungsdatei wird auf Ihrer Maschine heruntergeladen.

5. Gehen Sie in der lokalen Konsole des Offline Management Servers (`https://<IP-Adresse Ihres Management Servers>:<Port>`) zu **Einstellungen** –> **Lizenznutzung** und klicken Sie dann auf den Befehl **Über Datei aktivieren**.
6. Klicken Sie in dem geöffneten Dialogfenster unter **Ich habe eine Aktivierungsdatei** auf **Datei hochladen** – und wählen Sie dann die Aktivierungsdatei aus, die Sie von der Cloud-Konsole heruntergeladen haben.

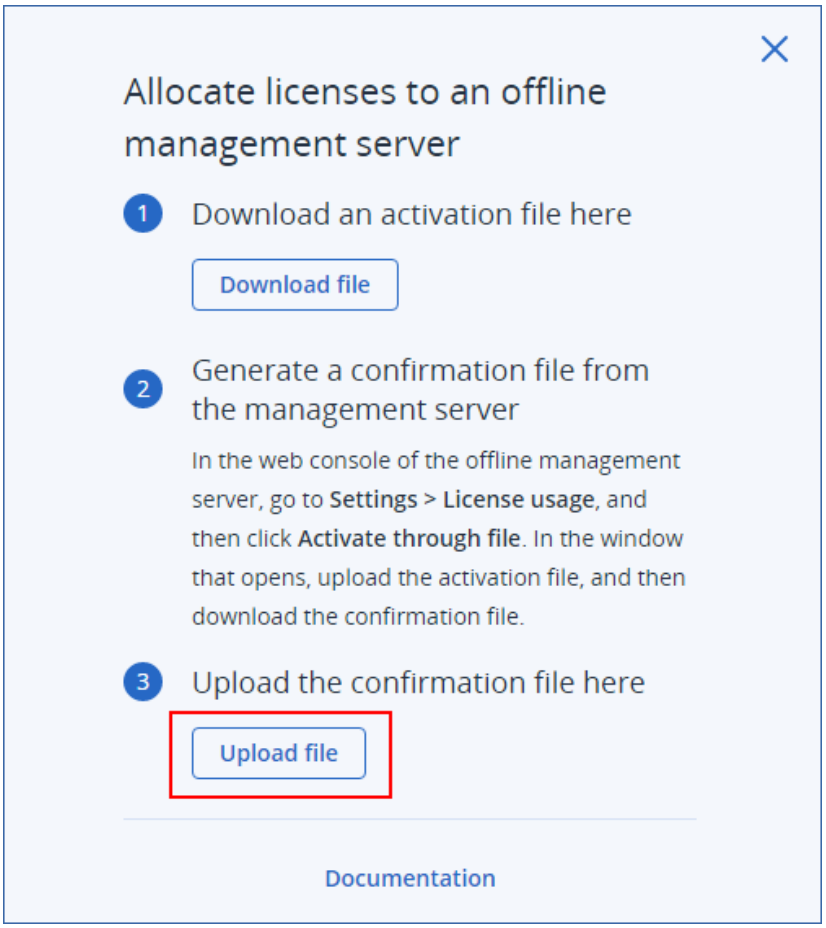



7. Klicken Sie in dem dann geöffneten Dialogfenster auf **Bestätigungsdatei herunterladen**.




Die Bestätigungsdatei wird auf Ihrer Maschine heruntergeladen.

8. Klicken Sie in der Cloud-Konsole (`https://cloud.acronis.com`) auf **Einstellungen** –> **Lizenznutzung**.
9. Wechseln Sie zu dem Management Server, dem Sie eine Lizenz zuordnen wollen, und klicken Sie dann auf **Lizenzen zuordnen**.
10. Klicken Sie in dem dann geöffneten Dialogfenster auf **Speichern**, ohne dabei irgendwelche Einstellungen zu ändern.
11. Klicken Sie im Dialogfenster **Lizenzen einem Offline Management Server zuordnen** auf **Datei hochladen** und wählen Sie dann die Bestätigungsdatei aus, die Sie von Ihrem Offline Management Server heruntergeladen haben.




Als Ergebnis werden die Lizenzierungsinformationen zwischen Ihrem Acronis Konto und dem Offline Management Server synchronisiert.

**Wichtig**
Wenn die geänderte Lizenz-Quota kleiner ist als die Anzahl der Protection Agenten, werden die am wenigsten ausgelasteten Agenten ihre Arbeit einstellen. Diese Auswahl erfolgt automatisch. Wenn dies nicht Ihren Anforderungen entspricht, können Sie die verfügbaren Lizenzen manuell neu zuweisen.

## Die Zuweisung von Lizenzen zu Workloads

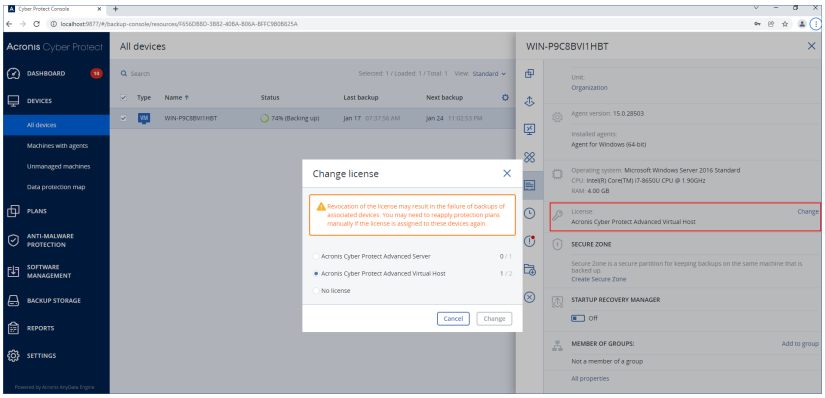
Ein Management Server verteilt die zugeordneten Lizenzen zwischen den Workloads, die auf diesem Server registriert sind.

Der Management Server wird einem Workload dann eine Lizenz zuweisen, wenn Sie erstmalig einen Schutzplan auf diesen Workload anwenden. Wenn dem Management Server mehr als eine Lizenz zugeordnet wurde, wird dem Workload die am besten geeignete Lizenz zugewiesen – in Abhängigkeit von der Art des Workloads, dessen Betriebssystem und der erforderlichen Schutzstufe.

Wenn Sie die zugewiesene Lizenz überprüfen wollen, müssen Sie in der Webkonsole des Management Servers den gewünschten Workload auswählen und dann auf **Details** klicken.

***So können Sie einem Workload eine Lizenz manuell neu zuweisen***

1. Klicken Sie in der lokalen Webkonsole des Management Servers auf **Geräte** und wählen Sie dann den gewünschten Workload aus.
2. Klicken Sie auf **Details**.
3. [Für lokale Management Server] Gehen Sie zum Bereich **Lizenz** und klicken Sie dort auf den Befehl **Ändern**.
4. [Für Cloud Management Server] Gehen Sie zum Bereich **Service-Quota** und klicken Sie dort auf den Befehl **Ändern**.
5. Wählen Sie die gewünschte Lizenz (Service-Quota) aus und klicken Sie dann auf **Ändern**.




## Einschränkungen

Bei Offline Management Servern wird die aktuelle Nutzung der Lizenz-Quota nur in der lokalen Konsole angezeigt. Offline Management Server synchronisieren diese Daten nicht mit Ihrem Acronis Konto und sie sind nicht in der Cloud-Konsole verfügbar.

## Bekannte Probleme und Sachverhalte

In der Cloud-Konsole wird die Lizenznutzung oder die Zuordnung der Lizenz **Virtueller Host** möglicherweise falsch angezeigt. Weitere Informationen finden Sie in diesem Knowledge Base-Artikel.

# Die Registrierung eines Management Servers aufheben

***So können Sie die Registrierung eines Online Management Servers aufheben***

1. Klicken Sie in der Cloud-Konsole (`https://cloud.acronis.com`) auf **Einstellungen** –> **Lizenznutzung**.
2. Finden Sie den gewünschten Management Server und klicken Sie dann auf **Registrierung aufheben**.
3. Das Fenster **Registrierung eines Management Servers aufheben** wird angezeigt.
4. Geben Sie die E-Mail-Adresse ein, die dem Konto zugeordnet ist, um die Deregistrierung zu bestätigen.
5. Klicken Sie auf das **Deregistrierung**.

Infolgedessen werden alle Lizenzen, die dem nicht registrierten Server zugeordnet waren, freigegeben und können einem anderen Management Server in Ihrem Konto zugeordnet werden. In der lokalen Konsole des nicht registrierten Management Servers werden die Lizenzen auf Null zurückgesetzt.

***So können Sie die Registrierung eines Offline Management Servers aufheben***

Es gibt zwei verschiedene Einstiegspunkte, um die Registrierung eines Offline Management Servers aufzuheben:

**In der lokalen Konsole**:

1. Klicken Sie in der lokalen Konsole auf **Registrierung aufheben** in der Zeile, in der das Konto angezeigt wird. Das Fenster **Registrierung eines Management Servers aufheben** wird angezeigt.
2. Geben Sie in das Feld **Anmeldename** die E-Mail-Adresse ein, die dem lokalen Administrator zugeordnet ist.
3. Klicken Sie auf **Registrierung aufheben**.
4. Es wird das Pop-up-Fenster **Die Aufhebung der Registrierung war erfolgreich** angezeigt.
5. Klicken Sie auf **Deregistrierungsdatei herunterladen**.
6. Klicken Sie in der Cloud-Konsole auf **Registrierung aufheben**. Das Fenster **Registrierung eines Management Servers aufheben** wird angezeigt.
7. Klicken Sie auf **Registrierung eines Offline Management Servers aufheben**. Das Fenster **Registrierung eines Offline Management Servers aufheben** wird angezeigt.
8. Klicken Sie auf **Durchsuchen** und wählen Sie dann die Deregistrierungsdatei aus, die Sie von der lokalen Konsole heruntergeladen haben.
9. Klicken Sie auf **Registrierung aufheben**.

**In der Cloud-Konsole**:

1. Melden Sie sich auf einer Maschine mit Internetzugriff an der Cloud-Konsole (`https://cloud.acronis.com`) an und klicken Sie dort auf **Einstellungen** –> **Lizenznutzung**.
2. Finden Sie den gewünschten Management Server und klicken Sie dann auf **Registrierung aufheben**. Das Fenster **Registrierung eines Management Servers aufheben** wird angezeigt.
3. Klicken Sie auf **Registrierung eines Offline Management Servers aufheben**. Das Fenster **Registrierung eines Offline Management Servers aufheben** wird angezeigt.
4. Gehen Sie in der lokalen Konsole desjenigen Management Servers, dessen Registrierung Sie aufheben wollen (`https://<IP-Adresse Ihres Management Servers>:<Port>`), zu **Einstellungen** –> **Lizenznutzung** und klicken Sie dann auf den Befehl **Registrierung aufheben**. Die Deregistrierungsdatei wird auf Ihrer Maschine heruntergeladen.
5. Gehen Sie in der Cloud-Konsole zurück zum Fenster **Registrierung eines Offline Management Servers aufheben**.
6. Klicken Sie auf **Durchsuchen** und wählen Sie dann die Deregistrierungsdatei aus, die Sie von der lokalen Konsole heruntergeladen haben.

7. Klicken Sie auf **Registrierung aufheben**.
8. Wenn Sie keinen Zugriff mehr auf die Maschine haben, auf welcher der Management Server installiert ist, können Sie alternativ auch auf **Ich habe keinen Zugriff auf die Maschine mit dem Management Server** klicken.

   **Warnung!**
   Diese Maschine wird dann dauerhaft blockiert und aus Ihrem Konto entfernt. Sie werden den Management Server daraufhin auf dieser Maschine nicht mehr registrieren können.

Infolgedessen werden alle Lizenzen, die dem nicht registrierten Server zugeordnet waren, freigegeben und können einem anderen Management Server in Ihrem Konto zugeordnet werden. In der lokalen Konsole des nicht registrierten Management Servers werden die Lizenzen auf Null zurückgesetzt.

# Die Lizenzierung in Acronis Cyber Protect 15 Update 2 und früheren Versionen

Um mit der Nutzung von Acronis Cyber Protect 15 Update 2 und früheren Versionen starten zu können, müssen Sie mindestens einen Lizenzschlüssel auf dem Management Server hinzufügen. Eine Lizenz wird einer Maschine dann automatisch zugewiesen, wenn ein Schutzplan auf die Maschine angewendet wird.

Sie können Lizenzen auch manuell zuweisen und widerrufen. Manuelle Aktionen mit Lizenzen sind nur für Organisationsadministratoren verfügbar. Weitere Informationen über die Administratoren finden Sie im Abschnitt '"Abteilungen und administrative Konten" (S. 685)'.

## Lizenzschlüssel zu einem Management Server hinzufügen

In Acronis Cyber Protect 15 Update 2 und älteren Versionen fügen Sie die Lizenzschlüssel dem Management Server hinzu.

***So können Sie Lizenzschlüssel zu einem Management Server hinzufügen***

1. Gehen Sie in der Cyber Protect-Webkonsole zu **Einstellungen** –> **Lizenzen**.
2. Klicken Sie auf **Schlüssel hinzufügen**.
3. Geben Sie einen oder mehrere Lizenzschlüssel ein (einen pro Zeile).
4. Klicken Sie auf **Hinzufügen**.
5. [Wenn Sie Abonnementlizenzschlüssel hinzufügen] Um eine Abonnementlizenz aktivieren zu können, müssen Sie an Ihrem Acronis Konto angemeldet werden.
   a. Geben Sie im Anmeldeformular die Anmeldedaten ein, die Sie für das Acronis Support-Portal verwenden (`https://account.acronis.com`) und klicken Sie dann auf **Anmelden**.
   b. Bestätigen Sie Ihr Konto und klicken Sie dann auf **Sync**.

c. Klicken Sie nach Abschluss der Aktion auf **Fertig**.

6. Klicken Sie im Panel **Lizenzschlüssel hinzufügen** auf **Fertig**.

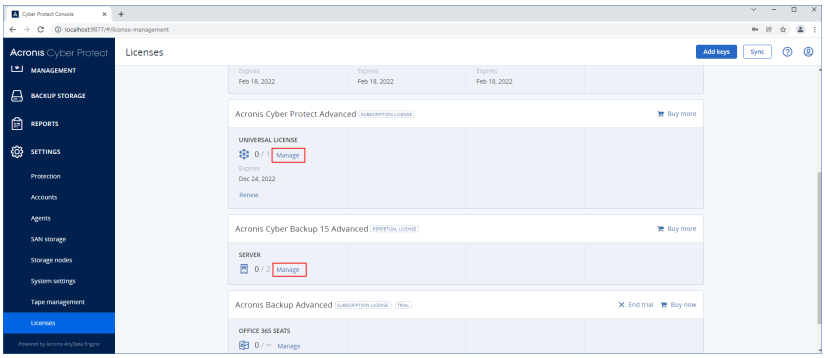
**Hinweis**
Sie können die Abonnementlizenzschlüssel, die in Ihrem Acronis Konto registriert sind, auch automatisch importieren, anstatt sie dem Management Server erneut hinzuzufügen. Wenn Sie die Lizenzschlüssel importieren wollen, klicken Sie im Panel **Lizenzschlüssel hinzufügen** zuerst auf den Befehl **Mit Acronis Konto synchronisieren** und melden Sie sich dann an Ihrem Acronis Konto an.

## Abonnementlizenzen verwalten

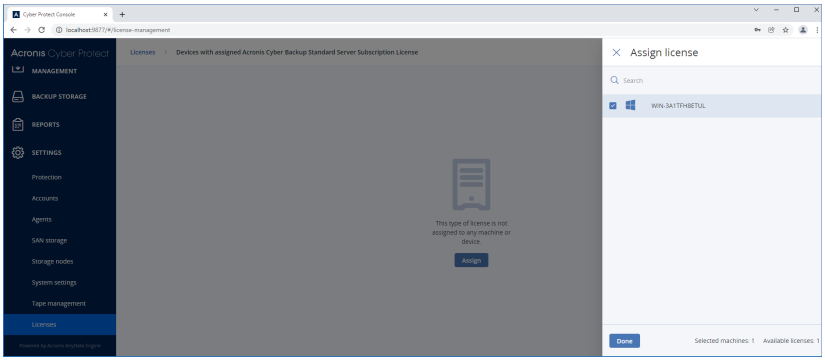
Bevor Sie einem Workload eine Lizenz zuweisen, müssen Sie den Lizenzschlüssel zum Management Server hinzufügen. Weitere Informationen über die entsprechende Durchführung finden Sie im Abschnitt '"Lizenzschlüssel zu einem Management Server hinzufügen" (S. 42)'.

***So können Sie einem Workload eine Abonnementlizenz zuweisen***

1. Gehen Sie in der Cyber Protect-Webkonsole zu **Einstellungen** –> **Lizenzen**.
2. Gehen Sie zur gewünschten Lizenz und klicken Sie dann auf **Verwalten**.




3. Klicken Sie auf **Zuweisen**.
   Die Workloads, denen Sie diese Lizenz zuweisen können, werden angezeigt.




4. Wählen Sie einen Workload aus und klicken Sie dann auf **Fertig**.

***So können Sie eine Abonnementlizenz von einem Workload widerrufen***

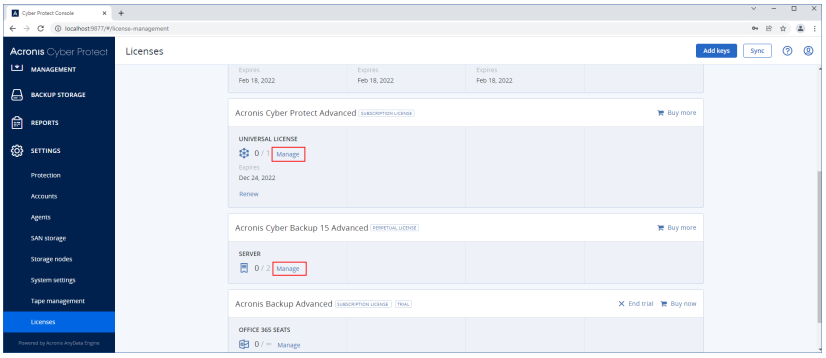
1. Gehen Sie in der Cyber Protect-Webkonsole zu **Einstellungen** –> **Lizenzen**.
2. Gehen Sie zur gewünschten Lizenz und klicken Sie dann auf **Verwalten**.
   Es werden alle Workloads angezeigt, denen diese Lizenz zugewiesen wurde.
3. Wählen Sie den Workload aus, für den Sie die Lizenz widerrufen wollen.
4. Klicken Sie auf **Widerrufen**.
5. Bestätigen Sie Ihre Entscheidung.
   Die widerrufene Lizenz wird freigegeben und Sie können diese dann einem anderen Workload zuweisen.

## Dauerlizenzen verwalten

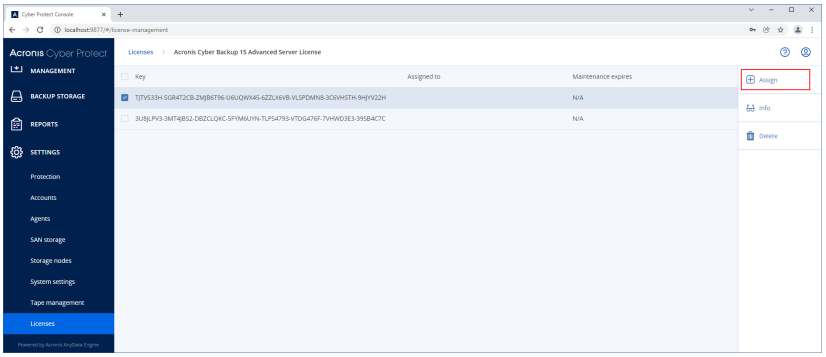
Bevor Sie einem Workload eine Lizenz zuweisen, müssen Sie den Lizenzschlüssel zum Management Server hinzufügen. Weitere Informationen über die entsprechende Durchführung finden Sie im Abschnitt '"Lizenzschlüssel zu einem Management Server hinzufügen" (S. 42)'.

***So können Sie einem Workload eine Dauerlizenz zuweisen***

1. Gehen Sie in der Cyber Protect-Webkonsole zu **Einstellungen** –> **Lizenzen**.
2. Gehen Sie zur gewünschten Lizenz und klicken Sie dann auf **Verwalten**.




   Die zur ausgewählten Lizenz gehörenden Lizenzschlüssel werden angezeigt.
3. Wählen Sie den Lizenzschlüssel aus, den Sie einem bestimmten Workload zuweisen wollen.
4. Klicken Sie auf **Zuweisen**.




   Die Workloads, denen Sie diesen Lizenzschlüssel zuweisen können, werden angezeigt.
5. Wählen Sie einen Workload aus und klicken Sie dann auf **Fertig**.

***So können Sie eine Dauerlizenz von einem Workload widerrufen***

1. Gehen Sie in der Cyber Protect-Webkonsole zu **Einstellungen** –> **Lizenzen**.
2. Wählen Sie die gewünschte Lizenz aus und klicken Sie dann auf **Verwalten**.
   Die zur ausgewählten Lizenz gehörenden Lizenzschlüssel werden angezeigt. Überprüfen Sie in der Spalte **Zugewiesen zu** den Workload, dem dieser Lizenzschlüssel zugewiesen wurde.
3. Wählen Sie den Lizenzschlüssel aus, den Sie widerrufen wollen.
4. Klicken Sie auf **Widerrufen**.
5. Bestätigen Sie Ihre Entscheidung.
   Der widerrufene Lizenzschlüssel verbleibt in der Lizenzliste und Sie können ihn dann einem anderen Workload zuweisen.

# Installation

## Installationsübersicht

Acronis Cyber Protect unterstützt zwei Methoden der Bereitstellung: on-premise (lokal) und Cloud. Der wesentliche Unterschied zwischen diesen beiden Varianten besteht darin, wo sich der Acronis Cyber Protect Management Server befindet.

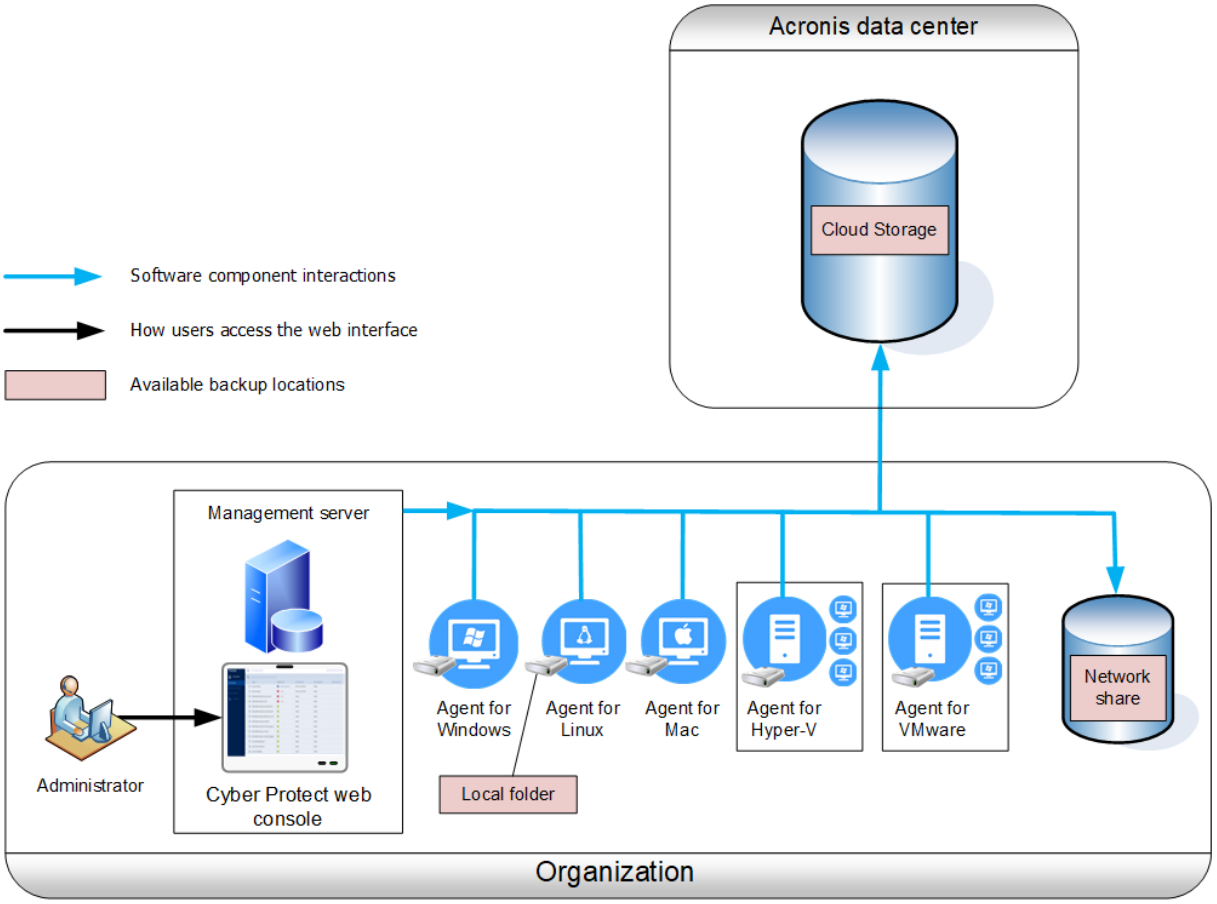
Der Management Server ist der zentrale Verwaltungspunkt für all Ihre Backups Bei der On-Premise-Bereitstellung ist der Management Server in Ihrem lokalen Netzwerk installiert – während er sich bei der Cloud-Bereitstellung in einem der Acronis Datacenter befindet. Die Benutzeroberfläche für diesen Server wird auch Cyber Protect-Webkonsole genannt.

Der Management Server ist für die Kommunikation mit den Protection Agenten verantwortlich und ermöglicht die Durchführung von allgemeinen Funktionen zur Planverwaltung. Vor jeder Schutzaktivität kontaktieren die Agenten den Management Server, um die Vorgaben zu überprüfen. Manchmal kann die Verbindung zum Management Server verloren gehen, wodurch die Bereitstellung neuer Schutzpläne verhindert wird. Wenn jedoch auf einer Maschine bereits ein Schutzplan bereitgestellt wurde, setzt der Agent die Schutzaktionen für 30 Tage (seit die Kommunikation mit dem Management Server verloren ging) fort.

Bei beiden Arten der Bereitstellung ist es erforderlich, dass ein Protection Agent auf jeder Maschine installiert ist, die Sie per Backup sichern wollen. Bei beiden werden dieselben Storage-Typen unterstützt. Der jeweilige Speicherplatz im Cloud Storage wird separat verkauft, unabhängig von der eigentlichen Acronis Cyber Protect-Lizenz.

## On-Premise-Bereitstellung

On-Premise-Bereitstellung bedeutet, dass alle Produktkomponenten in Ihrem lokalen Netzwerk installiert sind. Dies ist die einzige Bereitstellungsmethode, die bei einer Dauerlizenz verfügbar ist. Sie müssen diese Methode außerdem verwenden, wenn Ihre Maschinen über keine Internetverbindung verfügen.




## Speicherort des Management Servers

Sie können den Management Server auf einer Maschine installieren, die entweder unter Windows oder Linux läuft.

Wir empfehlen eine Installation unter Windows, weil Sie dann Agenten vom Management Server aus auf anderen Maschinen bereitstellen können. Mit einer Advanced-Lizenz ist es möglich, Organisationseinheiten (Abteilungen) zu erstellen und diesen Abteilungen dann Administratoren hinzuzufügen. Auf diese Weise können Sie die Schutzverwaltung an andere Personen delegieren, deren Zugriffsberechtigungen streng auf die entsprechenden Abteilungen begrenzt sind.

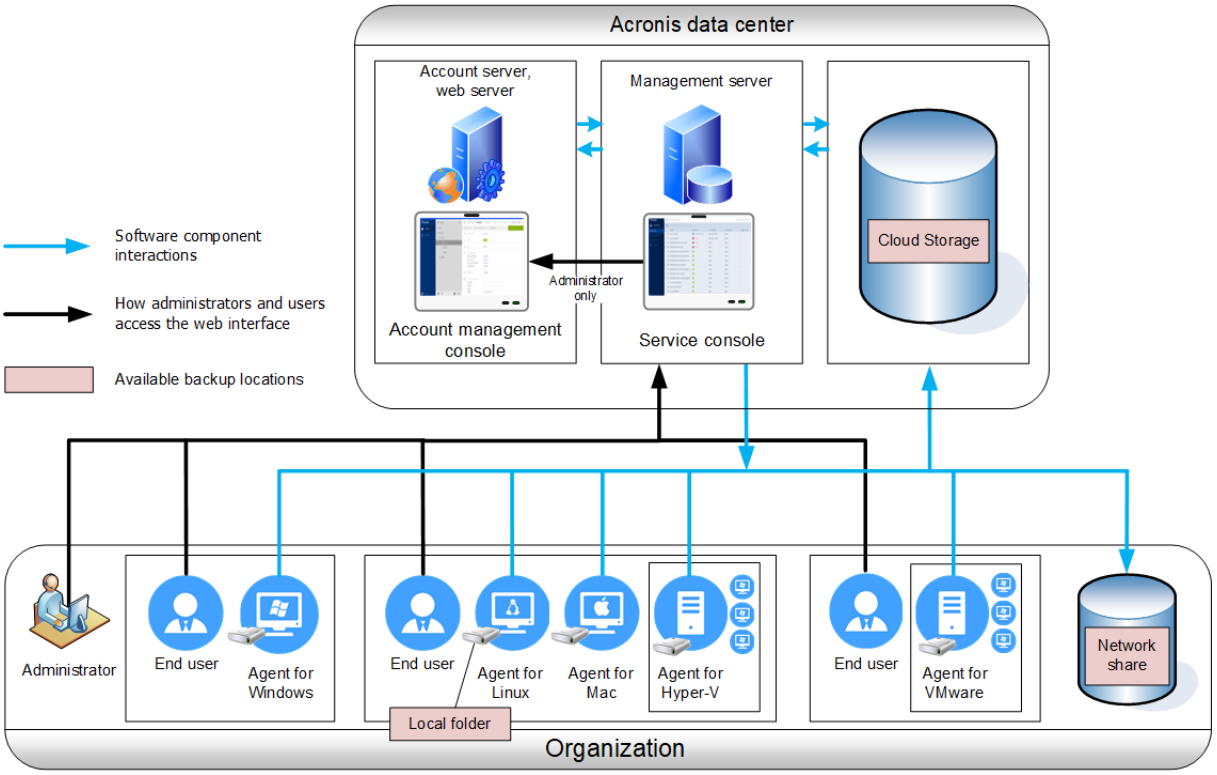
Eine Installation unter Linux empfiehlt sich dann, wenn Sie eine ausschließliche Linux-Umgebung haben. Sie müssen den Agenten hier auf jeder Maschine, die Sie per Backup sichern wollen, lokal installieren.

# Cloud-Bereitstellung

Cloud-Bereitstellung bedeutet, dass sich der Management Server in einem der Acronis Datacenter befindet. Der Vorteil dieses Ansatzes ist es, dass Sie den Management Server nicht in Ihrem lokalen Netzwerk vorhalten bzw. verwalten müssen. Sie können Acronis Cyber Protect auch als einen Cyber Protection Service ansehen, der Ihnen von Acronis bereitgestellt wird.

Der Zugriff auf den Account Server ermöglicht Ihnen, Benutzer zu erstellen, für diese Benutzer bestimmte Quotas über die Service-Nutzung festzulegen und Benutzergruppen (in Form von Abteilungen) zu erstellen, die die Struktur Ihres Unternehmens widerspiegeln. Jeder Benutzer kann auf die Cyber Protect Webkonsole zugreifen, den erforderlichen Agenten herunterladen und in wenigen Minuten auf seiner Maschine installieren.

Administrator-Konten können auf Abteilungs- oder Unternehmensebene erstellt werden. Jedes Konto hat eine Anzeige, die auf den jeweiligen Kontrollbereich begrenzt ist. Benutzer können jeweils immer nur auf ihre eigenen Backups zugreifen.




Die nachfolgende Tabelle fasst die Unterschiede zwischen On-Premise- und Cloud-Bereitstellung zusammen. Jede Spalte listet die Funktionen auf, die nur im entsprechenden Bereitstellungstyp verfügbar sind.

| On-Premise-Bereitstellung | Cloud-Bereitstellung |
|---|---|
| • Dauerlizenzen können verwendet werden<br>• Ein lokal bereitgestellter Management Server, der in Air-Gap-Umgebungen eingesetzt werden kann*<br>• SFTP-Server als Backup-Speicherort<br>• Acronis Cyber Infrastructure als Backup-Speicherort<br>• Bandgeräte und Acronis Storage Nodes als Backup-Speicherorte**<br>• Upgrade von früheren Versionen von Acronis | • Cloud-zu-Cloud-Backup von Microsoft 365-Daten, inklusive Data Protection für Gruppen, öffentlichen Ordnern, OneDrive-*** und SharePoint Online-Daten<br>• Cloud-zu-cloud-Backup von Google Workspace-Daten<br>• Der Agent für Mac unterstützt sowohl x64- als auch ARM-basierte Prozessoren (wie Apple Silicon M1 und M2)<br>• Agent für Virtuozzo (Backup von virtuellen |

| | |
|---|---|
| Cyber Protect (inkl. Acronis Backup für VMware) | Virtuozzo-Maschinen auf der Hypervisor-Ebene)<br>• Agent für oVirt (Backup von virtuellen oVirt KVM-Maschinen auf der Hypervisor-Ebene)<br>• Agent für Virtuozzo Hybrid Infrastructure (Backup von virtuellen Virtuozzo Hybrid Infrastructure-Maschinen auf der Hypervisor-Ebene)<br>• Disaster Recovery als Cloud Service**** |

Weitere Informationen darüber, wie Sie den Management Server in einer Air-Gap-Umgebung aktivieren können, finden Sie in Abschnitt '"So können Sie einen Offline Management Server aktivieren" (S. 28)'

** Die Funktion ist in der Standard Edition nicht verfügbar.

***Das OneDrive-Stammverzeichnis wird standardmäßig von Backup-Aktionen ausgeschlossen. Wenn Sie jedoch festlegen, dass bestimmte OneDrive-Dateien und -Ordner gesichert werden sollen, dann werden diese auch in das Backup aufgenommen. Dateien, die nicht auf dem Gerät vorhanden sind, werden im Archiv ungültige Inhalte haben.

*** Die Funktion ist nur mit dem Disaster Recovery-Add-on verfügbar.

# Komponenten

## Agenten

Agenten sind Applikationen, die auf den Maschinen, die von Acronis Cyber Protect verwaltetet werden, bestimmte Aktionen wie Backups oder Wiederherstellungen durchführen.

Der Agent für Windows wird zusammen mit dem Agenten für Exchange, dem Agenten für SQL, dem Agenten für Active Directory und dem Agenten für Oracle installiert. 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.

Einige Agenten können nur auf Maschinen mit bestimmten Rollen oder Applikationen installiert werden. So wird beispielsweise der Agent für Hyper-V auf Maschinen mit der Hyper-V-Rolle installiert, der Agent für SQL auf Maschinen mit SQL-Datenbanken, der Agent für Exchange auf Maschinen mit der Postfachrolle des Microsoft Exchange Servers und der Agent für Active Directory auf Domain Controllern.

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.

| Was möchten Sie sichern? | Welchen Agenten soll ich installieren? | Wo soll die Installation erfolgen? | Agent-Verfügbarkeit | |
|---|---|---|---|---|
| | | | On-Premise (lokal) | Cloud |
| **Physische Maschinen** | | | | |
| Laufwerke, Volumes und Dateien auf physischen Maschinen mit Windows | Agent für Windows | Auf der Maschine, die gesichert werden soll. | + | + |
| Laufwerke, Volumes und Dateien auf physischen Maschinen mit Linux | Agent für Linux | | + | + |
| Laufwerke, Volumes und Dateien auf physischen Maschinen mit macOS | Agent für Mac | | + | + |
| **Applikationen** | | | | |
| SQL-Datenbanken | Agent für SQL | Auf der Maschine, die den Microsoft SQL Server ausführt. | + | + |
| Exchange-Datenbanken und -Postfächer | Agent für Exchange | Auf der Maschine, auf der die Postfachrolle des Microsoft Exchange Servers ausgeführt wird.***** Wenn nur das Postfach- Backup benötigt wird, kann der Agent auf jeder Maschine installiert werden, die Netzwerkzugriff auf diejenige Maschine hat, auf welcher die Rolle 'Clientzugriff' des Microsoft Exchange | + | + Kein Postfach-Backup |

| | | | | |
|---|---|---|---|---|
| | | Servers aktiviert ist. | | |
| Microsoft 365-Postfächer | Agent für Office 365 | Auf einer Windows-Maschine, die über eine Internetverbindung verfügt. | + | + |
| 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 Scale Computing HC3-Maschinen | Agent für Scale Computing HC3 | Auf dem Scale Computing HC3-Host. | + | + |
| Virtuelle Maschinen, auf Windows Azure gehostet | Wie bei den physischen Maschinen*** | Auf der Maschine, die gesichert werden soll. | + | + |
| Virtuelle Maschinen, die auf Amazon EC2 gehostet werden | | | + | + |

| | | | | |
|---|---|---|---|---|
| Virtuelle Citrix XenServer-Maschinen | | | +**** | + |
| Virtuelle Red Hat Virtualization (RHV/RHEV)-Maschinen | | | | |
| 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 'LAN-freies Backup'.

***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 sie jedoch als virtuelle Maschine gezählt, wenn Sie in einer Cloud-Bereitstellung Quotas für eine bestimmte Anzahl von Maschinen festlegen.

****Mit einer Acronis Cyber Protect Advanced Virtual Host-Lizenz werden diese Maschinen als virtuelle Maschinen betrachtet (Pro-Host-Lizenzierung wird verwendet). Mit einer Acronis Cyber Protect Virtual Host-Lizenz werden diese Maschinen als physische Maschinen betrachtet (Pro-Maschine-Lizenzierung wird verwendet).

## Andere Komponenten

| Komponente | Funktion | Wo soll die Installation erfolgen? | Verfügbarkeit | |
|---|---|---|---|---|
| | | | On-Premise (lokal) | Cloud |
| Management Server | Der Management Server ist der zentrale Verwaltungspunkt für all Ihre Backups Bei einer On-Premise-Bereitstellung wird der Management Server in Ihrem lokalen Netzwerk installiert.<br>Er verwaltet die Agenten und stellt den Anwendern die webbasierte Benutzeroberfläche zur Verfügung. | Auf einer Maschine, die unter Windows oder Linux läuft. | + | - |
| Komponenten zur Remote-Installation | Speichert Agenten-Installationspakete in einem lokalen Ordner. | Auf der Windows-Maschine, die den Management Server ausführt. | + | - |
| Scan Service | Eine optionale Komponente, die Antimalware-Scans von Backups in einem Cloud Storage oder in einem lokalen oder Netzwerk-Ordner ermöglicht.<br>Der Scan Service erfordert eine Microsoft SQL Server- oder PostgreSQL-Datenbank. Er ist nicht mit der Standard-SQLite-Datenbank kompatibel, die der Management Server verwendet. | Auf der Windows- oder Linux-Maschine, die den Management Server ausführt. | + | - |

| | | | | |
|---|---|---|---|---|
| Bootable Media Builder | Erstellt ein Boot-Medium. | Auf einer Maschine, die unter Windows oder Linux läuft. | + | - |
| Befehlszeilenwerkzeug | Unterstützt eine Befehlszeilenschnittstelle über das Utility **acrocmd**. **acrocmd** enthält jedoch keine Tools, die die Befehle selbst physisch ausführen. Es stellt lediglich eine Befehlszeilenschnittstelle zu den entsprechenden Komponenten von Cyber Protect bereit – den Agenten und dem Management Server. | Auf einer Maschine, die unter Windows, Linux oder macOS läuft. | + | + |
| Acronis Cyber Protect 15 Monitor | Stellt eine grafische Benutzeroberfläche für den Agenten für Windows und den Agenten für Mac bereit. Er zeigt Informationen über den Schutzstatus der Maschine an, auf welcher der Agent installiert ist, und ermöglicht es den entsprechenden Anwendern, die Backup-Verschlüsselung und die Proxy-Server-Einstellungen zu konfigurieren.<br>Unter Windows verlangt der Acronis Cyber Protect 15 Monitor, dass der Agent für Windows auf derselben Maschine installiert ist. | Auf einer Maschine, die unter Windows oder macOS läuft. | + | + |
| Storage Node | Speichert Backups. Wird zur Katalogisierung und Deduplizierung benötigt. | Auf einer Maschine, die unter Windows | + | - |

| | | | | |
|---|---|---|---|---|
| | Der Storage Node setzt voraus, dass der Agent für Windows auf derselben Maschine installiert ist. | läuft. | | |
| Katalogdienst | Führt die Katalogisierung von Backups auf Storage Nodes durch. | Auf einer Maschine, die unter Windows läuft. | + | - |
| PXE Server | Ermöglicht es, Maschinen über das Netzwerk mit einem Boot-Medium zu starten. | Auf einer Maschine, die unter Windows läuft. | + | - |

# Acronis Cyber Protect zusammen mit anderen Sicherheitslösungen in Ihrer Umgebung verwenden

Sie können Acronis Cyber Protect allein oder zusammen mit anderen Sicherheitslösungen (wie z.B. einer eigenständigen Antivirus-Software) in Ihrer Umgebung verwenden.

Ohne eine andere Sicherheitslösung können Sie Acronis Cyber Protect zur umfassenden Cyber Protection oder für herkömmliches Backup & Recovery-Anwendungen nutzen – je nach vorhandener Lizenz und Bedarf. Ausführliche Informationen über die in jeder Edition enthaltenen Funktionen finden Sie im Abschnitt 'Acronis Cyber Protect 15 – Vergleich der Editionen (inkl. Cloud-Bereitstellung)'. Sie können den Umfang Ihrer Schutzpläne anpassen, indem Sie nur diejenigen Module aktivieren, die Sie benötigen.

Sie können Acronis Cyber Protect als komplette Cyber Protection-Lösung einsetzen (inklusive Schutz vor Viren und anderer Malware) – und das auch, wenn Sie bereits eine andere Sicherheitslösung in Ihrer Umgebung haben. In diesem Fall müssen Sie die andere Sicherheitslösung deaktivieren oder entfernen, um Konflikte zu vermeiden.

Alternativ dazu wolle Sie vielleicht Ihre Cyber Protection verbessern, ohne Ihre aktuell eingesetzte Sicherheitslösung zu deaktivieren oder zu entfernen. Auch das ist möglich. Sie müssen lediglich darauf achten, dass Sie das Antivirus & Antimalware Protection-Modul nicht in Ihren Schutzplänen einsetzen. Alle anderen Module können uneingeschränkt verwendet werden.

## Einschränkungen

- Antimalware-Scan von Backups – erfordert, dass Sie Scan Service zusammen mit dem Cyber Protect Management Server installieren.
- Remote-Zugriff über einen HTML5-Client – ist nur verfügbar, wenn der Cyber Protect Management Server auf einer Linux-Maschine installiert ist.

# Software-Anforderungen

## Unterstützte Webbrowser

Die Weboberfläche unterstützt folgende Webbrowser:

- Google Chrome 29 (oder später)
- Mozilla Firefox 23 (oder höher)
- Opera 16 (oder höher)
- Windows Internet Explorer 10 (oder höher)

**Hinweis**
Bei Cloud-Bereitstellungen wird der Internet Explorer nicht unterstützt.

- Microsoft Edge 25 (oder höher)
- Safari 8 (oder höher), unter den Betriebssystemen macOS oder iOS ausgeführt

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

## Unterstützte Betriebssysteme und Umgebungen

### Agenten

#### Agent für Windows

- Windows XP Professional SP1 (x64), SP2 (x64), SP3 (x86)
- Windows XP Professional SP2 (x86) – wird mit einer speziellen Version des Agenten für Windows unterstützt. Weitere Details und Einschränkungen für diese Unterstützung finden Sie im Abschnitt 'Agent für Windows XP SP2'.
- Windows XP Embedded SP3
- Windows Server 2003 SP1/2003 R2 und höher – die Editionen Standard und Enterprise (x86, x64)

**Hinweis**
Acronis Cyber Protect benötigt das Microsoft-Update KB940349, das nicht mehr separat heruntergeladen werden kann. Installieren Sie alle derzeit verfügbaren Updates für den Windows Server 2003, um sicherzustellen, dass die ursprünglich von KB940349 bereitgestellte Funktionalität auf Ihrer Maschine auch verfügbar ist.
Weitere Informationen zum Update KB940349 finden Sie in diesem Knowledge Base-Artikel.

- Windows Small Business Server 2003/2003 R2

- Windows Server 2008 – die Editionen Standard, Enterprise, Datacenter, Foundation und Web (x86, x64)
- Windows Small Business Server 2008
- Windows 7 – alle Editionen (x86, x64)

**Hinweis**
Wenn Sie Acronis Cyber Protect noch mit Windows 7 verwenden wollen, müssen Sie sicherstellen, dass Sie folgende Updates von Microsoft installiert haben:

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

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

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

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

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. Es gilt jedoch die folgende Ausnahme:

- Der Agent für SQL wird nicht für On-Premise-Bereitstellungen auf den Windows 7 Starter- und Home-Editionen (x86, x64) unterstützt

### Agent für Exchange (für Postfach-Backups)

Dieser Agent kann auf einer Maschine mit oder ohne Microsoft Exchange Server installiert werden.

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

### Agent für 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
- Windows 11 – alle Editionen
- Windows Server 2022 – alle Installationsoptionen, mit Ausnahme des Nano Servers

### Agent für Oracle

- Windows Server 2008 R2 – Standard, Enterprise, Datacenter und Web Editionen (x86, x64)
- Windows Server 2012 R2 – Standard, Enterprise, Datacenter und Web Editionen (x86, x64)

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

## Agent für Linux

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

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

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

- Red Hat Enterprise Linux 4.x, 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*, 8.6*, 8.7*
- Ubuntu 9.10, 10.04, 10.10, 11.04, 11.10, 12.04, 12.10, 13.04, 13.10, 14.04, 14.10, 15.04, 15.10, 16.04, 16.10, 17.04, 17.10, 18.04, 18.10, 19.04, 19.10, 20.04, 20.10, 21.04, 21.10, 22.04
- 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, 11, 12, 15

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

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

Wenn Ihre Linux-Distribution den D-Bus-Mechanismus nicht unterstützt (wie z.B. bei Red Hat Enterprise Linux 6.x oder CentOS 6.x), wird Acronis Cyber Protect den Standard-Speicherort für sichere Schlüssel verwenden, weil das Betriebssystem keinen D-Bus-kompatiblen Speicherort bereitstellt.

* Wird nur mit Kerneln von 4.18 bis 5.19 unterstützt

## Agent für Mac

**Hinweis**
ARM-basierte Prozessoren (wie Apple Silicon M1 und M2) werden nicht unterstützt.

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

## Agent für VMware (Virtuelle Appliance)

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

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

## Agent für VMware (Windows)

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

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

## Agent für Hyper-V

- Windows Server 2008 (nur x64) mit Hyper-V-Rolle, inklusive Server Core-Installationsmodus
- Windows Server 2008 R2 mit Hyper-V-Rolle, inklusive Server Core-Installationsmodus

- Microsoft Hyper-V Server 2008/2008 R2
- Windows Server 2012/2012 R2 mit Hyper-V-Rolle, inklusive Server Core-Installationsmodus
- Microsoft Hyper-V Server 2012/2012 R2
- Windows 8, 8.1 (nur x64) mit Hyper-V
- Windows 10 – die Editionen Pro, Education und Enterprise mit Hyper-V
- Windows Server 2016 mit Hyper-V-Rolle – alle Installationsoptionen, mit 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
- Windows Server 2022 mit Hyper-V – alle Installationsoptionen, mit Ausname des Nano Servers

### Agent für Scale Computing HC3 (Virtuelle Appliance)

Dieser Agent wird als virtuelle Appliance ausgeliefert, die über die Cyber Protect Webkonsole im Scale Computing HC3-Cluster bereitgestellt wird. Es gibt keinen Standalone-Installer für diesen Agenten.

Scale Computing Hypercore 8.8, 8.9, 9.0

## Management Server (nur bei On-Premise-Bereitstellung)

### Unter Windows:

- Windows 7 – alle Editionen (x86, x64)

  **Hinweis**
  Wenn Sie Acronis Cyber Protect noch mit Windows 7 verwenden wollen, müssen Sie sicherstellen, dass Sie folgende Updates von Microsoft installiert haben:
  - Windows 7 Extended Security Updates (ESU)
  - KB4474419
  - KB4490628

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

- Windows Server 2008 R2 – die Editionen Standard, Enterprise, Datacenter und Foundation
- 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 2008 R2/2012/2012 R2/2016
- Windows 10 – die Editionen Home, Pro, Education, Enterprise, IoT Enterprise und LTSC (früher LTSB)
- Windows Server 2016 – alle Installationsoptionen, mit Ausnahme des Nano Servers
- Windows Server 2019 – alle Installationsoptionen, mit Ausnahme des Nano Servers
- Windows 11 – alle Editionen
- Windows Server 2022 – alle Installationsoptionen, mit Ausnahme des Nano Servers

### Unter Linux:

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

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

**Linux mit Kernel 2.6.9 bis 5.19 und glibc 2.3.4 (oder höher)**, inklusive folgender x86_64-Distributionen:

x86-Distributionen werden nicht unterstützt.

- Red Hat Enterprise Linux 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*, 8.6*, 8.7*
- Ubuntu 9.10, 10.04, 10.10, 11.04, 11.10, 12.04, 12.10, 13.04, 13.10, 14.04, 14.10, 15.04, 15.10, 16.04, 16.10, 17.04, 17.10, 18.04, 18.10, 19.04, 19.10, 20.04, 20.10, 21.04, 21.10, 22.04
- 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, 11, 12, 15

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

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

- CloudLinux 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*
- ClearOS 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*
- AlmaLinux 8.4*, 8.5*
- Rocky Linux 8.4*
- 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`

Wenn Ihre Linux-Distribution den D-Bus-Mechanismus nicht unterstützt (wie z.B. bei Red Hat Enterprise Linux 6.x oder CentOS 6.x), wird Acronis Cyber Protect den Standard-Speicherort für sichere Schlüssel verwenden, weil das Betriebssystem keinen D-Bus-kompatiblen Speicherort bereitstellt.

* Wird nur mit Kerneln von 4.18 bis 5.19 unterstützt

## Storage Node (nur bei On-Premise-Bereitstellung)

- Windows Server 2008 – die Editionen Standard, Enterprise, Datacenter und Foundation (nur x64)
- Windows Small Business Server 2008
- Windows 7 – alle Editionen (nur x64)
- Windows Server 2008 R2 – die Editionen Standard, Enterprise, Datacenter und Foundation
- Windows Home Server 2011
- Windows MultiPoint Server 2010/2011/2012
- 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
- Windows 10 – die Editionen Home, Pro, Education, Enterprise und IoT Enterprise
- Windows Server 2016 – alle Installationsoptionen, mit Ausnahme des Nano Servers
- Windows Server 2019 – alle Installationsoptionen, mit Ausnahme des Nano Servers
- Windows Server 2022 – alle Installationsoptionen, mit Ausnahme des Nano Servers

## Agent für Windows XP SP2

Der Agent für Windows XP SP2 unterstützt nur die 32-Bit-Versionen von Windows XP SP2.

Wenn Sie Maschinen mit Windows XP SP1 (x64), Windows XP SP2 (x64) oder Windows XP SP3 (x86) sichern wollen, müssen Sie den regulären Agenten für Windows verwenden.

Der Agent für Windows XP SP2 erfordert eine Acronis Cyber Backup 12.5-Lizenz. Acronis Cyber Protect 15-Lizenzschlüssel werden nicht unterstützt.

## Installation

Der Agent für Windows XP SP2 benötigt mindestens 550 MB Speicherplatz und 150 MB Arbeitsspeicher (RAM). Bei der Durchführung von Backups belegt der Agent üblicherweise ca. 350 MB Arbeitsspeicher. Der Speicherbedarf kann – abhängig von der Menge der Daten, die ein Agent verarbeitet – kurzzeitig auf bis zu 2 GB steigen.

Der Agent für Windows XP SP2 kann nur lokal auf derjenigen Maschine installiert werden, die Sie per Backup sichern wollen. Um das Setup-Programm des Agenten herunterzuladen, klicken Sie in der oberen rechten Ecke zuerst auf das Kontosymbol und dann auf **Downloads** –> **Agent für Windows XP SP2**.

Der Cyber Protect Monitor und Bootable Media Builder können nicht installiert werden. Wenn Sie die ISO-Datei des Boot-Mediums herunterladen wollen, müssen klicken Sie in der oberen rechten Ecke zuerst auf das Kontosymbol klicken und dann auf **Downloads** –> **Boot-Medium**.

## Update

Der Agent für Windows XP SP2 bietet keine Unterstützung für die Funktion 'Remote-Update'. Um den Agenten zu aktualisieren, müssen Sie jeweils die neueste Version des Setup-Programms herunterladen und dann die Installation wiederholen.

Wenn Sie Windows XP von SP2 auf SP3 aktualisieren, müssen Sie anschließend den Agent für Windows XP SP2 deinstallieren und dann den regulären Agenten für Windows installieren.

## Einschränkungen

- Es können nur Backups auf Laufwerksebene durchgeführt werden. Aus einem Laufwerk- oder Volume-Backup können jedoch einzelne Dateien wiederhergestellt werden.
- Die Funktion 'Planung nach Ereignissen' wird nicht unterstützt.
- Startbedingungen für die Schutzplan-Ausführung werden nicht unterstützt.
- Es werden nur die folgenden Backup-Zielorte unterstützt:
  - Cloud Storage
  - Lokaler Ordner
  - Netzwerkordner
  - Einer Secure Zone
- Das Backup-Format **Version 12** sowie Funktionen, die das Backup-Format **Version 12** erfordern, werden nicht unterstützt. Insbesondere ist die Option Physischer Datenversand (Physical Data Shipping) nicht verfügbar. Die Option **Performance und Backup-Fenster** (sofern aktiviert) gilt nur für die Einstellungen auf der grünen Ebene.

- Die Auswahl einzelner Laufwerke/Volumes zur Durchführung einer Wiederherstellung sowie die manuelle Laufwerkszuordnung während einer Wiederherstellung werden von der Weboberfläche aus nicht unterstützt. Diese Funktion ist jedoch unter einem Boot-Medium verfügbar.
- Off-Host Data Processing wird nicht unterstützt.
- Der Agent für Windows XP SP2 kann folgende Aktionen mit Backups nicht durchführen:
  - Backups werden in eine virtuelle Maschine konvertiert
  - Volumes aus einem Backup mounten
  - Dateien aus einem Backup extrahieren
  - Export und manuelle Validierung eines Backups.

  Sie können diese Aktionen mithilfe eines anderen Agenten durchführen.
- Backups, die mit dem Agenten für Windows XP SP2 erstellt wurden, können nicht als virtuelle Maschine ausgeführt werden.

## Unterstützte Microsoft SQL Server-Versionen

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

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

## Unterstützte Microsoft Exchange Server-Versionen

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

## Unterstützte Microsoft SharePoint-Versionen

Acronis Cyber Protect 15 unterstützt folgende Microsoft SharePoint-Versionen:

- Microsoft SharePoint 2013
- Microsoft SharePoint Server 2010 SP1

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

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

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

## Unterstützte Oracle Database-Versionen

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

Es werden nur Einzelinstanz-Konfigurationen unterstützt.

## Unterstützte SAP HANA-Versionen

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

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

## Unterstützte Virtualisierungsplattformen

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

**Hinweis**
Folgende Hypervisor-Hersteller und -Versionen, für die die Methode **Backup innerhalb eines Gastbetriebssystems** unterstützt wird, wurden speziell getestet. Aber auch, wenn Sie einen Hypervisor einsetzen, dessen Anbieter oder Version unten nicht explizit aufgeführt ist, kann die Methode **Backup innerhalb eines Gastbetriebssystems** dennoch in allen erforderlichen Szenarien korrekt funktionieren.

Wenn bei Ihrer Kombination aus Hypervisor-Anbieter bzw. -Version bei der Verwendung von Acronis Cyber Protect Probleme auftreten, können Sie sich für weitere Untersuchungen an den Support wenden.

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

| | | |
|---|---|---|
| **VMware** | | |
| **VMware vSphere-Versionen:** 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7.0, 8.0<br>**VMware vSphere-Editionen:**<br>VMware vSphere Essentials*<br>VMware vSphere Essentials Plus*<br>VMware vSphere Standard*<br>VMware vSphere Advanced<br>VMware vSphere Enterprise<br>VMware vSphere Enterprise Plus | + | + |
| VMware vSphere Hypervisor (Free ESXi)** | | + |
| VMware Server (VMware Virtual Server)<br>VMware Workstation<br>VMware ACE<br>VMware Player | | + |
| **Microsoft*** ** | | |
| Windows Server 2008 (x64) mit Hyper-V<br>Windows Server 2008 R2 mit Hyper-V<br>Microsoft Hyper-V Server 2008/2008 R2<br>Windows Server 2012/2012 R2 mit Hyper-V<br>Microsoft Hyper-V Server 2012/2012 R2<br>Windows 8, 8.1 (x64) mit Hyper-V<br>Windows 10 mit Hyper-V<br>Windows Server 2016 mit Hyper-V – alle Installationsoptionen, mit Ausname des Nano Servers<br>Microsoft Hyper-V Server 2016<br>Windows Server 2019 mit Hyper-V – alle Installationsoptionen, mit Ausname des Nano Servers<br>Microsoft Hyper-V Server 2019<br>Windows Server 2022 mit Hyper-V – alle Installationsoptionen, mit Ausname des Nano Servers | + | + |
| Microsoft Virtual PC 2004 und 2007<br>Windows Virtual PC | | + |

| | | |
|---|---|---|
| Microsoft Virtual Server 2005 | | + |
| **Scale Computing** | | |
| Scale Computing Hypercore 8.8, 8.9, 9.0 | + | + |
| **Citrix** | | |
| 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, 7.6 | | 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<br>Red Hat Virtualization (RHV) 4.0, 4.1 | | + |
| Red Hat Virtualization (verwaltet von oVirt) 4.2, 4.3, 4.4<br>(nur bei der Cloud-Bereitstellung verfügbar) | + | + |
| Kernel-based Virtual Machines (KVM) | | + |
| Kernel-based Virtual Machines (KVM), verwaltet von oVirt 4.3 unter Red Hat Enterprise Linux 7.6, 7.7 oder CentOS 7.6, 7.7<br>(nur bei der Cloud-Bereitstellung und mit einer Advanced-Lizenz verfügbar) | + | + |
| Kernel-based Virtual Machines (KVM), verwaltet von oVirt 4.4 unter Red Hat Enterprise Linux 8 oder CentOS Stream 8.x<br>(nur bei der Cloud-Bereitstellungen und mit einer Advanced-Lizenz verfügbar) | + | + |
| Kernel-based Virtual Machines (KVM), verwaltet von oVirt 4.5 unter Red Hat Enterprise Linux 8 oder CentOS Stream 8.x<br>(nur bei der Cloud-Bereitstellungen und mit einer Advanced-Lizenz verfügbar) | + | + |
| **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** (nur bei der Cloud-Bereitstellung verfügbar) | | |
| 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 Hybrid Server 7.5 | + | Nur virtuelle Maschinen. Container werde nicht unterstützt. |
| **Virtuozzo Hybrid Infrastructure** (nur bei der Cloud-Bereitstellung verfügbar) | | |
| Virtuozzo Hybrid Infrastructure 3.5, 4.0, 4.5 | + | + |
| **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.

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

## Einschränkungen

- **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- und V2P-Migration. Den Agenten für Linux oder Boot-Medien verwenden, um Backups und Boot-Medien für Wiederherstellungen zu erstellen.
  - Eine virtuelle Maschine direkt aus einem Backup ausführen, welches mit dem Agenten für Linux oder einem Boot-Medium erstellt wurde.
  - Ein Backup, welches mit dem Agenten für Linux oder einem Boot-Medium erstellt wurde, in eine virtuelle Maschine konvertieren.
- **Verschlüsselte virtuelle Maschinen** (mit VMware vSphere 6.5 eingeführt)
  - Verschlüsselte virtuelle Laufwerke werden im Backup in einem unverschlüsselten Zustand gespeichert. Falls die Verschlüsselung der entsprechenden Daten für Sie wichtig ist, können Sie bei der Erstellung eines Schutzplans festlegen, dass die Backups selbst verschlüsselt werden.
  - Wiederhergestellte virtuelle Maschinen sind immer unverschlüsselt. Sie können die Verschlüsselung nach Abschluss der Wiederherstellung aber wieder manuell aktivieren.
  - Wenn Sie verschlüsselte virtuelle Maschinen per Backup sichern, empfehlen wir Ihnen, außerdem auch die virtuelle Maschine zu verschlüsseln, auf welcher der Agent für VMware ausgeführt wird. Ansonsten sind die ausgeführten Aktionen mit den verschlüsselten Maschinen möglicherweise langsamer als erwartet. Verwenden Sie den vSphere Webclient, um der Maschine des Agenten die **VM-Verschlüsselungsrichtlinie** zuzuweisen.
  - Verschlüsselte virtuelle Maschinen werden via LAN gesichert – und zwar auch dann, wenn Sie den SAN-Transportmodus für den Agenten konfiguriert haben. Der Agent wird stattdessen auf den NBD-Transportmodus zurückgreifen, weil VMware den SAN-Transportmodus beim Backup verschlüsselter virtueller Laufwerke nicht unterstützt.
- **Secure Boot** (mit VMware vSphere 6.5 eingeführt)
  Wenn eine virtuelle Maschine als neue virtuelle Maschine wiederhergestellt wurde, ist **Secure Boot** anschließend deaktiviert. Sie können die Option nach Abschluss der Wiederherstellung aber wieder manuell aktivieren.
- **ESXi-Konfigurations-Backups** werden nicht für VMware vSphere 7.0 unterstützt.

## Linux-Pakete

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

- Das Paket mit den Kernel-Headers oder Kernel-Quellen. Die Paketversion muss zur Kernel-Version passen.
- Das GNU Compiler Collection (GCC) Compiler System. Die GCC-Version muss dieselbe sein, mit der der Kernel kompiliert wurde.
- Das Tool 'Make'.
- Der Perl-Interpreter.

- Die Bibliotheken `libelf-dev`, `libelf-devel` oder `elfutils-libelf-devel`, um Kernels ab v4.15 zu erstellen, die mit dem Parameter CONFIG_UNWINDER_ORC=y konfiguriert wurden. Für einige Distributionen, wie z.B. Fedora 28, müssen diese separat von Kernel-Headern installiert werden.

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

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

## Sind die erforderlichen Pakete bereits installiert?

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

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

   ```
   cat /proc/version
   ```

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

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

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

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

   - Führen Sie unter Ubuntu folgende Befehle aus:

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

   Stellen Sie in jedem Fall sicher, dass die Paketversionen die gleichen sind wie in der `Linux-Version` von Schritt 1.
4. Mit folgendem Befehl können Sie überprüfen, ob der Perl-Interpreter installiert ist:

   ```
   perl --version
   ```

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

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

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

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

## Installation der Pakete aus dem Repository

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

| Linux-Distribution | Paketnamen | Art der Installation |
|---|---|---|
| Red Hat Enterprise Linux | **kernel-devel**<br>**gcc**<br>**make**<br>**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:<br>`yum install perl` |
| CentOS<br>Fedora | **kernel-devel**<br>**gcc**<br>**make**<br>**elfutils-libelf-devel** | Das Setup-Programm wird die Pakete automatisch herunterladen und installieren. |
| | **perl** | Führen Sie folgenden Befehl aus:<br>`yum install perl` |
| Ubuntu<br>Debian | **linux-headers**<br>**linux-image**<br>**gcc**<br>**make**<br>**perl** | Führen Sie folgende Befehle aus:<br>`sudo apt-get update`<br>`sudo apt-get install linux-headers-$(uname -r)`<br>`sudo apt-get install linux-image-$(uname -r)`<br>`sudo apt-get install gcc-<package version>`<br>`sudo apt-get install make`<br>`sudo apt-get install perl` |
| SUSE Linux<br>OpenSUSE | **kernel-source**<br>**gcc**<br>**make**<br>**perl** | sudo zypper install kernel-source<br>sudo zypper install gcc<br>sudo zypper install make<br>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.

## 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 Einer Secure Zone zugreifen zu können.

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

- Microsoft BitLocker Drive Encryption
- CheckPoint Harmony Endpoint
- McAfee Endpoint Encryption
- PGP Whole Disk Encryption

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

### Allgemeine Installationsregel

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

### Verwendung der Einer Secure Zone

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

1. Installieren Sie die Verschlüsselungssoftware.
2. Installieren Sie den Protection Agenten.
3. Einer Secure Zone erstellen.

4. Wenn Sie das Laufwerk oder dessen Volumes verschlüsseln, müssen Sie die Einer Secure Zone von der Verschlüsselung ausschließen.

## Allgemeine Backup-Regel

Sie können ein Laufwerk-Backup im Betriebssystem durchführen. Versuchen Sie nicht, das Backup mithilfe eines Boot-Mediums durchzuführen.

## Software-spezifische Recovery-Prozeduren

### Microsoft BitLocker-Laufwerksverschlüsselung and CheckPoint Harmony Endpoint

Sie können ein System wiederherstellen, indem Sie eine Wiederherstellung mit einen Neustart oder mit einem Boot-Medium durchführen.

***Wiederherstellung mit Neustart***

Wenn Sie ein verschlüsseltes System wiederherstellen wollen, befolgen Sie die im Abschnitt '"Eine physische Maschine wiederherstellen" (S. 330)' erläuterten Schritte.

Stellen Sie sicher, dass die Anforderungen im Abschnitt '"Recovery mit Neustart" (S. 338)' erfüllt sind.

**Hinweis**
Bei Bitlocker-verschlüsselten Volumes ist eine Wiederherstellung mit Neustart nur auf UEFI-basierten Maschinen möglich, die unter Windows 7 und höher oder Windows Server 2008 R2 und höher laufen. Bei CheckPoint-verschlüsselten Volumes ist eine Wiederherstellung mit Neustart nur auf UEFI-basierten Maschinen möglich, die unter Windows 10 und Windows 11 laufen.

Eine Wiederherstellung mit Neustart ist nicht verfügbar, wenn es sich um BIOS-basierte Maschinen oder um Maschinen mit Linux bzw. macOS handelt.

***Wiederherstellung mit einem Boot-Medium***

1. Booten Sie mit einem Boot-Medium.
2. Stellen Sie das System wieder her.

   **Wichtig**
   Die Backup-Daten werden unverschlüsselt wiederhergestellt.

3. Booten Sie das wiederhergestellte System neu.
4. Schalten Sie die Verschlüsselungssoftware ein.

Wenn Sie lediglich ein Volume (eine Partition) eines mehrfach partitionierten Laufwerks wiederherstellen müssen, dann sollten Sie die Wiederherstellung unter dem Betriebssystem durchführen. 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

Ein verschlüsseltes System-Volume kann nur mithilfe eines Boot-Mediums wiederhergestellt werden.

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

## Kompatibilität mit Dell EMC Data Domain Storages

Mit Acronis Cyber Protect können Sie auch Dell EMC Data Domain-Geräte als Backup Storage verwenden. Die Aufbewahrungssperre (der Governance-Modus) wird unterstützt.

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

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

***So können Sie die Variable unter Windows hinzufügen***

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

***So können Sie die Variable unter Linux hinzufügen***

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

```
export AR_RETENTION_LOCK_SUPPORT=1
```

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

***So können Sie die Variable in einer virtuellen Appliance hinzufügen***

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

```
export AR_RETENTION_LOCK_SUPPORT=1
```

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

# Systemanforderungen

Die folgende Tabelle gibt einen Überblick, wie viel Speicherplatz (Festplatte) und Arbeitsspeicher (RAM) für typische Installationen erforderlich sind. Die Installation wird mit den Standardeinstellungen durchgeführt.

| Zu installierende Komponenten | Für die Installation erforderlicher Speicherplatz | Belegter Arbeitsspeicher (Minimum) |
|---|---|---|
| Agent für Windows | 850 MB | 150 MB |
| Agent für Windows und einer der folgenden Agenten:<br>• Agent für SQL<br>• Agent für Exchange | 950 MB | 170 MB |
| Agent für Windows und einer der folgenden Agenten:<br>• Agent für VMware (Windows)<br>• Agent für Hyper-V | 1,170 MB | 180 MB |
| Agent für Office 365 | 500 MB | 170 MB |
| Agent für Linux | 2.0 GB | 130 MB |
| Agent für Mac | 500 MB | 150 MB |
| Nur bei On-Premise-Bereitstellungen | | |

| | | |
|---|---|---|
| Management Server unter Windows | 1.7 GB | 200 MB |
| Management Server unter Linux | 1.5 GB | 200 MB |
| Management Server und Agent für Windows | 2.4 GB | 360 MB |
| Management Server und Agenten auf einer Maschine mit Windows, Microsoft SQL Server, Microsoft Exchange Server und Active Directory-Domänendienste | 3.35 GB | 400 MB |
| Management Server und Agent für Linux | 4.0 GB | 340 MB |
| Storage Node und Agent für Windows<br>• Nur 64-Bit-Plattform<br>• Zur Nutzung von Deduplizierung sind mindestens 8 GB RAM erforderlich. Weitere Informationen finden Sie im Abschnitt '"Optimale Vorgehensweisen bei der Deduplizierung" (S. 665)'. | 1.1 GB | 330 MB |

Bei der Durchführung von Backups belegt ein Agent üblicherweise ca. 350 MB Arbeitsspeicher (bei einem Backup mit 500 GB Datenvolumen ermittelt). Der Speicherbedarf kann – abhängig von der Art und Menge der Daten, die ein Agent verarbeitet – kurzzeitig auf bis zu 2 GB steigen.

Die Sicherung zu großen Backup-Sätzen (600 GB oder größer) erfordert etwa 1 GB RAM pro 1 TB des Backup-Satzes.

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

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

Ein Management Server mit einem registrierten Workload belegt 200 MB Arbeitsspeicher. Unter einem Workload wird hier jede Art von geschützter Ressource verstanden - beispielsweise eine physische Maschine, eine virtuelle Maschine, ein Postfach oder eine Datenbank-Instanz. Für jeden zusätzlichen Workload werden etwa 2 MB benötigt. Ein Server mit 100 registrierten Workloads benötigt daher (in Ergänzung zum Speicherbedarf für das Betriebssystem und laufende Applikationen) ca. 400 MB Arbeitsspeicher.

Die maximale Anzahl an registrierbaren Workloads beträgt 900-1000. Dies Begrenzung beruht auf der im Management Server eingebetteten SQLite-Datenbank.

Wenn Sie diese Beschränkung umgehen wollen, müssen Sie während der Installation des Management Servers eine externe Microsoft SQL Server-Instanz spezifizieren. Mit einer externen SQL-Datenbank können Sie bis zu 8000 Workloads auf dem Management Server registrieren, ohne dass die Performance signifikant beeinträchtigt wird. Mit 8000 registrierten Workloads beansprucht die SQL Server-Instanz etwa 8 GB RAM.

Wenn Sie eine bessere Backup-Performance erreichen wollen, können Sie die Workloads in Gruppen verwalten. Dabei kann jede Gruppe bis zu 500 Workloads enthalten.

# 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. Angegebene Beschränkungen gelten sowohl für die Agenten als auch Boot-Medien.

| **Dateisystem** | **Unterstützt durch** | | | | **Einschränkungen** |
|---|---|---|---|---|---|
| | **Agenten** | **WinPE-basiertes Boot-Medium** | **Linux-basiertes Boot-Medium** | **Mac-basiertes Boot-Medium** | |
| **FAT16/32** | Alle Agenten | + | + | + | Keine Beschränkungen |
| **NTFS** | | + | + | + | |
| **ext2/ext3/ext4** | | + | + | - | |
| **HFS+** | Agent für Mac | - | - | + | |
| **APFS** | | - | - | + | • Wird ab macOS High Sierra 10.13 unterstützt<br>• Bei Wiederherstellungen zu einer anderen als der ursprünglichen (wie einer fabrikneuen) Maschine muss die ursprüngliche Laufwerkskonfiguration manuell neu erstellt werden. |

| | | | | | |
|---|---|---|---|---|---|
| **JFS** | Agent für Linux | - | + | - | • Kein Ausschluss von Dateien von einem Laufwerk-Backup<br>• Schnelle inkrementelle/differentielle Backups werden nicht unterstützt. |
| **ReiserFS3** | | - | + | - | |
| **ReiserFS4** | | - | + | - | • Kein Ausschluss von Dateien von einem Laufwerk-Backup<br>• Schnelle inkrementelle/differentielle Backups werden nicht unterstützt.<br>• Keine Größenänderung von Volumes während einer Wiederherstellung |
| **ReFS** | Alle Agenten | + | + | + | |
| **XFS** | | + | + | + | • Kein Ausschluss von Dateien von einem Laufwerk-Backup<br>• Schnelle inkrementelle/differentielle Backups werden nicht unterstützt.<br>• Keine Größenänderung von Volumes während einer Wiederherstellung<br>• Das Wiederherstellen von Dateien aus einem Backup, das auf einem Band gespeichert wurde, wird nicht unterstützt |

| | | | | | |
|---|---|---|---|---|---|
| **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<br>• Es können keine Dateien aus einem Backup ausgeschlossen werden<br>• 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. Ein Sektor-für-Sektor-Backup ist für jedes Dateisystem möglich, welches:

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

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

## Datendeduplizierung

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

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

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

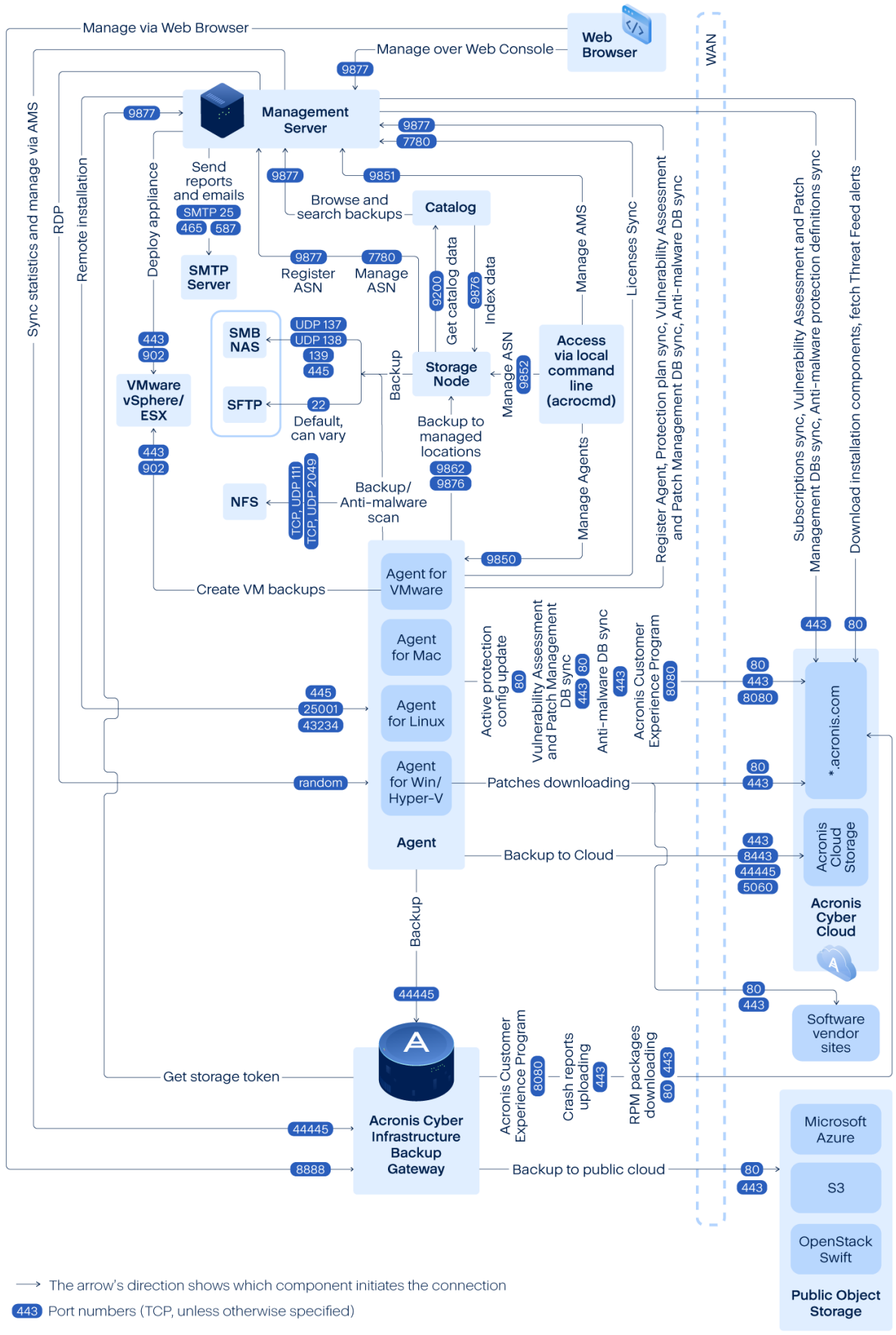
# Netzwerkverbindungsdiagramm für Acronis Cyber Protect

Dieses Thema enthält die Verbindungsdiagramme für Acronis Cyber Protect.

In unserer Knowledge Base finden Sie eine Liste der Ports, Dienste und Prozesse, die von Acronis Cyber Protect verwendet werden:

- Für Windows siehe Windows-Dienste und -Prozesse (65663).
- Für Linux siehe Linux-Komponenten, -Dienste und -Prozesse (67276).

# Netzwerkverbindungsdiagramm – Cyber Protect-Prozesse



**Wichtig**
Die ausgehenden Ports im Netzwerkdiagramm sind dynamisch. Einige Dienste können auch dynamische Ports für eingehende Verbindungen verwenden. Wenn Sie Netzwerkprobleme beheben, sollten Sie sicherstellen, dass der Datenverkehr über dynamische Ports erlaubt ist.

Die dynamischen Ports werden vom Betriebssystem verwaltet und zufällig zugewiesen. Der standardmäßige dynamische Port-Bereich in Windows liegt bei 49152–65535. Dieser Bereich kann je nach Betriebssystem variieren und manuell geändert werden.

Der **Management Server** ist die zentrale Komponente von Acronis Cyber Protect. Er exponiert zwei TCP-Ports: 7780 und 9877. Der per TLS geschützte Port 9877 wird verwendet, um sowohl die REST-API als auch eine webbasierte Benutzeroberfläche bereitzustellen. Die REST-API-Endpunkte authentifizieren Anfragen mithilfe von JWT-Tokens, die entweder als separater HTTP-Header repräsentiert oder als HTTP-Cookie codiert werden. Der Port 7780 implementiert das ZeroMQ-Protokoll mit einer ZMTP-CURVE-Authentifizierung und -Verschlüsselung. Der Port 7780 wird von den Agenten und dem Storage Node verwendet, um Verwaltungsnachrichten asynchron mit dem Management Server auszutauschen. Der Management Server kommuniziert zudem mit den Cloud Services, um Updates über standardmäßige HTTP- und HTTPS-Ports herunterzuladen.

Der **Storage Node** ist die Storage-Komponente von Acronis Cyber Protect. Es exponiert den TCP-Port 9876. Dieser Port wird zum Senden und Empfangen von Backup-Daten verwendet. Der Transport wird per TLS geschützt und die Authentifizierung erfolgt über MTLS (Mutual TLS). Das auf Applikationsebene arbeitende Protokoll ist eine propriäter Eigenentwicklung von Acronis. Der Storage Node kommuniziert mit den Backend-Storage-Systemen über die entsprechenden Protokolle und Authentifizierungsmechanismen.

Der **Katalog** ist eine Hilfskomponente von Acronis Cyber Protect. Sie indiziert die Daten auf dem Storage Node. Dafür greift sie über den Port 9876 auf diesen zu und exponiert den fertigen Index über den Port 9200.

Das **Backup Gateway** implementiert die nächste Generation des proprietären Datenzugriffsprotokolls von Acronis. Die gleiche Komponente wird in Acronis Cyber Cloud verwendet, wenn sich Kunden für die Option 'Cloud Backup' entscheiden. Das Gateway verwendet den TCP-Port 44445, der außerdem bei der IANA registriert ist. Die Datensicherung erfolgt über TLS und die Authentifizierung erfolgt über MTLS (Mutual TLS). Das Backup Gateway kann auch den Port 8888 für den HTTPS-basierten Management Service verwenden.

Der **Agent** kommuniziert mit dem Management Server, dem Storage Node und dem Backup Gateway über die oben beschriebenen Ports. Der Agent kann auch mit standardmäßigen Dateidiensten (SMB, NFS) kommunizieren, wenn diese als Backup-Ziel verwendet werden. In diesem Fall werden die Standard-Ports und die passenden Authentifizierungsprotokolle verwendet. Der Agent für VMware verwendet die VMware vSphere API über die Ports, die von VMware vSphere definiert werden, wenn diese Funktionalität konfiguriert ist.

Die Schwachstellenbewertung für Linux wird über einen CVSS-Dienst implementiert, der in Acronis Cyber Cloud bereitgestellt wird. Die Protection Agenten wählen dynamisch das nächstgelegene Datacenter per Ping aus einer Liste (https://cloud.acronis.com/services.json) aus.

# On-Premise-Bereitstellung

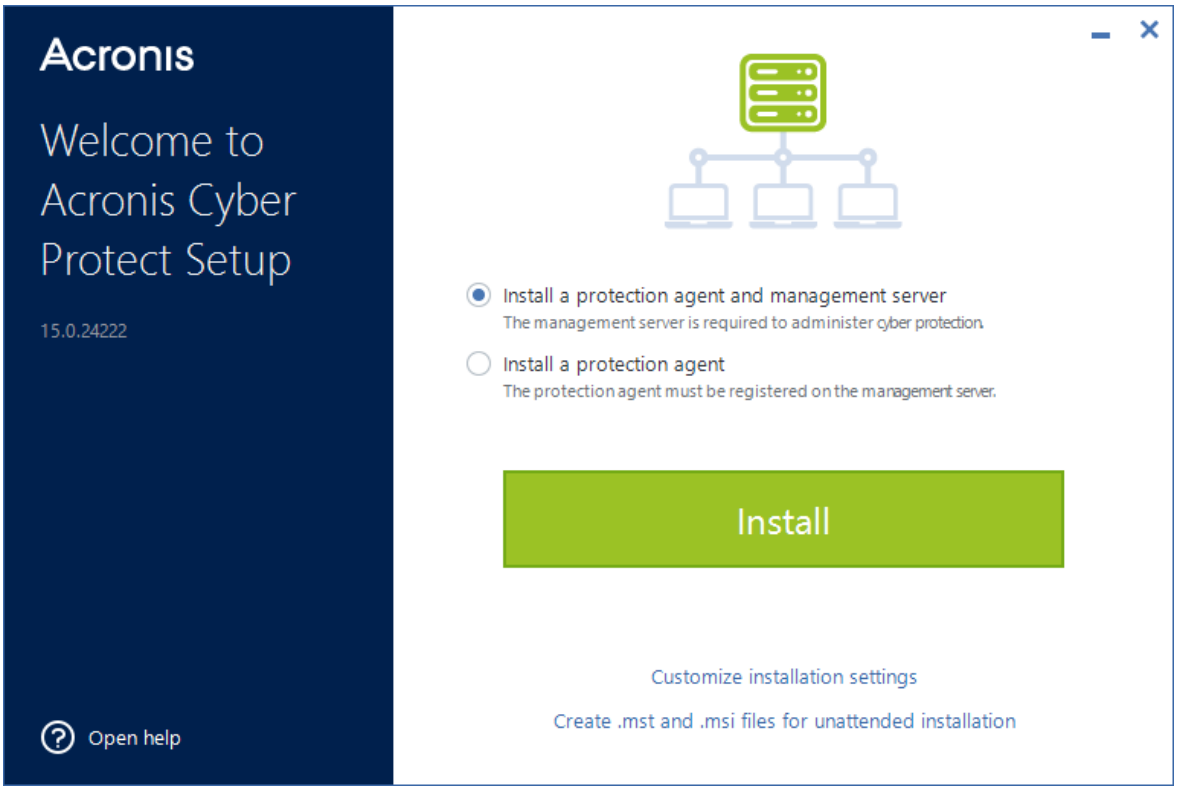
Eine On-Premise-Bereitstellung beinhaltet eine bestimmte Anzahl von Software-Komponenten, die im Abschnitt '"Komponenten" (S. 49)' beschrieben sind. Weitere Informationen über das Zusammenspiel zwischen diesen Komponenten und den erforderlichen Ports finden Sie im Abschnitt '"Netzwerkverbindungsdiagramm für Acronis Cyber Protect" (S. 83)'.

## Den Management Server installieren

### Installation unter Windows

***Installation des Management Servers***

1. Melden Sie sich als Administrator an und starten Sie das Acronis Cyber Protect Setup-Programm.
2. [Optional] Wenn Sie die Sprache des Setup-Programms ändern wollen, klicken Sie auf **Sprache einrichten**.
3. Akzeptieren Sie die Bedingungen der Lizenzvereinbarung sowie die Datenschutzerklärung und klicken Sie anschließend auf **Fertigstellen**.
4. Übernehmen Sie die Standardeinstellung '**Einen Protection Agenten und den Management Server installieren**'.



5. Gehen Sie nach einer der folgenden Möglichkeiten vor:
   - Klicken Sie auf **Installieren**.

     Dies ist die einfachste Möglichkeit, das Produkt zu installieren. Die meisten Installationsparameter sind dabei auf Standardwerte eingestellt.

     Folgende Komponenten werden installiert:
     - Management Server
     - Komponenten zur Remote-Installation
     - Agent für Windows
     - Andere Agenten (der Agent für Hyper-V, der Agent für Exchange, Agent für SQL und der Agent für Active Directory), falls ein entsprechender Hypervisor oder eine entsprechende Applikation auf der Maschine erkannt wird.
     - Bootable Media Builder
     - Befehlszeilenwerkzeug
     - Cyber Protect Monitor
   - Klicken Sie auf **Installationseinstellungen anpassen**, um die Einrichtung zu konfigurieren. Sie können auswählen, welche Komponenten installiert werden sollen, und einige zusätzliche Parameter spezifizieren. Weitere Informationen finden Sie hier: "Installationseinstellungen anpassen" (S. 88).
   - Klicken Sie auf **.mst- und .msi-Dateien für eine unbeaufsichtigte Installation erstellen**, um die Installationspakete zu extrahieren. Überprüfen oder ändern Sie die Installationseinstellungen, die der .mst-Datei hinzugefügt werden, und klicken Sie dann auf **Generieren**. Weitere Schritte dieser Prozedur sind nicht erforderlich.

     Wie Sie Agenten über Gruppenrichtlinien bereitstellen können, ist im Abschnitt '"Agenten per Gruppenrichtlinie bereitstellen" (S. 186)' erläutert.
6. Fahren Sie mit der Installation fort.
7. Klicken Sie nach Abschluss der Installation auf **Schließen**.

Um Ihren Management Server in Betrieb nehmen zu können, müssen Sie ihn durch Anmeldung an Ihrem Acronis Konto oder mithilfe einer Aktivierungsdatei aktivieren.

## Installationseinstellungen anpassen

In diesem Abschnitt werden Einstellungen erläutert, die während der Installation geändert werden können.

### Zu installierende Komponenten

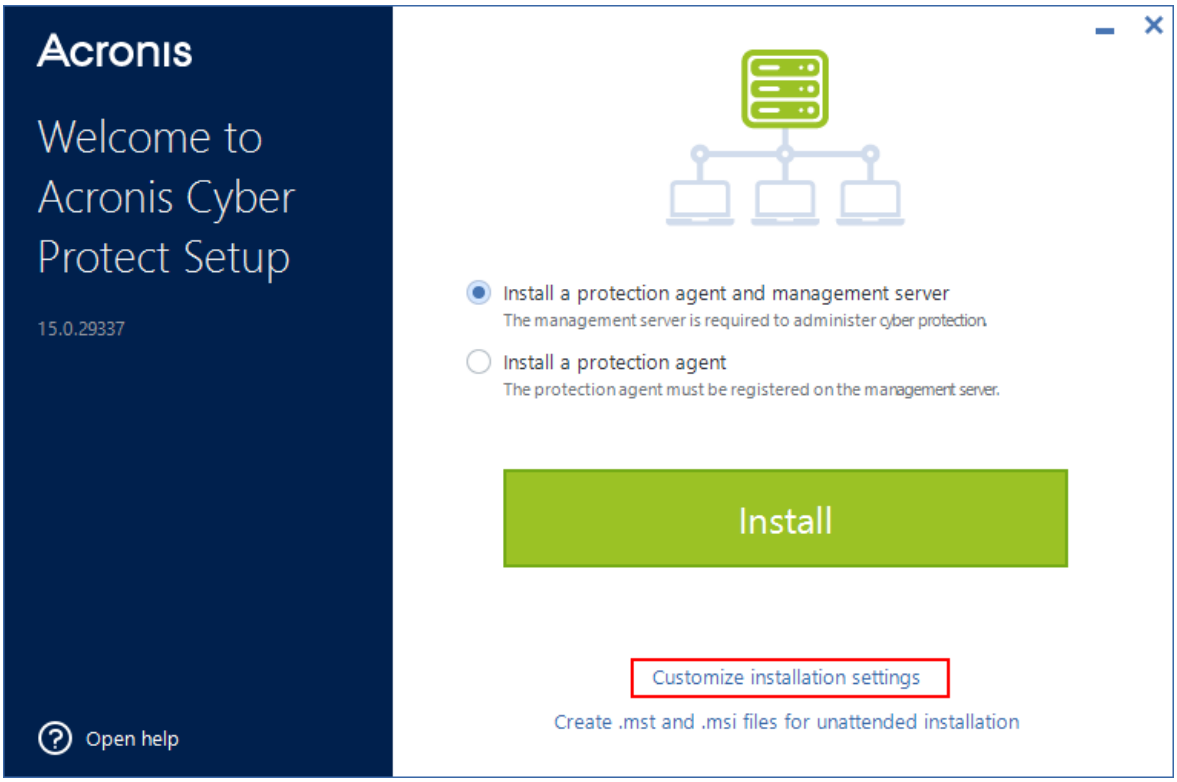
Je nachdem, ob Sie einen Management Server und einen Protection Agenten oder nur einen Protection Agenten installieren, sind die folgenden Komponenten standardmäßig ausgewählt:

| Management Server und Protection Agent | Nur Protection Agent |
|---|---|
| Management Server | Agent für Windows |
| Komponenten zur Remote-Installation | Bootable Media Builder |
| Agent für Windows | Befehlszeilenwerkzeug |
| Bootable Media Builder | Cyber Protect Monitor |
| Befehlszeilenwerkzeug | |
| Cyber Protect Monitor | |

Eine vollständige Liste der verfügbaren Komponenten finden Sie unter '"Komponenten" (S. 49)'.

***So können Sie optionale Komponenten installieren***

1. Klicken Sie im Installationsassistenten auf **Installationseinstellungen anpassen**.




2. Klicken Sie bei **Zu installierende Komponenten** auf **Ändern**.
3. Wählen Sie zuerst die gewünschten Komponenten aus und klicken Sie dann auf **Fertig**.
4. Konfigurieren Sie bei entsprechender Aufforderung die Einstellungen für die ausgewählten Komponenten.
5. Klicken Sie auf **Installieren**.

### Dienstanmeldekonto

Sie können das Konto, unter dem der Agent oder der Management-Dienst ausgeführt wird, mit den Optionen **Anmeldekonto für den Agenten-Dienst** bzw. **Anmeldekonto für den Management Server-Dienst** ändern.

Sie können eine der folgenden Optionen wählen:

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

  **Dienstbenutzer-Konten** (Service User-Konten) sind Windows-System-Konten, die verwendet werden, um Dienste auszuführen. Der Vorteil dieser Option 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** (Standard für den Dienst des Management Servers und des Storage Nodes).

  Die Kontonamen sind: **Acronis Agent User**, **AMS User** und **ASN User** jeweils für den Agenten, den Management Server bzw. den Storage Node.
- **Folgendes Konto verwenden**

  Wenn Sie das Produkt auf einem Domain Controller installieren, wird Sie das Setup-Programm auffordern, für jeden der Dienste vorhandene Konten (oder dasselbe Konto) zu spezifizieren. Das Setup-Programm erstellt aus Sicherheitsgründen nicht automatisch neue Konten auf einem Domain Controller.

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

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

  Bei der Auswahl der Option **Folgendes Konto verwenden** können Sie auch die Windows-Authentifizierung für den Microsoft SQL Server verwenden, wenn Sie den Management Server mit einer SQL-Datenbank konfigurieren.

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 die Benutzerrechte, die diesem während der Installation zugewiesen wurden, wieder entzogen werden, wird die entsprechende Komponente möglicherweise nicht richtig oder gar nicht mehr funktionieren.

# Erforderliche Benutzerrechte für das Dienst-Anmeldekonto

Ein Protection Agent wird auf einer Windows-Maschine als **Managed Machine Service** (MMS) ausgeführt. Das Konto, unter dem der Agent ausgeführt wird, muss über folgende Rechte verfügen,

damit der Agent korrekt funktioniert:

1. Der MMS-Benutzer muss Mitglied in den Gruppen **Sicherungs-Operatoren** und **Administratoren** sein. Auf einem Domain Controller muss der Benutzer Mitglied in der Gruppe der **Domänen-Admins** sein.
2. Der MMS-Benutzer muss die Berechtigung **Vollzugriff** auf den Ordner `%PROGRAMDATA%\Acronis` (bei Windows XP und Server 2003: `%ALLUSERSPROFILE%\Application Data\Acronis`) sowie auf dessen Unterordner erhalten.
3. Dem MMS-Benutzer muss die Berechtigung **Vollzugriff** für bestimmte Registry-Schlüssel in folgendem Schlüssel gewährt sein: `HKEY_LOCAL_MACHINE\SOFTWARE\Acronis`.
4. Dem MMS-Benutzer müssen unter Windows die folgenden Benutzerrechte zugewiesen werden:
   - **Als Dienst anmelden**
   - **Anpassen von Speicherkontingenten für einen Prozess**
   - **Ersetzen eines Tokens auf Prozessebene**
   - **Verändern der Firmwareumgebungsvariablen**

Der **ASN User** muss auf der Maschine, auf welcher der Acronis Storage Node installiert ist, über administrative Berechtigungen verfügen.

***So können Sie Benutzerrechte unter Windows zuweisen***

**Hinweis**
Diese Prozedur verwendet beispielsweise das Benutzerrecht **Anmelden als Dienst**. Die Schritte für die anderen Benutzerrechte sind die gleichen.

1. Melden Sie sich am Computer als Administrator an.
2. Öffnen Sie in der **Systemsteuerung** die **Verwaltung**. Alternativ können Sie auch Win+R auf der Tastatur drücken, dann **control admintools** eingeben und anschließend die Eingabetaste drücken.
3. Öffnen Sie die **Lokale Sicherheitsrichtlinien**.
4. Erweitern Sie den Unterpunkt **Lokale Richtlinien** und klicken Sie dann auf **Zuweisen von Benutzerrechten**.
5. Klicken Sie im rechten Fensterbereich mit der rechten Maustaste auf **Anmelden als Dienst** und wählen Sie den Befehl **Eigenschaften**.
6. Klicken Sie auf **Benutzer oder Gruppe hinzufügen...**, um einen neuen Benutzer hinzufügen zu können.
7. Suchen Sie im Fenster **Benutzer oder Gruppe hinzufügen...** den Benutzer, den Sie hinzufügen wollen, und klicken Sie anschließend auf **OK**.
8. Klicken Sie im Fenster **Eigenschaften von Anmelden als Dienst** auf **OK**, damit die Änderungen gespeichert werden.

**Hinweis**
Der Benutzer, den Sie zur Benutzerrichtlinie **Anmelden als Dienst** hinzugefügt haben, darf nicht in der Richtlinie **Anmelden als Dienst verweigern** (unter **Lokale Sicherheitsrichtlinien**) enthalten sein.

**Wichtig**
Wir raten davon ab, das Anmeldekonto nach Abschluss der Installation manuell zu ändern.

### Datenbank für den Management Server

Sie können den Management Server mit folgenden Datenbanken konfigurieren:

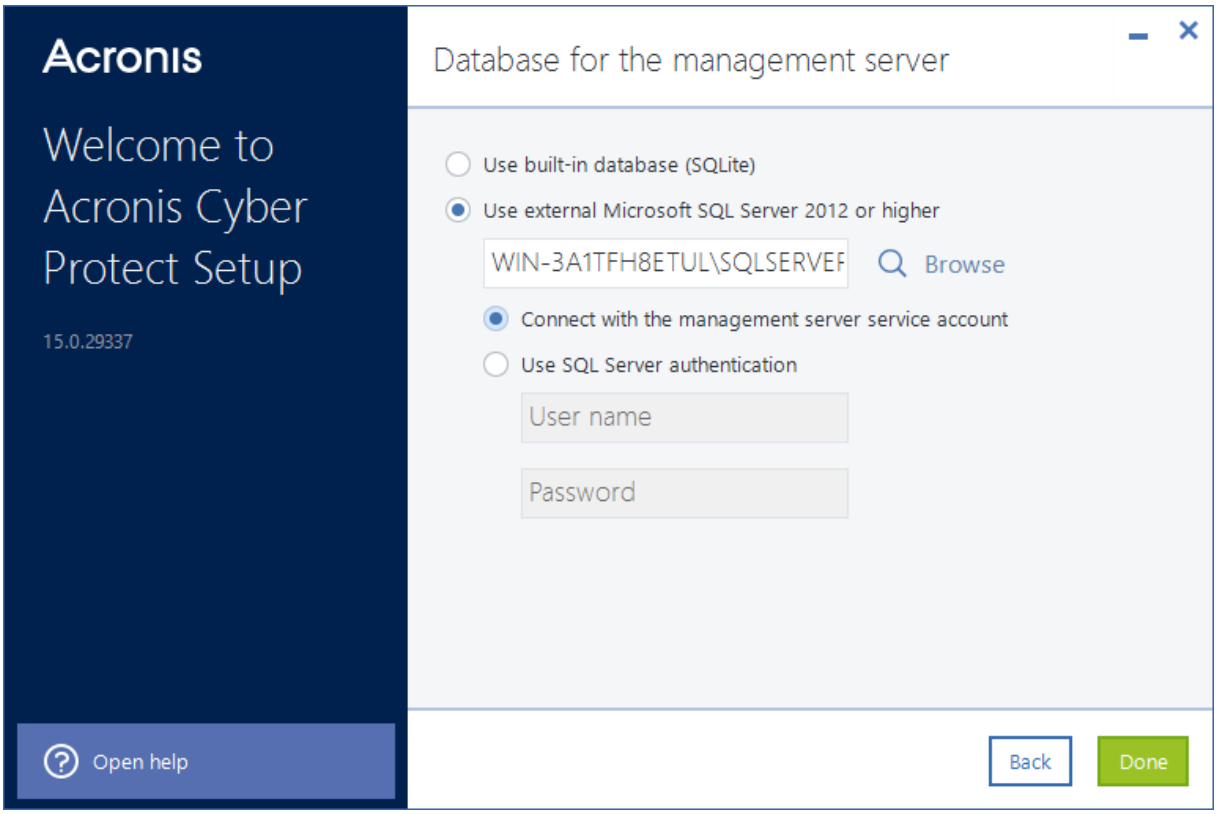
- SQLite

  Der Management Server verwendet standardmäßig die integrierte SQLite-Datenbank. Sie ermöglicht es, ca. 900-1000 Workloads auf dem Management Server zu registrieren. SQLite ist jedoch nicht mit dem Scan Service kompatibel.
- Microsoft SQL

  Mit Microsoft SQL können bis zu 8000 Workloads auf dem Management Server registriert werden, ohne dass die Performance signifikant beeinträchtigt wird. Dieselbe Microsoft SQL-Instanz kann vom Management Server, vom Scan Service und von anderen Programmen verwendet werden.

  Folgende MS SQL Server-Versionen werden unterstützt:
  - Microsoft SQL Server 2019 (unter Windows laufend)
  - Microsoft SQL Server 2017 (unter Windows laufend)
  - Microsoft SQL Server 2016
  - Microsoft SQL Server 2014
  - Microsoft SQL Server 2012

Wenn die Microsoft SQL-Instanz die Standardinstanz **MSSQLSERVER** ist, müssen Sie nur den Namen derjenigen Maschine spezifizieren, auf der die Instanz ausgeführt wird. Wenn die Instanz einen benutzerdefinierten Namen hat, müssen Sie diesen im folgenden Format spezifizieren: `Maschinenname\Instanzname`.




**Hinweis**
Überprüfen Sie, dass der SQL-Server-Browserdienst und das TCP/IP-Client-Protokoll auf der Maschine aktiviert sind, auf der die Microsoft SQL-Instanz läuft. Weitere Informationen über den Start des SQL-Server-Browserdienstes finden Sie unter http://msdn.microsoft.com/de-de/library/ms189093.aspx. Das TCP/IP-Protokoll kann mit einer ähnlichen Prozedur aktiviert werden.

Sie können folgende Authentifizierungsmethoden verwenden, um eine Verbindung mit der spezifizierten Microsoft SQL-Instanz herzustellen:

- Windows-Authentifizierung (**Mit dem Konto des Management Server Service verbinden**)
  Sie können diese Methode verwenden, wenn Sie das Anmeldekonto für den Management Server Service mit der Option **Folgendes Konto verwenden** konfiguriert haben – beispielsweise durch Spezifizieren von '`<MASCHINENNAME>\Administrator`. Das spezifizierte Konto muss im Microsoft SQL Server die Rolle **dbcreator** oder **sysadmin** haben.
  Weitere Informationen über das Anmeldekonto finden Sie im Abschnitt '"Erforderliche Benutzerrechte für das Dienst-Anmeldekonto" (S. 90)'.
- SQL Server-Authentifizierung
  Sie können diese Methode immer anwenden. Das spezifizierte Konto muss im Microsoft SQL Server die Rolle **dbcreator** oder **sysadmin** haben.

### Scan Service

Der Scan Service ist eine optionale Komponente, die Antimalware-Scans von Backups in einem Cloud Storage oder in einem lokalen oder Netzwerk-Ordner ermöglicht. Der Scan Service setzt voraus, dass der Management Server auf derselben Maschine installiert ist.

Durch die Installation von Scan Service erhalten Sie Zugriff auf folgende Funktionalitäten:

- Backup-Scanning-Pläne
- Widget für Backup-Scanning-Details
- Positivliste für Unternehmensapplikationen
- Safe Recovery
- Die Spalte **Status** in der Liste der Backups

Sie können den Scan Service während der Installation des Management Servers mitinstallieren oder ihn später hinzufügen, indem Sie die vorhandene Installation ändern. Weitere Informationen darüber, wie Sie optionale Komponenten wie den Scan Service installieren können, finden Sie im Abschnitt '"So können Sie optionale Komponenten installieren" (S. 89)'.

**Wichtig**
Der Scan Service ist nicht mit der Standard-SQLite-Datenbank kompatibel, die der Management Server verwendet.

Sie können den Scan Service mit einer Microsoft SQL- oder einer PostgerSQL-Datenbank konfigurieren. Weitere Informationen über die Auswahl eines solchen Systems finden Sie im Abschnitt '"Datenbank für Scan Service" (S. 95)'.

# Datenbank für Scan Service

Der Scan Service ist mit SQLite, der Standarddatenbank für den Management Server, nicht kompatibel.

Wenn Ihr Management Server also SQLite verwendet, können Sie den Scan Service nur mit einer PostgreSQL-Datenbank konfigurieren. Es werden die Versionen PostgreSQL 9.6 und höher unterstützt.

Wenn Ihr Management Server den Microsoft SQL Server verwendet, können Sie den Scan Service mit derselben Datenbank konfigurieren, ohne zusätzliche Einstellungen vornehmen zu müssen. Sie können den Scan Service auch mit einer PostgreSQL-Datenbank konfigurieren.

***So können Sie den Scan Service mit einer PostgreSQL-Datenbank konfigurieren***

1. Klicken Sie im Installationsassistenten unter **Datenbank für den Scan Service** auf **Ändern**.
2. Wählen Sie **PostgreSQL Server-Datenbank** aus.
3. Spezifizieren Sie den Host-Namen der PostgreSQL-Instanz oder die IP-Adresse und den Port.
4. Spezifizieren Sie die Anmeldedaten eines Benutzers, der über die Berechtigung **CREATEDB** verfügt oder ein Superuser ist.

   **Hinweis**
   Die SCRAM-SHA-256-Authentifizierungsmethode in PostgreSQL 10 und höher wird nicht unterstützt.

5. Klicken Sie auf **Fertig**.

## Ports

Sie können den Port, der von einem Webbrowser für den Zugriff auf den Management Server verwendet wird (Vorgabe: 9877), sowie den Port, der zur Kommunikation zwischen den Produktkomponenten verwendet wird (Vorgabe: 7780), anpassen. Wenn Sie den letztgenannten Port nach Abschluss der Installation ändern, müssen alle Komponenten neu registriert werden.

Die Windows-Firewall wird während der Installation automatisch konfiguriert. Wenn Sie eine andere Firewall verwenden, vergewissern Sie sich, dass die entsprechenden Ports in der Firewall für eingehende und rausgehende Anfragen geöffnet sind.

## Proxy-Server

Sie können bestimmen, ob die Protection Agenten einen HTTP-Proxy-Server verwenden sollen, wenn sie Backups zum bzw. Wiederherstellungen vom Cloud Storage durchführt.

Außerdem wird derselbe Proxy-Server dann für die Kommunikation zwischen den verschiedenen Acronis Cyber Protect-Komponenten verwendet.

Wenn Sie einen Proxy-Server verwenden wollen, müssen Sie dessen Host-Namen oder die IP-Adresse und die Port-Nummer spezifizieren. Wenn der Proxy-Server eine Authentifizierung erfordert, müssen Sie entsprechenden Anmeldedaten spezifizieren.

**Hinweis**
Ein Update der Schutzdefinitionen (Antivirus & Antimalware-Definitionen; Definitionen für die erweiterte Erkennung; Definitionen für die Schwachstellenbewertung und Patch-Verwaltung) ist nicht möglich, wenn Sie einen Proxy-Server verwenden.

## Installation unter Linux

### Vorbereitung

1. Wenn Sie den Agenten für Linux zusammen mit dem Management Server installieren wollen, müssen Sie sicherstellen, dass die erforderlichen Linux-Pakete auf der Maschine installiert sind.
2. Wählen Sie die Datenbank aus, die der Management Server verwenden soll.

### Beschränkung

Management Server, die auf Linux-Maschinen laufen, unterstützen keine Remote-Installation von Protection Agenten (wie sie z.B. bei der automatischen Erkennung verwendet wird). Weitere Informationen zu einem möglichen Workaround finden Sie in unserer Knowledge Base: https://kb.acronis.com/content/69553.

### Installation

Sie benötigen mindestens 4 GB freien Speicherplatz auf dem Laufwerk, um den Management Server installieren zu können.

***Installation des Management Servers***

1. Wechseln Sie als Root-Benutzer in das Verzeichnis mit der Installationsdatei, machen Sie die Datei ausführbar und starten Sie diese.

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

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

2. Akzeptieren Sie die Lizenzvereinbarung.
3. [Optional] Bestimmen Sie die Komponenten, die Sie installieren wollen.
   Standardmäßig werden die folgenden Komponenten installiert:
   - Management Server
   - Agent für Linux
   - Bootable Media Builder

4. Spezifizieren Sie den Port, den der Webbrowser verwenden soll, um auf den Management Server zuzugreifen. Der Standardwert ist 9877.
5. Spezifizieren Sie den Port, der zur Kommunikation zwischen den Produktkomponenten verwendet werden soll. Der Standardwert ist 7780.
6. Klicken Sie auf **Weiter**, um mit der Installation fortzufahren.
7. Wählen Sie nach Abschluss der Installation den Befehl **Webkonsole öffnen** und klicken Sie dann auf **Beenden**. Die Cyber Protect Webkonsole wird in Ihrem Standard-Webbrowser geöffnet.

Um Ihren Management Server in Betrieb nehmen zu können, müssen Sie ihn durch Anmeldung an Ihrem Acronis Konto oder mithilfe einer Aktivierungsdatei aktivieren.

## Acronis Die Cyber Protect Appliance

Mit der Acronis Cyber Protect Appliance können Sie ganz einfach eine virtuelle Maschine mit folgender Software erhalten:

- CentOS
- Acronis Cyber Protect Komponenten:
  - Management Server
  - Agent für Linux
  - Agent für VMware (Linux)

Die Appliance wird als.zip-Archiv bereitgestellt. Das Archiv enthält die .ovf- und .iso-Dateien. Sie können die.ovf-Datei auf einem ESXi-Host bereitstellen oder die.iso-Datei verwenden, um eine vorhandene virtuelle Maschine zu booten. Das Archiv enthält auch die.vmdk-Datei, die im selben Verzeichnis wie die.ovf-Datei gespeichert werden sollte..

**Hinweis**
Der VMware Host Client (ein Web-Client, der zur Verwaltung eigenständiger ESXi 6.0+ Hosts verwendet wird) erlaubt es nicht, OVF-Vorlagen bereitzustellen, die ein ISO-Image enthalten. Erstellen Sie in so einem Fall eine virtuelle Maschine, die die unteren Anforderungen erfüllt, und installieren Sie dann die Software mithilfe der.iso-Datei.

Die Anforderungen für die virtuelle Appliance sind wie folgt:

- Minimale Systemanforderungen:
  - 2 CPUs
  - 6 GB RAM
  - Ein virtuelles Laufwerk mit 10 GB (40 GB empfohlen)
- Klicken Sie in den Einstellungen der virtuellen VMware-Maschine folgende Befehle: **Optionen** (Registerkarte) –> **Allgemein** –> **Konfigurationsparameter** und überprüfen Sie dann, dass der Parameterwert `disk.EnableUUID` auf `true` eingestellt ist.

## Beschränkung

Management Server, die auf Linux-Maschinen (einschließlich der Acronis Cyber Protect-Appliance) laufen, unterstützen keine Remote-Installation von Protection Agenten (wie sie z.B. bei der automatischen Erkennung verwendet wird). Weitere Informationen zu einem möglichen Workaround finden Sie in unserer Knowledge Base: https://kb.acronis.com/content/69553.

## Die Installation der Software

1. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Stellen Sie die Appliance über die .ovf-Vorlage bereit. Schalten Sie die resultierende Maschine ein, nachdem das Deployment abgeschlossen wurde.
   - Booten Sie eine vorhandene virtuelle Maschine von der .iso-Datei.
2. Wählen Sie den Befehl **Acronis Cyber Protect installieren oder aktualisieren** und drücken Sie die **Eingabetaste**. Warten Sie, bis das einführende Setup-Fenster angezeigt wird.
3. [Optional] Wenn Sie die Installationseinstellungen ändern wollen, wählen Sie **Einstellungen ändern** und drücken Sie die **Eingabetaste**. Sie können folgende Einstellungen festlegen:
   - Der Host-Name der Appliance (Standardvorgabe ist: `AcronisAppliance-<Zufallssequenz>`).
   - Das Kennwort für das Konto 'root', welches zur Anmeldung an die Cyber Protect Webkonsole verwendet werden soll (Standardvorgabe ist: **nicht spezifiziert**).

     Wenn Sie die Standardvorgabe übernehmen, werden Sie nach der Installation von Acronis Cyber Protect aufgefordert, das Kennwort zu spezifizieren. Ohne dieses Kennwort werden Sie sich nicht an der Cyber Protect Webkonsole und der Cockpit Webkonsole anmelden können.
   - Netzwerkeinstellungen einer Netzwerkkarte:
     - **DHCP verwenden** (Standardvorgabe)
     - **Statische IP-Adresse festlegen**

     Wenn das Gerät mehrere Netzwerkkarten hat, wählt die Software eine davon zufällig aus und wendet diese Einstellungen auf das Gerät an.
4. Wählen Sie den Befehl **Mit den aktuellen Einstellungen installieren**.

Als Ergebnis werden CentOS und Acronis Cyber Protect auf der Maschine installiert.

## Weitere Aktionen

Nachdem die Installation abgeschlossen wurde, zeigt die Software die Links zur Cyber Protect Webkonsole und zur Cockpit Webkonsole an. Verbinden Sie sich mit der Cyber Protect Webkonsole, um mit der Verwendung von Acronis Cyber Protect zu beginnen: fügen Sie Geräte hinzu, erstellen Sie Backup-Pläne und so weiter.

Um virtuelle ESXi-Maschinen hinzufügen zu können, müssen Sie auf **Hinzufügen** –> **VMware ESXi** klicken – und dann die Adresse und Anmeldedaten für den vCenter Server oder den eigenständigen ESXi-Host spezifizieren.

In der Cockpit Webkonsole werden keine Einstellungen für Acronis Cyber Protect konfiguriert. Die Konsole dient nur der Übersichtlichkeit und Fehlersuche.

### Die Software per Update aktualisieren

1. Laden Sie das.zip-Archiv mit der neuen Appliance-Version herunter und entpacken Sie es.
2. Booten Sie die Maschine mit der .iso-Datei, die Sie im vorherigen Schritt entpackt haben.
   a. Speichern Sie die .iso-Datei in Ihrem vSphere-Datenspeicher.
   b. Mounten Sie die ISO-Datei als CD-/DVD-Laufwerk der Maschine.
   c. Starten Sie die Maschine neu.
   d. [Nur beim ersten Update] Drücken Sie auf **F2** und ändern Sie die Boot-Reihenfolge so, dass das CD/DVD-Laufwerk das primäre Boot-Gerät ist.
3. Wählen Sie den Befehl **Acronis Cyber Protect installieren oder aktualisieren** und drücken Sie die **Eingabetaste**.
4. Wählen Sie den Befehl **Update** und drücken Sie die **Eingabetaste**.
5. Sobald das Update abgeschlossen wurde, können Sie die .iso-Datei wieder vom CD/DVD-Laufwerk der Maschine trennen (unmounten).

Als Ergebnis wird ein Update von Acronis Cyber Protect durchgeführt. Falls auch die CentOS-Version in der .iso-Datei neuer als die Version auf dem Laufwerk ist, wird zuerst das Betriebssystem aktualisiert und dann das Update von Acronis Cyber Protect durchgeführt.

## Maschinen über die Cyber Protect-Webkonsole hinzufügen

Sie können eine Maschine auf eine der folgenden Arten hinzufügen:

- Indem Sie das Setup-Programm herunterladen und lokal auf der Zielmaschine ausführen.
- Indem Sie einen Protection Agenten remote auf der Zielmaschine installieren.

### Einschränkungen

- Die Möglichkeit zur Remote-Installation besteht nur, wenn ein Management Server auf einer Windows-Maschine läuft. Und auch auf den Zielmaschinen muss Windows laufen.
- Bei Maschinen, die unter Windows XP laufen, wird keine Remote-Installation unterstützt.
- Bei Domain Controllern wird keine Remote-Installation unterstützt. Wie Sie einen Protection Agenten auf einem Domain Controller installieren können, erfahren Sie im Abschnitt '"Installation unter Windows" (S. 109)'. Stellen Sie sicher, dass Sie die Installationseinstellungen anpassen, indem Sie unter **Anmeldekonto für den Agenten-Dienst** die Option **Folgendes Konto verwenden** wählen. Weitere Informationen zu dieser Option finden Sie im Abschnitt '"Erforderliche Benutzerrechte für das Dienst-Anmeldekonto" (S. 90)'.

## Eine unter Windows laufende Maschine hinzufügen

Sie können eine Windows-Maschine hinzufügen, indem Sie einen Protection Agent über die Cyber Protect-Webkonsole remote installieren oder indem Sie das Setup-Programm auf der Maschine herunterladen und lokal ausführen.

***So können Sie einen Agenten remote installieren***

**Wichtig**
Stellen Sie vor Beginn der Installation sicher, dass die Voraussetzungen für die Remote-Installation erfüllt sind und dass es in Ihrer Umgebung mindestens einen Agenten gibt, der als Deployment Agent dienen kann. Weitere Informationen dazu finden Sie in den Abschnitten '"Voraussetzungen für Remote-Installationen" (S. 101)' und '"Deployment Agent" (S. 103)'.

1. Gehen Sie in der Cyber Protect-Webkonsole zu **Geräte** –> **Alle Geräte**.
2. Klicken Sie auf **Hinzufügen**.
3. [Wenn Sie den Agenten für Windows installieren wollen] Klicken Sie auf **Windows**.
4. [Wenn Sie einen anderen unterstützten Agenten installieren wollen] Klicken Sie auf die Schaltfläche, die derjenigen Applikation entspricht, die Sie schützen wollen.
   Folgende Agenten sind verfügbar:
   - Agent für Hyper-V
   - Agent für SQL + Agent für Windows
   - Agent für Exchange + Agent für Windows
     Wenn Sie auf **Microsoft Exchange Server** –> **Exchange-Postfächer** geklickt haben und mindestens ein Agent für Exchange bereits registriert ist, dann gehen Sie zu Schritt 9.
   - Agent für Active Directory + Agent für Windows
   - Agent für Office 365
5. Wählen Sie in dem sich öffnenden Fensterbereich den Deployment Agenten aus.
6. Spezifizieren Sie den Host-Namen oder die IP-Adresse der Zielmaschine sowie die Anmeldedaten eines Kontos, welches über administrative Rechte auf dieser Maschine verfügt.
   Wir empfehlen, dass Sie das integrierte Administrator-Konto verwenden. Wenn Sie ein anderes Konto verwenden wollen, müssen Sie dieses Konto zur Gruppe der Administratoren hinzufügen und dann die Registry der Zielmaschine wie im nachfolgenden Artikel beschrieben ändern: https://support.microsoft.com/de-de/help/951016/description-of-user-account-control-and-remote-restrictions-in-windows.
7. Wählen Sie den Namen oder die IP-Adresse des Management Servers, über den bzw. die der Agent auf diesen Server zugreifen wird.
   Standardmäßig ist der Name des Servers vorausgewählt. Wenn Ihr Management Server über mehr als eine Netzwerkschnittstelle verfügt oder wenn Sie DNS-Probleme haben, die die Registrierung des Agenten fehlschlagen lassen, sollten Sie stattdessen die IP-Adresse auswählen.

8. Klicken Sie auf **Installieren**.
9. [Wenn Sie im Schritt 4 **Microsoft Exchange Server** –> **Exchange-Postfächer** ausgewählt haben] Spezifizieren Sie die Maschine, auf welcher die Server-Rolle **Clientzugriffe** (CAS) des Microsoft Exchange Servers aktiviert ist. Weitere Informationen dazu finden Sie im Abschnitt '"Postfach-Backup" (S. 479)'.

***So können Sie einen Agenten herunterladen und lokal installieren***

1. Klicken Sie in der rechten oberen Ecke der Cyber Protect-Webkonsole auf das Symbol für das Konto und anschließend auf **Downloads**.
2. Klicken Sie auf den Namen des Windows-Installers, den Sie benötigen.
   Das Setup-Programm wird auf Ihre Maschine heruntergeladen.
3. Starten Sie das Setup-Programm auf der Maschine, die Sie schützen wollen. Weitere Informationen dazu finden Sie im Abschnitt '"Installation unter Windows" (S. 109)'.

## Voraussetzungen für Remote-Installationen

- Damit die Installation auf einer Remote-Maschine erfolgreich ist, die mit Windows 7 oder höher läuft, muss die Option **Systemsteuerung** –> **Ordneroptionen** –> **Ansicht** –> **Freigabe-Assistent verwenden (empfohlen)** auf dieser Maschine *deaktiviert* sein.
- Zur erfolgreichen Installation auf einer Remote-Maschine, die *kein* Mitglied einer Active Directory-Domain ist, muss auf dieser Maschine die Benutzerkontensteuerung (UAC) *deaktiviert sein*. Weitere Informationen zur Deaktivierung der Option finden Sie im Abschnitt '"So können Sie UAC deaktivieren" (S. 102)'.
- Um die Remote-Installation auf einer Windows-Maschine durchführen zu können, werden standardmäßig die Anmeldedaten des integrierten Administratorkontos benötigt. Um eine Remote-Installation mit den Anmeldedaten eines anderen Administratorkontos durchführen zu können, müssen die Remote-Beschränkungen der Benutzerkontensteuerung (UAC) *deaktiviert* sein. Weitere Informationen zu deren Deaktivierung finden Sie im Abschnitt '"So können Sie die UAC-Remote-Beschränkungen deaktivieren" (S. 102)'.
- Auf der Remote-Maschine muss die Datei- und Druckerfreigabe *aktiviert* sein. So erhalten Sie Zugriff auf diese Option:
  - [Auf einer Maschine, die unter Windows 2003 Server läuft] Gehen Sie zu **Systemsteuerung** –> **Windows-Firewall** –> **Ausnahmen** –> **Datei- und Druckerfreigabe**.
  - [Auf einer Maschine, die unter Windows Server 2008, Windows 7 oder höher läuft] Gehen Sie zu **Systemsteuerung** –> **Windows-Firewall** –> **Netzwerk- und Freigabecenter** –> **Erweiterte Freigabeeinstellungen ändern**.
- Acronis Cyber Protect 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** and **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.

**Hinweis**
Bei Maschinen, die unter Windows XP laufen, wird keine Remote-Installation unterstützt.

**Hinweis**
Bei Domain Controllern wird keine Remote-Installation unterstützt. Wie Sie einen Protection Agenten auf einem Domain Controller installieren können, erfahren Sie im Abschnitt '"Installation unter Windows" (S. 109)'. Stellen Sie sicher, dass Sie die Installationseinstellungen anpassen, indem Sie unter **Anmeldekonto für den Agenten-Dienst** die Option **Folgendes Konto verwenden** wählen. Weitere Informationen zu dieser Option finden Sie im Abschnitt '"Erforderliche Benutzerrechte für das Dienst-Anmeldekonto" (S. 90)'.

## Anforderungen an die Benutzerkontensteuerung (UAC)

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

***So können Sie UAC deaktivieren***

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

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

***So können Sie die UAC-Remote-Beschränkungen deaktivieren***

1. Öffnen Sie den Registrierungseditor.
2. Suchen Sie folgenden Registry-Schlüssel: **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System**
3. Ändern Sie für den Wert **LocalAccountTokenFilterPolicy** die Einstellung auf **1**.
   Wenn der Wert '**LocalAccountTokenFilterPolicy**' nicht vorhanden ist, erstellen Sie diesen als DWORD (32 Bit). Weitere Informationen zu diesem Wert finden Sie in der Microsoft-

Dokumentation: https://support.microsoft.com/de-de/help/951016/description-of-user-account-control-and-remote-restrictions-in-windows.

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

## Deployment Agent

Wenn Sie Protection Agenten über die Cyber Protect-Webkonsole auf Remote-Maschinen installieren wollen, muss mindestens ein Agent bereits in Ihrer Umgebung installiert sein. Dieser Agent wird als Deployment Agent für die Remote-Installation dienen und eine Verbindung zum Management Server und der Remote-Zielmaschine herstellen.

Normalerweise ist der erste Protection Agent in der Umgebung derjenige Agent, den Sie zusammen mit dem Management Server installieren. Sie können aber jeden Agenten für Windows in der Umgebung als Deployment Agent auswählen.

**Hinweis**
Wenn Sie die automatische Erkennung verwenden, um die Protection Agenten auf mehreren Maschinen bereitzustellen, wird der Deployment Agent als Discovery Agent bezeichnet.

### Wie der Deployment Agent funktioniert

1. Der Deployment Agent verbindet sich mit dem Management Server und lädt die Datei `web_installer.exe` herunter.
2. Der Deployment Agent verbindet sich mit der Remote-Maschine, indem er den Host-Namen oder die IP-Adresse dieser Maschine sowie die von Ihnen spezifizierten Administrator-Ameldedaten verwendet. Anschließend wird der Agent die Datei `web_installer.exe` auf die Maschine hochladen.
3. Die Datei `web_installer.exe` wird auf der Remote-Maschine im unbeaufsichtigten Modus ausgeführt.
4. Je nach Umfang der gewünschten Installation, ruft der Webinstaller auf dem Management Server zusätzliche Installationspakete aus dem Ordner `installation_files` ab und installiert diese Pakete dann über den Befehl `msiexec` auf den Zielmaschinen.

   Der Ordner `installation_files` findet sich in folgendem Verzeichnis:
   - Unter Windows: `\Programme\Acronis\RemoteInstallationFiles\`
   - Unter Linux: `/usr/lib/Acronis/RemoteInstallationFiles/`
5. Nach Abschluss der Installation wird der Agent auf dem Management Server registriert.

## Komponenten zur Remote-Installation

Die Komponenten zur Remote-Installation werden standardmäßig mit installiert, wenn Sie den Management Server installieren.

Je nachdem, welches Betriebssystem die Maschine verwendet, auf der der Management Server läuft, können Sie diese Komponenten an folgenden Speicherorten finden:

- Windows: `%Program Files%\Acronis\RemoteInstallationFiles\installation_files`
- Linux: `/usr/lib/Acronis/RemoteInstallationFiles/installation_files`

Diese Speicherorte sind jedoch möglicherweise nicht verfügbar, wenn Sie ein Upgrade von einer älteren Version von Acronis Cyber Protect durchgeführt haben oder wenn Sie die **Komponenten zur Remote-Installation** ausdrücklich ausgeschlossen haben, als Sie den Management Server installiert haben. In diesem Fall müssen Sie die Komponenten zur Remote-Installation manuell hinzufügen, indem Sie Ihre bestehende Installation von Acronis Cyber Protect aktualisieren und entsprechend ändern.

***So können Sie die Komponenten zur Remote-Installation einer bestehenden Installation hinzufügen***

1. Laden Sie die neueste Installationsdatei für Acronis Cyber Protect von der Acronis-Website herunter.
   Wählen Sie die Installationsdatei aus, die der Bit-Anzahl Ihres Betriebssystems entspricht. In den meisten Fällen werden Sie die Installationsdatei für **Windows 64 Bit** benötigen. Wenn Sie die Protection Agenten remote auf 32-Bit-Maschinen installieren müssen, müssen Sie die Installationsdatei für **Windows 32/64 Bit** herunterladen.
2. Starten Sie auf der Maschine, auf welcher der Management Server ausgeführt wird, die Installationsdatei und wählen Sie anschließend den Befehl **Update**.
3. Starten Sie, nachdem das Update abgeschlossen wurde, die Installationsdatei erneut und wählen Sie dann den Befehl **Aktuelle Installation ändern**.
4. Wählen Sie **Komponenten zur Remote-Installation** und klicken Sie anschließend auf **Fertig**.

Nachdem die Installation abgeschlossen wurde, können Sie die Protection Agenten über die Cyber Protect-Webkonsole auf den Remote-Maschinen installieren.

## Eine unter Linux laufende Maschine hinzufügen

Sie können eine Linux-Maschine nur dadurch hinzufügen, dass Sie den Protection Agent lokal installieren. Remote-Installationen werden nicht unterstützt.

***So können Sie eine unter Linux laufende Maschine hinzufügen***

1. Klicken Sie in der Cyber Protect-Webkonsole auf **Alle Geräte** –> **Hinzufügen**.
2. Klicken Sie auf **Linux**.
   Das Setup-Programm wird auf Ihre Maschine heruntergeladen.
3. Starten Sie das Setup-Programm auf der Maschine, die Sie schützen wollen. Weitere Informationen dazu finden Sie im Abschnitt '"Installation unter Linux" (S. 111)'.

## Eine unter macOS laufende Maschine hinzufügen

Sie können eine macOS-Maschine nur dadurch hinzufügen, dass Sie den Protection Agent lokal installieren. Remote-Installationen werden nicht unterstützt.

***So können Sie eine unter macOS laufende Maschine hinzufügen***

1. Klicken Sie in der Cyber Protect-Webkonsole auf **Alle Geräte** –> **Hinzufügen**.
2. Klicken Sie auf **Mac**.

   Das Setup-Programm wird auf Ihre Maschine heruntergeladen.
3. Starten Sie das Setup-Programm auf der Maschine, die Sie schützen wollen. Weitere Informationen dazu finden Sie im Abschnitt '"Installation unter macOS" (S. 113)'.

## Ein vCenter oder einen ESXi-Host hinzufügen

Es gibt vier Methoden, wie Sie dem Management Server einen vCenter-Host oder einen eigenständigen ESXi-Host hinzufügen können:

- Den Agenten für VMware (Virtuelle Appliance) bereitstellen

  Diese Methode wird für die meisten Fälle empfohlen. Die virtuelle Appliance wird automatisch auf allen Hosts bereitgestellt, welcher von dem von Ihnen spezifizierten vCenter verwaltet wird. Sie können die Hosts auswählen und die Einstellungen der virtuellen Appliance anpassen.
- Den Agent für VMware (Windows) installieren

  Vielleicht wollen Sie den Agenten für VMware auf einer unter Windows laufenden physischen Maschine installieren, um ein 'offloaded' oder LAN-freies Backup durchzuführen.
  - **Offloaded Backup**

    Wird verwendet, wenn Ihre produktiven ESX(i)-Hosts so stark ausgelastet sind, dass eine Ausführung der virtuellen Appliances nicht wünschenswert ist.
  - **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. Ausführliche Informationen finden Sie im Abschnitt 'LAN-freies Backup'.

  Wenn der Management Server unter Windows läuft, wird der Agent automatisch auf der von Ihnen spezifizierten Maschine bereitgestellt. Ansonsten müssen Sie den Agenten manuell installieren.
- Einen bereits installierten Agenten für VMware registrieren

  Dieser Schritt ist notwendig, wenn Sie den Management Server neu installiert haben. Sie können außerdem den Agenten für VMware (Virtuelle Appliance), der über eine OVF-Vorlage bereitgestellt wird, registrieren und konfigurieren.
- Einen bereits registrierten Agenten für VMware konfigurieren

  Dieser Schritt ist notwendig, wenn Sie den Agenten für VMware (Windows) manuell installiert oder als Acronis Cyber Protect Appliance bereitgestellt haben. Außerdem können Sie einen

bereits konfigurierten Agenten für VMware mit einem anderen vCenter Server oder eigenständigen ESXi-Host verknüpfen.

### Den Agenten für VMware (Virtuelle Appliance) über die Weboberfläche bereitstellen

1. Klicken Sie auf **Alle Geräte** –> **Hinzufügen**.
2. Klicken Sie auf **VMware ESXi**.
3. Wählen Sie **Als virtuelle Appliance auf jedem Host eines vCenters bereitstellen**.
4. Spezifizieren Sie die Adresse und Anmeldedaten für den vCenter Server oder den eigenständigen ESXi-Host. 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 auf dem vCenter Server oder ESXi-Host verfügt.
5. Wählen Sie den Namen oder die IP-Adresse des Management Servers, über den bzw. die der Agent auf diesen Server zugreifen wird.
   Standardmäßig ist der Name des Servers vorausgewählt. Wenn Ihr Management Server über mehr als eine Netzwerkschnittstelle verfügt oder wenn Sie DNS-Probleme haben, die die Registrierung des Agenten fehlschlagen lassen, sollten Sie stattdessen die IP-Adresse auswählen.
6. [Optional] Klicken Sie auf **Einstellungen**, um die Deployment-Einstellungen anzupassen:
   - Die ESXi-Hosts, auf denen Sie den Agent bereitstellen wollen (nur, wenn im vorherigen Schritt ein vCenter Server spezifiziert wurde).
   - Den Namen der virtuellen Appliance.
   - Den Datenspeicher, wo die Appliance gespeichert werden soll.
   - Den Ressourcenpool oder die vApp, wo die Appliance aufgenommen wird.
   - Das Netzwerk, mit dem der Netzwerkadapter der virtuellen Appliance verbunden werden soll.
   - Die Netzwerkeinstellungen der virtuellen Appliance. Sie können Autokonfiguration per DHCP wählen oder die Werte (inkl. einer statischen IP-Adresse) manuell spezifizieren.
7. Klicken Sie auf **Bereitstellen**.

### Den Agent für VMware (Windows) installieren

#### Vorbereitung

Befolgen Sie die im Abschnitt 'Eine unter Windows laufende Maschine hinzufügen' beschriebenen Vorbereitungsschritte.

#### Installation

1. Klicken Sie auf **Alle Geräte** –> **Hinzufügen**.
2. Klicken Sie auf **VMware ESXi**.
3. Wählen Sie die Option **Auf einer unter Windows laufenden Maschine remote installieren**.
4. Wählen Sie den Deployment Agent.

5. Spezifizieren Sie den Host-Namen oder die IP-Adresse der Zielmaschine sowie die Anmeldedaten eines Kontos, welches über administrative Berechtigungen auf dieser Maschine verfügt.
6. Wählen Sie den Namen oder die IP-Adresse des Management Servers, über den bzw. die der Agent auf diesen Server zugreifen wird.
   Standardmäßig ist der Name des Servers vorausgewählt. Wenn Ihr Management Server über mehr als eine Netzwerkschnittstelle verfügt oder wenn Sie DNS-Probleme haben, die die Registrierung des Agenten fehlschlagen lassen, sollten Sie stattdessen die IP-Adresse auswählen.
7. Klicken Sie auf **Verbinden**.
8. Spezifizieren Sie die Adresse und Anmeldedaten für den vCenter Server oder den eigenständigen ESXi-Host – und klicken Sie dann auf **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 auf dem vCenter Server oder ESXi-Host verfügt.
9. Klicken Sie auf **Installieren**, damit der Agent eingerichtet wird.

## Einen bereits installierten Agenten für VMware registrieren

Dieser Abschnitt beschreibt, wie Sie einen Agenten für VMware über die Weboberfläche registrieren können.

Alternative Registrierungsmethoden:

- Sie können den Agenten für VMware (Virtuelle Appliance) registrieren, indem Sie den Management Server in der Benutzeroberfläche der virtuellen Appliance spezifizieren. Sie Schritt 3 unter 'Die virtuelle Appliance konfigurieren' im Abschnitt 'Den Agenten für VMware (Virtuelle Appliance) von einer OVF-Vorlage aus bereitstellen'.
- Der Agent für VMware (Windows) wird während seiner lokalen Installation registriert.

***So können Sie den Agenten für VMware registrieren***

1. Klicken Sie auf **Alle Geräte** –> **Hinzufügen**.
2. Klicken Sie auf **VMware ESXi**.
3. Wählen Sie die Option **Einen bereits installierten Agenten registrieren**.
4. Wählen Sie den Deployment Agent.
5. Wenn Sie den *Agenten für VMware (Windows)* registrieren, spezifizieren Sie den Host-Namen oder die IP-Adresse derjenigen Maschine, wo der Agent installiert ist, sowie die Anmeldedaten eines Kontos, welches über administrative Berechtigungen auf dieser Maschine verfügt.
   Wenn Sie den *Agenten für VMware (Virtuelle Appliance)* registrieren, spezifizieren Sie den Host-Namen oder die IP-Adresse der virtuellen Appliance sowie die Anmeldedaten für den vCenter Server oder den autonomen ESXi-Host, wo die Appliance ausgeführt wird.
6. Wählen Sie den Namen oder die IP-Adresse des Management Servers, über den bzw. die der Agent auf diesen Server zugreifen wird.

Standardmäßig ist der Name des Servers vorausgewählt. Wenn Ihr Management Server über mehr als eine Netzwerkschnittstelle verfügt oder wenn Sie DNS-Probleme haben, die die Registrierung des Agenten fehlschlagen lassen, sollten Sie stattdessen die IP-Adresse auswählen.

7. Klicken Sie auf **Verbinden**.
8. Spezifizieren Sie den Host-Namen oder die IP-Adresse des vCenter Servers oder ESXi-Hosts sowie die entsprechenden Zugriffsanmeldedaten – und klicken Sie dann auf **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 auf dem vCenter Server oder ESXi-Host verfügt.
9. Klicken Sie auf **Registrieren**, um den Agenten zu registrieren.

### Einen bereits registrierten Agenten für VMware konfigurieren

Dieser Abschnitt beschreibt, wie Sie einen Agenten für VMware mit einem vCenter Server oder ESXi in der Weboberfläche assoziieren. Alternativ können Sie das auch über die Konsole des Agenten für VMware (Virtuelle Appliance) tun.

Mit dieser Prozedur können Sie auch eine bestehende Assoziation des Agenten mit einem vCenter Server oder ESXi ändern. Sie können dies außerdem auch über die Konsole des Agenten für VMware (Virtuelle Appliance) vornehmen oder indem Sie auf folgende Befehle klicken: **Einstellungen** –> **Agenten** –> der betreffende Agent –> **Details** –> **vCenter/ESXi**.

***So können Sie den Agenten für VMware konfigurieren***

1. Klicken Sie auf **Alle Geräte** –> **Hinzufügen**.
2. Klicken Sie auf **VMware ESXi**.
3. Die Software zeigt den unkonfigurierten Agenten für VMware, der in der alphabetischen Reihenfolge zuerst angezeigt wird.
   Wenn alle Agenten auf dem Management Server konfiguriert sind, klicken Sie auf den Befehl **Einen bereits registrierten Agenten konfigurieren**. Die Software zeigt daraufhin den Agenten zuerst an, der in der alphabetischen Liste zuerst angezeigt wird.
4. Klicken Sie, falls notwendig, auf **Maschine mit Agent** und wählen Sie den Agenten aus, der konfiguriert werden soll.
5. Spezifizieren oder ändern Sie den Host-Namen oder die IP-Adresse des vCenter Servers oder ESXi-Hosts sowie die entsprechenden Zugriffsanmeldedaten. 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 auf dem vCenter Server oder ESXi-Host verfügt.
6. Klicken Sie auf **Konfigurieren**, um die Änderungen zu speichern.

## Einen Scale Computing HC3-Cluster hinzufügen

***So können Sie einen Scale Computing HC3-Cluster zum Cyber Protect Management Server hinzufügen***

1. Stellen Sie einen Agenten für Scale Computing HC3 (Virtuelle Appliance) im Cluster bereit.
2. Konfigurieren Sie dessen Verbindung mit dem Cluster und dem Cyber Protect Management Server.

# Agenten lokal installieren

## Installation unter Windows

***So installieren Sie den Agenten für Windows, den Agenten für Hyper-V, den Agenten für Exchange, den Agenten für SQL oder den Agenten für Active Directory***

1. Melden Sie sich als Administrator an und starten Sie das Acronis Cyber Protect Setup-Programm.
2. [Optional] Wenn Sie die Sprache des Setup-Programms ändern wollen, klicken Sie auf **Sprache einrichten**.
3. Akzeptieren Sie die Bedingungen der Lizenzvereinbarung sowie die Datenschutzerklärung und klicken Sie anschließend auf **Fertigstellen**.
4. Wählen Sie den Befehl **Einen Protection Agenten installieren**.
5. Gehen Sie nach einer der folgenden Möglichkeiten vor:
   - Klicken Sie auf **Installieren**.

     Dies ist die einfachste Möglichkeit, das Produkt zu installieren. Die meisten Installationsparameter sind dabei auf Standardwerte eingestellt.

     Folgende Komponenten werden installiert:
     - Agent für Windows
     - Andere Agenten (der Agent für Hyper-V, der Agent für Exchange, Agent für SQL und der Agent für Active Directory), falls ein entsprechender Hypervisor oder eine entsprechende Applikation auf der Maschine erkannt wird.
     - Bootable Media Builder
     - Befehlszeilenwerkzeug
     - Cyber Protect Monitor
   - Klicken Sie auf **Installationseinstellungen anpassen**, um die Einrichtung zu konfigurieren. Sie können auswählen, welche Komponenten installiert werden sollen, und einige zusätzliche Parameter spezifizieren. Weitere Informationen finden Sie hier: "Installationseinstellungen anpassen" (S. 88).
   - Klicken Sie auf **.mst- und .msi-Dateien für eine unbeaufsichtigte Installation erstellen**, um die Installationspakete zu extrahieren. Überprüfen oder ändern Sie die Installationseinstellungen, die der .mst-Datei hinzugefügt werden, und klicken Sie dann auf **Generieren**. Weitere Schritte dieser Prozedur sind nicht erforderlich.

     Wenn Sie Agenten über Gruppenrichtlinien bereitstellen wollen, dann gehen Sie wie im Abschnitt '"Agenten per Gruppenrichtlinie bereitstellen" (S. 186)' beschrieben vor.
6. Spezifizieren Sie den Management Server, auf dem die Maschine mit dem Agenten registriert werden soll:

a. Spezifizieren Sie den Host-Namen oder die IP-Adresse derjenigen Maschine, auf welcher der Management Server installiert ist.
b. Spezifizieren Sie die Anmeldedaten eines Management Server-Administrators oder ein Registrierungstoken.
   Weitere Informationen über die Generierung eines Registrierungstokens finden Sie im Abschnitt '"Schritt 1: Ein Registrierungstoken generieren" (S. 187)'.
c. Klicken Sie auf **Fertig**.

7. Bestimmen Sie bei Aufforderung, ob die Maschine mit dem Agenten dem Unternehmen oder einer der Abteilungen hinzugefügt werden soll.
   Die Aufforderung erscheint, wenn Sie mehr als eine Abteilung oder ein Unternehmen mit mindestens einer Abteilung verwalten. Anderenfalls wird die Maschine unaufgefordert der von Ihnen verwalteten Abteilung oder dem Unternehmen hinzugefügt. Weitere Informationen dazu finden Sie im Abschnitt '"Abteilungen und administrative Konten" (S. 685)'.
8. Fahren Sie mit der Installation fort.
9. Klicken Sie nach Abschluss der Installation auf **Schließen**.
10. Wenn Sie den Agenten für Exchange installiert haben, können Sie Exchange-Datenbanken per Backup sichern. Wenn Sie Exchange-Postfächer sichern wollen, gehen Sie folgendermaßen vor: öffnen Sie die Cyber Protect-Webkonsole, klicken Sie auf **Hinzufügen** –> **Microsoft Exchange Server** –> **Exchange-Postfächer** und spezifizieren Sie dann die Maschine, auf welcher die Server-Rolle **Clientzugriffe** (CAS) des Microsoft Exchange Servers aktiviert ist. Weitere Informationen dazu finden Sie im Abschnitt '"Postfach-Backup" (S. 479)'.

***So können Sie den Agenten für VMware (Windows), den Agenten für Office 365, den Agenten für Oracle oder den Agenten für Exchange auf einer Maschine ohne Microsoft Exchange Server installieren***

1. Melden Sie sich als Administrator an und starten Sie das Acronis Cyber Protect Setup-Programm.
2. [Optional] Wenn Sie die Sprache des Setup-Programms ändern wollen, klicken Sie auf **Sprache einrichten**.
3. Akzeptieren Sie die Bedingungen der Lizenzvereinbarung sowie die Datenschutzerklärung und klicken Sie anschließend auf **Fertigstellen**.
4. Wählen Sie den Befehl **Einen Protection Agenten installieren** und klicken Sie dann auf **Installationseinstellungen anpassen**.
5. Klicken Sie neben **Zu installierende Komponenten** auf **Ändern**.
6. Aktivieren Sie das Kontrollkästchen, welches zu dem Agenten gehört, den Sie installieren wollen. Deaktivieren Sie die Kontrollkästchen derjenigen Komponenten, die Sie nicht installieren wollen. Klicken Sie auf **Fertig**, um fortzufahren.
7. Spezifizieren Sie den Management Server, auf dem die Maschine mit dem Agenten registriert werden soll:
   a. Klicken Sie neben **Acronis Cyber Protect Management Server** auf **Spezifizieren**.

b. Spezifizieren Sie den Host-Namen oder die IP-Adresse derjenigen Maschine, auf welcher der Management Server installiert ist.
c. Spezifizieren Sie die Anmeldedaten eines Management Server-Administrators oder ein Registrierungstoken.

   Weitere Informationen über die Generierung eines Registrierungstokens finden Sie im Abschnitt '"Schritt 1: Ein Registrierungstoken generieren" (S. 187)'.
d. Klicken Sie auf **Fertig**.

8. Bestimmen Sie bei Aufforderung, ob die Maschine mit dem Agenten dem Unternehmen oder einer der Abteilungen hinzugefügt werden soll.

   Die Aufforderung erscheint, wenn Sie mehr als eine Abteilung oder ein Unternehmen mit mindestens einer Abteilung verwalten. Anderenfalls wird die Maschine unaufgefordert der von Ihnen verwalteten Abteilung oder dem Unternehmen hinzugefügt. Weitere Informationen dazu finden Sie im Abschnitt '"Abteilungen und administrative Konten" (S. 685)'.
9. [Optional] Ändern Sie bei Bedarf andere Installationseinstellungen. Informationen dazu finden Sie im Abschnitt '"Installationseinstellungen anpassen" (S. 88)'.
10. Klicken Sie auf **Installation**, um mit der Einrichtung fortzufahren.
11. Klicken Sie nach Abschluss der Installation auf **Schließen**.
12. [Nur, wenn Sie den Agenten für VMware (Windows) installieren] Führen Sie die im Abschnitt '"Einen bereits registrierten Agenten für VMware konfigurieren" (S. 108)' beschriebene Prozedur durch.
13. [Nur bei Installation des Agenten für Exchange] Öffnen Sie die Cyber Protect-Webkonsole, klicken Sie auf **Hinzufügen** –> **Microsoft Exchange Server** –> **Exchange-Postfächer** und spezifizieren Sie dann die Maschine, auf welcher die Server-Rolle **Clientzugriffe** (CAS) des Microsoft Exchange Servers aktiviert ist. Weitere Informationen dazu finden Sie im Abschnitt '"Postfach-Backup" (S. 479)'.

## Installation unter Linux

### Vorbereitung

1. Überprüfen Sie, dass die erforderlichen Linux-Pakete auf der Maschine installiert sind.
2. Wenn Sie den Agenten unter SUSE Linux installieren, sollten Sie sicherstellen, dass Sie `su` statt `sudo` verwenden. Anderenfalls kommt es zu folgendem Fehler, wenn Sie versuchen, den Agenten über die Cyber Protect-Webkonsole zu registrieren: `Der Webbrowser konnte nicht gestartet werden. Es ist keine Anzeige verfügbar.`

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

## Installation

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

***So installieren Sie den Agenten für Linux***

1. Wechseln Sie als Root-Benutzer in das Verzeichnis mit der Installationsdatei (eine .i686- oder .x86_64 file), machen Sie die Datei ausführbar und starten Sie diese.

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

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

2. Akzeptieren Sie die Lizenzvereinbarung.
3. Spezifizieren Sie, welche Komponenten installiert werden sollen:
   a. Aktivieren Sie das Kontrollkästchen **Acronis Cyber Protect Management Server**.
   b. Aktivieren Sie die Kontrollkästchen derjenigen Agenten, die Sie installieren wollen. Folgende Agenten sind verfügbar:
      - **Agent für Linux**
      - **Agent für Oracle**

      Der Agent für Oracle setzt voraus, dass auch der Agent für Linux installiert ist.
   c. Klicken Sie auf **Weiter**.
4. Spezifizieren Sie den Management Server, auf dem die Maschine mit dem Agenten registriert werden soll:
   a. Spezifizieren Sie den Host-Namen oder die IP-Adresse derjenigen Maschine, auf welcher der Management Server installiert ist.
   b. Spezifizieren Sie den Benutzernamen und das Kennwort eines Management Server-Administrators.
   c. Klicken Sie auf **Weiter**.
5. Bestimmen Sie bei Aufforderung, ob die Maschine mit dem Agenten dem Unternehmen oder einer der Abteilungen hinzugefügt werden soll, und drücken Sie dann die **Eingabetaste**.
   Diese Eingabeaufforderung erscheint, wenn das im vorherigen Schritt spezifizierte Konto mehr als eine Abteilung oder ein Unternehmen mit mindestens einer Abteilung verwaltet.
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**
Bei der Installation wird ein neuer Schlüssel generiert, der zum Signieren der Kernel-Module verwendet wird. Sie müssen diesen neuen Schlüssel in der sogenannten MOK-Liste (Machine Owner Key) registrieren, indem Sie die Maschine neu starten. Ohne die Registrierung des neuen Schlüssels wird Ihr Agent nicht funktionsfähig sein. Wenn Sie die UEFI Secure Boot-Funktion nach der Installation des Agenten aktivieren, müssen Sie den Agenten neu installieren.

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 (üblichweise englischen) Befehl **Enroll MOK** und registrieren Sie dann den Schlüssel mit dem im vorherigen Schritt empfohlenen Kennwort.
   - Anderenfalls können Sie auf **Beenden** klicken.

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

## Installation unter macOS

***So können Sie den Agenten für Mac installieren***

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 doppelt auf **Installieren** und dann einzeln auf **Fortsetzen**.
4. [Optional] Klicken Sie auf **Installationsspeicherort ändern**, um das Laufwerk zu ändern, auf dem die Software installiert wird. Standardmäßig ist das Laufwerk vorausgewählt, von dem das System gestartet wird.
5. Klicken Sie auf **Installieren**. Geben Sie bei Aufforderung die Anmeldedaten (Benutzername, Kennwort) des Administrators ein.
6. Spezifizieren Sie den Management Server, auf dem die Maschine mit dem Agenten registriert werden soll:
   a. Spezifizieren Sie den Host-Namen oder die IP-Adresse derjenigen Maschine, auf welcher der Management Server installiert ist.
   b. Spezifizieren Sie den Benutzernamen und das Kennwort eines Management Server-Administrators.
   c. Klicken Sie auf **Registrieren**.
7. Bestimmen Sie bei Aufforderung, ob die Maschine mit dem Agenten dem Unternehmen oder einer der Abteilungen hinzugefügt werden soll, und klicken Sie dann auf **Fertig**.
   Diese Eingabeaufforderung erscheint, wenn das im vorherigen Schritt spezifizierte Konto mehr als eine Abteilung oder ein Unternehmen mit mindestens einer Abteilung verwaltet.
8. Klicken Sie nach Abschluss der Installation auf **Schließen**.

# Unbeaufsichtigte Installation oder Deinstallation

## Unbeaufsichtigte Installation oder Deinstallation unter Windows

Dieser Abschnitt beschreibt, wie Sie Acronis Cyber Protect 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. 186)'.

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. [Nicht in allen Setup-Programmen verfügbar] Wählen Sie bei **Bit-Anzahl der Komponenten** entweder **32 Bit** oder **64 Bit**.
4. Wählen Sie bei **Zu installierende Komponenten** diejenigen Komponenten, die Sie aufspielen wollen, und klicken Sie dann auf **Fertig**.
   Die Installationspakete für diese Komponenten werden vom Setup-Programm extrahiert.
5. Wählen Sie bei **Acronis Cyber Protect Management Server** entweder **Anmeldedaten verwenden** oder **Registrierungstoken verwenden**. Spezifizieren Sie je nach Ihrer Wahl die Anmeldedaten oder das Registrierungstoken und klicken Sie dann auf **Fertig**.
   Weitere Informationen über die Generierung eines Registrierungstokens finden Sie im Abschnitt '"Schritt 1: Ein Registrierungstoken generieren" (S. 187)'.
6. [Nur, wenn Sie eine Installation auf einem Domain Controller durchführen] Wählen Sie bei **Anmeldekonto für den Agenten-Dienst** die Option **Folgendes Konto verwenden**. Spezifizieren Sie das Benutzerkonto, unter dem der Agenten-Dienst ausgeführt werden soll, und klicken Sie dann auf **Fertig**. Das Setup-Programm erstellt aus Sicherheitsgründen nicht automatisch neue Konten auf einem Domain Controller.

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

   Weitere Informationen zur Installation des Agenten auf einem schreibgeschützten Domain Controller (RODC, Read-only Domain Controller) finden Sie in diesem Knowledge Base-Artikel.
7. Überprüfen oder ändern Sie andere Installationseinstellungen, die der .mst-Datei hinzugefügt werden, und klicken Sie dann auf **Fortsetzen**.

8. Wählen Sie dann den Ordner aus, wo die .mst-Transform-Datei generiert wird und die .msi- und .cab-Installationspakete extrahiert werden, und klicken Sie dann auf **Generieren**.

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

### Das Produkt mithilfe der .mst-Transform-Datei installieren

Führen Sie in der Kommandozeile den nachfolgenden Befehl aus:

```
msiexec /i <package name> TRANSFORMS=<transform name>
```

Dabei ist:

- `<Paket-Name>` der Name der .msi-Datei ist. Als Name wird **AB.msi** oder **AB64.msi** verwendet (abhängig von der Bit-Tiefe des Betriebssystem)
- `<Transform-Name>` die Bezeichnung der Transform-Datei ist. Als Name wird **AB.msi.mst** oder **AB64.msi.mst** verwendet (abhängig von der Bit-Tiefe des Betriebssystem)

Beispiel: `msiexec /i AB64.msi TRANSFORMS=AB64.msi.mst`

### Das Produkt durch manuelle Spezifikation der Parameter installieren oder deinstallieren

Führen Sie in der Kommandozeile den nachfolgenden Befehl aus:

```
msiexec /i <package name><PARAMETER 1>=<value 1> ... <PARAMETER N>=<value n>
```

Wobei `<Paket-Name>` der Name der .msi-Datei ist. Als Name wird **AB.msi** oder **AB64.msi** verwendet (abhängig von der Bit-Tiefe des Betriebssystem)

Die verfügbaren Parameter und ihre Werte sind unter '"Allgemeine Parameter" (S. 116)' beschrieben.

**Beispiele**

- Den Management Server und die Komponenten zur Remote-Installation installieren.

  ```
  msiexec.exe /i ab64.msi /l*v my_log.txt /qn
  ADDLOCAL=AcronisCentralizedManagementServer,WebConsole,ComponentRegisterFeature
  TARGETDIR="C:\Program Files\Acronis" REBOOT=ReallySuppress CURRENT_LANGUAGE=en ACEP_
  AGREEMENT=1 AMS_USE_SYSTEM_ACCOUNT=1
  ```

- Den Agent für Windows, das Befehlszeilenwerkzeug und den Cyber Protect Monitor installieren. Die Maschine mit dem Agenten auf einem zuvor installierten Management Server registrieren.

  ```
  msiexec.exe /i ab64.msi /l*v my_log.txt /qn
  ADDLOCAL=AgentsCoreComponents,BackupAndRecoveryAgent,CommandLineTool,TrayMonitor
  TARGETDIR="C:\Program Files\Acronis" REBOOT=ReallySuppress CURRENT_LANGUAGE=en ACEP_
  AGREEMENT=1 MMS_CREATE_NEW_ACCOUNT=1 REGISTRATION_ADDRESS=10.10.1.1
  ```

- Den Management Server, den Storage Node, den Katalogdienst und den Protection Agenten aktualisieren.

```
msiexec.exe /i ab64.msi /l*v my_log.txt /qn
ADDLOCAL=AcronisCentralizedManagementServer,BackupAndRecoveryAgent,AgentsCoreComponen
ts,StorageServer,CatalogBrowser CATALOG_DATA_MIGRATION_PATH="C:\MyFolder\tmp"
```

### 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

## Allgemeine Parameter

`ADDLOCAL=<list of components>`

Die zu installierenden Komponenten, durch Kommata (ohne Leerzeichen) getrennt. 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 |
|---|---|---|---|
| AcronisCentralizedManagementServer | WebConsole | 32 Bit/64 Bit | Management Server |
| WebConsole | AcronisCentralizedManagementServer | 32 Bit/64 Bit | Web Console |
| ComponentRegisterFeature | AcronisCentralizedManagementServer | 32 Bit/64 Bit | Komponenten zur Remote-Installation |
| AtpScanService | AcronisCentralizedManagementServer | 32 Bit/64 Bit | Scan Service |
| AgentsCoreComponents | | 32 Bit/64 | Kernkomponenten für Agenten |

| | | | |
|---|---|---|---|
| | | Bit | |
| BackupAndRecoveryAgent | AgentsCoreComponents | 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 |
| OracleAgentFeature | BackupAndRecoveryAgent | 32 Bit/64 Bit | Agent für Oracle |
| ArxOnlineAgentFeature | AgentsCoreComponents | 32 Bit/64 Bit | Agent für Office 365 |
| AcronisESXSupport | AgentsCoreComponents | 32 Bit/64 Bit | Agent für VMware (Windows) |
| HyperVAgent | AgentsCoreComponents | 32 Bit/64 Bit | Agent für Hyper-V |
| ESXVirtualAppliance | | 32 Bit/64 Bit | Agent für VMware (Virtuelle Appliance) |
| ScaleVirtualAppliance | | 32 Bit/64 Bit | Agent für Scale Computing HC3 (Virtuelle Appliance) |
| CommandLineTool | | 32 Bit/64 Bit | Befehlszeilenwerkzeug |
| TrayMonitor | BackupAndRecoveryAgent | 32 | Cyber Protect Monitor |

| | | | |
|---|---|---|---|
| | | Bit/64 Bit | |
| BackupAndRecoveryBootableComponents | | 32 Bit/64 Bit | Bootable Media Builder |
| PXEServer | | 32 Bit/64 Bit | PXE Server |
| StorageServer | BackupAndRecoveryAgent | 64 Bit | Storage Node |
| CatalogBrowser | JRE 8 Update 111 oder höher | 64 Bit | Katalogdienst |

`TARGETDIR=<Pfad>`

Der Ordner, wo das Produkt installiert werden soll.

`REBOOT=ReallySuppress`

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

`CURRENT_LANGUAGE=<Sprach-ID>`

Die Sprache für das Produkt. Die verfügbaren Werte sind: `en`, `en_GB`, `cs`, `da`, `de`, `es_ES`, `fr`, `ko`, `it`, `hu`, `nl`, `ja`, `pl`, `pt`, `pt_BR`, `ru`, `tr`, `zh`, `zh_TW`.

`ACEP_AGREEMENT={0,1}`

Lautet der Wert `1`, dann wird die Maschine am 'Acronis Programm zur Kundenzufriedenheit (ACEP)' teilnehmen.

`REGISTRATION_ADDRESS=<Host-Name oder IP-Adresse>:<Port>`

Der Host-Name oder die IP-Adresse derjenigen Maschine, auf welcher der Management Server installiert ist. Die Agenten, der Storage Node und der Katalogdienst, die im Parameter `ADDLOCAL` spezifiziert sind, werden auf dem Management Server registriert. Die Port-Nummer ist zwingend erforderlich, wenn diese nicht dem Standardwert (9877) entspricht.

Zusammen mit diesem Parameter müssen Sie entweder den Parameter `REGISTRATION_TOKEN` oder die Parameter `REGISTRATION_LOGIN` und `REGISTRATION_PASSWORD` spezifizieren.

`REGISTRATION_TOKEN=<Token>`

Das Registrierungstoken, welches in der Cyber Protect Webkonsole generiert wurde (wie im Abschnitt 'Agenten per Gruppenrichtlinie bereitstellen' beschrieben).

`REGISTRATION_LOGIN=<Benutzername>`, `REGISTRATION_PASSWORD=<Kennwort>`

Der Benutzername und das Kennwort eines Management Servers-Administrators.

`REGISTRATION_TENANT=<Abteilungs-ID>`

Die Abteilung innerhalb der Organisation (dem Unternehmen). Die Agenten, der Storage Node und der Katalogdienst, die im Parameter `ADDLOCAL` spezifiziert sind, werden dieser Abteilung hinzugefügt.

Wenn Sie die Abteilungs-ID ermitteln wollen, klicken Sie in der Cyber Protect Webkonsole auf **Einstellungen** –> **Konten**, wählen Sie die gewünschte Abteilung aus und klicken Sie dann auf **Details**.

Dieser Parameter funktioniert nicht ohne `REGISTRATION_TOKEN` oder alternativ `REGISTRATION_LOGIN` sowie `REGISTRATION_PASSWORD`. In diesem Fall werden die Komponenten der Organisation hinzugefügt.

Ohne diesen Parameter werden die Komponenten der Organisation hinzugefügt.

```
REGISTRATION_REQUIRED={0,1}
```

Das Installationergebnis, wenn die Registrierung fehlschlägt. Wenn der Wert `1` beträgt, wird die Installation fehlschlagen. Wenn der Wert `0` beträgt, wird die Installation erfolgreich abgeschlossen, obwohl die Komponente nicht registriert wurde.

```
REGISTRATION_CA_SYSTEM={0,1}|REGISTRATION_CA_BUNDLE={0,1}|REGISTRATION_PINNED_PUBLIC_KEY=<Public-Key-Wert>
```

Diese sich gegenseitig ausschließenden Parameter definieren, wie die Zertifikatsüberprüfung des Management Servers während der Registrierung erfolgen soll. Überprüfen Sie das Zertifikat, wenn Sie die Authentizität des Management Server verifizieren wollen, um Man-in-the-Middle-Angriffe (MITM) zu verhindern.

Wenn der Wert `1` beträgt, wird zur Verifizierung die System-CA verwendet oder das mit dem Produkt mitgelieferte CA-Bundle. Wenn ein Pinned Public Key spezifiziert wird, wird die Verifizierung diesen Schlüssel verwenden. Wenn der Wert `0` beträgt oder die Parameter nicht spezifiziert wurden, wird die Zertifikatsverifikation nicht durchgeführt. Der Registrierungsdatenverkehr wird jedoch weiterhin verschlüsselt.

```
/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.

## Installationsparameter für den Management Server

```
WEB_SERVER_PORT=<Port-Nummer>
```

Der Port, den der Webbrowser verwenden soll, um auf den Management Server zuzugreifen. Der Standardwert ist 9877.

```
AMS_ZMQ_PORT=<Port-Nummer>
```

Der Port, der zur Kommunikation zwischen den Produktkomponenten verwendet werden soll. Der Standardwert ist 7780.

`SQL_INSTANCE=<Instanz>`

Die Datenbank, die der Management Server verwenden soll. Sie können jede Edition von Microsoft SQL Server 2012, Microsoft SQL Server 2014 oder Microsoft SQL Server 2016 wählen. Die von Ihnen gewählte Instanz kann auch von anderen Programmen noch verwendet werden.

Ohne diesen Parameter wird die integrierte SQLite-Datenbank verwendet.

`SQL_USER_NAME=<Benutzername>` und `SQL_PASSWORD=<Kennwort>`

Die Anmeldedaten eines Microsoft SQL Server-Anmeldekontos. Der Management Server wird mithilfe dieser Anmeldedaten mit der ausgewählten SQL Server-Instanz verbinden. Ohne diese Parameter wird der Management Server die Anmeldedaten des Management Server-Dienstkontos (**AMS User**) verwenden.

**Das Konto, unter dem der Dienst des Management Servers ausgeführt wird**

Spezifizieren Sie einen der folgenden Parameter:

- `AMS_USE_SYSTEM_ACCOUNT={0,1}`
  Wenn der Wert `1` beträgt, wird das Systemkonto verwendet.
- `AMS_CREATE_NEW_ACCOUNT={0,1}`
  Wenn der Wert `1` beträgt, wird ein neues Konto erstellt.
- `AMS_SERVICE_USERNAME=<Benutzername>` und `AMS_SERVICE_PASSWORD=<Kennwort>`
  Das spezifizierte Konto wird verwendet.

## Installationsparameter für den Agenten

`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.

`SET_ESX_SERVER={0,1}`

Wenn der Wert `0` beträgt, wird der zu installierende Agent für VMware nicht mit einem vCenter Server oder ESXi-Host verbunden. Gehen Sie nach der Installation wie im Abschnitt 'Einen bereits registrierten Agenten für VMware konfigurieren' beschrieben vor.

Wenn der Wert `1` beträgt, spezifizieren Sie folgende Parameter:

`ESX_HOST=<Host-Name oder IP-Adresse>`

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.

**Das Konto, unter dem der Dienst des Agenten ausgeführt wird**

Spezifizieren Sie einen der folgenden Parameter:

- `MMS_USE_SYSTEM_ACCOUNT={0,1}`
  Wenn der Wert `1` beträgt, wird das Systemkonto verwendet.
- `MMS_CREATE_NEW_ACCOUNT={0,1}`
  Wenn der Wert `1` beträgt, wird ein neues Konto erstellt.
- `MMS_SERVICE_USERNAME=<Benutzername>` und `MMS_SERVICE_PASSWORD=<Kennwort>`
  Das spezifizierte Konto wird verwendet.

## Installationsparameter für den Storage Node

**Das Konto, unter dem der Dienst des Storage Nodes ausgeführt wird**

Spezifizieren Sie einen der folgenden Parameter:

- `ASN_USE_SYSTEM_ACCOUNT={0,1}`
  Wenn der Wert `1` beträgt, wird das Systemkonto verwendet.
- `ASN_CREATE_NEW_ACCOUNT={0,1}`
  Wenn der Wert `1` beträgt, wird ein neues Konto erstellt.
- `ASN_SERVICE_USERNAME=<Benutzername>` und `ASN_SERVICE_PASSWORD=<Kennwort>`
  Das spezifizierte Konto wird verwendet.

## Katalogdienst-Installationsparameter

`CATALOG_DATA_MIGRATION_PATH=<path>`

Verwenden Sie diesen Parameter, um die Katalogdaten auf die neue Version des Katalogdienstes in Acronis Cyber Protect 15 Update 4 zu migrieren. Spezifizieren Sie den Pfad zu dem temporären Ordner, wohin die Katalogdaten exportiert werden sollen.

`SKIP_CATALOG_DATA_MIGRATION=1`

Verwenden Sie diesen Parameter, um die Migration der Katalogdaten zu überspringen.

Die Parameter `SKIP_CATALOG_DATA_MIGRATION` und `CATALOG_DATA_MIGRATION_PATH` schließen sich gegenseitig aus.

### Deinstallationsparameter

`REMOVE={<list of components>|ALL}`

Die zu entfernenden Komponenten, durch Kommata (ohne Leerzeichen) getrennt.

Die verfügbaren Komponenten sind weiter oben in diesem Abschnitt beschrieben.

Wenn der Wert `ALL` beträgt, werden alle Produkt-Komponenten deinstalliert. Sie können zusätzlich noch folgende Parameter spezifizieren:

`DELETE_ALL_SETTINGS={0, 1}`

Wenn der Wert `1` beträgt, werden auch die Protokolle (Logs), Tasks und Konfigurationseinstellungen des Produkts entfernt.

## Unbeaufsichtigte Installation oder Deinstallation unter Linux

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

***So können Sie das Produkt installieren oder deinstallieren***

1. Öffnen Sie die Applikation 'Terminal'.
2. Führen Sie folgenden Befehl aus:

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

   Wobei `<Paket-Name>` die Bezeichnung der Installationspakete ist (eine .i686- oder .x86_64-Datei).
3. [Nur bei Installation des Agenten für Linux] 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.

### Installationsparameter

#### Allgemeine Parameter

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

Die zu installierenden Komponenten, durch Kommata (ohne Leerzeichen) getrennt.

Folgende Komponenten sind für eine Installation verfügbar:

| Komponente | Komponenten-Beschreibung |
|---|---|
| AcronisCentralizedManagementServer | Management Server |
| BackupAndRecoveryAgent | Agent für Linux |
| BackupAndRecoveryBootableComponents | Bootable Media Builder |

Ohne diesen Parameter werden alle oberen Komponenten installiert.

`--language=<Sprach-ID>`

Die Sprache für das Produkt. Die verfügbaren Werte sind: `en`, `en_GB`, `cs`, `da`, `de`, `es_ES`, `fr`, `ko`, `it`, `hu`, `nl`, `ja`, `pl`, `pt`, `pt_BR`, `ru`, `tr`, `zh`, `zh_TW`.

`{-d|--debug}`

Wird der Parameter spezifiziert, dann wird das Installationsprotokoll (Log) im ausführlichen Modus (Verbose-Modus) geschrieben. Das Protokoll befindet sich in der Datei '**/var/log/trueimage-setup.log**'.

`{-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}`

Wird der Parameter spezifiziert, dann wird das Fehlen von erforderlichen Linux-Paketen während der Installation ignoriert.

### Installationsparameter für den Management Server

`{-W |--web-server-port=}<Port-Nummer>`

Der Port, den der Webbrowser verwenden soll, um auf den Management Server zuzugreifen. Der Standardwert ist 9877.

`--ams-tcp-port=<Port-Nummer>`

Der Port, der zur Kommunikation zwischen den Produktkomponenten verwendet werden soll. Der Standardwert ist 7780.

### Installationsparameter für den Agenten

Spezifizieren Sie einen der folgenden Parameter:

- `--skip-registration`
  - Der Agent wird nicht auf dem Management Server registriert.
- `{-C |--ams=}<Host-Name oder IP-Adresse>`
  - Der Host-Name oder die IP-Adresse derjenigen Maschine, auf welcher der Management Server installiert ist. Der Agent wird auf diesem Management Server registriert.

    Wenn Sie den Agenten und den Management Server mit einem Befehl installieren, wird der Agent auf diesem Management Server unabhängig vom Parameter `-C` registriert.

    Sie müssen zusammen mit diesem Parameter entweder den Parameter `token` oder die Parameter `login` und `password` spezifizieren.

    `--token=<Token>`

Das Registrierungstoken, welches in der Cyber Protect Webkonsole generiert wurde (wie im Abschnitt 'Agenten per Gruppenrichtlinie bereitstellen' beschrieben).

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

Die Anmeldedaten eines Management Server-Administrators.

`--unit=<Abteilungs-ID>`

Die Abteilung innerhalb der Organisation (dem Unternehmen). Der Agent wird dieser Abteilung hinzugefügt.

Wenn Sie die Abteilungs-ID ermitteln wollen, klicken Sie in der Cyber Protect Webkonsole auf **Einstellungen** –> **Konten**, wählen Sie die gewünschte Abteilung aus und klicken Sie dann auf **Details**.

Ohne diesen Parameter wird der Agent der Organisation (dem Unternemen) hinzugefügt.

`--reg-transport={https|https-ca-system|https-ca-bundle|https-pinned-public-key}`

Die Methode, wie die Zertifikatsüberprüfung des Management Servers während der Registrierung erfolgen soll. Überprüfen Sie das Zertifikat, wenn Sie die Authentizität des Management Server verifizieren wollen, um Man-in-the-Middle-Angriffe (MITM) zu verhindern.

Wenn der Wert `https` lautet oder der Parameter nicht spezifiziert wurde, wird die Zertifikatsverifikation nicht durchgeführt. Der Registrierungsdatenverkehr wird jedoch weiterhin verschlüsselt. Wenn der Wert *nicht* `https` lautet, wird zur Verifizierung die System-CA verwendet oder das mit dem Produkt mitgelieferte CA-Bundle oder der Pinned Public Key.

`--reg-transport-pinned-public-key=<Public-Key-Wert>`

Der Wert des Pinned Public Keys. Dieser Parameter sollte zusammen mit oder anstelle des Parameters `--reg-transport=https-pinned-public-key` spezifiziert werden.

- `--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.
- `--no-proxy-to-ams`
  - Der Protection Agent wird eine Verbindung zum Management Server herstellen, ohne den Proxy-Server zu verwenden, der durch die Parameter `--http-proxy-host` und `--http-proxy-port` spezifiziert wird.

## Deinstallationsparameter

`{-u|--uninstall}`

Das Produkt wird deinstalliert.

`--purge`

Die Protokolle (Logs), Tasks und Konfigurationseinstellungen des Produkts werden entfernt.

### 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.

### Beispiele

- Den Management Server installieren.

```
./AcronisCyberProtect_15_64-bit.x86_64 -a -i AcronisCentralizedManagementServer
```

- Den Management Server installieren, benutzerdefinierbare Ports spezifizieren.

```
./AcronisCyberProtect_15_64-bit.x86_64 -a -i AcronisCentralizedManagementServer --
web-server-port 6543 --ams-tcp-port 8123
```

- Den Agenten für Linux installieren und ihn auf dem spezifizierten Management Server registrieren.

```
./AcronisCyberProtect_15_64-bit.x86_64 -a -i BackupAndRecoveryAgent --ams 10.10.1.1 -
-login root --password 123456
```

- Den Agenten für Linux installieren und ihn auf dem spezifizierten Management Server und in der spezifizierten Abteilung registrieren.

```
./AcronisCyberProtect_15_64-bit.x86_64 -a -i BackupAndRecoveryAgent --ams 10.10.1.1 -
-login root --password 123456 -unit 01234567-89AB-CDEF-0123-456789ABCDEF
```

## Unbeaufsichtigte Installation oder Deinstallation unter macOS

Dieser Abschnitt beschreibt, wie Sie den Protection Agenten auf einer unter macOS laufenden Maschine und mithilfe der Befehlszeile im unbeaufsichtigten Modus installieren, registrieren und deinstallieren können. 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 der Platzhalter `<dmg_root>` für einen Name Ihrer Wahl steht.
2. Mounten Sie die .dmg-Datei.

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

   Wobei der Platzhalter `<dmg_file>` für den Name der Installationsdatei steht. Beispiel: **AcronisCyberProtect_15_MAC.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/AcronisCyberProtect_15_MAC.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 unter einem bestimmten Administratorkonto.

  ```
  sudo /Library/Application\
  Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -o register -a
  <management server address:port> -u <user name> -p <password>
  ```

  Der Parameter `<management server address:port>` steht für den Host-Namen oder die IP-Adresse der Maschine, auf welcher der Acronis Cyber Protect Management Server installiert ist. Die Port-Nummer ist zwingend erforderlich, wenn diese nicht dem Standardwert (9877) entspricht.

  Die Parameter `<user name>` und `<password>` stehen für die Anmeldedaten des Administratorkontos, unter dem der Agent registriert werden soll.
- Registrieren Sie den Agenten in einer bestimmten Abteilung.
  ```

```
sudo /Library/Application\
Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent  -o register -a
<management server address:port> -u <user name> -p <password> --tenant <unit ID>
```

Wenn Sie die Abteilungs-ID ermitteln wollen, klicken Sie in der Cyber Protect Webkonsole auf **Einstellungen** –> **Konten**, wählen Sie die gewünschte Abteilung aus und klicken Sie dann auf **Details**.

**Wichtig**
Administratoren können Agenten durch Spezifizierung der Abteilungs-ID nur auf ihrer Ebene der Organisationshierarchie registrieren. Abteilungsadministratoren können Maschinen in ihren eigenen Abteilungen und deren Unterabteilungen registrieren. Organisationsadministratoren können Maschinen in allen Abteilungen registrieren. Weitere Informationen über die verschiedenen Administratorkonten finden Sie im Abschnitt 'Benutzerkonten und Organisationseinheiten (Abteilungen) verwalten'.

- Registrieren Sie den Agenten mit einem Registrierungstoken.

```
sudo /Library/Application\
Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -o register -a
<management server address:port> --token <token>
```

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

**Wichtig**
Bei macOS 10.14 oder höher 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.

## Beispiele

Registrierung mit einem Benutzernamen und Kennwort.

- 
```
sudo /Library/Application\
Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -o register -a
https://10.250.144.179:9877 -u johndoe -p johnspassword
```

Registrierung mit einer Abteilungs-ID und Administrator-Anmeldedaten.

- 
```
sudo /Library/Application\
Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -o register -a
https://10.250.144.179:9877 -u johndoe -p johnspassword --tenant 4dd941c1-c03f-11ea-
86d8-005056bdd3a0
```

Registrierung mit einem Token.

- ```
  sudo /Library/Application\
  Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -o register -a
  https://10.250.144.179:9877 --token D91D-DC46-4F0B
  ```

***So können Sie den Agenten für Mac deinstallieren***

Führen Sie folgenden Befehl aus:

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

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

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

## Maschinen manuell registrieren

Neben der Möglichkeit, eine Maschine direkt während der Agenten-Installation auf dem Cyber Protect Management Server 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 in der Eingabeaufforderung der Maschine, auf welcher der Agent installiert ist, einen der folgenden Befehle aus:

- So können Sie die Maschine unter einem bestimmten Administratorkonto registrieren:

  ```
  <path to the registration tool> -o register -a <management server address:port> -u
  <user name> -p <password>
  ```

  Wobei `&lt;Pfad zum Registrierungstool&gt;` folgendes Verzeichnis ist:
  - unter Windows: `%ProgramFiles%\Acronis\RegisterAgentTool\register_agent.exe`
  - unter Linux: `/usr/lib/Acronis/RegisterAgentTool/RegisterAgent`
  - unter macOS: `/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent`

  `&lt;Management Server-Adresse:Port&gt;` steht für den Host-Namen oder die IP-Adresse der Maschine, auf welcher der Acronis Cyber Protect Management Server installiert ist. Wenn Sie den Standard-Port 9877 verwenden, müssen Sie diesen nicht explizit spezifizieren.

  Die Parameter `&lt;user name&gt;` und `&lt;password&gt;` stehen für die Anmeldedaten des Administratorkontos, unter dem der Agent registriert werden soll.
  ```

- Wenn Sie die Maschine in einer bestimmten Abteilung registrieren wollen, müssen Sie die ID der Abteilung angeben:

  ```
  <path to the registration tool> -o register -a <management server address:port> u
  <user name> -p <password> --tenant <unit ID>
  ```

  Wenn Sie die Abteilungs-ID ermitteln wollen, klicken Sie in der Cyber Protect Webkonsole auf **Einstellungen** –> **Konten**, wählen Sie die gewünschte Abteilung aus und klicken Sie dann auf **Details**.

  **Wichtig**
  Administratoren können Agenten nur auf ihrer Ebene der Organisationshierarchie registrieren. Abteilungsadministratoren können Agenten in ihren eigenen Abteilungen und deren Unterabteilungen registrieren. Organisationsadministratoren können Agenten in allen Abteilungen registrieren. Weitere Informationen über die verschiedenen Administratorkonten finden Sie im Abschnitt 'Benutzerkonten und Organisationseinheiten (Abteilungen) verwalten'.

- So können Sie die Maschine mithilfe eines Registrierungstokens registrieren:

  ```
  <path to the registration tool> -o register -a <management server address:port> --
  token <token>
  ```

  - 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'.

***So können Sie die Registrierung einer Maschine aufheben***

Führen Sie in der Eingabeaufforderung der Maschine, auf welcher der Agent installiert ist, folgenden Befehl aus:

```
<path to the registration tool> -o unregister
```

## Beispiele

### Windows

```
"%ProgramFiles%\Acronis\RegisterAgentTool\register_agent.exe" -o register -a
https://10.250.144.179:9877 -u johndoe -p johnspassword
```

```
"%ProgramFiles%\Acronis\RegisterAgentTool\register_agent.exe" -o register -a
https://10.250.144.179:9877 --tenant 590b1dd7-8adb-11ea-bf44-0050569deecf
```

```
"%ProgramFiles%\Acronis\RegisterAgentTool\register_agent.exe" -o register -a
https://10.250.144.179:9877 -u johndoe -p johnspassword --tenant 590b1dd7-8adb-11ea-
bf44-0050569deecf
```

```
"%ProgramFiles%\Acronis\RegisterAgentTool\register_agent.exe" -o register -a
https://10.250.144.179:9877 --token 3B4C-E967-4FBD
```

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

### Linux

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -a
https://10.250.144.179:9877 -u johndoe -p johnspassword
```

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -a
https://10.250.144.179:9877 --tenant 590b1dd7-8adb-11ea-bf44-0050569deecf
```

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -a
https://10.250.144.179:9877 -u johndoe -p johnspassword --tenant 590b1dd7-8adb-11ea-
bf44-0050569deecf
```

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -a
https://10.250.144.179:9877 --token 34F6-8C39-4A5C
```

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

### macOS

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent"
-o register -a https://10.250.144.179:9877 -u johndoe -p johnspassword
```

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -a
https://10.250.144.179:9877 --tenant 590b1dd7-8adb-11ea-bf44-0050569deecf
```

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -a
https://10.250.144.179:9877 -u johndoe -p johnspassword --tenant 590b1dd7-8adb-11ea-
bf44-0050569deecf
```

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent"
-o register -a https://10.250.144.179:9877 --token 9DBF-3DA9-4DAB
```

```
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:

```
<path to the registration tool> -o register -a <management server address:port> -u <user
name> -p <"password">
```

*Beispiel (für Windows):*

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -a
https://10.250.144.179:9877 -u johndoe -p "johns password"
```

Wenn Sie weiterhin eine Fehlermeldung erhalten:

1. Codieren Sie Ihr Kennwort im Base64-Format unter https://www.base64encode.org/.
2. Spezifizieren Sie das codierte Kennwort in der Befehlszeile unter Verwendung der Parameter -b oder --base64.

*Beispiel (für Windows):*

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -a
https://10.250.144.179:9877 -u johndoe -b -p am9obnNwYXNzd29yZA==
```

## Auf Software-Updates prüfen

Diese Funtionalität ist nur für Organisationsadministratoren verfügbar.

Acronis Cyber Protect prüft bei jeder Anmeldung an der Cyber Protect Webkonsole, ob auf der Acronis Website eine neue Version verfügbar ist. Wenn ja, wird in der Cyber Protect Webkonsole ein Download-Link auf die neue Version angezeigt – und zwar im unteren Seitenbereich auf den Registerkarten **Geräte**, **Pläne** und **Backup Storage**. Der Link ist außerdem auch auf den Seiten **Einstellungen** –> **Agenten** verfügbar.

Sie können die automatische Update-Überprüfung (de)aktivieren, indem Sie die Systemeinstellung **Updates**.

Über folgende Befehlskette können Sie auch manuell nach Updates suchen: Fragezeichensymbol (in der rechten oberen Ecke) –> **Über** –> **Auf Updates prüfen** oder Fragezeichensymbol –> **Auf Updates prüfen**.

## Migration des Management Servers

Sie können einen Management Server, der auf einer Windows-Maschine ausgeführt wird, zu einer anderen Windows-Maschine in derselben Umgebung migrieren.

Der Migrationsprozess besteht aus den folgenden Phasen:

1. "Aktionen auf der Quellmaschine" (S. 132)

   In dieser Phase bereiten Sie die Daten auf dem ursprünglichen Management Server für die Migration vor.
2. "Aktionen auf der Zielmaschine" (S. 133)

   In dieser Phase installieren und konfigurieren Sie einen neuen Management Server. Anschließend kopieren Sie die Daten vom ursprünglichen Management Server zum neuen Server.

## Voraussetzungen

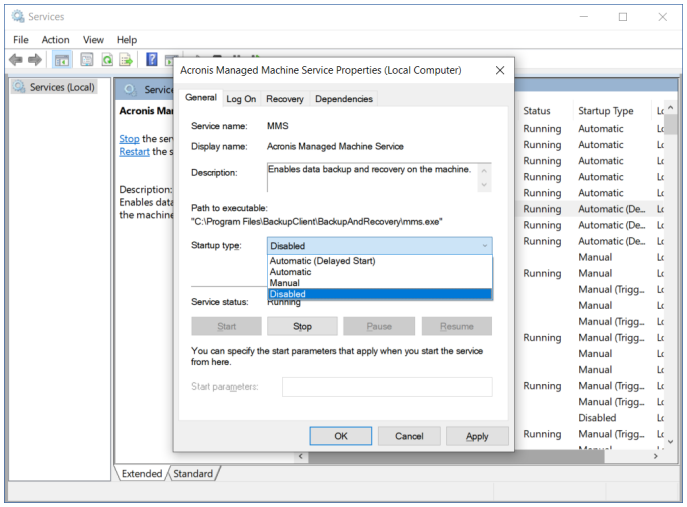
- Der Management Server verwendet eine externe Microsoft SQL Server-Datenbank. Die Microsoft SQL Server-Instanz wird auf einer dedizierten Maschine ausgeführt.
- Die Protection Agenten werden auf dem Management Server mit ihrem Host-Namen (und nicht mit ihrer IP-Adresse) registriert.
- Die Version des Management Servers ist Acronis Cyber Protect Update 4 (Build 29486) oder höher.
- Auf der Quell- und der Zielmaschine wird die gleiche Version des Management Servers installiert.

## Aktionen auf der Quellmaschine

In dieser Phase bereiten Sie die Daten vom ursprünglichen Management Server für die Migration vor.

***So können Sie die Daten für die Migration vorbereiten***

1. Stoppen Sie alle Dienste von Acronis auf der ursprünglichen Management Server-Maschine.
   a. Öffnen Sie **Services** und deaktivieren Sie dann, dass die Dienste von Acronis gestartet werden. Ausgenommen davon sind der **Acronis Active Protection Service** und **Acronis Cyber Protection Service**.




   b. Öffnen Sie **Regedit** und deaktivieren Sie dann den **Acronis Active Protection Service** und **Acronis Cyber Protection Service**, indem Sie deren Schlüssel bearbeiten:

- Öffnen Sie im Schlüssel `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AcronisCyberProtectionService` den Wert **Start** und setzen Sie dann die Wertdaten auf 4.
- Öffnen Sie im Schlüssel `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AcronisActiveProtectionService` den Wert **Start** und setzen Sie dann die Wertdaten auf 4.

2. Starten Sie die Management Server-Maschine neu und überprüfen Sie dann, dass die deaktivierten Dienste von Acronis nicht mehr ausgeführt werden.

**Hinweis**
Zwei Dienste, nämlich **Acronis Scheduler Service Helper** und **Acronis TIB Mounter Monitor**, werden möglicherweise noch ausgeführt. Sie können diese bedenkenlos ignorieren.

3. [Wenn die Komponente Cyber Protect Monitor auf der Maschine des Management Servers installiert ist] Beenden Sie den Acronis Cyber Protect Monitor.
4. Ändern Sie in der Windows-Eingabeaufforderung den Besitzer der Ordner `%ProgramData%\Acronis` und `%ProgramFiles%\Acronis`, indem Sie folgende Befehle ausführen:

```
takeown /f "%ProgramData%\Acronis" /r /d y
```

```
takeown /f "%ProgramFiles%\Acronis" /r /d y
```

5. Bearbeiten Sie die Zugriffsrechte für diese Ordner und deren Unterordner, indem Sie folgende Befehle ausführen:

```
icacls "%ProgramData%\Acronis" /grant everyone:F /t
```

```
icacls "%ProgramFiles%\Acronis" /grant everyone:F /t
```

6. Kopieren Sie die Ordner `%ProgramData%\Acronis` und `%ProgramFiles%\Acronis` zu einer Netzwerkfreigabe, auf die auch die neue Management Server-Maschine zugreifen kann.
7. Fahren Sie die ursprüngliche Management Server-Maschine herunter.

Befolgen Sie als nächstes die Prozedur im Abschnitt '"Aktionen auf der Zielmaschine" (S. 133)'.

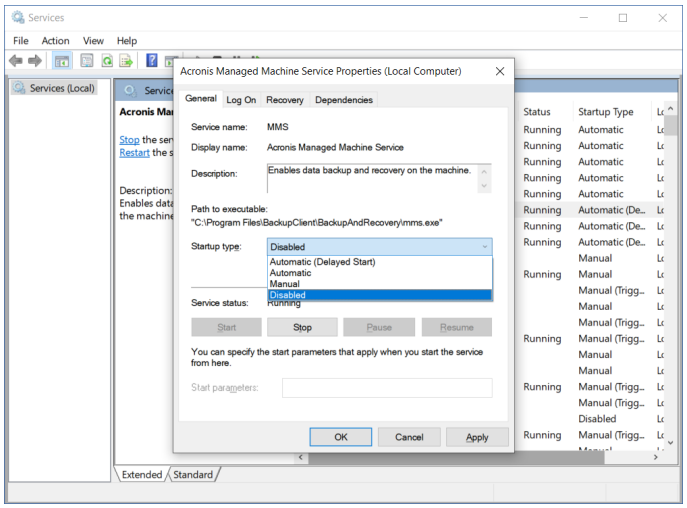
## Aktionen auf der Zielmaschine

In dieser Phase installieren und konfigurieren Sie einen neuen Management Server und migrieren dann die entsprechenden Daten zu diesem Server.

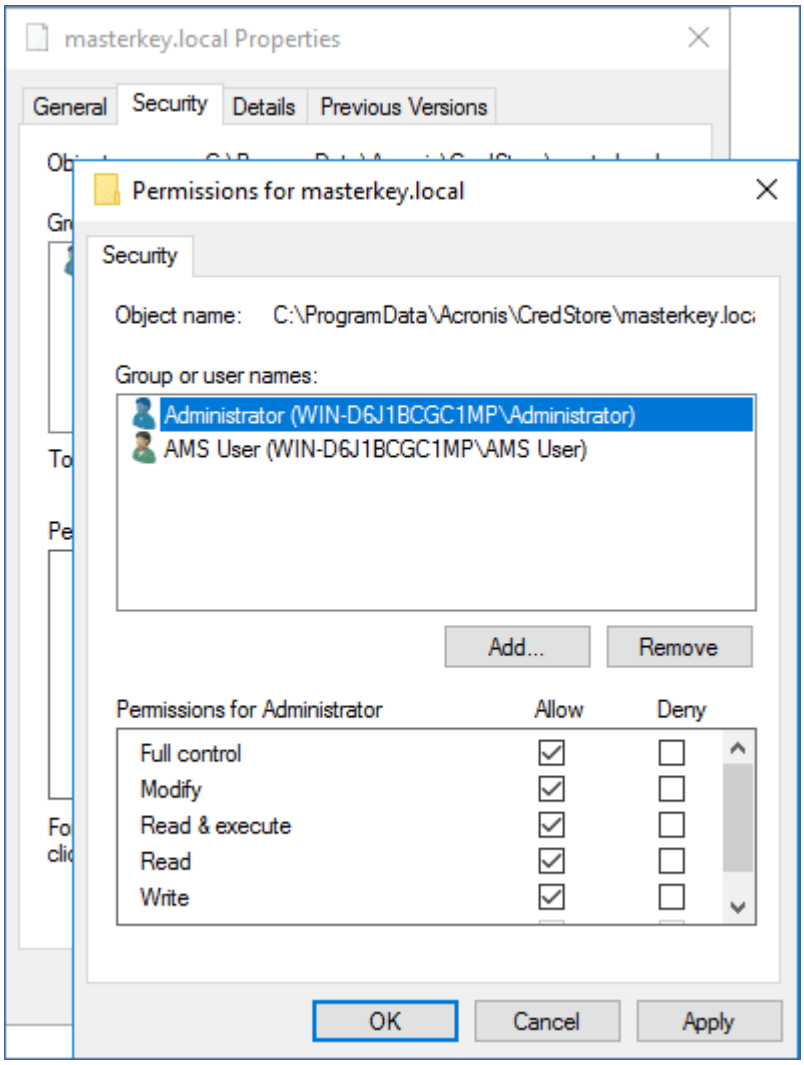
Bevor Sie die Aktionen auf der Maschine durchführen, sollten Sie sicherstellen, dass Sie die Prozedur im Abschnitt '"Aktionen auf der Quellmaschine" (S. 132)' abgeschlossen haben.

***So können Sie die Daten zum neuen Management Server migrieren***

1. Legen Sie den Host-Namen für die Maschine fest, auf der Sie den neuen Management Server installieren wollen. Der Namen dieser neuen Maschine muss mit dem Namen der Maschine übereinstimmen, auf der sich der ursprüngliche Management Server befindet.
2. Erstellen Sie eine Firewall-Regel, um den gesamten Datenverkehr über den TCP-Port 9877 zu blockieren.
3. Starten Sie das Setup-Programm von Acronis Cyber Protect.
   a. Akzeptieren Sie die Bedingungen der Lizenzvereinbarung sowie die Datenschutzerklärung und klicken Sie anschließend auf **Fertigstellen**.
   b. Klicken Sie auf **Installationseinstellungen anpassen**.
   c. Wählen Sie bei **Zu installierende Komponenten** nur die nachfolgenden Komponenten und klicken Sie dann auf **Fertig**.
      - Management Server
      - Komponenten zur Remote-Installation
      - Bootable Media Builder
      - Befehlszeilenwerkzeug
   d. Übernehmen Sie bei **Datenbank für den Management Server** die vorgegebene Option **Integriertes SQLite verwenden**.
   e. Verwenden Sie bei **Anmeldekonto für den Management Server-Dienst** die gleiche Option wie auf dem ursprünglichen Management Server.
4. Stoppen Sie alle Dienste von Acronis.
   a. Öffnen Sie **Services** und deaktivieren Sie für alle Dienste von Acronis, dass diese automatisch gestartet werden.




   b. Starten Sie die Maschine neu und überprüfen Sie dann, dass die deaktivierten Dienste von Acronis nicht mehr ausgeführt werden.
5. Gehen Sie zu `%ProgramData%\Acronis\CredStore` und passen Sie die Berechtigungen für die Datei `masterkey.local` folgendermaßen an:
   a. Gewähren Sie dem Benutzerkonto **Administrator** die Besitzrechte an der Datei.
   b. Gewähren Sie dem Benutzerkonto **Administrator** die Berechtigung **Vollzugriff**.




6. Gehen Sie zu `%ProgramData%\Acronis\AMS\AccessVault\config` und gewähren Sie dem Benutzerkonto **Administrator** für die nachfolgenden Dateien die Berechtigung **Vollzugriff**:
   - `%ProgramData%\Acronis\AMS\AccessVault\config\preferred`
   - `%ProgramData%\Acronis\AMS\AccessVault\config\preferred.json`
7. Ersetzen Sie die nachfolgenden Ordner durch die Ordner, die Sie von der ursprünglichen Management Server-Maschine zu einer Netzwerkfreigabe kopiert haben:
   - `%ProgramData%\Acronis`
   - `%ProgramFiles%\Acronis`

   **Wichtig**
   Überschreiben Sie die vorhandenen Ordner, ohne diese vorher zu löschen.

   **Hinweis**
   Wenn Sie eine Meldung sehen, dass der Ordner `%ProgramFiles%\Acronis\ShellExtentions` nicht ersetzt werden kann, können Sie diesen Ordner bedenkenlos überspringen.
8. Stellen Sie die Berechtigungen für folgende Dateien wieder her:

- `%ProgramData%\Acronis\CredStore\masterkey.local` – Entfernen Sie das Benutzerkonto **Administrator** aus der Liste der Benutzer mit Berechtigungen.
- `%ProgramData%\Acronis\AMS\AccessVault\config\preferred` – Gewähren Sie dem Benutzerkonto **Administrator** nur die Berechtigung **Lesen**.
- `%ProgramData%\Acronis\AMS\AccessVault\config\preferred.json` – Gewähren Sie dem Benutzerkonto **Administrator** nur die Berechtigung **Lesen**.

9. Erstellen Sie eine Verzeichnisverbindung für den Ordner `NGMP\latest`.
   - Gehen Sie in der Windows-Eingabeaufforderung zu `%ProgramData%\Acronis\NGMP` und löschen Sie dann den Ordner `latest`.

     ```
     cd %ProgramData%\Acronis\NGMP
     ```

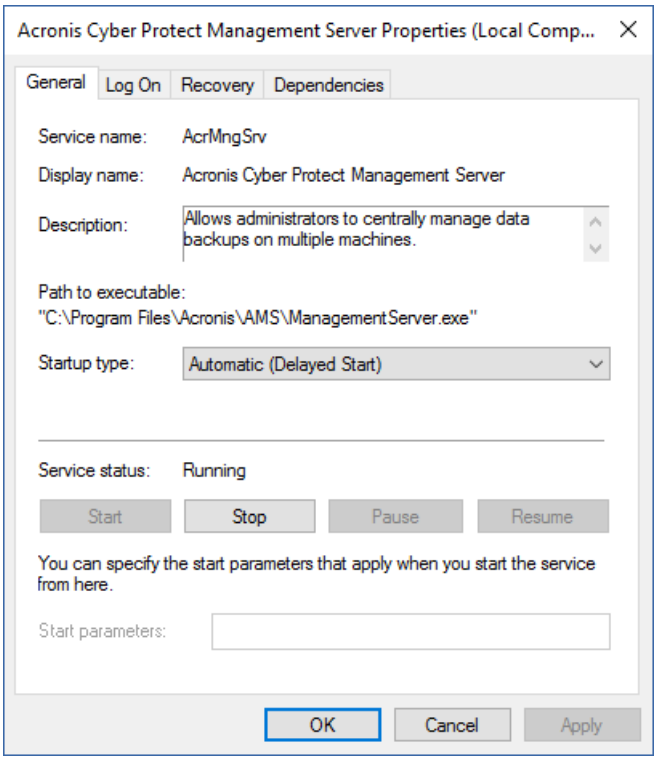
     ```
     rmdir latest
     ```

   - Erstellen Sie die Verzeichnisverbindung `latest` und verweisen Sie diese auf den Ordner, der nach der aktuellen NGMP-Version benannt ist. Beispielsweise:

     ```
     mklink /j latest C:\ProgramData\Acronis\NGMP\1.0.2653.0
     ```

10. Verweisen Sie den neuen Management Server auf die Microsoft SQL Server-Datenbank, die der ursprüngliche Management Server verwendet hat.
    a. Öffnen Sie **Regedit**.
    b. Ändern Sie im Schlüssel `HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\AMS\Settings` den Wert `AmsDmlDbProtocol`, indem Sie dessen Daten zu `config://C:\ProgramData\Acronis\AMS\mssql\dml_mssql.config` ändern.
11. Öffnen Sie **Services** und aktivieren Sie alle deaktivierten Dienste von Acronis.

    Legen Sie den Starttyp von **Acronis Cyber Protect Management Server** mit **Automatisch (Verzögerter Start)** fest – und den Starttyp für alle anderen Dienste von Acronis mit **Automatisch**.




12. Erlauben Sie in der Firewall den gesamten Datenverkehr über den TCP-Port 9877.
13. Starten Sie die Maschine neu und überprüfen Sie dann, dass alle Dienste von Acronis ausgeführt werden.
14. Führen Sie das Setup-Programm für Acronis Cyber Protect aus und installieren Sie folgende Elemente:
    - Agent für Windows
    - [Optional] Cyber Protect Monitor
15. Starten Sie die Maschine neu.

# Cloud-Bereitstellung

## 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. Merken Sie sich Ihren Anmeldenamen, der auf der Kontoaktivierungsseite angezeigt wird.
- **Ein Link zur Anmeldeseite der Cyber Protect Webkonsole.** Verwenden Sie diesen Link, um zukünftig auf die Konsole zuzugreifen. Die Anmeldedaten (Anmeldename, Kennwort) sind mit denen des vorherigen Schrittes identisch.

# Vorbereitung

## Schritt 1:

Wählen Sie den gewünschten Agenten aus – und zwar in Abhängigkeit davon, welche Art von Daten Sie sichern wollen. Informationen über die Agenten finden Sie im Abschnitt '"Komponenten" (S. 49)'.

## Schritt 2:

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

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

Falls Sie die Setup-Programme lokal speichern möchten, müssen Sie ein Paket herunterladen, welches alle Agenten zur Installation unter Windows enthält. Nutzen Sie dafür den Link im unteren Bereich der Seite '**Geräte hinzufügen**'. Es gibt sowohl 32-Bit- wie auch 64-Bit-Pakete. Mit diesem Paket können Sie festlegen, welche Komponenten installiert werden sollen. Diese Pakete ermöglichen Ihnen außerdem, eine unbeaufsichtigte Installation (beispielsweise per Gruppenrichtlinie) durchzuführen. Dieses erweiterte Szenario ist im Abschnitt '"Agenten per Gruppenrichtlinie bereitstellen" (S. 186)' beschrieben.

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

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

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

## Schritt 3:

Stellen Sie vor der Installation sicher, dass die Firewalls und anderen Komponenten Ihres Netzwerksicherheitssystems (z.B. ein Proxy-Server) eingehende und ausgehende Verbindungen über folgende TCP-Ports erlauben:

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

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

Die Agenten verwenden diese Ports, um mit dem Management Server zu kommunizieren.

- Die Ports **44445** und **55556**

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

Falls in Ihrem Netzwerk ein Proxy-Server aktiv ist, sollten Sie sich unter '"Proxy-Server-Einstellungen" (S. 140)' darüber informieren, ob und wann Sie diese Einstellungen für jede Maschine konfigurieren müssen, die einen Protection Agenten ausführt.

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

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

- Der Port **443**

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

- Der Port **902**

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

- Der Port **3333**

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

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

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

### Schritt 4:

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

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

**Hinweis**
Sie müssen diese nicht in der Firewall öffnen.

Der Active Protection Service überwacht den TCP-Port **6109**. Überprüfen Sie, dass er nicht von einem anderen Prozess verwendet wird.

#### Die vom Protection Agenten verwendeten Ports ändern

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

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

## 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. Gehen Sie alternativ 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
```

## 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">"ADDRESS"</value>
    <value name="Port" type="Tdword">"PORT"</value>
    <value name="Login" type="TString">"LOGIN"</value>
```

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

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

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. 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. Gehen Sie alternativ folgendermaßen vor, um den Agenten neu zu starten:
   a. Gehen Sie zu **Programme** –> **Dienstprogramme** –> **Terminal**
   b. Führen Sie folgende Befehle aus:

```
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.

## Installation der Agenten

### Unter 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:
   - Die zu installierenden Komponenten ändern (insbesondere, um die Installation des Cyber Protect Monitors und des Befehlszeilenwerkzeugs zu deaktivieren).
   - Die Methode ändern, mit der die Maschine im Cyber Protection Service registriert wird. Sie können von **Cyber Protect-Konsole verwenden** (Standard) auf **Anmeldedaten verwenden** oder **Registrierungstoken verwenden** umstellen.
   - Um den Installationspfad zu ändern.
   - Um das Konto für den Agenten-Dienst zu ändern.
   - 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 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.

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

   Weitere Informationen zur Installation des Agenten auf einem schreibgeschützten Domain Controller (RODC, Read-only Domain Controller) finden Sie in diesem Knowledge Base-Artikel.
7. Wenn Sie die Standardregistrierungsmethode **Cyber Protect-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 Cyber Protect Webkonsole 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.
9. **Hinweis**
   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 Cyber Protect Webkonsole verwendet wurde.

## 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**

   Der Agent für Virtuozzo kann nicht ohne den Agenten für Linux installiert werden.
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 Cyber Protect Webkonsole 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.

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

   Dadurch wird die Maschine dem Konto zugewiesen, welches zur Anmeldung an die Cyber Protect Webkonsole verwendet wurde.
7. Wenn im UEFI-BIOS der Maschine die Secure Boot-Funktion (kurz 'UEFI Secure Boot') aktiviert ist, werden Sie darüber informiert, dass Sie das System nach der Installation neu starten müssen. Denken Sie daran, welches Kennwort (das des root-Benutzers oder 'acronis') verwendet werden

soll.

**Hinweis**
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.

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

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

## 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 Cyber Protect Webkonsole 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.

10. **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 Cyber Protect Webkonsole verwendet wurde.

## Das Anmeldekonto auf Windows-Maschinen ändern

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

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

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

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

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

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

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

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

### Für das Anmeldekonto erforderliche Berechtigungen

Ein Protection Agent wird auf einer Windows-Maschine als Managed Machine Service (MMS) ausgeführt. Das Konto, unter dem der Agent ausgeführt wird, muss spezifische Rechte haben, damit

der Agent korrekt funktioniert. Daher sollten dem MMS-Benutzer folgende Berechtigungen zugewiesen werden:

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

### So können Sie die Benutzerrechte zuweisen

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

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

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

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

# Unbeaufsichtigte Installation oder Deinstallation

## 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. 186)'.

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. Wählen Sie bei **Zu installierende Komponenten** diejenigen Komponenten, die Sie aufspielen wollen, und klicken Sie dann auf **Fertig**.
   Die Installationspakete für diese Komponenten werden vom Setup-Programm extrahiert.
4. Wählen Sie bei den **Registrierungseinstellungen** den Befehl **Anmeldedaten verwenden** oder **Registrierungstoken verwenden**. Weitere Informationen über die Generierung eines Registrierungstokens finden Sie im Abschnitt '"Schritt 1: Ein Registrierungstoken generieren" (S. 187)'.
5. [Nur, wenn Sie eine Installation auf einem Domain Controller durchführen] Wählen Sie bei **Anmeldekonto für den Agenten-Dienst** die Option **Folgendes Konto verwenden**. Spezifizieren Sie das Benutzerkonto, unter dem der Agenten-Dienst ausgeführt werden soll, und klicken Sie dann auf **Fertig**. Das Setup-Programm erstellt aus Sicherheitsgründen nicht automatisch neue Konten auf einem Domain Controller.

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

   Weitere Informationen zur Installation des Agenten auf einem schreibgeschützten Domain Controller (RODC, Read-only Domain Controller) finden Sie in diesem Knowledge Base-Artikel.
6. Überprüfen oder ändern Sie andere Installationseinstellungen, die der .mst-Datei hinzugefügt werden, und klicken Sie dann auf **Fortsetzen**.

7. Wählen Sie dann den Ordner aus, wo die .mst-Transform-Datei generiert wird und die .msi- und .cab-Installationspakete extrahiert werden, und klicken Sie dann auf **Generieren**.

### Das Produkt mithilfe der .mst-Transform-Datei installieren

Führen Sie in der Kommandozeile den nachfolgenden Befehl aus.

*Befehlsvorlage:*

```
msiexec /i <package name> TRANSFORMS=<transform name>
```

Dabei ist:

- `<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 <package name><PARAMETER 1>=<value 1> ... <PARAMETER N>=<value n>
```

Wobei `<Paket-Name>` der Name der .msi-Datei ist. Alle verfügbaren Parameter und ihre Werte sind unter '"Grundlegende Parameter" (S. 151)' beschrieben.

*Befehlsvorlage (Deinstallation):*

```
msiexec /x <package name> <PARAMETER 1>=<value 1> ... <PARAMETER N>=<value n>
```

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

### 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.

# 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 Protect 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 Protect 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 Protect 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 Protect 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 Protect Service registriert wird. Dies darf kein Partner-Administrator-Konto sein.

`REGISTRATION_PASSWORD_ENCODED`

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

`REGISTRATION_TOKEN`

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

`SET_ESX_SERVER={0,1}`

- Wenn der Wert `0` beträgt, wird der zu installierende Agent für VMware nicht mit einem vCenter Server oder ESXi-Host verbunden. Wenn der Wert `1` beträgt, 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. Wenn der Wert `ALL` beträgt, werden alle Produkt-Komponenten deinstalliert.

Sie können zusätzlich noch folgende Parameter spezifizieren:

`DELETE_ALL_SETTINGS={0, 1}`

Wenn der Wert `1` beträgt, 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 Protect 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 Protect 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 Protect 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,OracleAgentFeature,T
rayMonitor TARGETDIR="C:\Program Files\BackupClient" REBOOT=ReallySuppress CURRENT_
LANGUAGE=en MMS_USE_SYSTEM_ACCOUNT=1 REGISTRATION_ADDRESS=https://cloud.company.com
REGISTRATION_LOGIN=johndoe REGISTRATION_PASSWORD_ENCODED=am9obnNwYXNzd29yZA==
```

- Den Agent für Windows, das Befehlszeilenwerkzeug und den Cyber Protection Monitor installieren. Die Maschine im Cyber Protect 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
```

## 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:

```
<package 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' beschrieben.

- Führen Sie folgenden Befehl aus, um die Installation mit Parametern zu starten, die in einer separaten Textdatei spezifiziert wurden:

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

  Dieser Ansatz kann nützlich sein, wenn Sie keine sensiblen Informationen über die Befehlszeile eingeben wollen. In diesem Fall können Sie die Konfigurationseinstellungen in einer separaten

Textdatei spezifizieren und sicherstellen, dass nur Sie auf diese zugreifen können. Verwenden Sie für jeden Parameter eine neue Zeile, gefolgt 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.

### Parameter für eine unbeaufsichtigte Installation oder Deinstallation

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

Die minimale Konfiguration für eine unbeaufsichtigte Installation beinhaltet den Parameter `-a` sowie die Registrierungsparameter (beispielsweise die Parameter `--login` und `--password` oder die Parameter `--rain` und `--token`). Sie können weitere Parameter verwenden, um Ihre Installation anzupassen.

#### Installationsparameter

## Grundlegende Parameter

`{-i |--id=}` `<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 Protect 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 Protect 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 Webkonsole generieren, wie im Abschnitt 'Agenten per Gruppenrichtlinie bereitstellen' erläutert.

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

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

    Die URL des Cyber Protect 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 Protect 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 Protect 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 Protect 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 Protect Service registrieren wollen. Weitere Informationen über die entsprechende Durchführung finden Sie im Abschnitt 'Maschinen manuell registrieren'.

## Zusätzliche Parameter

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

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

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

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

`--tmp-dir=<Speicherort>`

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

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

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

`--skip-prereq-check`

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

`--force-weak-snapapi`

Der Installer wird kein snapapi-Modul kompilieren. Stattdessen wird er ein vorgefertigtes Modul verwenden, welches möglicherweise nicht genau zum Linux-Kernel passt. 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
```

## Unbeaufsichtigte Installation oder Deinstallation unter macOS

Dieser Abschnitt beschreibt, wie Sie den Protection Agenten auf einer unter macOS laufenden Maschine und mithilfe der Befehlszeile im unbeaufsichtigten Modus installieren, registrieren und deinstallieren können. 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 der Platzhalter `<dmg_root>` für einen Name Ihrer Wahl steht.
2. Mounten Sie die .dmg-Datei.

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

   Wobei der Platzhalter `<dmg_file>` für den Name der Installationsdatei steht. 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/RegisterAgent -o register -t cloud -a
  <service address> -u <user name> -p <password>
  ```

  Wobei:

  Die `&lt;Cyber Protect Service-Adresse&gt;` ist diejenige Adresse, die Sie zum **Anmelden** am Cyber Protect Service verwenden. Beispiel:

  `&lt;Benutzername&gt;` und `&lt;Kennwort&gt;` für die Anmeldedaten des Kontos stehen, 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/RegisterAgent -o register -t cloud -a
  <service address> --token <token>
  ```

  Das Registrierungstoken ist eine Folge von 12 Zeichen, die durch Bindestriche in 3 Segmente separiert sind. Sie können ein Token in der Cyber Protect 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 Protect Service **angemeldet haben**. Beispiel:

  
  
  ```

**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.

### Beispiele

Registrierung mit einem Benutzernamen und Kennwort.

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

Registrierung mit einem Token.

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

***So können Sie den Agenten für Mac deinstallieren***

Führen Sie folgenden Befehl aus:

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

## Maschinen manuell registrieren

Neben der Möglichkeit, eine Maschine direkt während der Agenten-Installation im Cyber Protect 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 in der Eingabeaufforderung der Maschine, auf welcher der Agent installiert ist, einen der folgenden Befehle aus:

- So können Sie eine Maschine unter dem aktuellen Konto registrieren:

```
<path to the registration tool> -o register -s mms -t cloud --update
```

  - Wobei `<Pfad zum Registrierungstool>` folgendes Verzeichnis ist:
    - unter Windows: `%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe`
    - unter Linux: `/usr/lib/Acronis/RegisterAgentTool/RegisterAgent`
    - unter macOS: `/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent`
- So können Sie eine Maschine unter einem anderen Konto registrieren:

```
<path to the registration tool> -o register -t cloud -a <service address> -u <user name> -p <password>
```

  - Wobei `<Benutzername>` und `<Kennwort>` für die Anmeldedaten des entsprechenden Kontos stehen, unter dem der Agent registriert wird. Dies darf kein Partner-Administrator-Konto sein.
    Die `<Service-Adresse>` entspricht der URL, die zum **Anmelden** am Cyber Protect Service verwendet wird. Beispiel: `https://cloud.company.com`.
    
    
- So können Sie eine Maschine mit einem Registrierungstoken registrieren:

```
<path to the registration tool> -o register -t cloud -a <service address> --token <token>
```

  - 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'.
    Wenn Sie ein Registrierungstoken verwenden, müssen Sie die genaue Datacenter-Adresse als `<Service-Adresse>` spezifizieren. Dies ist die URL, die Sie sehen, sobald Sie sich am Cyber Protect Service **angemeldet haben**. Beispielsweise `https://eu2-cloud.company.com`.
    
    
    Sie dürfen hier nicht die Adresse `https://cloud.company.com` verwenden.

***So können Sie die Registrierung einer Maschine aufheben***

Führen Sie in der Eingabeaufforderung der Maschine, auf welcher der Agent installiert ist, folgenden Befehl aus:

```
<path to the registration tool> -o unregister
```

## Beispiele

### Windows

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

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

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

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

### Linux

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

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

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

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

### macOS

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

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

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

```
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:

```
<path to the registration tool> -o register -t cloud -a <service address> -u <user name>
-p <"password">
```

*Beispiel (für Windows):*

```
"%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/.
- Spezifizieren Sie das codierte Kennwort in der Befehlszeile unter Verwendung der Parameter -b oder --base64.

```
<path to the registration tool> -o register -t cloud -a <service address> -u <user name>
-b -p <encoded password>
```

*Beispiel (für Windows):*

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

## Den Agenten für oVirt (Virtuelle Appliance) bereitstellen

Informationen darüber, wie Sie den Agenten für oVirt (Virtual Appliance) bereitstellen und konfigurieren können, finden Sie in der Cyber Protection Cloud-Dokumentation.

## Den Agenten für Virtuozzo Hybrid Infrastructure (Virtuelle Appliance) bereitstellen

Informationen darüber, wie Sie den Agenten für Virtuozzo Hybrid Infrastructure (Virtual Appliance) bereitstellen und konfigurieren können, finden Sie in der Cyber Protection Cloud-Dokumentation.

# Automatische Erkennung von Maschinen

Mit der automatischen Erkennung können Sie:

- Die Installation von Protection Agenten sowie die Registrierung von Maschinen auf dem Management Server automatisieren, indem Sie die Maschinen in Ihrer Active Directory-Domain oder Ihrem lokalen Netzwerk erkennen lassen.

- Protection Agenten auf mehreren Maschinen installieren und aktualisieren.
- Synchronisierungen mit dem Active Directory verwenden, um die Bereitstellung von Ressourcen und Verwaltung von Maschinen in einer großen Active Directory-Domain zu erleichtern.

## Voraussetzungen

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

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

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

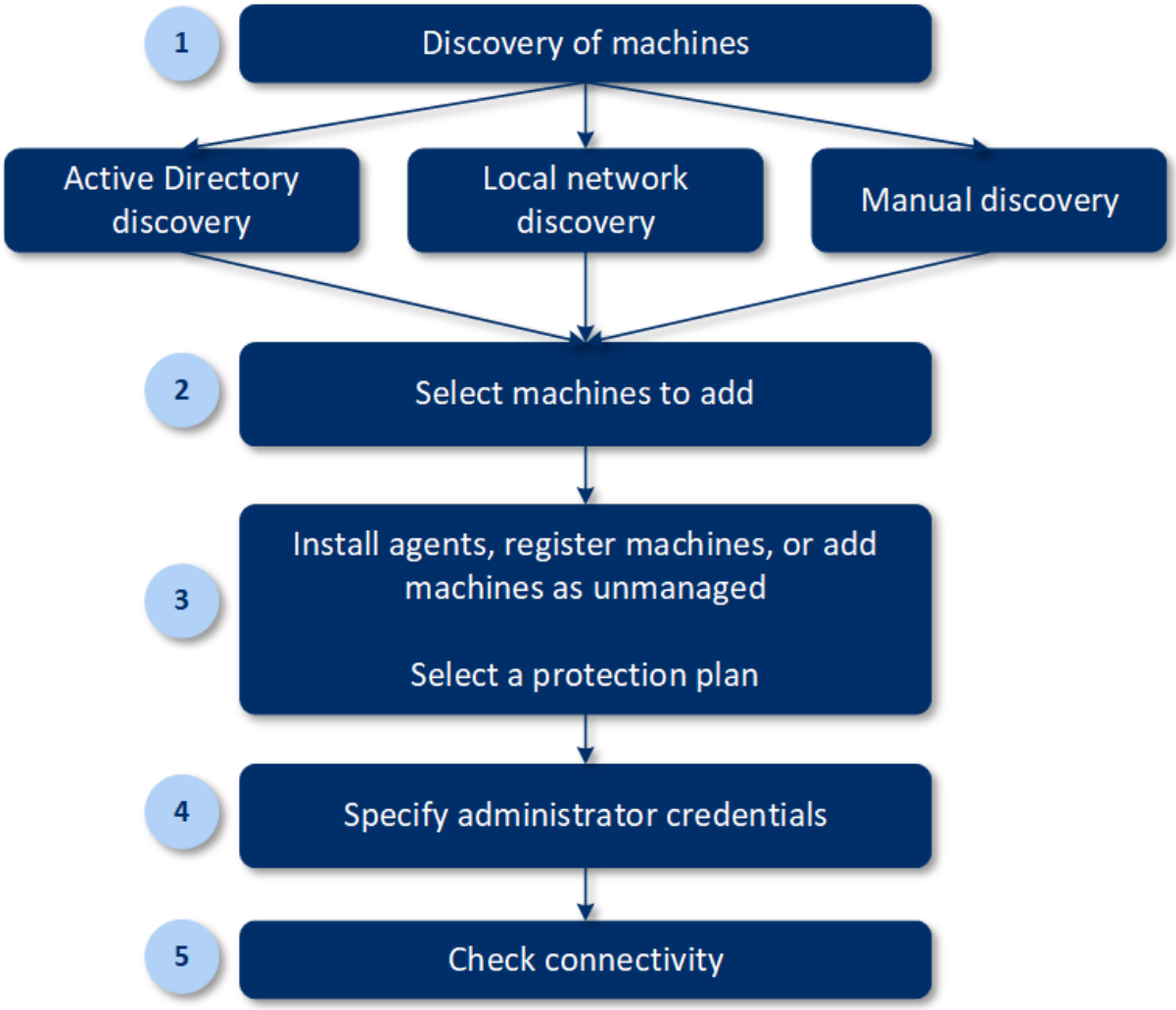
## So funktioniert die automatische Erkennung

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

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

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

Das nachfolgende Diagramm fasst den automatischen Erkennungsprozess zusammen.




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

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

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

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

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

4. Geben Sie die Administrator-Anmeldedaten für die ausgewählten Maschinen an.
5. Wählen Sie den Namen oder die IP-Adresse des Management Servers, über den bzw. die der Agent auf diesen Server zugreifen wird.
   Standardmäßig ist der Name des Servers vorausgewählt. Wenn Ihr Management Server über mehr als eine Netzwerkschnittstelle verfügt oder wenn Sie DNS-Probleme haben, die die Registrierung des Agenten fehlschlagen lassen, sollten Sie stattdessen die IP-Adresse auswählen.
6. Überprüfen Sie, ob Sie mit den angegebenen Anmeldedaten eine Verbindung zu den Maschinen herstellen können.

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

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

## Automatische und manuelle Erkennung

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

***So können Sie Maschinen erkennen***

1. Gehen Sie in der Webkonsole 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 kann, 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, was nach der Erkennung geschehen soll:
   - **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'. Sie können bis zu 100 Agenten gleichzeitig installieren.

     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 Protect 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 Webkonsole 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] **Die Abteilung, wo die Maschinen registriert werden sollen** – bestimmen Sie die Abteilung, in welcher 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 benutzerdefinierten Administrators spezifizieren wollen, müssen Sie zusätzliche manuelle Vorbereitungen durchführen. Eine Beschreibung dazu finden Sie hier: 'Eine unter Windows laufende Maschine hinzufügen' –> 'Vorbereitung'.

11. Wählen Sie den Namen oder die IP-Adresse des Management Servers, über den bzw. die der Agent auf diesen Server zugreifen wird.
    Standardmäßig ist der Name des Servers vorausgewählt. Wenn Ihr Management Server über mehr als eine Netzwerkschnittstelle verfügt oder wenn Sie DNS-Probleme haben, die die Registrierung des Agenten fehlschlagen lassen, sollten Sie stattdessen die IP-Adresse auswählen.
12. 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.

## 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 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 Protect 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 Protect 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 Protect bereit – den Agenten und dem Management Server. Er wird installiert, sofern er ausgewählt wurde. |
| Bootable Media Builder | Mit dieser Komponente können Benutzer ein Boot-Medium erstellen. Wenn es ausgewählt ist, wird es auf den Windows-Maschinen installiert. |

## 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 Protect 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.

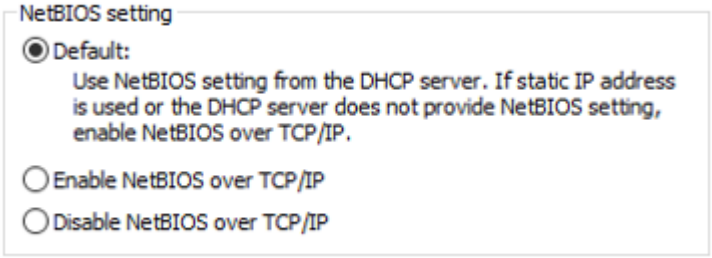
Diese Maschinen werden nach der Installation des Protection Agenten im Bereich **Geräte** –> **Maschinen mit Agenten** angezeigt.

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

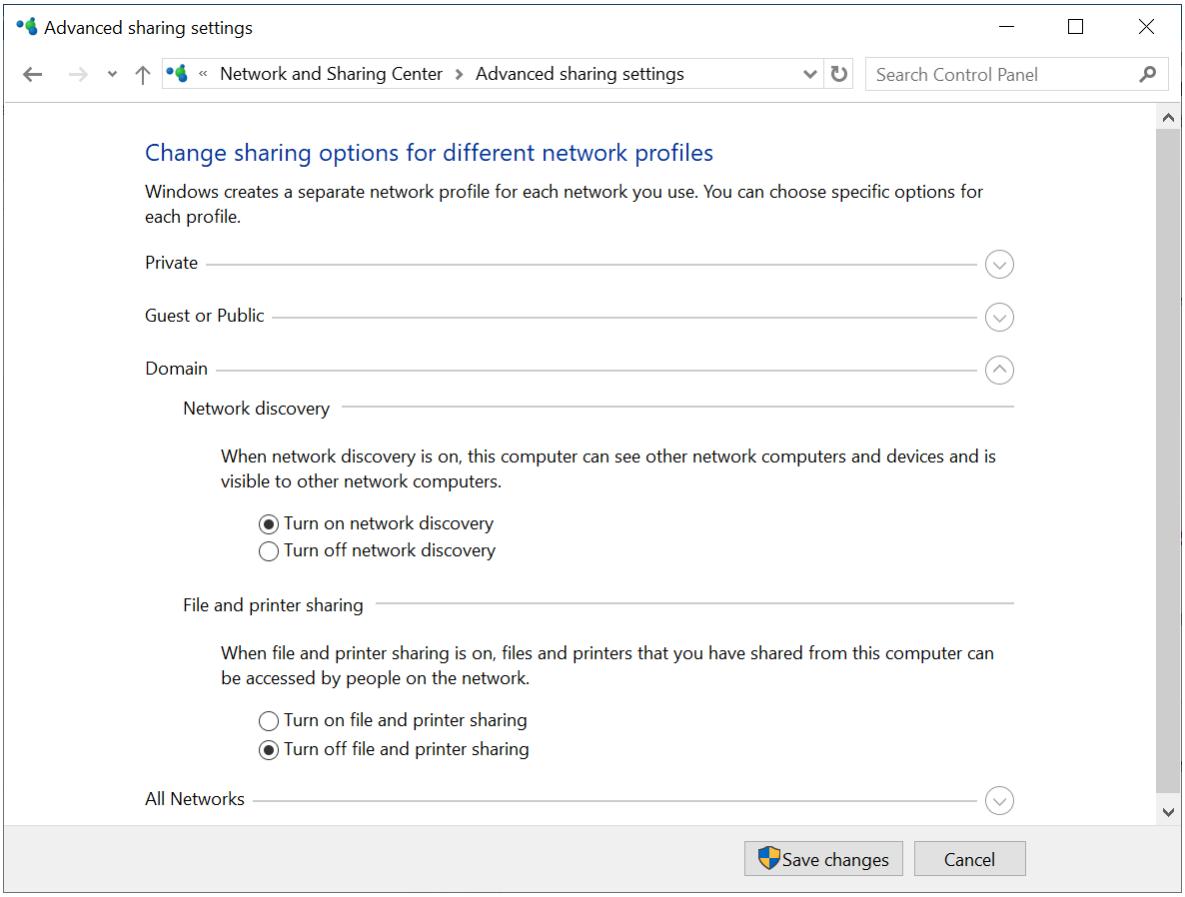
## Problembehebung (Troubleshooting)

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

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




- Schalten Sie über **Systemsteuerung** –> **Netzwerk- und Freigabecenter** –> **Erweiterte Freigabeeinstellungen** die Netzwerkerkennung ein.




- Überprüfen Sie, dass der **Hostdienst für den Funktionssuchanbieter** auf der Maschine läuft, die die Erkennung durchführt, und zudem auf den Maschinen, die erkannt werden sollen.
- Überprüfen Sie, dass der **Hostdienst für den Funktionssuchanbieter** auf den Maschinen läuft, die erkannt werden sollen.

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

## Bevor Sie beginnen

### Systemanforderungen für den Agenten

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

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.

**Hinweis**
vStorage APIs muss auf dem ESXi-Host installiert sein, um Backups von virtuellen Maschinen aktivieren zu können. Siehe: https://kb.acronis.com/de/content/14931.

### 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**.

# Deployment der OVF-Vorlage

## Speicherort der OVF-Vorlage

Die OVF-Vorlage besteht aus einer .ovf-Datei und zwei .vmdk-Dateien.

### Bei On-Premise-Bereitstellungen

Nachdem die Installation des Management Servers abgeschlossen ist, befinden sich das OVF-Paket der virtuellen Appliance im Ordner '**%ProgramFiles%\Acronis\ESXAppliance**' (unter Windows) oder '**/usr/lib/Acronis/ESXAppliance**' (unter Linux).

### Bei Cloud-Bereitstellungen

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.

## Deployment der OVF-Vorlage

1. Stellen Sie sicher, dass die Maschine, die den vSphere Client ausführt, auf die OVF-Vorlagen-Dateien zugreifen kann.
2. Starten Sie den vSphere Client und melden Sie sich am vCenter Server an.
3. 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 in Cloud-Bereitstellungen beim Konfigurieren der Netzwerkverbindungen darauf, ein Netzwerk auszuwählen, das eine Internetverbindung zulässt, damit sich der Agent korrekt in der Cloud registrieren kann. Wenn Sie in On-Premise-Bereitstellungen eine Netzwerkverbindung konfigurieren, sollten Sie darauf achten, ein Netzwerk auszuwählen, welches den Management Server enthält.

# 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 **Betrieb** –> **Einschalten**. 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. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:

- Wenn die Proxy-Einstellungen während der Installation des Agenten spezifiziert wurden, suchen Sie nach dem folgenden Abschnitt:

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

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

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

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

f. Speichern Sie die Datei.

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

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

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

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

j. Führen Sie den Befehl **`reboot`** aus:

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 werden Backups schneller erstellt, wenn der Agent solche virtuelle Maschinen sichert, die auf 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 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. Gehen Sie bei **Server-Name/IP** folgendermaßen vor:
      - Wählen Sie bei einer On-Premise-Bereitstellungen die Option **Lokal** aus. Spezifizieren Sie den Host-Namen oder die IP-Adresse derjenigen Maschine, auf welcher der Management Server installiert ist.
      - Wählen Sie bei einer Cloud-Bereitstellung die Option **Cloud** aus. Die Software zeigt die Adresse des Cyber Protection Service an. Ändern Sie diese Adresse nicht, solange es keine anderslautenden Anweisungen gibt.
   c. Gehen Sie bei **Benutzername** und **Kennwort** folgendermaßen vor:
      - Spezifizieren Sie bei einer On-Premise-Bereitstellung die Anmeldedaten eines Management Server-Administrators.
      - Spezifizieren Sie bei einer Cloud-Bereitstellung 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.

# Den Agenten für Scale Computing HC3 (Virtuelle Appliance) bereitstellen

## Bevor Sie beginnen

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

### Systemanforderungen für den Agenten

Wenn Sie die virtuelle Appliance bereitstellen, können Sie zwischen verschiedenen Kombinationen von vCPUs und RAM wählen. 2 vCPUs und 4 GiB RAM sind für die meisten Operationen optimal und ausreichend. Wir empfehlen, diese Ressourcen auf 4 vCPUs und 8 GiB 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.

Die eigenen virtuellen Laufwerke der Appliance belegen nicht mehr als 6 GB.

### Wie viele Agenten benötige ich?

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

Wenn Sie mehr als einen Agenten in einem Cluster haben, werden die virtuellen Maschinen automatisch gleichmäßig zwischen den Agenten verteilt, sodass jeder Agent eine 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. Diese passiert jedoch nicht, wenn ein Agent beschädigt wird oder manuell aus dem Scale Computing HC3-Cluster gelöscht wird. Eine Neuverteilung wird in diesem Fall nur dann gestartet, wenn Sie einen solchen Agenten über die Cyber Protect-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

## Die virtuelle Appliance bereitstellen

1. Melden Sie sich an Ihrem Cyber Protect Konto an.
2. Klicken Sie auf **Geräte** –> **Alle Geräte** –> **Hinzufügen** –> **Scale Computing HC3**.
3. Wählen Sie die Anzahl der virtuellen Appliances, die Sie bereitstellen wollen.
4. Spezifizieren Sie die IP-Adresse oder den Host-Namen des Scale Computing HC3-Clusters.
5. Spezifizieren Sie die Anmeldedaten eines Kontos, dem in diesem Cluster die Rolle **VM erstellen/bearbeiten** zugewiesen wurde.
6. Spezifizieren Sie eine Netzwerkfreigabe, die zur temporären Speicherung der Image-Datei für die virtuelle Appliance verwendet werden soll. Es sind mindestens 2 GB freier Speicherplatz erforderlich.
7. Spezifizieren Sie die Anmeldedaten eines Kontos, welches Lese- und Schreibrechte für diese Netzwerkfreigabe hat.
8. Klicken Sie auf **Bereitstellen**.

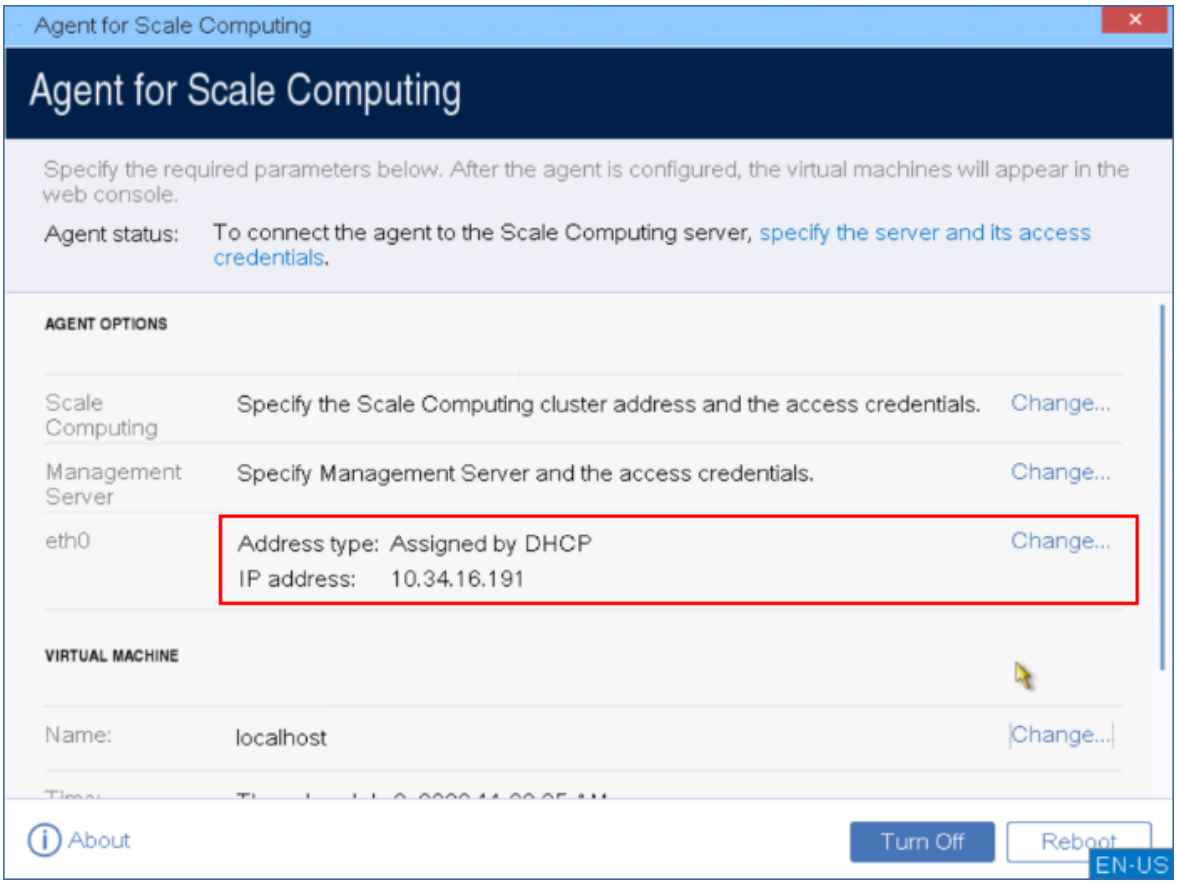
Konfigurieren Sie die virtuelle Appliance, nachdem die Bereitstellung abgeschlossen wurde.

## Die virtuelle Appliance konfigurieren

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

***So konfigurieren Sie die virtuelle Appliance***

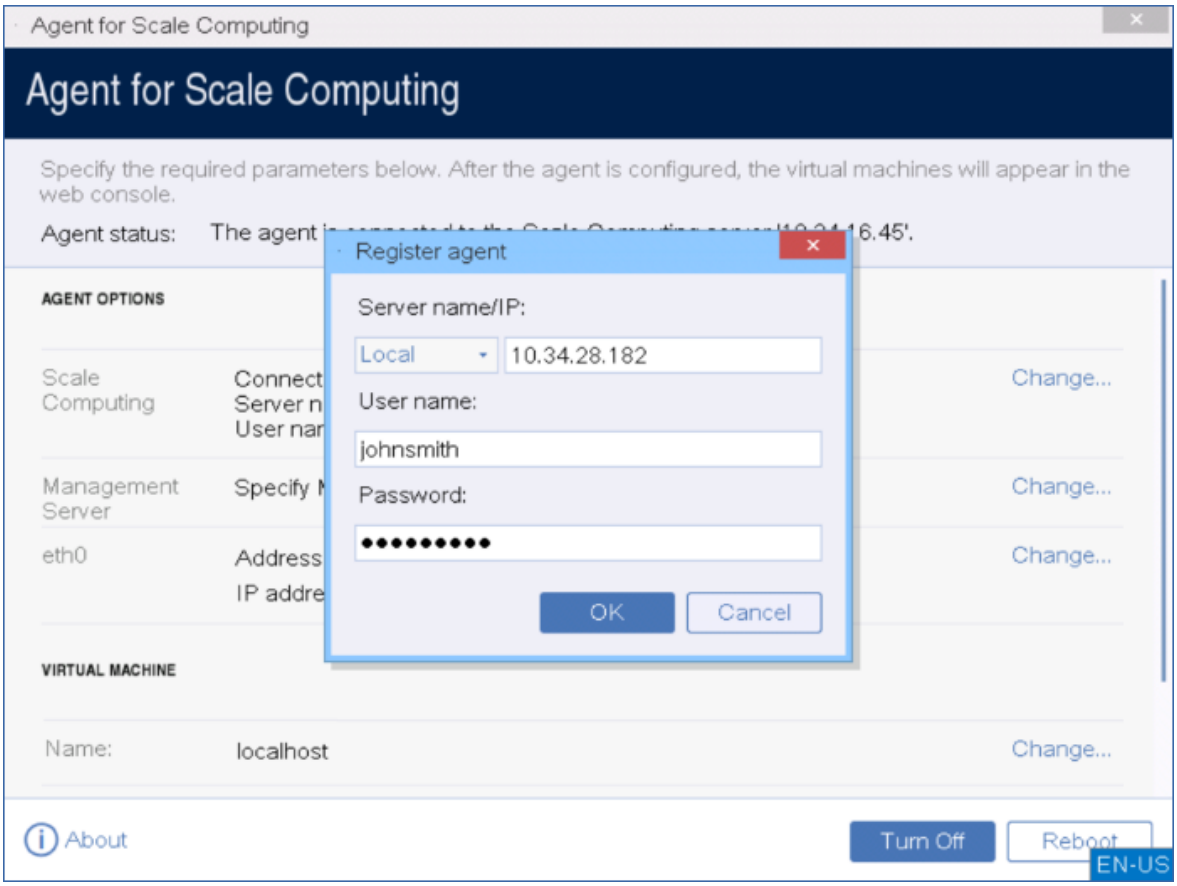
1. Melden Sie sich an Ihrem Scale Computing HC3-Konto an.
2. Wählen Sie die virtuelle Maschine mit dem Agenten aus, den Sie konfigurieren müssen, und klicken Sie dann auf **Konsole**.
3. Konfigurieren Sie die Netzwerkschnittstellen der Appliance. Abhängig von der Anzahl der Netzwerke, die die Appliance 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.



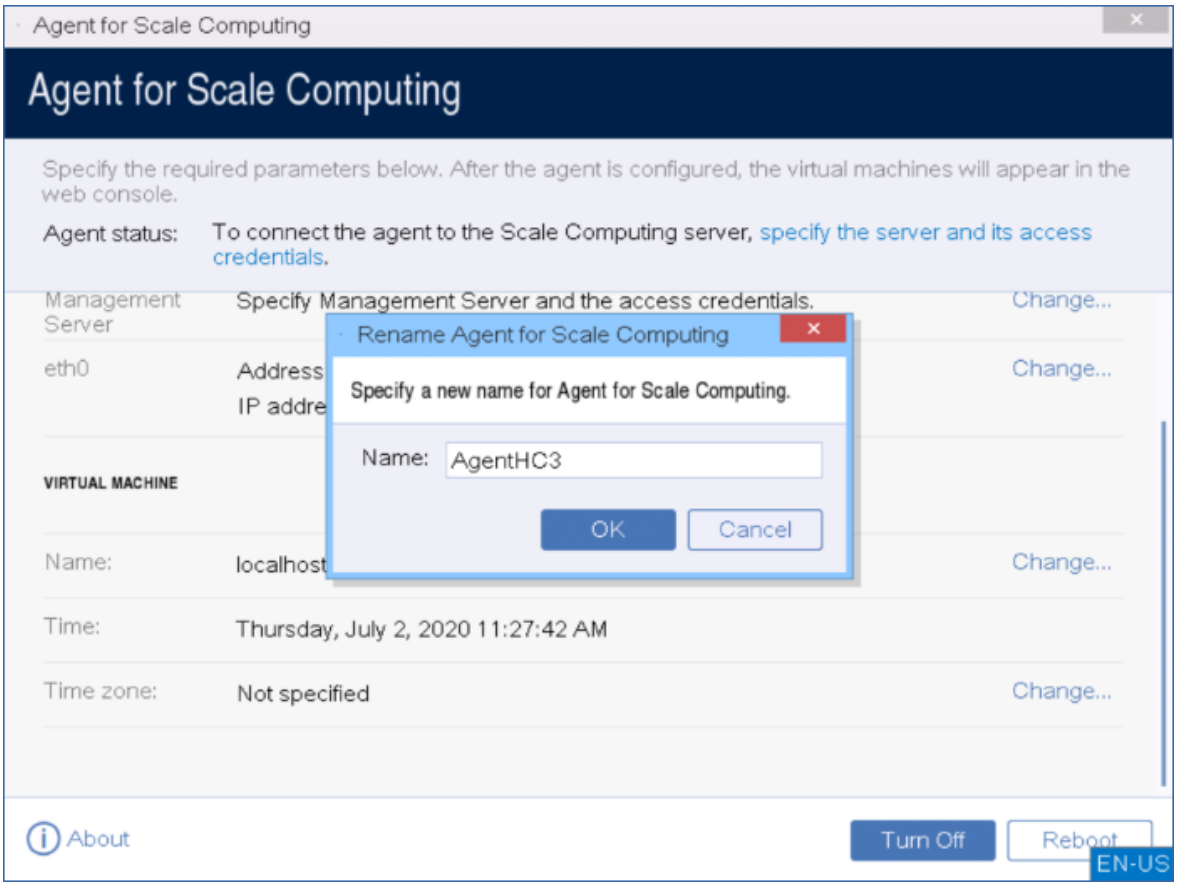

4. Spezifizieren Sie die Adresse und Anmeldedaten des Scale Computing HC3-Clusters:
   - Der DNS-Name oder die IP-Adresse des Clusters.
   - Geben Sie in den Feldern **Benutzername** und **Kennwort** die Ameldedaten für das Scale Computing HC3-Konto ein, dem die passenden Rollen zugewiesen wurden.

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


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



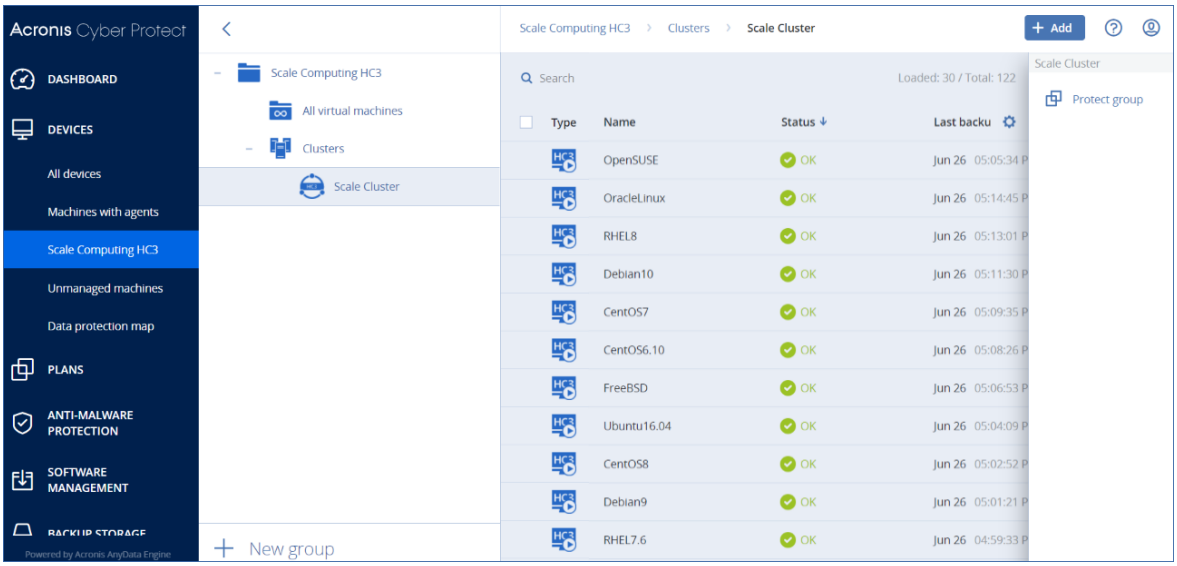

6. [Optional] Spezifizieren Sie einen Namen für den Agenten. Dieser Name wird in der Cyber Protect Webkonsole angezeigt.




7. [Optional] Stellen Sie durch die Auswahl Ihres Standortes sicher, dass alle geplanten Aktionen zur korrekten Zeit ausgeführt werden.

***So können Sie die virtuellen Maschinen im Scale Computing HC3-Cluster schützen***

1. Melden Sie sich an Ihrem Cyber Protect Konto an.
2. Gehen Sie zu **Geräte** –> **Scale Computing HC3** –> <Ihr Cluster> – oder suchen Sie Ihre Maschinen unter **Geräte** –> **Alle Geräte**.
3. Wählen Sie die gewünschten Maschinen aus und wenden Sie einen Schutzplan auf diese an.



## Agent für Scale Computing HC3 – erforderliche Rollen

Dieser Abschnitt beschreibt die Rollen, die für Aktionen mit virtuellen Scale Computing HC3-Maschinen sowie für die Bereitstellung der virtuellen Appliance erforderlich sind.

| Aktion | Rolle |
|---|---|
| Backup einer virtuellen Maschine | Backup<br>VM erstellen/bearbeiten<br>VM löschen |
| Recovery zu einer existierenden virtuellen Maschine | Backup<br>VM erstellen/bearbeiten<br>VM-Energiesteuerung<br>VM löschen<br>Cluster-Einstellungen |
| Recovery zu einer neuen virtuellen Maschine | Backup<br>VM erstellen/bearbeiten<br>VM-Energiesteuerung<br>VM löschen<br>Cluster-Einstellungen |
| Bereitstellung der virtuellen Appliance | VM erstellen/bearbeiten |

# 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 zur Installation unter Windows** heruntergeladen haben. Auf der Seite **Geräte hinzufügen** in der Cyber Protect Webkonsole 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 Cyber Protect Webkonsole 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 Cyber Protect Webkonsole 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. Überprüfen oder ändern Sie die Installationseinstellungen, die der .mst-Datei hinzugefügt werden. Wenn Sie die Art der Verbindung mit dem Management Server spezifizieren, wählen Sie die Option **Ein Registrierungstoken verwenden** und geben Sie dann das von Ihnen generierte Token ein.
6. Klicken Sie 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**.

# Virtuellen Appliances aktualisieren

## On-Premise-Bereitstellungen

Wenn Sie eine virtuelle Appliance (Agent für VMware oder Agent für Scale Computing HC3) aktualisieren wollen, deren Version kleiner als 15.24426 (im September 2020 freigegeben) ist, gehen Sie wie in Abschnitt '"Update der Agenten" (S. 190)' beschrieben vor.

***So können Sie eine virtuelle Appliance mit der Version 15.24426 oder höher aktualisieren***

1. Laden Sie das Update-Paket (wie unter http://kb.acronis.com/latest beschrieben) herunter.
2. Speichern Sie die `tar.bz`-Dateien im folgenden Verzeichnis auf der Maschine des Management Servers:
   - Windows: `C:\Programme\Acronis\VirtualAppliances\va-updates`
   - Linux: `/usr/lib/Acronis/VirtualAppliances/va-updates`
3. Klicken Sie in der Cyber Protect Webkonsole auf **Einstellungen** –> **Agenten**.
   Die Software zeigt eine Liste der Maschinen an. Maschinen mit veralteten virtuellen Appliances sind mit einem orangefarbenen Ausrufezeichen gekennzeichnet.
4. Wählen Sie die Maschinen aus, auf denen Sie die virtuellen Appliances aktualisieren wollen. Diese Maschinen müssen online sein.
5. Klicken Sie auf **Agent aktualisieren**.
6. Wählen Sie den Deployment Agent.
7. Spezifizieren Sie die Anmeldedaten eines Kontos, welches auf der Zielmaschine über administrative Berechtigungen verfügt.
8. Wählen Sie den Name/die IP-Adresse, den/die der Agent verwenden soll, um auf den Management Server zuzugreifen.
   Standardmäßig wird der Name des Servers vorausgewählt. Sie müssen diese Einstellung möglicherweise ändern, wenn der DNS-Server nicht in der Lage ist, den Namen in die IP-Adresse aufzulösen (wodurch es zu einem Fehler bei der Registrierung der virtuellen Appliance kommt).

Der Update-Fortschritt wird auf der Registerkarte **Aktivitäten** angezeigt.

**Hinweis**
Alle Backups, die während des Updates ausgeführt werden, werden fehlschlagen.

## Cloud-Bereitstellung

Informationen darüber, wie Sie eine virtuelle Appliance bei einer Cloud-Bereitstellung aktualisieren können, finden Sie im Abschnitt 'Update der Agenten' in der Cloud-Dokumentation.

# Update der Agenten

## 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.

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

Sie können die Agenten über die Cyber Protect Webkonsole aktualisieren oder indem Sie deren Installation wiederholen (mit jeder verfügbaren Möglichkeit). Wenn Sie mehrere Agenten gleichzeitig aktualisieren wollen, können Sie die nachfolgende Prozedur verwenden.

***So können Sie die Agenten über die Cyber Protect Webkonsole aktualisieren***

1. [Nur bei On-Premise-Bereitstellungen ] Führen Sie ein Update des Management Servers durch.
2. [Nur bei On-Premise-Bereitstellungen ] Stellen Sie sicher, dass die Installationspakete auf der Maschine mit dem Management Server vorhanden sind. Die genauen Schritte sind im Abschnitt 'Eine unter Windows laufende Maschine hinzufügen' –> 'Installationspakete' erläutert.
3. Klicken Sie in der Cyber Protect Webkonsole auf **Einstellungen** –> **Agenten**.
   Die Software zeigt eine Liste der Maschinen an. Maschinen mit einer veralteten Agenten-Version sind mit einem orangefarbenen Ausrufezeichen gekennzeichnet.
4. Wählen Sie die Maschinen aus, auf denen Sie die Agenten aktualisieren wollen. Diese Maschinen müssen online sein.
5. Klicken Sie auf **Agent aktualisieren**.
6. Wählen Sie den Deployment Agent.
7. Spezifizieren Sie die Anmeldedaten eines Kontos, welches auf der Zielmaschine über administrative Berechtigungen verfügt.
8. Wählen Sie den Namen oder die IP-Adresse des Management Servers, über den bzw. die der Agent auf diesen Server zugreifen wird.
   Standardmäßig ist der Name des Servers vorausgewählt. Wenn Ihr Management Server über mehr als eine Netzwerkschnittstelle verfügt oder wenn Sie DNS-Probleme haben, die die Registrierung des Agenten fehlschlagen lassen, sollten Sie stattdessen die IP-Adresse auswählen.
9. [Nur bei On-Premise-Bereitstellungen] Der Update-Fortschritt wird auf der Registerkarte **Aktivitäten** angezeigt.

**Hinweis**
Alle Backups, die während des Updates ausgeführt werden, werden fehlschlagen.

***So können Sie die Cyber Protect-Definitionen auf einer Maschine aktualisieren***

1. Klicken Sie auf **Einstellungen** –> **Agenten**.
2. Wählen Sie die Maschine aus, auf welcher Sie die Cyber Protect-Definitionen aktualisieren wollen, und klicken Sie dann auf **Definitionen aktualisieren**. Diese Maschine muss online sein.

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

1. Klicken Sie auf **Einstellungen** –> **Agenten**.
2. Wählen Sie die Maschine aus, der Sie die Updater-Rolle zuweisen wollen, klicken Sie auf **Details**, dann in den Bereich **Cyber Protect-Definitionen** und aktivieren Sie schließlich 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**.

# Upgrade auf Acronis Cyber Protect 15

Wenn Sie ein früheres Produkt auf Acronis Cyber Protect 15 upgraden wollen, können Sie dies auf folgende Arten machen:

- Direkt, ohne das frühere Produkt vorher zu deinstallieren.
  Diese Option ist jedoch nur für Acronis Backup 12.5 Update 5 (Build 16180) und höher verfügbar.
- Indem Sie das ältere Produkt deinstallieren und dann eine neue Kopie von Acronis Cyber Protect 15 installieren.
  Diese Option ist für alle berechtigten Produkte verfügbar. Weitere Informationen über diese Produkte finden Sie in diesem Knowledge Base-Artikel.

**Hinweis**
Wir empfehlen, dass Sie vor dem Upgrade ein Backup Ihres Systems erstellen. Dies ermöglicht es Ihnen, die ursprüngliche Konfiguration wiederherzustellen, falls das Upgrade fehlschlagen sollte.

Um das Upgrade zu starten, starten Sie den Installer und befolgen Sie dann die Bildschirmanweisungen.

Der Management Server in Acronis Cyber Protect 15 ist abwärtskompatibel und unterstützt auch die Agenten der Version 12.5. Diese Agenten unterstützen jedoch keine Cyber Protect-Funktionen.

Das Upgrade der Agenten hat keinen Einfluss auf bereits vorhandene Backup-Sets und deren Einstellungen.

# Das Produkt deinstallieren

Wenn Sie einzelne Produktkomponenten von einer Maschine wieder entfernen wollen, müssen Sie das entsprechende Setup-Programm ausführen, dann die Option zur Änderung des Produktes wählen und schließlich die Kontrollkästchen derjenigen Komponente deaktivieren, die Sie entfernen wollen. Die Links zu den Setup-Programmen 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.

**Warnung!**
Bei On-Premise-Bereitstellungen sollten Sie bei der Auswahl der zu deinstallierenden Komponenten sehr vorsichtig sein.

Wenn Sie versehentlich den Management Server deinstallieren, wird die Cyber Protect Webkonsole nicht mehr verfügbar sein und werden Sie die Maschinen, die auf dem deinstallierten Management Server registriert waren, nicht mehr sichern bzw. wiederherstellen können.

## Unter Windows:

1. Melden Sie sich als Administrator an.
2. Gehen Sie zu **Systemsteuerung** und wählen Sie **Programme und Funktionen** (oder **Software** bei Windows XP) –> **Acronis Cyber Protect** –> **Deinstallieren**.
3. [Optional] Aktivieren Sie das Kontrollkästchen **Protokolle (Logs) und Konfigurationseinstellungen entfernen**.
   Wenn Sie einen Agenten deinstallieren, aber vorhaben, den Agenten später erneut zu installieren, lassen Sie dieses Kontrollkästchen deaktiviert. Wenn Sie das Kontrollkästchen aktivieren, wird die Maschine möglicherweise in der Cyber Protect Webkonsole dupliziert – und die Backups der alten Maschine werden nicht mehr mit der neuen Maschine assoziiert sein.
4. Bestätigen Sie Ihre Entscheidung.

## 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**.
   Wenn Sie einen Agenten deinstallieren, aber vorhaben, den Agenten später erneut zu installieren, lassen Sie dieses Kontrollkästchen deaktiviert. Wenn Sie das Kontrollkästchen aktivieren, wird die Maschine möglicherweise in der Cyber Protect Webkonsole dupliziert – und die Backups der alten Maschine werden nicht mehr mit der neuen Maschine assoziiert sein.
3. Bestätigen Sie Ihre Entscheidung.

## 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.

# 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 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 virtuelle Appliance (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 virtuelle Appliance 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 virtuelle Appliance anschließen.
4. Klicken Sie mit der rechten Maustaste auf die virtuelle Appliance und wählen Sie **Von Festplatte löschen**. Bestätigen Sie Ihre Entscheidung.

# Maschinen aus der Cyber Protect Webkonsole entfernen

Wenn Sie einen Agenten deinstallieren, wird dessen Registrierung im Management Server aufgehoben und anschließend die Maschine, auf welcher der Agent installiert war, automatisch aus der Cyber Protect Webkonsole entfernt.

Wenn während dieser Aktion jedoch die Verbindung zum Management Server verloren geht (z.B. aufgrund eines Netzwerkproblems), kann es vorkommen, dass nur der Agent deinstalliert wird, dessen Maschine aber weiterhin in der Webkonsole angezeigt wird. In so einem Fall müssen Sie die Maschine dann manuell aus der Webkonsole entfernen.

***So können Sie eine Maschine manuell aus der Webkonsole entfernen***

1. Gehen Sie in der Cyber Protect Webkonsole zu **Einstellungen** –> **Agenten**.
2. Wählen Sie die Maschine aus, auf welcher der Agent installiert war.

3. Klicken Sie auf **Löschen**.

# Auf die Cyber Protect Webkonsole zugreifen

Wenn Sie auf die Cyber Protect Webkonsole zugreifen wollen, geben Sie die Adresse der Anmeldeseite in die Adresszeile eines Webbrowsers ein und melden Sie sich dann an (wie unten beschrieben).

## On-Premise-Bereitstellung

Die Adresse der Anmeldeseite entspricht der IP-Adresse oder dem Namen der Maschine, auf welcher der Management Server installiert ist.

Sowohl das HTTP- als auch das HTTPS-Protokoll werden über denselben TCP-Port unterstützt, der bei der Management Server-Installation konfiguriert werden kann. Der Standard-Port ist 9877.

Sie können den Management Server so konfigurieren, dass der Zugriff per HTTP auf die Cyber Protect Webkonsole verboten ist und das SSL-Zertifikat einer unabhängigen Zertifizierungsstelle verwendet wird.

### Unter Windows:

Falls der Management Server unter Windows installiert ist, können Sie sich auf zwei Arten an der Cyber Protect Webkonsole anmelden:

- Klicken Sie auf **Anmelden**, um sich als der aktuelle Windows-Benutzer anzumelden.
  Dies ist die einfachste Möglichkeit, wenn Sie sich an derselben Maschine anmelden wollen, auf welcher auch der Management Server installiert ist.
  Falls der Management Server auf einer anderen Maschine installiert ist, funktioniert diese Methode unter folgenden Bedingungen:
  - Die Maschine, über die Sie sich anmelden, befindet sich in derselben Active Directory-Domain wie der Management Server.
  - Sie sind als ein Domain-Benutzer angemeldet.

  Wir empfehlen, dass Sie Ihren Webbrowser für die integrierte Windows-Authentifzierung konfigurieren. Anderenfalls wird Sie der Browser nach Anmeldedaten (Benutzername, Kennwort) fragen. Sie können diese Option jedoch auch deaktivieren.
- Klicken Sie auf **Benutzername und Kennwort eingeben** und spezifizieren Sie die Anmeldedaten (Benutzernamen, Kennwort).

Ihr Konto muss auf jeden Fall zur Liste der Management Server-Administratoren gehören. Auf der Maschine, die den Management Server ausführt, enthält diese Liste standardmäßig die Windows-Benutzergruppe **Administratoren**. Weitere Informationen finden Sie im Abschnitt 'Administratoren und Abteilungen'.

***So können Sie die Option 'Als der aktuelle Windows-Benutzer anmelden' deaktivieren***

1. Gehen Sie auf der Maschine, auf welcher der Management Server installiert ist, zum Verzeichnis `C:\Program Files\Acronis\AccountServer`.

2. Öffnen Sie die Datei **account_server.json** zur Bearbeitung.
3. Gehen Sie zum Abschnitt "Connectors" und löschen Sie dann die folgenden Zeilen:

```
{
"type": "sspi",
"name": "1 Windows Integrated Logon",
"id": "sspi",
"config": {}
},
```

4. Gehen Sie zum Abschnitt "checksum", und ändern Sie dann den Wert für "sum" wie folgt:

```
"sum": "FWY/8e8C6c0AgNl0BfCrjgT4v2uj7RQNmaIYbwbjpzU="
```

5. Starten Sie den Acronis Service Manager Service neu (wie im Abschnitt 'Ein von einer vertrauenswürdigen Zertifizierungsstelle ausgestelltes Zertifikat verwenden' beschrieben).

### Unter Linux:

Wenn der Management Server unter Linux installiert ist, spezifizieren Sie die Anmeldedaten (Benutzername, Kennwort) eines Kontos, welches zur Liste der Management Server-Administratoren gehört. Auf der Maschine, auf der der Management Server ausgeführt wird, befindet sich standardmäßig nur der Benutzer **root** auf dieser Liste. Weitere Informationen finden Sie im Abschnitt 'Administratoren und Abteilungen'.

## Cloud-Bereitstellung

Die Adresse der Anmeldeseite ist https://backup.acronis.com/. Die Anmeldedaten (Benutzername, Kennwort) entsprechen denen Ihres Acronis Kontos.

Falls Ihr Konto vom Backup-Administrator erstellt wurde, müssen Sie das Konto noch aktivieren und das Kennwort festlegen, indem Sie auf den entsprechenden Link in Ihrer Aktivierungs-E-Mail klicken.

## Die Sprache ändern

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

## Einen Webbrowser für die integrierte Windows-Authentifzierung konfigurieren

Sie können die integrierte Windows-Authentifzierung nutzen, wenn Sie für den Zugriff auf die Cyber Protect Webkonsole eine unter Windows laufende Maschine und einen unterstützten Browser verwenden.

Wir empfehlen, dass Sie Ihren Webbrowser für die integrierte Windows-Authentifzierung konfigurieren. Anderenfalls wird Sie der Browser nach Anmeldedaten (Benutzername, Kennwort) fragen.

## Internet Explorer, Microsoft Edge, Opera oder Google Chrome konfigurieren

Wenn sich die Maschine, auf welcher der Browser ausgeführt wird, in derselben Active Directory-Domain wie die Maschine befindet, auf welcher der Management Server läuft, können Sie die Anmeldeseite der Backup Console in die 'Sites'-Liste für die Sicherheits-Zone **Lokales Intranet** aufnehmen.

Sollte dies nicht zutreffen, dann nehmen Sie die Anmeldeseite der Backup Console in die Liste der Sicherheits-Zone **Vertrauenswürdige Sites** auf und aktivieren Sie die Einstellung **Automatische Anmeldung mit aktuellem Benutzernamen und Kennwort**.

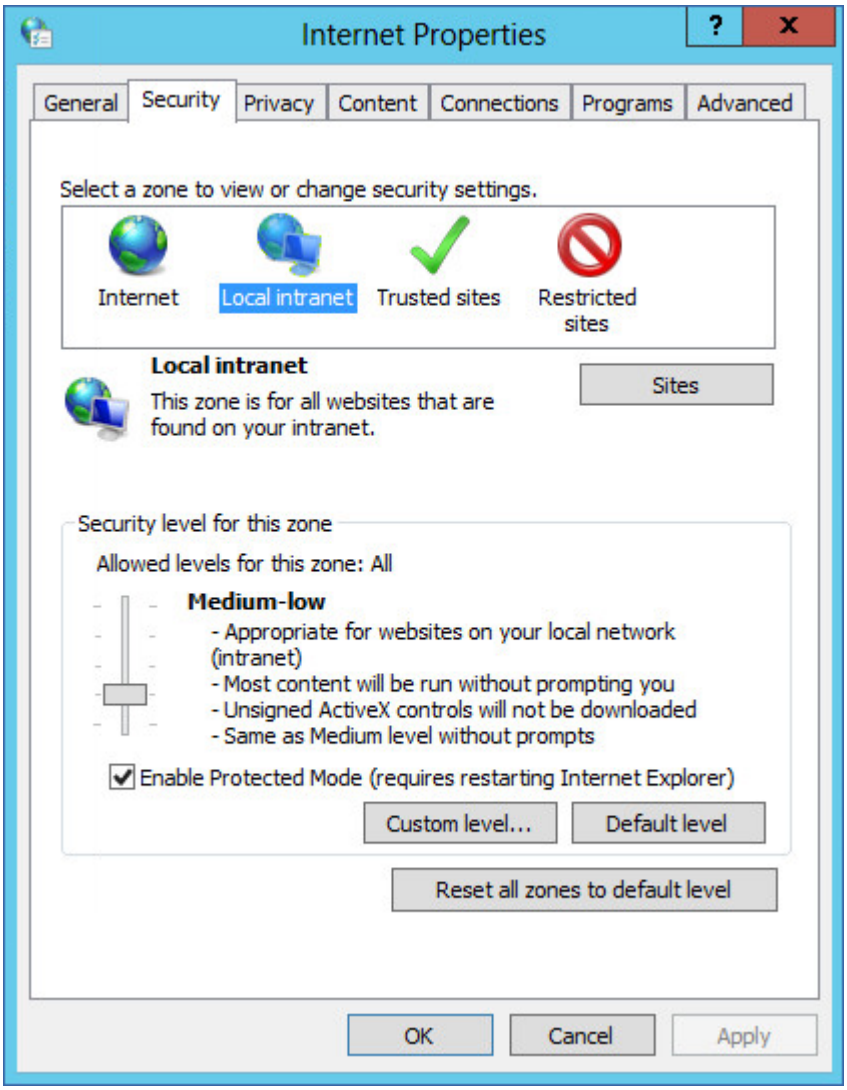
Entsprechende Schritt-für-Schritt-Anleitungen finden Sie weiter unten in diesem Abschnitt. Da diese Browser Windows-Einstellungen verwenden, können Sie die Browser in einer Active Directory-Domain mithilfe einer Gruppenrichtlinie konfigurieren.

## Mozilla Firefox konfigurieren

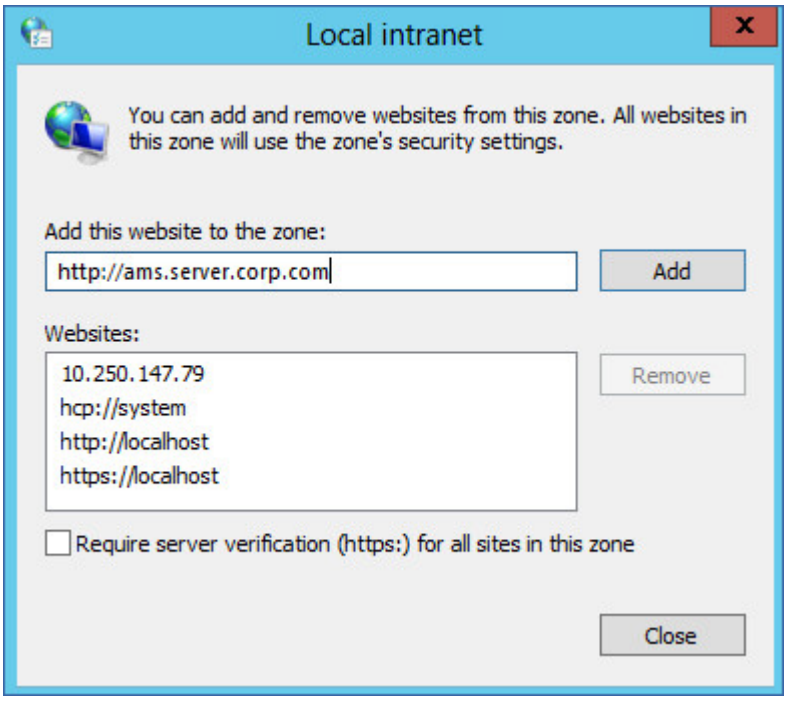
1. Firefox wird folgendermaßen konfiguriert: geben Sie die URL `about:config` ein und klicken Sie auf die Schaltfläche **Ich bin mir der Gefahren bewusst!**.
2. Verwenden Sie das Feld **Suchen:**, um die Einstellung `network.negotiate-auth.trusted-uris` zu finden.
3. Klicken Sie doppelt auf den angezeigten Einstellungsnamen und geben Sie dann die Adresse der Cyber Protect Webkonsole-Anmeldeseite ein.
4. Wiederholen Sie die Schritte 2-3 zusätzlich für die Einstellung `network.automatic-ntlm-auth.trusted-uris`.
5. Schließen Sie das Fenster `about:config`.

## Die Konsole zur Liste der lokalen Intranet-Sites hinzufügen

1. Gehen Sie zu **Systemsteuerung** –> **Internetoptionen**.
2. Wählen Sie in der Registerkarte **Sicherheit** das Symbol für **Lokales Intranet**.



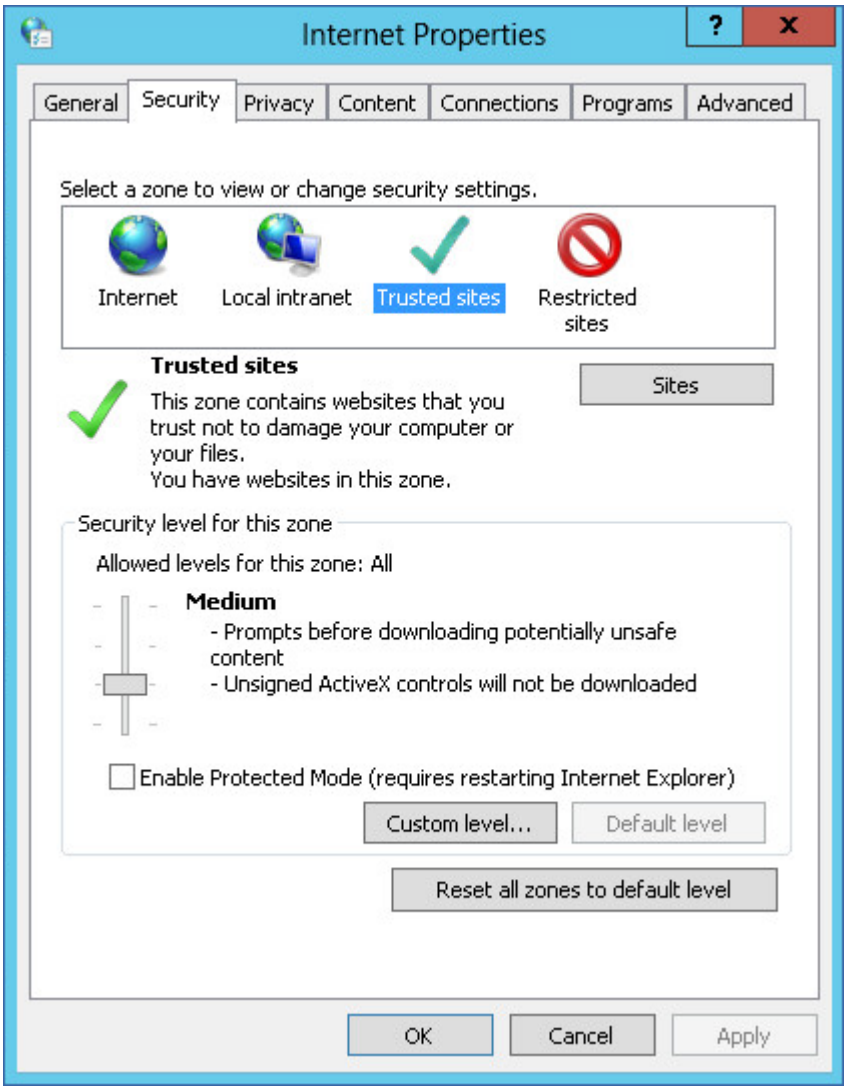

3. Klicken Sie auf **Sites**.
4. Geben Sie bei **Diese Website zur Zone hinzufügen** die Adresse der Anmeldeseite der Cyber Protect Webkonsole ein – und klicken Sie dann auf **Hinzufügen**.



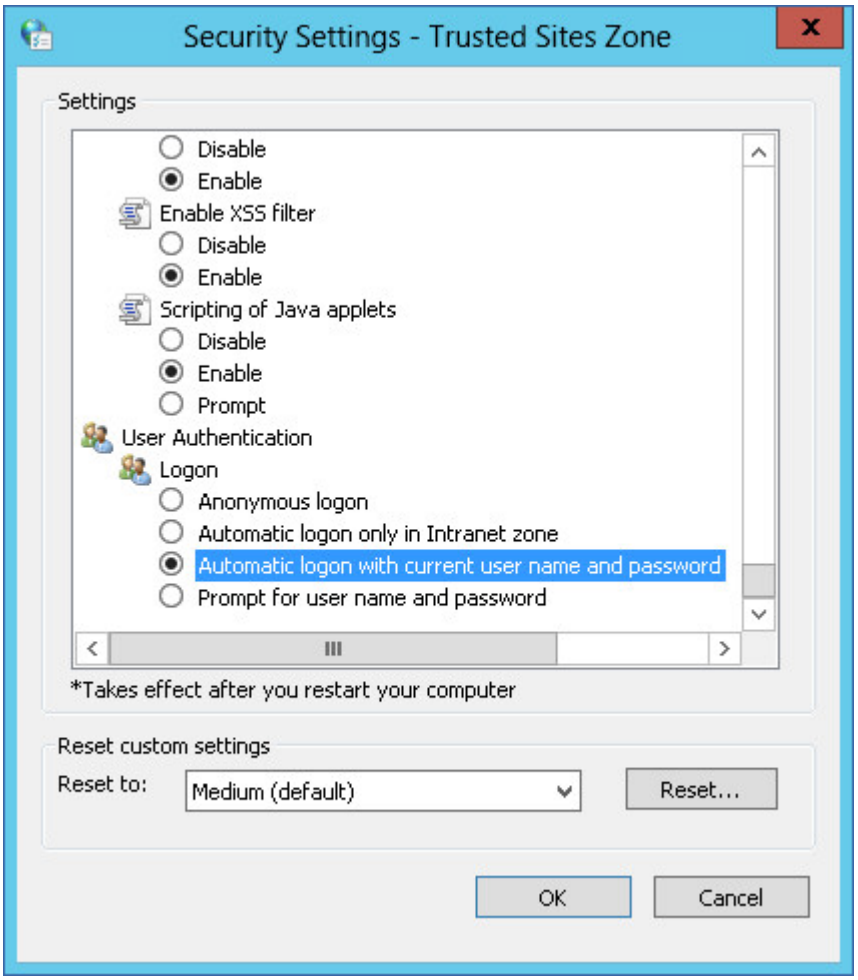

5. Klicken Sie auf **Schließen**.
6. Klicken Sie auf **OK**.

## Die Konsole zur Liste der vertrauenswürdigen Sites hinzufügen

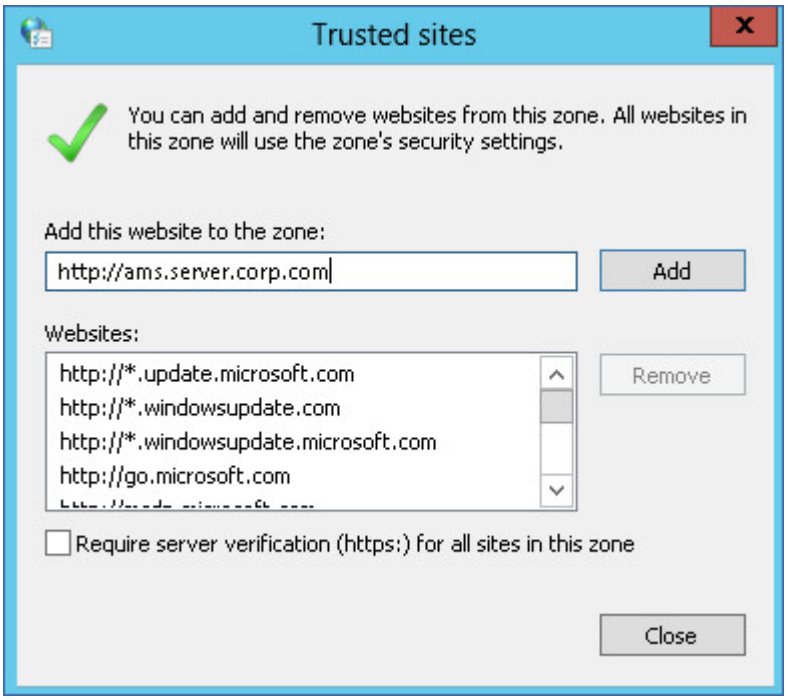
1. Gehen Sie zu **Systemsteuerung** –> **Internetoptionen**.
2. Wählen Sie in der Registerkarte **Sicherheit** das Symbol für **Vertrauenswürdige Sites** aus – und klicken Sie dann auf **Stufe anpassen**.




3. Wählen Sie im Abschnitt **Anmeldung** die Option **Automatische Anmeldung mit aktuellem Benutzernamen und Kennwort** und klicken Sie dann auf **OK**.




4. Wählen Sie in der Registerkarte **Sicherheit** (während das Symbol für **Vertrauenswürdige Sites** weiterhin ausgewählt ist) den Befehl **Sites**.
5. Geben Sie bei **Diese Website zur Zone hinzufügen** die Adresse der Anmeldeseite der Cyber Protect Webkonsole ein – und klicken Sie dann auf **Hinzufügen**.




6. Klicken Sie auf **Schließen**.
7. Klicken Sie auf **OK**.

# Nur HTTPS-Verbindungen zur Webkonsole erlauben

Aus Sicherheitsgründen können Sie unterbinden, dass Benutzer über das HTTP-Protokoll auf die Cyber Protect-Webkonsole zugreifen und stattdessen nur HTTPS-Verbindungen zulassen.

***So können Sie nur HTTPS-Verbindungen zur Webkonsole zulassen***

1. Öffnen Sie auf dier Maschine, die den Management Server ausführt, die nachfolgende Konfigurationsdatei in einem Text-Editor:
   - Unter Windows: `%ProgramData%\Acronis\ApiGateway\api_gateway.json`
   - Unter Linux: `/var/lib/Acronis/ApiGateway/api_gateway.json`
2. Suchen Sie den folgenden Abschnitt:

```
"tls": {
  "auto_redirect" : false,
  "cert_file": "cert.pem",
```

3. Ändern Sie den Wert `"auto_redirect"` von `false` auf `true`.
   Wenn die Zeile `"auto_redirect"` fehlen sollte, müssen Sie diese manuell hinzufügen:

```
"auto_redirect": true,
```

4. Speichern Sie die Datei `api_gateway.json`.

**Wichtig**
Gehen Sie vorsichtig vor und löschen Sie nicht versehentlich Kommas, Klammern und Anführungszeichen in der Konfigurationsdatei.

5. Starten Sie wie nachfolgend beschrieben den Acronis Service Manager Service neu.

***So können Sie den Acronis Service Manager Service unter Windows neu starten***

***Unter Windows:***

1. Klicken Sie im **Start**-Menü auf **Ausführen** und geben Sie ein: **cmd**
2. Klicken Sie auf **OK**.
3. Führen Sie folgende Befehle aus:

```
net stop asm
net start asm
```

***Unter Linux:***

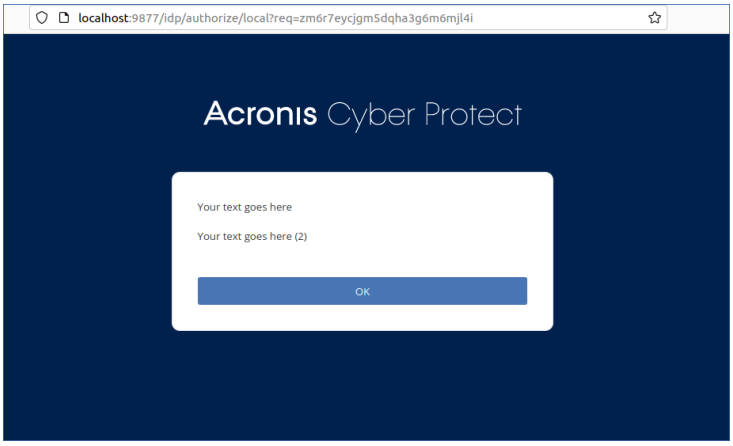
1. Öffnen Sie die Applikation **Terminal**.
2. Führen Sie folgenden Befehl (in einem beliebigen Verzeichnis) aus:

```
sudo service acronis_asm restart
```

# Der Webkonsole eine benutzerdefinierte Mitteilung hinzufügen

Sie können der Cyber Protect-Webkonsole eine benutzerdefinierte Mitteilung hinzufügen.

Diese Mitteilung wird vor jedem Anmeldeversuch angezeigt.



## Voraussetzungen

Wenn auf die Maschine, auf welcher der Management Server läuft, irgendwelche Schutzpläne angewendet werden, sollten Sie sicherstellen, dass die Selbstschutzfunktion deaktiviert ist. Anderenfalls werden Sie die Konfigurationsdatei nicht bearbeiten können.

Weitere Informationen zur Aktivierung bzw. Deaktivierung des Selbstschutzes finden Sie im Abschnitt '"Selbstschutz" (S. 545)'.

***So können Sie der Webkonsole eine benutzerdefinierte Mitteilung hinzufügen***

***Unter Windows:***

1. Melden Sie sich an der Maschine an, auf welcher der Management Server installiert ist. Ihr Konto muss über Administratorrechte verfügen.
2. Gehen Sie zu `%Program Files%\Acronis\AccountServer`.
3. [Optional] Erstellen Sie eine Backup-Kopie der Datei `AccountServer.zip`.
4. Gehen Sie zu `%Program Files%\Acronis\AccountServer\AccountServer.zip\static\locale`.
5. Entpacken Sie die JSON-Datei, die der Sprache entspricht, die Sie in der Cyber Protect-Webkonsole verwenden. Wenn Sie beispielsweise Englisch verwenden, müssen Sie die Datei `en.json` entpacken.

   **Hinweis**
   Um die Datei bearbeiten zu können, dürfen Sie diese nicht einfach per Doppelklick öffnen, sondern müssen die Datei entpacken.

6. Öffnen Sie die entpackte Datei, um diese zu bearbeiten. Sie können einen Texteditor wie Notepad oder Notepad++ verwenden.
7. Wechseln Sie in die nachfolgende Zeile und fügen Sie an deren Ende ein Komma ein:

   ```
   "APP_LOGINFORM_LOGIN_BUTTON": "Log in",
   ```

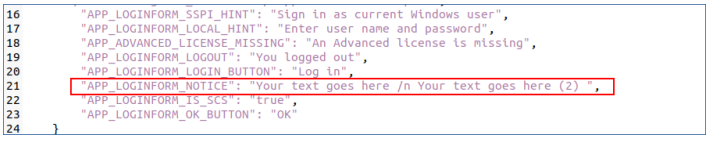
8. Fügen Sie unter der Zeile `"APP_LOGINFORM_LOGIN_BUTTON": "Log in"` folgende Zeilen ein:

   ```
   "APP_LOGINFORM_NOTICE": "<Type your custom message here>",
   ```

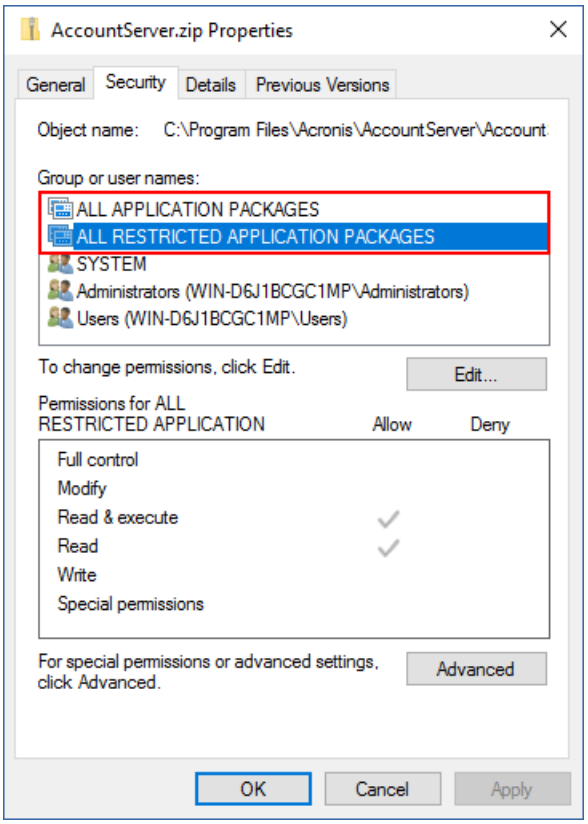
   ```
   "APP_LOGINFORM_IS_SCS": "true",
   ```

   ```
   "APP_LOGINFORM_OK_BUTTON": "OK"
   ```

   Beispiel:



9. Speichern Sie die Änderungen und platzieren Sie die bearbeitete JSON-Datei wieder im Verzeichnis `%Program Files%\Acronis\AccountServer\AccountServer.zip\static\locale`.
10. Klicken Sie mit der rechten Maustaste auf die Datei `AccountServer.zip` und gehen Sie dann zu **Eigenschaften** –> **Sicherheit**, um zu überprüfen, dass `ALLE ANWENDUNGSPAKETE` and `ALLE EINGESCHRÄNKTEN ANWENDUNGSPAKETE` unter **Gruppen- oder Benutzernamen** mit den Berechtigungen **Lesen** sowie **Lesen & Ausführen** hinzugefügt wurden.




**Hinweis**

Wenn `ALLE EINGESCHRÄNKTEN ANWENDUNGSPAKETE` fehlen sollten, entfernen Sie `ALLE ANWENDUNGSPAKETE` von der Liste und fügen Sie es dann wieder erneut hinzu. Der Eintrag `ALLE EINGESCHRÄNKTEN ANWENDUNGSPAKETE` wird automatisch erscheinen, wenn Sie `ALLE ANWENDUNGSPAKETE` hinzufügen.

11. Starten Sie den **Acronis Service Manager Service** neu (wie im Abschnitt '"So können Sie den Acronis Service Manager Service neu starten" (S. 209)' beschrieben).

***Unter Linux:***

1. Melden Sie sich an der Maschine an, auf welcher der Management Server installiert ist.
2. Gehen Sie zu `/usr/lib/Acronis/AccountServer`.
3. Stellen Sie sicher, dass Sie Schreibrechte für die Datei `AccountServer.zip` haben.
4. [Optional] Erstellen Sie eine Backup-Kopie der Datei `AccountServer.zip`.
5. Gehen Sie zu `/usr/lib/Acronis/AccountServer/static/locale`.

6. Entpacken Sie die JSON-Datei, die der Sprache entspricht, die Sie in der Cyber Protect-Webkonsole verwenden. Wenn Sie beispielsweise Englisch verwenden, müssen Sie die Datei `en.json` entpacken.
7. Öffnen Sie die entpackte Datei, um diese zu bearbeiten.
8. Wechseln Sie in die nachfolgende Zeile und fügen Sie an deren Ende ein Komma ein:

   ```
   "APP_LOGINFORM_LOGIN_BUTTON": "Log in",
   ```

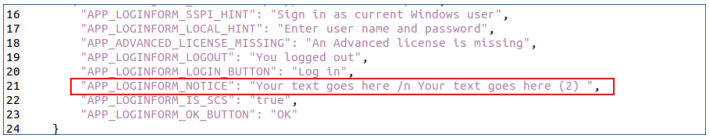
9. Fügen Sie unter der Zeile `"APP_LOGINFORM_LOGIN_BUTTON": "Log in"` folgende Zeilen ein:

   ```
   "APP_LOGINFORM_NOTICE": "<Type your custom message here>",
   ```

   ```
   "APP_LOGINFORM_IS_SCS": "true",
   ```

   ```
   "APP_LOGINFORM_OK_BUTTON": "OK"
   ```

   Zum Beispiel:

10. Speichern Sie die Änderungen und platzieren Sie die bearbeitete JSON-Datei wieder im Verzeichnis `/usr/lib/Acronis/AccountServer/static/locale`.
11. Starten Sie den **Acronis Service Manager Service** neu (wie im Abschnitt '"So können Sie den Acronis Service Manager Service neu starten" (S. 209)' beschrieben).

# SSL-Zertifikatseinstellungen

Dieser Abschnitt beschreibt, wie Sie:

- Einen Protection Agent konfigurieren können, der ein selbstsigniertes SSL-Zertifikat verwendet, das vom Management Server generiert wurde.
- Das selbstsignierte SSL-Zertifikat, das vom Management Server generierte wurde, zu einem Zertifikat ändern können, das von einer vertrauenswürdigen Zertifizierungsstelle (wie GoDaddy, Comodo oder GlobalSign) ausgestellt wurde. Wenn Sie dies tun, wird das vom Management Server verwendet Zertifikat, auf jeder Maschine als vertrauenswürdig behandelt. Daher erscheint keine Webbrowser-Sicherheitswarnung, wenn Sie sich per HTTPS-Protokoll an der Cyber Protect Webkonsole anmelden.

Sie können Sie den Management Server optional so konfigurieren, dass er den Zugriff auf die Cyber Protect Webkonsole per HTTP verbietet – und alle Benutzer auf HTTPS umgeleitet werden.

## Ein selbstsigniertes Zertifikat verwenden

***So können Sie einen Protection Agent in Windows konfigurieren***

1. Öffnen Sie auf der Maschine mit dem Agenten den Registrierungs-Editor.
2. Suchen Sie folgenden Registry-Schlüssel: **HKEY_LOCAL_ MACHINE\Software\Acronis\BackupAndRecovery\Settings\CurlOptions.**
3. Legen Sie für den **VerifyPeer**-Wert **0** fest.
4. Überprüfen Sie, dass der **VerifyHost**-Wert mit **0** festgelegt ist.
5. Starten Sie den Managed Machine Service (MMS) neu:
   a. Klicken Sie im **Start**-Menü auf **Ausführen** und geben Sie Folgendes ein: **cmd**
   b. Klicken Sie auf **OK**.
   c. Führen Sie folgende Befehle aus:

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

***So können Sie einen Protection Agent in Linux konfigurieren***

1. Öffnen Sie auf der Maschine mit dem Agenten die Datei **/etc/Acronis/BackupAndRecovery.config** zur Bearbeitung**.**
2. Gehen Sie zum Schlüssel **CurlOptions** und legen Sie den Wert für **VerifyPeer** auf **0** fest. Überprüfen Sie, dass der Wert für **VerifyHost** mit **0** festgelegt ist.
3. Speichern Sie Ihre vorgenommenen Änderungen.
4. Starten Sie den Managed Machine Service (MMS) neu, indem Sie folgenden Befehl in einem beliebigen Verzeichnis ausführen:

```
sudo service acronis_mms restart
```

***So können Sie einen Protection Agent in macOS konfigurieren***

1. Stoppen Sie auf der Maschine mit dem Agenten den Managed Machine Service (MMS):
   a. Gehen Sie zu **Programme** –> **Dienstprogramme** –> **Terminal**
   b. Führen Sie folgenden Befehl aus:

```
sudo launchctl stop acronis_mms
```

2. Öffnen Sie die Datei **/Library/Application Support/Acronis/Registry/BackupAndRecovery.config** zur Bearbeitung.
3. Gehen Sie zum Schlüssel **CurlOptions** und legen Sie den Wert für **VerifyPeer** auf **0** fest. Überprüfen Sie, dass der Wert für **VerifyHost** mit **0** festgelegt ist.
4. Speichern Sie Ihre vorgenommenen Änderungen.
5. Starten Sie den Managed Machine Service (MMS), indem Sie folgenden Befehl in Terminal ausführen:

```
sudo launchctl starts acronis_mms
```

## Ein von einer vertrauenswürdigen Zertifizierungsstelle ausgestelltes Zertifikat verwenden

***So können Sie die SSL-Zertifikatseinstellungen konfigurieren***

1. Stellen Sie sicher, dass Sie Folgendes haben:

| Wenn Sie Zertifikats- und Schlüsseldateien verwenden | Wenn Sie eine PFX-Datei verwenden |
|---|---|
| Die Zertifikatsdatei (im .pem-Format) | Die PFX-Datei |
| Die Datei mit dem privaten Schlüssel für das Zertifikat (üblicherweise im .key-Format) | |
| Das Kennwort für den privaten Schlüssel (wenn der Schlüssel kennwortgeschützt ist) | Das Kennwort für die PFX-Datei, wenn die Datei kennwortgeschützt ist |

2. Kopieren Sie die Dateien zu der Maschine, die den Management Server ausführt.
3. Öffnen Sie auf dieser Maschine die nachfolgende Konfigurationsdatei in einem Text-Editor:
   - Unter Windows: `%ProgramData%\Acronis\ApiGateway\api_gateway.json`
   - Unter Linux: `/var/lib/Acronis/ApiGateway/api_gateway.json`
4. Suchen Sie den folgenden Abschnitt:

```
"tls": {
    "cert_file": "cert.pem",
    "key_file": "key.pem",
    "passphrase": "",
```

5. Spezifizieren Sie zwischen den Anführungszeichen in der Zeile `"cert_file"` den vollständigen Pfad zur Zertifikatsdatei oder der PFX-Datei.

   Zum Beispiel:

| Betriebssystem | Wenn Sie ein Zertifikat und ein Schlüsselpaar verwenden | Wenn Sie eine .pfx-Datei verwenden |
|---|---|---|
| Windows (beachten Sie die nach vorne geneigten Schrägstriche) | `"cert_file": "C:/certificate/local-domain.ams.pem"` | `"cert_file": "C:/certificate/local-domain.ams.pfx"` |
| Linux | `"cert_file": "/home/user/local-domain.ams.pem"` | `"cert_file": "/home/user/local-domain.ams.pfx"` |

6. Spezifizieren Sie zwischen den Anführungszeichen in der Zeile `"key_file"` den vollständigen Pfad zur privaten Schlüsseldatei oder derjenigen PFX-Datei, die den Zertifikatsschlüssel enthält.
   Normalerweise enthält eine PFX-Datei sowohl das Zertifikat als auch dessen Schlüssel. Spezifizieren Sie in diesem Fall in der Zeile `"key_file"` denselben Pfad wie im vorherigen Schritt.
   Zum Beispiel:

| Betriebssystem | Wenn Sie ein Zertifikat und ein Schlüsselpaar verwenden | Wenn Sie eine .pfx-Datei verwenden |
|---|---|---|
| Windows (beachten Sie die nach vorne geneigten Schrägstriche) | `"key_file": "C:/certificate/private.key"` | `"cert_file": "C:/certificate/local-domain.ams.pfx"` |
| Linux | `"key_file": "/home/user/private.key"` | `"cert_file": "/home/user/local-domain.ams.pfx"` |

7. [Optional] Wenn der private Schlüssel oder die PFX-Datei kennwortgeschützt ist, müssen Sie in der Zeile `"passphrase"` das Kennwort zwischen den Anführungszeichen spezifizieren.
   Beispiel: `"passphrase": "mein Kennwort"`

   **Hinweis**
   Falls die Zeile `"passphrase": ""`, in Ihrer `api_gateway.json`-Konfigurationsdatei fehlt, müssen Sie diese manuell hinzufügen.
   Beispiel:

```
"tls": {
    "cert_file": "cert.pem",
    "key_file": "key.pem",
    "passphrase": "my password",
}
```

8. Speichern Sie die Datei `api_gateway.json`.

   **Wichtig**
   Gehen Sie vorsichtig vor und löschen Sie nicht versehentlich Kommas, Klammern und Anführungszeichen in der Konfigurationsdatei.

9. Starten Sie wie nachfolgend beschrieben den Acronis Service Manager Service neu.

***So können Sie den Acronis Service Manager Service neu starten***

***Unter Windows:***

1. Klicken Sie im **Start**-Menü auf **Ausführen** und geben Sie ein: **cmd**
2. Klicken Sie auf **OK**.
3. Führen Sie folgende Befehle aus:

```
net stop asm
net start asm
```

***Unter Linux:***

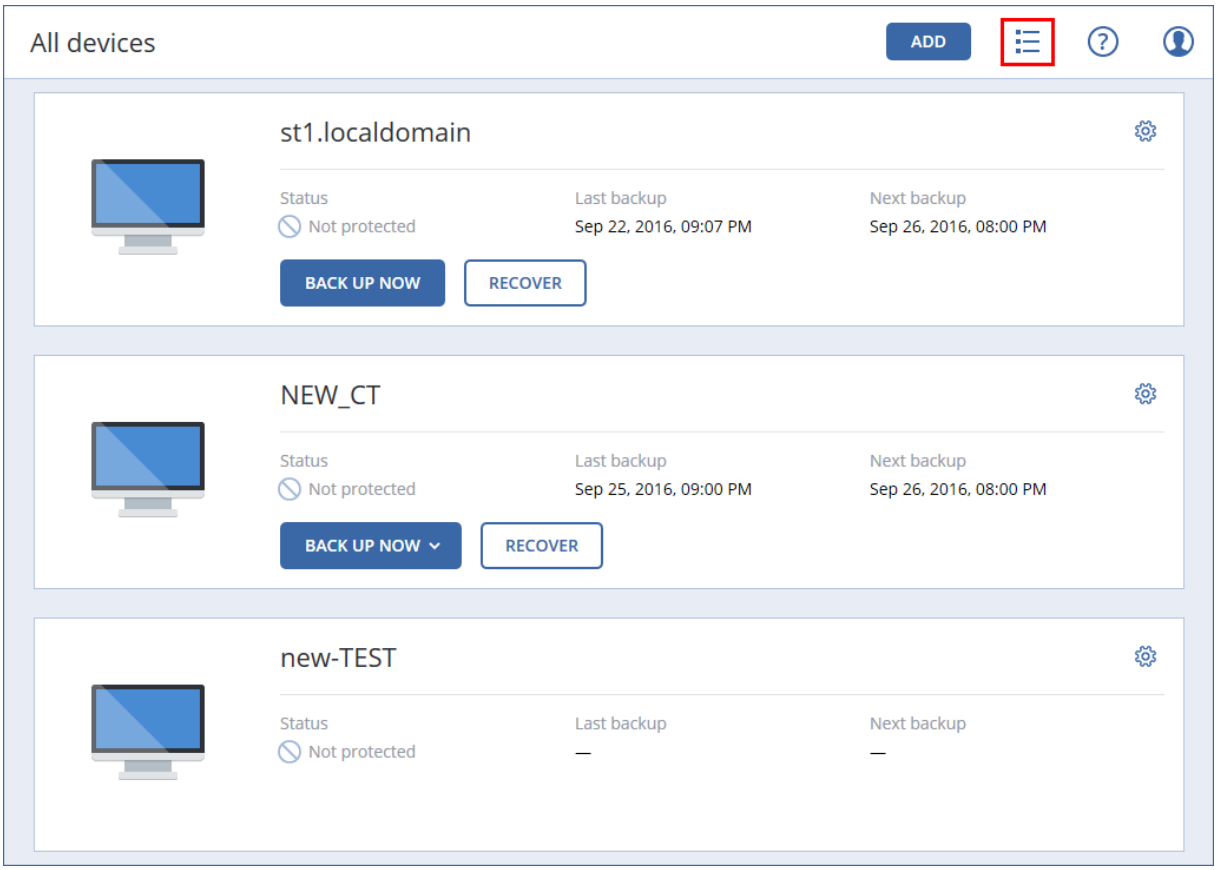
1. Öffnen Sie die Applikation **Terminal**.
2. Führen Sie folgenden Befehl (in einem beliebigen Verzeichnis) aus:

```
sudo service acronis_asm restart
```

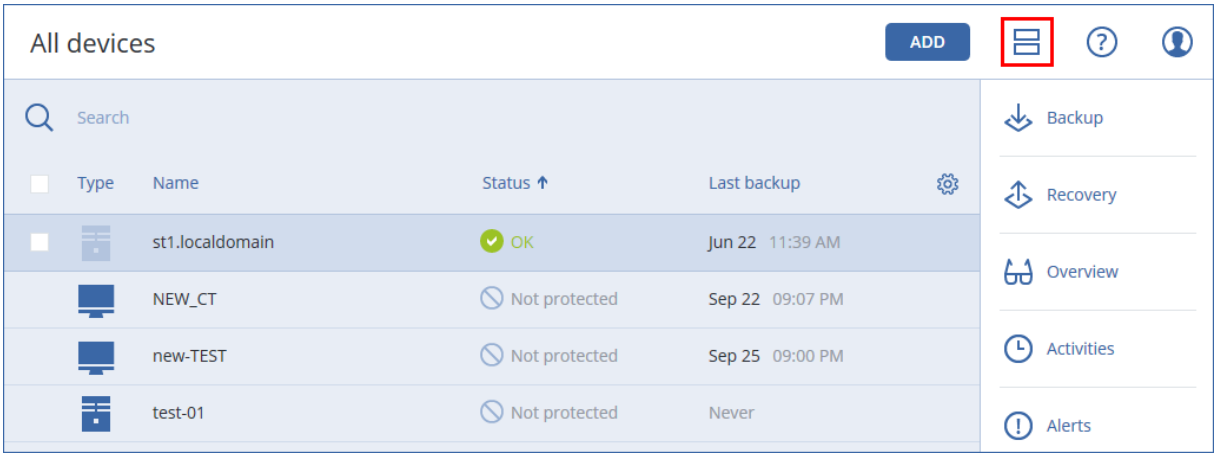
# Die Ansichten der Cyber Protect Webkonsole

Die Cyber Protect Webkonsole hat zwei Ansichten: eine einfache Ansicht und eine Tabellenansicht. Um zwischen den Ansichten umzuschalten, klicken Sie in der oberen rechten Ecke auf das entsprechende Symbol.

Die einfache Ansicht unterstützt lediglich eine kleine Anzahl von Maschinen.




Bei einer größeren Anzahl von Maschinen wird automatisch die Tabellenansicht aktiviert.




Beide Ansichten stellen ansonsten dieselben Funktionen und Operationen bereit. In diesem Dokument wird die Tabellenansicht verwendet, um den Zugriff auf die Operationen zu beschreiben.

Wenn eine Maschine online oder offline geht, dauert es einige Zeit, bis sich ihr Status in der Cyber Protect-Webkonsole ändert.

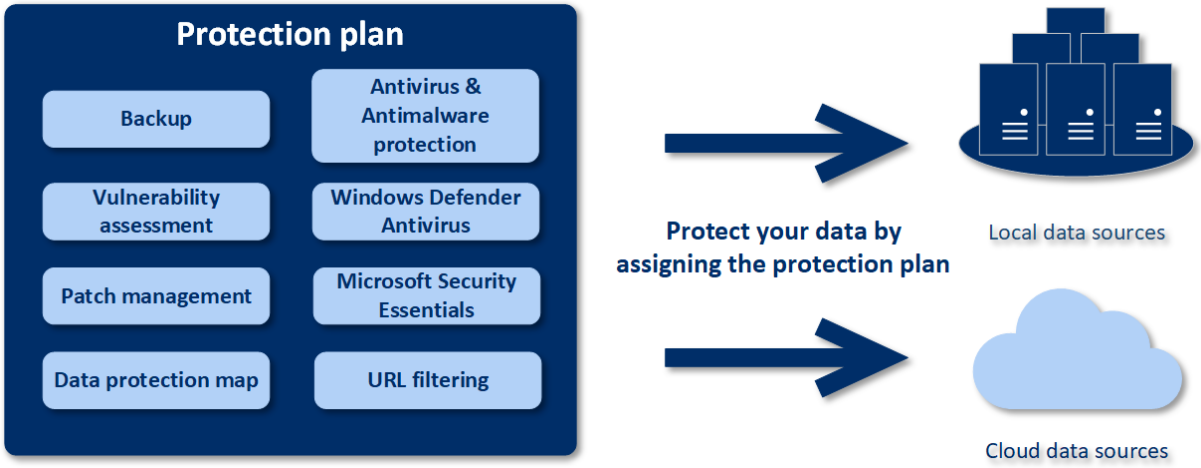
Der Maschinenstatus wird jede Minute überprüft. Wenn der auf dieser Maschine installierte Agent keine Daten überträgt und bei fünf aufeinanderfolgenden Prüfungen keine Antwort gegeben hat, wird die Maschine als offline angezeigt. Die Maschine wird wieder als online angezeigt, wenn sie auf einen Status-Check antwortet oder mit einer Datenübertragung beginnt.

# Schutzplan und Module

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

- Backup – ermöglicht Ihnen, Ihre Datenquellen zu einem lokalen Storage oder Cloud Storage zu sichern.
- Antivirus & Antimalware Protection – ermöglicht Ihnen, Ihre Maschinen mit der integrierten Antimalware-Lösung zu überprüfen.
- URL-Filterung – 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 – ermöglicht Ihnen, die Einstellungen des Windows Defenders zu verwalten, um Ihre Umgebung zu schützen.
- Microsoft Security Essentials – ermöglicht Ihnen, die Einstellungen der Microsoft Security Essentials zu verwalten, um Ihre Umgebung zu schützen.
- Schwachstellenbewertung – 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 – 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 – 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.



# 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.

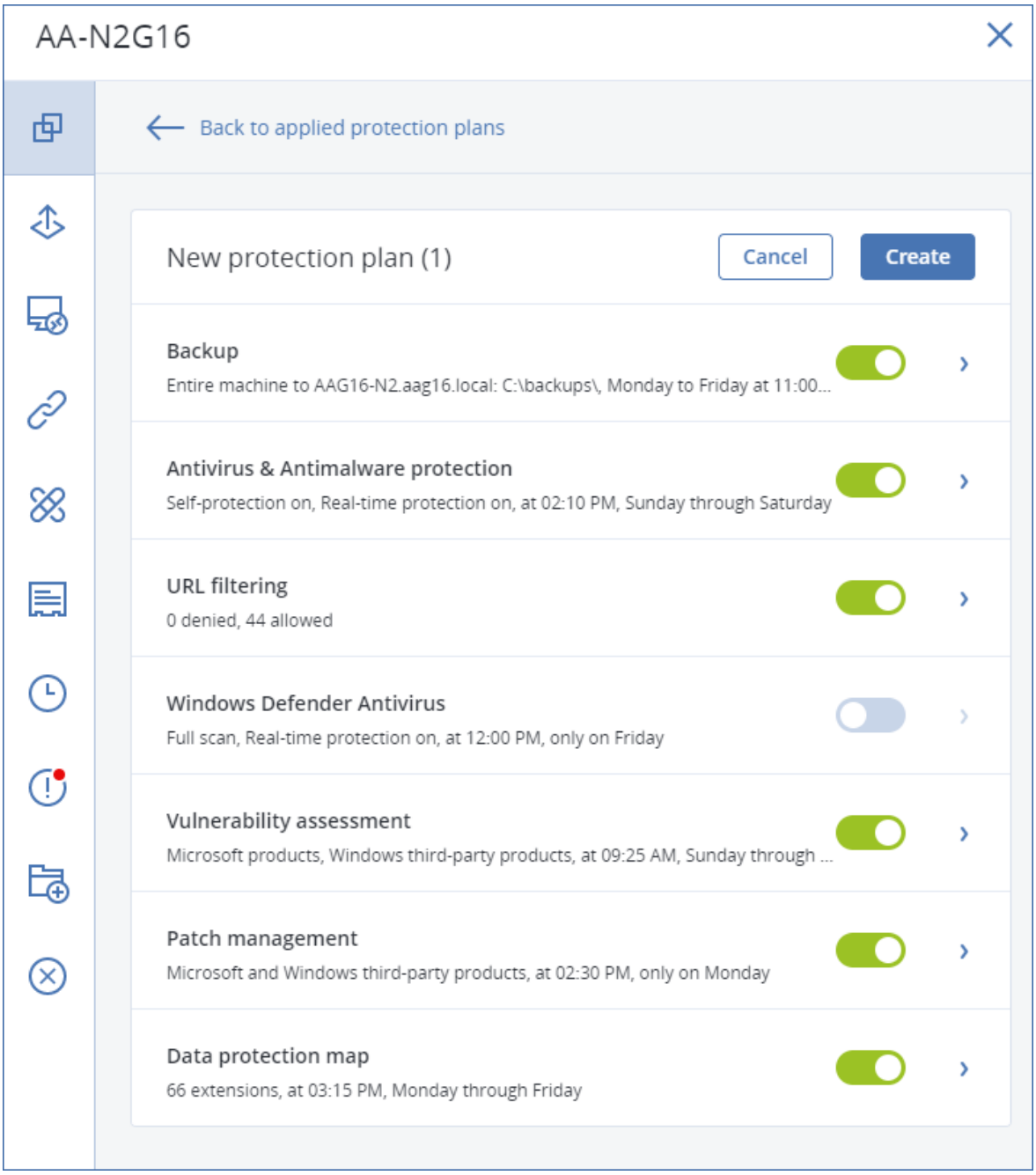
Ein Schutzplan kann auf zwei Arten erstellt werden:

- 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.

Betrachten wir die erste Möglichkeit.

***So können Sie den ersten Schutzplan erstellen***

1. Gehen Sie in der Cyber Protect Webkonsole 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 Schutzplan-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.

# 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, in dem nur das Backup-Modul aktiviert ist. Die Schutzpläne können nur dann kombiniert werden, wenn Sie Module haben, deren Funktionalitäten sich nicht überschneiden. Wenn die gleichen Module in mehr als einem Schutzplan aktiviert sind, müssen Sie die entstandenen 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 dann die vorhandene Quota und weisen Sie eine neue zu.

## Aktionen mit Schutzplänen

Weitere Informationen über die Erstellung eines Schutzplans finden Sie im Abschnitt 'Einen Schutzplan erstellen'.

### Verfügbare Aktionen für einen Schutzplan

Sie können die folgenden Aktionen mit einem Schutzplan durchführen:

- Einen Plan umbenennen
- Module (de)aktivieren und alle Modul-Einstellungen bearbeiten
- Einen Plan (de)aktivieren

  Ein deaktivierter Plan wird auf einem Gerät, auf dem er angewendet wurde, nicht ausgeführt.

  Diese Aktion ist nützlich für Administratoren, die beabsichtigen, dasselbe Gerät später mit demselben Plan zu schützen. Der Plan wird nicht vom Gerät widerrufen und der Administrator muss den Plan nur wieder aktivieren, um den Schutz wiederherzustellen.
- Einen Plan auf Geräte oder eine Gruppe von Geräten anwenden
- Einen Plan von einem Gerät widerrufen

  Ein Plan zu widerrufen bedeutet, dass dieser nicht mehr auf ein Gerät angewendet wird.

  Diese Aktion ist nützlich für Administratoren, die beabsichtigen, dasselbe Gerät nicht so schnell wieder mit demselben Plan schützen müssen/wollen. Um den Schutz durch einen widerrufenen Plan wiederherstellen zu können, muss der Administrator den Namen dieses Plans kennen, ihn aus der Liste der verfügbaren Pläne auswählen und ihn dann erneut auf das gewünschte Gerät anwenden.
- Einen Plan importieren/exportieren

**Hinweis**
Sie können nur Schutzpläne importieren, die in Acronis Cyber Protect 15.0 erstellt wurden. Schutzpläne, die mit älteren Versionen erstellt wurden, sind mit Acronis Cyber Protect 15 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 die gewünschte Schutzfunktion aus und klicken Sie dann **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.

# 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.

**Hinweis**
Wenn bei lokalen Bereitstellungen nur Standard-Lizenzen auf dem Management Server vorhanden sind, kann ein Schutzplan nicht auf mehrere physische Maschinen angewendet werden. Jede physische Maschine muss ihren eigenen Schutzplan haben.

***So können Sie den ersten Schutzplan mit aktiviertem Backup-Modul erstellen***

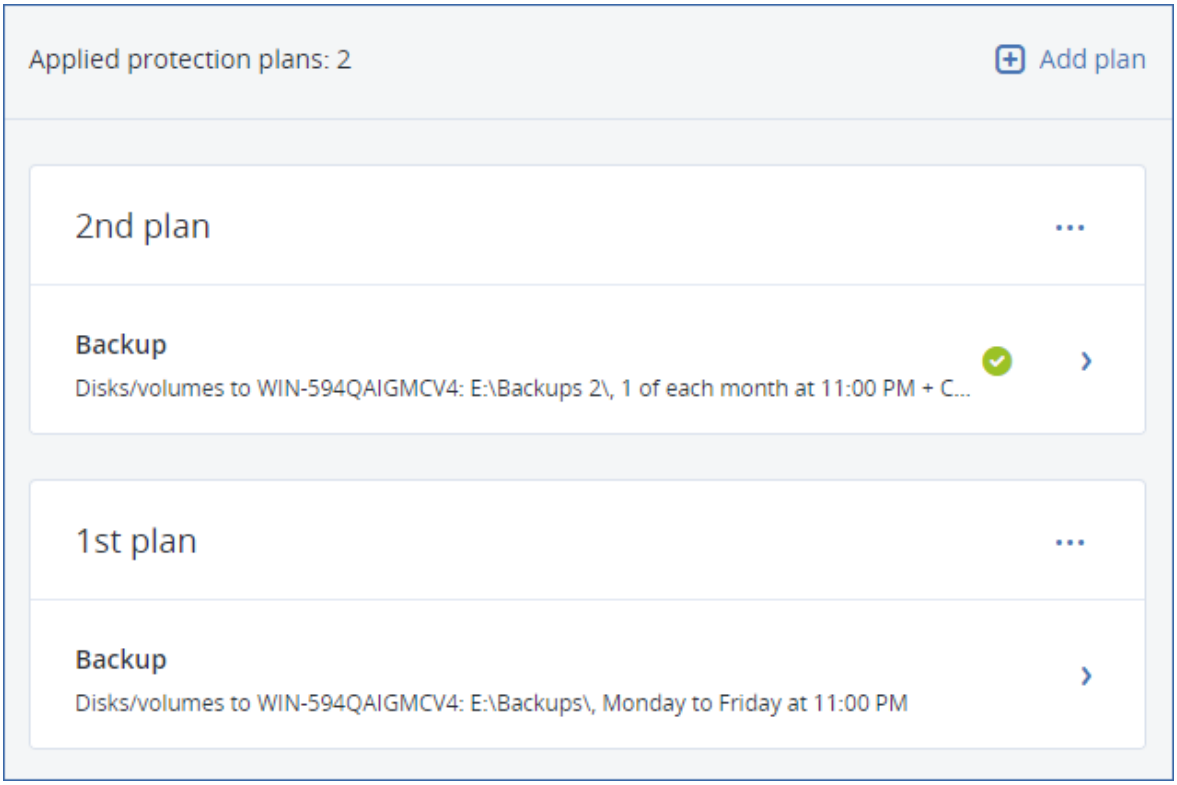
1. Wählen Sie Maschinen, die Sie per Backup sichern wollen.
2. Klicken Sie auf den Befehl **Schützen**.
   Die Software zeigt die Schutzpläne an, die auf die Maschine angewendet werden. Wenn der Maschine noch keine Pläne zugewiesen wurden, wird Ihnen der Standard-Schutzplan angezeigt, der angewendet 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 auf den entsprechenden Schutzplan-Fensterbereich.
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**.

# Backup-Modul-Spickzettel

**Wichtig**
Einige der in diesem Abschnitt beschriebenen Funktionen stehen nur bei On-Premise-Bereitstellungen zur Verfügung.

Die nachfolgende Tabelle fasst alle verfügbaren Backup-Modul-Parameter zusammen. Verwenden Sie diese Tabelle, um einen Schutzplan zu erstellen, der am besten zu Ihren Bedürfnissen passt.

| BACKUP-QUELLE | Elemente für das Backup<br>Auswahlmethoden | Backup-Ziel | Planung<br>Backup-Schemata<br>(nicht für die | Aufbewahrungsdauer |
|---|---|---|---|---|

| | | | Cloud) | |
|---|---|---|---|---|
| Laufwerke/Volumes (physische Maschinen) | Direkte Auswahl<br>Richtlinienregeln<br>Dateifilter | Cloud<br>Lokaler Ordner<br>Netzwerkordner<br>SFTP-Server*<br>NFS*<br>Secure Zone*<br>Verwalteter Speicherort*<br>Bandgerät* | Nur inkrementell (Einzeldatei)*<br>Nur vollständig<br>Wöchentlich vollständig, täglich inkrementell<br>Monatlich vollständig, wöchentlich differentiell, täglich inkrementell (GVS)<br>Benutzerdefiniert (V-D-I) | Nach Backup-Alter (einzelne Regel/per Backup-Set)<br>Nach Backup-Anzahl<br>Nach der Gesamtgröße der Backups*<br>Unbegrenzt aufbewahren |
| Laufwerke/Volumes (virtuelle Maschinen) | Richtlinienregeln<br>Dateifilter | Cloud<br>Lokaler Ordner<br>Netzwerkordner<br>SFTP-Server*<br>NFS*<br>Verwalteter Speicherort*<br>Bandgerät* | | |
| Dateien (nur physische Maschinen) | Direkte Auswahl<br>Richtlinienregeln<br>Dateifilter | Cloud<br>Lokaler Ordner<br>Netzwerkordner<br>SFTP-Server*<br>NFS*<br>Secure Zone*<br>Verwalteter Speicherort*<br>Bandgerät | Nur vollständig<br>Wöchentlich vollständig, täglich inkrementell<br>Monatlich vollständig, wöchentlich differentiell, täglich inkrementell (GVS)<br>Nur inkrementell (Einzeldatei)* | |

| | | | | |
|---|---|---|---|---|
| ESXi-Konfiguration | Direkte Auswahl | Lokaler Ordner<br>Netzwerkordner<br>SFTP-Server<br>NFS* | Benutzerdefiniert (V-D-I) | |
| Systemzustand (nur bei Cloud-Bereitstellungen) | Direkte Auswahl | Cloud<br>Lokaler Ordner<br>Netzwerkordner | Nur vollständig<br>Wöchentlich vollständig, täglich inkrementell<br>Benutzerdefiniert (V-I) | |
| SQL-Datenbanken | Direkte Auswahl | Cloud<br>Lokaler Ordner<br>Netzwerkordner<br>Verwalteter Speicherort*<br>Bandgerät | | |
| Exchange-Datenbanken | Direkte Auswahl | | | |
| Exchange-Postfächer | Direkte Auswahl | Cloud<br>Lokaler Ordner<br>Netzwerkordner<br>Verwalteter Speicherort* | Nur inkrementell (Einzeldatei) | |
| Microsoft 365-Postfächer | Direkte Auswahl | | | Nach Backup-Alter (einzelne Regel/per Backup-Set)<br>Nach Backup-Anzahl<br>Unbegrenzt aufbewahren |

* Siehe die unteren Einschränkungen.

# Einschränkungen

## SFTP-Server und Bandgerät

- Diese Speicherorte können nicht als Backup-Ziel für Maschinen verwendet werden, die unter macOS laufen.
- Diese Speicherorte können nicht als Ziel für applikationskonformen Backups verwendet werden.
- Das Backup-Schema **Nur inkrementell (Einzeldatei)** ist nicht verfügbar, wenn diese Speicherorte als Backup-Ziel verwendet werden.
- Die Aufbewahrungsregel **Nach der Gesamtgröße der Backups** ist für diese Speicherorte nicht verfügbar.

## NFS

- Backups zu NFS-Freigaben sind unter Windows nicht verfügbar.
- Das Backup-Schema **Nur inkrementell (Einzeldatei)** für Dateien (physische Maschinen) ist nicht verfügbar, wenn Sie Backups zu NFS-Freigaben erstellen.

## Einer Secure Zone

- Eine Secure Zone kann nicht auf einem Mac erstellt werden.

## Verwalteter Speicherort

- Ein verwalteter Speicherort mit aktivierter Deduplizierungs- oder Verschlüsselungsfunktion kann nicht als Backup-Ziel verwendet werden:
  - Wenn das Backup-Schema auf **Nur inkrementell (Einzeldatei)** festgelegt ist
  - Wenn das Backup-Format auf **Version 12** festgelegt ist
  - Für Laufwerk-Backups von Maschinen, die unter macOS laufen
  - Für Backups von Exchange-Postfächern und Microsoft 365-Postfächern.
- Die Aufbewahrungsregel **Nach der Gesamtgröße der Backups** ist für einen verwalteten Speicherort mit aktivierter Deduplizierungsfunktion nicht verfügbar.

## Nur inkrementell (Einzeldatei)

- Das Backup-Schema **Nur inkrementell (Einzeldatei)** ist nicht verfügbar, wenn ein SFTP-Server oder ein Bandgerät als Backup-Ziel verwendet wird.
- Das Backup-Schema **Nur inkrementell (Einzeldatei)** für Dateien (physische Maschinen) ist nur dann verfügbar, wenn der primäre Backup-Speicherort die Acronis Cloud ist.

### Nach der Gesamtgröße der Backups

- Die Aufbewahrungsregel **Nach der Gesamtgröße der Backups** ist nicht verfügbar:
  - Wenn das Backup-Schema auf **Nur inkrementell (Einzeldatei)** festgelegt ist
  - Wenn ein SFTP-Server, ein Bandgerät oder ein verwalteter Speicherort mit aktivierter Deduplizierungsfunktion als Backup-Ziel verwendet wird.

# Daten für ein Backup auswählen

## Eine komplette Maschine auswählen

Unter dem 'Backup einer kompletten Maschine' versteht man ein Backup, das alle festeingebauten Laufwerke (interne „Nicht-Wechsellaufwerke“) der betreffenden Maschine umfasst.

Wenn Sie ein solches Backup konfigurieren wollen, müssen Sie unter **Backup-Quelle** die Option **Komplette Maschine**auswählen.

**Wichtig**
Externe Laufwerke (wie USB-Sticks oder USB-Festplatten) werden nicht in ein Backup der **Kompletten Maschine** einbezogen. Wenn Sie solche Laufwerke sichern wollen, müssen Sie ein Backup vom Typ **Laufwerke/Volumes** konfigurieren. Weitere Informationen über Laufwerk-Backups finden Sie im Abschnitt '"Laufwerke/Volumes auswählen" (S. 226)'.

## 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.

**Hinweis**
Das OneDrive-Stammverzeichnis wird standardmäßig von Backup-Aktionen ausgeschlossen. Wenn Sie jedoch festlegen, dass bestimmte OneDrive-Dateien und -Ordner gesichert werden sollen, dann werden diese auch in das Backup aufgenommen. Dateien, die nicht auf dem Gerät vorhanden sind, werden im Archiv ungültige Inhalte haben.

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 von einem Laufwerk-Backup auszuschließen.

## Direkte Auswahl

Eine direkte Auswahl ist nur für physische Maschinen verfügbar. Um auf einer virtuellen Maschine eine direkte Auswahl von Laufwerken/Volumes zu ermöglichen, müssen Sie den Protection Agenten im Gastbetriebssystem der VM installieren.

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

- `[Alle 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.
- `[Fest eingebaute Volumes (physische Maschinen)]` – 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 Boot- und System-Volumes aus. Diese Kombination entspricht dem minimalen Datensatz, der für die Wiederherstellbarkeit eines Betriebssystems aus einem Backup notwendig ist.

- `[BOOT+SYSTEM-LAUFWERK (physische Maschinen)]` – wählt alle Volumes des Laufwerks aus, auf denen sich die Boot- und System-Volumes befinden. Wenn sich das Boot- und das System-Volume nicht auf demselben Speicherort befinden, wird nichts ausgewählt. Diese Regel gilt nur für physische Maschinen.
- `[Laufwerk 1]` – wählt das erste Laufwerk der Maschine aus, einschließlich aller Volumes auf diesem Laufwerk. Um ein anderes Laufwerk auszuwählen, müssen Sie nur die entsprechende Laufwerksnummer eingeben.

### Regeln für Linux

- `/dev/hda1` – wählt das erste Volume auf dem ersten IDE-Laufwerk aus.
- `/dev/sda1` – wählt das erste Volume auf dem ersten SCSI-Laufwerk aus.
- `/dev/md1` – wählt das erste Software-RAID-Laufwerk aus.

Verwenden Sie zur Auswahl anderer Basis-Volumes den Parameter '`/dev/xdyN`', wobei:

- 'x' dem Laufwerkstyp entspricht
- 'y' der Laufwerksnummer entspricht ('a' für das erste Laufwerk, 'b' für das zweite usw.)
- 'N' der Volume-Nummer entspricht.

Wenn Sie ein logisches Volume auswählen wollen, müssen Sie dessen Pfad so spezifizieren, wie er nach dem Ausführen des Befehls `ls /dev/mapper` (unter dem root-Konto) angezeigt wird. Beispiel:

```
[root@localhost ~]# ls /dev/mapper/
control vg_1-lv1 vg_1-lv2
```

Diese Ausgabe zeigt zwei logische Volumes an, **lv1** und **lv2**, die zur Volume-Gruppe **vg_1** gehören. Geben Sie Folgendes ein, um diese Volumes per Backup zu sichern:

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

### Regeln für macOS

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

## Was wird im Backup eines Laufwerks oder Volumes gespeichert?

Ein Laufwerk- bzw. Volume-Backup speichert das **Dateisystem** des entsprechenden Laufwerks bzw. Volumes 'als Ganzes'. Dabei werden auch alle zum Booten des Betriebssystems erforderlichen Informationen eingeschlossen. Aus solchen Backups können Laufwerke oder Volumes komplett wiederhergestellt werden – aber auch einzelne Dateien oder Ordner.

Wenn die Backup-Option '**Sektor-für-Sektor (Raw-Modus)**' aktiviert ist, werden in einem Laufwerk-Backup alle Sektoren des Laufwerks gespeichert. Das Sektor-für-Sektor-Backup kann verwendet

werden, um Laufwerke mit nicht erkannten oder nicht unterstützten Dateisystemen sowie anderen proprietären Datenformaten zu sichern.

### Windows

Ein Volume-Backup speichert alle Dateien und Ordner des gewählten Volumes, unabhängig von ihren Attributen (inkl. versteckter oder System-Dateien), den Boot-Record, die FAT (File Allocation Table) und – sofern vorhanden – auch das Stammverzeichnis (Root) und die Spur Null (Track Zero), inkl. Master Boot Record (MBR).

Ein Laufwerk-Backup speichert alle Volumes des betreffenden Laufwerks (inkl. versteckter Volumes wie Wartungs-Volumes von Herstellern) und die Spur Null (Track Zero) mit dem Master Boot Record (MBR).

Folgende Elemente sind *nicht* in einem Laufwerk- oder Volume-Backup enthalten (und genauso wenig in einem Backup auf Dateiebene):

- Die Auslagerungsdatei (pagefile.sys) und die Datei, die ein Abbild des Hauptspeichers ist, wenn der Computer in den Ruhezustand wechselt (hiberfil.sys). Nach einer Wiederherstellung werden die Dateien an passender Position mit einer Größe von Null erneut erzeugt.
- Wenn das Backup unter dem Betriebssystem durchgeführt wird (und nicht mit einem Boot-Medium oder durch Sicherung von virtuellen Maschinen auf Hypervisor-Ebene):
  - Windows Schattenspeicher (Shadow Storage). Der auf diesen verweisende Pfad wird über den Registry-Wert **VSS Default Provider** bestimmt, der im Registry-Schlüssel **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup** gefunden werden kann. Das bedeutet, dass bei Betriebssystemen ab Windows 7 keine Windows-Systemwiederherstellungspunkte gesichert werden.
  - Wenn die Backup-Option **VSS (Volume Shadow Copy Service)** aktiviert ist, werden alle Dateien und Ordner, die im Registry-Schlüssel **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToSnapshot** spezifiziert sind, nicht per Backup gesichert.

### Linux

Ein Volume-Backup speichert alle Dateien und Verzeichnisse des gewählten Laufwerkes (unabhängig von ihren Attributen), einen Boot-Record und den Dateisystem-Super-Block.

Ein Laufwerk-Backup speichert alle Volumes des Laufwerks, inkl. der Spur Null (Track Zero) mit dem 'Master Boot Record' (MBR).

### Mac

Ein Laufwerk oder Volume-Backup speichert alle Dateien und Verzeichnisse des ausgewählten Laufwerks oder Volumes – plus einer Beschreibung des Volume-Layouts.

Folgende Elemente werden dabei ausgeschlossen:

- System-Metadaten, wie etwa das Dateisystem-Journal und der Spotlight-Index.
- Der Papierkorb
- Time Machine-Backups

Laufwerke und Volumes auf einem Mac werden physisch auf Dateiebene gesichert. Bare Metal Recovery (Wiederherstellung auf fabrikneuer Hardware) von Laufwerk- und Volume-Backups ist möglich, aber der Backup-Modus 'Sektor-für-Sektor' ist nicht verfügbar.

## Dateien/Verzeichnisse auswählen

Datei-Backups sind für physische und virtuelle Maschinen verfügbar, die von einem Agenten gesichert werden, der im Gastbetriebssystem installiert ist.

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.

**Hinweis**
Das OneDrive-Stammverzeichnis wird standardmäßig von Backup-Aktionen ausgeschlossen. Wenn Sie jedoch festlegen, dass bestimmte OneDrive-Dateien und -Ordner gesichert werden sollen, dann werden diese auch in das Backup aufgenommen. Dateien, die nicht auf dem Gerät vorhanden sind, werden im Archiv ungültige Inhalte haben.

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 noch verfeinern.

### Direkte Auswahl

1. Wählen Sie bei **Backup-Quelle** die Option **Dateien/Ordner**.
2. Klicken Sie auf **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. 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**.

### Auswahlregeln für Windows

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

- `/usr` – wählt das Verzeichnis für alle benutzerbezogenen Programme aus.
- `/etc` – wählt das Verzeichnis der Systemkonfigurationsdateien aus.

- Vorlagen:
  - `[Ordner 'Alle Benutzerprofile']` – 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.
- Vorlagen:
  - `[Ordner 'Alle Benutzerprofile']` – wählt **/Users** aus. Dies ist der Ordner, in dem sich standardmäßig alle Benutzerprofile befinden.

Beispiele:

- Um **datei.txt** auf Ihrem Desktop sichern zu können, 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.

## Einen Systemzustand auswählen

Ein Backup des Systemzustands ist für Maschinen verfügbar, die unter Windows 7 oder höher 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

## 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.
- Wenn Sie ein Backup der ESXi-Konfiguration erstellen wollen, wird der Agent für VMware eine SSH-Verbindung zum ESXi-Host über den TCP-Port 22 herstellen. Vergewissern Sie sich, dass diese Verbindung nicht von Ihrer Firewall blockiert wird.
- Sie müssen das Kennwort des 'root'-Kontos auf dem ESXi-Host kennen.

### Einschränkungen

- ESXi-Konfigurations-Backups werden nicht für VMware vSphere 7.0 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 **Backup**.
3. Wählen Sie bei **Backup-Quelle** die Option **ESXi-Konfiguration**.
4. Spezifizieren Sie bei **'root'-Kennwort für ESXi** das Kennwort für das jeweilige 'root'-Konto auf jedem der ausgewählten ESXi-Hosts – oder verwenden Sie dasselbe Kennwort für alle Hosts.

# Kontinuierliche Datensicherung (CDP)

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.

**Hinweis**
Die Funktionen variieren zwischen den verschiedenen Editionen. Einige der in dieser Dokumentation beschriebenen Funktionen sind daher möglicherweise mit Ihrer Lizenz nicht verfügbar. Ausführliche Informationen über die in jeder Edition enthaltenen Funktionen finden Sie im Abschnitt 'Acronis Cyber Protect 15 – Vergleich der Editionen (inkl. Cloud-Bereitstellung)'.

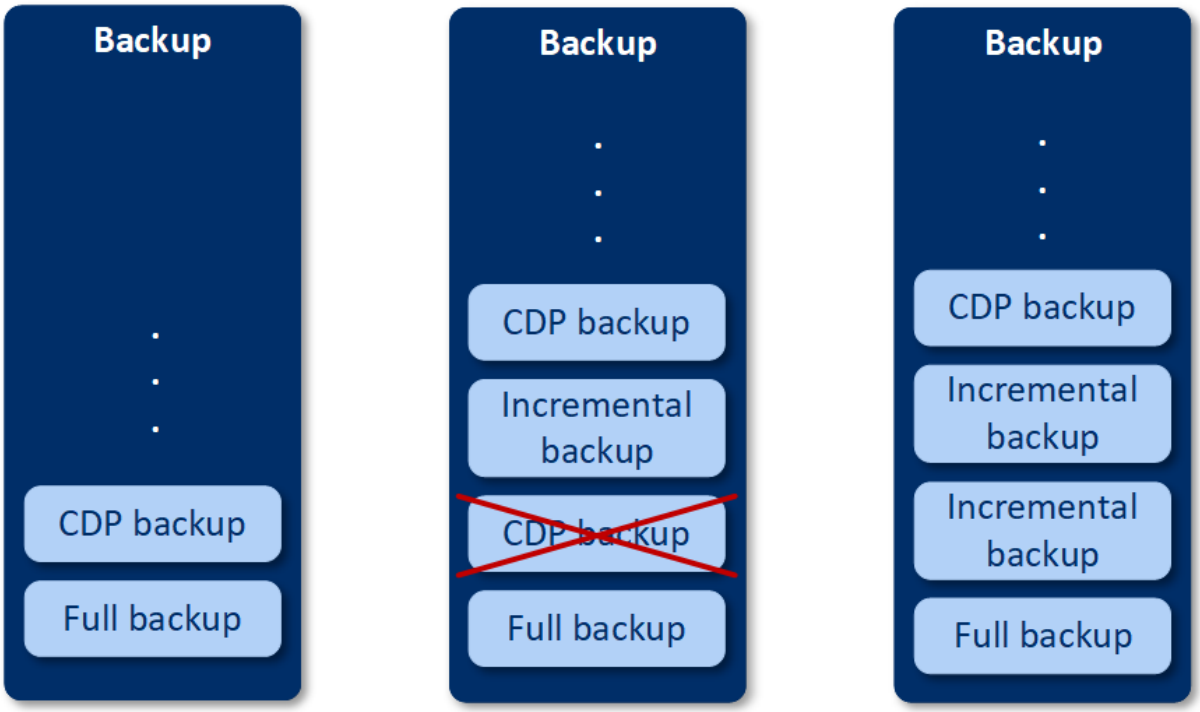
## Und so funktioniert es

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<br>Applikationen können spezifiziert werden (nicht obligatorisch) |

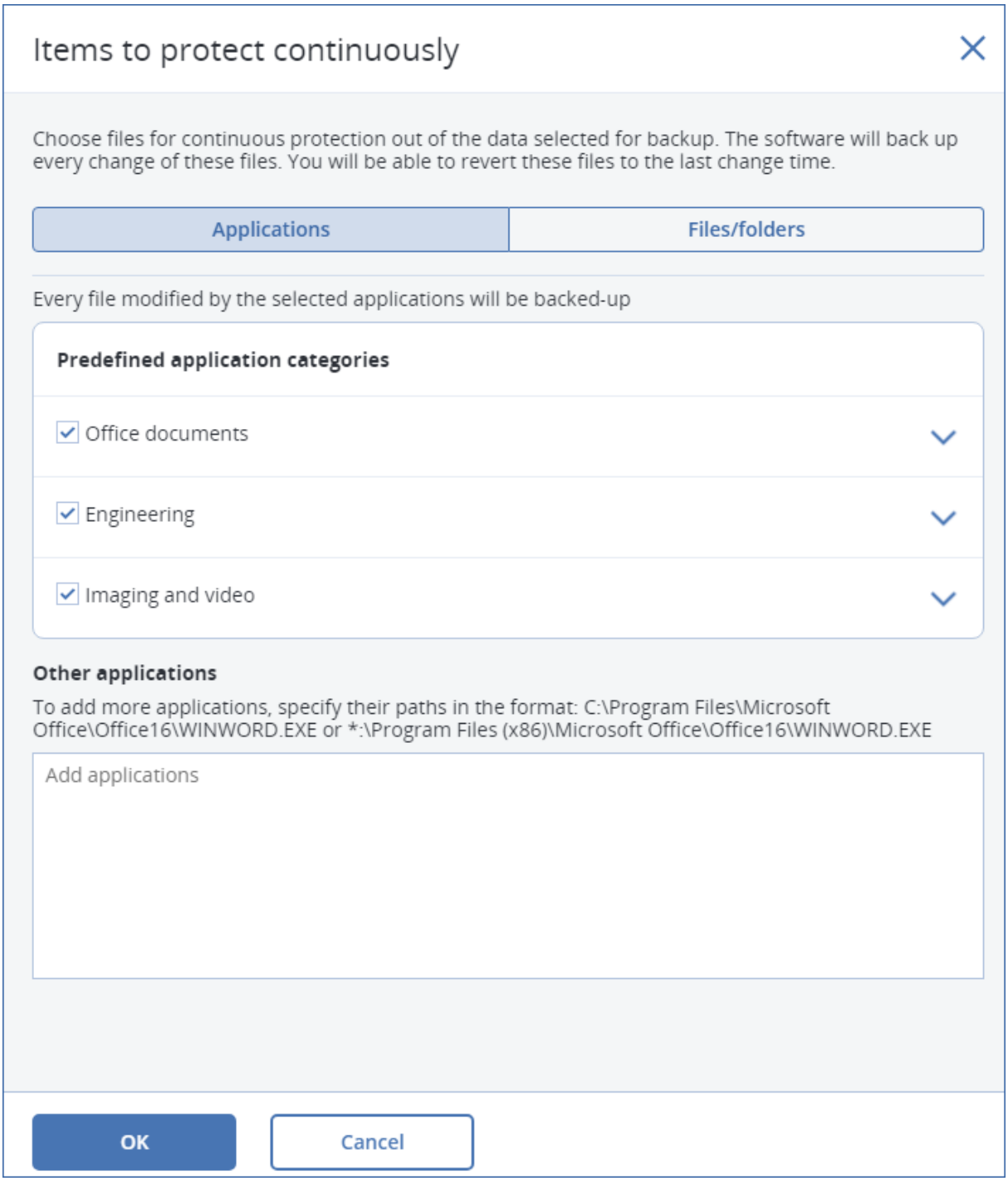
Folgende Backup-Ziele werden für die kontinuierliche Datensicherung (CDP) unterstützt:

- 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 Cyber Protect Webkonsole einen Schutzplan 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:

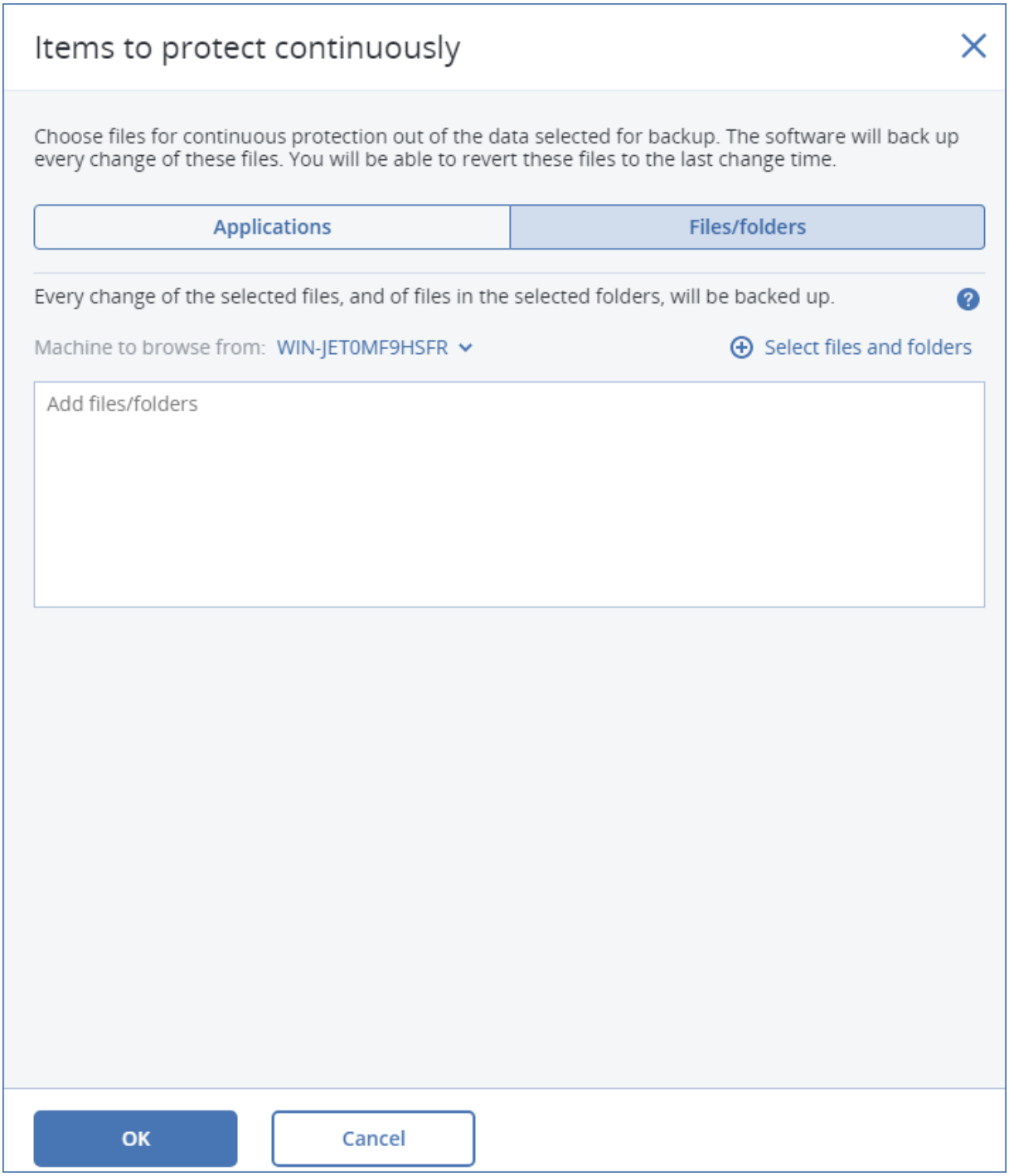
  `C:\Program Files\Microsoft Office\Office16\WINWORD.EXE`

  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.




1. **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**.

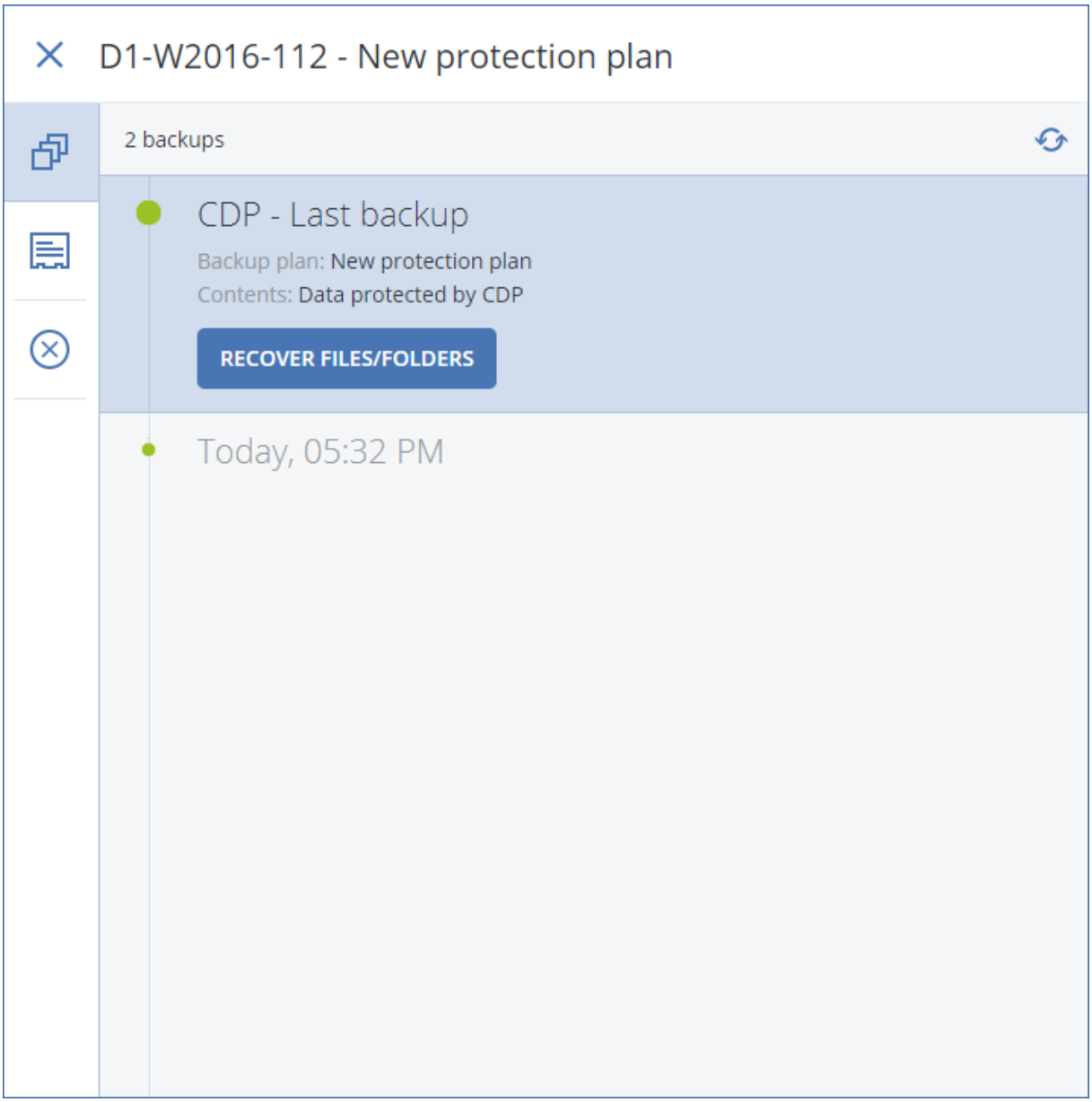
2. Klicken Sie auf **Erstellen**.

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.

# Ein Ziel auswählen

**Wichtig**
Einige der in diesem Abschnitt beschriebenen Funktionen stehen nur bei On-Premise-Bereitstellungen zur Verfügung.

***So können Sie einen Backup-Speicherort auswählen***

1. Klicken Sie auf **Backup-Ziel**:
2. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Wählen Sie einen zuvor bereits verwendeten oder einen vordefinierten Backup-Speicherort aus
   - Klicken Sie auf **Speicherort hinzufügen** und spezifizieren Sie einen neuen Backup-Speicherort.

## Unterstützte Speicherorte

- **Cloud Storage**
  Die Backups werden im Cloud-Datacenter gespeichert.
- **Lokaler 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.
- **Acronis Cyber Infrastructure**

Acronis Cyber Infrastructure kann verwendet werden, um einen hochzuverlässigen Software-Defined-Storage mit integrierter Datenredundanz und automatischen Selbstreparaturfähigkeiten zu erstellen. Der Storage kann als Gateway zur Speicherung von Backups in Microsoft Azure oder in einer der verschiedenen Storage-Lösungen, die mit S3 oder Swift kompatibel sind, konfiguriert werden. Der Storage kann auch das NFS-Backend verwenden. Weitere Informationen dazu finden Sie hier: 'Über Acronis Cyber Infrastructure'.

**Wichtig**
Backups zu Acronis Cyber Infrastructure sind nicht für macOS-Maschinen verfügbar.

- **NFS-Ordner** (auf Maschinen verfügbar, die mit Linux oder macOS laufen)

  Überprüfen Sie, dass auf der Linux-Maschine, auf welcher der Agent für Linux installiert ist, das nfs-utils-Paket 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.

  Ein NFS-Ordner, der per Kennwort geschützt ist, kann nicht als Backup-Ziel verwendet werden.
- **Einer Secure Zone** (verfügbar, falls auf jeder der ausgewählten Maschinen eine verfügbar ist)

  Die 'Einer 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 Einer Secure Zone sowie deren Vorteile und Beschränkungen finden Sie im Abschnitt 'Über die Einer Secure Zone'.
- **SFTP**

  Geben Sie den Namen oder die Adresse des SFTP-Servers ein. Folgende Schreibweisen werden unterstützt:

  `sftp://<server>`

  `sftp://<server>/<ordner>`

  Nach Eingabe der Anmeldedaten können Sie die Ordner des Servers durchsuchen.

  Sie können bei jeder Schreibweise außerdem auch einen Port, Benutzernamen und ein Kennwort angeben:

  `sftp://<server>:<port>/<ordner>`

  `sftp://<benutzername>@<server>:<port>/<ordner>`

  `sftp://<benutzername>:<kennwort>@<server>:<port>/<ordner>`

  Wird keine Port-Nummer spezifiziert, dann wird Port 22 verwendet.

  Benutzer, für die ein SFTP-Zugriff ohne Kennwort konfiguriert wurde, können keine Backups zu einem SFTP-Ziel erstellen.

  Die Erstellung von Backups zu FTP-Servern wird nicht unterstützt.

## Erweiterte Storage-Optionen

- **Per Skript festgelegt** (nur für unter Windows laufende Maschinen)

  Sie können die Backups einer jeden Maschine in einem per Skript festgelegten Ordner speichern lassen. Die Software unterstützt Skripte, die in JScript, VBScript oder Python 3.5 geschrieben sind. Wenn der Schutzplan bereitgestellt wird, führt die Software das Skript auf jeder Maschine aus. Die Skript-Ausgabe für jede Maschine sollte ein Ordnerpfad (lokal oder im Netzwerk) sein. Falls ein entsprechender Ordner nicht existiert, wird er automatisch erstellt (Einschränkung: Skripte, die in Python geschrieben sind, können keine Ordner auf Netzwerkfreigaben erstellen). In der Registerkarte **Backup Storage** wird jeder Ordner als separater Backup-Speicherort angezeigt.

  Wählen Sie bei **Skript-Typ** die Skript-Sprache (**JScript**, **VBScript** oder **Python**). Dann können Sie das Skript importieren, kopieren oder über die Zwischenablage einfügen. Spezifizieren Sie für Netzwerkordner die Zugriffsanmeldedaten mit den Lese-/Schreibberechtigungen.

  Beispiele:

  - Folgendes **JScript**-Skript gibt den Backup-Speicherort für eine Maschine im Format `\\bkpsrv\<Maschinenname>` aus:

    ```
    WScript.Echo("\\\\bkpsrv\\" + WScript.CreateObject
    ("WScript.Network").ComputerName);
    ```

  - Folgendes **JScript**-Skript gibt den Backup-Speicherort als Ordner auf derjenigen Maschine aus, wo das Skript ausgeführt wird:

    ```
    WScript.Echo("C:\\Backup");
    ```

    **Hinweis**
    Bei der Pfadangabe für den Speicherort in diesen Skripten wird zwischen Groß- und Kleinschreibung unterschieden. Daher werden `C:\Backup` und `C:\backup` in der Cyber Protect-Webkonsole als unterschiedliche Speicherorte angezeigt. Sie müsse außerdem auch einen Großbuchstaben für den Laufwerksbuchstaben verwenden.

  - Folgendes **VBScript**-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.

- **Storage Node**

  Ein Storage Node ist ein Server, der zur optimalen Nutzung verschiedener Ressourcen (z.B. Storage-Kapazitäten, Netzwerkbandbreiten oder CPU-Last der Produktionsserver) entwickelt wurde, die zur Sicherung der Unternehmensdaten erforderlich sind. Dieses Ziel wird durch

Organisation und Verwaltung von (verwalteten) Speicherorten erreicht, die als dedizierte Storages für die Backups des Unternehmens dienen.

Sie können einen zuvor bereits erstellten Speicherort auswählen oder einen neuen erstellen, indem Sie auf **Speicherort hinzufügen** –> **Storage Node** klicken. Weitere Informationen über die verfügbaren Einstellungen finden Sie im Abschnitt 'Einen verwalteten Speicherort hinzufügen'.

Möglicherweise werden Sie aufgefordert, den Benutzernamen und das Kennwort für den Storage Node einzugeben. Die Mitglieder folgender Windows-Gruppen auf der Maschine, auf welcher ein Storage Node installiert ist, können auf alle verwalteten Speicherorte auf dem Storage Node zugreifen:

- **Administratoren**
- **Acronis ASN Remote Users**

  Diese Gruppe wird automatisch erstellt, wenn der Storage Node installiert wird. Diese Gruppe ist standardmäßig leer. Sie können die Benutzer zu dieser Gruppe manuell hinzufügen.

- **Band**

  Wenn ein Bandgerät an die zu sichernde Maschine oder einen Storage Node angeschlossen wird, wird in der Speicherortliste der Standard-Band-Pool angezeigt. Dieser Pool wird automatisch erstellt.

  Sie können den Standard-Pool auswählen oder einen neuen erstellen, indem Sie auf **Speicherort hinzufügen** –> **Band** klicken. Zu Informationen über die verfügbaren Pool-Einstellungen siehe den Abschnitt 'Einen Pool erstellen'.

# Über Einer Secure Zone

Die 'Einer 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 Einer Secure Zone gespeicherten Backups verloren. Aus diesem Grund sollten Sie ein Backup nicht alleine nur in der Einer Secure Zone speichern, sondern möglichst noch an einem oder sogar mehreren anderen Speicherorten. In Unternehmensumgebungen kann eine Einer Secure Zone beispielsweise als praktischer Zwischenspeicher für Backups dienen, wenn ein normalerweise verwendeter Speicherort temporär nicht verfügbar ist (z.B. aufgrund einer fehlenden oder zu langsamen Daten- oder Netzwerkanbindung).

## Wann ist die Verwendung der Einer Secure Zone sinnvoll?

Einer Secure Zone:

- Ermöglicht es, bei einer Laufwerkswiederherstellung dasselbe Laufwerk als Recovery-Ziel zu verwenden, auf dem das entsprechende Laufwerk-Backup selbst gespeichert ist.
- Bietet eine kosteneffektive und praktische Methode, um Ihre Daten leicht gegen Software-Fehler, Virusangriffe und Bedienungsfehler abzusichern.

- Ermöglicht es, dass bei Backup- oder Recovery-Aktionen die gesicherten Daten nicht unbedingt auf einem anderen Medium liegen oder über eine Netzwerkverbindung bereitgestellt werden müssen. Diese Funktion ist besonders für Benutzer von Mobilgeräten nützlich.
- Eignet sich gut als primäres Backup-Ziel, wenn Backups per Replikation noch an anderen Speicherorten gesichert werden.

## Einschränkungen

- Auf dem Mac ist die Einrichtung bzw. Verwendung einer Einer Secure Zone nicht möglich.
- Die Einer Secure Zone kann nur als normales Volume auf einem Laufwerk vom Typ 'Basis' angelegt/verwendet werden. Sie kann weder auf einem dynamischen Datenträger liegen, noch als logisches Volume (einem per LVM verwalteten Volume) erstellt werden.
- Die Einer Secure Zone verwendet FAT32 als Dateisystem. Da FAT32 eine Dateigrößenbeschränkung von 4 GB hat, werden größere Backups bei der Speicherung in der Einer Secure Zone entsprechend aufgeteilt. Dies hat jedoch keinen Einfluss auf die Geschwindigkeit oder spätere Wiederherstellungsprozesse.

## Wie die Erstellung der Einer Secure Zone ein Laufwerk umwandelt

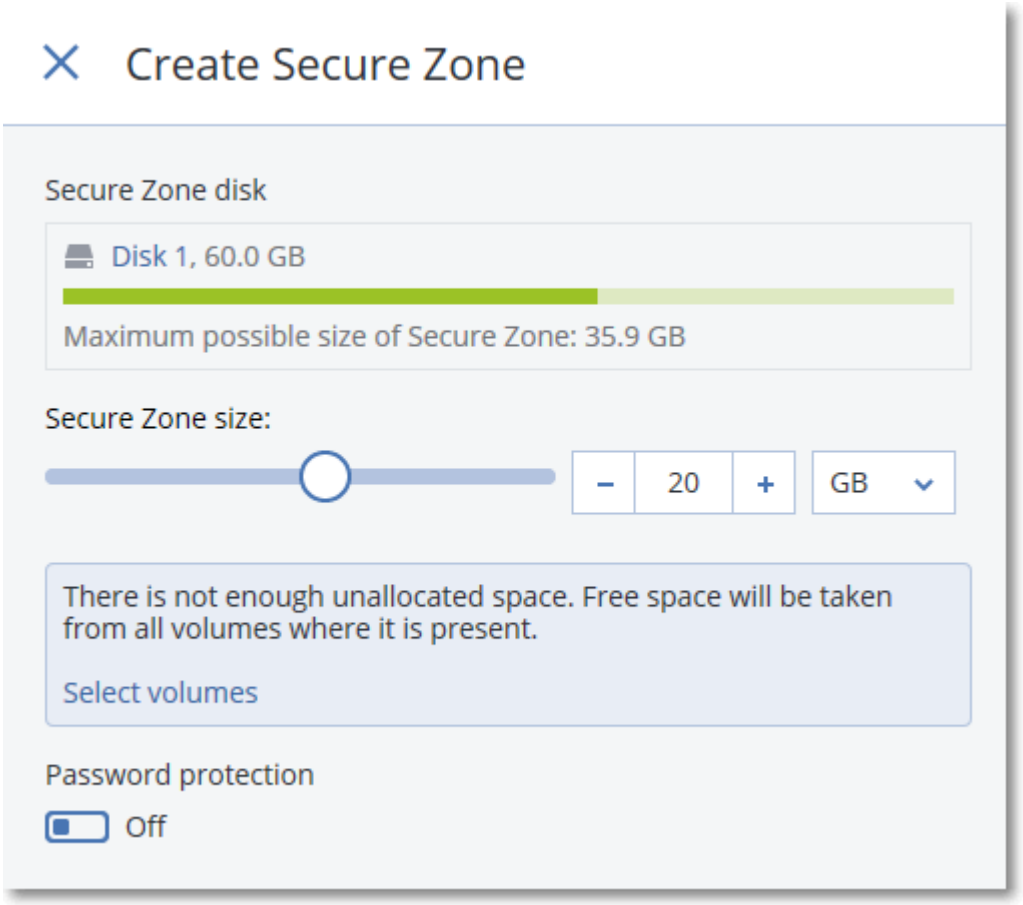
- Die Einer Secure Zone wird immer am Ende des entsprechenden Laufwerks erstellt.
- Sollte der 'nicht zugeordnete' Speicherplatz am Ende des Laufwerks nicht ausreichen, jedoch zwischen den Volumes (Partitionen) noch weiterer 'nicht zugeordneter' Speicherplatz vorhanden sein, so werden die entsprechenden 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 Einer 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 Einer Secure Zone erstellen

1. Wählen Sie die Maschine aus, auf der Sie die Einer Secure Zone erstellen wollen.
2. Klicken Sie auf **Details** –> **Einer Secure Zone erstellen**.
3. Klicken Sie unter **Laufwerk für die Einer 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 Einer Secure Zone.
4. Geben Sie die gewünschte Größe der Einer 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 Einer Secure Zone zugreifen zu können. Um ein Backup in die Einer 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 Einer Secure Zone erstellt hat.

Die Einer Secure Zone kann nun unter **Backup-Ziel** ausgewählt werden, wenn Sie einen Schutzplan erstellen.

### So können Sie eine Einer Secure Zone löschen

1. Wählen Sie eine Maschine aus, auf der sich eine Einer Secure Zone befindet.
2. Klicken Sie auf **Details**.
3. Klicken Sie zuerst auf das Zahnradsymbol neben dem Element **Einer Secure Zone** und 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 Einer Secure Zone komplett gelöscht – inklusive aller Backups, die in ihr gespeichert waren.

## Über Acronis Cyber Infrastructure

Acronis Cyber Protect 15 unterstützt eine Integration mit Acronis Cyber Infrastructure 3.5 Update 5 oder höher.

Backups zu Acronis Cyber Infrastructure sind nicht für macOS-Maschinen verfügbar.

### Bereitstellung

Um Acronis Cyber Infrastructure verwenden zu können, müssen Sie es in Ihrer lokalen Umgebung auf fabrikneuen Systemen installieren. Es werden mindestens fünf physische Server empfohlen, um die Vorteile des Produkts voll ausschöpfen zu können. Wenn Sie nur die Gateway-Funktionalität benötigen, können Sie einen physischen oder virtuellen Server verwenden – oder einen Gateway-Cluster mit so vielen Servern konfigurieren, wie Sie wünschen.

Stellen Sie sicher, dass die Zeiteinstellungen zwischen dem Management Server und dem Acronis Cyber Infrastructure synchronisiert werden. Die Zeiteinstellungen für Acronis Cyber Infrastructure

können während der Bereitstellung konfiguriert werden. Die Zeitsynchronisation erfolgt standardmäßig per NTP (Network Time Protocol).

Sie können mehrere Instanzen von Acronis Cyber Infrastructure bereitstellen und diese alle auf demselben Management Server registrieren.

## Registrierung

Die Registrierung erfolgt über die Weboberfläche von Acronis Cyber Infrastructure. Acronis Cyber Infrastructure kann nur von Organisationsadministratoren und nur in der Organisation (dem Unternehmen) registriert werden. Nach der Registrierung steht der Storage allen Organisationseinheiten (Abteilungen) zur Verfügung. Es kann jeder Abteilung oder der Organisation (dem Unternehmen) als Backup-Speicherort hinzugefügt werden.

Der umgekehrte Vorgang (Aufhebung der Registrierung) wird in der Benutzeroberfläche von Acronis Cyber Protect durchgeführt. Klicken Sie auf **Einstellungen** –> **Storage-Knoten**. Klicken Sie dann auf die gewünschte Acronis Cyber Infrastructure-Instanz und dann auf **Löschen**.

## Einen Backup-Speicherort hinzufügen

Es kann nur ein Backup-Speicherort auf jeder Acronis Cyber Infrastructure-Instanz zu einer Abteilung oder Organisation (Unternehmen) hinzugefügt werden. Ein auf Abteilungsebene hinzugefügter Speicherort ist für diese Abteilung und für die Organisationsadministratoren verfügbar. Ein auf Organisationsebene (Unternehmensebene) hinzugefügter Speicherort ist nur für Organisationsadministratoren verfügbar.

Wenn Sie einen Speicherort hinzufügen, erstellen und definieren Sie dessen Namen. Wenn Sie einen vorhandenen Speicherort zu einem neuen oder anderen Management Server hinzufügen müssen, aktivieren Sie das Kontrollkästchen **Einen vorhandenen Speicherort verwenden...**, klicken Sie dann auf **Durchsuchen** und wählen Sie abschließend den Speicherort aus der Liste aus.

Wenn auf dem Management Server mehrere Instanzen von Acronis Cyber Infrastructure registriert sind, können Sie beim Hinzufügen eines Speicherortes auch die gewünschte Cyber Infrastructure-Instanz auswählen.

## Backup-Schemata, Aktionen und Einschränkungen

Ein direkter Zugriff auf den Acronis Cyber Infrastructure von einem Boot-Medium aus ist nicht möglich. Um mit Acronis Cyber Infrastructure arbeiten zu können, müssen Sie das Medium auf dem Management Server registrieren und dieses dann über die Cyber Protect Webkonsole verwalten.

Ein Zugriff auf den Acronis Cyber Infrastructure über das Befehlszeilenwerkzeug ist nicht möglich.

Acronis Cyber Infrastructure und der Cloud Storage gleichen sich überwiegend, was die verfügbaren Backup-Schemata und Backup-Aktionen angeht. Der einzige Unterschied besteht darin, dass Backups bei der Ausführung eines Schutzplans auch *vom* Acronis Cyber Infrastructure aus repliziert werden können.

## Dokumentation

Der vollständige Dokumentationssatz für Acronis Cyber Infrastructure ist auf der Acronis Website verfügbar.

# Planung

**Wichtig**
Einige der in diesem Abschnitt beschriebenen Funktionen stehen nur bei On-Premise-Bereitstellungen zur Verfügung.

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 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.

Die Planungsparameter hängen vom Backup-Ziel ab.

## Wenn der Cloud Storage als Backup-Ziel dient

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.

Sie können die Backup-Planung so einstellen, 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'.

**Wichtig**
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.

## Wenn andere Speicherorte als Backup-Ziel dienen

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 neue Backup-Format 'Einzeldatei'[1].

  Dieses Schema ist nicht verfügbar, wenn ein ein Bandgerät oder ein SFTP-Server als Backup-Ziel verwendet wird.
- **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.

---

[1] Ein neues Backup-Format, in dem das anfängliche Voll-Backup sowie die nachfolgenden inkrementellen Backups gemeinsam in Form einer einzigen .tib-Datei (statt einer Kette von Dateien) gespeichert werden. Dieses Format nutzt die Geschwindigkeit der inkrementellen Backup-Methode und vermeidet dabei gleichzeitig deren größten Nachteil: das schwierige Löschen veralteter Backups. Die Software kennzeichnet diejenigen Blöcke, die von veralteten Backups verwendet werden, als 'frei' und schreibt neue Backups in diese neuen Blöcke. Dies führt zu einer extrem schnellen Bereinigung, bei gleichzeitig minimalem Ressourcenverbrauch. Das Backup-Format 'Einzeldatei' ist nicht verfügbar, wenn als Backup-Ziel ein Storage (wie etwa ein SFTP-Server) verwendet wird, der keine wahlfreien Lese- und Schreib-Zugriffe (Random Access Read and Write) zulässt.

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.

  Klicken Sie auf das Zahnradsymbol und dann auf **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**
  Bei Cloud-Bereitstellungen ist diese Option standardmäßig aktiviert und der vorgegebene maximale Verzögerungswert beträgt 30 Minuten. Bei On-Premise-Bereitstellungen werden alle Backups standardmäßig genau nach Planung gestartet.

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

## Planung nach Ereignissen

Wenn Sie einen Schutzplan konfigurieren, können Sie in den 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.

  **Hinweis**
  Weil die Planung auf einem erfolgreichen Backup-Ereignis basiert, wird der Scheduler bei einem fehlgeschlagenen Backup den Task erst dann wieder ausführen, wenn ein Operator den Plan manuell ausführt und diese Aktion dann erfolgreich abgeschlossen wurde.

- **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 | Windows, Linux, | Windows | Windows | Windows, Linux, | Windows | Windows |

| | | | | | | |
|---|---|---|---|---|---|---|
| Dateien (physische Maschinen) | macOS | | | macOS | | |
| Laufwerke/Volumes (virtuelle Maschinen) | Windows, Linux | – | – | – | – | – |
| ESXi-Konfiguration | Windows, Linux | – | – | – | – | – |
| Microsoft 365-Postfächer | Windows | – | – | – | – | Windows |
| Exchange-Datenbanken und -Postfächer | Windows | – | – | – | – | Windows |
| SQL-Datenbanken | Windows | – | – | – | – | Windows |

## 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**.

## 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 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 | Microsoft 365-Postfächer | Exchange-Datenbanken und -Postfächer | SQL-Datenbanken |
|---|---|---|---|---|---|---|
| Benutzer ist inaktiv | Windows | – | – | – | – | – |
| Der Host des Backup-Speicherorts ist verfügbar | Windows, Linux, macOS | Windows, Linux | Windows, Linux | Windows | Windows | Windows |
| Benutzer sind abgemeldet | Windows | – | – | – | – | – |
| Entspricht dem Zeitintervall | Windows, Linux, macOS | Windows, Linux | – | – | – | – |
| Akkubelastung senken | Windows | – | – | – | – | – |

| | | | | | | |
|---|---|---|---|---|---|---|
| Nicht starten, wenn eine getaktete Verbindung besteht | Windows | – | – | – | – | – |
| Nicht starten, wenn eine Verbindung mit folgenden WLANs besteht: | Windows | – | – | – | – | – |
| IP-Adresse des Gerätes überprüfen | Windows | – | – | – | – | – |

## 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.

## 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

Das Backup erfolgt normalerweise immer werktags um 21:00 Uhr zu einem Netzwerkordner. 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.

## 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.

## 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.

## 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, 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.

## 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-Symbol 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.

## 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-Symbol 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.

## 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.

# Aufbewahrungsregeln

**Wichtig**
Einige der in diesem Abschnitt beschriebenen Funktionen stehen nur bei On-Premise-Bereitstellungen zur Verfügung.

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[1] 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 ein SFTP-Server oder ein Bandgerät 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.

[1] Eine Gruppe von Backups, auf die eine einzelne Aufbewahrungsregel angewendet werden kann. Beim Backup-Schema 'Benutzerdefiniert' entsprechen die Backup-Sätze den Backup-Methoden ('Vollständig', 'Differentiell' und 'Inkrementell'). In allen anderen Fällen sind die Backups-Sätze 'Monatlich', 'Täglich', 'Wöchentlich' und 'Stündlich'. Ein 'monatliches' Backup ist dasjenige Backup, das als erstes in einem bestimmten Monat erstellt wird. Ein 'wöchentliches' Backup ist das erste Backup, welches an demjenigen Wochentag erstellt wird, wie er über die Option 'Wöchentliches Backup' festgelegt wurde (klicken Sie auf das Zahnradsymbol und dann auf die Befehle 'Backup-Optionen' –> 'Wöchentliche Backups'). Wenn ein 'wöchentliches' Backup das erste Backup ist, welches seit Anbruch eines Monats erstellt wurde, so wird dieses Backup als 'monatliches' Backup betrachtet. In diesem Fall wird ein wöchentliches Backup an dem ausgewählten Tag der nächsten Woche erstellt. Ein 'tägliches' Backup ist das erste Backup, welches nach Anbruch eines Tages erstellt wird – es sei denn, dieses Backup fällt unter die Definition eines monatlichen oder wöchentlichen Backups. Ein 'stündliches' Backup ist das erste Backup, welches nach Anbruch einer Stunde erstellt wird – es sei denn, dieses Backup fällt unter die Definition eines 'monatlichen', 'wöchentlichen' oder 'täglichen' Backups.

## Was Sie zudem noch wissen sollten

- Das letzte Backup, das durch den Schutzplan erstellt wurde, wird in jedem Fall aufbewahrt. Es sei denn, Sie konfigurieren eine Aufbewahrungsregel, damit die Backups vor dem Start einer neuen Backup-Aktion bereinigt werden, und setzen in dieser Regel die Anzahl der aufzubewahrenden Backups auf Null.

  **Warnung!**
  Wenn Sie eine Aufbewahrungsregel auf diese Weise anwenden, um das letzte verbliebene Backup zu löschen, kann es passieren, dass Sie gar kein Backup mehr zur Wiederherstellung Ihrer Daten verfügbar haben, falls der anstehende Backup-Prozess fehlschlagen sollte.

- Backups auf Bändern werden solange nicht gelöscht, bis das Band überschrieben wird.
- 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' 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 Management-Server gelöscht wird. Wenn Sie die vom Backup-Plan erstellten Backups nicht mehr benötigen, können Sie diese löschen (wie im Abschnitt 'Backups löschen' beschrieben).

# 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 Schutzplan-Fensterbereich 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 Schutzplan-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 bei Cloud-Bereitstellungen das Verzeichnis '**%ProgramFiles%\BackupClient**' – und bei On-Premise-Bereitstellungen das Verzeichnis '**%ProgramFiles%\Acronis**'.
   - 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 bei Cloud-Bereitstellungen das Verzeichnis '**%ProgramFiles%\BackupClient**' – und bei On-Premise-Bereitstellungen das Verzeichnis '**%ProgramFiles%\Acronis**'.
   - Unter Linux: **/usr/sbin/acropsh -m manage_creds --reset**

***So ändern Sie die Verschlüsselungseinstellungen über den Cyber Protect Monitor***

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 Protect 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.

# 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 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 Einer Secure Zone als Backup-Ziel verwendet wird
- Wenn ein verwalteter Speicherort mit aktivierter Deduplizierung oder Verschlüsselung als Backup-Ziel verwendet wird

## So können Sie die Beglaubigungsfunktion verwenden

Um die Beglaubigungsfunktion für alle Dateien, die für ein Backup ausgewählt wurden (ausgenommen Dateien mit digitalen Signaturen), zu aktivieren, müssen Sie beim Erstellen des entsprechenden Schutzplans den Schalter **Beglaubigung (Notarization)** einschalten.

Wenn Sie eine Wiederherstellung konfigurieren, werden die beglaubigten Dateien durch ein spezielles Symbol gekennzeichnet. Das bedeutet, dass Sie die Authentizität dieser Dateien überprüfen können.

## Und so funktioniert es

Der Agent berechnet während eines Backups die Hash-Werte der gesicherten Dateien, erstellt einen Hash-Baum (basierend auf der Ordnerstruktur), speichert diesen Hash-Baum mit im Backup und sendet dann das Stammverzeichnis (Root) des Hash-Baums an den Notary Service. Der Notary Service speichert das Wurzelverzeichnis des Hash-Baums in der Blockchain-Datenbank von Ethereum. Damit wird sichergestellt, dass dieser Wert nicht mehr geändert werden kann.

Wenn die Authentizität einer Datei überprüft werden soll, berechnet der Agent den Hash-Wert der Datei und vergleicht diesen dann mit dem Hash-Wert, der im Hash-Baum innerhalb des Backups gespeichert ist. Sollten diese Hash-Werte nicht übereinstimmen, wird die Datei als 'nicht authentisch' eingestuft. Im anderen Fall ist die Authentizität der Datei durch den Hash-Baum verbürgt.

Um zu verifizieren, dass der Hash-Baum selbst nicht kompromittiert wurde, sendet der Agent den Wert des Hash-Baum-Wurzelverzeichnisses an den Notary Service. Der Notary Service vergleicht diesen Wert mit dem, der in der Blockchain-Datenbank gespeichert ist. Wenn die Hash-Werte übereinstimmen, ist die ausgewählte Datei garantiert authentisch. Falls nicht, zeigt die Software über eine Nachricht an, dass die Datei nicht authentisch ist.

# Konvertierung zu einer virtuellen Maschine

**Wichtig**
Einige der in diesem Abschnitt beschriebenen Funktionen stehen nur bei On-Premise-Bereitstellungen zur Verfügung.

Nur Laufwerk-Backups können zu einer virtuellen Maschine konvertiert werden. Wenn ein Backup das System-Volume und alle Informationen enthält, die für den Start des entsprechenden Betriebssystems erforderlich sind, kann auch die resultierende virtuelle Maschine selbstständig starten. Ansonsten können Sie die entsprechenden virtuellen Laufwerke zu einer anderen virtuellen Maschine hinzufügen.

## Konvertierungsmethoden

- **Regelmäßige Konvertierung**
  Es gibt zwei Möglichkeiten, eine regelmäßige Konvertierung zu konfigurieren:
  - **Die Konvertierung zum Teil eines Schutzplans machen**
    Die Konvertierung wird nach jedem Backup (falls für den primären Speicherort konfiguriert) oder nach jeder Replikation (falls für den zweiten und weitere Speicherort(e) konfiguriert) durchgeführt.
  - **Einen separaten Konvertierungsplan erstellen**
    Mit dieser Methode können Sie eine separate Konvertierungsplanung spezifizieren.
- **Recovery zu einer neuen virtuellen Maschine**
  Mit dieser Methode können Sie Laufwerke für die Wiederherstellung auswählen und die Einstellungen für jedes virtuelle Laufwerk anpassen. Verwenden Sie diese Methode, wenn Sie die Konvertierung nur einmal oder gelegentlich durchführen wollen. Beispielsweise, um eine Migration von physisch zu virtuell durchzuführen.

## Was Sie über Konvertierungen wissen müssen

### Diese Typen von virtuellen Maschinen werden unterstützt

Die Konvertierung eines Backups zu einer virtuellen Maschine kann von dem Agenten durchgeführt werden, der das Backup erstellt hat – oder auch von einem anderen Agenten durchgeführt werden.

Um eine Konvertierung zu VMware ESXi, Hyper-V oder Scale Computing HC3 durchzuführen, benötigen Sie einen ESXi-, Hyper-V- bzw. Scale Computing HC3-Host und einen Protection Agenten

(Agenten für VMware, Agenten für Hyper-V oder Agenten für Scale Computing HC3), der diesen Host verwaltet.

Eine Konvertierung zu VHDX-Dateien setzt voraus, dass die Dateien als virtuelle Festplatten mit einer virtuellen Hyper-V-Maschine verbunden werden.

Die folgende Tabelle fasst die Arten von virtuellen Maschinen zusammen, die von den Agenten erstellt werden können:

| VM-Typ | Agent für VMware | Agent für Hyper-V | Agent für Windows | Agent für Linux | Agent für Mac | Agent für Scale Computing HC3 |
|---|---|---|---|---|---|---|
| VMware ESXi | + | – | – | – | – | – |
| Microsoft Hyper-V | – | + | – | – | – | – |
| VMware Workstation | + | + | + | + | – | – |
| VHDX-Dateien | + | + | + | + | – | – |
| Scale Computing HC3 | – | – | – | – | – | + |

## Einschränkungen

- Der Agent für Windows, der Agent für VMware (Windows) und der Agent für Hyper-V können keine Backups konvertieren, die auf einer NFS-Freigabe gespeichert sind.
- Backups, die auf einer NFS-Freigabe oder einem SFTP-Server gespeichert sind, können nicht in einem separaten Konvertierungsplan konvertiert werden.
- Backups, die in einer Einer Secure Zone gespeichert sind, können nur von dem Agenten konvertiert werden, der auf derselben Maschine läuft.
- Backups können nur in einem separaten Konvertierungsplan zu einer virtuellen Scale Computing HC3-Maschine konvertiert werden.
- Backups, die logische Linux-Volumes (LVMs) enthalten, können nur konvertiert werden, wenn sie mit dem Agenten für VMware, dem Agenten für Hyper-V oder dem Agenten für Scale Computing HC3 erstellt wurden und auf den gleichen Hypervisor ausgerichtet sind. Eine Hypervisor-übergreifende Konvertierung wird nicht unterstützt.
- Wenn die Backups einer Windows-Maschine zu VMware Workstation- oder VHDX-Dateien konvertiert werden, übernimmt die resultierende virtuelle Maschine den CPU-Typ von derjenigen Maschine, die die Konvertierung durchführt. Als Ergebnis werden auch die entsprechenden CPU-

Treiber im Gastbetriebssystem installiert. Beim Start auf einem Host mit einem anderen CPU-Typ zeigt das Gastsystem einen Treiberfehler an. Aktualisieren Sie diesen Treiber manuell.

### Regelmäßige Konvertierung zu ESXi und Hyper-V versus eine virtuelle Maschine aus einem Backup ausführen

Beide Aktionen liefern Ihnen eine virtuelle Maschine, die in wenigen Sekunden, nachdem die ursprüngliche Maschine fehlgeschlagen ist, gestartet werden kann.

Eine regelmäßige Konvertierung beansprucht CPU- und Arbeitsspeicher-Ressouren. Die Dateien der virtuellen Maschine belegen fortlaufend Speicherplatz im Datenspeicher (Storage). Dies ist möglicherweise nicht praktikabel, wenn ein Produktions-Host zur Konvertierung verwendet wird. Dafür wird die Performance der virtuellen Maschine nur durch die Ressourcen des Hosts beschränkt.

Im zweiten Fall werden nur dann Ressourcen beansprucht, wenn die virtuelle Maschine ausgeführt wird. Platz im Datenspeicher (Storage) ist nur dann erforderlich, um Änderungen, die an den virtuellen Laufwerken durchgeführt werden, zu speichern. Die Ausführungsgeschwindigkeit der virtuellen Maschine ist jedoch möglicherweise niedriger, da der Host nicht direkt auf die virtuellen Laufwerke zugreift, sondern mit dem Agenten kommuniziert, der die entsprechenden Daten aus dem Backup liest. Zudem existiert die virtuelle Maschine nur temporär.

## Konvertierung zu einer virtuellen Maschine in einem Schutzplan

Sie können für jeden Backup- oder Replikations-Speicherort, der in einem Schutzplan vorhanden ist, die Option 'Konvertierung zu einer virtuellen Maschine' konfigurieren. Nach jedem Backup oder jeder Replikation wird dann die Konvertierung durchgeführt.

Informationen zu Voraussetzungen und Einschränkungen finden Sie im Abschnitt 'Was Sie über Konvertierungen wissen müssen'.

***So können Sie eine Konvertierung zu einer virtuellen Maschine in einem Schutzplan einrichten***

1. Entscheiden Sie, von welchem Backup-Speicherort aus Sie die Konvertierung durchführen wollen.
2. Klicken Sie im Schutzplan-Fensterbereich unterhalb von diesem Speicherort auf den Befehl **Zu VM konvertiert**.
3. Aktivieren Sie den Schalter **Konvertierung**.
4. Bestimmen Sie bei **Konvertieren zu** den Typ der virtuellen Zielmaschine. Sie können eine der folgenden Optionen wählen:
   - **VMware ESXi**
   - **Microsoft Hyper-V**
   - **VMware Workstation**
   - **VHDX-Dateien**
5. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:

- Für VMware ESXi und Hyper-V: klicken Sie auf **Host**, wählen Sie den Zielhost und spezifizieren Sie die Vorlage für den Namen der neuen Maschine.
- Für andere Arten von virtuellen Maschinen: spezifizieren Sie bei **Pfad**, wo die Dateien der virtuellen Maschinen und die Dateinamensvorlage gespeichert werden sollen.

Der Standardname ist **[Maschinenname]_konvertiert**.

6. [Optional] Klicken Sie auf **Agent, der die Konvertierung durchführt** und bestimmen Sie dann einen Agenten.

   Das kann der Agent sein, der (standardmäßig) das Backup durchführt – oder ein Agent, der auf einer anderen Maschine installiert ist. Im letzteren Fall müssen die Backups an einem gemeinsam nutzbaren/freigegebenen Ort gespeichert sein (z.B. ein Netzwerkordner), damit die andere Maschine darauf zugreifen kann.
7. [Optional] Für VMware ESXi und Hyper-V können Sie auch 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.
   - Den Laufwerk-Provisioning-Modus ändern Die Standardeinstellung ist **Thin** für VMware ESXi und **Dynamisch erweiterbar** für Hyper-V.
   - Klicken Sie auf **VM-Einstellungen**, um die Größe des Arbeitsspeichers, die Anzahl der Prozessoren und die Netzwerkverbindungen für die virtuelle Maschine zu ändern.
8. Klicken Sie auf **Fertig**.

## Wie die 'regelmäßige Konvertierung zu VM' arbeitet

Wie die regelmäßige Konvertierungen ablaufen, hängt davon ab, wo die virtuelle Maschine erstellt werden soll.

- **Bei Auswahl, dass die virtuelle Maschine als ein Satz von Dateien gespeichert werden soll:** Erstellt jede Konvertierung die virtuelle Maschine von Grund aus neu.
- **Bei Auswahl, dass die virtuelle Maschine auf einem Virtualisierungsserver erstellt werden soll:** Aktualisiert die Software eine existierende virtuelle Maschine statt sie neu zu erstellen, wenn ein inkrementelles oder differentielles Backup konvertiert wird. Eine solche Konvertierung ist normalerweise schneller. Sie geht sparsamer mit Netzwerkverkehr und CPU-Ressourcen des Hosts um, der die Konvertierung durchführt. Falls eine virtuelle Maschine nicht aktualisiert werden kann, erstellt die Software auch diese von Grund auf neu.

Nachfolgend finden Sie eine genauere Beschreibung beider Fälle.

### Bei Auswahl, dass die virtuelle Maschine als ein Satz von Dateien gespeichert werden soll

Als Folge der ersten Konvertierung wird eine neue virtuelle Maschine erstellt. Jede nachfolgende Konvertierung wird diese Maschine jeweils ganz neu erstellen. Zuerst wird die alte Maschine temporär umbenannt. Dann wird eine neue virtuelle Maschine erstellt, die den vorherigen Namen der alten Maschine hat. Sobald diese Aktion erfolgreich abgeschlossen wurde, wird die alte Maschine gelöscht. Wenn die Aktion fehlschlägt, wird die neue Maschine gelöscht und die alte

Maschine erhält ihren früheren Namen zurück. Auf diese Art schließt die Konvertierung immer mit einer einzelnen Maschine ab. Jedoch wird während der Konvertierung zusätzlicher Speicherplatz benötigt, um die alte Maschine aufzunehmen.

### Bei Auswahl, dass die virtuelle Maschine auf einem Virtualisierungsserver erstellt werden soll

Die erste Konvertierung erstellt eine ganz neue virtuelle Maschine. Jede nachfolgende Konvertierung arbeitet folgendermaßen:

- Falls es seit der letzten Konvertierung ein *Voll-Backup* gegeben hat, wird die virtuelle Maschine ganz neu erstellt (wie zuvor in diesem Abschnitt beschrieben).
- Anderenfalls wird die existierende virtuelle Maschine so aktualisiert, dass sie die Änderungen seit der letzten Konvertierung widerspiegelt. Wenn eine Aktualisierung (Update) nicht möglich ist (beispielsweise, weil Sie die zwischenzeitlichen Snapshots gelöscht haben, siehe nachfolgend), wird die virtuelle Maschine ganz neu erstellt.

**Zwischenzeitliche Snapshots**

Um die virtuelle Maschine aktualisieren zu können, speichert die Software einige zwischenzeitliche Snapshots von ihr. Sie werden **Backup...** und **Replica...** genannt und sollten behalten werden. Nicht mehr benötigte Snapshots werden automatisch gelöscht.

Der jüngste **Replikat...**-Snapshot korrespondiert mit dem Ergebnis der letzten Konvertierung. Sie können zu diesem Snapshot zurückgehen, falls Sie die Maschine auf dieses Stadium zurücksetzen wollen – beispielsweise, weil Sie mit der Maschine gearbeitet haben und nun durchgeführte Änderungen verwerfen wollen.

Andere Snapshots sind nur zur internen Verwendung durch die Software.

## Replikation

**Wichtig**
Einige der in diesem Abschnitt beschriebenen Funktionen stehen nur bei On-Premise-Bereitstellungen zur Verfügung.

Diese Abschnitt beschreibt, wie Sie eine Backup-Replikation als Teil eines Schutzplans ausführen können. Informationen über die Erstellung eines separaten Replikationsplans finden Sie im Abschnitt 'Off-Host Data Processing'.

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.

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
- Einem SFTP-Server
- Einem von einem Storage Node verwalteten Speicherort

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

- Einem lokalen Ordner
- Einem Netzwerkordner
- Dem Cloud Storage
- Einem SFTP-Server
- Einem von einem Storage Node verwalteten Speicherort
- Einem Bandgerät

***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 *vom* zuletzt ausgewählten Backup- oder Replikations-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' beschrieben).

4. [Optional] Spezifizieren Sie bei **Zu VM konvertieren** die Einstellungen für die Konvertierung zu einer virtuellen Maschine (wie im Abschnitt 'Konvertierung zu einer virtuellen Maschine' beschrieben).
5. [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' beschrieben Diese Einstellung bestimmt die Replikations-Performance.
6. [Optional] Wiederholen Sie die Schritte 1-5 für alle weiteren Speicherorte, zu denen die Backups repliziert werden sollen. Es werden bis zu fünf aufeinanderfolgende Speicherorte unterstützt (der erste eingeschlossen).

**Wichtig**
Wenn Sie Backup und Replikation im selben Schutzplan aktivieren, müssen Sie sicherstellen, dass die Replikation abgeschlossen wird, bevor das nächste geplante Backup ausgeführt wird. Sollte die Replikation gerade noch ausgeführt werden, dann wird das geplante Backup nicht gestartet. Wenn ein geplantes Backup beispielsweise alle 24 Stunden läuft, wird es nicht gestartet, wenn die Replikation 26 Stunden zur Fertigstellung benötigt.

Wenn Sie diese Abhängigkeit vermeiden wollen, müssen Sie einen separaten Plan für die Backup-Replikation verwenden. Weitere Informationen zu diesem speziellen Plan finden Sie im Abschnitt '"Backup-Replikation" (S. 373)'.

# Überlegungen für Benutzer mit Advanced-Lizenzen

## Tipp:

Es ist möglich, Backups *aus* dem Cloud Storage zu replizieren, indem Sie einen separaten Replikationsplan erstellen. Weitere Informationen dazu finden Sie im Abschnitt 'Off-Host Data Processing'.

## Einschränkungen

- Die Replikation von Backups *von* einem Speicherort, der von einem Storage Node verwaltet wird, zu einem lokalen Ordner wird nicht unterstützt. Mit 'lokaler Ordner' ist ein Ordner auf der Maschine mit dem Agenten gemeint, der das Backup erstellt hat.
- Die Replikation von Backups *zu* einem verwalteten Speicherort mit aktivierter Deduplizierung wird nicht unterstützt, wenn die Backups das Backup-Format '**Version 12**' verwenden.

## Welche Maschine führt diese Aktion aus?

Die Replikation eines Backups *von* einem Speicherort wird durch denjenigen Agenten initiiert, der das Backup erstellt hat – und wird durchgeführt:

- Von diesem Agenten – sofern der Speicherort *kein* nicht von einem Storage Node verwaltet wird.
- Von dem korrespondierendem Storage Node – sofern der Speicherort verwaltet wird. Die Replikation eines Backups vom verwalteten Speicherort zum Cloud Storage wird jedoch von dem Agenten durchgeführt, der das Backup erstellt hat.

Aus der oberen Erläuterung folgt zudem, dass die Aktion nur dann durchgeführt wird, wenn die Maschine mit dem Agenten angeschaltet ist.

### Backups zwischen verwalteten Speicherorten replizieren

Die Replikation eines Backups von einem verwalteten Speicherort zu einem anderen verwalteten Speicherort wird vom Storage Node durchgeführt.

Wenn der Zielspeicherort dedupliziert wird (möglicherweise auf einem anderen Storage Node), sendet der als Quelle fungierende Storage Node nur solche Datenblöcke, die auf dem als Ziel fungierenden Depot noch nicht vorhanden sind. Oder anders ausgedrückt: der Storage Node führt (wie ein Agent) die Deduplizierung an der Quelle durch. Das reduziert den Netzwerkverkehr, wenn Sie Daten zwischen örtlich getrennten Storage Nodes replizieren.

## Ein Backup manuell starten

1. Wählen Sie eine Maschine aus, die über mindestens einen auf sie angewendeten Schutzplan verfügt.
2. Klicken Sie auf **Backup**.
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.

## Backup-Optionen

**Wichtig**
Einige der in diesem Abschnitt beschriebenen Funktionen stehen nur bei On-Premise-Bereitstellungen zur Verfügung.

Wenn Sie die Backup-Optionen ändern wollen, klicken Sie auf das Zahnradsymbol neben dem Schutzplan-Namen und dann auf das Element **Backup-Optionen**.

## 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** | **Scale Computing** | **Windows** |
| Alarmmeldungen | + | + | + | + | + | + | + | + | + | + |
| Backup-Konsolidierung | + | + | + | + | + | + | + | + | + | - |
| Backup-Dateiname | + | + | + | + | + | + | + | + | + | + |
| Backup-Format | + | + | + | + | + | + | + | + | + | + |
| Backup-Validierung | + | + | + | + | + | + | + | + | + | + |
| CBT (Changed Block Tracking) | + | - | - | - | - | - | + | + | + | + |
| Cluster-Backup-Modus | - | - | - | - | - | - | - | - | - | + |
| Komprimierungsgrad | + | + | + | + | + | + | + | + | + | + |
| E-Mail-Benachrichtigungen | + | + | + | + | + | + | + | + | + | + |
| Fehlerbehandlung | | | | | | | | | | |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Bei Fehler erneut versuchen | + | + | + | + | + | + | + | + | + | + |
| 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 | + | + | + | - | - | - | - | - | - | - |
| Dateifilter | + | + | + | + | + | + | + | + | + | - |
| Snapshot für Datei-Backups | - | - | - | + | + | + | - | - | - | - |
| Protokollabschneidung | - | - | - | - | - | - | + | + | - | Nur SQL |
| LVM-Snapshot-Erfassung | - | + | - | - | - | - | - | - | - | - |
| Mount-Punkte | - | - | - | + | - | - | - | - | - | - |
| Multi-Volume-Snapshot | + | + | - | + | + | - | - | - | - | - |
| Performance und Backup-Fenster | + | + | + | + | + | + | + | + | + | + |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Physischer Datenversand | + | + | + | + | + | + | + | + | + | - |
| Vor-/Nach-Befehle | + | + | + | + | + | + | + | + | + | + |
| Befehle vor/nach der Datenerfassung | + | + | + | + | + | + | + | - | - | + |
| SAN-Hardware-Snapshots | - | - | - | - | - | - | + | - | - | - |
| Planung | | | | | | | | | | |
| Startzeiten in einem Zeitfenster verteilen | + | + | + | + | + | + | + | + | + | + |
| Die Anzahl gleichzeitig ausgeführter Backups begrenzen | - | - | - | - | - | - | + | + | + | - |
| Sektor-für-Sektor-Backup | + | + | - | - | - | - | + | + | + | - |
| Aufteilen | + | + | + | + | + | + | + | + | + | + |
| Bandverwaltung | + | + | + | + | + | + | + | + | + | + |
| Task-Fehlerbehandlung | + | + | + | + | + | + | + | + | + | + |
| Task-Startbedingungen | + | + | - | + | + | - | + | + | + | + |
| VSS (Volume Shadow Copy Service) | + | - | - | + | - | - | - | + | - | + |
| VSS (Volume Shadow Copy Service) für virtuelle | - | - | - | - | - | - | + | + | + | - |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Maschinen | | | | | | | | | | |
| Wöchentliche Backups | + | + | + | + | + | + | + | + | + | + |
| Windows-Ereignisprotokoll | + | - | - | + | - | - | + | + | + | + |

# Alarmmeldungen

## Keine erfolgreichen Backups für eine spezifizierte Anzahl aufeinanderfolgender Tage

Die Voreinstellung ist: **Deaktiviert**.

Diese Option bestimmt, ob eine Alarmmeldung generiert wird, wenn der Schutzplan innerhalb des spezifizierten Zeitraums kein erfolgreiches Backup durchgeführt hat. Zusätzlich zu fehlgeschlagenen Backups zählt die Software hier auch Backups, die nicht planungsgemäß ausgeführt wurden (verpasste Backups).

Die Alarmmeldungen werden pro Maschine generiert und in der Registerkarte **Alarmmeldungen** angezeigt.

Sie können spezifizieren, ab wie vielen aufeinanderfolgenden Tagen ohne Backups eine Alarmmeldung generiert wird.

# Backup-Konsolidierung

Diese Option bestimmt, ob Backups während einer Bereinigung konsolidiert oder komplette Backup-Ketten gelöscht werden sollen.

Die Voreinstellung ist: **Deaktiviert**.

Konsolidierung ist ein Prozess, bei dem zwei oder mehr aufeinander folgende, abhängige Backups zu einem einzelnen Backup kombiniert werden.

Eine Aktivierung dieser Option bewirkt, dass ein Backup, welches während einer Bereinigung gelöscht werden soll, zusammen mit dem nächsten abhängigen Backup (inkrementell oder differentiell) konsolidiert wird.

Bei deaktivierter Option wird das Backup solange aufbewahrt, bis alle abhängigen Backups gelöscht werden. Dieser hilft, die potenziell zeitaufwendige Konsolidierung zu vermeiden, benötigt aber extra Speicherplatz für von der Löschung zurückgestellte Backups. Das Alter oder die Anzahl der Backups kann daher die Werte überschreiten, die in den entsprechenden Aufbewahrungsregeln spezifiziert wurden.

**Wichtig**
Beachten Sie, dass eine Konsolidierung nur eine bestimmte Art der Datenbereinigung ist, jedoch keine Alternative zu einer richtigen Löschung ist. Das resultierende Backup wird keine Daten enthalten, die im gelöschten Backup vorlagen, die jedoch im aufbewahrten inkrementellen oder differentiellen Backup fehlten.

Diese Option ist *nicht* wirksam, wenn einer der folgenden Umstände zutrifft:

- Als Backup-Ziel wurde ein Bandgerät oder der Cloud Storage festgelegt.
- Als Backup-Schema wurde **Nur inkrementell (Einzeldatei)** festgelegt.
- Als Backup-Format wurde '**Version 12**' festgelegt.

Backups, die auf Bändern gespeichert sind, können nicht konsolidiert werden. 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. Backups, die auf einem Band gespeichert sind, werden nur dann nicht mehr in der Benutzeroberfläche angezeigt, wenn das entsprechende Band gelöscht oder überschrieben wird.

## 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 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 (traditionelles Format) |
| Backup-Format **Version 12** | Eine TIBX-Datei pro Backup-Kette (ein vollständiges oder differentielles Backup und alle davon abhängigen inkrementellen Backups) | |

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 oder Bandgeräte). 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

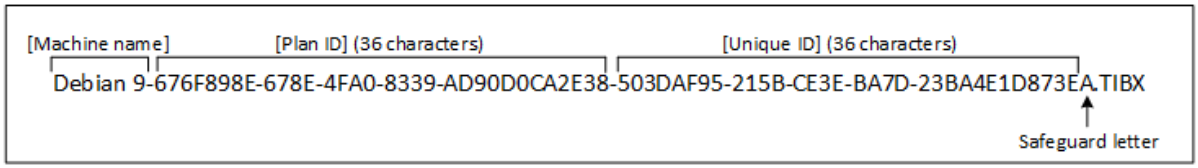
Der standardmäßig vorgegebene Backup-Dateiname lautet: `[Maschinenname]-[Plan-ID]-[Eindeutige ID]A`.

Der standardmäßig vorgegebene Dateiname für Postfach-Backups lautet: `[Postach-ID]_mailbox_[Plan-ID]A`.

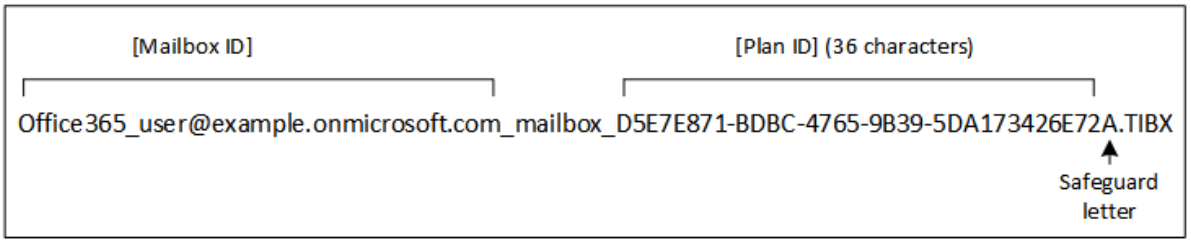
Der Name wird aus den folgenden Variablen zusammengesetzt:

- `[Maschinenname]` – Diese Variable wird mit dem Namen der Maschine ersetzt (derselbe Name, der in der Cyber Protect-Webkonsole angezeigt wird) – und zwar für alle Arten von Backup-Daten, ausgenommen Microsoft 365-Postfächer. Bei Microsoft 365-Postfächern wird die Variable mit dem UPN (User Principal Name, Benutzerprinzipalnamen) des Postfachs ersetzt.
- `[Plan-ID]` – Diese Variable wird mit einem eindeutigen Bezeichner (einer ID) des Schutzplans ersetzt. Der Wert dieser ID ändert sich auch dann nicht, wenn der Plan umbenannt wird.
- `[Eindeutige ID]` – Diese Variable wird mit einem eindeutigen Bezeichner (einer ID) der ausgewählten Maschine bzw. des ausgewählten Postfaches ersetzt. Dieser Wert ändert sich auch dann nicht, wenn die Maschine umbenannt oder der UPN (Benutzerprinzipalname) des Postfachs geändert wird.
- `[Postfach-ID]` – Diese Variable wird mit dem UPN (Benutzerprinzipalnamen) des Postfachs ersetzt.
- `"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 verdeutlicht den Standard-Backup-Dateinamen für Postfächer.




## Namen ohne Variablen

Die nachfolgenden Beispiele illustrieren, welche finalen Backup-Dateien sich ergeben, wenn Sie für ein Backup den Dateinamen '`MeinBackup`' 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
...
```

Beim Backup-Format 'Version 11' mit dem Backup-Schema **Nur inkrementell (Einzeldatei)**:

```
MyBackup.xml
MyBackup.tib
```

Beim Backup-Format 'Version 11' mit anderen Backup-Schemata:

```
MyBackup.xml
MyBackup_2016_9_13_14_49_20_403F.tib
MyBackup_2016_9_14_14_43_00_221F.tib
MyBackup_2016_9_15_14_45_56_300F.tib
...
```

## Verwendung von Variablen

Neben den standardmäßig verwendeten Variablen können Sie noch die Variable `[Plan-Name]` verwenden, die mit dem Namen des Schutzplans ersetzt wird.

Sind mehrere Maschinen oder Postfächer zum Backup ausgewählt, muss der Backup-Dateiname die Variable `[Maschinenname]`, `[Postfach-ID]` oder `[Eindeutige ID]` enthalten.

## Backup-Dateiname versus 'vereinfachte Dateibenennung'

Durch die Verwendung von 'Nur-Text' (Plain Text) und/oder Variablen können Sie die gleichen Dateinamen konstruieren wie in früheren Versionen von Acronis Cyber Protect. „Vereinfachte“ Dateinamen können jedoch nicht rekonstruiert werden, denn in Version 12 erhält ein Dateiname einen Zeitstempel (außer es wird das Backup-Format 'Einzeldatei' verwendet).

## Anwendungsbeispiele

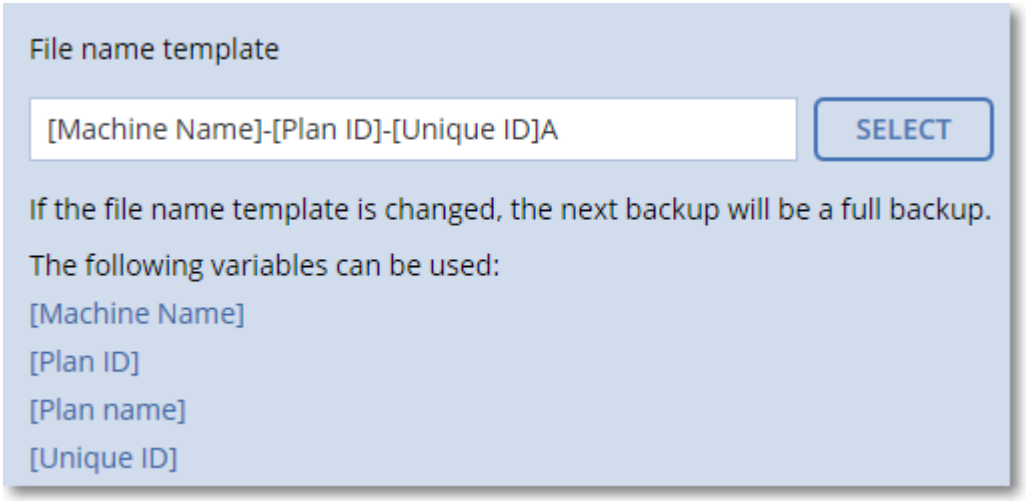
- **Benutzerfreundliche Dateinamen anzeigen**

  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 Cyber Protect Webkonsole 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. Klicken Sie dazu in den Backup-Optionen des Schutzplans zuerst auf **Backup-Dateiname** und dann auf **Auswahl**, um das gewünschte Backup auszuwählen.

Die Schaltfläche **Durchsuchen** 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).




- **Upgrade von früheren Produktversionen**

  Wenn ein Schutzplan während eines Upgrades nicht automatisch migriert wird, müssen Sie den Plan neu erstellen und auf die alte Backup-Datei verweisen. Wenn nur eine Maschine zum Backup ausgewählt wurde, klicken Sie auf **Durchsuchen** und wählen Sie das benötigte Backup aus. Wenn mehrere Maschinen zum Backup ausgewählt wurden, müssen Sie den alten Backup-Dateinamen durch die Verwendung von Variablen neu erstellen.

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

## Backup-Format

Die Option bestimmt das Format der Backups, die vom Schutzplan erstellt werden. Sie ist nur für Schutzpläne verfügbar, die das frühere Backup-Format Version 11 verwenden. In diesem Fall können Sie über die Option auf das neue Format Version 12 umstellen. Nachdem Sie diese Änderung durchgeführt haben, ist die Option nicht mehr verfügbar.

Diese Option gilt *nicht* für Postfach-Backups. Denn Postfach-Backups werden immer im neuen Format erstellt.

Die Voreinstellung ist: **Automatische Auswahl**.

Sie können eine der folgenden Optionen wählen:

- **Automatische Auswahl**

  Version 12 wird verwendet, außer der Schutzplan muss bestehende Backups erweitern, die mit früheren Produktversionen erstellt wurden.
- **Version 12**

  Ein für die meisten Fälle empfehlenswertes, neues Format für schnelles Backup und Recovery. Jede Backup-Kette (ein vollständiges oder differentielles Backup und alle davon abhängigen inkrementellen Backups) wird als einzelne TIBX-Datei gespeichert.

  Bei diesem Format ist die Aufbewahrungsregel **Nach der Gesamtgröße der Backups** nicht verfügbar.
- **Version 11**

  Das frühere Format (Legacy-Format), welches aus Gründen der Abwärtskompatibilität beibehalten wurde. Es ermöglicht Ihnen, an bestehende Backups, die mit älteren Produktversionen erstellt wurden, neue Backups anzuhängen (im Rahmen einer Backup-Kette).

  Verwenden Sie dieses Format (mit jedem Backup-Schema – außer mit **Nur inkrementell (Einzeldatei)**) außerdem, wenn Sie vollständige, inkrementelle und differentielle Backups als separate Dateien vorliegen haben wollen.

  Diese Format wird automatisch ausgewählt, wenn es sich bei dem Backup-Ziel (oder einem Replikationsziel) um einen verwalteten Speicherort mit aktivierter Deduplizierung oder einen verwalteten Speicherort mit aktivierter Verschlüsselung handelt. Wenn Sie das Backup-Format auf **Version 12** ändern, wird das Backup fehlschlagen.

**Hinweis**
Sie können Datenbankverfügbarkeitsgruppen (DAG) nicht im Backup-Format 'Version 11' sichern. Die Sicherung der DAG wird nur im Backup-Format 'Version 12' unterstützt.

## 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. Sie können die Namen dieser Dateien mithilfe der Option 'Backup-Dateiname' bestimmen. 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 (traditionelles Format) |
| Backup-Format **Version 12** | Eine TIBX-Datei pro Backup-Kette (ein vollständiges oder differentielles Backup und alle davon abhängigen inkrementellen Backups) | |

## Das Backup-Format auf 'Version 12' (TIBX) ändern

Wenn Sie das Backup-Format von 'Version 11' (TIB-Format) zu 'Version 12' (TIBX-Format) ändern, hat dies folgende Auswirkungen:

- Das nächste ausgeführte Backup wird ein Voll-Backup sein.
- Bei Backup-Speicherorten, die mit einem Datei-Manager durchsucht werden können (wie etwa lokale Ordner oder Netzwerklaufwerke), wird eine neue TIBX-Datei erstellt. Die neue Datei übernimmt den Namen der Originaldatei, wird jedoch mit dem Suffix **_v12A** erweitert.
- Aufbewahrungsregeln und Replikationen werden nur auf neue Backups angewendet.
- Die alten Backups werden nicht gelöscht, sondern bleiben über die Registerkarte **Backup Storage** weiter verfügbar. Sie können diese jedoch auch manuell löschen.
- Die alten Cloud Backups werden nicht auf die Quota **Cloud Storage** angerechnet.
- Die alten lokalen Backups werden solange auf die Quota **Lokales Backup** angerechnet, bis diese von Ihnen gelöscht werden.
- Wenn Ihr Backup-Ziel (oder Replikationsziel) ein verwalteter Speicherort mit aktivierter Deduplizierung ist, werden die Backups fehlschlagen.

### Archiv-interne Deduplizierung

Das Backup-Format 'Version 12' unterstützt eine innerhalb des Archivs erfolgende Deduplizierung (Archiv-interne Deduplizierung).

Die Archiv-interne Deduplizierung verwendet eine Client-seitige Deduplizierung und bietet folgende Vorteile:

- Deutlich reduzierte Backup-Größe, mit integrierter Deduplizierung auf Block-Ebene für jede Art von Daten
- Eine effiziente Handhabung von festen NTFS-Links (Hard Links) stellt sicher, dass es keine Duplikate auf dem Storage gibt
- Hash-basiertes Chunking (Blockerstellung)

**Hinweis**
Die Archiv-interne Deduplizierung ist standardmäßig für alle Backups im TIBX-Format aktiviert. Sie müssen diese nicht extra in den Backup-Optionen aktivieren – und Sie können sie auch nicht deaktivieren.

## Backup-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. Diese Aktion wird vom Protection Agenten durchgeführt.

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.

## 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.

## Cluster-Backup-Modus

Diese Optionen gelten für Datenbank-Backups von Microsoft SQL Server und Microsoft Exchange Server.

Diese Optionen gelten nur dann, wenn der Cluster selbst (Microsoft SQL Server-AlwaysOn-Verfügbarkeitsgruppe (AAG) oder Microsoft Exchange Server-Datenbankverfügbarkeitsgruppe (DAG)) als Backup-Quelle ausgewählt ist, statt einzelner Knoten oder Datenbanken innerhalb des Clusters. Wenn Sie einzelne Elemente innerhalb des Clusters auswählen, wird das Backup nicht Cluster-konform sein und es werden nur die ausgewählten Kopien der Elemente gesichert.

### Microsoft SQL Server

Diese Option bestimmt den Backup-Modus für die SQL Server-AlwaysOn-Verfügbarkeitsgruppen (AAG). Damit diese Option wirksam werden kann, muss der Agent für SQL auf allen entsprechenden AAG-Knoten installiert sein. Weitere Informationen über das Backup von AlwaysOn-Verfügbarkeitsgruppen finden Sie im Abschnitt 'AlwaysOn-Verfügbarkeitsgruppen (AAG) sichern'.

Die Voreinstellung ist: **Sekundäres Replikat, falls möglich.**

Sie können eine der folgenden Varianten wählen:

- **Sekundäres Replikat, falls möglich**
  Falls alle sekundären Replikate offline sind, wird das primäre Replikat gesichert. Eine Sicherung des primären Replikats kann die Performance des SQL Servers ausbremsen, dafür sind die Backup-Daten aber auf dem neuesten Stand.
- **Sekundäres Replikat**
  Falls alle sekundären Replikate offline sind, wird das Backup fehlschlagen. Backups von sekundären Replikaten haben keinen Einfluss auf die SQL Server-Performance und ermöglichen Ihnen, das Backup-Fenster zu erweitern. Passive Replikate können jedoch Informationen enthalten, die nicht mehr aktuell sind, da solche Replikate oft so eingestellt sind, dass sie asynchron (verzögert) aktualisiert werden.
- **Primäres Replikat**
  Falls das primäre Replikat offline ist, wird das Backup fehlschlagen. Eine Sicherung des primären Replikats kann die Performance des SQL Servers ausbremsen, dafür sind die Backup-Daten aber auf dem neuesten Stand.

Unabhängig vom Wert dieser Option und zur Gewährleistung der Datenbankkonsistenz überspringt die Software solche Datenbanken, die sich beim Start des Backups *nicht* im Stadium **SYNCHRONISIERT** oder **WIRD SYNCHRONISIERT** befinden. Falls alle Datenbanken übersprungen werden, schlägt das Backup fehl.

## Microsoft Exchange Server

Diese Option bestimmt den Backup-Modus für die Exchange Server-Datenbankverfügbarkeitsgruppen (DAG). Damit diese Option wirksam werden kann, muss der Agent für Exchange auf allen entsprechenden DAG-Knoten installiert sein. Weitere Informationen über das Backup von Datenbankverfügbarkeitsgruppen finden Sie im Abschnitt 'Datenbankverfügbarkeitsgruppen (DAG) sichern'.

Die Voreinstellung ist: **Passive Kopie, falls möglich.**

Sie können eine der folgenden Varianten wählen:

- **Passive Kopie, falls möglich**
  Falls alle passiven Kopien offline sind, wird die aktive Kopie gesichert. Eine Sicherung der aktiven Kopie kann die Performance des Exchange Servers ausbremsen, dafür sind die Backup-Daten aber auf dem neuesten Stand.
- **Passive Kopie**
  Falls alle passiven Kopien offline sind, wird das Backup fehlschlagen. Backups von passiven Kopien haben keinen Einfluss auf die Exchange-Server-Performance und ermöglichen Ihnen, das Backup-Fenster zu erweitern. Passive Kopien können jedoch Informationen enthalten, die nicht mehr aktuell sind, da diese oft so eingestellt sind, dass sie asynchron (verzögert) aktualisiert werden.

- **Aktive Kopie**

  Falls die aktive Kopie offline ist, wird das Backup fehlschlagen. Eine Sicherung der aktiven Kopie kann die Performance des Exchange Servers ausbremsen, dafür sind die Backup-Daten aber auf dem neuesten Stand.

Unabhängig vom Wert dieser Option und zur Gewährleistung der Datenbankkonsistenz überspringt die Software solche Datenbanken, die sich beim Start des Backups *nicht* im Stadium **FEHLERFREI** oder **AKTIV** befinden. Falls alle Datenbanken übersprungen werden, schlägt das Backup fehl.

## Komprimierungsgrad

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.

## E-Mail-Benachrichtigungen

Diese Option ermöglicht es Ihnen, E-Mail-Benachrichtigungen zu Ereignissen einzurichten, die während eines Backups auftreten.

Diese Option ist nur bei On-Premise-Bereitstellungen verfügbar. Bei Cloud-Bereitstellungen werden die Einstellungen pro Konto konfiguriert, wenn ein Konto erstellt wird.

Die Voreinstellung ist: **Die Systemeinstellungen verwenden.**

Sie können entweder die Systemeinstellungen verwenden oder diese mit benutzerdefinierten Werten überschreiben, die dann nur für diesen Plan gelten. Die Systemeinstellungen werden wie im Abschnitt 'E-Mail-Benachrichtigungen' beschrieben konfiguriert.

**Wichtig**
Wenn die Systemeinstellungen geändert werden, sind davon alle Schutzpläne betroffen, welche die Systemeinstellungen verwenden.

Stellen Sie vor Aktivierung dieser Option sicher, dass die **E-Mail-Server**-Einstellungen konfiguriert wurden.

***So konfigurieren Sie die E-Mail-Benachrichtigungen für einen Schutzplan***

1. Wählen Sie den Befehl **Die Einstellungen für diesen Schutzplan anpassen**.
2. Geben Sie im Feld **E-Mail-Adressen der Empfänger** die Ziel-E-Mail-Adressen ein. Sie können mehrere Adressen eingeben, müssen diese aber je per Semikolon trennen.
3. [Optional] Ändern Sie bei **Betreff** den Inhalt der Betreffzeile für die E-Mail-Benachrichtigungen. Sie können dafür folgende Variablen verwenden:
   - `[Alert]` – Alarmübersicht
   - `[Device]` – Gerätename.
   - `[Plan]` – der Name des Plans, der den Alarm generiert hat.
   - `[ManagementServer]` – der Host-Name der Maschine, auf welcher der Management Server installiert ist.
   - `[Unit]` – der Name der Abteilung, zu welcher die Maschine gehört.

   Die Standard-Betreffszeile für Benachrichtigungen lautet: `[Alert]` **Gerät:** `[Device]` **Plan:** `[Plan]`
4. Aktivieren Sie die Kontrollkästchen für diejenigen Ereignisse, zu denen Sie Benachrichtigungen erhalten wollen. Sie können aus einer Liste aller Alarmmeldungen auswählen, die während eines Backups auftreten können (nach Schweregrad gruppiert).

# 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. Intervall zwischen den Versuchen: 30 Sekunden.**

Wenn ein behebbarer Fehler auftritt, versucht das Programm, die erfolglose Aktion erneut durchzuführen. Sie können das Zeitintervall und die Anzahl der Versuche einstellen. Die Versuche werden aufgegeben, wenn entweder die Aktion erfolgreich ist ODER die angegebene Anzahl an Versuchen erreicht wurde, je nachdem, was zuerst eintritt.

Wenn 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. Intervall zwischen den Versuchen: 5 Minuten.**

Wenn die Snapshot-Erfassung einer virtuellen Maschine fehlschlägt, versucht das Programm, die Aktion zu wiederholen. Sie können das Zeitintervall und die Anzahl der Versuche einstellen. Die Versuche werden aufgegeben, wenn entweder die Aktion erfolgreich ist ODER die angegebene Anzahl an Versuchen erreicht wurde, je nachdem, was zuerst eintritt.

## Schnelles inkrementelles/differentielles Backup

Diese Option gilt für inkrementelle und differentielle Backups auf Laufwerksebene.

Diese Option gilt nicht (ist immer deaktiviert) für Volumes, die mit den Dateisystemen JFS, ReiserFS3, ReiserFS4, ReFS oder XFS formatiert sind.

Die Voreinstellung ist: **Aktiviert**.

Inkrementelle oder differentielle Backups erfassen nur jeweils geänderte Daten. Um das Backup-Verfahren zu beschleunigen, ermittelt das Programm, ob eine Datei geändert wurde oder nicht – und zwar anhand von Dateigröße und Zeitstempel der jeweils letzten Änderung. Ist diese Funktion ausgeschaltet, so vergleicht das Programm die Quelldateien und die Dateien, die bereits im Backup gespeichert sind, stattdessen anhand des kompletten Dateiinhaltes.

## Dateifilter

Durch die Verwendung von Dateifiltern können Sie festlegen, dass nur bestimmte Dateien und Ordner in ein Backup aufgenommen oder von einem Backup ausgeschlossen werden.

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

Dateifilter sind nicht wirksam, wenn sie auf dynamische Laufwerke (LVM- oder LDM-Volumes) einer virtuellen Maschine angewendet werden, die von einem Agenten für VMware, einem Agenten für Hyper-V oder einem Agenten für Scale Computing im agentenlosen Modus gesichert wird.

***So können Sie Dateifilter aktivieren***

1. Erweitern Sie in einem Schutzplan das **Backup**-Modul.
2. Klicken Sie in den **Backup-Optionen** auf den Befehl **Ändern**.
3. Wählen Sie **Dateifilter**.
4. Verwenden Sie eine der nachfolgend beschriebenen Optionen.

### Dateien einschließen oder ausschließen, die bestimmten 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** als **Backup-Format** 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**).

  **Wichtig**

  Wenn das Betriebssystem einer gesicherten Maschine während eines Laufwerk-Backups nicht korrekt erkannt wird, funktionieren keine Dateifilter mit vollständigem Pfad. Bei einem Ausschlussfilter wird eine Warnung angezeigt. Wenn ein Einschlussfilter vorhanden ist, wird das Backup fehlschlagen.

  Ein Filter mit vollständigem Pfaden beinhaltet den jeweiligen Laufwerksbuchstaben (in Windows) oder das jeweilige Stammverzeichnis (in Linux oder macOS). Ein Beispiel für einen vollständigen Dateipfad: **C:\Temp\Datei.tmp**. Ein Filter, der den Laufwerksbuchstaben oder das Stammverzeichnis enthält – zum Beispiel **C:\Temp\Datei.tmp** oder **C:\Temp*** – wird zu einer Warnung oder einem Fehler führen.

  Ein Filter, der nicht den Laufwerksbuchstaben oder das Stammverzeichnis verwendet (z.B. **Temp*** oder **Temp\File.tmp**), oder ein Filter, der mit einem Sternchen (*) beginnt (z.B. ***C:**), wird zu keiner Warnung bzw. keinem Fehler führen. Wenn das Betriebssystem der gesicherten Maschine jedoch nicht korrekt erkannt wird, werden auch diese Filter nicht funktionieren.

- **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).

**Hinweis**
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.

## Snapshot für Datei-Backups

Diese Option gilt nur für Backups auf Dateiebene.

Diese Option definiert, ob die Dateien bei einem Backup nacheinander gesichert oder mithilfe eines einmaligen Daten-Snapshots erfasst werden.

**Hinweis**
Dateien, die auf Netzwerkfreigaben gespeichert sind, werden immer nacheinander gesichert.

Die Voreinstellung ist:

- Wenn nur Maschinen zum Backup ausgewählt wurden, die unter Linux laufen: **Keinen Snapshot erstellen.**
- Ansonsten: **Snapshot erstellen, sofern möglich.**

Sie können eine der folgenden Optionen wählen:

- **Snapshot erstellen, sofern möglich**
  Dateien direkt sichern, sofern kein Snapshot möglich ist.

- **Snapshot immer erstellen**

  Der Snapshot ermöglicht es, alle Dateien zu sichern – auch solcher, die mit einem exklusiven Zugriff geöffnet sind. Die gesicherten Dateien haben alle den gleichen Backup-Zeitpunkt. Wählen Sie diese Einstellung nur, wenn diese Faktoren kritisch sind, d.h. ein Backup der Dateien ohne den vorhergehenden Snapshot keinen Sinn macht. Wenn kein Snapshot erstellt werden kann, wird das Backup fehlschlagen.
- **Keinen Snapshot erstellen**

  Dateien immer direkt sichern. Der Versuch, Dateien zu sichern, die per exklusivem Zugriff geöffnet sind, führt hier zu einem Fehler. Außerdem ist die Backup-Zeit der Dateien nicht gleich.

## Forensische Daten

Schadprogramme wie 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

**Hinweis**
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 Cyber Protect Webkonsole 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 Cyber Protect Webkonsole 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.

## Beglaubigung von Backups mit forensischen Daten

Um sicherzustellen, dass ein Forensik-Backup wirklich genau dem erfassten Image entspricht und dass dieses nicht kompromittiert wurde, führt das Backup-Modul bei Backups mit forensischen Daten eine Beglaubigung (Notarization) durch.

### Und so funktioniert es

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

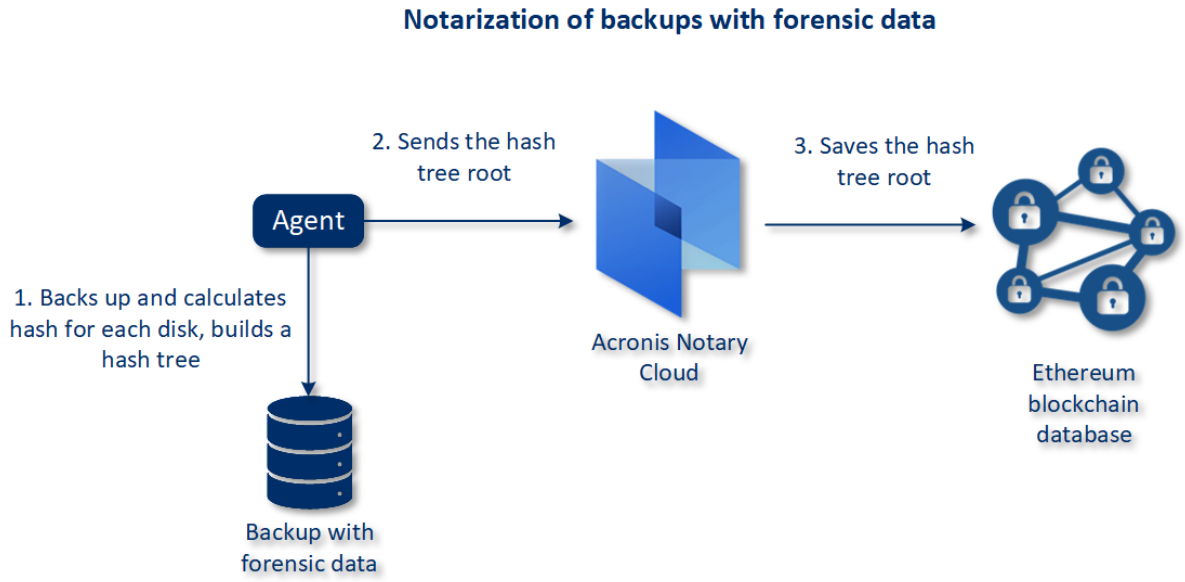
Der Agent berechnet während eines Backups die Hash-Werte der gesicherten Laufwerke, erstellt einen Hash-Baum, speichert diesen Hash-Baum mit im Backup und sendet dann das Stammverzeichnis (Root) des Hash-Baums an den Notary Service. Der Notary Service speichert das Wurzelverzeichnis des Hash-Baums in der Blockchain-Datenbank von Ethereum. Damit wird sichergestellt, dass dieser Wert nicht mehr geändert werden kann.

Wenn die Authentizität des Laufwerks mit den forensischen Daten überprüft werden soll, berechnet der Agent den Hash-Wert des Laufwerks und vergleicht diesen dann mit dem Hash-Wert, der im Hash-Baum innerhalb des Backups gespeichert ist. Sollten diese Hash-Werte nicht übereinstimmen,

wird das Laufwerk als 'nicht authentisch' eingestuft. Im anderen Fall ist die Authentizität des Laufwerks durch den Hash-Baum verbürgt.

Um zu verifizieren, dass der Hash-Baum selbst nicht kompromittiert wurde, sendet der Agent den Wert des Hash-Baum-Wurzelverzeichnisses an den Notary Service. Der Notary Service vergleicht diesen Wert mit dem, der in der Blockchain-Datenbank gespeichert ist. Wenn die Hash-Werte übereinstimmen, ist das ausgewählte Laufwerk garantiert authentisch. Falls nicht, zeigt die Software über eine Nachricht an, dass das Laufwerk nicht authentisch ist.

Das untere Schema soll den Beglaubigungsprozess für Backups mit forensischen Daten verdeutlichen.




Wenn Sie das beglaubigte Laufwerk-Backup manuell verifizieren wollen, können Sie dessen Zertifikat abrufen und die mit dem Zertifikat angezeigte Verifizierungsprozedur befolgen (mithilfe des Tools tibxread).

## Das Zertifikat für Backups mit forensischen Daten abrufen

Gehen Sie folgendermaßen vor, um das Zertifikat eines Backups mit forensischen Daten von der Konsole aus abzurufen:

1. Gehen Sie zu **Backup Storage** und wählen Sie das gewünschte Backup mit forensischen Daten aus.
2. Stellen Sie die komplette Maschine wieder her.
3. Das System öffnet die Anzeige **Laufwerkszuordnung**.
4. KlickenSie auf das Symbol **Zertifikat abrufen** für das entsprechende Laufwerk.
5. Das System wird das Zertifikat generieren und das Zertifikat in einem neuen Browser-Fenster öffnen. Unter dem Zertifikat wird Ihnen eine Anweisung angezeigt, wie Sie das beglaubigte Laufwerk-Backup manuell verifizieren können.

## Das Tool "tibxread" zum Abrufen von Backup-Daten

Cyber Protect 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. Es befindet sich an folgendem Speicherort: `C:\Program Files\Acronis\BackupAndRecovery`.

Folgende Speicherorte werden unterstützt:

- Ein lokales Laufwerk
- Ein Netzwerkordner (CIFS/SMB), auf den ohne Anmeldedaten zugegriffen werden kann.
  Bei einem kennwortgeschützten Netzwerkordner können Sie diesen mithilfe von Betriebssystemtools als lokalen Ordner mounten – und diesen lokalen Ordner dann als Datenquelle für das Tool verwenden.
- Der Cloud Storage
  Sie müssen die URL, den Port und das Zertifikat angeben. Die URL und der Port können aus dem entsprechenden Windows-Registry-Schlüssel oder bei Linux-/Mac-Maschinen aus den entsprechenden Konfigurationsdateien ermittelt werden.
  Für Windows:

  ```
  HKEY_LOCAL_
  MACHINE\SOFTWARE\Acronis\BackupAndRecovery\Settings\OnlineBackup\FesAddressCache\Defa
  ult\<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 (diese 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:<br>• Name des lokalen Pfads (in Windows)<br>`c:/upload/backups`<br>• Name des lokalen Pfads (in Linux)<br>`/var/tmp`<br>• SMB/CIFS<br>`\\server\folder`<br>• Cloud Storage<br>`--loc=<IP_address>:443 --cert=<path_to_certificate> [--storage_path=/1]`<br>`<IP-Adresse>` – Sie können die IP-Adresse unter Windows im folgenden Registry-Schlüssel finden: HKEY_LOCAL_ |

| | |
|---|---|
| | MACHINE\SOFTWARE\Acronis\BackupAndRecovery\Settings\OnlineBackup\FesAddressCache\Default\<Mandanten-Anmeldename>\FesUri<br>`<Pfad_zum_Zertifikat>` – der Pfad zur Zertifikatsdatei, um auf Cyber Cloud zugreifen zu können. Unter Windows lautet der Pfad für das Zertifikat: `C:\ProgramData\Acronis\BackupAndRecovery\OnlineBackup\Default\<Benutzername>.crt` – wobei <Benutzername> Ihrem Kontonamen entspricht, den Sie für den Zugriff auf Cyber 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.<br>Ausgabebeispiel ohne '`--raw`':<br>`GUID Date Date timestamp`<br>`---- ------ --------------`<br>`516FCE73-5E5A-49EF-B673-A9EACB4093B8 18.12.2019 16:01:05 1576684865`<br>`516FCE73-5E5A-49EF-B673-A9EACB4093B9 18.12.2019 16:02:05 1576684925`<br>Ausgabebeispiel mit '`--raw`':<br>`516FCE73-5E5A-49EF-B673-A9EACB4093B8 18.12.2019 16:01:05 1576684865`<br>`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.<br>Beispiel:<br>`1%`<br>`2%`<br>`3%`<br>`4%`<br>`...`<br>`100%` |

## Protokollabschneidung

Diese Option gilt für Backups von Microsoft SQL Server-Datenbanken und für Laufwerk-Backups mit aktiviertem Microsoft SQL Server-Applikations-Backup.

Diese Option bestimmt, ob die SQL-Transaktionsprotokolle nach einem erfolgreichen Backup abgeschnitten werden.

Die Voreinstellung ist: **Aktiviert**.

Wenn diese Option aktiviert ist, kann eine Datenbank nur auf einen Zeitpunkt zurückgesetzt (wiederhergestellt) werden, zu dem es ein von der Software erstelltes Backup gibt. Deaktivieren Sie diese Option, wenn Sie die Transaktionsprotokolle mithilfe der integrierten Backup-Engine des Microsoft SQL Servers sichern. Sie können die Transaktionsprotokolle nach der Wiederherstellung anwenden – und damit eine Datenbank auf einen beliebigen Zeitpunkt zurücksetzen (wiederherstellen).

## LVM-Snapshot-Erfassung

Diese Option gilt nur für physische Maschinen.

Diese Option gilt für Laufwerk-Backups von Volumes, die vom Linux Logical Volume Manager (LVM) verwaltet werden. Solche Volumes werden auch als 'logische Volumes' bezeichnet.

Diese Option definiert, wie der Snapshot eines logischen Volumes erfasst wird. Die Backup-Software kann dies eigenständig tun oder den Linux Logical Volume Manager (LVM) beanspruchen.

Die Voreinstellung ist: **Durch die Backup-Software**.

- **Durch die Backup-Software**. Die Snapshot-Daten werden überwiegend im RAM gehalten. Das Backup ist schneller und es wird kein nicht zugeordneter Speicherplatz auf der Volume-Gruppe benötigt. Wir empfehlen die Voreinstellung 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.

## Mount-Punkte

Diese Option ist nur unter Windows und für ein Datei-basiertes Backup wirksam, dessen Datenquelle gemountete Volumes oder freigegebene Cluster-Volumes enthält.

Diese Option ist nur wirksam, wenn Sie einen Ordner als Backup-Quelle auswählen, der in der Verzeichnishierarchie höher als der Mount-Punkt liegt. (Ein Mount-Punkt ist ein Ordner, an den ein zusätzliches Volume logisch angeschlossen ist).

- Wenn ein solcher Ordner (oder ein übergeordneter Ordner) als Backup-Quelle ausgewählt wird – und die Option **Mount-Punkte** aktiviert wurde – dann werden alle auf dem gemounteten Volume liegenden Dateien in das Backup aufgenommen. Wenn die Option **Mount-Punkte** deaktiviert wurde, bleibt der Mount-Punkt im Backup leer.

  Bei der Wiederherstellung eines übergeordneten Ordners hängt die Frage, ob auch der Inhalt des Mount-Punktes wiederhergestellt wird (oder nicht) davon ab, ob die Option **Mount-Punkte** für die Recovery-Aktion aktiviert oder deaktiviert wurde.
- Wenn Sie den Mount-Punkt direkt auswählen oder einen Ordner innerhalb des gemounteten Volumes, dann werden die gewählten Ordner wie herkömmliche Ordner betrachtet. Sie werden

unabhängig vom Status der Backup-Option **Mount-Punkte** gesichert – genauso, wie sie unabhängig vom Status der Recovery-Option **Mount-Punkte** wiederhergestellt werden.

Die Voreinstellung ist: **Deaktiviert**.

**Hinweis**
Sie können virtuelle Maschinen vom Typ Hyper-V sichern, die auf einem freigegebenen Cluster-Volume liegen, indem Sie die benötigten Dateien oder das komplette Volume per Datei-basiertem Backup sichern. Fahren Sie die virtuellen Maschinen herunter, um zu gewährleisten, dass sie in einem konsistenten Zustand gesichert werden.

**Beispiel**

Angenommen, der Ordner **C:\Daten1** ist der Mount-Punkt für ein gemountetes Volume. Das Volume enthält die Verzeichnisse **Ordner1** und **Ordner2**. Sie erstellen einen Schutzplan für ein Datei-Backup Ihrer Daten.

Wenn Sie das Volume C per Kontrollkästchen auswählen und dafür die Option **Mount-Punkte** aktivieren, wird der Ordner **C:\Daten1** in Ihrem Backup auch die Verzeichnisse **Ordner1** und **Ordner2** enthalten. Wenn Sie die gesicherten Daten dann später wiederherstellen, sollten Sie an die entsprechende, gewünschte Einstellung der Option **Mount-Punkte** für Recovery-Aktionen denken.

Wenn Sie das Volume C per Kontrollkästchen auswählen und die Option **Mount-Punkte** jedoch deaktivieren, wird der Ordner **C:\Daten1** in Ihrem Backup leer sein.

Wenn Sie die Verzeichnisse **Daten1**, **Ordner1** oder **Ordner2** direkt selbst per Kontrollkästchen zum Backup auswählen, werden diese markierten Ordner wie herkömmliche Ordners in Backup aufgenommen – unabhängig vom Status der Option **Mount-Punkte**.

## Multi-Volume-Snapshot

Diese Option gilt nur für Backups von physischen Maschinen, die mit Windows oder Linux laufen.

Diese Option gilt für Laufwerk-Backups. Diese Option gilt auch für Backups auf Dateiebene, wenn diese unter Verwendung eines Snapshots erstellt werden. (Die Option Snapshot für Datei-Backups bestimmt, ob bei einem solchen Backup ein Snapshot benutzt wird oder nicht.)

Diese Option bestimmt, ob die Snapshots bei mehreren Volumes gleichzeitig oder nacheinander erfasst werden sollen.

Die Voreinstellung ist:

- Wenn mindestens eine Maschine, die mit Windows läuft, zum Backup ausgewählt wurde: **Aktiviert**.
- Wenn keine Maschine ausgewählt ist (dies ist der Fall, wenn Sie die Erstellung eines Schutzplans von der Seite **Pläne** –> **Backup** beginnen): **Aktiviert**.
- Ansonsten: **Deaktiviert**.

Wenn diese Option aktiviert ist, werden die Snapshots aller zu sichernden Volumes gleichzeitig erstellt. Verwenden Sie diese Option, um ein zeitkonsistentes Backup von Daten zu erstellen, die über mehrere Volumes verteilt sind (z.B. für eine Oracle-Datenbank).

Wenn diese Option deaktiviert ist, werden die Snapshots der Volumes nacheinander erfasst. Falls sich die Daten also über mehrere Volumes erstrecken, werden diese zu unterschiedlichen Zeiten gesichert. Das resultierende Backup ist daher möglicherweise nicht konsistent.

# One-Click Recovery

Mit der One-Click Recovery-Funktion können Anwender das letzte Laufwerk-Backup ihrer Maschinen automatisch wiederherstellen. Dabei kann es sich um ein Backup der kompletten Maschine oder um ein Backup bestimmter Laufwerke oder Volumes auf dieser Maschine handeln.

Diese Funktion ist auf der Maschine eines Anwenders verfügbar, wenn ein Administrator sie zusammen mit dem Startup Recovery Manager aktiviert hat. Der Administrator kann diese Aktion nur über die Befehlszeilenschnittstelle durchführen. Weitere Informationen darüber, wie Sie den Startup Recovery Manager und die One-Click Recovery-Funktion aktivieren können, finden Sie in der Befehlszeilenreferenz.

Die One-Click Recovery-Funktion unterstützt folgende Backup Storages:

1. Einer Secure Zone
2. Netzwerk-Storages
3. Cloud Storage

Wenn ein bestimmter Storage-Typ nicht verfügbar ist oder es dort keine Laufwerk-Backups gibt, wird der Benutzer aufgefordert, den nächsten Storage-Typ zu verwenden.

Wenn mehr als ein Backup-Set (auch *Archiv* genannt) mit Laufwerk-Backups im Storage vorliegt, wählt die One-Click Recovery-Funktion dasjenige Backup-Set aus, das als letztes aktualisiert wurde. Der Benutzer kann kein anderes Backup-Set auswählen.

Die One-Click Recovery-Funktion unterstützt folgende Aktionen:

- Automatische Wiederherstellung aus dem letzten Backup
- Wiederherstellung aus einem bestimmten Backup (auch *Recovery-Punkt* genannt) innerhalb des automatisch ausgewählten Backup-Sets

## Eine Maschine per One-Click Recovery wiederherstellen

### Voraussetzungen

- Ein Administrator hat die One-Click Recovery-Funktion auf der ausgewählten Maschine aktiviert.
- Es gibt mindestens ein Laufwerk-Backup der ausgewählten Maschine.

***So können Sie eine Maschine wiederherstellen***

1. Starten Sie die Maschine neu, die Sie wiederherstellen wollen.
2. Drücken Sie während des Neustarts die Taste F11, um zum Startup Recovery Manager zu gelangen.
3. Wählen Sie die gewünschte One-Click Recovery-Option aus:
   - Drücken Sie die Taste 1 auf der Tastatur, um automatisch das letzte Backup wiederherstellen zu lassen.
   - Drücken Sie die Taste 2 auf der Tastatur, um ein anderes Backup aus dem jüngsten Backup-Set wiederherzustellen.
     - Wenn Sie ein bestimmtes Backup (auch *Recovery-Punkt* genannt) auswählen wollen, drücken Sie die dazugehörige Nummer auf der Tastatur.

Die grafische Benutzeroberfläche wird gestartet und verschwindet dann wieder. Die Prozedur wird ohne sie fortgesetzt. Wenn die Wiederherstellung abgeschlossen wurde, wird Ihre Maschine neu gestartet.

## Performance und Backup-Fenster

Mit dieser Option können Sie für jede Stunde innerhalb einer Woche eine von drei Backup-Performance-Stufen (hoch, niedrig, verboten) festlegen. Auf diese Weise können Sie ein Zeitfenster definieren, in dem Backups gestartet und ausgeführt werden dürfen. Die hohen und niedrigen Performane-Stufen sind in Bezug auf Prozesspriorität und Ausgabegeschwindigkeit konfigurierbar.

Diese Option ist nicht verfügbar für Backups, die von Cloud Agenten ausgeführt werden – wie z.B. Website-Backups oder Backups von Servern, die sich auf einer Cloud-Recovery-Site befinden.

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.

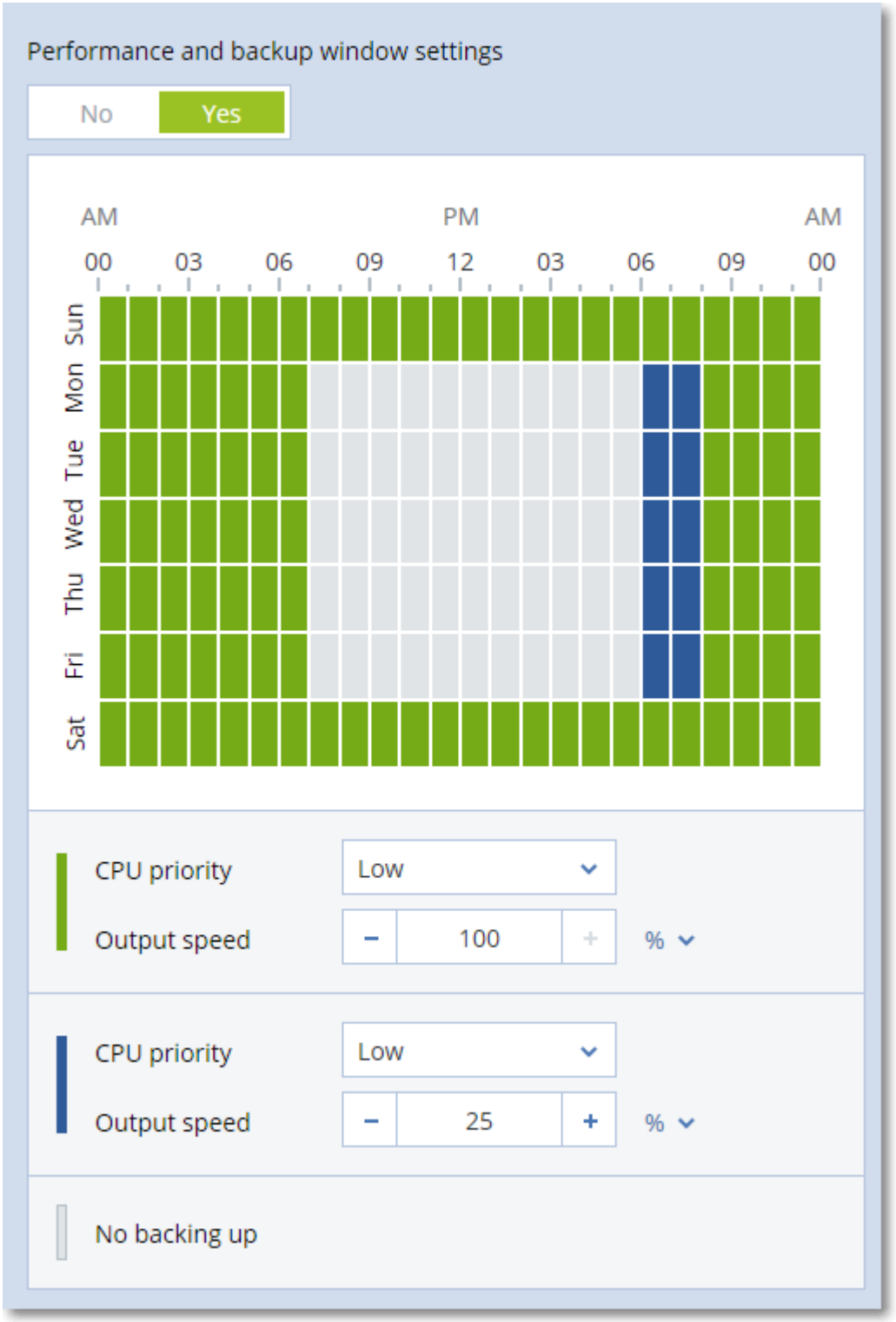
Auch wenn geplante Backups blockiert werden, kann ein Backup immer noch manuell gestartet werden. Es werden die Performance-Parameter der letzten Stunde verwendet, zu der Backups erlaubt waren.

## 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:

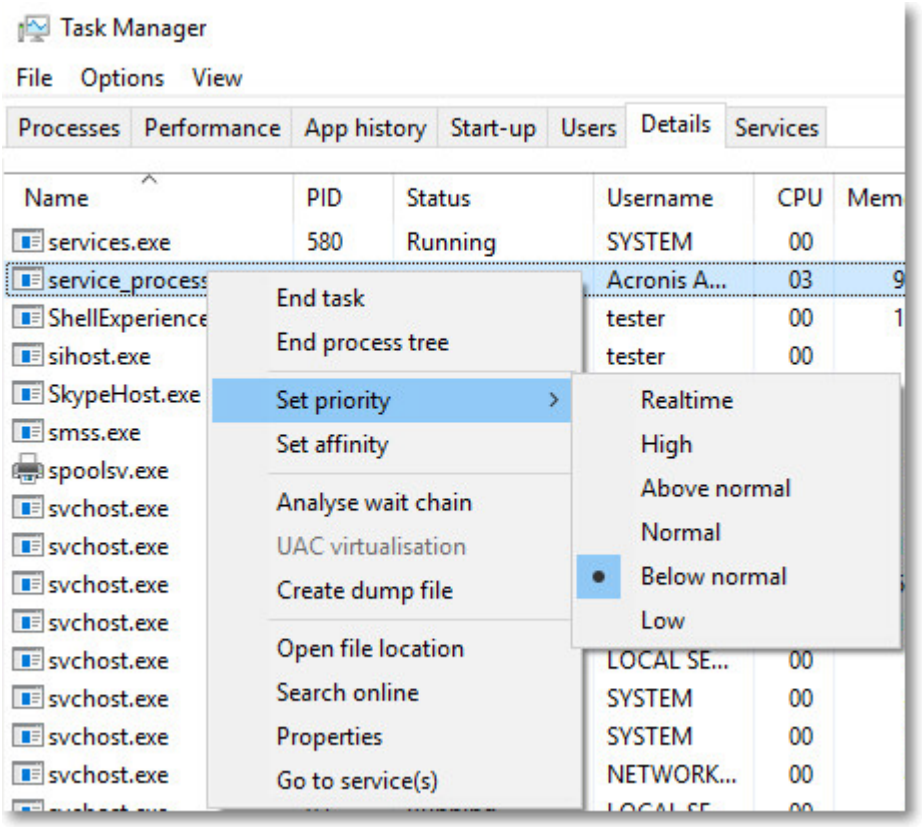
**Niedrig** – in Windows, entspricht **Niedriger als normal**.

**Normal** – in Windows, entspricht **Normal**.

**Hoch** – in Windows, entspricht **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).

## Physischer Datenversand

Diese Option gilt, wenn als Backup-Ziel der Cloud Storage verwendet wird und das Backup-Format 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 und Agenten für Hyper-V erstellt wurden. Backups, die von einem Boot-Medium aus erstellt wurden, werden nicht unterstützt.

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 Organisationsadministratoren in On-Premise-Bereitstellungen und Administratoren in Cloud-Bereitstellungen 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.

   Gehen Sie folgendermaßen vor, um auf diese Weboberfläche zuzugreifen:

   - Bei On-Premise-Bereitstellungen: melden Sie sich an Ihrem Acronis Konto an und klicken Sie bei **Physischer Datenversand** auf den Befehl **Zur Tracking-Konsole gehen**.
   - Bei Cloud-Bereitstellungen: melden Sie sich am Management-Portal an, klicken Sie 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.

## 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.

Das Programm führt die Replikation *nach* Ausführung des Nach-Backup-Befehls aus.

Das Programm unterstützt keine interaktiven Befehle, d.h. Befehle, die eine Reaktion des Benutzers erfordern, wie z.B. 'Pause'.

## Befehl vor dem Backup

***So spezifizieren Sie einen Befehl bzw. eine Stapelverarbeitungsdatei, die vor dem Start des Backups ausgeführt wird***

1. Aktivieren Sie den Schalter **Einen Befehl vor dem Backup ausführen**.
2. Geben Sie im Feld **Befehl** ein Kommando ein oder wählen Sie eine vorbereitete Stapelverarbeitungsdatei aus dem Dateisystem aus. Das Programm unterstützt keine interaktiven Befehle, d.h. Befehle, die eine Reaktion des Benutzers erfordern (wie z.B. 'Pause').
3. Spezifizieren Sie im Eingabefeld **Arbeitsverzeichnis** einen Pfad zu einem Verzeichnis, in dem der Befehl bzw. die Stapelverarbeitungsdatei durchgeführt werden soll.
4. Tragen Sie Argumente für die Befehlsausführung in das Feld **Argumente** ein, wenn das erforderlich ist.
5. Wählen Sie in der unteren Tabelle die passenden Optionen, abhängig vom Ergebnis, das Sie erreichen wollen.
6. Klicken Sie auf **Fertig**.

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

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

### 'Nach-Backup'-Befehl

***So spezifizieren Sie einen Befehl bzw. eine Stapelverarbeitungsdatei, die ausgeführt wird, wenn ein Backup erfolgreich abgeschlossen wurde.***

1. Aktivieren Sie den Schalter **Einen Befehl nach dem Backup ausführen**.
2. Geben Sie im Feld **Befehl** ein Kommando ein oder wählen Sie eine vorbereitete Stapelverarbeitungsdatei aus dem Dateisystem aus.
3. Spezifizieren Sie im Eingabefeld **Arbeitsverzeichnis** einen Pfad zu einem Verzeichnis, in dem der Befehl bzw. die Stapelverarbeitungsdatei durchgeführt werden soll.
4. Tragen Sie, sofern erforderlich, in das Feld **Argumente** entsprechende Parameter für die Befehlsausführung ein.
5. Aktivieren Sie das Kontrollkästchen **Backup scheitern lassen, wenn die Befehlsausführung fehlschlägt**, sofern eine erfolgreiche Ausführung des Befehls besonders wichtig für Sie ist. Der Befehl wird als 'fehlgeschlagen' betrachtet, wenn sein Exit-Code ungleich Null ist. Sollte die Befehlsausführung fehlschlagen, erhält der Backup-Status den Wert '**Fehler**'.
   Wenn das Kontrollkästchen deaktiviert ist, hat das Ergebnis der Befehlsausführung keinen Einfluss darauf, ob die Backup-Ausführung als erfolgreich oder fehlgeschlagen eingestuft wird. Sie können das Ergebnis der Befehlsausführung in der Registerkarte **Aktivitäten** überwachen.
6. Klicken Sie auf **Fertig**.

## Befehle vor/nach der Datenerfassung

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

Das folgende Schema zeigt, wann diese Befehle ausgeführt werden.

<table>
<tr><td></td><td colspan="4"><b><----------</b> <b>Backup</b> <b>----------></b></td><td></td></tr>
<tr><td>Befehl vor dem Backup</td><td>Befehl vor Datenerfassung</td><td>Datenerfassung</td><td>Befehl nach Datenerfassung</td><td></td><td>'Nach-Backup'-Befehl</td></tr>
</table>

Wenn die Option Volume Shadow Copy Service (VSS) 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.

## Befehl vor Datenerfassung

***So spezifizieren Sie einen Befehl bzw. eine Stapelverarbeitungsdatei, die vor der Datenerfassung ausgeführt wird***

1. Aktivieren Sie den Schalter **Einen Befehl vor der Datenerfassung ausführen**.
2. Geben Sie im Feld **Befehl** ein Kommando ein oder wählen Sie eine vorbereitete Stapelverarbeitungsdatei aus dem Dateisystem aus. Das Programm unterstützt keine interaktiven Befehle, d.h. Befehle, die eine Reaktion des Benutzers erfordern (wie z.B. 'Pause').
3. Spezifizieren Sie im Eingabefeld **Arbeitsverzeichnis** einen Pfad zu einem Verzeichnis, in dem der Befehl bzw. die Stapelverarbeitungsdatei durchgeführt werden soll.
4. Tragen Sie Argumente für die Befehlsausführung in das Feld **Argumente** ein, wenn das erforderlich ist.
5. Wählen Sie in der unteren Tabelle die passenden Optionen, abhängig vom Ergebnis, das Sie erreichen wollen.
6. Klicken Sie auf **Fertig**.

| **Kontrollkästchen** | **Auswahl** | | | |
|---|---|---|---|---|
| **Backup scheitern lassen, wenn die Befehlsausführung fehlschlägt*** | Ausgewählt | Deaktiviert | Ausgewählt | Deaktiviert |
| **Datenerfassung erst ausführen, wenn die Befehlsausführung abgeschlossen ist** | Ausgewählt | Ausgewählt | Deaktiviert | Deaktiviert |
| **Ergebnis** | | | | |
| | **Voreinstellung** Datenerfassung nur ausführen, nachdem der Befehl erfolgreich durchgeführt wurde. Backup 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.

## 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**<br>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.

## SAN-Hardware-Snapshots

Diese Option gilt für die Backups von virtuellen VMware ESXi-Maschinen.

Die Voreinstellung ist: **Deaktiviert**.

Diese Option bestimmt, ob SAN-Snapshots verwendet werden sollen, wenn ein Backup durchgeführt wird.

Wenn diese Option deaktiviert ist, werden die Inhalte der virtuellen Laufwerke aus einem VMware-Snapshot ausgelesen. Der Snapshot wird über die komplette Dauer des Backups aufbewahrt.

Wenn diese Option aktiviert ist, werden die Inhalte der virtuellen Laufwerke aus einem SAN-Snapshot ausgelesen. Ein VMware-Snapshot wird erstellt und kurzfristig aufbewahrt, um die virtuellen Laufwerke in einen konsistenten Zustand zu bringen. Wenn kein SAN-Snapshot ausgelesen werden kann, wird das Backup fehlschlagen.

Überprüfen Sie vor Aktivierung dieser Option, ob die im Abschnitt 'SAN-Hardware-Snapshots verwenden' aufgelisteten Anforderungen erfüllt sind.

## 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:

- On-Premise-Bereitstellung: **Alle Backups genau nach Planung starten.**
- Cloud-Bereitstellung: **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, 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.

## Sektor-für-Sektor-Backup

Die Option gilt nur für Backups auf Laufwerksebene.

Diese Option definiert, ob von einem Laufwerk/Volume eine exakte Kopie auf physischer Ebene erstellt werden soll.

Die Voreinstellung ist: **Deaktiviert**.

Wenn diese Option aktiviert ist, werden beim Backup eines Laufwerks/Volumes alle vorhandenen Sektoren gesichert – einschließlich der Sektoren von 'nicht zugeordnetem' und 'freiem' Speicherplatz. Das resultierende Backup wird die gleiche Größe wie das gesicherte Laufwerk haben (sofern die Option 'Komprimierungsgrad' auf **Ohne** eingestellt ist). Die Software schaltet automatisch auf den Sektor-für-Sektor-Modus um, wenn ein Laufwerk ein Dateisystem verwendet, welches nicht erkannt oder nicht unterstützt wird.

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

## Aufteilen

Diese Option gilt für die Backup-Schemata **Nur vollständig**; **Wöchentlich vollständig, täglich inkrementell**; **Monatlich vollständig, wöchentlich differentiell, täglich inkrementell (GVS)** und **Benutzerdefiniert**.

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

Die Voreinstellung ist: **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.

# Bandverwaltung

Diese Optionen sind wirksam, wenn es sich bei dem Backup-Ziel um ein Bandgerät handelt.

## Datei-Recovery für auf Bändern gespeicherte Laufwerk-Backups aktivieren

Die Voreinstellung ist: **Deaktiviert**.

Falls dieses Kontrollkästchen aktiviert ist, erstellt die Software bei jedem Backup zusätzliche Dateien auf einem Festplattenlaufwerk der Maschine, an der das Bandgerät angeschlossen ist. Datei-Recovery von Laufwerk-Backups ist möglich, solange diese zusätzlichen Dateien intakt sind. Die Dateien werden automatisch gelöscht, wenn das Band, auf dem die entsprechenden Backups gespeichert sind, gelöscht, entfernt oder überschrieben wird.

Die Speicherorte der zusätzlichen Dateien sind:

- In Windows XP und Server 2003: **%ALLUSERSPROFILE%\Application Data\Acronis\BackupAndRecovery\TapeLocation**.
- In Windows 7 und höheren Versionen von Windows: **%PROGRAMDATA%\Acronis\BackupAndRecovery\TapeLocation**.
- Unter Linux: **/var/lib/Acronis/BackupAndRecovery/TapeLocation**.

Der von diesen zusätzlichen Dateien belegte Speicherplatz hängt von der Anzahl der Dateien im entsprechenden Backup ab. Beim Voll-Backup eines Laufwerks mit ungefähr 20.000 Dateien (typisches Laufwerk-Backup einer Workstation) belegen die zusätzlichen Dateien ca. 150 MB. Das Voll-Backup eines Servers mit 250.000 Dateien kann etwa 700 MB an zusätzlichen Dateien erzeugen. Sollten Sie sicher sein, dass Sie die Wiederherstellung einzelner Dateien nicht benötigen, dann können Sie das Kontrollkästchen deaktiviert lassen, um Speicherplatz zu sparen.

Falls die zusätzlichen Dateien während des Backups nicht erstellt wurden oder falls sie gelöscht wurden, dann können Sie sie immer noch durch erneutes scannen derjenigen Bänder erstellen, die das Backup enthalten.

## Band nach jedem erfolgreichen Backup einer Maschine zurück in den Slot verschieben

Die Voreinstellung ist: **Aktiviert**.

Falls Sie diese Option deaktivieren, verbleibt ein Band in dem Laufwerk, nachdem eine Aktion mit dem Band abgeschlossen wurde. Ansonsten wird die Software das Band wieder zurück zu dem Slot verschieben, wo es sich vor der Aktion befand. Falls, laut Schutzplan, auf das Backup weitere Aktionen folgen (beispielsweise eine Backup-Validierung oder Replikation zu einem anderen Speicherort), so wird das Band nach Abschluss dieser Aktionen wieder zurück in seinen Slot verschoben.

Wenn diese Option und die Option **Bänder nach jedem erfolgreichen Backup einer Maschine auswerfen** aktiviert sind, wird das Band ausgeworfen.

## Bänder nach jedem erfolgreichen Backup einer Maschine auswerfen

Die Voreinstellung ist: **Deaktiviert**.

Wenn dieses Kontrollkästchen aktiviert wird, wirft die Software Bänder nach jedem erfolgreichen Backup einer jeden Maschine aus. Falls, laut Schutzplan, auf das Backup weitere Aktionen folgen (beispielsweise eine Backup-Validierung oder Replikation zu einem anderen Speicherort), so werden die Bänder nach Abschluss dieser Aktionen ausgeworfen.

## Band im autonomen Bandlaufwerk bei Erstellung eines Voll-Backups überschreiben

Die Voreinstellung ist: **Deaktiviert**.

Diese Option gilt nur für autonome Bandlaufwerke. Wenn diese Option aktiviert ist, wird ein in das Laufwerk eingelegtes Band jedes Mal überschrieben, wenn ein Voll-Backup erstellt wird.

## Folgende Bandgeräte und Laufwerke verwenden

Mit dieser Option können Sie Bandgeräte und Bandlaufwerke spezifizieren, die vom Schutzplan verwendet werden sollen.

Ein Bandpool enthält Bänder von allen Bandgeräten, die an eine Maschine angeschlossen sind – egal ob es ein Storage Node oder eine Maschine mit einem installierten Protection Agenten ist (oder beides). Wenn Sie einen Bandpool als Backup-Speicherort auswählen, wählen Sie indirekt auchz die Maschine aus, an welche das/die Bandgeräte angeschlossen sind. Standardmäßig können Band-Backups auf alle Bandlaufwerke und alle Bandgeräte geschrieben werden, die an diese Maschine angeschlossen sind. Wenn einige der Geräte oder Laufwerke nicht angeschlossen oder nicht betriebsbereit sind, verwendet der Schutzplan diejenigen, die verfügbar sind.

Sie können aber auch auf die Option **Nur ausgewählte Geräte und Laufwerke** klicken und denn bestimmte Bandgeräte/-laufwerke aus der Liste auswählen. Wenn Sie ein komplettes Gerät auswählen, wählen Sie auch all dessen Laufwerke aus. Das bedeutet, dass jedes dieser Laufwerke von dem Schutzplan verwendet werden kann. Wenn das ausgewählte Gerät oder Laufwerk fehlt oder nicht betriebsbereit ist und keine anderen Geräte ausgewählt wurden, wird das Backup fehlschlagen.

Mit dieser Option können Sie Backups kontrollieren, die von mehreren Agenten zu einer großen Bandbibliothek mit mehreren Laufwerken durchgeführt werden. Beispielsweise kann das Backup eines großen Datei-Servers oder einer Dateifreigabe nicht gestartet werden, wenn mehrere Agenten ihre Maschinen innerhalb desselben Backup-Fensters sichern, da die Agenten alle Laufwerke belegen. Wenn Sie den Agenten beispielsweise erlauben, die Laufwerke 2 und 3 zu verwenden, wird Laufwerk 1 für den Agenten reserviert, der die Dateifreigabe sichert.

## Multistreaming

Die Voreinstellung ist: **Deaktiviert**.

Multistreaming ermöglicht es Ihnen, die Daten eines Agenten in mehrere Datenströme aufzuteilen und diese Ströme dann gleichzeitig auf verschiedene Bänder zu schreiben. Dies führt zu schnelleren Backups und ist insbesonders nützlich, wenn der Agent einen höheren Datendurchsatz als das/die Bandlaufwerk(e) hat.

Das Kontrollkästchen **Multistreaming** ist nur verfügbar, wenn Sie bei der Option **Nur ausgewählte Geräte und Laufwerke** mehr als ein Bandlaufwerk ausgewählt haben. Die Anzahl der ausgewählten Laufwerke entspricht der Anzahl der gleichzeitigen Datenströme von einem Agenten. Wenn eines der ausgewählten Laufwerke beim Start eines Backups nicht verfügbar ist, wird das Backup fehlschlagen.

Wenn Sie Bänder mit einem Multistream- oder Multistream- und Multiplex-Backup wiederherstellen wollen, benötigen Sie mindestens die gleiche Anzahl von Laufwerken, die zum Erstellen dieses Backups verwendet wurden.

Sie können die Multistreaming-Einstellungen eines bereits vorhandenen Schutzplans nicht nachträglich ändern. Wenn Sie andere Einstellungen verwenden oder die ausgewählten Bandlaufwerke ändern möchten, müssen Sie einen neuen Schutzplan erstellen.

Multistreaming ist sowohl für lokal angeschlossene Bandlaufwerke als auch für Bandlaufwerke, die an einen Storage Node angeschlossen sind, verfügbar.

## Multiplexing

Die Voreinstellung ist: **Deaktiviert**.

Multiplexing ermöglicht es Ihnen, Datenströme von mehreren Agenten auf ein einziges Band zu schreiben. Dies kann zu einer besseren Auslastung von schnellen Bandlaufwerken führen. Standardmäßig ist der Multiplexing-Faktor – also die Anzahl der Agenten, die Daten an ein einzelnes Band senden – auf zwei (2) eingestellt. Sie können diesen Wert auf bis zu zehn (10) erhöhen.

Multiplexing ist nützlich in großen Umgebungen mit vielen Backup-Aktionen. Die Performance eines einzelnen Backups wird dadurch nicht verbessert.

Um das schnellstmögliche Backup in einer großen Umgebung zu erzielen, müssen Sie den Durchsatz Ihrer Agenten, Ihres Netzwerks und Ihrer Bandlaufwerke analysieren. Stellen Sie dann den Multiplexing-Faktor entsprechend ein, aber überhöhen Sie diesen nicht. Beispiel: Wenn Ihre Agenten Daten mit 70 Mbit/s liefern, Ihr Bandlaufwerk mit 250 Mbit/s schreibt und es keine Engpässe in Ihrem Netzwerk gibt, setzen Sie den Multiplexing-Faktor auf drei (3). Ein Multiplexing-Faktor von vier (4) würde zu einem „Übermultiplexing“ führen und die Performance des Backups wieder verringern. Üblicherweise liegt der Multiplexing-Faktor zwischen zwei (2) und fünf (5).

Aufgrund ihrer Struktur sind per Multiplexing erstellte Backups langsamer bei Wiederherstellungen. Je größer der Multiplexing-Faktor, desto langsamer wird die Wiederherstellung. Die gleichzeitige Wiederherstellung von mehreren Backups, die auf ein einzelnes Multiplex-Band geschrieben wurden, wird nicht unterstützt.

Sie können ein oder mehrere bestimmte Bandlaufwerke für das Multiplexing auswählen oder die Multiplexing-Option für jedes verfügbare Bandlaufwerk verwenden. Multiplexing ist nicht für lokal angeschlossene Bandlaufwerke verfügbar.

Sie können die Multiplexing-Einstellungen eines bereits vorhandenen Schutzplans nicht nachträglich ändern. Erstellen Sie einen neuen Schutzplan, wenn Sie andere Einstellungen verwenden wollen.

Innerhalb eines Schutzplans sind folgende Kombinationen aus Multistreaming und Multiplexing möglich:

- **Beide Optionen (Multistreaming und Multiplexing) sind deaktiviert.**
  Jeder Agent sendet Daten an ein einzelnes Bandlaufwerk.
- **Nur die Multistreaming-Option ist ausgewählt.**
  Jeder Agent sendet Daten an mindestens zwei Bandlaufwerke gleichzeitig.
- **Nur die Multiplexing-Option ist ausgewählt.**
  Jeder Agent sendet Daten an ein Bandlaufwerk, das Datenströme von mehreren Agenten gleichzeitig annimmt. Die maximale Anzahl der Datenströme, die ein Bandlaufwerk akzeptieren kann, ist im Schutzplan festgelegt und kann nicht im laufenden Betrieb geändert werden.
- **Beide Optionen (Multistreaming und Multiplexing) sind aktiviert.**
  Jeder Agent sendet Daten an mindestens zwei Bandlaufwerke, die Datenströme von mehreren Agenten gleichzeitig annehmen.

Ein Bandlaufwerk kann jeweils nur eine Art von Backup gleichzeitig schreiben – entweder gemultiplext oder nicht gemultiplext. Dies hängt davon ab, welcher Schutzplan zuerst gestartet wurde.

## Verwende Bandsätze innerhalb des Band-Pools, der für das Backup ausgewählt wurde

Die Voreinstellung ist: **Deaktiviert**.

Bänder innerhalb eines Pools können in so genannte **Bandsätze** gruppiert werden.

Falls Sie diese Option deaktiviert lassen, werden die Daten zu allen Bändern gesichert, die zu einem Pool gehören. Wenn diese Option aktiviert ist, können Sie Backups nach vordefinierten oder benutzerdefinierten Regeln trennen.

- **Einen separaten Bandsatz verwenden für jede** (wählen Sie eine Regel: **Backup-Typ**, **Gerätetyp**, **Gerätename**, **Tag im Monat**, **Wochentag**, **Monat des Jahres**, **Jahr**, **Datum**)
  Wenn diese Variante ausgewählt ist, können Sie Bandsätze nach einer vordefinierten Regel organisieren. Sie können beispielsweise separate Bandsätze für jeden Wochentag haben oder die Backups einer jeden Maschine auf einem separaten Bandsatz speichern.
- **Eine benutzerdefinierte Regel für Bandsätze spezifizieren**
  Wenn diese Variante ausgewählt ist, können Sie eine eigene Regel zur Organisation der Bandsätze spezifizieren. Diese Regel kann folgende Variablen enthalten:

| Variablensyntax | Variablenbeschreibung | Verfügbare Werte |
|---|---|---|
| `[Resource Name]` | Die Backups einer jeden Maschine werden auf einem separaten Bandsatz gespeichert. | Die Namen der Maschinen, die auf dem Management Server registriert sind. |
| `[Backup Type]` | Vollständige, inkrementelle und differentielle Backups werden auf separaten Bandsätzen gespeichert. | `full`, `inc`, `diff` |
| `[Resource Type]` | Die Backups von Maschinen werden je nach Typ auf einem separaten Bandsatz gespeichert. | `Server essentials`, `Server`, `Workstation`, `Physical machine`, `VMware Virtual Machine`, `Virtual-PC Virtual Machine`, `Virtual Server Virtual Machine`, `Hyper-V Virtual Machine`, `Parallels Virtual Machine`, `XEN Virtual Machine`, `KVM Virtual Machine`, `RHEV Virtual Machine`, `Parallels Cloud Virtual Machine` |
| `[Day]` | Die Backups eines jeden Tags im Monat werden auf einem separaten Bandsatz gespeichert. | `01`, `02`, `03`, ..., `31` |
| `[Weekday]` | Die Backups eines jeden Tags in der Woche werden auf einem separaten Bandsatz gespeichert. | `Sunday`, `Monday`, `Tuesday`, `Wednesday`, `Thursday`, `Friday`, `Saturday` |
| `[Month]` | Die Backups eines jeden Monats im Jahr werden auf einem separaten Bandsatz gespeichert. | `January`, `February`, `March`, `April`, `May`, `June`, `July`, `August`, `September`, `October`, `November`, `December` |
| `[Year]` | Die Backups eines jeden Jahres werden auf einem separaten Bandsatz gespeichert. | `2017`, `2018`, ... |

- Wenn Sie beispielsweise die Regel mit `[Resource Name]-[Backup Type]` spezifizieren, so erhalten Sie einen separates Bandsatz für jedes vollständige, inkrementelle und differentielle Backup einer jeden Maschine, auf die der Schutzplan angewendet wird.

Sie können außerdem Bandsätze für einzelne Bänder spezifizieren. In diesem Fall wird die Software zuerst Backups auf Bänder schreiben, deren Bandsatzwert mit dem Wert des Ausdrucks übereinstimmt, der im Schutzplan spezifiziert wurde. Dann werden, falls nötig, andere Bänder aus demselben Pool genommen. Danach werden, falls der Pool wiederauffüllbar ist, Bänder aus dem Pool **Freie Bänder** verwendet.

Wenn Sie beispielsweise den Bandsatz `Monday` für Band 1 spezifizieren, `Tuesday` für Band 2 usw. – und dann `[Weekday]` in den Backup-Optionen spezifizieren, wird am jeweiligen Tag der Woche das entsprechende Band verwendet.

## 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**.

## 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.

## 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 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 Drittanbieter-Software zum Backup von Exchange Server-Daten verwenden. Hintergrund ist, dass die Protokollabschneidung die aufeinanderfolgenden Transaktionsprotokoll-Backups beeinträchtigt.
- Falls Sie eine Drittanbieter-Software zum Backup der SQL Server-Daten verwenden. Hintergrund ist, dass die Drittanbieter-Software das resultierende Laufwerk-Backup als sein eigenes Voll-Backup ansehen wird. Als Folge wird das nächste differentielle Backup der SQL Server-Daten fehlschlagen. Die Backups werden solange fehlschlagen, bis die Drittanbieter-Software das nächste eigene Voll-Backup erstellt.
- Falls andere VSS-kompatible Applikationen auf der Maschine laufen und es aus irgendwelchen Gründen notwendig ist, deren Protokolle zu behalten.

Eine Aktivierung dieser Option bewirkt kein Abschneiden von Microsoft SQL Server-Protokollen. Wenn Sie das SQL Server-Protokoll nach einem Backup abschneiden lassen wollen, müssen Sie die Backup-Option 'Protokollabschneidung aktivieren.

## VSS (Volume Shadow Copy Service) für virtuelle Maschinen

Diese Option definiert, ob die virtuellen Maschinen mit stillgelegten (quiesced) Snapshots erfasst werden sollen. Um einen stillgelegten Snapshot zu erfassen, wendet die Backup-Software den VSS (Volumenschattenkopiedienst) innerhalb der virtuellen Maschine an – und zwar mithilfe der VMware Tools oder der Hyper-V-Integrationsdienste.

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' 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. Wir empfehlen, dass Sie diese Option immer aktiviert lassen, auch für virtuelle Maschinen, auf denen keine VSS-konformen Applikationen laufen. Anderenfalls kann auch die Intaktheit des Dateisystems innerhalb des erfassten Backups nicht gewährleistet werden.

**Hinweis**
Diese Option hat keinen Einfluss auf virtuelle Scale Computing HC3-Maschinen. Bei diesen hängt das Stilllegen (Quiescing) davon ab, ob die Scale-Tools auf der virtuellen Maschine installiert sind oder nicht.

## Wöchentliche Backups

Diese Option bestimmt, welche Backups in Aufbewahrungsregeln und Backup-Schemata als 'wöchentlich' betrachtet werden. Ein 'wöchentliches' Backup ist dasjenige Backup, das als erstes in einer Woche erstellt wird.

Die Voreinstellung ist: **Montag**.

## Windows-Ereignisprotokoll

Diese Option gilt nur für Windows-Betriebssysteme.

Diese Option definiert, ob die Agenten für alle Backup-Aktionen entsprechende Ereigniseinträge im Windows-Anwendungsereignisprotokoll hinterlegen sollen. Sie können die Protokolleinträge über die Windows-Ereignisanzeige einsehen, die per Eingabebefehl (eventvwr.exe) oder per Menü (**Systemsteuerung** –> **Verwaltung** –> **Ereignisanzeige**) aufgefrufen werden kann. Sie können die Ereignisse filtern, die geloggt werden.

Die Voreinstellung ist: **Deaktiviert**.

# Recovery

## Spickzettel für Wiederherstellungen

Die nachfolgende Tabelle fasst alle verfügbaren Recovery-Methoden zusammen. Verwenden Sie diese Tabelle, um diejenige Recovery-Methode zu finden, die am besten zu Ihren Bedürfnissen passt.

| Recovery-Quelle | Recovery-Methode |
|---|---|
| Physische Maschine (Windows oder Linux) | Weboberfläche verwenden<br>Boot-Medium verwenden |
| Physische Maschine (Mac) | Boot-Medium verwenden |
| Virtuelle Maschine (VMware, Hyper-V oder Scale Computing HC3) | Weboberfläche verwenden<br>Boot-Medium verwenden |
| ESXi-Konfiguration | Boot-Medium verwenden |
| Dateien/Ordner | Weboberfläche verwenden<br>Dateien aus dem Cloud Storage herunterladen<br>Boot-Medium verwenden<br>Dateien aus lokalen Backups extrahieren |
| Systemzustand | Weboberfläche verwenden |
| SQL-Datenbanken | Weboberfläche verwenden |
| Exchange-Datenbanken | Weboberfläche verwenden |
| Exchange-Postfächer | Weboberfläche verwenden |
| Microsoft 365-Postfächer | Weboberfläche verwenden |
| Oracle-Datenbanken | Oracle Explorer-Tool verwenden |

### Hinweis für Mac-Benutzer

- Ab Mac OS X 10.11 El Capitan werden bestimmte System-Dateien/-Ordner/-Prozesse mit dem erweiterten Datei-Attribut 'com.apple.rootless' gekennzeichnet und so besonders geschützt. Diese Funktion zur Wahrung der Systemintegrität wird auch SIP (System Integrity Protection) genannt. Zu den geschützten Dateien gehörten vorinstallierte Applikationen sowie die meisten Ordner in /system, /bin, /sbin, /usr.

  Solchermaßen geschützte Dateien und Ordner können bei einer Recovery-Aktion nicht überschrieben werden, wenn die Wiederherstellung unter dem Betriebssystem selbst ausgeführt

wird. Wenn es notwendig ist, diese geschützten Dateien zu überschreiben, müssen Sie die Wiederherstellung stattdessen mit einem Boot-Medium durchführen.

- Ab macOS Sierra 10.12 können selten verwendete Dateien mit der Funktion 'In iCloud speichern' in die Cloud verschoben werden. Von diesen Dateien werden im Dateisystem kleine 'Fußabdrücke' gespeichert. Bei einem Backup werden dann diese Datenfußabdrücke statt der Originaldateien gesichert.

  Wenn Sie einen solchen Datenfußabdruck an ursprünglichen Speicherort wiederherstellen, wird er mit der iCloud synchronisiert und die Originaldatei ist wieder verfügbar. Wenn Sie einen Datenfußabdruck an einem anderen Speicherort wiederherstellen, ist keine Synchronisierung möglich und ist die Originaldatei daher nicht verfügbar.

# Safe Recovery

Das Backup-Image eines Betriebssystems kann mit Malware infiziert sein. Diese kann die Maschine, auf welcher das Backup wiederhergestellt wird, erneut infizieren.

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

**Einschränkungen**:

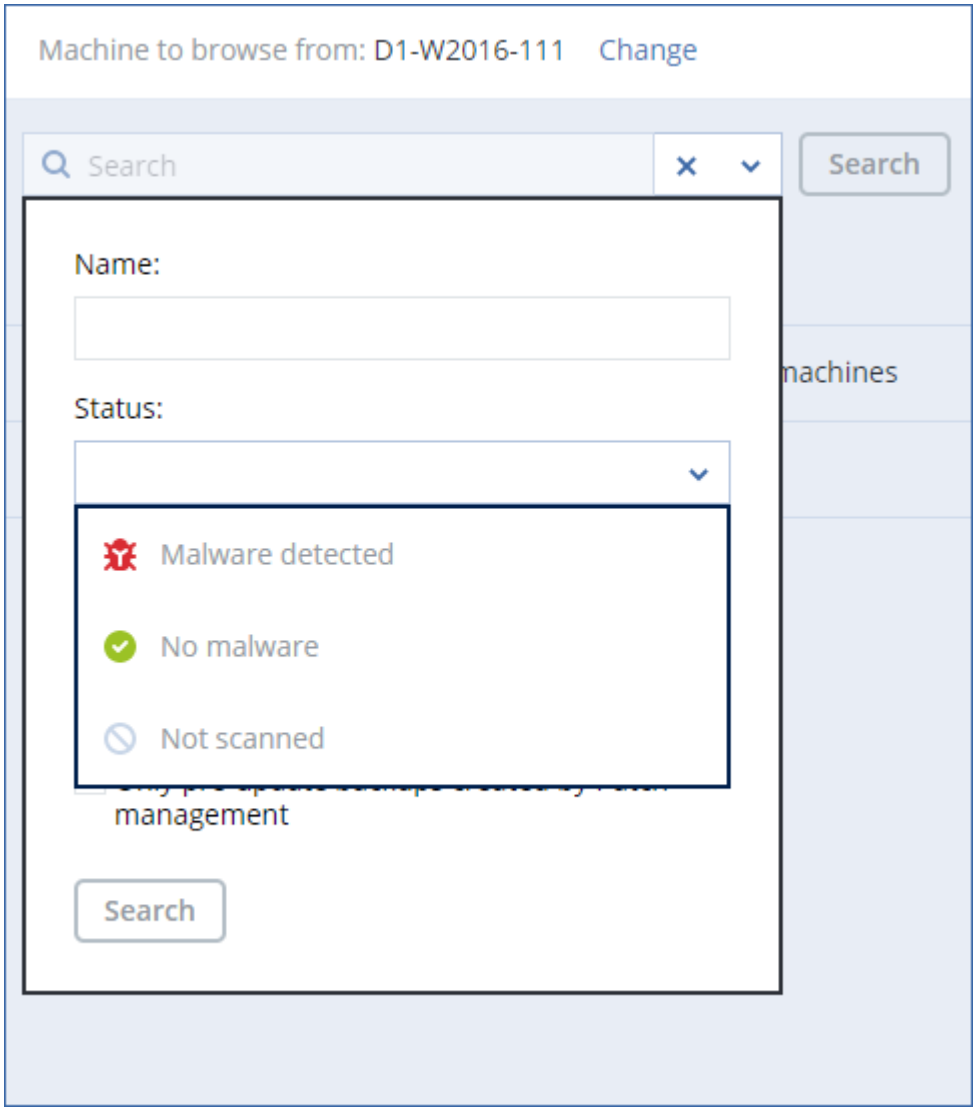
- Die Safe Recovery-Funktion wird nur für physische und virtuelle Windows-Maschinen unterstützt, auf denen zudem der Agent für Windows installiert ist.
- Es werden nur Backups vom Typ **Komplette Maschine** oder **Laufwerke/Volumes** unterstützt.
- Es werden nur Volumes mit NTFS-Dateisystem unterstützt. Nicht-NTFS-Volumes werden wiederhergestellt, ohne dass diese nach Malware gescannt werden.
- Safe Recovery wird nicht für Backups der kontinuierlichen Datensicherung (CDP) unterstützt. Eine Maschine wird auf der Grundlage des letzten regelmäßigen Backups wiederhergestellt – ohne die Daten im CDP-Backup. Wenn Sie die CDP-Daten wiederherstellen wollen, müssen Sie eine Wiederherstellung von **Dateien/Ordnern** ausführen.

## 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.




# 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. Um die Datei herunterzuladen, müssen Sie auf folgende Befehle klicken: in der rechten oberen Ecke auf das Symbol für das Konto klicken –> **Downloads** –> **Boot-Medium**.
2. 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.

Sie können das Boot-Medium alternativ auch mithilfe des Bootable Media Builders erstellen.

***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 dem Laufwerk werden gelöscht.

3. Klicken Sie auf **Erstellen**.
4. Warten Sie, bis die Software das Boot-Medium erstellt hat.

# Recovery einer Maschine

## Eine physische Maschine wiederherstellen

In diesem Abschnitt wird beschrieben, wie Sie eine physische Maschine über die Cyber Protect-Webkonsole wiederherstellen.

Verwenden Sie ein Boot-Medium statt der Cyber Protect-Webkonsole, wenn Sie Folgendes wiederherstellen müssen:

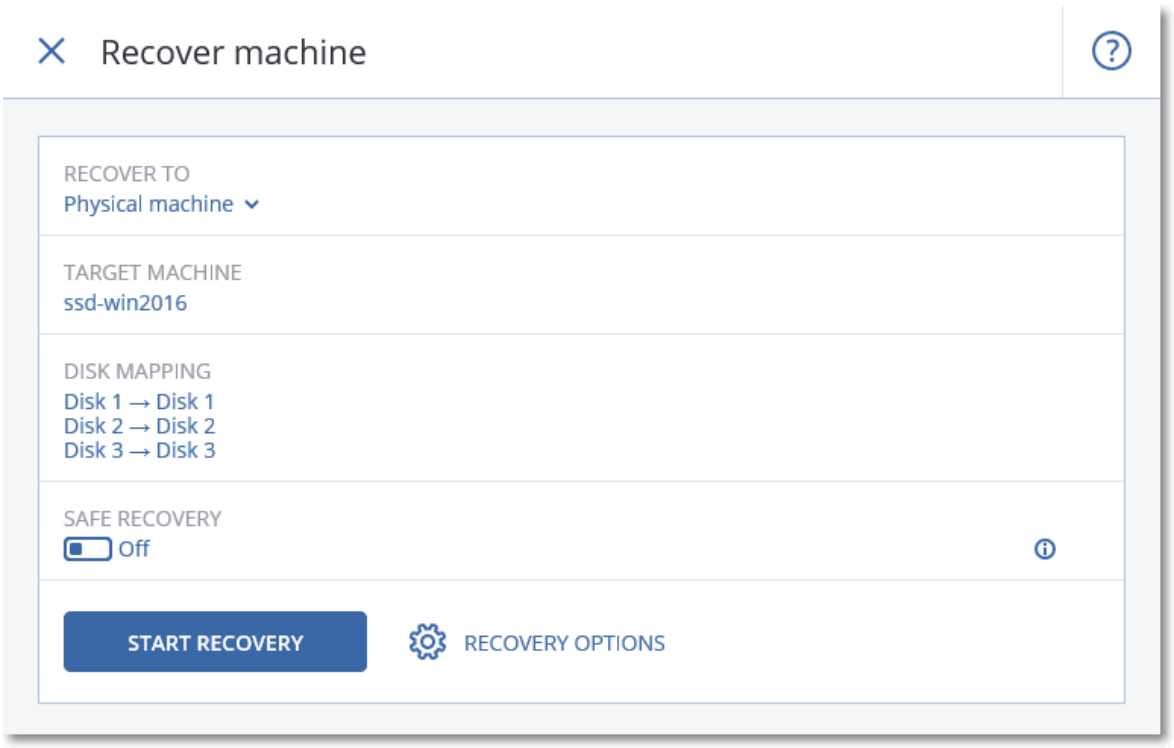
- Ein macOS-Betriebssystem
- Ein beliebiges Betriebssystem, das auf fabrikneuer Hardware (Bare Metal Recovery) oder zu einer Offline-Maschine wiederhergestellt werden soll

- 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.

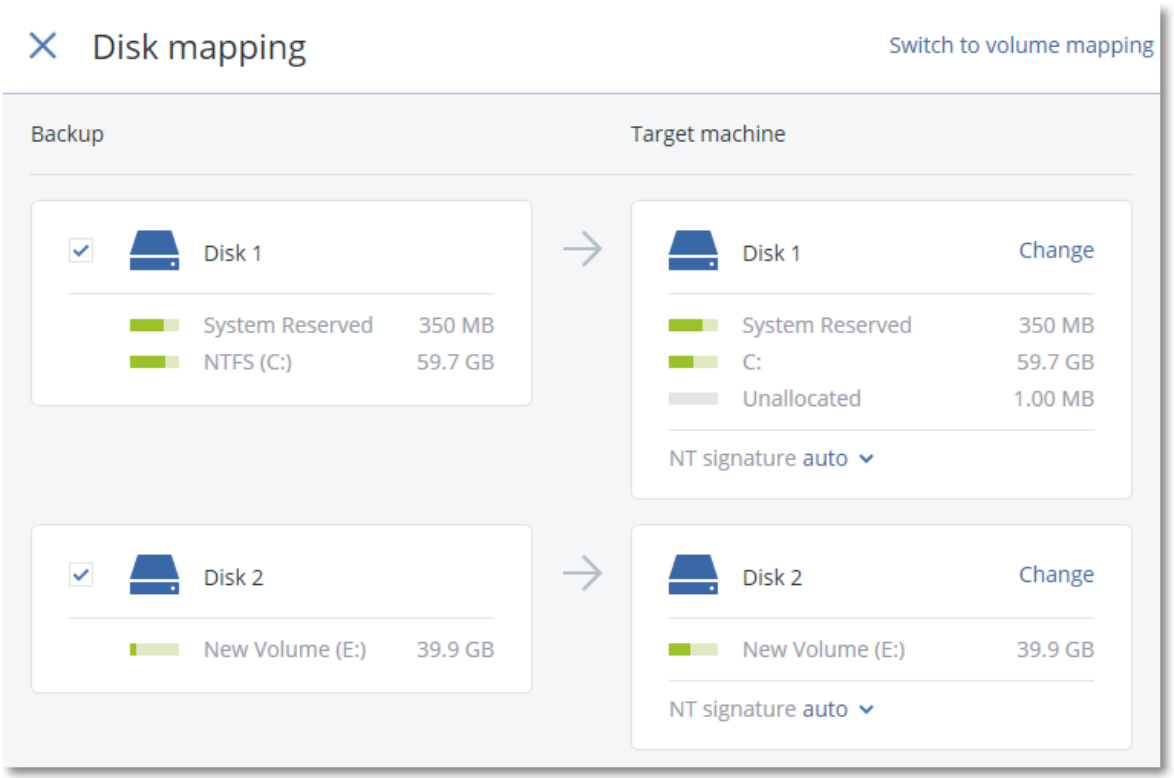
Die Wiederherstellung eines Betriebssystems und die Wiederherstellung von Volumes, die per BitLocker oder CheckPoint verschlüsselt wurden, erfordert einen Neustart. Weitere Informationen dazu finden Sie im Abschnitt '"Recovery mit Neustart" (S. 338)'.

***So können Sie eine physische Maschine wiederherstellen***

1. Wählen Sie die Maschine aus, die per Backup gesichert wurde.
2. Klicken Sie auf **Recovery**.
3. Wählen Sie einen Recovery-Punkt. Beachten Sie dabei, dass Recovery-Punkte nach Speicherorten gefiltert werden.
   Falls die Maschine offline ist, werden keine Recovery-Punkte angezeigt. Gehen Sie nach einer der folgenden Möglichkeiten vor:
   - Sollte sich das Backup im Cloud Storage oder einem freigegebenen Storage befinden (d.h., dass andere Agenten auf diesen zugreifen können), dann klicken Sie zuerst auf den Befehl **Maschine auswählen**. Wählen Sie anschließend eine Zielmaschine, die online ist, und dann den gewünschten Recovery-Punkt.
   - Wählen Sie einen Recovery-Punkt auf der Registerkarte 'Backup Storage'.
   - Stellen Sie die Maschine so wieder her, wie es im Abschnitt 'Laufwerke mithilfe eines Boot-Mediums wiederherstellen' beschrieben ist.
4. Klicken Sie auf **Recovery** –> **Komplette Maschine**.
   Die Software weist die Laufwerke im Backup automatisch den Laufwerken der Zielmaschine zu.
   Wenn Sie eine andere physische Maschine als Recovery-Ziel verwenden wollen, klicken Sie auf **Zielmaschine** und wählen Sie dann eine Zielmaschine aus, die online ist.




5. Falls die Zuordnung erfolglos war oder falls Sie mit dem Zuordnungsergebnis unzufrieden sind, können Sie auf **Laufwerkszuordnung** klicken, um die Laufwerke manuell zuzuordnen.
   Im Bereich 'Zuordnung' können Sie außerdem bestimmte Laufwerke oder Volumes für die Wiederherstellung auswählen. Mit dem Link **Wechseln zu...** (in der oberen rechten Ecke) können Sie zwischen Wiederherstellung von Laufwerken und Volumes wechseln.



6. [Optional] Aktivieren Sie den Switch **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.

## Eine physische Maschine zu einer virtuellen Maschine wiederherstellen

Sie können das Backup einer physischen Maschine zu einer virtuellen Maschine wiederherstellen.

Eine Wiederherstellung zu einer virtuellen Maschine ist möglich, wenn mindestens ein Agent für den entsprechenden Ziel-Hypervisor in Ihrer Umgebung installiert und auf dem Management Server registriert ist. Eine Wiederherstellung zu VMware ESXi erfordert beispielsweise, dass der Agent für VMware in der Umgebung installiert und auf dem Management Server registriert ist.

Einige Optionen sind nur bei der Cloud-Bereitstellung verfügbar.

Weitere Informationen zu den unterstützten Pfaden für Migrationen vom Typ 'physisch zu virtuell' (P2V) finden Sie im Abschnitt '"Migration von Maschinen" (S. 537)'.

**Hinweis**
Sie können keine Backups von physischen macOS-Maschinen als virtuelle Maschinen wiederherstellen.

***So können Sie eine physische Maschine als virtuelle Maschine wiederherstellen***

1. Wählen Sie die Maschine aus, die per Backup gesichert wurde.
2. Klicken Sie auf **Recovery**.
3. Wählen Sie einen Recovery-Punkt. Beachten Sie dabei, dass Recovery-Punkte nach Speicherorten gefiltert werden.
   Falls die Maschine offline ist, werden keine Recovery-Punkte angezeigt. Gehen Sie nach einer der folgenden Möglichkeiten vor:
   - Sollte sich das Backup im Cloud Storage oder einem gemeinsam genutzten Storage befinden (d.h., dass andere Agenten auf diesen zugreifen können), dann klicken Sie zuerst auf den Befehl **Maschine auswählen**. Wählen Sie anschließend eine Maschine aus, die online ist, und dann den gewünschten Recovery-Punkt.
   - Wählen Sie einen Recovery-Punkt auf der Registerkarte 'Backup Storage'.
   - Stellen Sie die Maschine so wieder her, wie es im Abschnitt '"Laufwerke und Volumes mithilfe eines Boot-Mediums wiederherstellen" (S. 339)' beschrieben ist.

4. Klicken Sie auf **Recovery** –> **Komplette Maschine**.
5. Wählen Sie unter **Wiederherstellungsziel** die Option **Virtuelle Maschine**.
6. Klicken Sie auf **Zielmaschine**.
   a. Wählen Sie den Hypervisor.

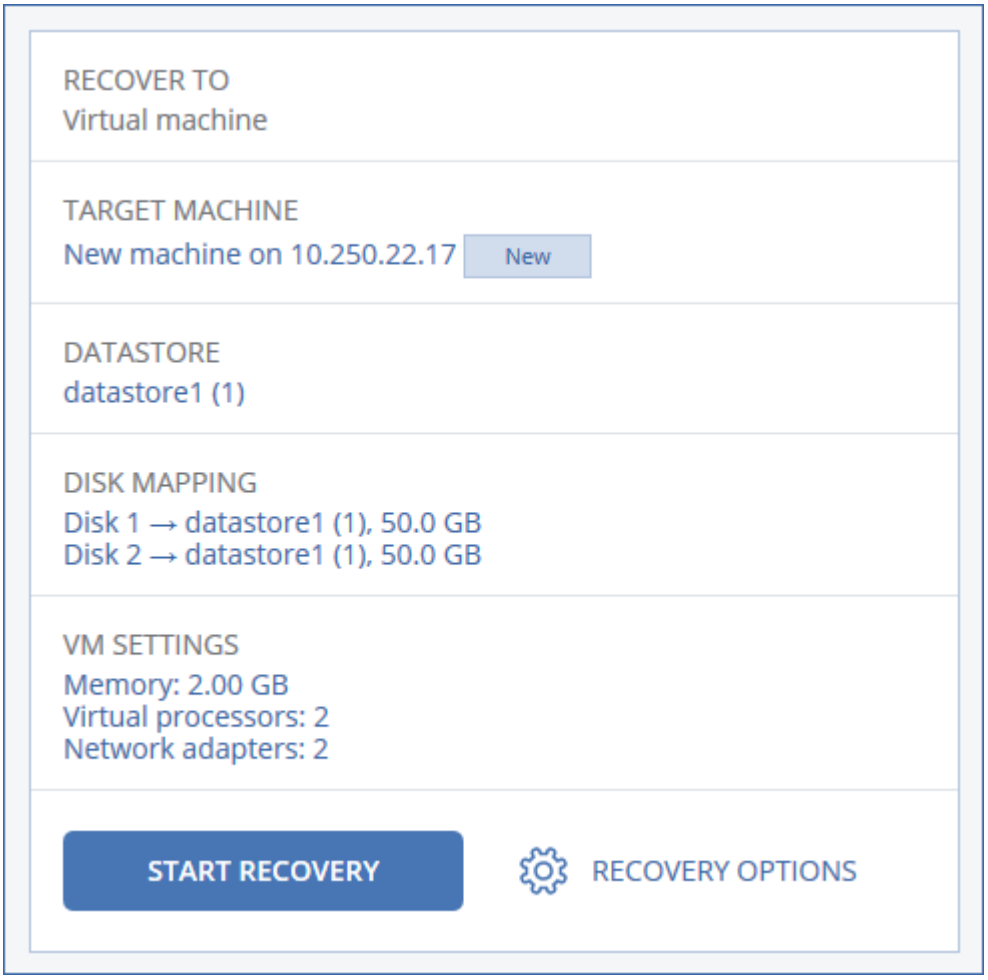
      **Hinweis**
      Es muss mindestens ein Agent für diesen Hypervisor in Ihrer Umgebung installiert und auf dem Management Server registriert sein.

   b. Bestimmen Sie, ob eine neue oder eine vorhandene Maschine als Recovery-Ziel verwendet werden soll. Die Option 'Neue Maschine' ist vorteilhafter, da hier die Laufwerkskonfiguration im Backup nicht exakt mit der Laufwerkskonfiguration der Zielmaschine übereinstimmen muss.
   c. Wählen Sie den Host und spezifizieren Sie einen Namen für die neue Maschine – oder wählen Sie eine bereits vorhandene Zielmaschine aus.
   d. Klicken Sie auf **OK**.
7. [Für Virtuozzo Hybrid Infrastructure ] Klicken Sie auf **VM-Einstellungen** und wählen Sie dann **Variante** (Englisch: Flavor) aus. Sie können optional die Größe des Arbeitsspeichers, die Anzahl der Prozessoren und die Netzwerkverbindungen für die virtuelle Maschine ändern.
8. [Optional] [Wenn Sie eine Wiederherstellung zu einer Maschine durchführen] Sie können zusätzliche Recovery-Optionen konfigurieren, die Sie benötigen:
   - [Nicht für Virtuozzo Hybrid Infrastructure und Scale Computing HC3 verfügbar] Wenn Sie das Speicherziel für die virtuelle Maschine auswählen wollen, klicken Sie auf **Datenspeicher** für ESXi, **Pfad** für Hyper-V bzw. Virtuozzo oder **Storage-Domain** für Red Hat Virtualization (oVirt) – und bestimmten Sie dann den Datenspeicher (Storage) für die virtuelle Maschine.
   - Klicken Sie auf **Laufwerkszuordnung**, um den Datenspeicher (Storage), die Schnittstelle und den Provisioning-Modus für jedes virtuelle Laufwerk auszuwählen. Im Bereich 'Zuordnung' können Sie bestimmte Laufwerke für die Wiederherstellung auswählen.

     **Hinweis**
     Sie können diese Einstellungen nicht ändern, wenn Sie einen Virtuozzo-Container oder eine virtuelle Maschine für Virtuozzo Hybrid Infrastructure wiederherstellen. Für Virtuozzo Hybrid Infrastructure können Sie nur die Storage-Richtlinie für die Ziellaufwerke auswählen. Wählen Sie dafür das gewünschte Ziellaufwerk aus und klicken Sie dann auf **Ändern**. Klicken Sie in dem sich öffnenden Blatt auf das Zahnradsymbol, wählen Sie die Storage-Richtlinie aus und klicken Sie dann auf **Fertig**.

   - [Für VMware ESXi, Hyper-V, Virtuozzo und Red Hat Virtualization/oVirt verfügbar] Klicken Sie auf **VM-Einstellungen**, um die Größe des Arbeitsspeichers, die Anzahl der Prozessoren und

die Netzwerkverbindungen für die virtuelle Maschine zu ändern.




9. Klicken Sie auf **Recovery starten**.
10. [Wenn Sie eine vorhandene virtuelle Maschine als Recovery-Ziel verwenden] Bestätigen Sie, dass Sie die Laufwerke überschreiben wollen.

Der Recovery-Fortschritt wird auf der Registerkarte **Aktivitäten** angezeigt.

## Eine virtuelle Maschine wiederherstellen

Sie können das Backup einer virtuellen Maschine zu einer physischen Maschine oder auch zu einer anderen virtuellen Maschine wiederherstellen.

Eine Wiederherstellung zu einer virtuellen Maschine ist möglich, wenn mindestens ein Agent für den entsprechenden Ziel-Hypervisor in Ihrer Umgebung installiert und auf dem Management Server registriert ist. Eine Wiederherstellung zu VMware ESXi erfordert beispielsweise, dass der Agent für VMware in der Umgebung installiert und auf dem Management Server registriert ist.

Einige Optionen sind nur bei der Cloud-Bereitstellung verfügbar.

Weitere Informationen zu den unterstützten Pfaden für Migrationen vom Typ 'virtuell zu physisch' (V2P) oder 'virtuell zu virtuell' (V2V) finden Sie im Abschnitt '"Migration von Maschinen" (S. 537)'.

**Hinweis**
Sie können keine virtuellen Maschinen mit macOS zu einem Hyper-V-Host wiederherstellen, weil macOS von Hyper-V nicht unterstützt wird. Sie können virtuelle Maschinen mit macOS zu einem VMware-Host wiederherstellen, wenn dieser auf Mac-Hardware installiert ist.

**Wichtig**
Eine virtuelle Maschine muss gestoppt werden, wenn Sie eine andere Maschine zu ihr wiederherstellen wollen. Standardmäßig stoppt die Software die Maschine ohne weitere Nachfrage. Wenn die Wiederherstellung abgeschlossen wurde, müssen Sie die Maschine manuell wieder starten. Sie können dieses vorgegebene Verhalten mithilfe der Recovery-Option für die VM-Energieverwaltung ändern (klicken Sie dafür auf **Recovery-Optionen** –> **VM-Energieverwaltung**).

***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'.
2. Klicken Sie auf **Recovery** –> **Komplette Maschine**.
3. [Bei Wiederherstellung zu einer physischen Maschine] Wählen Sie unter **Recovery zu** die Option **Physische Maschine**.
   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 '"Eine physische Maschine wiederherstellen" (S. 330)' fort. Falls dies nicht zutrifft, empfehlen wir Ihnen, eine Migration vom Typ 'virtuell zu physisch' (V2P) mithilfe eines Boot-Mediums durchzuführen.
4. [Optional] Standardmäßig ist die ursprüngliche Maschine als Zielmaschine vorausgewählt. 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.

      **Hinweis**
      Es muss mindestens ein Agent für diesen Hypervisor in Ihrer Umgebung installiert und auf dem Management Server registriert sein.

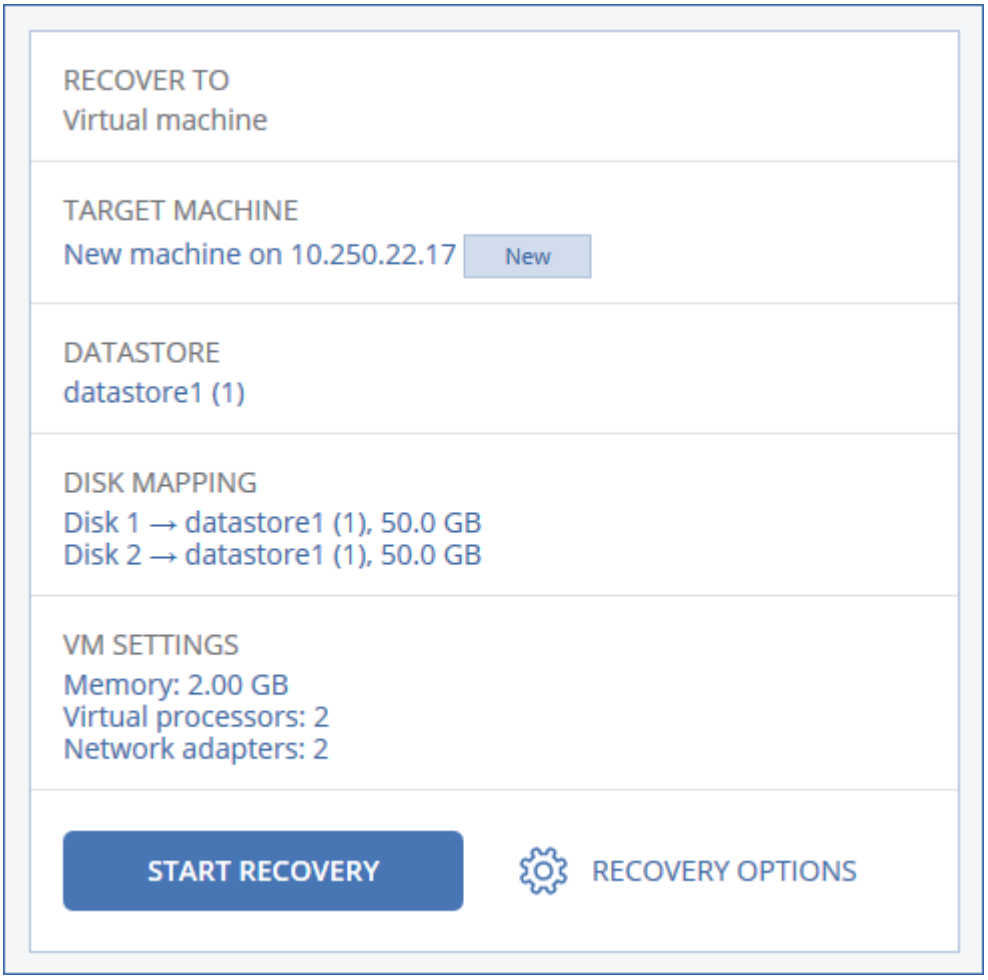
   b. Bestimmen Sie, ob eine neue oder eine vorhandene Maschine als Recovery-Ziel verwendet werden soll.
   c. Wählen Sie den Host und spezifizieren Sie dann einen Namen für die neue Maschine – oder wählen Sie eine bereits vorhandene Zielmaschine aus.
   d. Klicken Sie auf **OK**.

5. [Für Virtuozzo Hybrid Infrastructure ] Klicken Sie auf **VM-Einstellungen** und wählen Sie dann **Variante** (Englisch: Flavor) aus. Sie können optional die Größe des Arbeitsspeichers, die Anzahl der Prozessoren und die Netzwerkverbindungen für die virtuelle Maschine ändern.
6. [Optional] [Wenn Sie eine Wiederherstellung zu einer Maschine durchführen] Sie können zusätzliche Recovery-Optionen konfigurieren, die Sie benötigen:
   - [Nicht für Virtuozzo Hybrid Infrastructure und Scale Computing HC3 verfügbar] Wenn Sie das Speicherziel für die virtuelle Maschine auswählen wollen, klicken Sie auf **Datenspeicher** für ESXi, **Pfad** für Hyper-V bzw. Virtuozzo oder **Storage-Domain** für Red Hat Virtualization (oVirt) – und bestimmten Sie dann den Datenspeicher (Storage) für die virtuelle Maschine.
   - Klicken Sie auf **Laufwerkszuordnung**, um den Datenspeicher (Storage), die Schnittstelle und den Provisioning-Modus für jedes virtuelle Laufwerk auszuwählen. Im Bereich 'Zuordnung' können Sie bestimmte Laufwerke für die Wiederherstellung auswählen.

     **Hinweis**
     Sie können diese Einstellungen nicht ändern, wenn Sie einen Virtuozzo-Container oder eine virtuelle Maschine für Virtuozzo Hybrid Infrastructure wiederherstellen. Für Virtuozzo Hybrid Infrastructure können Sie nur die Storage-Richtlinie für die Ziellaufwerke auswählen. Wählen Sie dafür das gewünschte Ziellaufwerk aus und klicken Sie dann auf **Ändern**. Klicken Sie in dem sich öffnenden Blatt auf das Zahnradsymbol, wählen Sie die Storage-Richtlinie aus und klicken Sie dann auf **Fertig**.

   - [Für VMware ESXi, Hyper-V, Virtuozzo und Red Hat Virtualization/oVirt verfügbar] Klicken Sie auf **VM-Einstellungen**, um die Größe des Arbeitsspeichers, die Anzahl der Prozessoren und

die Netzwerkverbindungen für die virtuelle Maschine zu ändern.




7. Klicken Sie auf **Recovery starten**.
8. [Wenn Sie eine vorhandene virtuelle Maschine als Recovery-Ziel verwenden] Bestätigen Sie, dass Sie die Laufwerke überschreiben wollen.

Der Recovery-Fortschritt wird auf der Registerkarte **Aktivitäten** angezeigt.

## Recovery mit Neustart

Ein Neustart ist erforderlich, wenn Sie Folgendes wiederherstellen:

- Ein Betriebssystem
- Volumes, die mit BitLocker oder CheckPoint verschlüsselt wurden

**Wichtig**
Verschlüsselte Volumes, die per Backup gesichert wurden, werden als unverschlüsselte Volumes wiederhergestellt.

## Anforderungen

- Die Wiederherstellung von Volumes, die bei der Sicherung verschlüsselt waren, setzt voraus, dass sich auf derselben Maschine ein unverschlüsseltes Volume befindet. Dieses Volume muss außerdem über mindestens 1 GB freien Speicherplatz verfügen. Anderenfalls wird die Wiederherstellung fehlschlagen.
- Für die Wiederherstellung eines verschlüsselten System-Volumes sind keine weiteren Maßnahmen erforderlich. Wenn Sie ein verschlüsseltes Nicht-System-Volume wiederherstellen wollen, müssen Sie es zunächst sperren. Beispielsweise, indem Sie eine Datei öffnen, die sich auf diesem Volume befindet. Anderenfalls wird die Wiederherstellung ohne einen Neustart fortgesetzt, wodurch es passieren kann, dass das wiederhergestellte Volume von Windows nicht erkannt wird.

## Problembehebung (Troubleshooting)

Falls die Wiederherstellung fehlschlägt und Ihre Maschine mit der Fehlermeldung `Datei kann nicht von der Partition abgerufen werden` neu startet, sollten Sie die Secure Boot-Funktion deaktivieren. Weitere Informationen dazu finden Sie im Abschnitt Deaktivieren des sicheren Starts („Disabling Secure Boot“) in der Microsoft-Dokumentation.

# Laufwerke und Volumes mithilfe eines Boot-Mediums wiederherstellen

Informationen über die Erstellung eines Boot-Mediums finden Sie im Abschnitt '"Ein Boot-Medium erstellen" (S. 329)'.

***So können Sie Laufwerke und Volumes mithilfe eines Boot-Mediums wiederherstellen***

1. Booten Sie die Zielmaschine mit einem Boot-Medium.
2. [Nur bei macOS] Wenn Sie APFS-formatierte 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**.

**Hinweis**
Ab macOS 11 Big Sur kann das System-Volume nicht mehr gesichert und wiederhergestellt werden. Wenn Sie ein bootfähiges macOS-System wiederherstellen wollen, müssen Sie das Daten-Volume wiederherstellen und dann macOS darauf installieren.

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 und den Port des Proxy-Servers. Ansonsten können Sie diesen Schritt überspringen.
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.
   - 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 zuerst bei **Backup-Inhalte** die gewünschten **Laufwerke** oder **Volumes** aus und anschließend die Elemente, die Sie wiederherstellen wollen. Klicken Sie auf **OK**, um Ihre Auswahl zu bestätigen.

   **Wichtig**
   Wenn die gesicherte Maschine über dynamische Laufwerke oder logische Volumes (LVM) verfügt, wählen Sie die Option **Volumes**.
10. Die Software ordnet unter **Recovery-Ziel** die ausgewählten Laufwerke automatisch den Ziellaufwerken zu.
    Falls die Zuordnung erfolglos ist oder falls Sie mit dem Zuordnungsergebnis unzufrieden sind, können Sie die Laufwerke auch manuell zuordnen.

    **Hinweis**
    Eine Änderung des Laufwerk-Layouts kann die Bootfähigkeit des Betriebssystems beeinflussen. Verwenden Sie möglichst das ursprüngliche Laufwerkslayout der Maschine, außer Sie sind sich über das Ergebnis der Änderung absolut sicher.
11. [Nur bei macOS] Um ein APFS-formatiertes Daten-Volume als bootfähiges macOS-System wiederherstellen zu können, müssen Sie im Bereich **macOS-Installation** das Kontrollkästchen **macOS auf dem wiederhergestellten macOS-Daten-Volume installieren** aktiviert lassen.
    Nach der Wiederherstellung wird das System neu gebootet und die macOS-Installation automatisch gestartet. Sie benötigen eine Internetverbindung, damit der Installer die erforderlichen Dateien herunterladen kann.

Wenn Sie das APFS-formatierte Daten-Volume nicht als bootfähiges System wiederherstellen müssen, können Sie das Kontrollkästchen **macOS auf dem wiederhergestellten macOS-Daten-Volume installieren** deaktivieren. Sie können dieses Volume auch später noch bootfähig machen, indem Sie macOS manuell darauf installieren.

12. [Nur bei Linux] Falls die gesicherte Maschine logische Volumes (LVM) hat 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.
    c. Bestätigen Sie Ihre Wahl.
13. [Optional] Klicken Sie auf **Recovery-Optionen**, um zusätzliche Einstellungen zu spezifizieren.
14. Wählen Sie **OK**, um die Wiederherstellung zu starten.

## Universal Restore verwenden

Moderne Betriebssysteme behalten normalerweise ihre Bootfähigkeit, wenn sie auf abweichender Hardware (beinhaltet auch VMware- und Hyper-V-Maschinen) wiederhergestellt werden. Falls ein Betriebssystem nach einer Wiederherstellung dennoch nicht mehr bootet, können Sie das Tool 'Universal Restore' verwenden, um diejenigen Treiber und Module zu aktualisieren, die das Betriebssystem zum Starten auf der neuen Hardware/Maschine benötigt.

Universal Restore kann für Windows und Linux verwendet werden.

***So verwenden Sie Universal Restore***

1. Booten Sie die Maschine mithilfe eines Boot-Mediums.
2. Klicken Sie auf den Befehl **Universal Restore anwenden**.
3. Sollte es mehrere Betriebssysteme auf der Maschine geben, dann wählen Sie dasjenige System aus, welches von Universal Restore angepasst werden soll.
4. [Nur bei Windows] Konfigurieren Sie die 'Erweiterten Einstellungen'.
5. Klicken Sie auf **OK**.

## Universal Restore unter Windows

### Vorbereitung

#### Treiber vorbereiten

Bevor Sie Universal Restore auf ein Windows-Betriebssystem anwenden, sollten Sie sicherstellen, dass Sie über die passenden Treiber für den neuen Festplatten-Controller und den Chipsatz des Mainbords verfügen. Diese Treiber sind für den Start des Betriebssystem unerlässlich. Verwenden Sie (sofern vorhanden) die Treiber-CD/-DVD, die der Hardware-Hersteller Ihrem

Computer/Mainboard beigelegt hat – oder laden Sie benötigten Treiber von der Website des Herstellers herunter. Die Treiber sollten die Dateierweiterung *.inf verwenden. Wenn Sie die Treiber im Format *.exe, *.cab oder *.zip herunterladen, extrahieren Sie diese mit einer entsprechenden Dritthersteller-Anwendung.

Eine empfehlenswerte Vorgehensweise ist es, die benötigten Treiber (für die in Ihrer Organisation verwendete Hardware) an einem zentralen Aufbewahrungsort ('Repository') zu speichern und dabei nach Gerätetyp oder Hardware-Konfiguration zu sortieren. Sie können eine Kopie des Treiber-Repositorys zur leichteren Verwendung auch auf DVD oder USB-Stick vorhalten. Suchen Sie daraus die benötigten Treiber aus, um diese dem bootfähigen Medium hinzufügen zu können. Erstellen Sie dann für jeden Ihrer Server ein benutzerdefiniertes Boot-Medium mit den benötigten Treibern (und der benötigten Netzwerk-Konfiguration). Alternativ können Sie den Pfad zum Repository auch bei jeder Verwendung von Universal Restore spezifizieren.

### Überprüfen Sie, dass auf die Treiber in der bootfähigen Umgebung zugegriffen werden kann.

Überprüfen Sie, dass Sie beim Arbeiten mit dem bootfähigen Medium auf das Gerät mit den Treibern zugreifen können. Ein WinPE-basiertes Medium sollte dann zum Einsatz kommen, wenn ein Gerät unter Windows verfügbar ist, von einem Linux-basierten Medium aber nicht erkannt wird.

## Universal Restore-Einstellungen

### Automatische Suche nach Treibern

Spezifizieren Sie, wo das Programm nach Treibern für die Hardware-Abstraktionsschicht (HAL, Hardware Abstraction Layer) sowie für Festplatten-Controller und Netzwerkkarten suchen soll:

- Befinden sich die Treiber auf einem Datenträger (CD/DVD) des Herstellers oder einem anderen Wechselmedium, dann aktivieren Sie **Wechselmedien durchsuchen**.
- Liegen die Treiber in einem Netzwerkordner oder auf einem bootfähigen Medium, so spezifizieren Sie den Pfad zu diesem Ordner durch Anklicken von **Ordner durchsuchen**.

Zusätzlich wird Universal Restore den Standardspeicherort (Ordner) für Treiber durchsuchen. Dessen genaue Position ist über den Registry-Wert **DevicePath** definiert, der im Registry-Schlüssel **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion** gefunden werden kann. Üblicherweise befindet sich dieser Speicherordner im Unterverzeichnis 'WINDOWS/inf'.

Universal Restore führt im spezifizierten Ordner und seinen Unterordnern eine rekursive Suche durch, ermittelt dann unter allen verfügbaren Festplatten-Controller- und HAL-Treibern diejenigen, die am besten geeignet sind, und installiert diese Treiber schließlich im System. Universal Restore sucht außerdem nach Treibern für Netzwerkkarten. Der Pfad zu einem gefundenen Treiber wird dem Betriebssystem dann von Universal Restore mitgeteilt. Falls die Hardware über mehrere Netzwerkkarten verfügt, versucht Universal Restore, die Treiber für alle Karten zu konfigurieren.

### Auf jeden Fall zu installierende Massenspeichertreiber

Sie benötigen diese Einstellung falls:

- Die Hardware einen speziellen Massenspeicher-Controller verwendet – z.B. einen RAID- (insbesondere NVIDIA RAID) oder Fibre Channel-Adapter.
- Sie ein System zu einer virtuellen Maschine migriert haben, die einen SCSI-Festplatten-Controller verwendet. Verwenden Sie diejenigen SCSI-Treiber, die zusammen mit Ihrer Virtualisierungssoftware ausgeliefert werden. Alternativ können Sie die neueste Treiberversion vermutlich auch von der Website des betreffenden Software-Herstellers herunterladen.
- Falls die automatische Suche nach Treibern nicht hilft, das System zu booten.

Spezifizieren Sie die entsprechenden Treiber, indem Sie auf den Befehl **Treiber hinzufügen** klicken. Treiber, die hier definiert werden, werden auch dann (mit entsprechenden Warnmeldungen) installiert, wenn das Programm einen besseren Treiber findet.

### Der Universal Restore-Prozess

Klicken Sie auf **OK**, nachdem Sie die benötigten Einstellungen spezifiziert haben.

Falls Universal Restore an den angegebenen Speicherorten keinen kompatiblen Treiber findet, zeigt es eine Eingabeaufforderung für das Problemgerät an. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:

- Fügen Sie den Treiber einem der zuvor spezifizierten Speicherorte hinzu und klicken Sie dann auf **Wiederholen**.
- Klicken Sie auf **Ignorieren**, falls Sie sich nicht mehr an den Speicherort erinnern können, damit der Prozess fortgesetzt wird. Sollte das Ergebnis nicht zufriedenstellend sein, dann wenden Sie Universal Restore erneut an. Spezifizieren Sie bei Konfiguration der Aktion den benötigten Treiber.

Sobald Windows bootet, wird es die Standardprozedur zur Installation neuer Hardware initialisieren. Der Treiber für die Netzwerkkarte wird ohne weitere Nachfrage installiert, sofern er eine passende Microsoft Windows-Signatur hat. Anderenfalls verlangt Windows eine Bestätigung, dass der unsignierte Treiber installiert werden soll.

Danach können Sie die Netzwerk-Verbindung konfigurieren und weitere Treiber spezifizieren (beispielsweise für die Grafikkarte und USB-Geräte).

## Universal Restore unter Linux

Universal Restore kann auf Linux-Betriebssysteme mit der Kernel-Version 2.6.8 (oder höher) angewendet werden.

Wenn Universal Restore auf ein Linux-Betriebssystem angewendet wird, aktualisiert es ein temporäres Dateisystem, das auch als 'Initial RAM-Disk' (initrd) bekannt ist. Dadurch wird gewährleistet, dass das Betriebssystem auch auf neuer, abweichender Hardware booten kann.

Universal Restore kann dieser 'Initial RAM-Disk' benötigte Module für die neue Hardware hinzufügen (einschließlich Gerätetreiber). Es findet die benötigten Module normalerweise im Verzeichnis **/lib/modules**. Falls Universal Restore ein benötigtes Modul nicht finden kann, schreibt es den Dateinamen des Moduls in das Log.

Universal Restore kann unter Umständen die Konfiguration des GRUB-Boot-Loaders ändern. Dies kann beispielsweise notwendig sein, um die Bootfähigkeit des Systems zu gewährleisten, falls die neue Maschine ein anderes Volume-Layout als die ursprüngliche hat.

Universal führt keine Änderungen am Linux-Kernel durch!

### Zur ursprünglichen 'Initial RAM-Disk' zurücksetzen

Sie können bei Bedarf zur ursprünglichen 'Initial RAM-Disk' zurücksetzen.

Die 'Initial RAM-Disk' ist auf der Maschine in Form einer Datei gespeichert. Bevor Universal Restore die 'Initial RAM-Disk' zum ersten Mal aktualisiert, speichert es diese als Kopie ab – und zwar im gleichen Verzeichnis. Der Name dieser Kopie entspricht dem Dateinamen, ergänzt um das Suffix _ **acronis_backup.img**. Diese Kopie wird auch dann nicht überschrieben, wenn Sie Universal Restore mehrmals ausführen (beispielsweise nachdem Sie fehlende Treiber hinzugefügt haben).

Sie können folgendermaßen vorgehen, um zur ursprünglichen 'Initial RAM-Disk' zurückzukehren:

- Benennen Sie die Kopie passend um. Führen Sie beispielsweise einen Befehl, der ungefähr so aussieht:

  ```
  mv initrd-2.6.16.60-0.21-default_acronis_backup.img initrd-2.6.16.60-0.21-default
  ```

- Spezifizieren Sie die Kopie in der Zeile **initrd** der GRUB-Boot-Loader-Konfiguration.

# Dateien wiederherstellen

## Dateien 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 nachfolgenden Möglichkeiten vor:

   - [Empfohlen] Sollte sich das Backup im Cloud Storage oder einem freigegebenen Storage befinden (d.h., dass andere Agenten auf diesen zugreifen können), dann klicken Sie zuerst auf den Befehl **Maschine auswählen**. Wählen Sie anschließend eine Zielmaschine, die online ist, und dann den gewünschten Recovery-Punkt.
   - Wählen Sie einen Recovery-Punkt auf der Registerkarte 'Backup Storage'.
   - Laden Sie die Dateien aus dem Cloud Storage herunter.
   - Verwenden Sie ein Boot-Medium.
4. Klicken Sie auf **Wiederherstellen** –> **Dateien/Ordner**.

5. Wechseln Sie zum benötigten Ordner oder verwenden Sie die 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'

   **Hinweis**
   Für Laufwerk-Backups, die im Cloud Storage gespeichert sind, ist keine Suchfunktion verfügbar.

6. Wählen Sie die Dateien, die Sie wiederherstellen wollen.
7. Falls Sie die Dateien als .zip-Archiv speichern wollen, müssen Sie zuerst auf **Download** klicken, dann den Zielspeicherort für die Daten bestimmen und schließlich auf **Speichern** klicken. Ansonsten können Sie diesen Schritt überspringen.
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 Scale Computing HC3 installiert ist (sofern die Dateien von einer virtuellen ESXi-, Hyper-V- oder Scale Computing HC3-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.
10. Klicken Sie auf **Recovery starten**.
11. Wählen Sie eine der folgenden Optionen zum Überschreiben:

    - **Vorhandene Dateien überschreiben**
    - **Vorhandene Datei überschreiben, wenn diese älter ist**
    - **Vorhandene Dateien nicht überschreiben**

Der Recovery-Fortschritt wird auf der Registerkarte **Aktivitäten** angezeigt.

## Dateien aus dem Cloud Storage herunterladen

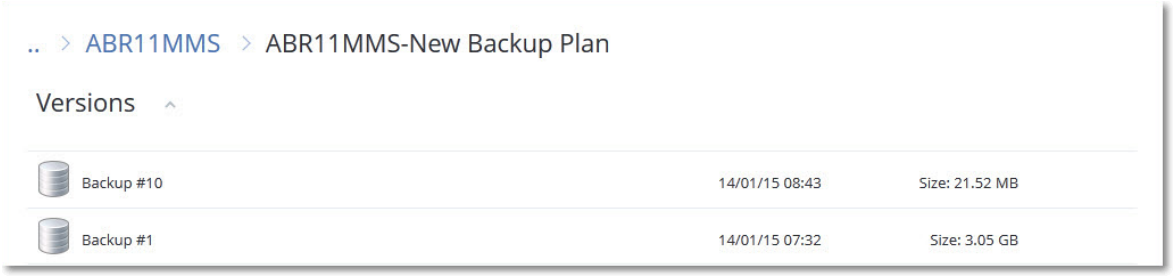
Sie können den Cloud Storage durchsuchen, die Inhalte von Backups einsehen und benötigte Dateien herunterladen.

## 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.

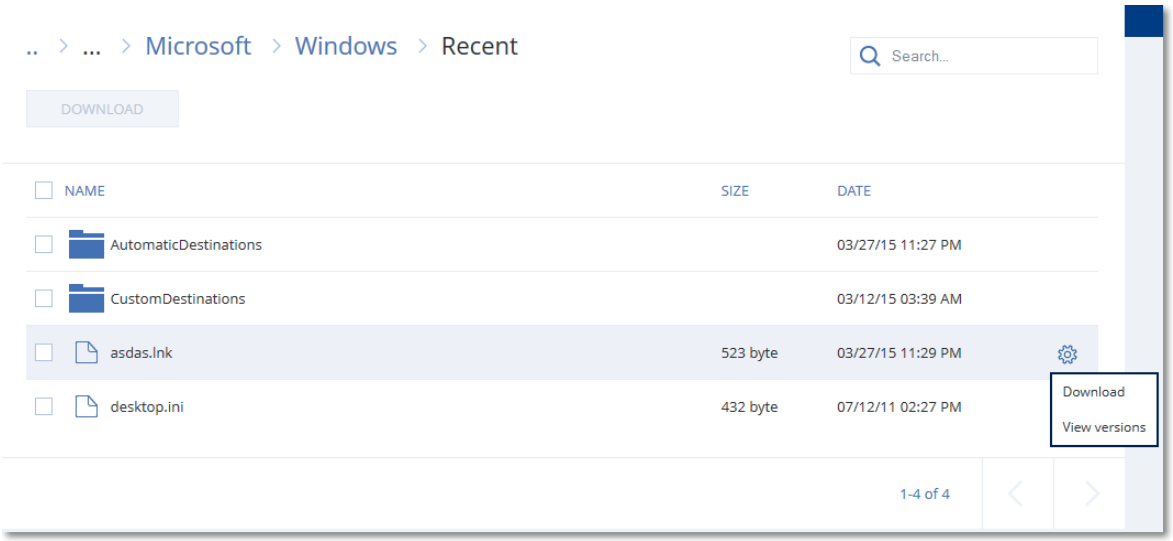
***So laden Sie Dateien aus dem Cloud Storage herunter***

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 gewünschten 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**.

## Die Authentizität von Dateien mit dem Notary Service überprüfen

Falls die Beglaubigungsfunktion (Notarization) während eines Backups aktiviert wurde, können Sie später bei Bedarf die Authentizität einer gesicherten Datei überprüfen.

***So können Sie die Authentizität von Dateien überprüfen***

1. Wählen Sie die gewünschte Datei aus, wie es in den Schritten 1-6 des Abschnitts 'Dateien über die Weboberfläche wiederherstellen' oder in den Schritten 1-5 des Abschnitts 'Dateien aus dem Cloud Storage herunterladen' beschrieben ist.
2. Überprüfen Sie, dass die ausgewählte Datei mit dem folgenden Symbol gekennzeichet ist:  .
   Das bedeutet, dass die Datei 'beglaubigt' (notarized) ist.
3. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Klicken Sie auf **Verifizieren**.
     Die Software überprüft die Authentizität der Datei und zeigt das Ergebnis an.
   - Klicken Sie auf **Zertifikat abrufen**.
     Ein Zertifikat, das die Dateibeglaubigung bestätigt, wird in einem Webbrowser-Fenster geöffnet. In dem Fenster werden außerdem Anweisungen angezeigt, wie Sie die Dateiauthentizität manuell überprüfen können.

## Eine Datei mit ASign signieren

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' beschrieben ist.
2. Überprüfen Sie im linken Fensterbereich, dass der korrekte Zeitpunkt (Datum, Uhrzeit) ausgewählt wurde.
3. Klicken Sie auf **Diese Dateiversion signieren**.
4. Spezifizieren Sie das Kennwort für das Cloud Storage-Konto, unter dem das Backup gespeichert wurde. Der Anmeldename des Kontos wird im Eingabeaufforderungsfenster angezeigt.
   Die Benutzeroberfläche des ASign Service wird in einem Webbrowser-Fenster geöffnet.
5. Fügen Sie bei Bedarf weitere Unterzeichner hinzu, indem Sie deren E-Mail-Adressen spezifizieren. Nach dem Versenden der Einladungen können keine weiteren Unterzeichner mehr hinzugefügt oder entfernt werden. Überprüfen Sie daher, dass auch wirklich alle Personen in der Liste sind, deren Signatur erforderlich ist.
6. Klicken Sie auf **Zum Signieren einladen**, damit die Einladung an die Unterzeichner versendet wird.
   Jeder Unterzeichner erhält eine E-Mail-Nachricht mit der Signatur-Aufforderung. Wenn alle angeforderten Unterzeichner die Datei signiert haben, wird diese noch vom Notary Service beglaubigt und signiert.
   Sie erhalten jeweils Benachrichtigungen, wenn ein Unterzeichner die Datei signiert hat und wenn der komplette Prozess abgeschlossen wurde. Sie können auf die ASign-Webseite zugreifen, indem Sie in einer der E-Mail-Nachrichten, die Sie erhalten, auf **Details anzeigen** klicken.
7. Gehen Sie nach Abschluss des Prozesses zur ASign-Webseite und klicken Sie auf **Dokument abrufen**, um ein .pdf-Dokument herunterzuladen, welches folgende Informationen enthält:
   - Eine Signaturzertifikatsseite mit den zusammengestellten Signaturen.
   - Eine Audit-Trail-Seite mit einem Verlauf folgender Aktivitäten: wann die Einladung an die Unterzeichner gesendet wurde, wann der Unterzeichner die Datei signiert hat usw.

## Dateien mit einem Boot-Medium wiederherstellen

Genau Informationen über die Erstellung eines Boot-Mediums finden Sie im Abschnitt 'Ein Boot-Medium erstellen'.

***So können Sie Dateien mithilfe eines Boot-Mediums wiederherstellen***

1. Booten Sie die Zielmaschine mit dem Boot-Medium.
2. Klicken Sie entweder auf **Diese Maschine lokal verwalten** oder zweimal auf **Rescue Bootable Media** (abhängig vom verwendeten Typ des Mediums).
3. Falls in Ihrem Netzwerk ein Proxy-Server verwendet wird, klicken Sie auf **Extras** –> **Proxy-Server** und spezifizieren Sie dann den Host-Namen/die IP-Adresse und den Port des Proxy-Servers. Ansonsten können Sie diesen Schritt überspringen.
4. Klicken Sie innerhalb der Willkommensseite auf **Recovery**.
5. Klicken Sie auf **Daten wählen** und dann auf **Durchsuchen**.
6. 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.
   - 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.
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. Wählen Sie bei **Backup-Inhalte** das Element **Ordner/Dateien**.
9. Wählen Sie Daten, die Sie wiederherstellen wollen. Klicken Sie auf **OK**, um Ihre Auswahl zu bestätigen.
10. Spezifizieren Sie bei **Recovery-Ziel** einen gewünschten Ordner. Optional können Sie neuere Dateiversionen vor Überschreibung schützen oder einige Dateien von der Wiederherstellung ausschließen.
11. [Optional] Klicken Sie auf **Recovery-Optionen**, um zusätzliche Einstellungen zu spezifizieren.
12. Wählen Sie **OK**, um die Wiederherstellung zu starten.

**Hinweis**
Ein Band-Speicherort benötigt viel Platz und passt möglicherweise nicht in den Arbeitsspeicher (RAM), wenn Sie mit einem Boot-Medium (Linux- oder WinPE-basiert) Wiederherstellungen oder erneute Scans durchführen. Für Linux müssen Sie einen anderen Speicherort mounten, um die Daten auf einer Festplatte oder einer Netzwerkfreigabe speichern zu können. Siehe Acronis Cyber Backup Advanced: Den Ordner 'TapeLocation' ändern (KB 27445). Für Windows PE gibt es derzeit kein Workaround.

## 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.

# Den 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 Speicherorten gefiltert werden.

4. Klicken Sie auf **Systemzustand wiederherstellen**.
5. Bestätigen Sie, dass der vorliegende Systemzustand mit der Version überschrieben werden soll, die im Backup vorliegt.

Der Recovery-Fortschritt wird auf der Registerkarte **Aktivitäten** angezeigt.

# Eine ESXi-Konfiguration wiederherstellen

Um eine ESXi-Konfiguration wiederherstellen zu können, benötigen Sie ein Linux-basiertes Boot-Medium. Genau Informationen über die Erstellung eines Boot-Mediums finden Sie im Abschnitt 'Ein Boot-Medium erstellen'.

Wenn Sie für die Wiederherstellung einer ESXi-Konfiguration einen anderen als den ursprünglichen Host als Ziel verwenden wollen und der ursprüngliche ESXi-Host noch mit dem vCenter Server verbunden ist, sollten Sie diesen ursprünglichen Host vom vCenter Server trennen und entfernen, um unerwartete Probleme bei der Wiederherstellung zu vermeiden. Wenn Sie den ursprünglichen Host gemeinsam mit dem wiederhergestellten Host weiter behalten/verwenden wollen, können Sie ihn nach Abschluss der Wiederherstellung wieder hinzufügen.

Evtl. auf dem Host laufende virtuelle Maschinen werden nicht in das ESXi-Konfigurations-Backup eingeschlossen. Sie können diese jedoch separat per Backup sichern und wiederherstellen.

***So stellen Sie eine ESXi-Konfiguration wieder her***

1. Booten Sie die Zielmaschine mit dem Boot-Medium.
2. Klicken Sie auf **Diese Maschine lokal verwalten**.
3. Klicken Sie innerhalb der Willkommensseite auf **Recovery**.
4. Klicken Sie auf **Daten wählen** und dann auf **Durchsuchen**.
5. Spezifizieren Sie den Backup-Speicherort:
   - Wählen Sie den gewünschten Ordner unter **Lokale Ordner** oder **Netzwerkordner** aus.

   Klicken Sie auf **OK**, um Ihre Auswahl zu bestätigen.
6. Wählen Sie bei **Anzeigen** das Element **ESXi-Konfiguration**.
7. Wählen Sie das Backup, aus dem die Daten wiederhergestellt werden sollen. Geben Sie das Kennwort für das Backup an, falls Sie dazu aufgefordert werden.
8. Klicken Sie auf **OK**.
9. Bei **Für neue Datenspeicher zu verwendende Laufwerke** gehen Sie folgendermaßen vor:
   - Wählen Sie bei **ESXi wiederherstellen zu** dasjenige Laufwerk, auf dem die Host-Konfiguration wiederhergestellt werden soll. Wenn Sie den ursprünglichen Host als Ziel für die Wiederherstellung der Konfiguration verwenden, wird das ursprüngliche Laufwerk standardmäßig vorausgewählt.
   - [Optional] Wählen Sie bei **Für neue Datenspeicher verwenden** die Laufwerke, auf denen die neuen Datenspeicher erstellt werden sollen. Beachten Sie, dass dabei alle (möglicherweise bereits vorhandenen) Daten auf den ausgewählten Laufwerken verloren gehen. Falls Sie die

virtuellen Maschinen in den vorhandenen Datenspeichern bewahren wollen, wählen Sie kein Laufwerk aus.

10. Falls Sie Laufwerke für neue Datenspeicher auswählen, bestimmen Sie auch die Methode, wie diese erstellt werden sollen. Verwenden Sie dazu die Befehle **Einen Datenspeicher auf allen ausgewählten Laufwerken erstellen: Einen Datenspeicher pro Laufwerk erstellen** oder **Einen Datenspeicher auf allen ausgewählten Laufwerken erstellen**.
11. [Optional] Ändern Sie gegebenenfalls bei **Netzwerkzuordnung**, wie die automatische Zuordnung die (im Backup vorliegenden) virtuellen Switche den physischen Netzwerkadaptern zugeordnet hat.
12. [Optional] Klicken Sie auf **Recovery-Optionen**, um zusätzliche Einstellungen zu spezifizieren.
13. Wählen Sie **OK**, um die Wiederherstellung zu starten.

# Recovery-Optionen

Wenn Sie die Recovery-Optionen ändern wollen, klicken Sie während der Konfiguration der Wiederherstellung auf **Recovery-Optionen**.

## Verfügbarkeit der Recovery-Optionen

Art und Umfang der verfügbaren Recovery-Optionen sind abhängig von:

- Der Umgebung, in welcher der Agent seine Recovery-Aktionen durchführt (Windows, Linux, macOS oder ein Boot-Medium).
- Die Art der wiederherzustellenden Daten (Laufwerke, Dateien, virtuelle Maschinen, Applikationsdaten).

Die nachfolgende Tabelle fasst die Verfügbarkeit der Recovery-Optionen zusammen:

| | **Laufwerke** | | | **Dateien** | | | | **Virtuelle Maschinen** | **SQL und Exchange** |
|---|---|---|---|---|---|---|---|---|---|
| | Windows | Linux | Boot-Medium | Windows | Linux | macOS | Boot-Medium | ESXi, Hyper-V, Scale Computing HC3 | Windows |
| Backup-Validierung | + | + | + | + | + | + | + | + | + |
| Boot-Modus | + | - | - | - | - | - | - | + | - |
| Zeitstempel | - | - | - | + | + | + | + | - | - |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| für Dateien | | | | | | | | | |
| Fehlerbehandlung | + | + | + | + | + | + | + | + | + |
| Dateifilter (Ausschluss) | - | - | - | + | + | + | + | - | - |
| Flashback | + | + | + | - | - | - | - | + | - |
| Wiederherstellung mit vollständigem Pfad | - | - | - | + | + | + | + | - | - |
| Mount-Punkte | - | - | - | + | - | - | - | - | - |
| Performance | + | + | - | + | + | + | - | + | + |
| Vor-/Nach-Befehle | + | + | - | + | + | + | - | + | + |
| SID ändern | + | - | - | - | - | - | - | - | - |
| VM-Energieverwaltung | - | - | - | - | - | - | - | + | - |
| "Bandverwaltung" (S. 361) > Laufwerks-Cache zur Beschleunigung der Wiederherstellung verwenden | - | - | - | + | + | + | - | - | - |
| Windows-Ereignisprotokoll | + | - | - | + | - | - | - | Nur Hyper-V | + |
| Nach der Wiederherstellung einschalten | - | - | - | - | - | - | + | - | - |

## Backup-Validierung

Diese Option definiert, ob ein Backup vor der Wiederherstellung der darin enthaltenen Daten zu validieren ist, um sicherzustellen, dass das Backup nicht beschädigt ist. Diese Aktion wird vom Protection Agenten durchgeführt.

Die Voreinstellung ist: **Deaktiviert**.

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.

## Boot-Modus

Diese Option ist nur wirksam, wenn Sie eine physische oder virtuelle Maschine aus einem Laufwerk-Backup wiederherstellen, welches ein Windows-Betriebssystem enthält.

Mit dieser Option können Sie den Boot-Modus (BIOS oder UEFI) festlegen, den Windows nach der Wiederherstellung verwenden soll. Wenn der Boot-Modus der ursprünglichen Maschine anders als der ausgewählte Boot-Modus ist, wird die Software:

- Das Laufwerk, auf dem Sie das System-Volume wiederherstellen, entsprechend dem ausgewählten Boot-Modus initialisieren (MBR für BIOS, GPT für UEFI).
- Das Windows-Betriebssystem so anpassen, dass es mit dem ausgewählten Boot-Modus starten kann.

Die Voreinstellung ist: **Wie bei der Zielmaschine.**

Sie können eine der folgenden Varianten wählen:

- **Wie bei der Zielmaschine**
  Der Agent, der auf dem Zielmaschine läuft, erkennt den aktuell von Windows verwendeten Boot-Modus und nimmt dann die Einstellungen entsprechend dem erkannten Boot-Modus vor.
  Dies ist der sicherste Wert, der automatisch zu einem bootfähigen System führt – außer die unten aufgeführten Einschränkungen treffen zu. Da die Option **Boot-Modus** unter einem Boot-Medium

nicht verfügbar ist, verhält sich der Agent des Boot-Mediums immer so, als wäre dieser Wert ausgewählt worden.

- **Wie bei der gesicherten Maschine**

  Der Agent, der auf dem Zielmaschine läuft, liest den Boot-Modus aus dem Backup aus und nimmt dann die Einstellungen so vor, dass sie zu diesem Boot-Modus passen. Damit können Sie ein System auch auf einer anderen Maschine wiederherstellen, wenn diese Maschine einen anderen Boot-Modus verwendet, und dann das Laufwerk in der gesicherten Maschine austauschen.
- **BIOS**

  Der Agent, der auf der Zielmaschine läuft, nimmt die Einstellungen zur Verwendung des BIOS-Modus vor.
- **UEFI**

  Der Agent, der auf der Zielmaschine läuft, nimmt die Einstellungen zur Verwendung des UEFI-Modus vor.

Sobald eine Einstellung geändert wurde, wird die Laufwerkszuordnungsprozedur wiederholt. Dies wird einige Zeit benötigen.

### Empfehlungen

Wenn Sie Windows zwischen UEFI und BIOS migrieren müssen:

- Stellen Sie das komplette Laufwerk, auf dem sich das System-Volume befindet, wieder her. Wenn Sie nur das System-Volume über ein vorhandenes Volume wiederherstellen, wird der Agent das Ziellaufwerk nicht richtig initialisieren können.
- Beachten Sie, dass Sie mit dem BIOS-Standard den Speicherplatz auf Festplatten nur bis zu einer Grenze von 2 TB ansprechen können.

### Einschränkungen

- Eine Migration zwischen UEFI und BIOS wird unterstützt für:
  - Die 64-Bit-Versionen aller Windows-Betriebssysteme, beginnend mit Windows 7
  - Die 64-Bit-Versionen aller Windows-Betriebssysteme, beginnend mit Windows Server 2008 SP1
- Eine Migration zwischen UEFI und BIOS wird nicht unterstützt, wenn sich das Backup auf einem Bandgerät befindet.

Wenn die Migration eines Systems zwischen UEFI und BIOS nicht unterstützt wird, verhalten sich die Agenten so, als wäre die Einstellung **Wie bei der gesicherten Maschine** ausgewählt worden. Wenn die Zielmaschine sowohl UEFI als auch BIOS unterstützen, müssen Sie den Boot-Modus manuell aktivieren, der der ursprünglichen Maschine entspricht. Anderenfalls wird das System nicht mehr booten.

## Zeitstempel für Dateien

Diese Option gilt nur für die Wiederherstellung von Dateien.

Diese Option bestimmt, ob wiederhergestellte Dateien den ursprünglichen Zeitstempel aus dem Backup übernehmen – oder ob ihnen das Datum/die Zeit des aktuellen Wiederherstellungszeitpunkts zugewiesen wird.

Wenn diese Option aktiviert ist, werden den Dateien die aktuelle Zeit und das aktuelle Datum zugewiesen.

Die Voreinstellung ist: **Aktiviert**.

## Fehlerbehandlung

Diese Optionen ermöglichen Ihnen vorzugeben, wie auftretende Fehler während einer Recovery-Aktion behandelt werden.

### Erneut versuchen, wenn ein Fehler auftritt

Die Voreinstellung ist: **Aktiviert. Anzahl der Versuche: 30. Intervall zwischen den Versuchen: 30 Sekunden.**

Wenn ein behebbarer Fehler auftritt, versucht das Programm, die erfolglose Aktion erneut durchzuführen. Sie können das Zeitintervall und die Anzahl der Versuche einstellen. Die Versuche werden aufgegeben, wenn entweder die Aktion erfolgreich ist ODER die angegebene Anzahl an Versuchen erreicht wurde, je nachdem, was zuerst eintritt.

### Während der Durchführung keine Meldungen bzw. Dialoge anzeigen (Stiller Modus)

Die Voreinstellung ist: **Deaktiviert**.

Wenn der stille Modus eingeschaltet ist, kann das Programm Situationen automatisch behandeln, die einen Benutzereingriff erfordern, falls das möglich ist. Falls eine Aktion nicht ohne Benutzereingriff fortfahren kann, wird sie fehlschlagen. Detaillierte Informationen über die Aktion, einschließlich eventueller Fehler, finden Sie im Log der Aktion.

### Systeminformationen speichern, wenn eine Wiederherstellung mit Neustart fehlschlägt

Diese Option gilt für Wiederherstellungen von Laufwerken/Volumes zu einer physischen Maschine, die unter Windows oder Linux läuft.

Die Voreinstellung ist: **Deaktiviert**.

Wenn diese Option aktiviert ist, können Sie einen Ordner auf einem lokalen Laufwerk (einschließlich an die Zielmaschine angeschlossene USB-Sticks und Festplatten) oder eine Netzwerkfreigabe spezifizieren, wo die Protokoll-, Systeminformations- und Crash-Dump-Dateien gespeichert werden sollen. Diese Informationen können den Mitarbeitern des technischen Supports helfen, das entsprechende Problem zu identifizieren.

## Dateifilter (Ausschluss)

Diese Option gilt nur für die Wiederherstellung von Dateien.

Diese Option definiert, welche Dateien und Ordner während eines Recovery-Prozesses übersprungen und so von der Liste der wiederherzustellenden Elemente ausgeschlossen werden.

**Hinweis**
Ausschließungen überschreiben eine mögliche Auswahl von wiederherzustellenden Datenelementen. Falls Sie beispielsweise festlegen, dass die Datei 'MeineDatei.tmp' wiederhergestellt werden soll und Sie aber zudem alle .tmp-Dateien ausschließen, dann wird 'MeineDatei.tmp' nicht wiederhergestellt.

## Dateisicherheitseinstellungen

Diese Option gilt, wenn Sie Dateien aus Laufwerk- und Datei-Backups von NTFS-formatierten Volumes wiederherstellen.

Diese Option definiert, ob die NTFS-Zugriffsrechte für Dateien zusammen mit den Dateien wiederhergestellt werden.

Die Voreinstellung ist: **Aktiviert**.

Sie können wählen, ob die Dateien bei der Wiederherstellung ihre ursprünglichen Zugriffsrechte aus dem Backup beibehalten sollen – oder ob sie die NTFS-Berechtigungen desjenigen Ordner übernehmen sollen, in dem sie wiederhergestellt werden.

## Flashback

Diese Option gilt – ausgenommen beim Mac – für die Wiederherstellung von Laufwerken und Volumes auf physischen und virtuellen Maschinen.

Wenn diese Option aktiviert ist, werden nur solche Daten wiederhergestellt, hinsichtlicher derer sich das Backup und das Ziellaufwerk unterscheiden. Dies beschleunigt die Datenwiederherstellung auf dasselbe Laufwerk wie dasjenige, das ursprünglich im Backup gesichert wurde, insbesondere wenn sich das Volume-Layout des Laufwerks nicht geändert hat. Der Datenvergleich erfolgt auf Blockebene.

Bei physischen Maschinen ist der Datenvergleich auf Blockebene eine zeitaufwendige Aktion. Wenn es eine schnelle Verbindung zum Backup Storage gibt, benötigt die Wiederherstellung des kompletten Laufwerks weniger Zeit als die Berechnung der Datenunterschiede. Wir empfehlen daher, die Option nur bei einer langsamen Verbindung zum Backup Storage zu aktivieren (also beispielsweise, wenn sich das Backup in der Cloud oder in einem Remote-Netzwerkordner befindet).

Bei der Wiederherstellung einer physischen Maschine hängt die Voreinstellung vom Backup-Speicherort ab:

- Befindet sich das Backup im Cloud Storage, dann ist die Voreinstellung: **Aktiviert**.
- Bei anderen Backup-Speicherorten ist die Voreinstellung: **Deaktiviert**.

Bei der Wiederherstellung einer virtuellen Maschine ist die Voreinstellung: **Aktiviert**.

## Wiederherstellung mit vollständigem Pfad

Diese Option gilt nur, wenn Daten aus einem Datei-Backup wiederhergestellt werden.

Wenn diese Option aktiviert wird, erhalten die Dateien am Zielspeicherort wieder ihren vollständigen (ursprünglichen) Pfad.

Die Voreinstellung ist: **Deaktiviert**.

## Mount-Punkte

Diese Option gilt nur unter Windows und wenn Daten aus einem Datei-Backup wiederhergestellt werden.

Aktivieren Sie diese Option, um Dateien und Ordner wiederherzustellen, die auf gemounteten Volumes gespeichert waren und mit aktivierter Option 'Mount-Punkte' gesichert wurden.

Die Voreinstellung ist: **Deaktiviert**.

Diese Option ist nur wirksam, wenn Sie einen Ordner wiederherstellen wollen, der in der Verzeichnishierarchie höher als der Mount-Punkt liegt. Wenn Sie einen Ordner innerhalb des Mount-Punktes oder den Mount-Punkt selbst für eine Recovery-Aktion wählen, werden die gewählten Elemente unabhängig vom Wert der Option '**Mount-Punkte**' wiederhergestellt.

**Hinweis**
Beachten Sie, dass für den Fall, dass das Volume zum Recovery-Zeitpunkt nicht gemountet ist, die Daten direkt zu demjenigen Ordner wiederhergestellt werden, der zum Backup-Zeitpunkt der Mount-Punkt war.

## Performance

Diese Option bestimmt, welche Priorität dem Recovery-Prozess innerhalb des Betriebssystems zugewiesen wird.

Die verfügbaren Einstellungen sind: **Niedrig**, **Normal**, **Hoch**.

Voreinstellung ist: **Normal**.

Die Priorität eines Prozesses, der in einem System ausgeführt wird, bestimmt, wie viele CPU-und System-Ressourcen ihm zugewiesen werden. Durch ein Herabsetzen der Recovery-Priorität werden mehr Ressourcen für andere Applikationen freigeben. Das Heraufsetzen der Recovery-Priorität kann den Wiederherstellungsprozess beschleunigen, indem z.B. CPU-Ressourcen von anderen gleichzeitig laufenden Prozessen abgezogen werden. Der Effekt ist aber abhängig von der totalen CPU-

Auslastung und anderen Faktoren wie der Schreibgeschwindigkeit der Festplatte oder dem Datenverkehr im Netzwerk.

## Vor-/Nach-Befehle

Diese Option ermöglicht die Definition von Befehlen, die automatisch vor oder nach der Datenwiederherstellung durchgeführt werden.

So benutzen Sie diese Vor- bzw. Nach-Befehle:

- Starten Sie den Befehl **Checkdisk**, damit logische Fehler im Dateisystem, physische Fehler oder fehlerhafte Sektoren vor Beginn oder nach Ende der Recovery-Aktion gefunden und behoben werden.

Das Programm unterstützt keine interaktiven Befehle, d.h. Befehle, die eine Reaktion des Benutzers erfordern (wie z.B. 'Pause').

Ein 'Nach-Recovery'-Befehl wird nicht ausgeführt, wenn die Wiederherstellung einen Neustart benötigt bzw. ausführt.

### Befehl vor Recovery

***So spezifizieren Sie einen Befehl bzw. eine Stapelverarbeitungsdatei, die vor dem Start der Wiederherstellung ausgeführt wird***

1. Aktivieren Sie den Schalter **Einen Befehl vor der Wiederherstellung ausführen**.
2. Geben Sie im Feld **Befehl** ein Kommando ein oder wählen Sie eine vorbereitete Stapelverarbeitungsdatei aus dem Dateisystem aus. Das Programm unterstützt keine interaktiven Befehle, d.h. Befehle, die eine Reaktion des Benutzers erfordern (wie z.B. 'Pause').
3. Spezifizieren Sie im Eingabefeld **Arbeitsverzeichnis** einen Pfad zu einem Verzeichnis, in dem der Befehl bzw. die Stapelverarbeitungsdatei durchgeführt werden soll.
4. Tragen Sie Argumente für die Befehlsausführung in das Feld **Argumente** ein, wenn das erforderlich ist.
5. Wählen Sie in der unteren Tabelle die passenden Optionen, abhängig vom Ergebnis, das Sie erreichen wollen.
6. Klicken Sie auf **Fertig**.

| **Kontrollkästchen** | **Auswahl** | | | |
|---|---|---|---|---|
| **Wiederherstellung scheitern lassen, wenn die Befehlsausführung fehlschlägt*** | Ausgewählt | Deaktiviert | Ausgewählt | Deaktiviert |
| **Wiederherstellung** | Ausgewählt | Ausgewählt | Deaktiviert | Deaktiviert |

| | | | | |
|---|---|---|---|---|
| **erst ausführen, wenn die Befehlsausführung abgeschlossen ist** | | | | |
| **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.

## Bandverwaltung

Sie können folgende Recovery-Optionen für die Bandverwaltung verwenden.

### Laufwerks-Cache zur Beschleunigung der Wiederherstellung verwenden

Die Voreinstellung ist: **Deaktiviert**.

Wir empfehlen dringend, dass Sie die Option **Laufwerks-Cache zur Beschleunigung der Wiederherstellung verwenden** nutzen, wenn Sie Dateien aus einem Image-Archiv wiederherstellen wollen. Anderenfalls kann die Wiederherstellungsaktion sehr viel Zeit in Anspruch nehmen. Mit dieser Option wird das Band sequentiell eingelesen, ohne dass es zu Unterbrechungen und Rückspulen kommt.

## SID ändern

Diese Option ist gültig, wenn Sie Windows 8.1/Windows Server 2012 R2 (oder früher) wiederherstellen.

Diese Option ist nicht gültig, wenn eine Wiederherstellung zu einer virtuellen Maschine (als Ziel) durchgeführt wird und dafür ein Agent für VMware, ein Agent für Hyper-V oder ein Agent für Scale Computing HC3 verwendet wird.

Die Voreinstellung ist: **Deaktiviert**.

Die Software kann eine eindeutige SID (Computer Security Identifier) für das wiederhergestellte Betriebssystem erstellen. Sie benötigen diese Option nur, wenn Sie die Betriebsfähigkeit von Drittanbieter-Software sicherstellen müssen, die von der Computer-SID abhängt.

Eine Änderung der SID auf einem bereitgestellten oder wiederhergestellten System wird von Microsoft offiziell nicht unterstützt. Wenn Sie diese Option verwenden, tun Sie dies also auf eigenes Risiko hin.

## VM-Energieverwaltung

Diese Optionen 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 Scale Computing HC3 verwendet wird.

### Virtuelle Zielmaschinen bei Start der Wiederherstellung ausschalten

Die Voreinstellung ist: **Aktiviert**.

Eine vorhandene Maschine kann nicht als Wiederherstellungsziel verwendet werden, solange sie online ist. Mit dieser Option wird die Zielmaschine automatisch ausgeschaltet, sobald die Wiederherstellung startet. Möglicherweise vorhandene/aktive Benutzer werden dabei von der Maschine getrennt und nicht gespeicherte Daten gehen verloren.

Deaktivieren Sie das Kontrollkästchen für diese Option, wenn Sie die virtuelle Maschinen vor der Wiederherstellung manuell ausschalten wollen.

### Virtuelle Zielmaschine nach Abschluss der Wiederherstellung einschalten

Die Voreinstellung ist: **Deaktiviert**.

Wenn eine Maschine (aus einem Backup) zu einer anderen Maschine wiederhergestellt wird, kann es passieren, dass das Replikat der vorhandenen Maschine anschließend im Netzwerk erscheint. Sie können dies vermeiden, wenn Sie die wiederhergestellte Maschine manuell einschalten, nachdem Sie die notwendigen Vorsichtsmaßnahmen getroffen haben.

## Windows-Ereignisprotokoll

Diese Option gilt nur für Windows-Betriebssysteme.

Diese Option definiert, ob die Agenten für alle Recovery-Aktionen entsprechende Ereigniseinträge im Windows-Anwendungsereignisprotokoll hinterlegen sollen. Sie können die Protokolleinträge über die Windows-Ereignisanzeige einsehen, die per Eingabebefehl (eventvwr.exe) oder per Menü (**Systemsteuerung** –> **Verwaltung** –> **Ereignisanzeige**) aufgefrufen werden kann. Sie können die Ereignisse filtern, die geloggt werden.

Die Voreinstellung ist: **Deaktiviert**.

## Nach der Wiederherstellung einschalten

Diese Option ist wirksam, wenn Sie ein Boot-Medium gestartet haben und mit diesem arbeiten.

Die Voreinstellung ist: **Deaktiviert**.

Diese Option ermöglicht den Neustart der Maschine in das wiederhergestellte Betriebssystem ohne weitere Aktion eines Benutzers.

# Disaster Recovery

Dieses Feature ist nur bei den Cloud-Bereitstellungen von Acronis Cyber Protect verfügbar. Eine detaillierte Beschreibung dieser Funktionalität finden Sie unter https://www.acronis.com/support/documentation/DisasterRecovery/index.html#43224.html.

# Aktionen mit Backups

## Die Registerkarte 'Backup Storage'

In der Registerkarte **Backup Storage** werden die Backups all der Maschinen angezeigt, die jemals auf dem Management Server registriert wurden. Dazu gehören auch Offline-Maschinen und Maschinen, die nicht mehr 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.

Unter Windows übernehmen Backup-Dateien die Zugriffsberechtigungen von ihrem übergeordneten Ordner. Wir empfehlen daher, dass Sie die Leserechte für diesen Ordner einschränken.

Im Cloud Storage haben Benutzer jedoch immer nur Zugriff auf Ihre jeweils eigenen Backups. Bei einer Cloud-Bereitstellung kann ein Administrator die Backups eines jeden Kontos einsehen, welches zu derselben Gruppe 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.

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.

**Warnung!**
Versuchen Sie nicht, die Backup-Dateien manuell zu bearbeiten, weil dies die Dateien beschädigen und damit die Backups unbrauchbar machen könnte. Wir empfehlen außerdem, dass Sie Backups exportieren oder die Backup-Replikation verwenden, statt die Backup-Dateien manuell zu verschieben.

***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.

# Volumes aus einem Backup mounten

Indem Sie die Volumes eines Laufwerk-Backups (Images) mounten, können Sie auf diese Volumes so zugreifen, als wären es physische Laufwerke.

Wenn Sie Volumes im 'Lese/Schreib'-Modus mounten, können Sie die in diesen vorliegenden Backup-Inhalte verändern. Das bedeutet: Dateien und Ordner speichern, verschieben, erstellen oder löschen und ausführbare Programme starten (sofern diese nur aus einer Datei bestehen). Die Software erstellt in diesem Modus ein inkrementelles Backup, welches alle Änderungen enthält, die Sie am Backup-Inhalt durchführen. Beachten Sie, dass keine der nachfolgenden Backups diese Änderungen enthalten werden.

## Anforderungen

- Diese Funktionalität steht nur unter Windows und bei Verwendung des Windows Datei-Explorers zur Verfügung.
- Auf der Maschine, auf der Sie das Mounten durchführen, muss der Agent für Windows installiert sein.
- Das im Backup vorliegende Dateisystem muss von der Windows-Version, die auf der Maschine läuft, unterstützt werden.
- Das Backup selbst muss entweder in einem lokalen Ordner, in einer Netzwerkfreigabe (SMB/CIFS) oder in einer Secure Zone gespeichert sein.

## Anwendungsszenarien

- **Daten freigeben**
  Gemountete Volumes können einfach im Netzwerk freigegeben werden.
- **Notlösung zur Wiederherstellung einer Datenbank**

Mounten Sie ein Volume, das eine SQL-Datenbank von einer kürzlich ausgefallenen Maschine enthält. Sie erhalten so Zugriff auf die im Backup gespeicherte Datenbank, bis die ausgefallene Maschine wiederhergestellt ist. Sie können diesen Ansatz auch dazu verwenden, um ein granulares Recovery von Microsoft SharePoint-Daten mithilfe des SharePoint Explorers durchzuführen.

- **Offline Virus-Bereinigung**

  Wenn eine Maschine mit einem Virus infiziert ist, können Sie ein Backup dieser Maschine als Volume mounten und dieses dann von einem Antivirus-Programm bereinigen lassen. Anschließend können Sie die Maschine aus diesem bereinigten Backup wiederherstellen. Eine Alternative zu dieser Prozedur besteht natürlich in der Wiederherstellung eines Backups, welches erst gar nicht infiziert ist, jedoch ist ein solches nicht immer verfügbar.
- **Fehlerüberprüfung**

  Wenn die Wiederherstellung eines Volumes fehlschlägt (insbesondere bei gleichzeitiger Größenanpassung des Volumes), kann dies an einem Fehler im gespeicherten Dateisystem (des Backups) liegen. Mounten Sie in diesem Fall das Backup im 'Lese/Schreib'-Modus. Überprüfen Sie das gemountete Volume dann mit dem Befehl **chkdsk /r** auf Fehler. Sobald die Fehler behoben wurden und das dazugehörige inkrementelle Backup erstellt wurde, können Sie das System aus diesem korrigierten Backup wiederherstellen.

***So können Sie ein Volume aus einem Backup mounten***

1. Verwenden Sie den Windows Datei-Explorer, um den Speicherort des Backups aufzurufen.
2. Klicken Sie doppelt auf die Backup-Datei. Standardmäßig werden die Dateinamen nach folgender Vorlage erstellt:

   `<Maschinenname> - <Schutzplan-GUID>`
3. Wenn das Backup verschlüsselt ist, müssen Sie das entsprechende Kennwort eingeben. Ansonsten können Sie diesen Schritt überspringen.

   Der Windows Datei-Explorer zeigt die Recovery-Punkte an.
4. Klicken Sie doppelt auf einen gewünschten Recovery-Punkt.

   Der Windows Datei-Explorer zeigt die im Backup gespeicherten Volumes an.

   **Hinweis**
   Wenn Sie auf ein Volume doppelt klicken, können Sie dessen Inhalte einsehen/durchsuchen. Sie können Dateien/Ordner aus dem Backup zu einem beliebigen Ordner im Dateisystem kopieren.
5. Klicken Sie mit der rechten Maustaste auf das zu mountende Volume – und wählen Sie anschließend einen der nachfolgenden Befehle:
   - **Mounten**

     **Hinweis**
     Nur das letzte Backup im Archiv (der Backup-Kette) kann im 'Lese/Schreib'-Modus gemountet werden.

- **Im Nur-Lesen-Modus mounten**

6. Sollte das Backup in einer Netzwerkfreigabe gespeichert sein, müssen Sie bei Bedarf die entsprechenden Anmeldedaten angeben, um auf die Freigabe zugreifen zu können. Ansonsten können Sie diesen Schritt überspringen.

   Das ausgewählte Volume wird von der Software gemountet. Dem Volume wird dabei standardmäßig der erste freie Laufwerksbuchstabe zugewiesen.

***So können Sie ein Volume wieder trennen (unmounting)***

1. Gehen Sie im Windows Datei-Explorer zur obersten Ebene des Verzeichnisbaums (das Element '**Computer**' bzw. unter Windows 8.1 (und später) '**Dieser PC**').
2. Klicken Sie mit der rechten Maustaste auf das gemountete Volume.
3. Klicken Sie auf **Trennen**.
4. Wenn das Volume im 'Lese/Schreib'-Modus gemountet wurde und dabei sein Inhalt geändert wurde, müssen Sie auswählen, ob ein inkrementelles Backup erstellt werden soll, in dem die erfolgten Änderungen gespeichert werden. Ansonsten können Sie diesen Schritt überspringen.

   Das Mounten des ausgewählten Volumes wird von der Software aufgehoben und das entsprechende Laufwerk vom Dateisystem getrennt.

# Backups validieren

Validierung ist eine Aktion, mit der geprüft wird, ob es grundsätzlich möglich ist, dass Daten, die in einem Backup gespeichert sind, wiederhergestellt werden können. Weitere Informationen zu dieser Aktion finden Sie im Abschnitt '"Validierung" (S. 374)'.

***So können Sie ein Backup validieren***

1. Wählen Sie den gesicherten Workload aus.
2. Klicken Sie auf **Recovery**.
3. Wählen Sie einen Recovery-Punkt. Beachten Sie dabei, dass Recovery-Punkte nach Speicherorten gefiltert werden.

   Falls der Workload offline ist, werden keine Recovery-Punkte angezeigt. Gehen Sie nach einer der folgenden Möglichkeiten vor:

   - Sollte sich das Backup im Cloud Storage oder einem gemeinsam genutzten Storage befinden (d.h., dass andere Agenten auf diesen zugreifen können), dann klicken Sie zuerst auf den Befehl **Maschine auswählen**. Wählen Sie anschließend einen Ziel-Workload aus, der online ist, und dann den gewünschten Recovery-Punkt.
   - Wählen Sie einen Recovery-Punkt auf der Registerkarte 'Backup Storage' aus. Weitere Informationen über die dort verfügbaren Backups finden Sie im Abschnitt '"Die Registerkarte 'Backup Storage'" (S. 364)'.
4. Klicken Sie auf das Zahnradsymbol und anschließend auf **Validieren**.
5. Wählen Sie den Agenten aus, der die Validierung durchführen soll.
6. Wählen Sie die Validierungsmethode aus.

7. Wenn das Backup verschlüsselt ist, müssen Sie das entsprechende Kennwort bereitstellen.
8. Klicken Sie auf **Start**.

# Backups exportieren

Mit der Aktion 'Exportieren' wird von einem Backup eine unabhängige Kopie an einem von Ihnen spezifizierten Speicherort erstellt. Das ursprüngliche Backup bleibt dabei unverändert. Durch Exportieren können Sie ein bestimmtes Backup aus einer Kette inkrementeller und differentieller Backups separieren, um so beispielsweise Wiederherstellungen zu beschleunigen, ein Backup besser auf ein Wechselmedium speichern zu können oder andere Aktionen mit dem Backup besser durchführen zu können.

Das Ergebnis einer Exportieren-Aktion ist immer ein vollständiges Backup. Wenn Sie eine komplette Backup-Kette an einen anderen Speicherort replizieren und mehrfache Recovery-Punkte bewahren wollen, müssen Sie einen Backup-Replikationsplan verwenden.

Der Backup-Dateiname des exportierten Backups hängt davon ab, welchen Wert die Option 'Backup-Format' hat:

- Beim Format **Version 12** mit einem beliebigen Backup-Schema gilt: der Backup-Dateiname entspricht – abgesehen von einer fortlaufenden Nummer (Sequenznummer) – dem Namen des ursprünglichen Backups. Wenn mehrere Backups aus derselben Backup-Kette zum gleichen Speicherort exportiert werden, wird an die Dateinamen aller Backups (mit Ausnahme des ersten) eine vierstellige Sequenznummer angehängt.
- Beim Backup-Format **Version 11** mit dem Backup-Schema **Nur inkrementell (Einzeldatei)** gilt: der Backup-Dateiname entspricht exakt dem Backup-Dateinamen des ursprünglichen Backups. Wenn mehrere Backups aus derselben Backup-Kette an den gleichen Speicherort exportiert werden, wird jeder Exportaktion das zuvor exportierte Backup überschreiben.
- Beim Format **Version 11** mit allen anderen Backup-Schemata gilt: der Backup-Dateiname entspricht – abgesehen von einem Zeitstempel – dem Namen des ursprünglichen Backups. Die Zeitstempel der exportierten Backups entsprechen dem Zeitpunkt, an dem der Export durchgeführt wurde.

Das exportierte Backup übernimmt die Verschlüsselungseinstellungen und das Kennwort des ursprünglichen Backups. Wenn Sie ein verschlüsseltes Backup exportieren, müssen Sie das entsprechende Kennwort spezifizieren.

***So können Sie ein Backup exportieren***

1. Wählen Sie 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'.

4. Klicken Sie auf das Zahnradsymbol und anschließend auf **Exportieren**.
5. Wählen Sie den Agenten aus, der das Exportieren durchführen soll.
6. Wenn das Backup verschlüsselt ist, müssen Sie das entsprechende Kennwort bereitstellen. Ansonsten können Sie diesen Schritt überspringen.
7. Spezifizieren Sie das Speicherziel für den Export.
8. Klicken Sie auf **Start**.

# Backups löschen

**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 Cyber Protect Webkonsole 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:
   - Wenn Sie ein einzelnes Backup löschen wollen, müssen Sie das entsprechende Backup zuerst auswählen, dann auf das Zahnradsymbol klicken und abschließend auf den Befehl **Löschen**.
   - 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:

- Um ein einzelnes Backup zu löschen: klicken Sie auf **Backups anzeigen**, wählen Sie das zu löschende Backup aus, klicken Sie auf das Zahnradsymbol und abschließend auf den Befehl **Löschen**.
- 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' 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.

# Die Registerkarte 'Pläne'

Mit einer Advanced-Lizenz können Sie Schutzpläne und andere Pläne über die Registerkarte **Pläne** verwalten.

Jeder Bereich der Registerkarte **Pläne** enthält alle Pläne eines bestimmten Typs. Folgende Bereiche sind verfügbar:

- **Schutz**
- **Backup-Scanning**
- **Backup-Replikation**
- **Validierung**
- **Bereinigung**
- **Konvertierung zu VM**
- **VM-Replikation**
- **Boot-Medium**. In diesem Bereich werden Schutzpläne angezeigt, die für Maschinen erstellt wurden, die mit Boot-Medien gestartet werden, und nur auf solche Maschinen angewendet werden können.

Sie können in jedem Bereich einen Plan erstellen, bearbeiten, (de)aktivieren, löschen, starten und dessen Ausführung überwachen.

Die Aktionen 'Klonen' und 'Stoppen' sind nur für Schutzpläne verfügbar. Anders als beim Stoppen eines Backups über die Registerkarte **Geräte** werden beim Stoppen eines Schutzplans die Backups auf allen Geräten angehalten, denen dieser Plan zugewiesen wurde. Wenn die Startzeiten der Backups für mehrere Geräte innerhalb eines bestimmten Zeitfenster verteilt sind, wird das Anhalten eines Schutzplans bewirken, dass gerade laufende Backups gestoppt werden oder die Ausführung der entsprechenden Backups verhindert wird.

Sie können einen Plan außerdem als Datei exportieren oder einen früher exportierten Plan importieren.

## Off-Host Data Processing

Die meisten Aktionen eines Schutzplans – wie Replikation, Validierung und Aufbewahrungsregeln anwenden – werden von dem Agenten durchgeführt, der auch das Backup erstellt. Für die Maschine, auf welcher der Agent läuft, bedeutet das aber auch weitere Arbeitslasten – selbst wenn der Backup-Prozess selbst schon längst abgeschlossen ist.

Durch die Möglichkeit, Antimalware-Scans, Replikations-, Validierungs, Bereinigungs- und Konvertierungspläne vom eigentlichen Schutzplan trennen zu können, erhalten Sie die Flexibilität:

- Um einen/mehrere anderen Agenten zu bestimmen, der diese Aktionen durchführen soll
- Um diese Aktionen außerhalb der Spitzenzeiten zu planen, sodass die Netzwerkbelastung gesenkt wird

- Um diese Aktionen aus den Hauptgeschäftszeiten zu verschieben, wenn die Festlegung eine dedizierten Agenten nicht in Ihren Plänen enthalten ist

Wenn Sie einen Storage Node verwenden, macht es Sinn, einen dedizierten Agenten auf derselben Maschine zu installieren.

Anders als bei den Backup- und VM-Replikationsplänen, die mit den Zeiteinstellungen der Maschinen arbeiten, auf denen die Agenten laufen, werden Off-Host Data Processing-Pläne nach den Zeiteinstellungen der Maschine des Management-Servers ausgeführt.

# Backup-Scanning-Plan

## Unterstützte Speicherorte

Sie können Backups an folgenden Speicherorten nach Malware scannen lassen: **Cloud Storage**, **Lokaler Ordner** und **Netzwerkordner**. Auf den Speicherort **Lokaler Ordner** kann nur ein Agent zugreifen, der auf derselben Maschine installiert ist.

Weitere Informationen über das Scannen von Backups und dabei geltenden Einschränkungen finden Sie im Abschnitt ÄAntimalware-Scan von Backups'.

***So können Sie einen Backup-Scanning-Plan erstellen***

1. Klicken Sie in der Cyber Protect Webkonsole auf **Pläne** –> **Backup-Scanning**.
2. Klicken Sie auf **Plan erstellen**.
3. [Optional] Wenn Sie den Namen des Plans ändern wollen, müssen Sie auf das Stiftsymbol neben dem vorgegebenen Namen klicken.
4. Wählen Sie den Agenten, der das Scannen durchführen soll.
5. Wählen Sie den Backup-Speicherort oder einzelne Backups zum Scannen aus.
   Sie können mehrere Backup-Standorte gleichzeitig auswählen. Wenn Sie einem Plan mehrere einzelne Backups hinzufügen wollen, müssen Sie die Backups einzeln nacheinander hinzufügen.
6. [Wenn **Cloud Storage** oder **Netzwerkordner** ausgewählt wurde] Geben Sie bei Aufforderung die Anmeldedaten an, um auf den ausgewählten Backup Storage zugreifen zu können.
7. [Wenn ein verschlüsseltes Backup ausgewählt wurde] Geben Sie das Kennwort an, um auf das Backup zugreifen zu können. Wenn ein Depot oder mehrere verschlüsselte Backups ausgewählt wurden, können Sie ein einziges Kennwort spezifizieren. Wenn das Kennwort für ein bestimmtes Backup nicht korrekt ist, wird eine Alarmmeldung angezeigt. Es werden nur Backups gescannt, für die ein korrektes Kennwort angegeben wurde.
8. Konfigurieren Sie die Planung für den Scan.
9. Klicken Sie, wenn Sie fertig sind, auf **Erstellen**.

Als Ergebnis wird der Backup-Scanning-Plan erstellt.

# Backup-Replikation

## Unterstützte Speicherorte

Die folgende Tabelle fasst Backup-Speicherorte zusammen, die von Backup-Replikationsplänen unterstützt werden.

| Backup-Speicherort | Als Quelle unterstützt | Als Ziel unterstützt |
|---|---|---|
| Cloud Storage | + | + |
| Lokaler Ordner | + | + |
| Netzwerkordner | + | + |
| NFS-Ordner | – | – |
| Einer Secure Zone | – | – |
| SFTP-Server | – | – |
| Verwalteter Speicherort* | + | + |
| Bandgerät | – | + |

* Überprüfen Sie die Einschränkungen, die unter '"Überlegungen für Benutzer mit Advanced-Lizenzen" (S. 273)' beschrieben sind.

***So können Sie einen Backup-Replikationsplan erstellen***

1. Klicken Sie auf **Pläne** –> **Backup-Replikation**.
2. Klicken Sie auf **Plan erstellen**.
   Die Software zeigt eine Vorlage für den neuen Plan an.
3. [Optional] Wenn Sie den Namen des Plans ändern wollen, klicken Sie auf den vorgegebenen Standardnamen.
4. Klicken Sie auf **Agent** und bestimmen Sie den Agenten, der die Replikation durchführen soll.
   Sie können jeden Agenten auswählen, der auf die als Quelle und Ziel dienenden Backup-Speicherorte zugreifen kann.
5. Klicken Sie auf **Zu replizierende Elemente** und bestimmen Sie dann die Backups, die dieser Plan replizieren soll.
   Mit dem Schalter **Speicherorte** / **Backups** (in der rechten oberen Ecke) können Sie zwischen der Auswahl von Backups und der Auswahl kompletter Speicherorte wechseln.
   Wenn die ausgewählten Backups verschlüsselt sind, müssen diese alle dasselbe Verschlüsselungskennwort verwenden. Erstellen Sie für Backups, die unterschiedliche Verschlüsselungskennwörter verwenden, separate Backup-Pläne.
6. Klicken Sie auf **Ziel** und spezifizieren Sie anschließend den Zielspeicherort.

7. [Optional] Bestimmen Sie bei **Art der Replikation**, welche Backups repliziert werden sollen. Sie können eine der folgenden Optionen wählen:
   - **Alle Backusp** (Standardvorgabe)
   - **Nur Voll-Backups**
   - **Nur jeweils das letzte Backup**
8. [Optional] Klicken Sie auf **Planung**, wenn Sie die Planung ändern wollen.
9. [Optional] Klicken Sie auf **Aufbewahrungsregeln** und spezifizieren Sie die gewünschten Aufbewahrungsregeln für den Zielspeicherot (wie im Abschnitt 'Aufbewahrungsregeln' beschrieben).
10. Wenn die Backups, die bei **Zu replizierende Elemente** ausgewählt wurden, verschlüsselt sind, müssen Sie den Schalter **Backup-Kennwort** aktivieren und dann das entsprechende Verschlüsselungskennwort eingeben. Ansonsten können Sie diesen Schritt überspringen.
11. [Optional] Wenn Sie die Plan-Optionen ändern wollen, klicken Sie auf das Zahnradsymbol.
12. Klicken Sie auf **Erstellen**.

# 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.

Bei der Validierung eines Backup-Speicherortes werden alle Backups überprüft, die an diesem Ort gespeichert sind.

## Und so funktioniert es

Ein Validierungsplan bietet Ihnen zwei Validierungsmethoden. Wenn Sie beide Methoden auswählen, werden die Aktionen nacheinander ausgeführt.

- **Eine Prüfsumme für jeden Datenblock berechnen, der im Backup gespeichert ist**
  Weitere Informationen zur Validierung durch Berechnung einer Prüfsumme finden Sie im Abschnitt 'Backup-Validierung'.
- **Eine virtuelle Maschine aus einem Backup heraus ausführen**
  Diese Methode funktioniert nur für Laufwerk-Backups, die ein Betriebssystem enthalten. Um diese Methode verwenden zu können, benötigen Sie einen ESXi- oder Hyper-V-Host und einen Protection Agenten (einen Agenten für VMware oder für Hyper-V), der diesen Host verwaltet.
  Der Agent führt eine virtuelle Maschine aus einem Backup aus und verbinden sich dann mit den VMware Tools oder dem Hyper-V-Taktdienst, um zu überprüfen, ob das Betriebssystem erfolgreich gestartet wurde. Wenn die Verbindung fehlschlägt, versucht der Agent, alle zwei Minuten (und maximal fünfmal) eine Verbindung herzustellen. Falls keine der Verbindungsversuche erfolgreich ist, schlägt die Validierung fehl.
  Unabhängig von der Anzahl der Validierungspläne und der validierten Backups: der Agent, der die Validierung durchführt, führt immer nur jeweils eine virtuelle Maschine aus. Sobald das

Ergebnis der Validierung feststeht, löscht der Agent die betreffende virtuelle Maschine wieder und führt anschließend die nächste aus.

Wenn die Validierung fehlschlägt, können Sie im Bereich **Aktivitäten** (der Registerkarte **Überblick**) zu den entsprechenden Details runterblättern.

## Unterstützte Speicherorte

Die folgende Tabelle fasst Backup-Speicherorte zusammen, die von Validierungsplänen unterstützt werden.

| Backup-Speicherort | Eine Prüfsumme berechnen | Eine VM ausführen |
|---|---|---|
| Cloud Storage | + | + |
| Lokaler Ordner | + | + |
| Netzwerkordner | + | + |
| NFS-Ordner | – | – |
| Einer Secure Zone | – | – |
| SFTP-Server | – | – |
| Verwalteter Speicherort | + | + |
| Bandgerät | + | – |

***Einen neuen Validierungsplan erstellen***

1. Klicken Sie auf **Pläne** –> **Validierung**.
2. Klicken Sie auf **Plan erstellen**.
   Die Software zeigt eine Vorlage für den neuen Plan an.
3. [Optional] Wenn Sie den Namen des Plans ändern wollen, klicken Sie auf den vorgegebenen Standardnamen.
4. Klicken Sie auf **Agent** und bestimmen Sie den Agenten, der die Validierung durchführen soll.
   Wenn Sie eine Validierung durchführen wollen, indem Sie eine virtuelle Maschine aus einem Backup ausführen, müssen Sie einen Agenten für VMware oder Agenten für Hyper-V auswählen. Ansonsten können Sie jeden Agenten auswählen, der auf dem Management Server registriert ist und auf den Backup-Speicherort zugreifen kann.
5. Klicken Sie auf **Zu validierende Elemente** und bestimmen Sie dann die Backups, die dieser Plan überprüfen soll.
   Mit dem Schalter **Speicherorte** / **Backups** (in der rechten oberen Ecke) können Sie zwischen der Auswahl von Backups und der Auswahl kompletter Speicherorte wechseln.
   Wenn die ausgewählten Backups verschlüsselt sind, müssen diese alle dasselbe Verschlüsselungskennwort verwenden. Erstellen Sie für Backups, die unterschiedliche Verschlüsselungskennwörter verwenden, separate Backup-Pläne.

6. [Optional] Bestimmen Sie bei **Validierungsquelle**, welche Backups überprüft werden sollen. Sie können eine der folgenden Optionen wählen:
   - **Alle Backups**
   - **Nur jeweils das letzte Backup**
7. [Optional] Klicken Sie auf **Art der Validierung** und wählen Sie dann eine der nachfolgenden Methoden:
   - **Prüfsummen-Verifizierung**

     Die Software wird eine Prüfsumme für jeden Datenblock berechnen, der im Backup gespeichert ist.
   - **Als virtuelle Maschine ausführen**

     Die Software wird eine virtuelle Maschine aus jedem Backup heraus ausführen.
8. Wenn Sie die Option **Als virtuelle Maschine ausführen** wählen:
   a. Klicken Sie auf **Zielmaschine** und bestimmen Sie dann den Typ der virtuellen Maschine (ESXi oder Hyper-V), den Host und die Vorlage für den Maschinennamen.

      Der Standardname ist **[Maschinenname]_validieren**.
   b. Klicken Sie auf **Datenspeicher** für ESXi oder **Pfad** für Hyper-V – und bestimmten Sie dann den Datenspeicher für die neue virtuelle Maschine.
   c. [Optional] Den Laufwerk-Provisioning-Modus ändern

      Die Standardeinstellung ist **Thin** für VMware ESXi und **Dynamisch erweiterbar** für Hyper-V.
   d. [Optional] Klicken Sie auf **VM-Einstellungen**, um die Größe des Arbeitsspeichers und die Netzwerkverbindungen der virtuellen Maschine zu ändern.

      Die virtuelle Maschine ist standardmäßig *nicht* mit einem Netzwerk verbunden und die Größe ihres Arbeitsspeichers entspricht der der ursprünglichen Maschine.

   **Hinweis**
   Der Schalter **VM-Takt (Heartbeat)** ist immer aktiviert, um den Status des Takts der virtuellen Maschine zu überprüfen, der von den Hypervisor Tools im Gastbetriebssystem (den VMware Tools oder den Hyper-V Integration Services) gemeldet wird, wenn Sie eine virtuelle Maschine aus einem Backup ausführen. Dieser Schalter ist für zukünftige Versionen vorgesehen, weswegen Sie ihn derzeit nicht beeinflussen können.
9. [Optional] Klicken Sie auf **Planung**, wenn Sie die Planung ändern wollen.
10. Wenn die Backups, die bei **Zu validierende Elemente** ausgewählt wurden, verschlüsselt sind, müssen Sie den Schalter **Backup-Kennwort** aktivieren und dann das entsprechende Verschlüsselungskennwort eingeben. Ansonsten können Sie diesen Schritt überspringen.
11. [Optional] Wenn Sie die Plan-Optionen ändern wollen, klicken Sie auf das Zahnradsymbol.
12. Klicken Sie auf **Erstellen**.

# Bereinigung

Eine Bereinigung ist eine Aktion, die veraltete Backups gemäß von spezifizierten Aufbewahrungsregeln löscht.

## Unterstützte Speicherorte

Bereinigungspläne unterstützten alle Backup-Speicherorte – ausgenommen NFS-Ordner, SFTP-Server und die Einer Secure Zone.

***Einen neuen Bereinigungsplan erstellen***

1. Klicken Sie auf **Pläne** –> **Bereinigung**.
2. Klicken Sie auf **Plan erstellen**.
   Die Software zeigt eine Vorlage für den neuen Plan an.
3. [Optional] Wenn Sie den Namen des Plans ändern wollen, klicken Sie auf den vorgegebenen Standardnamen.
4. Klicken Sie auf **Agent** und bestimmen Sie den Agenten, der die Bereinigung durchführen soll.
   Sie können jeden Agenten auswählen, der auf den Backup-Speicherort zugreifen kann.
5. Klicken Sie auf **Zu bereinigende Elemente** und bestimmten Sie dann die Backups, die dieser Plan bereinigen soll.
   Mit dem Schalter **Speicherorte** / **Backups** (in der rechten oberen Ecke) können Sie zwischen der Auswahl von Backups und der Auswahl kompletter Speicherorte wechseln.
   Wenn die ausgewählten Backups verschlüsselt sind, müssen diese alle dasselbe Verschlüsselungskennwort verwenden. Erstellen Sie für Backups, die unterschiedliche Verschlüsselungskennwörter verwenden, separate Backup-Pläne.
6. [Optional] Klicken Sie auf **Planung**, wenn Sie die Planung ändern wollen.
7. [Optional] Klicken Sie auf **Aufbewahrungsregeln** und spezifizieren Sie die gewünschten Aufbewahrungsregeln (wie im Abschnitt 'Aufbewahrungsregeln' beschrieben).
8. Wenn die Backups, die bei **Zu bereinigenden Elemente** ausgewählt wurden, verschlüsselt sind, müssen Sie den Schalter **Backup-Kennwort** aktivieren und dann das entsprechende Verschlüsselungskennwort eingeben. Ansonsten können Sie diesen Schritt überspringen.
9. [Optional] Wenn Sie die Plan-Optionen ändern wollen, klicken Sie auf das Zahnradsymbol.
10. Klicken Sie auf **Erstellen**.

# Konvertierung zu einer virtuellen Maschine

Sie können einen separaten Plan für die Konvertierung zu einer virtuellen Maschine erstellen und diesen Plan manuell oder zeitgesteuert ausführen.

Informationen zu Voraussetzungen und Einschränkungen finden Sie im Abschnitt 'Was Sie über Konvertierungen wissen müssen'.

***So können Sie einen Plan für die Konvertierung zu einer virtuellen Maschine erstellen***

1. Klicken Sie auf **Pläne** –> **Konvertierung zu VM**.
2. Klicken Sie auf **Plan erstellen**.
   Die Software zeigt eine Vorlage für den neuen Plan an.
3. [Optional] Wenn Sie den Namen des Plans ändern wollen, klicken Sie auf den vorgegebenen Standardnamen.
4. Bestimmen Sie bei **Konvertieren zu** den Typ der virtuellen Zielmaschine. Sie können eine der folgenden Optionen wählen:
   - **VMware ESXi**
   - **Microsoft Hyper-V**
   - **Scale Computing HC3**
   - **VMware Workstation**
   - **VHDX-Dateien**

   **Hinweis**
   Um Speicherplatz zu sparen, werden bei jeder Konvertierung zu VHDX-Dateien die entsprechenden VHDX-Dateien am Zielort überschrieben, die bei der vorherigen Konvertierung erstellt wurden.
5. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - [Für VMware ESXi, Hyper-V und Scale Computing HC3] Klicken Sie auf **Host**, wählen Sie den Zielhost und spezifizieren Sie die Vorlage für den Namen der neuen Maschine.
   - [Für andere Arten von virtuellen Maschinen] Spezifizieren Sie bei **Pfad**, wo die Dateien der virtuellen Maschinen und die Dateinamensvorlage gespeichert werden sollen.

   Der Standardname ist **[Maschinenname]_konvertiert**.
6. Klicken Sie auf **Agent** und bestimmen Sie den Agenten, der die Konvertierung durchführen soll.
7. Klicken Sie auf **Zu konvertierende Elemente** und bestimmen Sie dann die Backups, die dieser Plan zu virtuellen Maschinen konvertieren soll.
   Mit dem Schalter **Speicherorte** / **Backups** (in der rechten oberen Ecke) können Sie zwischen der Auswahl von Backups und der Auswahl kompletter Speicherorte wechseln.
   Wenn die ausgewählten Backups verschlüsselt sind, müssen diese alle dasselbe Verschlüsselungskennwort verwenden. Erstellen Sie für Backups, die unterschiedliche Verschlüsselungskennwörter verwenden, separate Backup-Pläne.
8. [Nur für VMware ESXi und Hyper-V] Klicken Sie auf **Datenspeicher** für ESXi oder **Pfad** für Hyper-V – und bestimmten Sie dann den Datenspeicher (Storage) für die virtuelle Maschine.
9. [Nur für VMware ESXi und Hyper-V] Wählen Sie den Laufwerk-Provisioning-Modus. Die Standardeinstellung ist **Thin** für VMware ESXi und **Dynamisch erweiterbar** für Hyper-V.
10. [Optional] [Für VMware ESXi, Hyper-V und Scale Computing HC3] Klicken Sie auf **VM-Einstellungen**, um die Größe des Arbeitsspeichers, die Anzahl der Prozessoren und die Netzwerkverbindungen für die virtuelle Maschine zu ändern.
11. [Optional] Klicken Sie auf **Planung**, wenn Sie die Planung ändern wollen.

12. Wenn die Backups, die bei **Zu konvertierende Elemente** ausgewählt wurden, verschlüsselt sind, müssen Sie den Schalter **Backup-Kennwort** aktivieren und dann das entsprechende Verschlüsselungskennwort eingeben. Ansonsten können Sie diesen Schritt überspringen.
13. [Optional] Wenn Sie die Plan-Optionen ändern wollen, klicken Sie auf das Zahnradsymbol.
14. Klicken Sie auf **Erstellen**.

# Boot-Medium

**Wichtig**
Einige der in diesem Abschnitt beschriebenen Funktionen stehen nur bei On-Premise-Bereitstellungen zur Verfügung.

## Boot-Medium

Ein Boot-Medium ist ein physisches Medium (CD, DVD, USB-Stick oder andere Wechselmedien, die vom BIOS einer Maschine als Boot-Gerät unterstützt werden), das es Ihnen ermöglicht, den Protection Agenten in einer Linux-basierten Umgebung oder unter WinPE (Windows Preinstallation Environment) auszuführen, damit er auch ohne die Hilfe eines bereits vorhandenen Betriebssystems laufen kann.

Ein Boot-Medium wird am häufigsten verwendet, um:

- Ein Betriebssystem wiederherzustellen, das nicht mehr bootet
- Auf Daten zuzugreifen und zu sichern, die in einem beschädigten System überlebt haben
- Ein Betriebssystem auf fabrikneue Computer zu verteilen
- Volumes vom Typ 'Basis' oder 'Dynamisch' auf fabrikneuen Geräten einzurichten
- Laufwerke, die ein nicht unterstütztes Dateisystem verwenden, mit einem Sektor-für-Sektor-Backup zu sichern
- Daten offline zu sichern, die nicht online gesichert werden können – z.B., weil die Daten von einer laufenden Applikation gesperrt werden oder weil der Zugriff auf diese anderweit beschränkt ist.

Eine Maschine kann außerdem auch mithilfe des Acronis PXE Servers, der Windows Deployment Services (WDS) oder des Microsoft Remote Installation Service (RIS) über das Netzwerk gebootet werden. Diese Server können (dank der hochgeladenen, bootfähigen Komponenten) selbst als eine Art Boot-Medium betrachtet werden. Sie können mithilfe desselben Assistentens entweder ein Boot-Medium erstellen oder den PXE Server bzw. die WDS/RIS-Dienste konfigurieren.

## Sollten Sie ein Boot-Medium selbst erstellen oder ein vorgefertigtes Boot-Medium herunterladen?

Sie können über den Bootable Media Builder Ihre eigenen Boot-Medien (Linux-basiert oder WinPE-basiert) für Windows-, Linux- oder macOS-Computer erstellen. Für ein Boot-Medium mit vollem Funktionsumfang müssen Sie einen Acronis Cyber Protect Lizenzschlüssel spezifizieren. Ohne diesen Schlüssel kann Ihr Boot-Medium nur Wiederherstellungsaktionen durchführen.

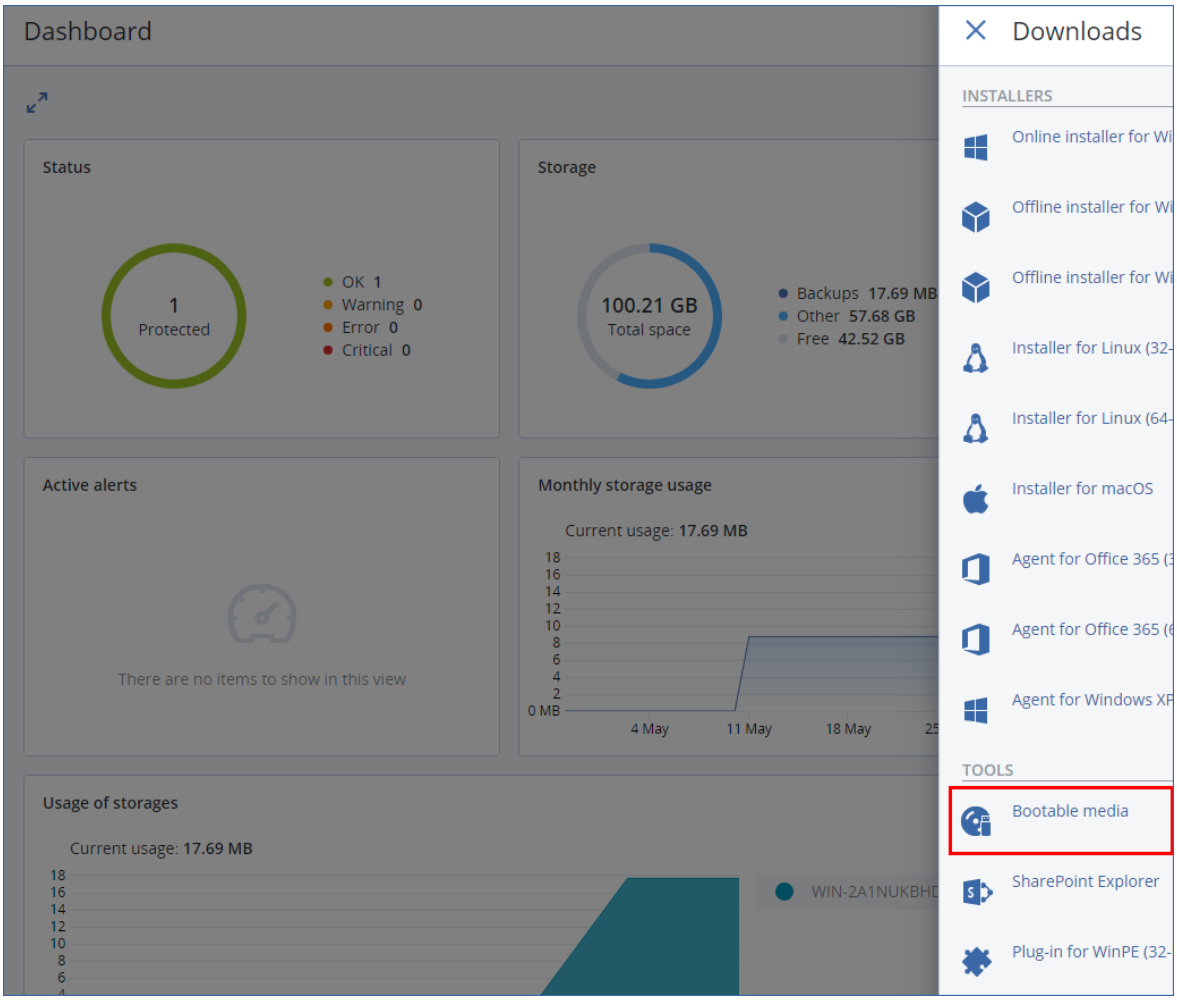
**Hinweis**
Das Boot-Medium unterstützt keine Hybrid-Laufwerke.

Sie können aber auch ein vorgefertigtes Boot-Medium herunterladen (nur auf Linux-basiert). Sie können das heruntergeladene Boot-Medium nur für Wiederherstellungsaktionen verwenden und um die Acronis Universal Restore-Funktionalität zu nutzen. Sie können keine Daten sichern, Backups validieren oder exportieren, Laufwerke verwalten oder über das Boot-Medium mit Skripten verwenden. Das vorgefertigte Boot-Medium ist nicht für macOS-Computer geeignet.

**Hinweis**
Das vorgefertigte Boot-Medium bietet keine Unterstützung für folgende Speicherorte: Storage Node, Bänder und SFTP-Server. Wenn Sie diese Speicherorte in Ihrer On-Premise-Bereitstellung verwenden wollen, müssen Sie Ihr eigenes, benutzerdefiniertes Boot-Medium mit dem Bootable Media Builder erstellen. Siehe: https://kb.acronis.com/de/content/61566.

***So können Sie ein vorgefertigtes Boot-Medium herunterladen***

1. Klicken Sie in der rechten oberen Ecke der Cyber Protect Webkonsole auf das Symbol für das Konto und anschließend auf **Downloads**.
2. Wählen Sie die Option **Boot-Medium**.




Sie können die heruntergeladene ISO-Datei auf eine CD/DVD brennen oder ein bootfähiges USB-Flash-Laufwerk erstellen. Um einen USB-Stick (als Vorbereitung) 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.

Wenn auf die Cyber Protect Webkonsole nicht zugegriffen werden kann, können Sie das vorgefertigte Boot-Medium auch über Ihr Konto im Bereich 'Kundenservice und Support' der Acronis Website herunterladen:

1. Gehen Sie dafür zu: https://account.acronis.com.
2. Suchen Sie Acronis Cyber Protect und klicken Sie anschließend auf **Downloads**.
3. Suchen Sie auf der sich öffnenden Seite den Eintrag **Zusätzliche Downloads** und klicken Sie dann dann auf den Eintrag **Boot-Medium-ISO (für Windows und Linux)**.

# Linux-basiertes oder WinPE-basiertes Boot-Medium?

## Linux-basiert

Ein Linux-basiertes Medium enthält einen bootfähigen Protection Agenten, der auf einem Linux-Kernel beruht. Der Agent kann auf jeder PC-kompatiblen Hardware booten und dort Aktionen ausführen, einschließlich auf fabrikneuer Hardware und Maschinen mit einem beschädigten oder nicht unterstützten Dateisystem. Die Aktionen können entweder lokal oder remote über die Cyber Protect Webkonsole konfiguriert und gesteuert werden.

Eine Liste der Hardware, die von Linux-basierten Boot-Medien unterstützt wird, können Sie hier finden: http://kb.acronis.com/content/55310.

## WinPE-basiert

Ein WinPE-basierte Boot-Medium enthält ein funktionsreduziertes Windows, welches WinPE (für Windows Preinstallation Environment) genannt wird, sowie ein Acronis-Plug-in für dieses WinPE. Bei diesem Plug-in handelt es sich um eine speziell angepasste Variante des Protection Agenten, damit dieser unter WinPE laufen kann.

WinPE hat sich gerade bei großen IT-Umgebungen mit unterschiedlicher Hardware als sehr praktische bootfähige Lösung erwiesen.

**Vorteile:**

- Die Verwendung von Acronis Cyber Protect für ein WinPE-Medium bietet mehr Funktionalität als die Verwendung Linux-basierter Boot-Medien. Wenn Sie Ihre PC-kompatible Hardware mit einem WinPE-Medium booten, können Sie nicht nur einen Protection Agenten ausführen, sondern auch spezielle WinPE-Befehle, Skripte und andere Plug-ins, die Sie in das WinPE-Medium eingebunden haben.

- Boot-Medien auf PE-Basis helfen, Linux-bezogene Probleme zu umgehen, z.B. fehlende Unterstützung für RAID-Controller oder gewisse RAID-Level. Auf WinPE 2.x (und höher) basierende Medien ermöglichen es, benötigte Gerätetreiber dynamisch zu laden.

**Beschränkungen:**

- Boot-Medien, die auf WinPE vor Version 4.0 basieren, können keine Maschinen booten, die UEFI (Unified Extensible Firmware Interface) verwenden.
- Wenn eine Maschine mit einem PE-basierten Boot-Medium gestartet wird, können Sie keine optischen Medien wie CDs, DVDs oder Blu-ray-Medien (BD) als Backup-Ziel auswählen.

# Bootable Media Builder

Der Bootable Media Builder ist ein spezielles Werkzeug zur Erstellung eines Boot-Mediums. Es ist nur für On-Premise-Bereitstellungen verfügbar.

Der Bootable Media Builder wird standardmäßig mitinstalliert, wenn Sie den Management Server installieren. Sie können den Media Builder auch einzeln auf jeder Maschine installieren, die unter Windows oder Linux läuft. Es werden dieselben Betriebssysteme unterstützt wie bei den entsprechenden Agenten.

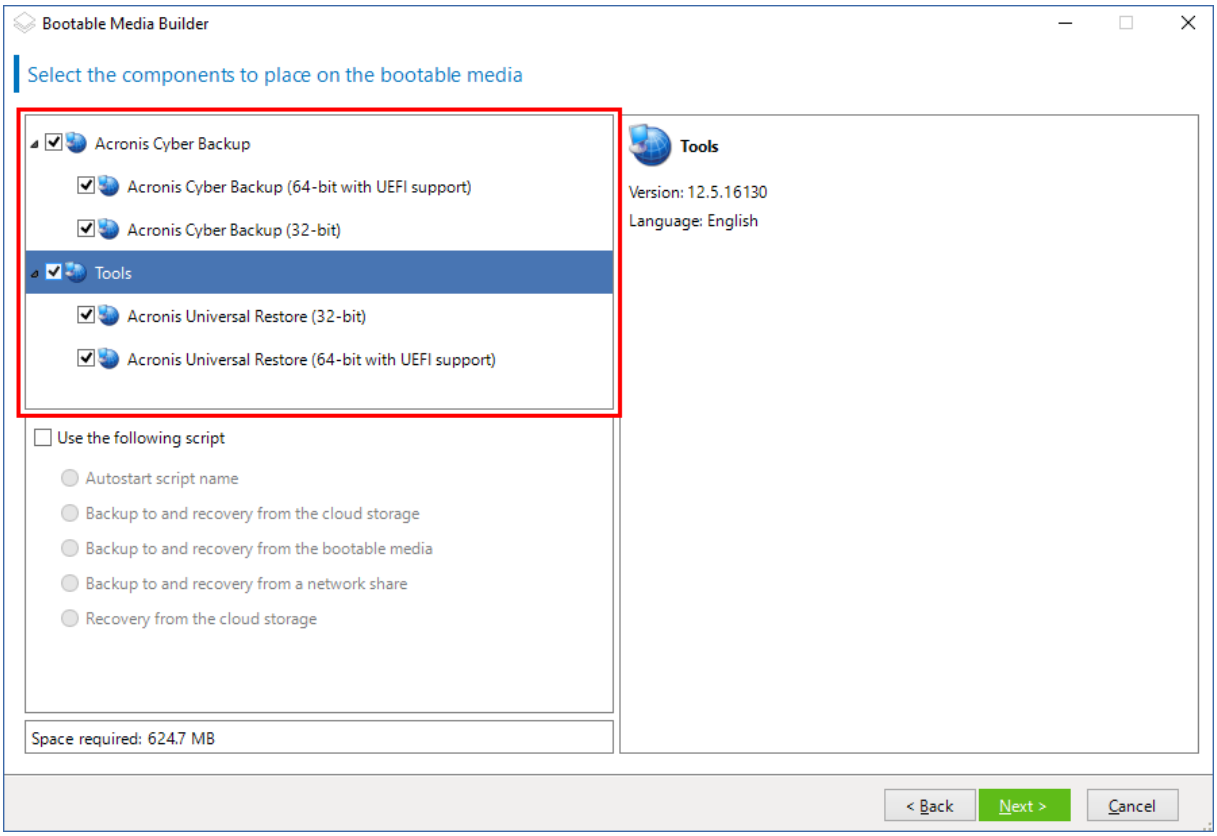
## Warum sollten Sie den Media Builder verwenden?

Das vorgefertigte Boot-Medium, das in der Cyber Protect Webkonsole zum Download bereitgestellt wird, kann nur für Wiederherstellungen verwendet werden. Diese Medium basiert auf einem Linux-Kernel. Anders als Windows PE ist es hier nicht möglich, eigene benutzerdefinierte Treiber in das Medium mit zu integrieren.

- Mit dem Media Builder können Sie ein benutzerdefiniertes und voll funktionsfähiges Boot-Medium erstellten (entweder Linux- oder WinPE-basiert), welches über die Backup-Funktionalität verfügt.
- Neben der Möglichkeit, ein physisches Boot-Medium zu erstellen, können Sie dessen Komponenten auch zum Netzwerk-Booten über die Windows Deployment Services (WDS) hochladen.
- Das vorgefertigte Boot-Medium bietet keine Unterstützung für folgende Speicherorte: Storage Node, Bänder und SFTP-Server. Wenn Sie diese Speicherorte in Ihrer lokalen On-Premise-Bereitstellung verwenden wollen, müssen Sie Ihr eigenes, benutzerdefiniertes Boot-Medium mit dem Bootable Media Builder erstellen. Siehe: https://kb.acronis.com/de/content/61566.

## 32 oder 64 Bit?

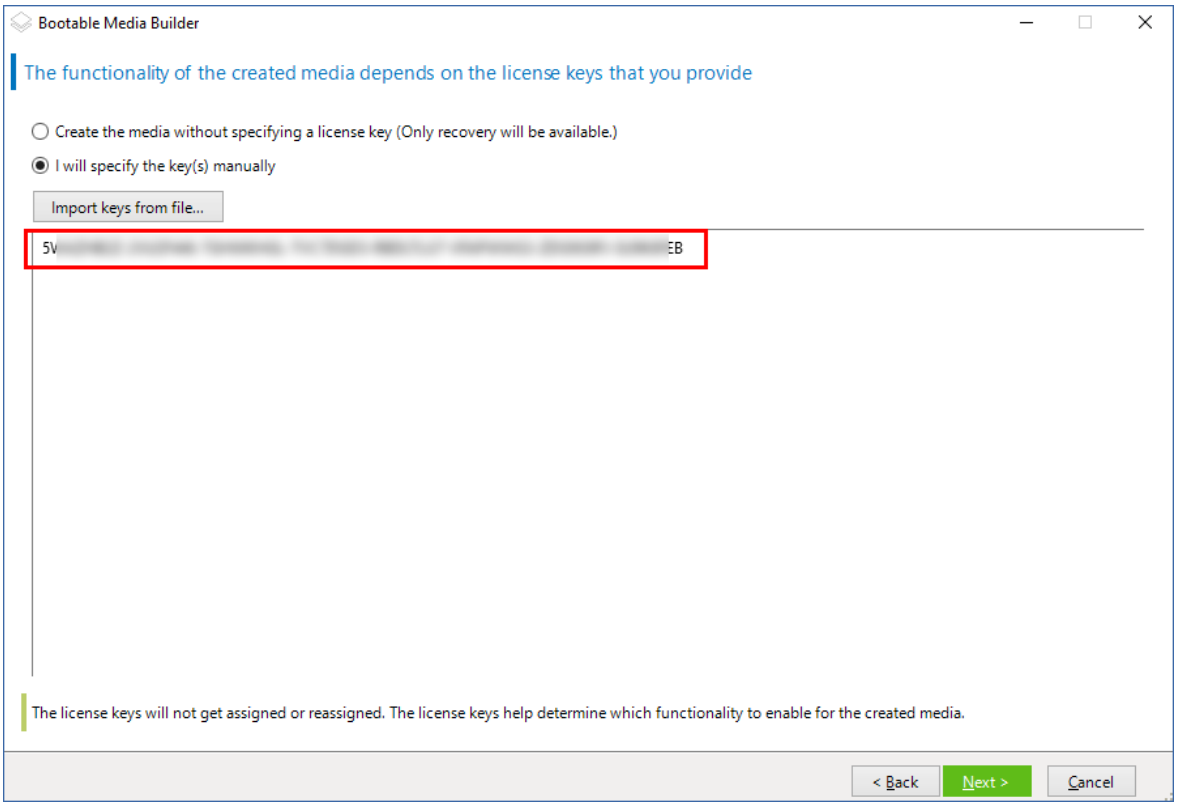
Der Bootable Media Builder kann Boot-Medien mit 32-Bit- und 64-Bit-Komponenten erstellen. Um eine Maschinen zu booten, die ein modernes UEFI (Unified Extensible Firmware Interface) verwendet, benötigen Sie normalerweise ein 64-Bit-Boot-Medium.



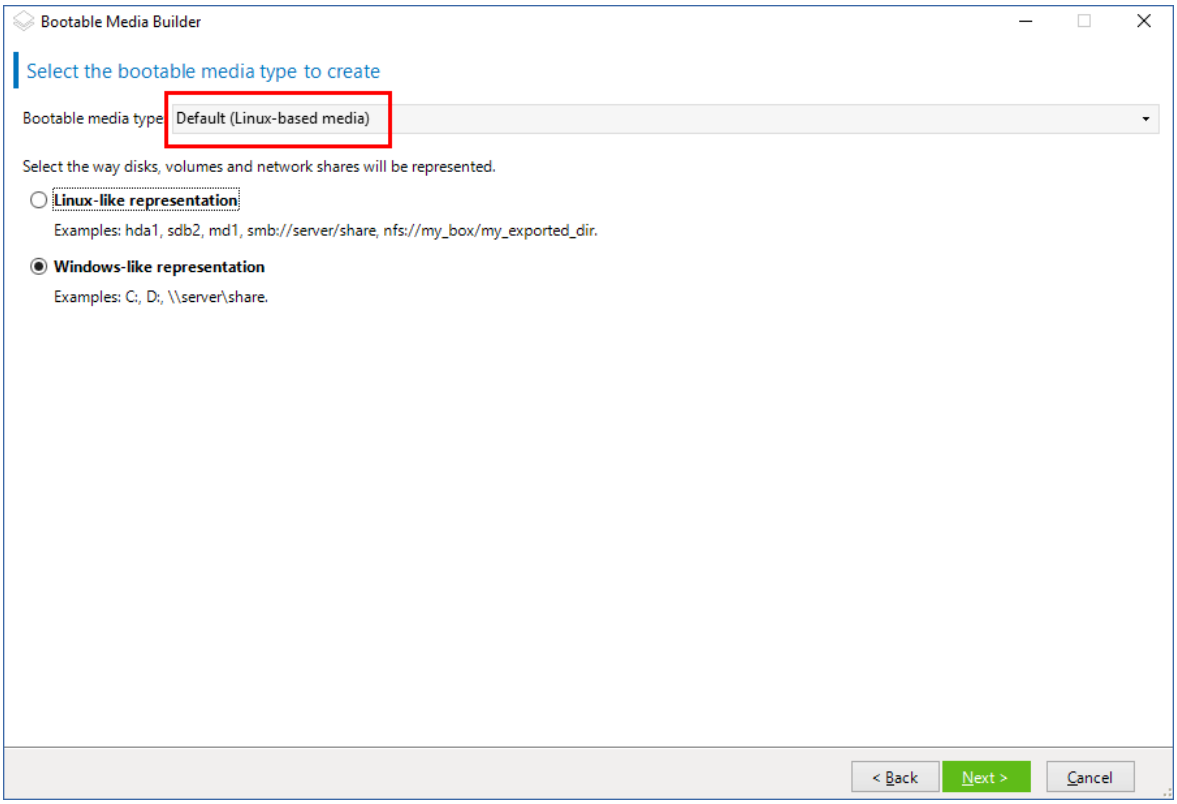

## Linux-basiertes Boot-Medium

***So erstellen Sie ein Boot-Medium, das auf Linux basiert***

1. Starten Sie den **Bootable Media Builder**.
2. Wenn Sie ein Boot-Medium mit vollem Funktionsumfang erstellen wollen, müssen Sie einen Acronis Cyber Protect Lizenzschlüssel spezifizieren. Dieser Schlüssel wird verwendet, um festzulegen, welche Funktionen das Boot-Medium enthalten soll. Es werden keine Lizenzen von irgendwelchen Maschinen widerrufen.
   Wenn Sie keinen Lizenzschlüssel spezifizieren, kann das resultierende Boot-Medium nur für Wiederherstellungsaktionen verwendet werden.




3. Wählen Sie den gewünschten **Typ des Boot-Mediums: Standard (Linux-basiertes Medium)**.
   Bestimmen Sie, wie die Volumes und Netzwerkressourcen angezeigt werden sollen:
   - Ein Medium mit Linux-typischer Volume-Darstellung zeigt die Volumes beispielsweise als hda1 und sdb2 an. Es versucht, MD-Geräte und logische Volumes (vom LVM verwaltet) vor Start einer Wiederherstellung zu rekonstruieren.
   - Ein Medium, mit Windows-typischer Volumes-Darstellung repräsentiert die Volumes über Laufwerksbuchstaben – beispielsweise Laufwerk C: und D:. Es bietet Zugriff auf dynamische Volumes (LDM verwaltet).




4. [Optional] Sie können Parameter für den Linux-Kernel spezifizieren. Wenn Sie mehrere Parameter eingeben wollen, trennen Sie diese per Leerzeichen.

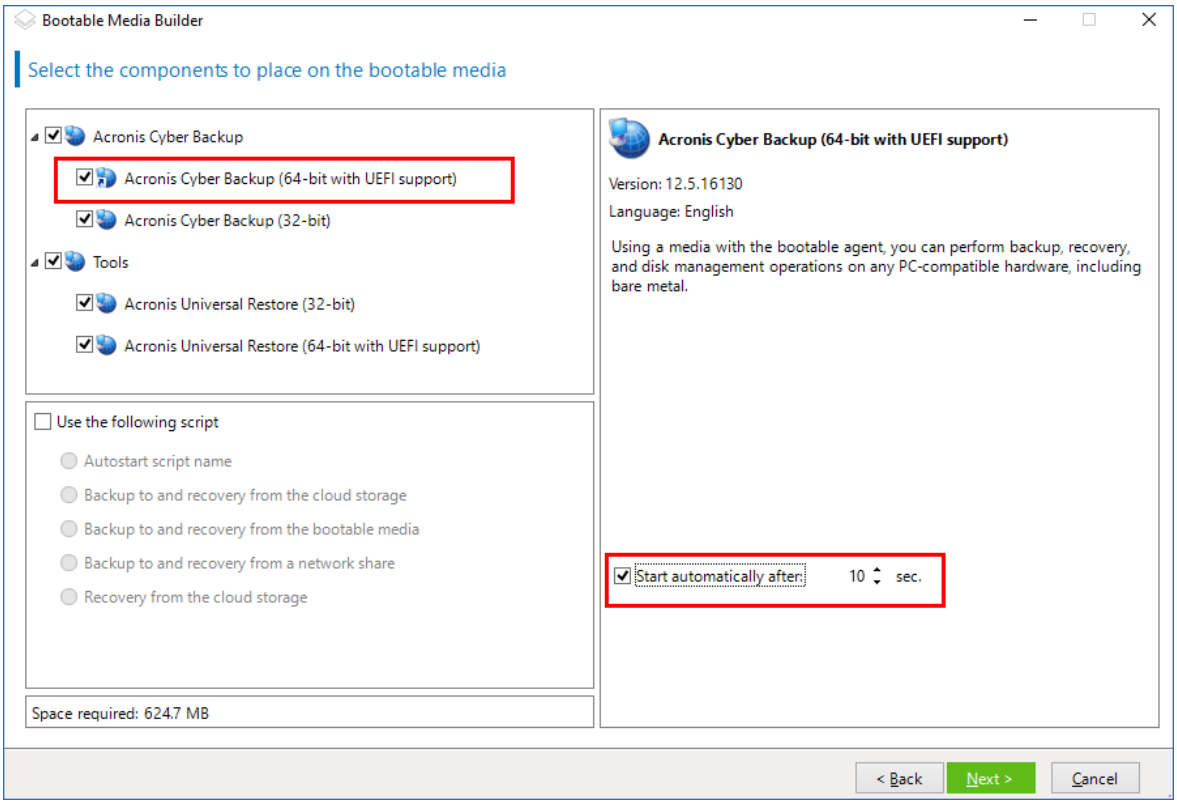
   Geben Sie beispielsweise Folgendes ein, wenn Sie beim Starten des Mediums einen bestimmten Anzeigemodus für eine bootfähigen Agenten auswählen wollen: **vga=ask**

   Weitere Informationen über die verfügbaren Parameter finden Sie im Abschnitt 'Kernel-Parameter'.
5. [Optional] Bestimmen Sie die Sprache, die für das Boot-Medium verwendet werden soll.
6. Wählen Sie die Komponenten, die auf dem Medium eingerichtet werden sollen: den bootfähigen Acronis Cyber Protect Agenten und/oder Universal Restore (wenn Sie das System auf abweichender Hardware wiederherstellen wollen).

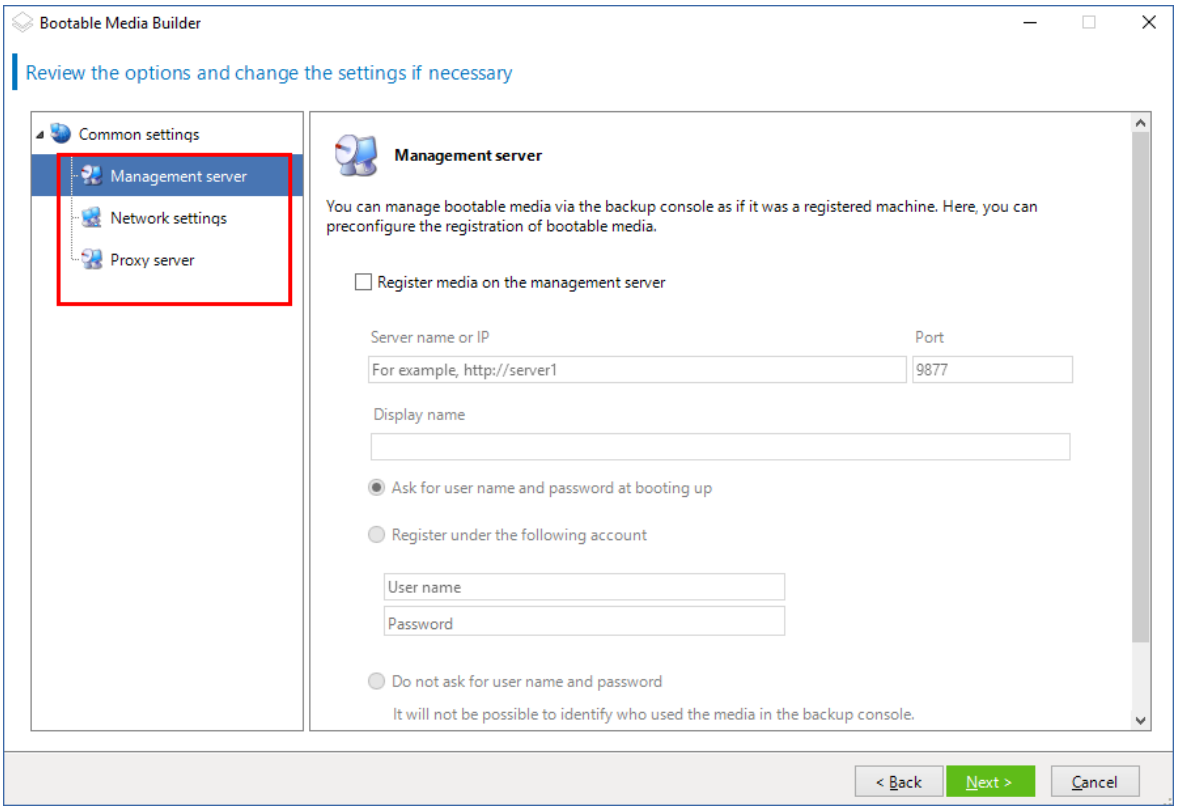
   Mit dem bootfähigen Agenten können Sie Backup-, Recovery- und Laufwerksverwaltungsaktionen auf PC-kompatibler Hardware (einschließlich fabrikneuen Maschinen) durchführen.

   Mit Universal Restore können Sie die Bootfähigkeit eines Betriebssystems, welches Sie auf abweichender Hardware oder auf einer virtuellen Maschine wiederhergestellt haben, gewährleisten bzw. wiederherstellen. Das Tool findet und installiert Treiber für solche Geräte, die für den Betriebssystemstart notwendig sind. Das sind insbesondere Treiber für Storage-Controller (Festplatten-Controller) sowie für das Mainboard und dessen Chipsatz.
7. [Optional] Spezifizieren Sie ein Timeout-Intervall für das Boot-Menü, sowie diejenige Komponente, die nach Ablauf dieses Zeitlimits automatisch gestartet werden soll. Klicken Sie dafür auf die gewünschte Komponente im oberen linken Fensterbereich und legen Sie dann das Intervall für die Komponente fest. Dies ermöglicht einen unbeaufsichtigten Betrieb vor Ort, wenn per WDS/RIS gebootet wird.

Wenn diese Einstellung nicht konfiguriert wird, wartet der Loader des Boot-Mediums darauf, dass Sie auswählen, ob das Betriebssystem (sofern vorhanden) oder eine entsprechende Komponente gestartet werden soll.




8. [Optional] Wenn Sie die Aktionen des bootfähigen Agenten automatisieren wollen, aktivieren Sie das Kontrollkästchen **Folgendes Skript verwenden**. Wählen Sie dann eines der Skripte aus und spezifizieren Sie die Parameter für das Skript.
9. [Optional] Bestimmen Sie, wie das Medium beim Booten auf dem Management Server registriert werden soll. Zu weiteren Informationen über die Registrierungseinstellungen siehe den Abschnitt 'Management Server'.




10. [Optional] Spezifzieren Sie die Netzwerkeinstellungen: TCP/IP-Einstellungen, die den Netzwerkkarten der Maschine zugewiesen werden. Weitere Informationen dazu finden Sie im Abschnitt '"Netzwerkeinstellungen" (S. 400)'.
11. [Optional] Spezifizieren Sie einen Netzwerk-Port: Der TCP-Port, den der bootfähige Agent auf eingehende Verbindungen überwacht.
12. [Optional] Falls in Ihrem Netzwerk ein Proxy-Server aktiv ist, spezifizieren Sie dessen Host-Namen/IP-Adresse und Port.
13. Wählen Sie den Typ des Mediums aus. Sie können:
    - Ein ISO-Image erstellen. Dann können Sie es auf eine CD/DVD brennen, einen bootfähigen USB-Stick damit erstellen oder es an eine virtuelle Maschine anschließen (mounten).
    - Eine ZIP-Datei erstellen.
    - Die gewählten Komponenten auf den Acronis PXE Server hochladen
    - Die gewählten Komponenten auf einen WDS/RIS hochladen.
14. [Optional] Fügen Sie Windows System-Treiber zur Verwendung durch Universal Restore hinzu. Dieses Fenster erscheint, wenn Universal Restore dem Medium hinzugefügt wurde und nicht 'WDS/RIS' als Medium ausgewählt wurde.
15. Spezifizieren Sie bei Aufforderung den Host-Namen/die IP-Adresse und Anmeldedaten für WDS/RIS an – oder einen Pfad, wo die ISO-Datei des Mediums gespeichert werden soll.
16. Überprüfen Sie Ihre Einstellungen im Fenster 'Zusammenfassung' und klicken Sie dann auf **Fertig stellen**.

## Kernel-Parameter

In diesem Fenster können Sie einen oder mehrere Parameter des Linux-Kernel angeben. Diese werden automatisch wirksam, wenn das bootfähige Medium startet.

Typischerweise kommen diese Parameter zur Anwendung, wenn während der Arbeit mit bootfähigen Medien Probleme auftauchen. Normalerweise brauchen Sie in dieses Feld nichts einzutragen.

Sie können jeden dieser Parameter auch durch Drücken der Taste 'F11' im Boot-Menü angeben.

### Parameter

Trennen Sie mehrere Parameter mit Leerzeichen.

**acpi=off**

Deaktiviert ACPI (Advanced Configuration and Power Interface). Dieser Parameter kann hilfreich sein, wenn bei einer bestimmten Hardware-Konfiguration Probleme auftauchen.

**noapic**

Deaktiviert APIC (Advanced Programmable Interrupt Controller). Dieser Parameter kann hilfreich sein, wenn bei einer bestimmten Hardware-Konfiguration Probleme auftauchen.

**vga=ask**

Erfragt den Grafikkartenmodus, der in der grafischen Benutzeroberfläche eines bootfähigen Mediums verwendet werden soll. Ist kein **vga**-Parameter angegeben, wird der Videomodus automatisch erkannt.

**vga=** *mode_number*

Spezifiziert den Grafikkartenmodus, der in der grafischen Benutzeroberfläche des Boot-Mediums verwendet werden soll. Die Modus-Nummer wird unter *mode_number* im Hexadezimalformat angegeben, z.B.: **vga=0x318**

Die Bildschirmauflösung und die Anzahl der Farben für eine Modus-Nummer können sich von Maschine zu Maschine unterscheiden. Es wird empfohlen, zunächst den Parameter **vga=ask** zu verwenden, um einen Wert für *mode_number* auszuwählen.

**quiet**

Deaktiviert die Anzeige von Pop-up-Meldungen während der Linux-Kernel geladen wird und startet danach die Management Konsole.

Dieser Parameter wird implizit bei der Erstellung von bootfähigen Medien spezifiziert; Sie können ihn jedoch im Boot-Menü entfernen.

Wenn der Parameter nicht angegeben ist, werden alle Meldungen beim Start angezeigt, gefolgt von einer Eingabeaufforderung. Geben Sie bei der Eingabeaufforderung folgenden Befehl ein, um die Management Konsole zu starten: **/bin/product**

**nousb**

Deaktiviert, dass das USB-Subsystem geladen wird.

**nousb2**

Deaktiviert die USB 2.0-Unterstützung. USB 1.1-Geräte arbeiten, auch wenn dieser Parameter gesetzt ist. Mit dem Parameter können Sie manche USB-Laufwerke im USB 1.1-Modus verwenden, wenn sie im USB 2.0-Modus nicht arbeiten.

**nodma**

Deaktiviert den Speicherdirektzugriff (DMA) für alle IDE-Festplatten. Verhindert auf mancher Hardware ein Einfrieren des Kernels.

**nofw**

Deaktiviert die Unterstützung für die FireWire (IEEE1394)-Schnittstelle.

**nopcmcia**

Deaktiviert die Erkennung von PCMCIA-Hardware.

**nomouse**

Deaktiviert die Maus-Unterstützung.

*module_name* **=off**

Deaktiviert das Modul, dessen Name in *module_name* angeben ist. Um beispielsweise die Nutzung des SATA-Moduls zu deaktivieren, geben Sie folgenden Wert an: **sata_sis=off**

**pci=bios**

Erzwingt die Verwendung des PCI-BIOS statt direkt auf die Hardware-Geräte zuzugreifen. Dieser Parameter kann hilfreich sein, z.B. wenn die Maschine eine nicht standardgemäße PCI Host-Bridge hat.

**pci=nobios**

Deaktiviert die Verwendung des PCI BIOS und erlaubt nur direkte Hardware-Zugriffsmethoden. Dieser Parameter kann z.B. hilfreich sein, wenn das bootfähige Medium nicht startet und dies wahrscheinlich durch das BIOS verursacht wird.

**pci=biosirq**

Verwendet PCI BIOS-Aufrufe, um die Interrupt Routing-Tabelle zu erhalten. Dieser Parameter kann hilfreich sein, wenn es dem Kernel nicht gelingt, Unterbrechungsanforderungen (IRQs) zuzuordnen oder den sekundären PCI-Bus auf dem Mainboard zu finden.

Auf einigen Maschinen funktionieren diese Aufrufe möglicherweise nicht richtig. Es kann unter Umständen aber der einzige Weg sein, die Interrupt Routing-Tabelle anzuzeigen.

**LAYOUTS=en-US, de-DE, fr-FR, ...**

Spezifiziert das Tastaturlayout, das in der grafischen Benutzeroberfläche des Boot-Mediums verwendet werden soll.

Ohne diesen Parameter können nur zwei Layouts verwendet werden: Englisch (USA) und dasjenige Layout, welches der Sprache entspricht, die im Boot-Menü des Mediums ausgewählt wurde.

Sie können jedes der folgenden Layouts verwenden:

Belgisch **be-BE**

Tschechisch: **cz-CZ**

Englisch: **en-GB**

Englisch (USA): **en-US**

Französisch: **fr-FR**

Französisch (Schweiz): **fr-CH**

Deutsch: **de-DE**

Deutsch (Schweiz): **de-CH**

Italienisch: **it-IT**

Polnisch: **pl-PL**

Portugiesisch: **pt-PT**

Portugiesisch (Brasilien): **pt-BR**

Russisch: **ru-RU**

Serbisch (Kyrillische Zeichen): **sr-CR**

Serbisch (Lateinische Zeichen): **sr-LT**

Spanisch: **es-ES**

Wenn Sie unter einem Boot-Medium arbeiten, können Sie mit der Tastenkombination Strg+Umschalt durch die verfügbaren Layouts wechseln.

## Skripte in Boot-Medien

Wenn Sie möchten, dass ein Boot-Medium eine bestimmte Folge von Aktionen ausführt, können Sie beim Erstellen des Mediums im Bootable Media Builder ein Skript definieren. Das Medium wird bei jedem Boot-Vorgang dieses Skript ausführen, statt die Benutzeroberfläche anzuzeigen.

Sie können eines der vordefinierten Skripte auswählen oder ein benutzerdefiniertes Skript auf Grundlage der Skript-Konventionen erstellen.

### Vordefinierte Skripte

Der Bootable Media Builder stellt folgende vordefinierte Skripte bereit:

- Backup zu und Recovery aus dem Cloud Storage (**entire_pc_cloud**)
- Backup zu und Recovery von einem Boot-Medium (**entire_pc_cloud**)
- Backup zu und Recovery von einer Netzwerkfreigabe (**entire_pc_share**)
- Recovery aus dem Cloud Storage (**golden_image**)

Die Skripte können auf der Maschine, auf welcher der Bootable Media Builder installiert ist, in folgenden Verzeichnissen gefunden werden:

- Unter Windows: %**ProgramData%\Acronis\MediaBuilder\scripts**
- Unter Linux: **/var/lib/Acronis/MediaBuilder/scripts/**

### Backup zu und Recovery aus dem Cloud Storage

Das Skript sichert eine Maschine in den Cloud Storage oder stellt die Maschine aus dem jüngsten (neuesten) Backup wieder her, welches von diesem Skript im Cloud Storage erstellt wurde. Das Skript fordert den Benutzer beim Starten auf, zwischen Backup oder Recovery zu wählen, und startet dann die Benutzeroberfläche.

Spezifizieren Sie im Bootable Media Builder folgende Skript-Parameter:

1. Die Anmeldedaten (Benutzername, Kennwort) für den Cloud Storage.
2. [Optional] Ein Kennwort, welches das Skript verwendet, um die Backups zu verschlüsseln oder auf diese zuzugreifen.

### Backup zu und Recovery von einem Boot-Medium

Das Skript sichert eine Maschine zu einem Boot-Medium oder stellt die Maschine aus dem jüngsten (neuesten) Backup wieder her, welches von diesem Skript auf demselben Medium erstellt wurde. Das Skript fordert den Benutzer beim Starten auf, zwischen Backup oder Recovery zu wählen, und startet dann die Benutzeroberfläche.

Sie können im Bootable Media Builder ein Kennwort spezifizieren, welches das Skript verwendet, um die Backups zu verschlüsseln oder auf diese zuzugreifen.

### Backup zu und Recovery von einer Netzwerkfreigabe

Das Skript sichert eine Maschine zu einer Netzwerkfreigabe oder stellt die Maschine aus dem jüngsten (neuesten) Backup wieder her, welches sich in einer Netzwerkfreigabe befindet. Das Skript fordert den Benutzer beim Starten auf, zwischen Backup oder Recovery zu wählen, und startet dann die Benutzeroberfläche.

Spezifizieren Sie im Bootable Media Builder folgende Skript-Parameter:

1. Den Netzwerkfreigabepfad.
2. Die Anmeldedaten (Benutzername, Kennwort) für die Netzwerkfreigabe.
3. [Optional] Den Backup-Dateinamen. Der Standardwert ist **AutoBackup**. Wenn Sie möchten, dass das Skript die Backups an ein bereits vorhandenes Backup anhängt oder ein Backup mit einem

„nicht-standardmäßigen“ Namen wiederherstellt, müssen Sie den Standardwert gegen den gewünschten Dateinamen dieses Backups austauschen.

**So ermitteln Sie den Backup-Dateinamen**

a. Gehen Sie in der Cyber Protect Webkonsole zum Bereich **Backup Storage** –> **Speicherorte**.

b. Wählen Sie die Netzwerkfreigabe aus (klicken Sie auf **Speicherort hinzufügen**, wenn die Freigabe noch nicht aufgeführt ist).

c. Wählen Sie das Backup.

d. Klicken Sie auf **Details**. Der Dateiname wird unter **Backup-Dateiname** angezeigt.

4. [Optional] Ein Kennwort, welches das Skript verwendet, um die Backups zu verschlüsseln oder auf diese zuzugreifen.

### Aus dem Cloud Storage wiederherstellen

Das Skript wird die Maschine aus dem jüngsten (neuesten) Backup im Cloud Storage wiederherstellen. Das Skript wird beim Start folgende Angaben vom Benutzer abfragen:

1. Die Anmeldedaten (Benutzername, Kennwort) für den Cloud Storage.
2. Das Kennwort, falls das Backup verschlüsselt wurde.

Wir empfehlen, dass Sie nur die Backups einer einzigen Maschine unter diesem Cloud Storage-Konto speichern. Falls nämlich das Backup einer anderen Maschine vorliegt und dieses neuer als das Backup der aktuellen Maschine ist, wird das Skript dieses (neuere) Backup der anderen Maschine verwenden.

## Benutzerdefinierte Skripts

**Wichtig**
Um benutzerdefinierte Skripte erstellen zu können, müssen Sie sich mit der Befehlssprache Bash und JSON (JavaScript Object Notation) auskennen. Falls Sie mit Bash nicht vertraut sind, ist 'http://www.tldp.org/LDP/abs/html' eine gute Adresse für den Einstieg. Die Spezifikationen für JSON finden Sie unter der Adresse 'http://www.json.org'.

### Die Dateien eines Skripts

Ihr Skript muss sich auf der Maschine, auf welcher der Bootable Media Builder installiert ist, in folgenden Verzeichnissen befinden:

- Unter Windows: %**ProgramData%\Acronis\MediaBuilder\scripts**
- Unter Linux: **/var/lib/Acronis/MediaBuilder/scripts/**

Ein Skript muss aus mindestens drei Dateien bestehen:

- **<Skriptdatei>.sh** – eine Datei mit Ihrem Bash-Skript. Verwenden Sie beim Erstellen des Skripts nur einen begrenzten Satz von Shell-Befehlen, wie er unter der Adresse 'https://busybox.net/downloads/BusyBox.html' aufgeführt ist. Es können außerdem noch

folgende Befehle verwendet werden:

- `acrocmd` – das Befehlszeilenwerkzeug für Backup und Recovery
- `product` – der Befehl, mit dem die Benutzeroberfläche des Boot-Mediums gestartet wird

Diese Datei und alle weiteren Dateien, die das Skript einschließt (beispielsweise durch Verwendung des Befehls 'dot'), müssen im Unterordner **bin** gespeichert sein. Spezifizieren Sie die Pfade der weiteren Dateien im Skript in folgender Form: **/ConfigurationFiles/bin/<irgendeine_Datei>**.

- **autostart** – eine Datei zum Starten von **<Skriptdatei>.sh**. Die Dateiinhalte müssen folgendermaßen aussehen:

```
#!/bin/sh
. /ConfigurationFiles/bin/variables.sh
. /ConfigurationFiles/bin/<script_file>.sh
. /ConfigurationFiles/bin/post_actions.sh
```

- **autostart.json** – eine JSON-Datei mit folgenden Inhalten:
  - Der/die im Bootable Media Builder anzuzeigende Skript-Name/-Beschreibung.
  - Die Namen der Skript-Variablen, die über den Bootable Media Builder konfiguriert werden sollen.
  - Die Parameter der Steuerlemente, die im Bootable Media Builder für jede Variable angezeigt werden.

### Die Struktur von 'autostart.json'

## Top-Level-Objekt

| Paar | | Erforderlich | Beschreibung |
|---|---|---|---|
| **Name** | **Wertetyp** | | |
| `displayName` | Zeichenfolge | Ja | Der im Bootable Media Builder anzuzeigende Skriptname. |
| `description` | Zeichenfolge | Nein | Die im Bootable Media Builder anzuzeigende Skriptbeschreibung. |
| `timeout` | Zahl | Nein | Eine Zeitverzögerung (in Sekunden) für das Boot-Menü, bevor das Skript gestartet wird. Falls das Paar nicht spezifiziert ist, gilt eine Zeitverzögerung von 10 Sekunden. |
| `variables` | Objekt | Nein | Jede Variable für **<Skriptdatei>.sh**, die Sie über den Bootable Media Builder konfigurieren wollen.<br><br>Der Wert sollte ein Satz der folgenden Paare sein: der String-Identifier einer Variable und das Objekt der Variablen (vergl. untere Tabelle). |

## Variablenobjekt

| Paar | | Erforderlich | Beschreibung |
|---|---|---|---|
| **Name** | **Wertetyp** | | |
| `displayName` | Zeichenfolge | Ja | Der in **<Skriptdatei>.sh** verwendete Variablenname. |
| `type` | Zeichenfolge | Ja | Der Typ eines Steuerelements, welches im Bootable Media Builder angezeigt wird. Dieses Steuerelement wird verwendet, um den Variablenwert zu konfigurieren.<br>Eine Auflistung aller unterstützten Typen finden Sie in der unteren Tabelle. |
| `description` | Zeichenfolge | Ja | Die Steuerelementbezeichnung, die im Bootable Media Builder über dem Steuerungselement angezeigt wird. |
| `default` | eine Zeichenfolge (String), falls `type` Folgendes ist: `string`, `multiString`, `password` oder `enum`<br>eine Zahl, falls `type` Folgendes ist: `number`, `spinner` oder `checkbox` | Nein | Der Standardwert für das Steuerelement. Falls das Paar nicht spezifiziert ist, wird der Standardwert ein leerer String oder eine Null sein (abhängig vom Steuerelementtyp).<br>Der Standardwert für ein Kontrollkästchen kann `0` (deaktivierter/abgewählter Zustand) oder `1` sein (aktivierter/ausgewählter Zustand). |
| `order` | Zahl<br>(nicht negativ) | Ja | Die Reihenfolge der Steuerelemente im Bootable Media Builder. Je höher der Wert ist, umso tiefer wird das Steuerelement relativ zu anderen in **autostart.json** definierten Steuerelementen platziert. Der Anfangswert muss `0` sein. |
| `min`<br>(nur für `spinner`) | Zahl | Nein | Der kleinste Wert für das Drehsteuerelement in einem Drehfeld. Falls das Paar nicht spezifiziert ist, wird der Wert auf `0` gesetzt. |
| `max`<br>(nur für `spinner`) | Zahl | Nein | Der größte Wert für das Drehsteuerelement in einem Drehfeld. Falls das Paar nicht spezifiziert ist, wird der Wert auf `100` gesetzt. |

| | | | |
|---|---|---|---|
| `step`<br>(nur für `spinner`) | Zahl | Nein | Der Schrittwert (Inkrement) für das Drehsteuerelement in einem Drehfeld. Falls das Paar nicht spezifiziert ist, wird der Wert auf `1` gesetzt. |
| `items`<br>(nur für `enum`) | Array von Strings | Ja | Eine Folge von Werten für ein Listenfeld (Drop-down-Liste). |
| `required`<br>(für `string`, `multiString`, `password` und `enum`) | Zahl | Nein | Spezifiziert, ob der Steuerelementwert leer sein darf (`0`) oder nicht (`1`). Falls das Paar nicht spezifiziert ist, kann der Steuerelementwert leer sein. |

## Steuerelementtyp

| Name | Beschreibung |
|---|---|
| `string` | Ein einzeiliges, nicht weiter beschränktes Textfeld, welches zur Eingabe oder Bearbeitung kurzer Zeichenfolgen (Strings) verwendet wird. |
| `multiString` | Ein mehrzeiliges, nicht weiter beschränktes Textfeld, welches zur Eingabe oder Bearbeitung längerer Zeichenfolgen (Strings) verwendet wird. |
| `password` | Ein einzeiliges, nicht weiter beschränktes Textfeld, welches zur sicheren Eingabe von Kennwörtern verwendet wird. |
| `number` | Ein einzeiliges, nur Zahlen zulassendes Textfeld, welches zur Eingabe oder Bearbeitung von Nummern verwendet wird. |
| `spinner` | Ein einzeiliges, nur Zahlen zulassendes Textfeld, welches zur Eingabe oder Bearbeitung von Nummern mit einem Drehsteuerelement verwendet wird. Wird auch Drehfeld genannt. |
| `enum` | Ein Standardlistenfeld (Drop-Down-Liste), mit einem festen Satz von vordefinierten Werten. |
| `checkbox` | Ein Kontrollkästchen mit zwei Zuständen – deaktiviert (abgewählt) oder aktiviert (ausgewählt). |

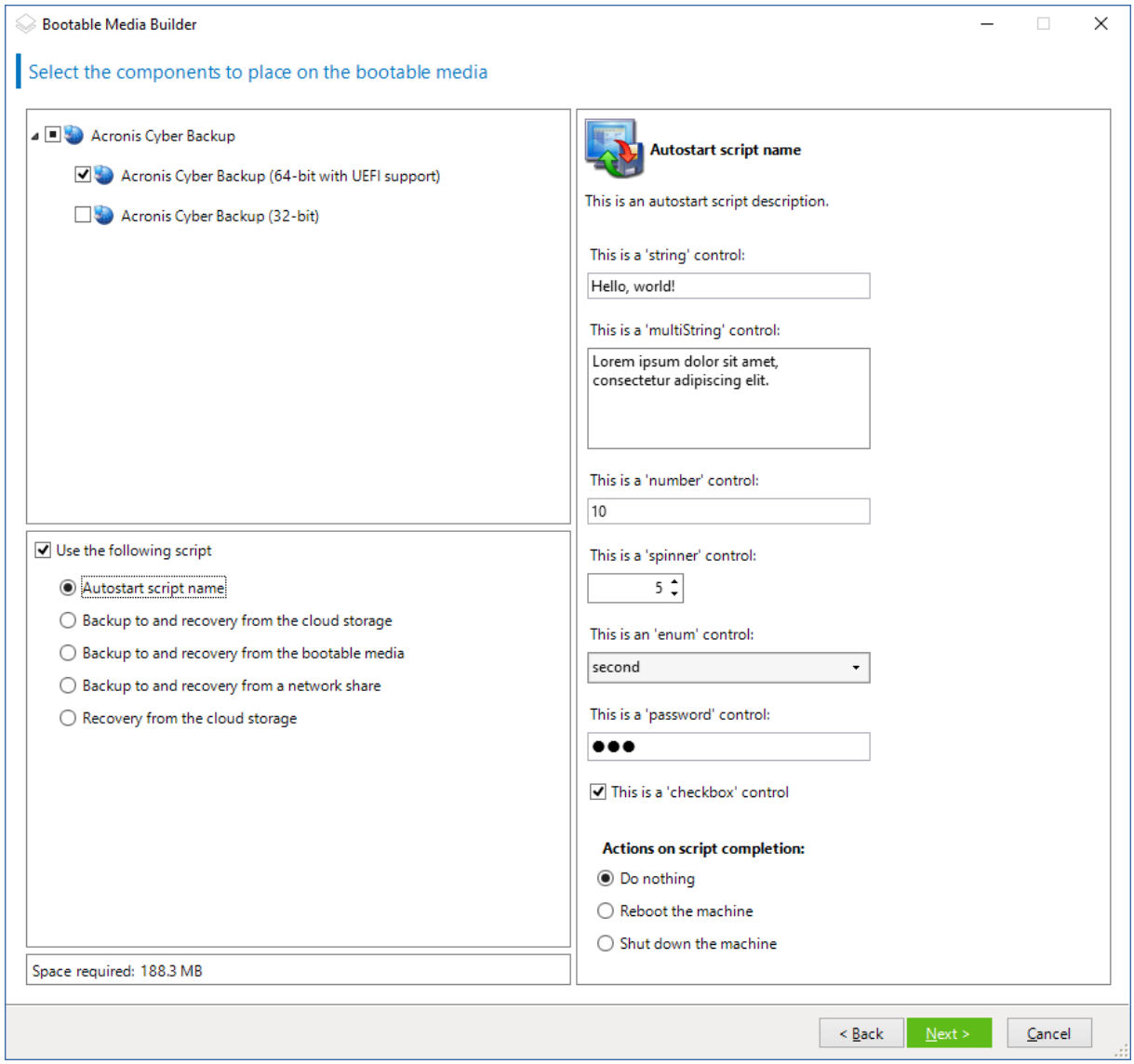
Die untere **autostart.json**-Beispielsdatei enthält alle verwendbaren Typen von Steuerelementen, die zur Konfiguration von Variablen für die Datei **<script_file>.sh** verwendet werden können.

```
{
        "displayName": "Autostart script name",
        "description": "This is an autostart script description.",
        "variables": {
```

```
        "var_string": {
                "displayName": "VAR_STRING",
                "type": "string", "order": 1,
                "description": "This is a 'string' control:", "default": "Hello,
world!"
        },
        "var_multistring": {
                "displayName": "VAR_MULTISTRING",
                "type": "multiString", "order": 2,
                "description": "This is a 'multiString' control:",
                "default": "Lorem ipsum dolor sit amet,\nconsectetur adipiscing elit."
        },
        "var_number": {
                "displayName": "VAR_NUMBER",
                "type": "number", "order": 3,
                "description": "This is a 'number' control:", "default": 10
        },
        "var_spinner": {
                "displayName": "VAR_SPINNER",
                "type": "spinner", "order": 4,
                "description": "This is a 'spinner' control:",
                "min": 1, "max": 10, "step": 1, "default": 5
        },
        "var_enum": {
                "displayName": "VAR_ENUM",
                "type": "enum", "order": 5,
                "description": "This is an 'enum' control:",
                "items": ["first", "second", "third"], "default": "second"
        },
        "var_password": {
                "displayName": "VAR_PASSWORD",
```

```
                "type": "password", "order": 6,
                "description": "This is a 'password' control:", "default": "qwe"
            },
            "var_checkbox": {
                "displayName": "VAR_CHECKBOX",
                "type": "checkbox", "order": 7,
                "description": "This is a 'checkbox' control", "default": 1
            }
        }
}
```

Und so sieht es im Bootable Media Builder aus.



## Management Server

Wenn Sie ein Boot-Medium erstellen, können Sie über eine Option vorkonfigurieren, ob ein Medium auf dem Management Server registriert werden soll.

Durch Registrierung des Mediums können Sie dieses direkt über die Cyber Protect Webkonsole verwalten – genauso, als wäre es eine normale registrierte Maschine. Neben der Bequemlichkeit eines Remote-Zugriffs erhält ein Administrator dadurch die Möglichkeit, alle unter dem Boot-Medium durchgeführten Aktionen zu verfolgen. Die Aktionen werden unter **Aktivitäten** protokolliert, sodass eingesehen werden kann, wer/wann eine Aktion gestartet hat/wurde.

Wurde die Registrierung nicht vorkonfiguriert, so das Medium auch noch registriert werden, wenn damit eine Maschine gebootet wird.

***So können Sie die Registrierung auf dem Management Server vorkonfigurieren***

1. Aktivieren Sie das Kontrollkästchen **Medium auf dem Management Server registrieren**.
2. Spezifizieren Sie im Feld **Server-Name oder IP** den Host-Namen oder die IP-Adresse derjenigen Maschine, auf welcher der Management Server installiert wurde. Sie können eins der folgenden Formate wählen:
   - `http://<server>`. Beispielsweise `http://10.250.10.10` oder `http://server1`
   - `<IP-Adresse>`. Beispielsweise `10.250.10.10`
   - `<Host-Name>`. Beispielsweise `server1` oder `server1.beispiel.com`
3. Spezifizieren Sie bei **Port** den Port, der zum Zugriff auf den Management Server verwendet werden soll. Der Standardwert ist 9877.
4. Spezifizieren Sie bei **Anzeigename**, mit dem diese Maschine in der Cyber Protect Webkonsole angezeigt werden soll. Wenn Sie das Feld frei lassen, wird der Anzeigename folgendermaßen eingestellt:
   - Falls die Maschine schon früher einmal auf dem Management Server registriert wurde, wird sie denselben Namen erhalten.
   - Ansonsten wird entweder der vollqualifizierte Domain-Name (FQDN) oder die IP-Adresse der Maschine verwendet.
5. Bestimmen Sie, mit welchem Konto das Medium auf dem Management Server registriert werden soll. Folgende Optionen sind verfügbar:
   - **Benutzername und Kennwort beim Booten abfragen**

     Die Anmeldedaten müssen jedes Mal eingegeben werden, wenn eine Maschine mit dem Medium gebootet wird.

     Für eine erfolgreiche Registrierung muss das Konto zur Liste der Management Server-Administratoren gehören (**Einstellungen** –> **Konten**). Das Medium wird in der Cyber Protect Webkonsole unter der Organisation oder einer bestimmten Abteilung verfügbar sein – in Abhängigkeit von den Berechtigungen, die dem spezifizierten Konto zugewiesen wurden.

Die Anmeldedaten können auch über die Benutzeroberfläche des Boot-Mediums geändert werden. Klicken Sie dazu auf **Extras** –> **Medium auf dem Management Server registrieren**.

- **Für folgendes Konto registrieren**

  Die Maschine wird jedes Mal automatisch registriert, wenn Sie mit dem Medium gebootet wird.

  Das spezifizierte Konto muss zur Liste der Management Server-Administratoren gehören (**Einstellungen** –> **Konten**). Das Medium wird in der Cyber Protect Webkonsole unter der Organisation oder einer bestimmten Abteilung verfügbar sein – in Abhängigkeit von den Berechtigungen, die dem spezifizierten Konto zugewiesen wurden.

  Die Registrierungsparameter können *nicht* über die Benutzeroberfläche des Boot-Mediums geändert werden.

## Netzwerkeinstellungen

Sie erhalten während der Erstellung eines Boot-Mediums die Möglichkeit, die Netzwerkverbindungen vorzukonfigurieren, die vom bootfähigen Agenten verwendet werden. Die folgenden Parameter können vorkonfiguriert werden:

- IP-Adresse
- Subnetzmaske
- Gateway
- DNS-Server
- WINS-Server

Sobald der bootfähige Agent auf einer Maschine gestartet ist, wird die Konfiguration auf die Netzwerkkarte (NIC) der Maschine angewendet. Wenn die Einstellungen nicht vorkonfiguriert wurden, benutzt der Agent eine DHCP-Autokonfiguration. Sie haben außerdem die Möglichkeit, die Netzwerkeinstellungen manuell vorzunehmen, sobald der bootfähige Agent auf der Maschine läuft.

### Mehrfache Netzwerkverbindungen vorkonfigurieren

Sie können die TCP/IP-Einstellungen für bis zu zehn Netzwerkkarten vorkonfigurieren. Um sicherzustellen, dass jede Netzwerkkarte die passenden Einstellungen bekommt, sollten Sie das Medium auf dem Server erstellen, für den das Medium konfiguriert wird. Wenn Sie eine existierende NIC im Assistentenfenster anwählen, werden ihre Einstellungen zur Speicherung auf das Medium übernommen. Die MAC-Adresse jeder existierenden NIC wird ebenso auf dem Medium gespeichert.

Sie können die Einstellungen ändern, mit Ausnahme der MAC-Adresse; oder Einstellungen für nicht existierende NICs konfigurieren, falls das nötig ist.

Sobald der bootfähige Agent auf dem Server gestartet ist, fragt er die Liste der verfügbaren NICs ab. Diese Liste ist nach den Steckplätzen sortiert, die von den NICs belegt werden. An der Spitze stehen die, die dem Prozessor am nächsten liegen.

Der bootfähige Agent teilt jeder bekannten NIC die passenden Einstellungen zu, wobei die NICs anhand ihrer MAC-Adressen identifiziert werden. Nachdem die NICs mit bekannten MAC-Adressen konfiguriert wurden, bekommen die verbliebenen NICs (beginnend mit der untersten in der Liste) die Einstellungen zugewiesen, die Sie für unbekannte NICs vorkonfiguriert haben.

Sie können bootfähige Medien für jede beliebige Maschine konfigurieren – und nicht nur für die Maschine, auf der das Medium erstellt wurde. Um dies durchzuführen, konfigurieren Sie die NICs entsprechend ihrer Steckplatzreihenfolge in der betreffenden Maschine. NIC1 besetzt den zum Prozessor am nächsten liegenden Steckplatz, NIC2 wiederum den folgenden und so weiter. Wenn der bootfähige Agent auf der Maschine startet, wird er keine NICs mit bekannter MAC-Adresse finden und daher die NICs in der von Ihnen bestimmten Reihenfolge konfigurieren.

**Beispiel**

Der bootfähige Agent könnte einen der Netzwerkadapter zur Kommunikation mit der Management Konsole innerhalb des Produktionsnetzwerks nutzen. Für diese Verbindung könnte eine automatische Konfiguration durchgeführt werden. Größere Datenmengen für eine Wiederherstellung könnten über die zweite NIC übertragen werden, die in das dafür bestimmte Backup-Netzwerk mithilfe statischer TCP/IP-Einstellungen eingebunden ist.

## Netzwerk-Port

Wenn Sie ein Boot-Medium erstellen, können Sie den Netzwerk-Port vorkonfigurieren, den der bootfähige Agent nach eingehenden Verbindungen vom Utility `acrocmd` überwacht. Es besteht die Wahl zwischen:

- dem Standard-Port
- dem aktuell verwendeten Port
- einem neuen Port (geben Sie die Port-Nummer ein)

Sofern kein Port vorkonfiguriert wurde, verwendet der Agent die Standard-Port-Nummer 9876.

## Treiber für Universal Restore

Während der Erstellung des Boot-Mediums haben Sie die Möglichkeit, dem Medium bestimmte Windows-Treiber hinzuzufügen. Diese Treiber werden von Universal Restore verwendet, um ein Windows-System, das auf eine abweichenden Hardware migriert wurde, booten zu können.

Sie können Universal Restore konfigurieren:

- um das Medium nach Treibern zu durchsuchen, die für die Ziel-Hardware am geeignetsten sind
- um die Massenspeichertreiber einzubinden, die Sie ausdrücklich vom Medium aus spezifizieren. Dies ist notwendig, wenn die Ziel-Hardware einen besonderen Massenspeicher-Controller für Festplatten und ähnliche Laufwerke verwendet (wie SCSI-, RAID- oder Fibre Channel-Adapter).

Die Treiber werden im dem sichtbaren Treiber-Ordner auf dem bootfähigen Medium hinterlegt. Da die Treiber nicht in den Arbeitsspeicher der Zielmaschine geladen werden, muss das betreffende Medium während der ganzen Universal Restore-Aktion eingelegt bzw. angeschlossen bleiben.

Einem bootfähigen Medium können Sie Treiber hinzufügen, wenn Sie ein Wechselmedium (bzw. dessen ISO-Abbild) oder ein entfernbares Medium (z. B. einen USB-Stick) erstellen. Treiber können nicht auf WDS/RIS hochgeladen werden.

Die Treiber können nur in Gruppen zu der Liste hinzugefügt werden – und zwar, indem die INF-Dateien oder -Ordner hinzugefügt werden, die solche Dateien enthalten. Die Wahl einzelner Treiber aus den INF-Dateien ist nicht möglich; der Media Builder informiert Sie jedoch über den Inhalt der Dateien.

***So fügen Sie Treiber hinzu:***

1. Klicken Sie auf **Hinzufügen** und wählen Sie dann die INF-Datei oder einen Ordner, der die gewünschten INF-Dateien enthält.
2. Wählen Sie die INF-Datei oder den betreffenden Ordner aus.
3. Klicken Sie auf **OK**.

Die Treiber können nur in Gruppen aus der Liste entfernt werden – und zwar durch Löschen der INF-Dateien.

***So entfernen Sie Treiber:***

1. Wählen Sie die INF-Datei aus.
2. Klicken Sie auf **Entfernen**.

## WinPE-basierte Boot-Medien

Der Bootable Media Builder ermöglicht zwei Methoden, um Acronis Cyber Protect in WinPE einzubinden:

- Erstellen Sie ein komplett neues PE-ISO-Image, in welches Sie das Plug-in integrieren.
- Fügen Sie das Acronis-Plug-in einer WIM-Datei zur späteren Verwendung hinzu (manuelle ISO-Erstellung, dem Image noch andere Tools hinzufügen usw.).

Sie können WinRE-basierte PE-Images ohne zusätzliche Vorbereitung erstellen – oder die PE-Images nach der Installation des Windows Automated Installation Kits (AIK) oder des Windows Assessment and Deployment Kits (ADK) erstellen.

### WinRE-basierte PE-Images

Die Erstellung von WinRE-basierten Images wird für folgende Betriebssysteme unterstützt:

- Windows 7 (64 Bit)
- Windows 8, 8.1, 10 (32 Bit und 64 Bit)
- Windows Server 2012, 2016, 2019 (64 Bit)

## PE-Images

Nach der Installation des Windows Automated Installation Kits (AIK) oder Windows Assessment and Deployment Kits (ADK) unterstützt der Bootable Media Builder solche WinPE-Distributionen, die auf einem der folgenden Kernel basieren:

- Windows Vista (PE 2.0)
- Windows Vista SP1 und Windows Server 2008 (PE 2.1).
- Windows 7 (PE 3.0), mit oder ohne das 'Supplement for Windows 7 SP1' (PE 3.1)
- Windows 8 (PE 4.0)
- Windows 8.1 (PE 5.0)
- Windows 10 (PE für Windows 10)

Bootable Media Builder unterstützt sowohl 32-Bit- wie auch 64-Bit-WinPE-Distributionen. Die 32-Bit-WinPE-Distributionen funktionieren auch auf 64-Bit-Hardware. Sie benötigen jedoch 64-Distributionen, um von einer Maschine booten zu können, die UEFI (Unified Extensible Firmware Interface) verwendet.

PE-Images, die auf WinPE 4 (und höher) basieren, benötigen zum Arbeiten ca. 1 GB RAM.

**Hinweis**
Die Funktionalität zur Laufwerksverwaltung ist bei Boot-Medien, die auf Windows PE 4.0 und höher basieren, nicht verfügbar. Die Laufwerksverwaltung wird daher für Windows 7 und frühere Betriebssysteme unterstützt. Um Laufwerksverwaltungsaktionen unter Windows 8 und höher durchführen zu können, müssen Sie den Acronis Disk Director installieren. Weitere Informationen finden Sie in diesem Knowledge Base-Artikel: https://kb.acronis.com/de/content/47031.

## Vorbereitung: WinPE 2.x und 3.x

Um PE 2.x oder 3.x-Images erstellen oder modifizieren zu können, installieren Sie den Bootable Media Builder auf einer Maschine, auf der das Windows Automated Installation Kit (WAIK) installiert ist. Wenn Sie keine Maschine mit AIK haben, gehen Sie wie nachfolgend beschrieben vor.

***So bereiten Sie eine Maschine mit AIK vor***

1. Download und Installation des Windows Automated Installation Kit.
   Automated Installation Kit (AIK) für Windows Vista (PE 2.0):
   http://www.microsoft.com/Downloads/details.aspx?displaylang=de&FamilyID=c7d4bc6d-15f3-4284-9123-679830d629f2
   Automated Installation Kit (AIK) für Windows Vista SP1 und Windows Server 2008 (PE 2.1):
   http://www.microsoft.com/Downloads/details.aspx?familyid=94BB6E34-D890-4932-81A5-5B50C657DE08&displaylang=de
   Automated Installation Kit (AIK) für Windows 7 (PE 3.0):

http://www.microsoft.com/downloads/de-de/details.aspx?FamilyID=696DD665-9F76-4177-A811-39C26D3B3B34

Automated Installation Kit (AIK) Supplement for Windows 7 SP1 (PE 3.1):
http://www.microsoft.com/de-de/download/details.aspx?id=5188

Die Systemanforderungen für die Installation finden Sie, wenn Sie auf die unteren Links klicken.

2. [Optional] Brennen Sie das WAIK auf DVD oder kopieren Sie es auf ein Flash-Laufwerk (USB-Stick).
3. Installieren Sie Microsoft .NET Framework von diesem Kit (NETFXx86 oder NETFXx64, abhängig von Ihrer Hardware).
4. Installieren Sie Microsoft Core XML (MSXML) 5.0 oder 6.0 Parser von diesem Kit.
5. Installieren Sie Windows AIK von diesem Kit.
6. Installieren Sie Bootable Media Builder auf der gleichen Maschine.

Es ist empfehlenswert, dass Sie sich mit der dem Windows AIK beiliegenden Hilfe-Dokumentation vertraut machen. Um auf die Dokumentation zuzugreifen, wählen Sie **Microsoft Windows AIK –> Dokumentation** im Startmenü.

## Vorbereitung: WinPE 4.0 (und höher)

Um Images von PE 4 (oder höher) erstellen oder ändern zu können, installieren Sie den Bootable Media Builder auf einer Maschine, auf der das 'Windows Assessment and Deployment Kit' (ADK) installiert ist. Wenn Sie keine Maschine mit dem ADK haben, gehen Sie wie nachfolgend beschrieben vor.

***So bereiten Sie eine Maschine mit dem ADK vor***

1. Laden Sie das Installationsprogramm für das 'Assessment and Deployment Kit' herunter.

   Assessment and Deployment Kit (ADK) für Windows 8 (PE 4.0): https://www.microsoft.com/de-DE/download/details.aspx?id=30652.

   Assessment and Deployment Kit (ADK) für Windows 8.1 (PE 5.0): http://www.microsoft.com/de-DE/download/details.aspx?id=39982.

   Assessment and Deployment Kit (ADK) für Windows 10 (PE für Windows 10): https://msdn.microsoft.com/de-de/windows/hardware/dn913721%28v=vs.8.5%29.aspx.

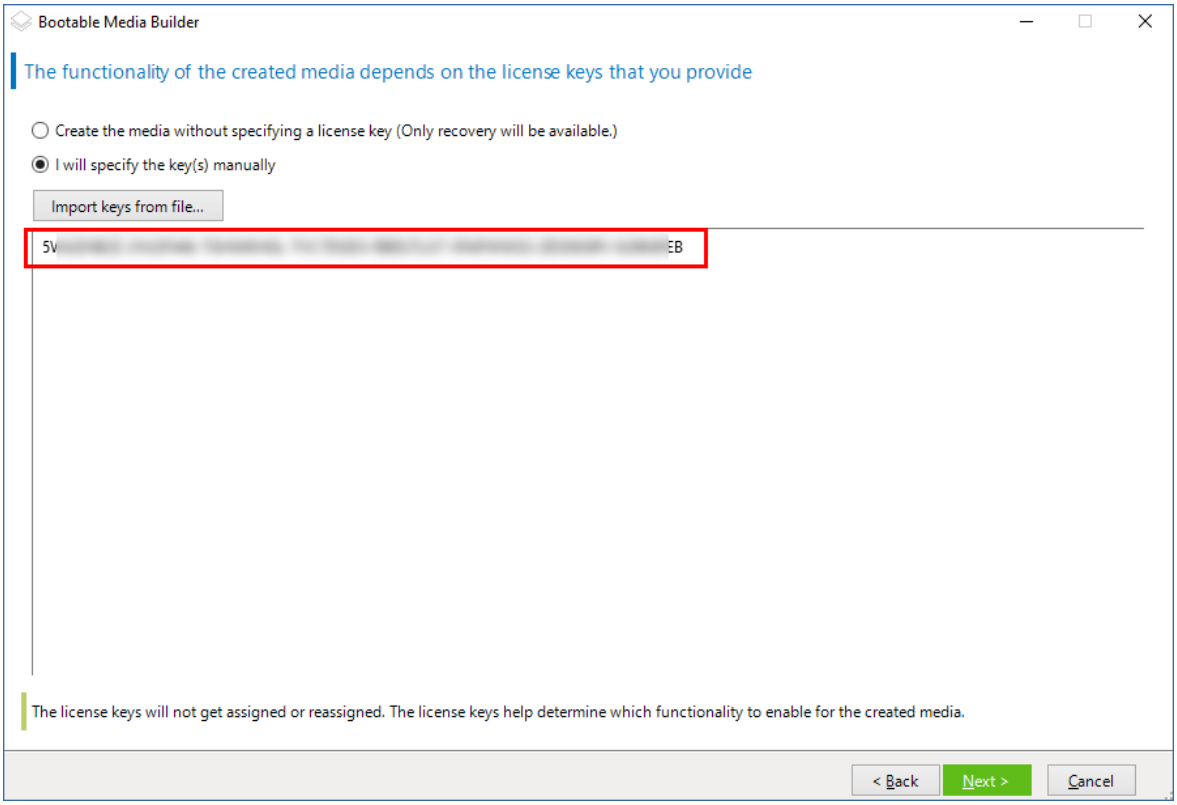
   Die Systemanforderungen für die Installation finden Sie, wenn Sie auf die unteren Links klicken.
2. Installieren Sie das 'Assessment and Deployment Kit' auf der Maschine.
3. Installieren Sie Bootable Media Builder auf der gleichen Maschine.

## Das Acronis Plug-in einem WinPE-Image hinzufügen

***So können Sie das Acronis Plug-in einem WinPE-Image hinzufügen***

1. Starten Sie den Bootable Media Builder.
2. Wenn Sie ein Boot-Medium mit vollem Funktionsumfang erstellen wollen, müssen Sie einen Acronis Cyber Protect Lizenzschlüssel spezifizieren. Dieser Schlüssel wird verwendet, um

festzulegen, welche Funktionen das Boot-Medium enthalten soll. Es werden keine Lizenzen von irgendwelchen Maschinen widerrufen.
Wenn Sie keinen Lizenzschlüssel spezifizieren, kann das resultierende Boot-Medium nur für Wiederherstellungsaktionen verwendet werden.



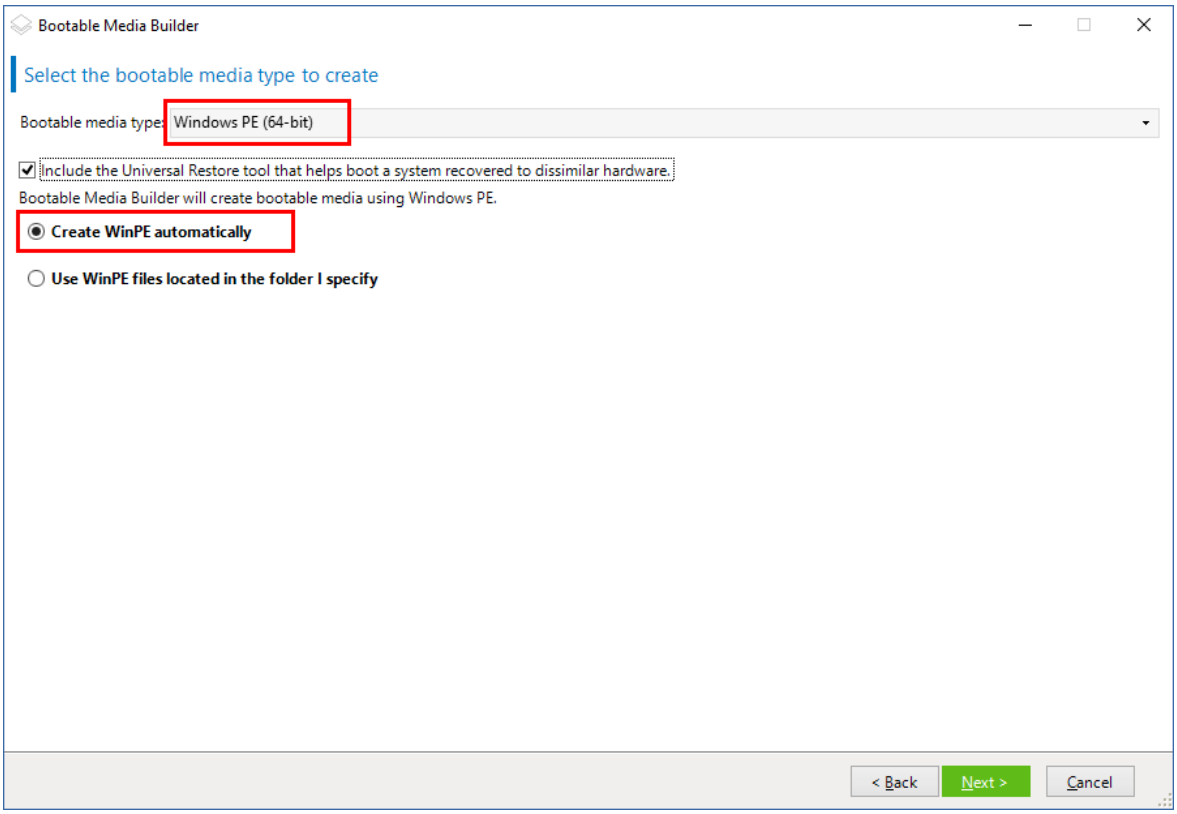

3. Wählen Sie den gewünschten **Typ des Boot-Mediums: Windows PE** oder **Typ des Boot-Mediums: Windows PE (64 Bit)**. Sie benötigen ein 64-Bit-Medium, um eine Maschine booten zu können, die UEFI (Unified Extensible Firmware Interface) verwendet.

   Wenn Sie '**Typ des Boot-Mediums: Windows PE**' gewählt haben, tun Sie zuerst Folgendes:

   - Klicken Sie auf **Plug-in für WinPE (32 Bit) herunterladen**.
   - Speichern Sie das Plug-in im folgenden Ordner: **%PROGRAM_ FILES%\Acronis\BootableComponents\WinPE32**.

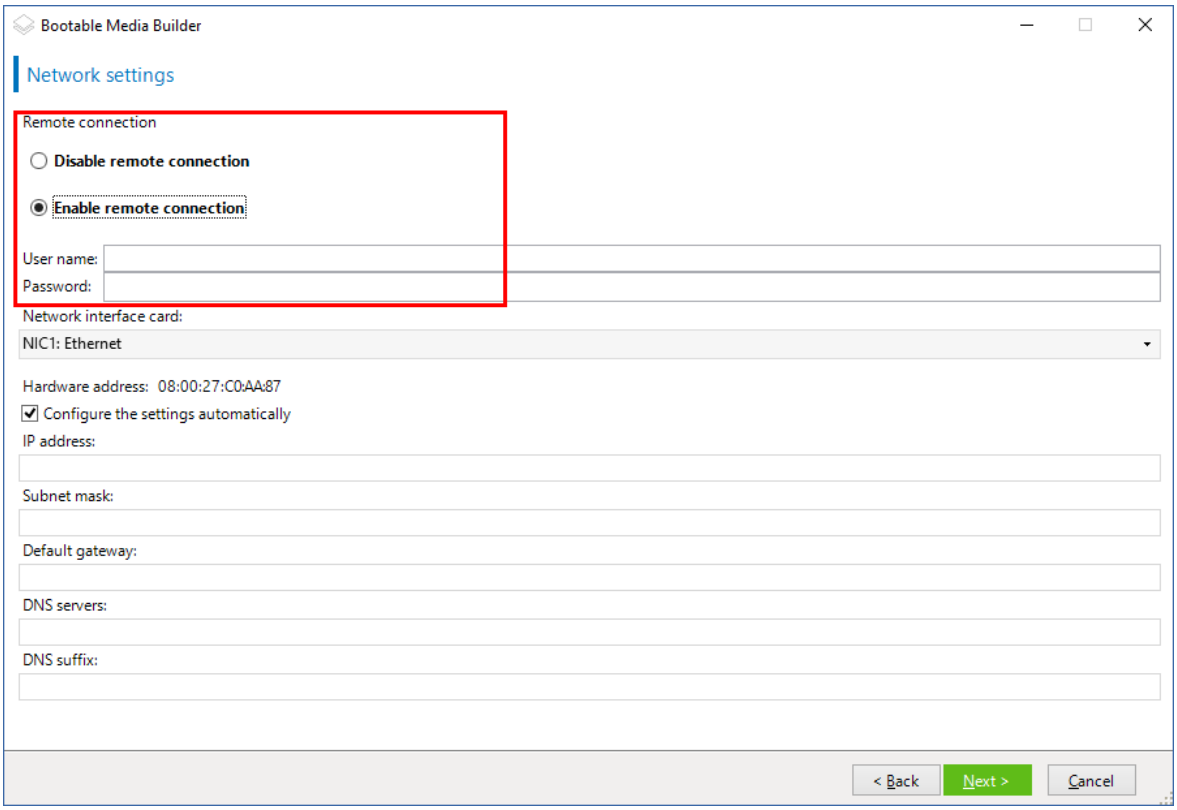
   Falls Sie ein Betriebssystem auch auf abweichender Hardware oder auf einer virtuellen Maschine wiederherstellen wollen und dabei die Bootfähigkeit des Systems gewährleisten wollen, aktivieren Sie das Kontrollkästchen **Das Universal Restore-Tool einschließen...**.
4. Wählen Sie den Befehl **WinPE automatisch erstellen**.

   Die Software führt das passende Skript aus und wechselt dann zum nächsten Fenster.




5. Bestimmen Sie die Sprache, die für das Boot-Medium verwendet werden soll.
6. Wählen Sie, ob Remote-Verbindungen für eine per Boot-Medium gestartete Maschine (de)aktiviert werden sollen. Wenn Sie die Option aktivieren, geben Sie die Anmeldedaten (Benutzername, Kennwort) ein, die per Befehlszeile spezifiziert werden sollen, falls das `acrocmd`-Werkzeug auf einer anderen Maschine ausgeführt wird. Wenn Sie diese Felder leer lassen, wird ist eine Remote-Verbindung über die Befehlszeilenschnittstelle auch ohne Anmeldedaten möglich sein.

   Diese Anmeldedaten werden auch benötigt, wenn Sie das Medium auf dem Management Server über die Cyber Protect Webkonsole registrieren.




7. Spezifizieren Sie die Netzwerkeinstellungen für die Netzwerkadapter der Maschine oder wählen Sie eine Autokonfiguration per DHCP.

**Hinweis**
Die Netzwerkeinstellungen sind nur mit den Lizenzen für Acronis Cyber Protect 15 Advanced und Acronis Cyber Protect 15 Backup Advanced verfügbar. Einen entsprechenden ausführlichen Funktionsvergleich finden Sie in diesem Knowledge Base-Artikel.

8. [Optional] Bestimmen Sie, wie das Medium beim Booten auf dem Management Server registriert werden soll. Zu weiteren Informationen über die Registrierungseinstellungen siehe den Abschnitt 'Management Server'.
9. [Optional] Spezifizieren Sie die Windows-Treiber, die Windows PE hinzugefügt werden sollen.

   Wenn Sie eine Maschine mit Windows PE booten, ermöglichen Ihnen diese Treiber, auf Geräte zuzugreifen, wo sich das Backup befindet. Verwenden Sie 32-Bit-Treiber, sofern Sie eine 32-Bit-WinPE-Distribution verwenden – oder 64-Bit-Treiber, sofern Sie eine 64-Bit-WinPE-Distribution einsetzen.

   Sie können auf die hinzugefügten Treiber auch verweisen, wenn Sie Universal Restore für Windows konfigurieren. Fügen Sie für Universal Restore entweder 32-Bit- oder 64-Bit-Treiber hinzu – in Abhängigkeit davon, ob Sie ein 32-Bit- oder 64-Bit-Betriebssystemvariante von Windows wiederherstellen wollen.

   So fügen Sie Treiber hinzu:

   - Klicken Sie auf **Hinzufügen** und spezifizieren Sie dann den Pfad zu der benötigten . inf-Datei (beispielsweise für einen SCSI-, RAID- oder SATA-Controller, eine Netzwerkkarte, ein

Bandlaufwerk oder ein anderes Gerät).
- Wiederholen Sie dieses Prozedur für jeden Treiber, den Sie in das resultierende WinPE-Medium aufnehmen wollen.

10. Wählen Sie, ob Sie ein ISO- oder WIM-Image erstellen wollen – oder ob das Medium auf einen Server (WDS oder RIS) hochgeladen werden soll.
11. Geben Sie den vollen Pfad (einschließlich Dateiname) zur resultierenden Image-Datei an – oder spezifizieren Sie den Server (inklusive Benutzername und Kennwort, um auf den Server zugreifen zu können).
12. Überprüfen Sie Ihre Einstellungen im Fenster 'Zusammenfassung' und klicken Sie dann auf **Fertig stellen**.
13. Brennen Sie die ISO-Datei auf CD oder DVD (mit dem Brennprogramm eines Drittherstellers) oder bereiten Sie einen bootfähigen USB-Stick vor.

Sobald eine Maschine mit WinPE gebootet wird, werden die Agenten automatisch gestartet.

***So erstellen Sie ein PE-Image (eine ISO-Datei) von der resultierenden WIM-Datei:***

- Überschreiben Sie die vorgegebene Datei 'boot.wim' (im Windows PE-Ordner) mit der neu erstellten .wim-Datei. Geben Sie (für das obere Beispiel) Folgendes ein:

```
copy c:\AcronisMedia.wim c:\winpe_x86\ISO\sources\boot.wim
```

- Verwenden Sie das Tool **Oscdimg**. Geben Sie (für das obere Beispiel) Folgendes ein:

```
oscdimg -n -bc:\winpe_x86\etfsboot.com c:\winpe_x86\ISO c:\winpe_x86\winpe_x86.iso
```

**Warnung!**
(Sie sollten dieses Beispiel nicht kopieren und einfügen. Geben Sie den Befehl stattdessen manuell ein, weil er sonst nicht funktioniert.)

Weitere Informationen zur Anpassung von Windows PE 2.x und 3.x finden Sie im Windows PE-Benutzerhandbuch (Winpe.chm). Informationen zur Anpassung von Windows PE 4.0 (und höher) sind in der Microsoft TechNet-Bibliothek verfügbar.

# Es wird eine Verbindung mit einer Maschine aufgebaut, die per Boot-Medium gestartet wurde

Sobald eine Maschine mithilfe eines Boot-Medium gestartet wurde, erscheint ein Konsolenfenster mit den IP-Adressen, die per DHCP oder als manuell vorkonfigurierte Werte zugewiesen wurden.

## Netzwerkeinstellungen konfigurieren

Klicken Sie zum Ändern der Netzwerkeinstellungen für eine aktuelle Sitzung im Startfenster auf **Netzwerk konfigurieren**. Das erscheinende Fenster **Netzwerkeinstellungen** ermöglicht Ihnen, die Netzwerkeinstellungen für jede Netzwerkkarte (NIC) auf der Maschine zu konfigurieren.

Während einer Sitzung durchgeführte Änderungen gehen nach dem Neustart der Maschine verloren.

### VLANs hinzufügen

Sie können im Fenster **Netzwerkeinstellungen** VLANs (Virtual Local Area Networks, virtuelle lokale Netzwerke) hinzufügen. Verwenden Sie diese Funktionalität, falls Sie auf einen Backup-Speicherort zugreifen müssen, der sich in einem spezifischen VLAN befindet.

VLANs werden hauptsächlich dazu verwendet, um lokale Netzwerke (LANs) in logische Teilnetze zu segmentieren. Eine Netzwerkkarte (NIC), die mit einem *Zugriffs*-Port des Switches verbunden ist, kann immer auf das in der Port-Konfiguration spezifizierte VLAN zugreifen. Eine Netzwerkkarte (NIC), die mit einem *Trunk*-Port des Switches verbunden ist, kann nur dann auf die in der Port-Konfiguration erlaubten VLANs zugreifen, wenn Sie die VLANs in den Netzwerkeinstellungen spezifizieren.

***So ermöglichen Sie den Zugriff auf ein VLAN über einen Trunk-Port***

1. Klicken Sie auf **VLAN hinzufügen**.
2. Wählen Sie die Netzwerkkarte aus, die Zugriff auf dasjenige lokale Netzwerk bereitstellt, welches das benötigte VLAN enthält.
3. Spezifizieren Sie den VLAN-Bezeichner (Identifier).

Nachdem Sie auf **OK** geklickt haben, erscheint in der Liste der Netzwerkkarten ein neuer Eintrag.

Sollten Sie ein VLAN entfernen wollen, dann klicken Sie auf den erforderlichen VLAN-Eintrag – und anschließend auf **VLAN entfernen**.

## Lokale Verbindung

Um direkt auf einer Maschine arbeiten zu können, die mit einem Boot-Medium gestartet wurde, müssen Sie im Startfenster auf **Diese Maschine lokal verwalten** klicken.

## Remote-Verbindung

Um sich remote mit einem Medium verbinden zu können, müssen Sie dieses auf dem Management Server konfigurieren (wie im Abschnitt 'Medien auf dem Management Server registrieren' beschrieben).

# Medien auf dem Management Server registrieren

Durch Registrierung eines Boot-Mediums können Sie dieses direkt über die Cyber Protect Webkonsole verwalten – genauso, als wäre es eine normale registrierte Maschine. Dies gilt für alle Boot-Medien, egal welche Boot-Methode verwendet wird (physische Medien, Startup Recovery Manager, Acronis PXE Server, WDS oder RIS). In macOS erstellte Boot-Medien können jedoch nicht registriert werden.

Eine Registrierung von Boot-Medien ist nur möglich, wenn mindestens eine Acronis Cyber Protect Advanced-Lizenz auf dem Management Server hinzugefügt wurde.

Sie können ein Medium von der Benutzeroberfläche des Boot-Mediums aus registrieren.

Die Registrierungsparameter können in der Option 'Management Server' des Bootable Media Builder vorkonfiguriert werden. Wenn alle Registrierungsparameter vorkonfiguriert wurden, wird das resultierende Medium in der Cyber Protect Webkonsole automatisch angezeigt. Wenn nur einige der Parameter vorkonfiguriert wurden, sind einige Schritte der nachfolgenden Prozeduren möglicherweise nicht verfügbar.

## Das Boot-Medium von seiner eigenen Benutzeroberfläche aus registrieren

Das Medium kann mit dem Bootable Media Builder erstellt oder heruntergeladen werden.

***So registrieren Sie ein Boot-Medium von seiner eigenen Benutzeroberfläche aus***

1. Starten Sie die Maschine mit dem Boot-Medium.
2. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Klicken Sie im Startfenster unter **Management Server** auf **Bearbeiten**.
   - Klicken Sie in der Benutzeroberfläche des Boot-Mediums auf **Extras** –> **Medium auf dem Management Server registrieren**.
3. Spezifizieren Sie bei **Registrieren auf** den Host-Namen oder die IP-Adresse derjenigen Maschine, auf welcher der Management Server installiert ist. Sie können eins der folgenden Formate wählen:
   - `http://<server>`. Beispielsweise `http://10.250.10.10` oder `http://server`
   - `<IP-Adresse>`. Beispielsweise `10.250.10.10`
   - `<Host-Name>`. Beispielsweise `server` oder `server.beispiel.com`
4. Geben Sie bei **Benutzername** und **Kennwort** die Anmeldedaten eines Kontos ein, welches Mitglied der Management Server-Administratoren ist (**Einstellungen** –> **Konten**). Das Medium wird in der Cyber Protect Webkonsole unter der Organisation oder einer bestimmten Abteilung verfügbar sein – in Abhängigkeit von den Berechtigungen, die dem spezifizierten Konto zugewiesen wurden.
5. Spezifizieren Sie bei **Anzeigename**, mit dem diese Maschine in der Cyber Protect Webkonsole angezeigt werden soll. Wenn Sie das Feld frei lassen, wird der Anzeigename folgendermaßen eingestellt:
   - Falls die Maschine schon früher einmal auf dem Management Server registriert wurde, wird sie denselben Namen erhalten.
   - Ansonsten wird entweder der vollqualifizierte Domain-Name (FQDN) oder die IP-Adresse der Maschine verwendet.
6. Klicken Sie auf **OK**.

# Lokale Aktionen mit einem Boot-Medium

Die Aktionen, die Sie mit einem Boot-Medium durchführen können, sind den Backup- und Wiederherstellungsaktionen sehr ähnlich, die Sie unter dem regulären Betriebssystem durchführen können. Die Unterschiede sind wie folgt:

1. Bei einem Boot-Medium mit Windows-typischer Darstellung hat ein Volume denselben Laufwerksbuchstaben wie unter Windows selbst. Volumes, die unter Windows keine Laufwerksbuchstaben haben (wie etwa das Volume 'System-reserviert') bekommen freie Laufwerksbuchstaben in der Reihenfolge ihres Vorkommens auf den Laufwerken zugewiesen.

   Sollte das Boot-Medium kein Windows auf der Maschine erkennen können oder mehrere Windows-Versionen erkennen, dann wird allen Volumes (einschließlich solchen ohne Laufwerksbuchstaben) in der Reihenfolge ihres Vorkommens auf den Laufwerken ein Buchstabe zugewiesen. Daher können die Laufwerksbuchstaben dann von denen unter Windows vorliegenden abweichen. So könnte beispielsweise die Zuordnung des Laufwerks D: unter dem Boot-Medium dem Laufwerk E: entsprechen, welches Windows verwendet.

   **Hinweis**
   Wir empfehlen, dass Sie den Volumes eindeutige Namen zuweisen.

2. Ein Boot-Medium mit Linux-typische Darstellung zeigt lokale Laufwerke und Volumes als 'unmounted' an (sda1, sda2...).
3. Mit einem Boot-Medium erstellte Backups werden mit einer vereinfachten Dateibenennung gekennzeichnet. Backups erhalten nur dann Standardnamen, wenn diese einem bereits existierenden Archiv, welches einen Standarddateinamen verwendet, hinzugefügt werden – oder falls der Zielort keine vereinfachte Dateibenennung unterstützt.
4. Ein Boot-Medium mit Linux-typischer Volume-Darstellung kann keine Backups auf NTFS-formatierte Volumes schreiben. Wechseln Sie bei Bedarf zu einem Medium mit Windows-typischer Volume-Darstellung. Wenn Sie die Volume-Darstellung des Boot-Mediums umschalten wollen, klicken Sie auf **Extras** –> **Volume-Darstellung ändern**.
5. Tasks können nicht per Planung gestartet werden. Wenn Sie eine Aktion wiederholen wollen, müssen Sie diese ganz neu konfigurieren.
6. Der Speicherzeitraum für Ereignisse (Logs) ist auf die aktuelle Sitzung beschränkt. Sie können die gesamte Ereignisliste oder gefilterte Logs in eine Datei speichern.
7. Zentrale Depots werden im Verzeichnisbaum des Fensters **Archiv** nicht angezeigt.

   Um auf ein verwaltetes Depot zuzugreifen, geben Sie im Feld **Pfad** ein:

   **bsp://knoten_adresse/depot_name/**

   Um auf ein zentrales, nicht verwaltetes Depot zuzugreifen, tragen Sie den vollen Pfad zum Ordner des Depots ein.

   Nach Eingabe der Anmeldedaten sehen Sie eine Liste der Archive, die sich im Depot befinden.

## Einen Anzeigemodus einstellen

Wenn Sie eine Maschine mit einem Linux-basierten Boot-Medium starten, wird der Anzeigemodus basierend auf der vorliegenden Hardware-Konfiguration (Monitor- und Grafikkarten-Spezifikationen) automatisch erkannt. Sollte der Anzeigemodus nicht korrekt erkannt werden, gehen Sie folgendermaßen vor:

1. Drücken Sie im Boot-Menü auf F11.
2. Geben Sie in der Befehlszeile Folgendes ein: **vga=ask**, fahren Sie dann mit dem Boot-Vorgang fort.
3. Wählen Sie aus der Liste der verfügbaren Anzeigemodi den passenden durch Eingabe der entsprechenden Nummer aus (z.B. **318**) und drücken Sie dann die **Eingabetaste**.

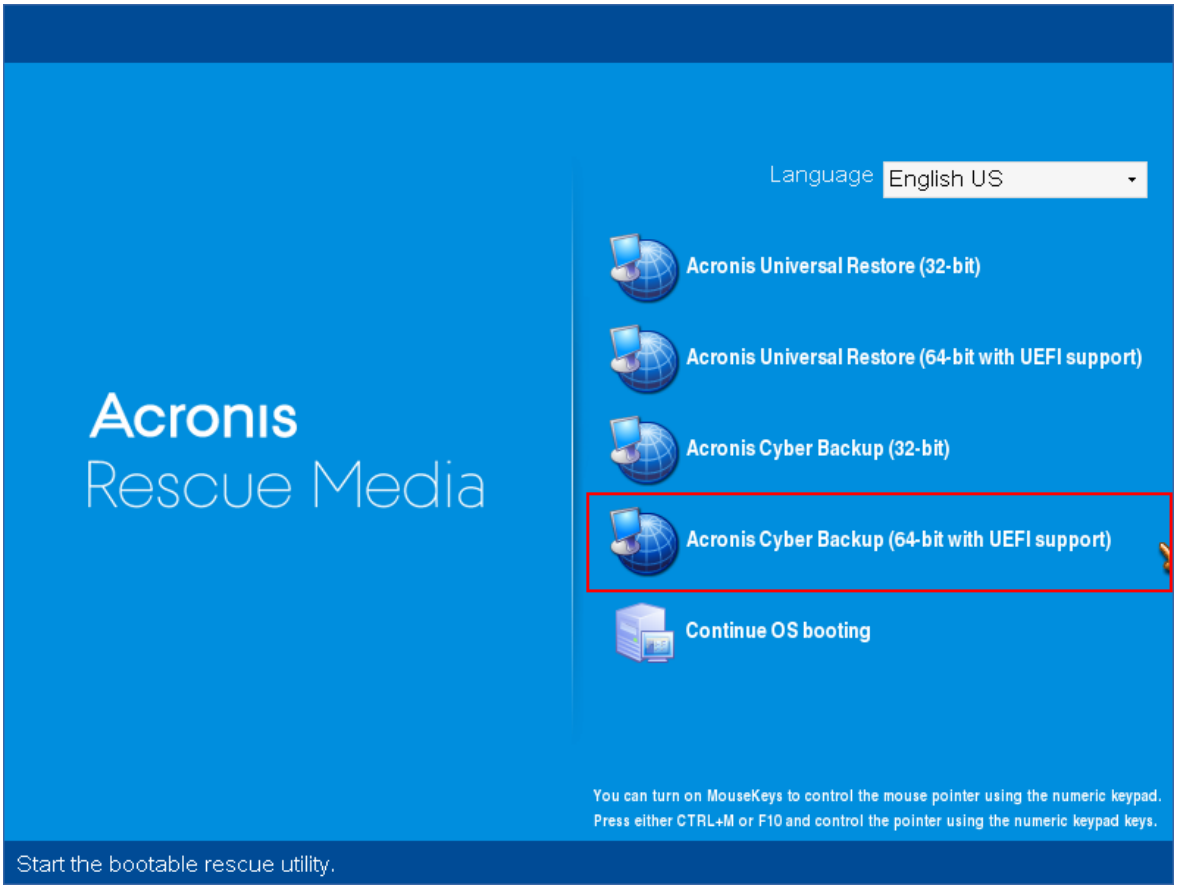
Falls Sie diese Prozedur nicht jedes Mal ausführen wollen, wenn Sie eine bestimmte Hardwarekonfiguration mit einem Boot-Medium starten, erstellen Sie das Medium mit der entsprechenden Modus-Nummer (in unserem Beispiel: **vga=0x318**) neu, indem Sie den Wert im Fenster **Kernel-Parameter** eingeben.

## Backups mit einem Boot-Medium bei einem lokalen System

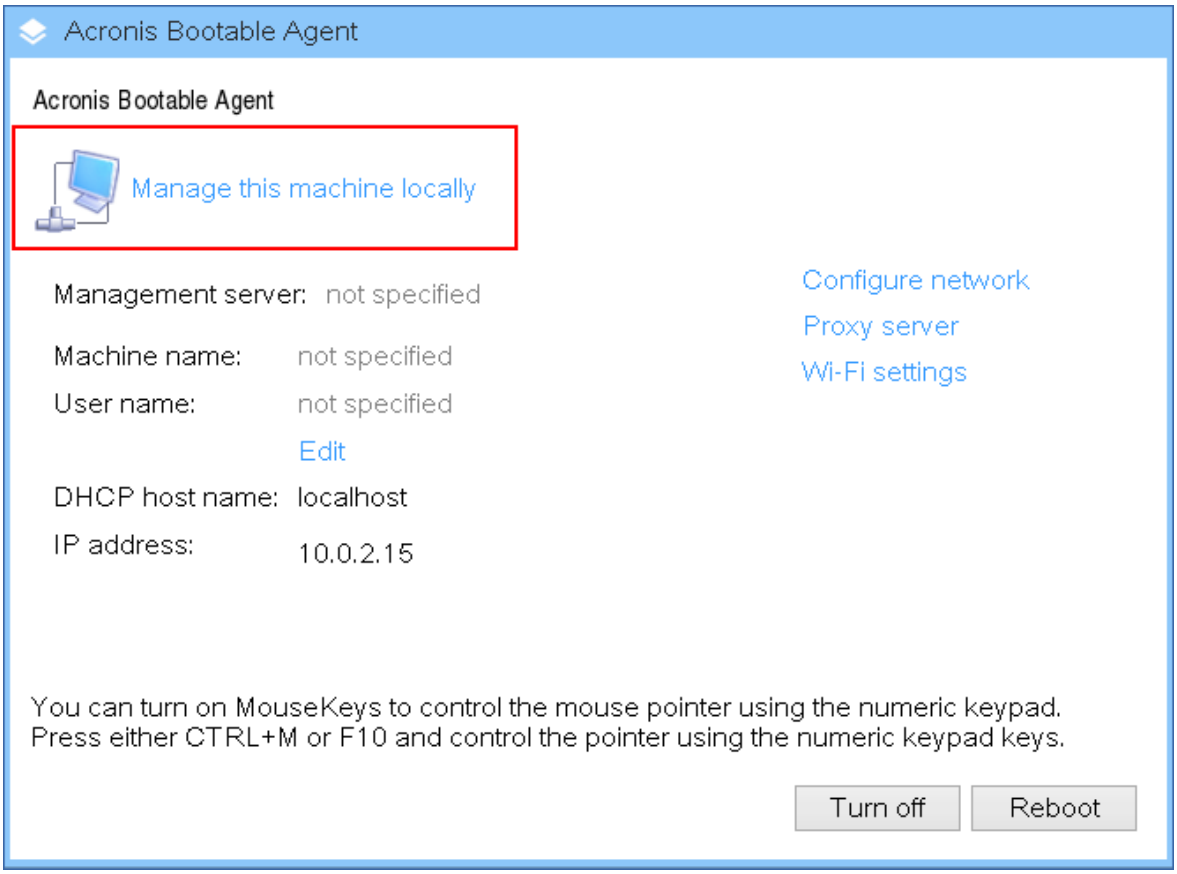
Sie Backups nur mit einem Boot-Medium erstellen, das Sie mit dem Bootable Media Builder und unter Verwendung Ihres Acronis Cyber Protect Lizenzschlüssels erstellt haben. Weitere Informationen über die Erstellung eines Boot-Mediums finden Sie in den Abschnitten Linux-basiertes Boot-Medium bzw. Windows-PE-basiertes Boot-Medium.

***So können Sie Daten mit einem Boot-Medium per Backup sichern***

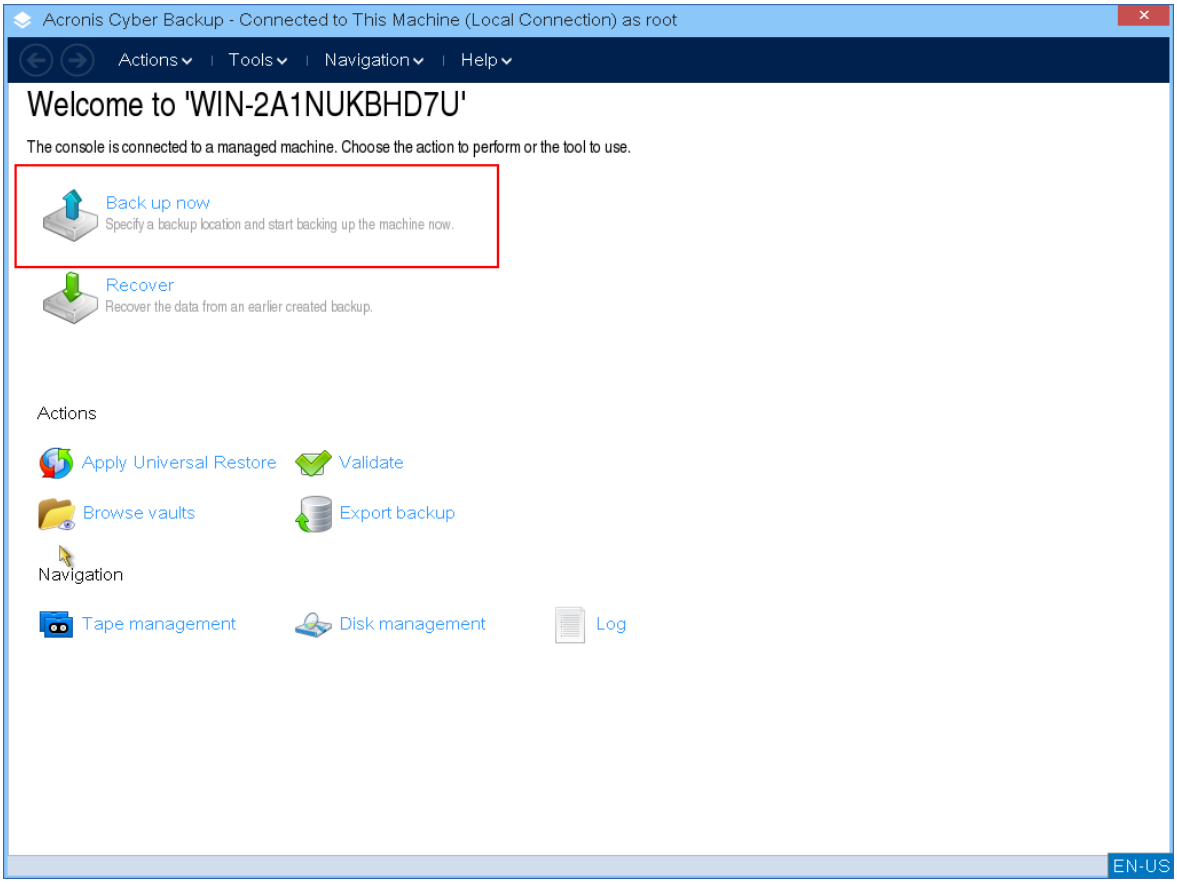
1. Booten Sie mit einem Acronis Boot-Medium.




2. Klicken Sie auf **Diese Maschine lokal verwalten**, wenn Sie die lokale Maschine sichern wollen. Anweisungen für Remote-Verbindungen finden Sie im Abschnitt 'Medien auf dem Management Server registrieren'.



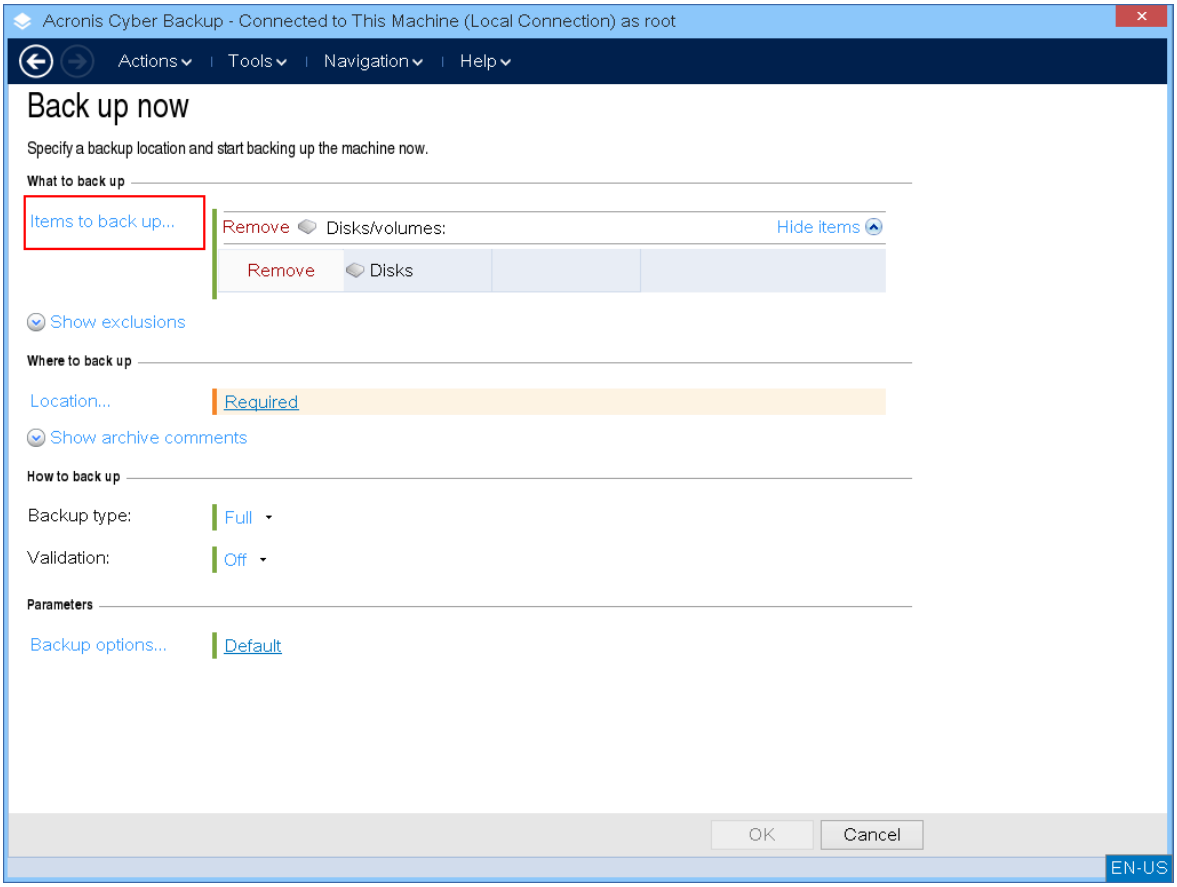

3. Klicken Sie auf **Backup jetzt**.



4. Alle festeningebaute Laufwerke der Maschine werden automatisch für das Backup ausgewählt. Wenn Sie die zu sichernden Daten ändern wollen, klicken Sie auf **Elemente für das Backup** und wählen Sie dann die gewünschten Laufwerke oder Volumes aus.

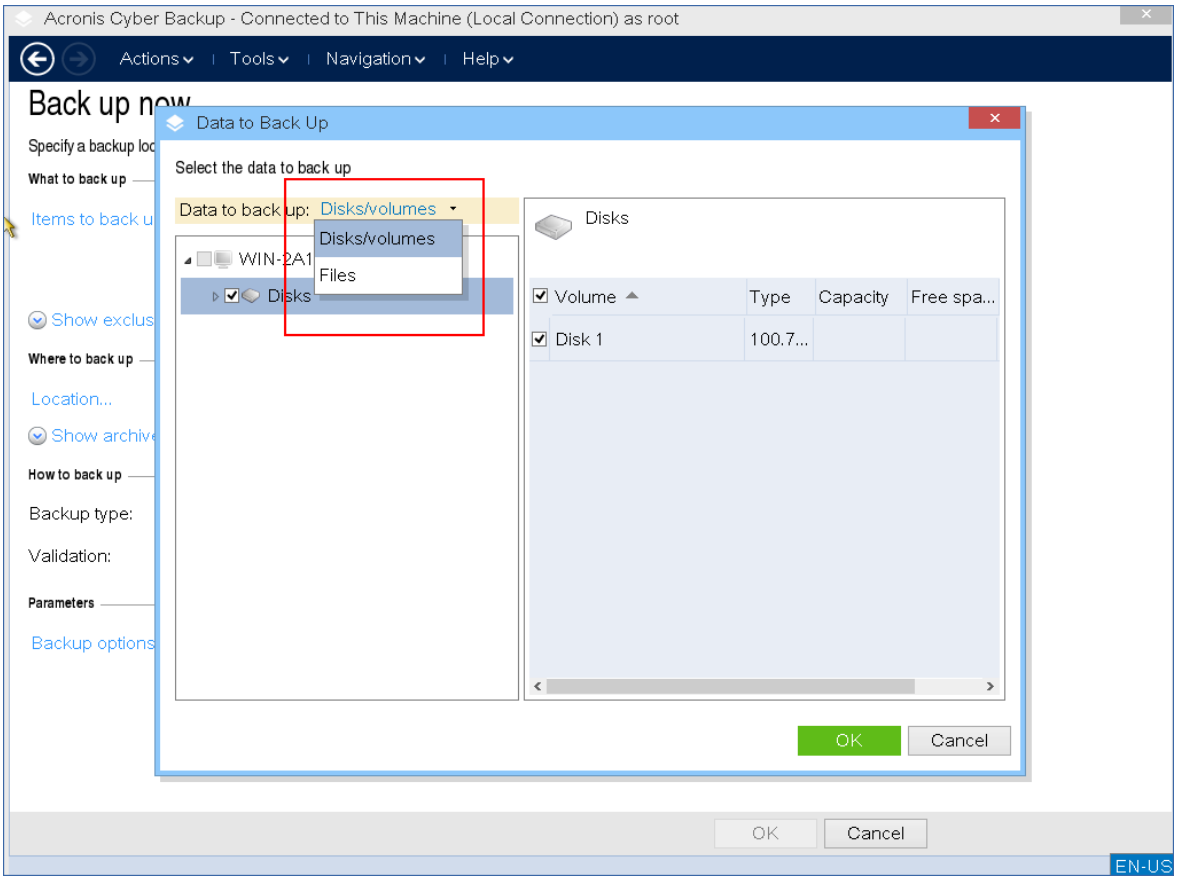
   Wenn Sie die zu sichernden Daten auswählen, kann es vorkommen, dass Sie folgende Meldung sehen: "*Diese Maschine kann nicht direkt ausgewählt werden. Auf der Maschine ist eine frühere Version des Agenten installiert. Verwenden Sie Richtlinienregeln, um diese Maschine zum Backup auszuwählen.*" Dies ist ein Problem der Benutzeroberfläche, das sicher ignoriert werden kann. Fahren Sie fort, indem Sie die einzelnen Laufwerke oder Volumes auswählen, die Sie sichern wollen.

   **Hinweis**
   Bei einem Linux-basierten Boot-Medium sehen Sie möglicherweise Laufwerksbuchstaben, die sich von denen in Windows unterscheiden. Versuchen Sie, das benötige Laufwerk/Volume anhand seiner Größe oder Bezeichnung zu identifizieren.

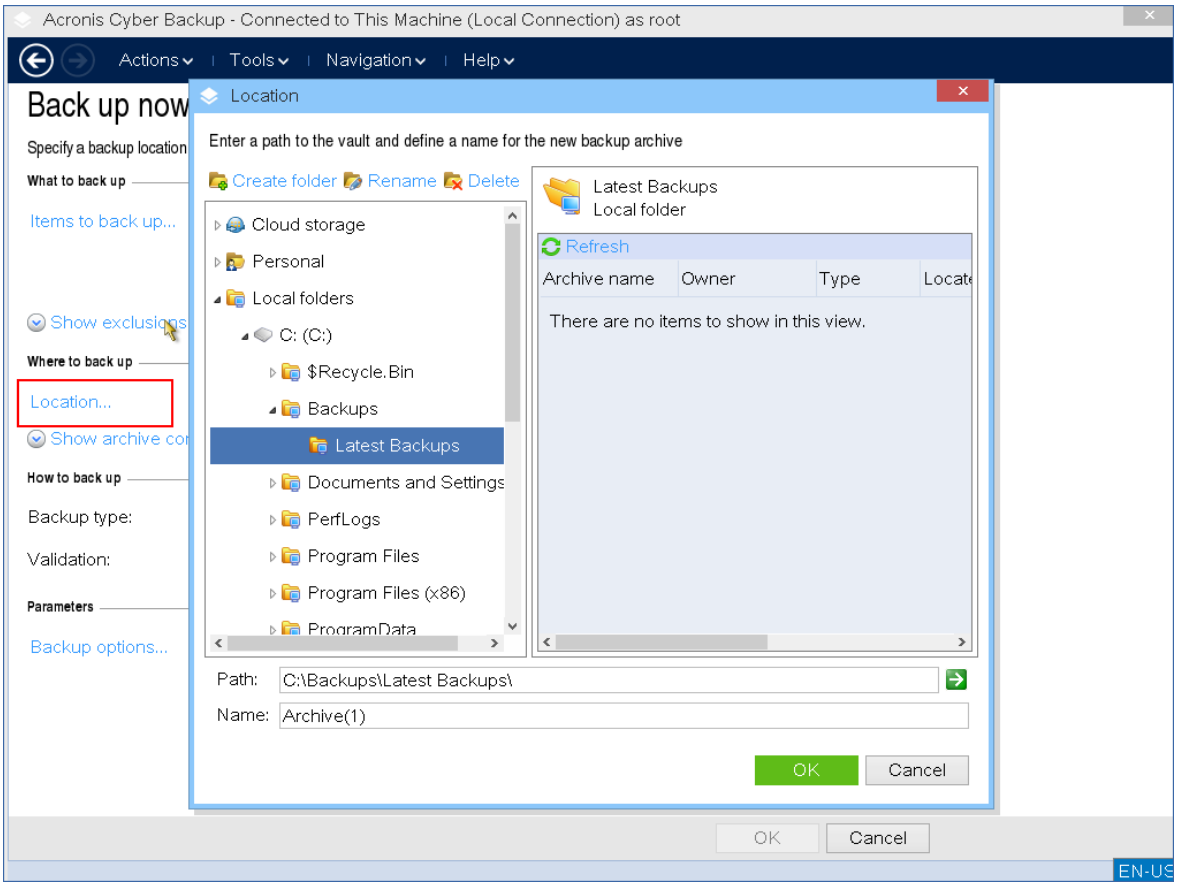



5. Wenn Sie Dateien oder Ordner statt Laufwerken sichern wollen, wechseln Sie bei **Daten für das Backup** zu **Dateien**.

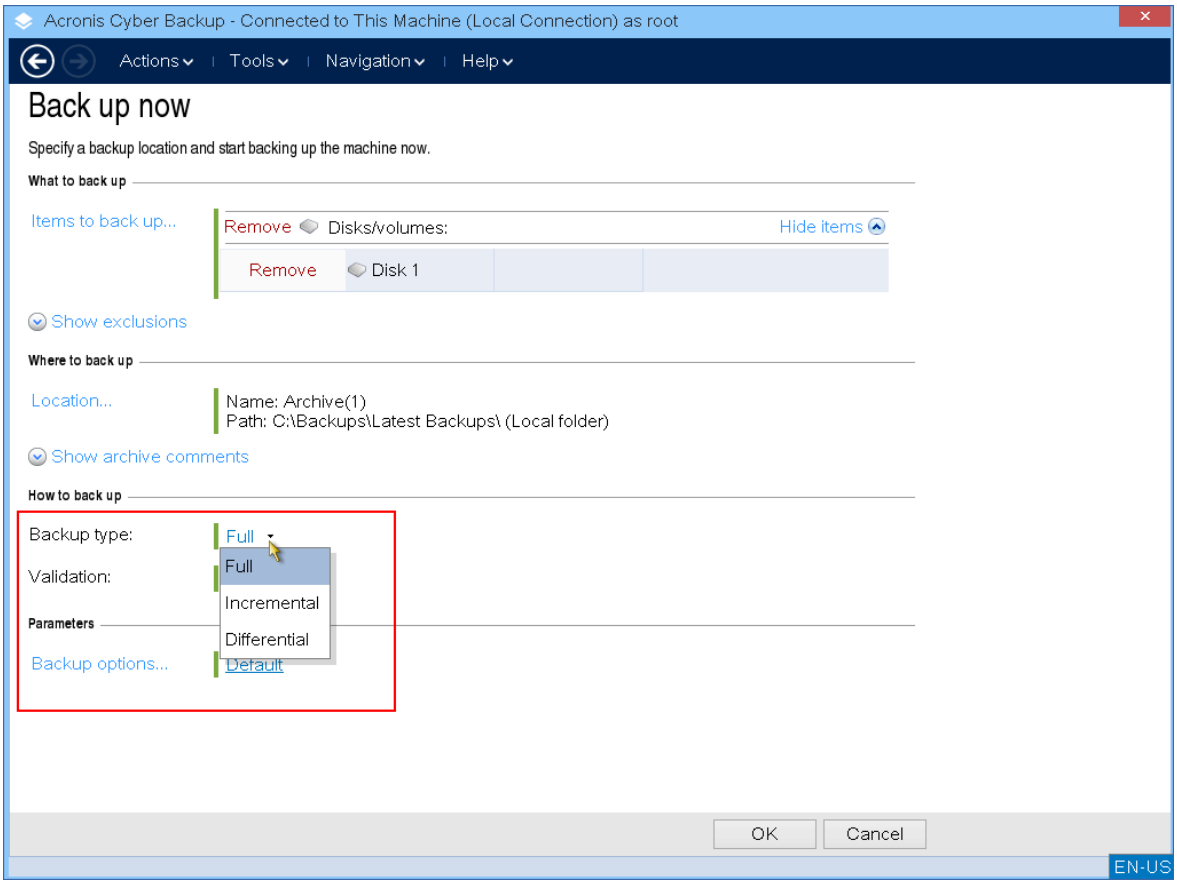
   Unter einem Boot-Medium sind nur Laufwerk/Volume- oder Datei/Ordner-Backups verfügbar. Andere Backup-Typen, wie z.B. Datenbank-Backups, sind nur verfügbar, wenn die Applikation unter dem regulären Betriebssystem (wie Windows) ausgeführt wird.



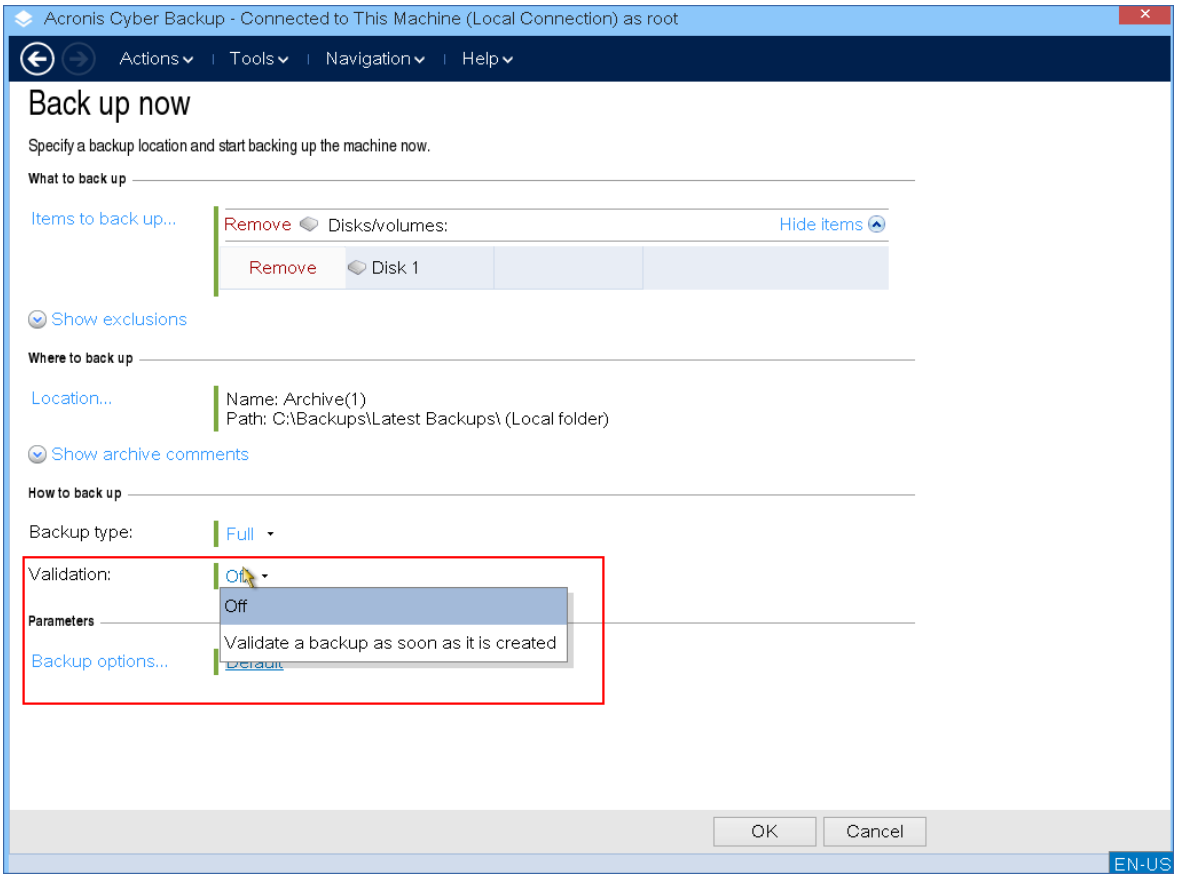

6. Klicken Sie auf **Speicherort**, um das Backup-Ziel festzulegen.



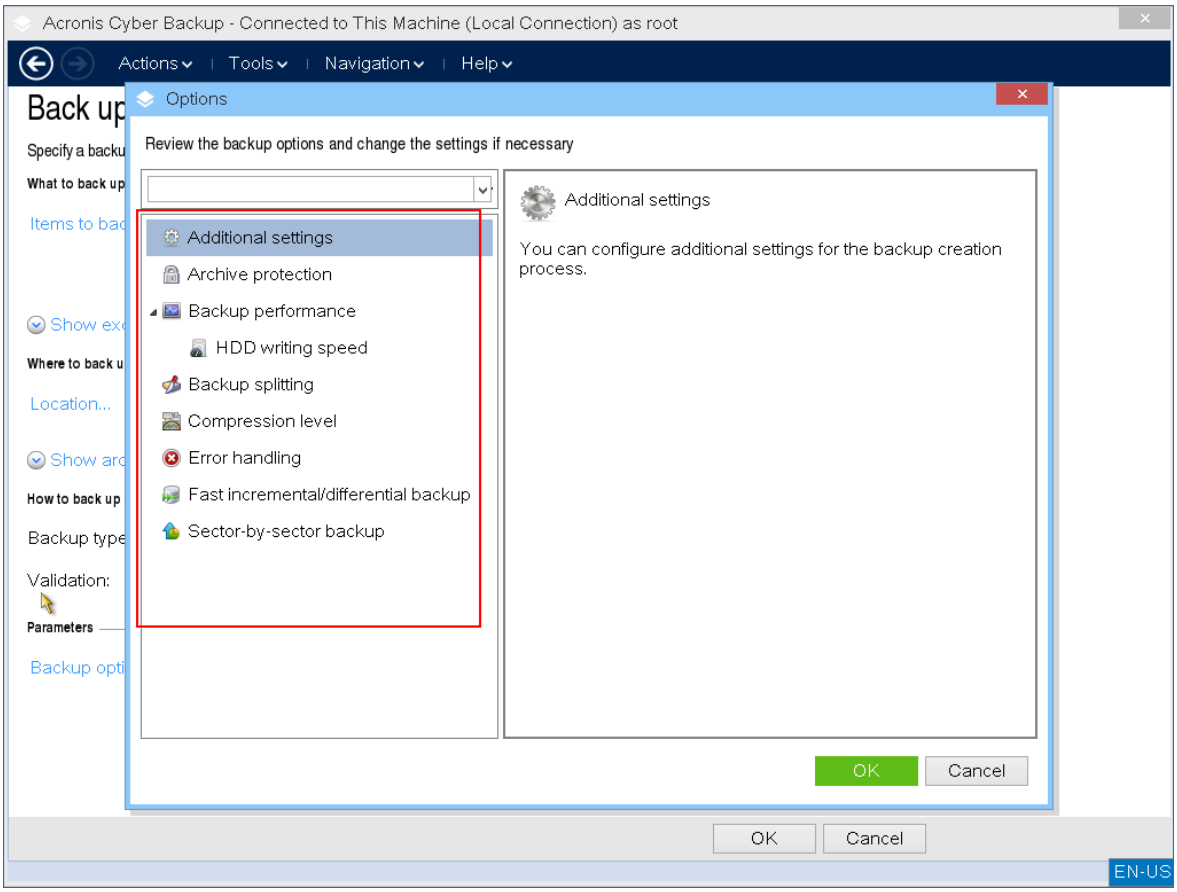

7. Spezifizieren Sie den Namen und Speicherort für Ihr Backup.
8. Spezifizieren Sie den Backup-Typ. Wenn dies das erste Backup an diesem Speicherort ist, wird ein vollständiges Backup erstellt. Wenn Sie eine Backup-Kette fortsetzen wollen, können Sie **Inkrementell** oder **Differentiell** wählen, um Speicherplatz einzusparen. Weitere Informationen zu Backup-Typen finden Sie unter: https://kb.acronis.com/content/1536.




9. [Optional] Wenn Sie die Backup-Datei überprüfen wollen, wählen Sie **Backup direkt nach Erstellung valildieren**.

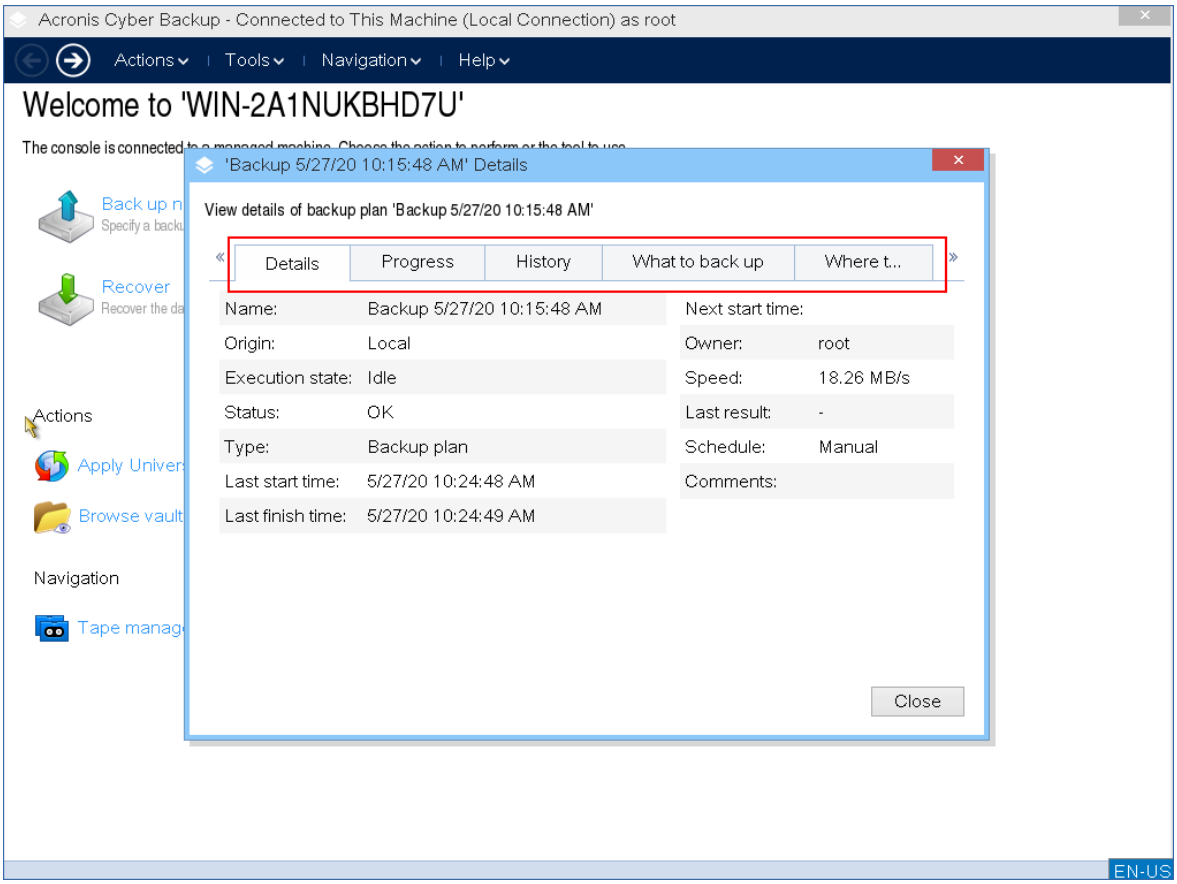



10. [Optional] Spezifizieren Sie die Backup-Optionen, die Sie eventuell benötigen – z.B. ein Kennwort für die Backup-Datei, eine Backup-Aufteilung oder die Fehlerbehandlung.




11. Klicken Sie auf **OK**, um das Backup zu starten.

    Das Boot-Medium liest die Daten von Laufwerk, komprimiert diese in eine .tib(x)-Datei und schreibt diese Datei dann zum Backup-Ziel (also dem ausgewählten Speicherort). Es wird kein Laufwerk-Snapshot erstellt, da es keine laufenden Applikationen gibt.
12. Sie können den Status des Backup-Tasks sowie weitere Informationen über das Backup in dem erscheinenden Fenster überprüfen.

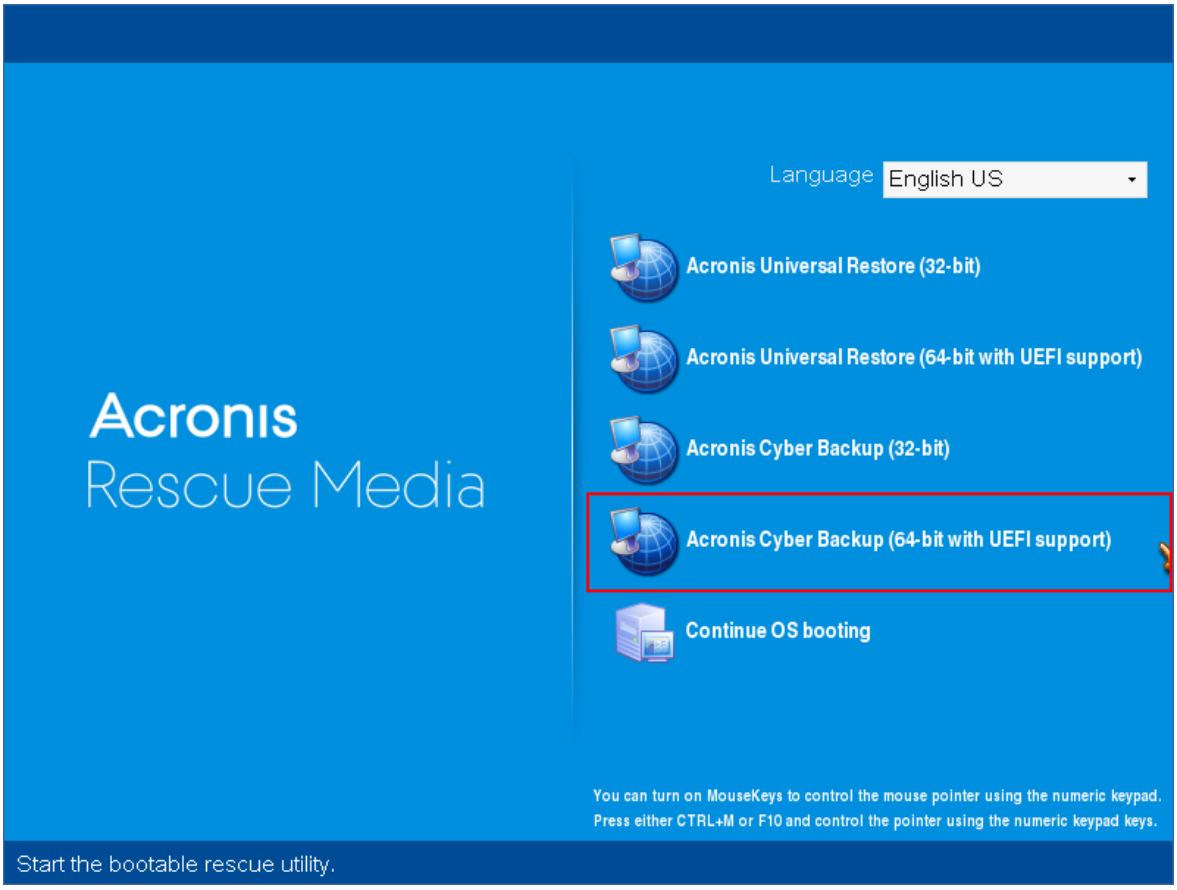



## Wiederherstellung mit einem Boot-Medium bei einem lokalen System

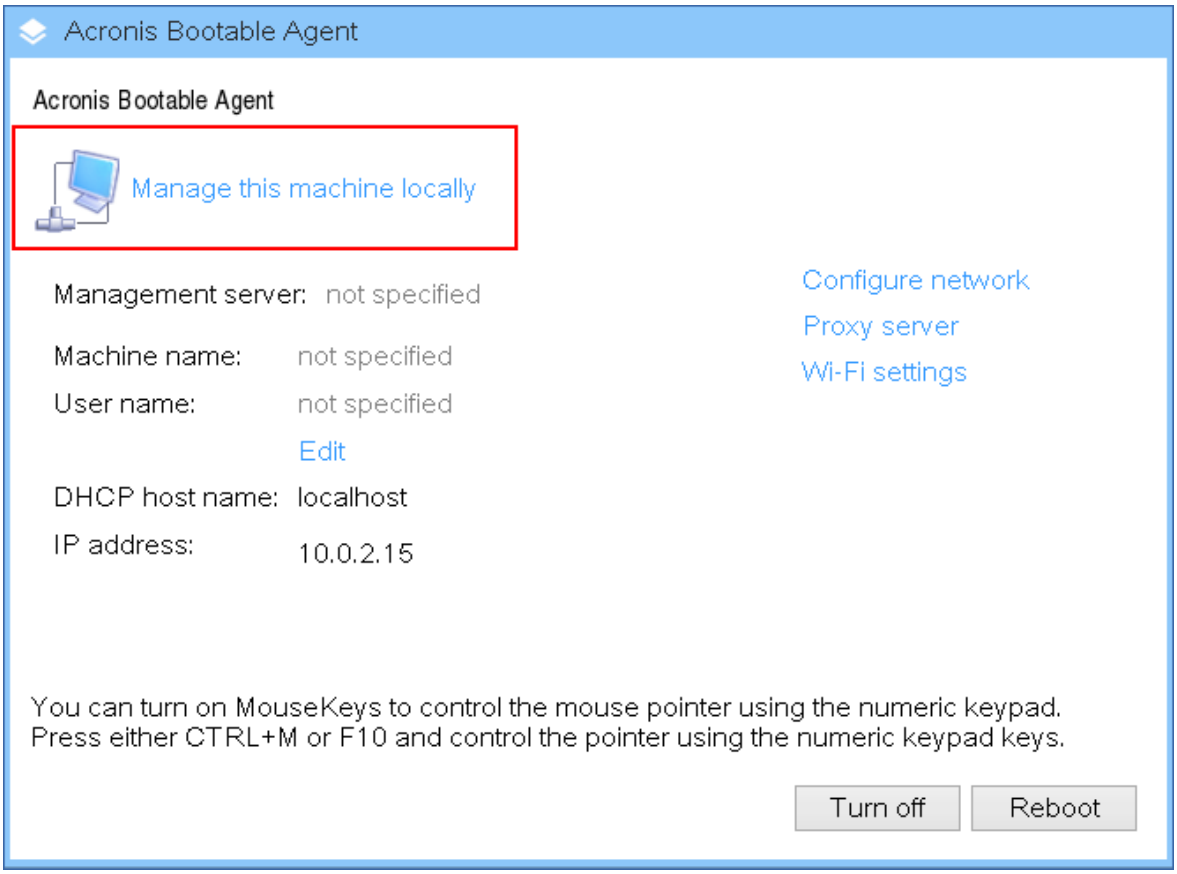
Wiederherstellungsaktionen können sowohl mit Boot-Medien durchgeführt werden, die mit dem Bootable Media Builder erstellt wurden, als einem vorgefertigte Boot-Medium, das Sie herunterladen können.

***So können Sie Daten mit einem Boot-Medium wiederherstellen***

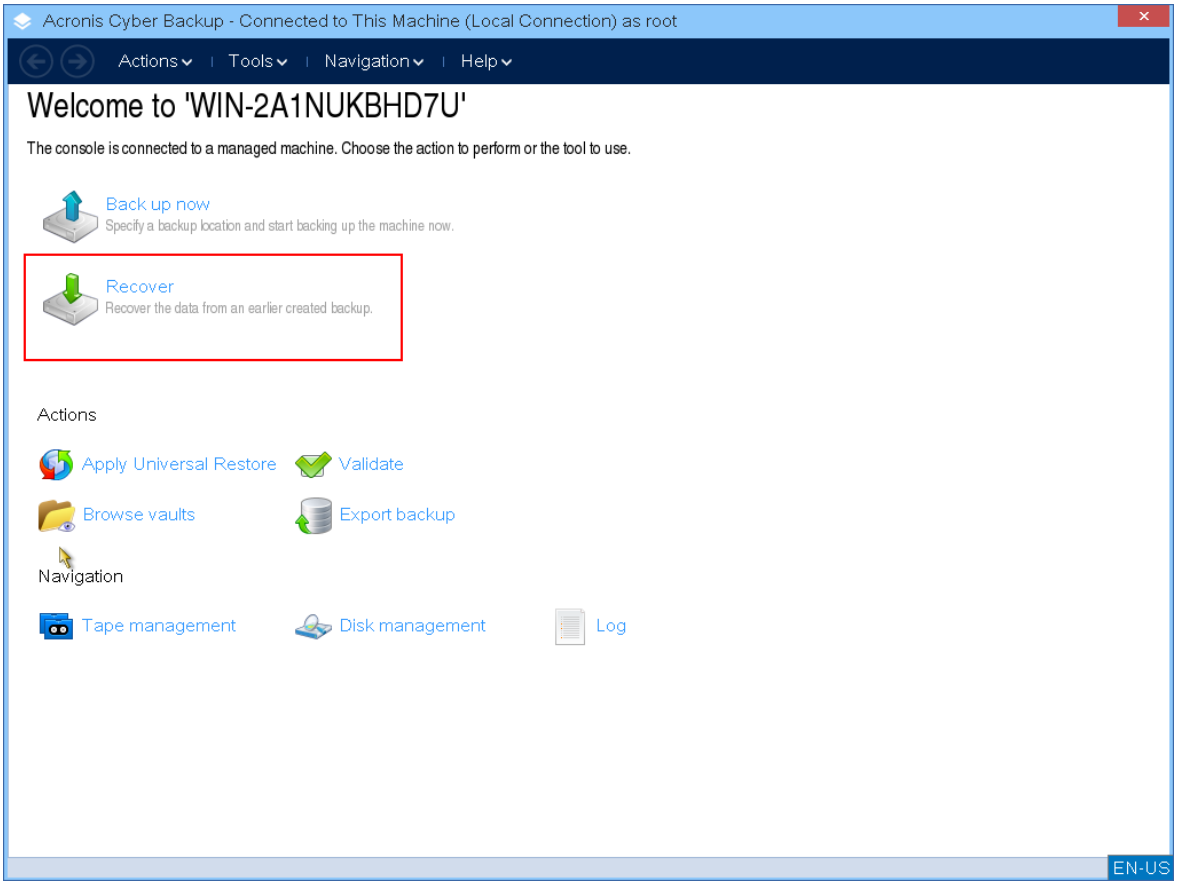
1. Booten Sie mit einem Acronis Boot-Medium.



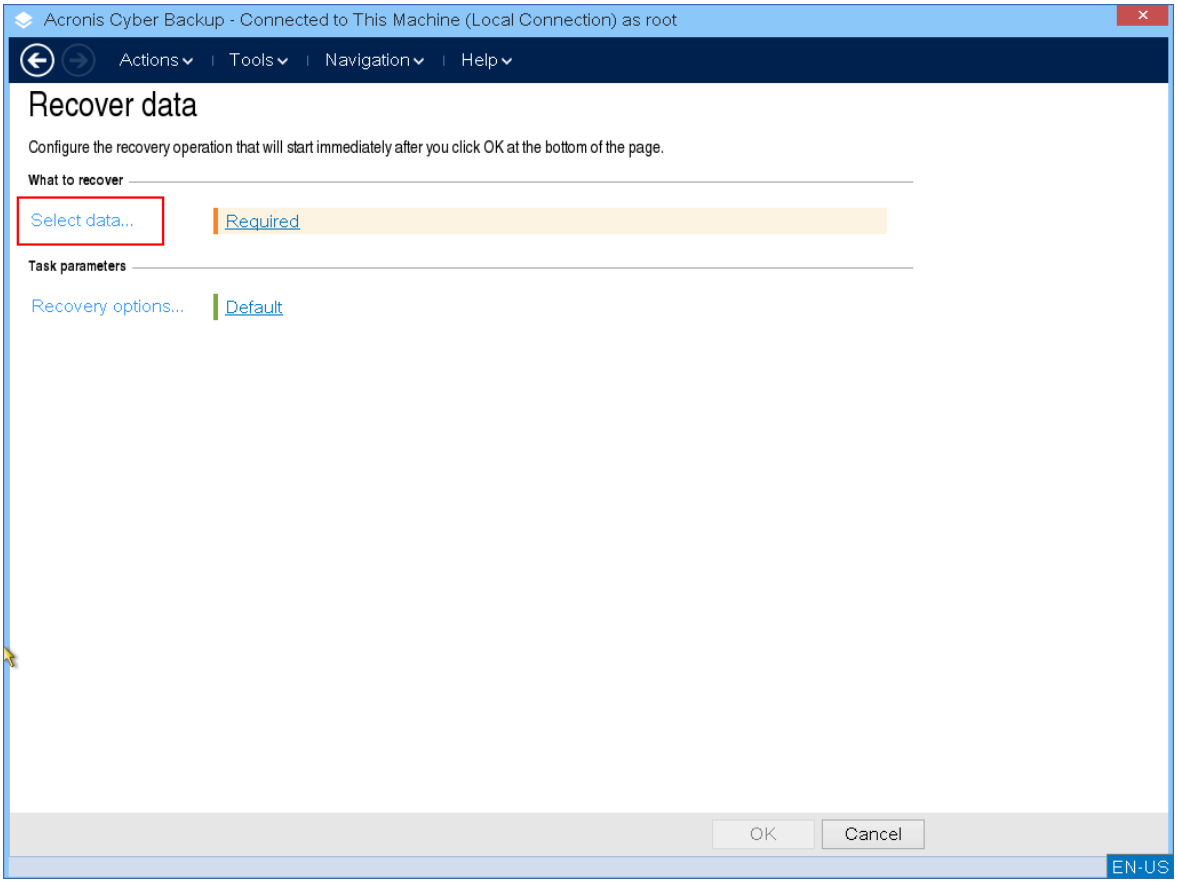

2. Klicken Sie auf **Diese Maschine lokal verwalten**, wenn Sie Daten zu einer lokalen Maschine wiederherstellen wollen. Anweisungen für Remote-Verbindungen finden Sie im Abschnitt 'Medien auf dem Management Server registrieren'.



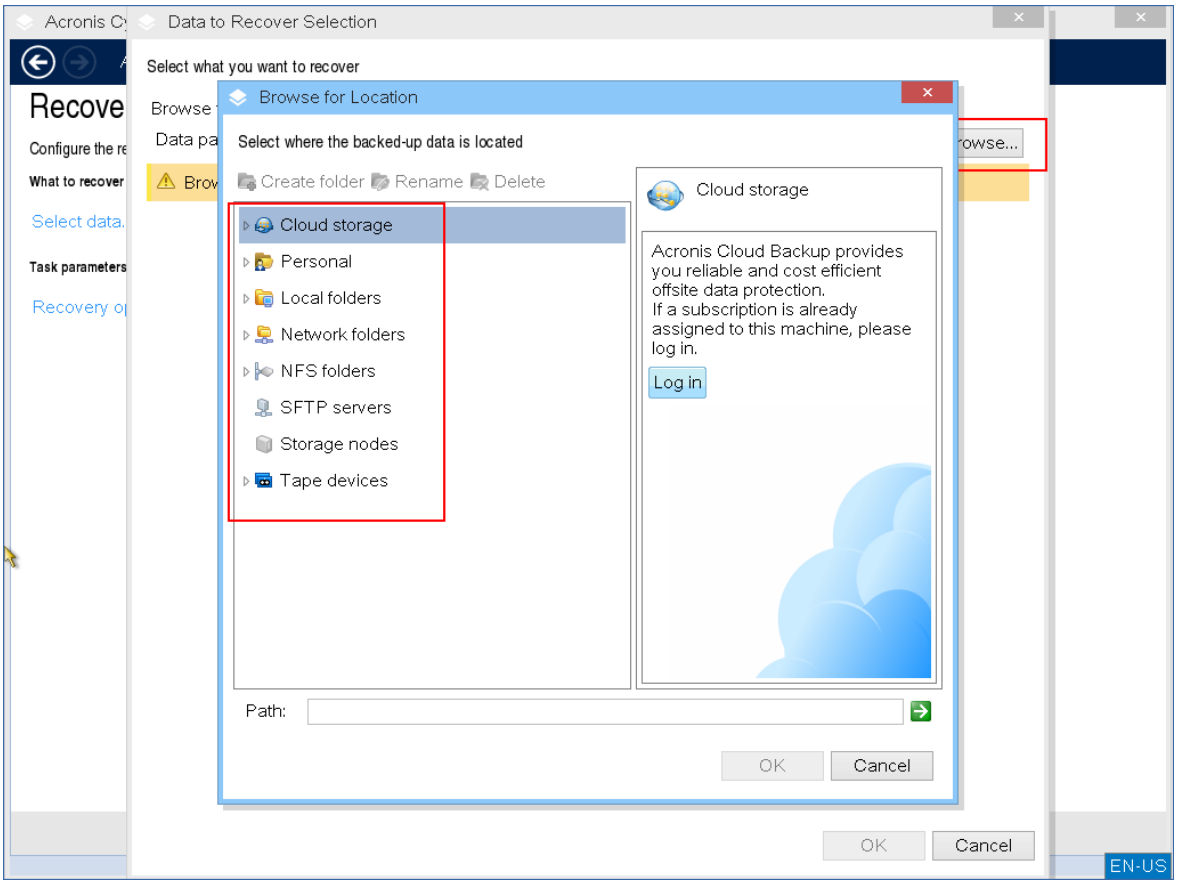

3. Klicken Sie auf **Recovery**.



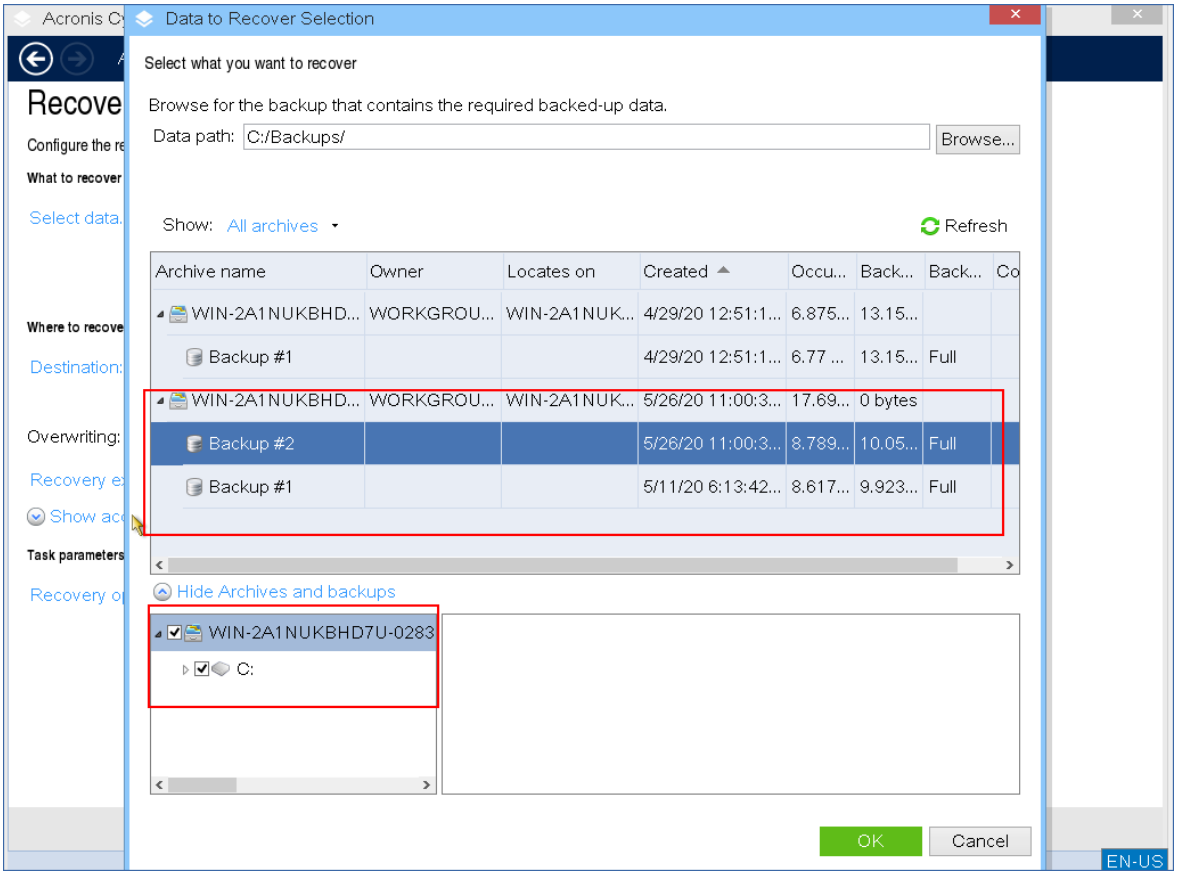
4. Klicken Sie bei **Recovery-Quelle** auf **Daten wählen**.



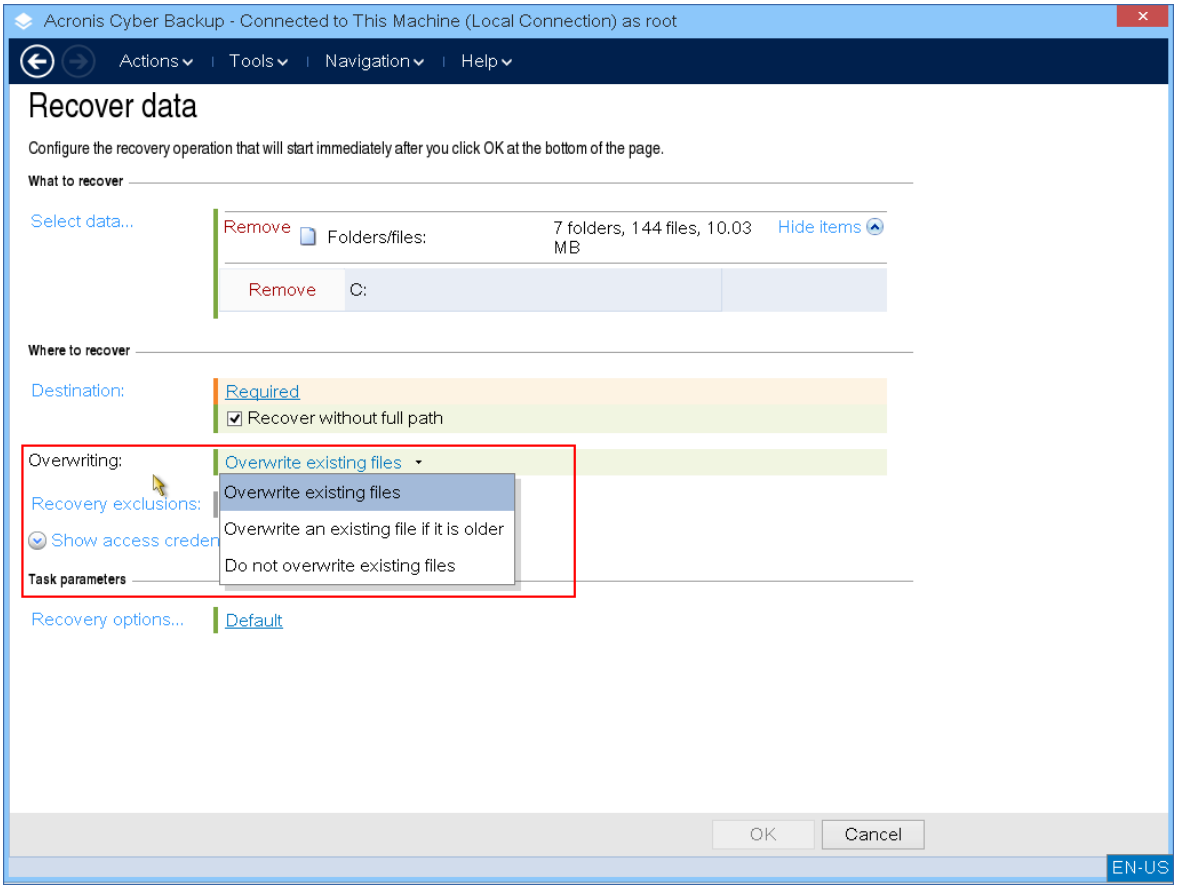

5. klicken Sie auf **Durchsuchen** und wählen Sie den Speicherort des gewünschten Backups aus.



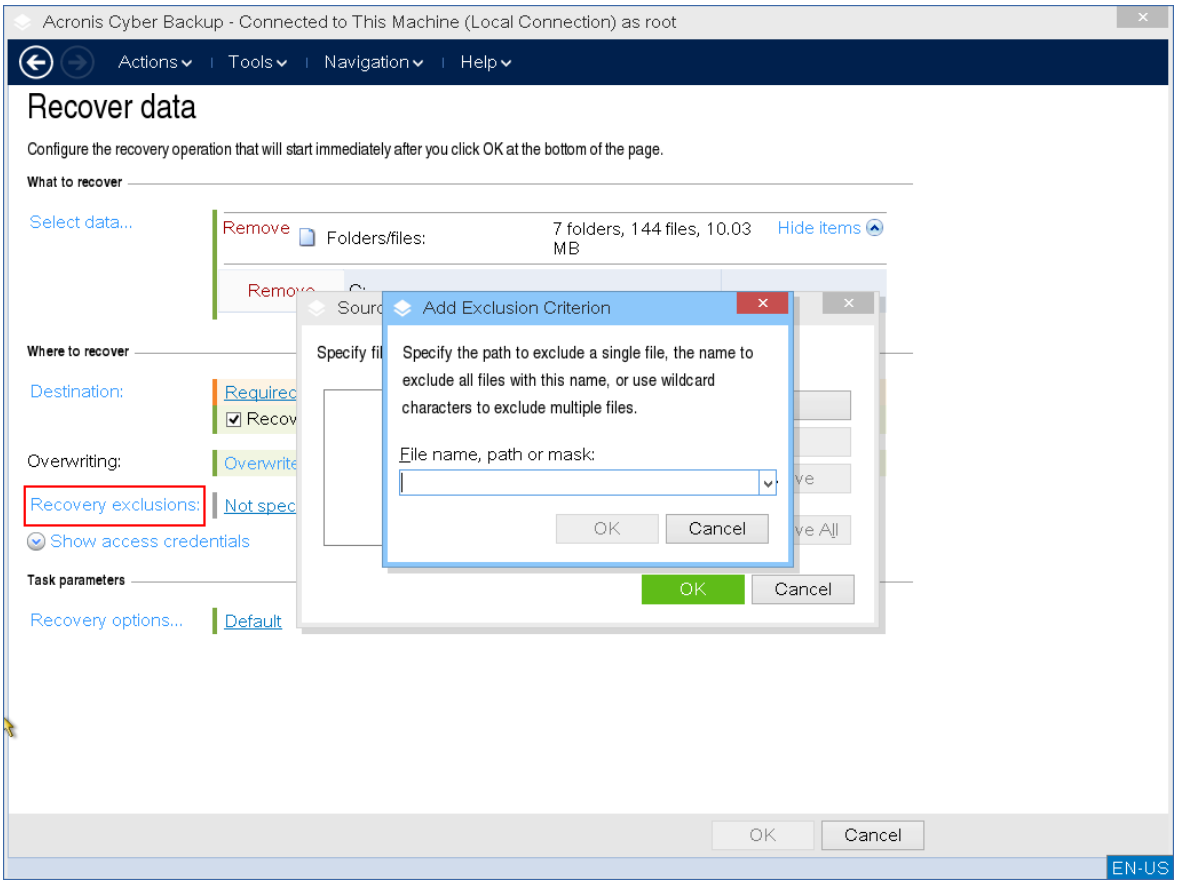

6. Wählen Sie die Backup-Datei, die Sie wiederherstellen wollen.



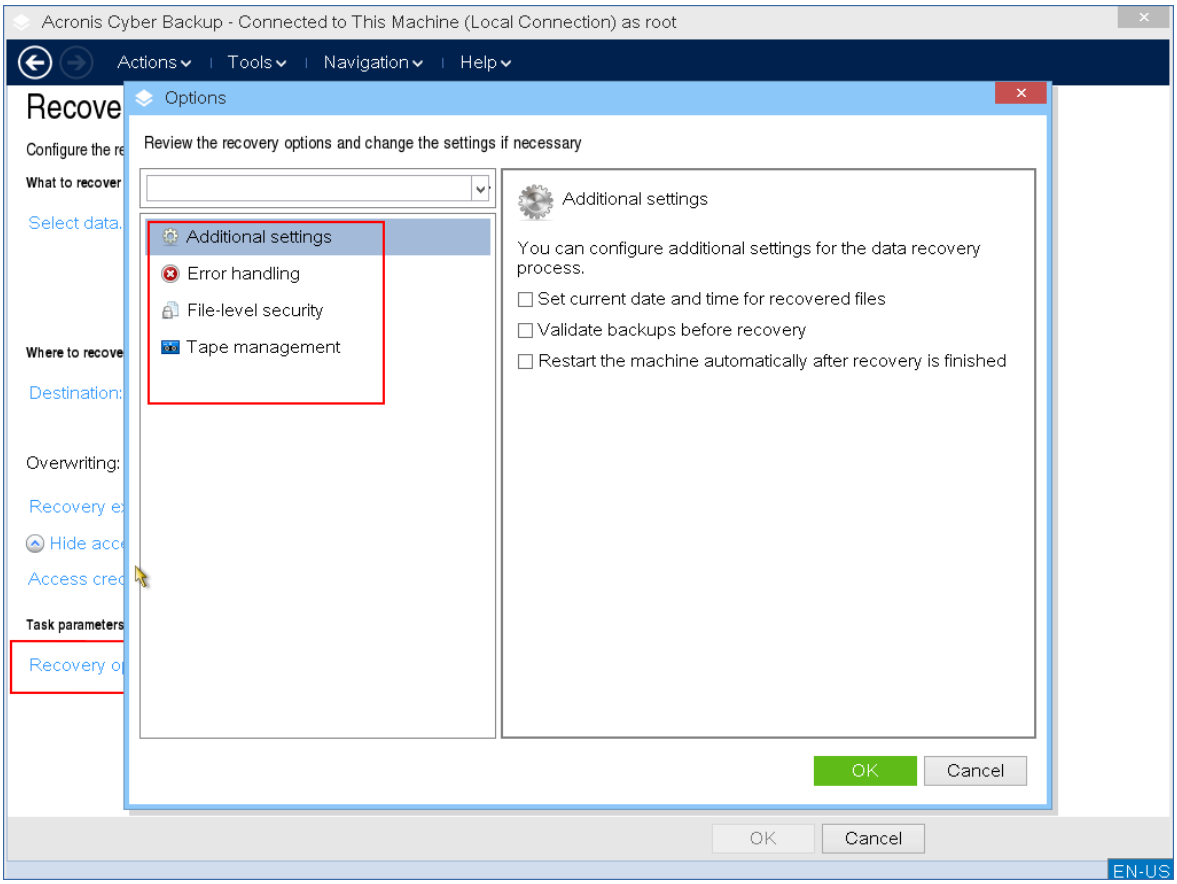
7. Wählen Sie im unteren linken Fensterbereich die wiederherzustellenden Laufwerke/Volumes (oder Dateien/Ordner) aus und klicken Sie dann auf **OK**.
8. [Optional] Ändern Sie die Regeln zum Überschreiben.




9. [Optional] Ändern Sie Ausschlüsse für die Wiederherstellung.




10. [Optional] Ändern Sie Recovery-Optionen.




11. Überprüfen Sie, ob Ihre Einstellungen richtig sind, und klicken Sie dann auf **OK**.

**Hinweis**
Wenn Sie Daten auf abweichender Hardware wiederherstellen wollen, müssen Sie Acronis Universal Restore verwenden.
Acronis Universal Restore ist nicht verfügbar, wenn sich das Backup in einer Acronis Einer Secure Zone befindet.

## Laufwerksverwaltung mit einem Boot-Medium

Mit einem Acronis Boot-Medium können Sie die Laufwerks-/Volume-Konfiguration einer Maschine für Wiederherstellungen von Volume-Images vorbereiten, die mit Acronis Cyber Protect gesichert wurden.

Nachdem ein Laufwerk gesichert und sein Image an einem sicheren Speicherplatz hinterlegt wurde, kann es vorkommen, dass sich die Laufwerkskonfiguration der Maschine durch Austausch einer Festplatte oder durch Hardware-Verlust ändert. In einem solchen Fall können Sie die erforderliche Laufwerkskonfiguration neu erstellen, sodass das Volume-Image wie „ursprünglich vorliegend“ wiederhergestellt werden kann – oder mit einer geänderten Laufwerks-/Volume-Struktur, die Sie für notwendig halten.

Treffen Sie alle notwendigen Vorsichtsmaßnahmen, um mögliche Datenverluste zu vermeiden.

**Wichtig**

Alle Laufwerk- und Volume-Aktionen beinhalten ein gewisses Risiko für Datenverluste. Aktionen auf System- oder Daten-Volumes müssen sehr sorgfältig ausgeführt werden, um mögliche Probleme mit dem Boot-Ablauf oder Laufwerksdatenspeicher zu vermeiden.
Aktionen mit Laufwerken und Volumes benötigen eine gewisse Zeit – und jeder Stromverlust, jedes unbeabsichtigte Ausschalten der Maschine oder versehentliche Drücken des Reset-Schalters während der Prozedur kann zur Beschädigung des Volumes und Datenverlusten führen.

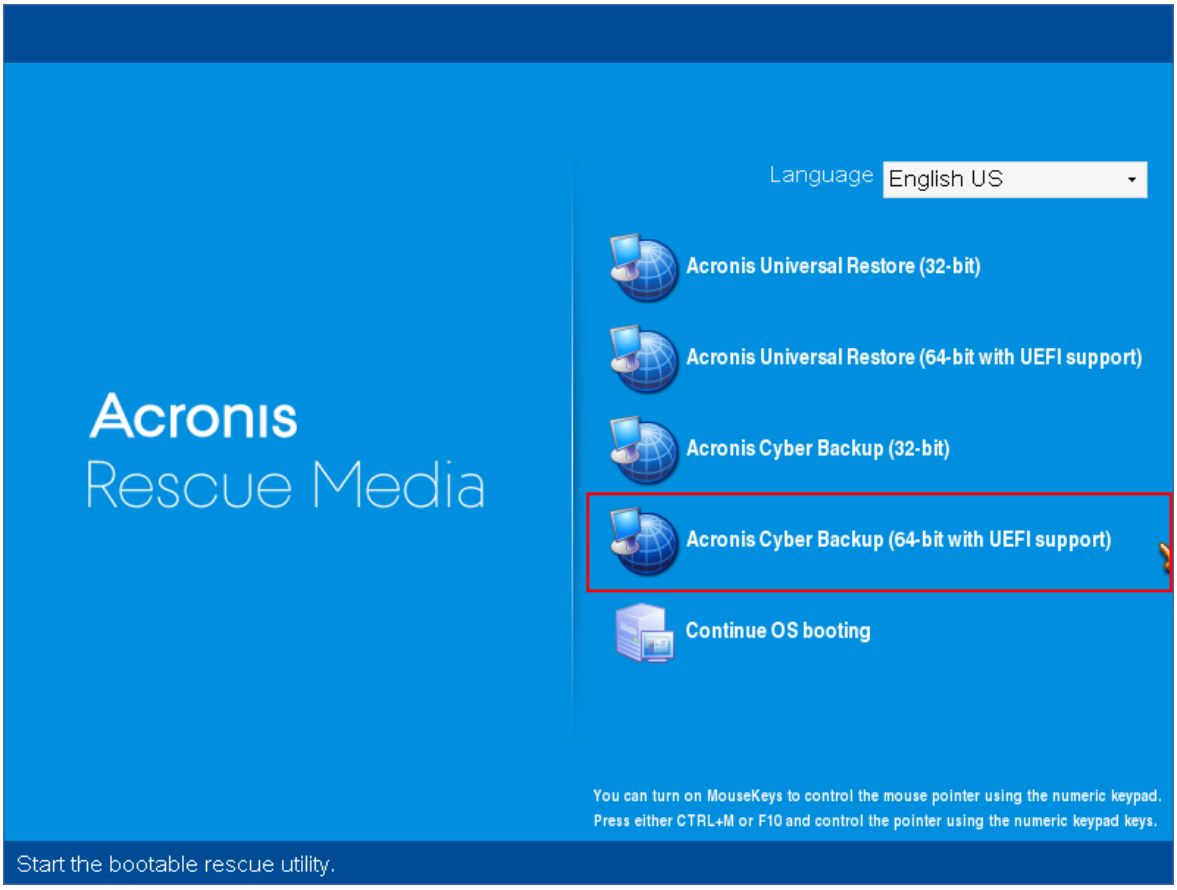
Sie können Laufwerksverwaltungsaktionen auf einer fabrikneuen, einer Nicht-Windows-Maschine oder auf einer Maschine ausführen, die nicht mehr booten kann. Sie benötigen ein Boot-Medium, das Sie mit dem Bootable Media Builder und unter Verwendung Ihres Acronis Cyber Protect Lizenzschlüssels erstellt haben. Weitere Informationen über die Erstellung eines Boot-Mediums finden Sie in den Abschnitten Linux-basiertes Boot-Medium bzw. Windows-PE-basiertes Boot-Medium.

**Hinweis**

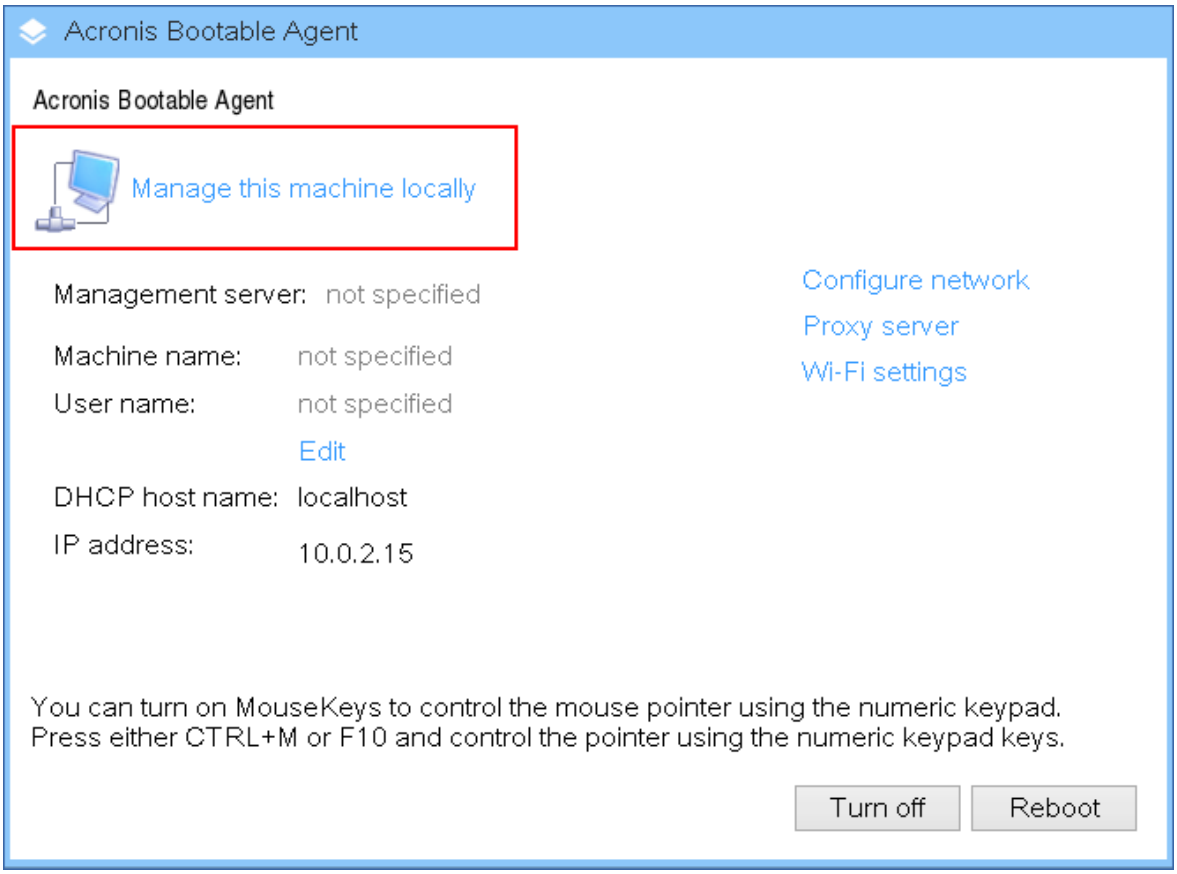
Die Funktionalität zur Laufwerksverwaltung ist bei Boot-Medien, die auf Windows PE 4.0 und höher basieren, nicht verfügbar. Die Laufwerksverwaltung wird daher für Windows 7 und frühere Betriebssysteme unterstützt. Um Laufwerksverwaltungsaktionen unter Windows 8 und höher durchführen zu können, müssen Sie den Acronis Disk Director installieren. Weitere Informationen finden Sie in diesem Knowledge Base-Artikel: https://kb.acronis.com/de/content/47031.

***So können Sie Laufwerksverwaltungsaktionen durchführen***

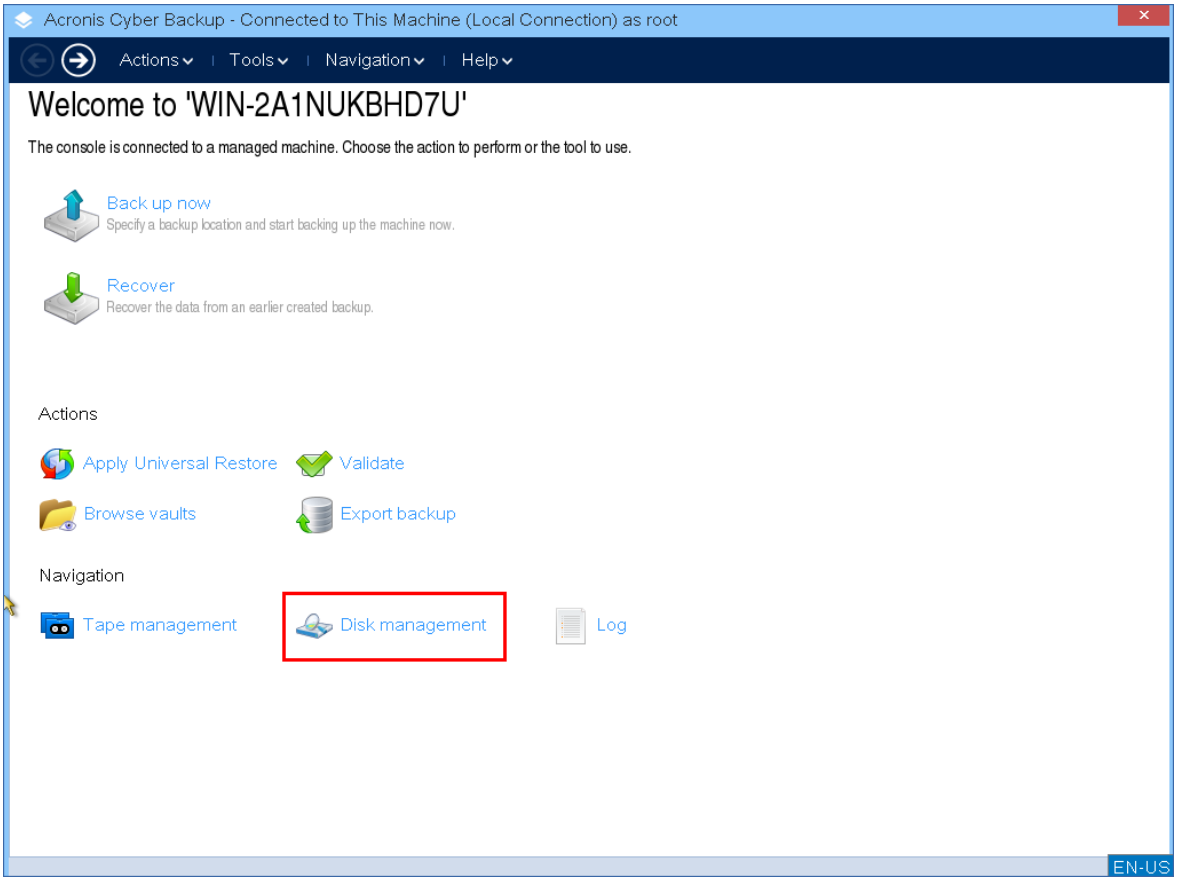
1. Booten Sie mit einem Acronis Boot-Medium.




2. Klicken Sie auf **Diese Maschine lokal verwalten**, wenn Sie auf der lokalen Maschine arbeiten wollen. Anweisungen für Remote-Verbindungen finden Sie im Abschnitt 'Medien auf dem Management Server registrieren'.




3. Klicken Sie auf **Laufwerksverwaltung**.



**Hinweis**
Aktionen zur Laufwerksverwaltung funktionieren unter einem bootfähigen Medium möglicherweise nicht korrekt, falls auf der Maschine Speicherplätze (Storage Spaces) konfiguriert sind.

## Unterstützte Dateisysteme

Das Boot-Medium unterstützt die Laufwerksverwaltung mit folgenden Dateisystemen:

- FAT 16/32
- NTFS

Wenn Sie mit einem Volume, das ein anderes Dateisystem hat, Aktionen durchzuführen müssen, empfehlen wir Ihnen die Verwendung des Acronis Disk Director. Dieses Programm bietet noch mehr Tools und Utilities, um Festplatten und Volumes mit den folgenden Dateisystemen zu verwalten:

- FAT 16/32
- NTFS
- Ext2
- Ext3
- HFS+
- HFSX
- ReiserFS
- JFS
- Linux SWAP

## Grundlegende Vorsichtsmaßnahmen

Treffen Sie alle notwendigen Vorsichtsmaßnahmen, um mögliche Schäden an der Laufwerks- bzw. Volume-Struktur oder Datenverlust abzuwenden und beachten Sie folgende Richtlinien:

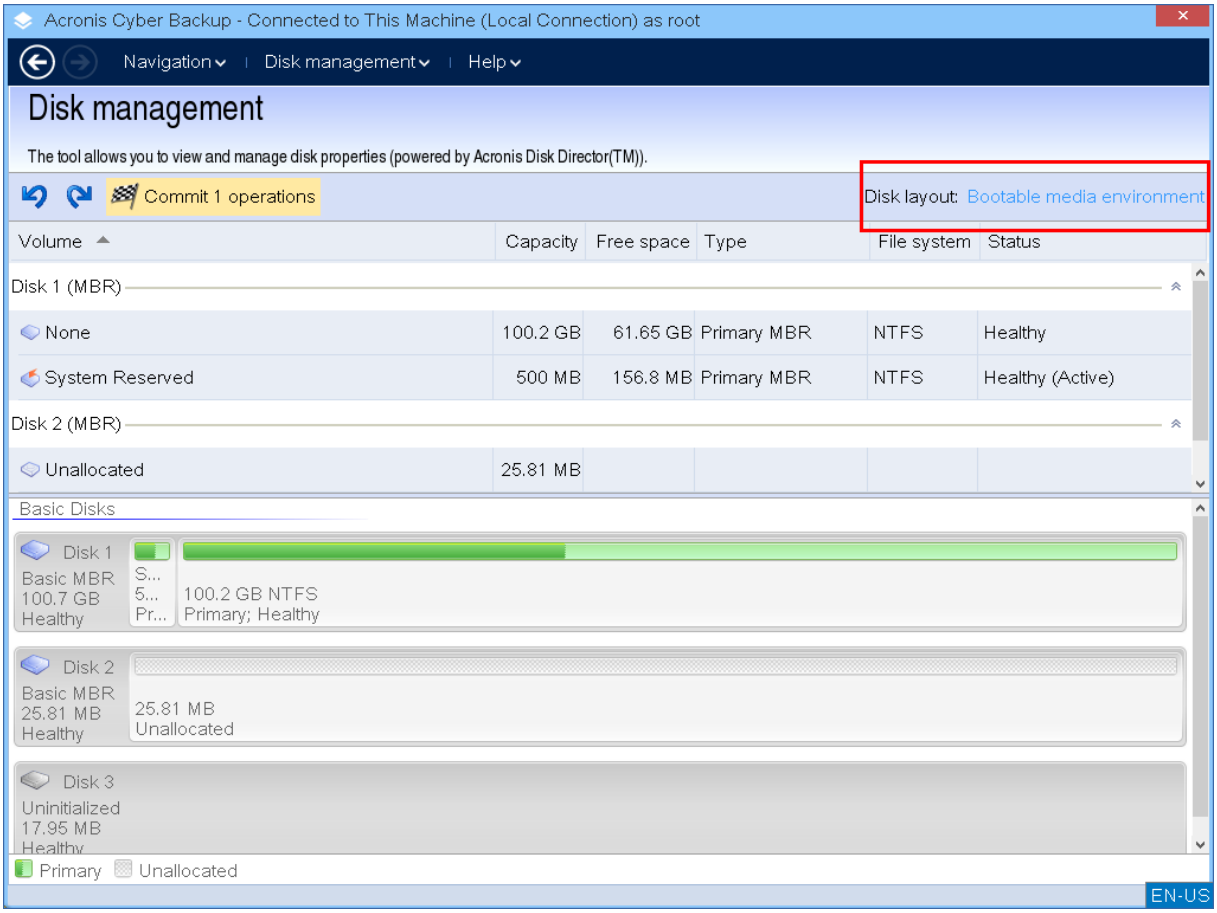
1. Erstellen Sie von Laufwerken, auf denen Volumes erstellt oder verwaltet werden, ein Backup. Indem Sie wichtige Daten auf ein anderes Laufwerk, eine Netzwerkfreigabe oder Wechselmedien sichern, können Sie – wohl wissend, dass Ihre Daten gut geschützt sind – beruhigt mit Ihren Laufwerken bzw. Volumes arbeiten.
2. Überprüfen Sie Ihr Festplattenlaufwerk, um sicherzustellen, dass dieses voll funktionstüchtig ist und keine defekten Sektoren oder Dateisystemfehler enthält.
3. Führen Sie keine Laufwerks- bzw. Volume-Aktionen aus, während andere Programme mit Low-Level-Zugriff auf Laufwerke ausgeführt werden.

## Auswählen des Betriebssystems für die Datenträgerverwaltung

Auf einer Maschine mit zwei oder mehr Betriebssystemen hängt die Laufwerks- bzw. Volume-Darstellung davon ab, welches Betriebssystem gerade läuft. Ein und dasselbe Volume kann unter

verschiedenen Betriebssystemen unterschiedliche Laufwerksbuchstaben haben.

Wenn Sie eine Laufwerksverwaltungsaktion durchführen, müssen Sie spezifizieren, für welches Betriebssystem das Laufwerkslayout angezeigt wird. Klicken Sie dafür auf den Namen des Betriebssystems neben der **Laufwerkslayout**-Kennzeichnung und wählen Sie in dem sich öffnenden Fenster das gewünschte Betriebssystem aus.




## Laufwerksaktionen

Mit dem Boot-Medium können Sie folgende Laufwerksverwaltungsaktionen durchführen:

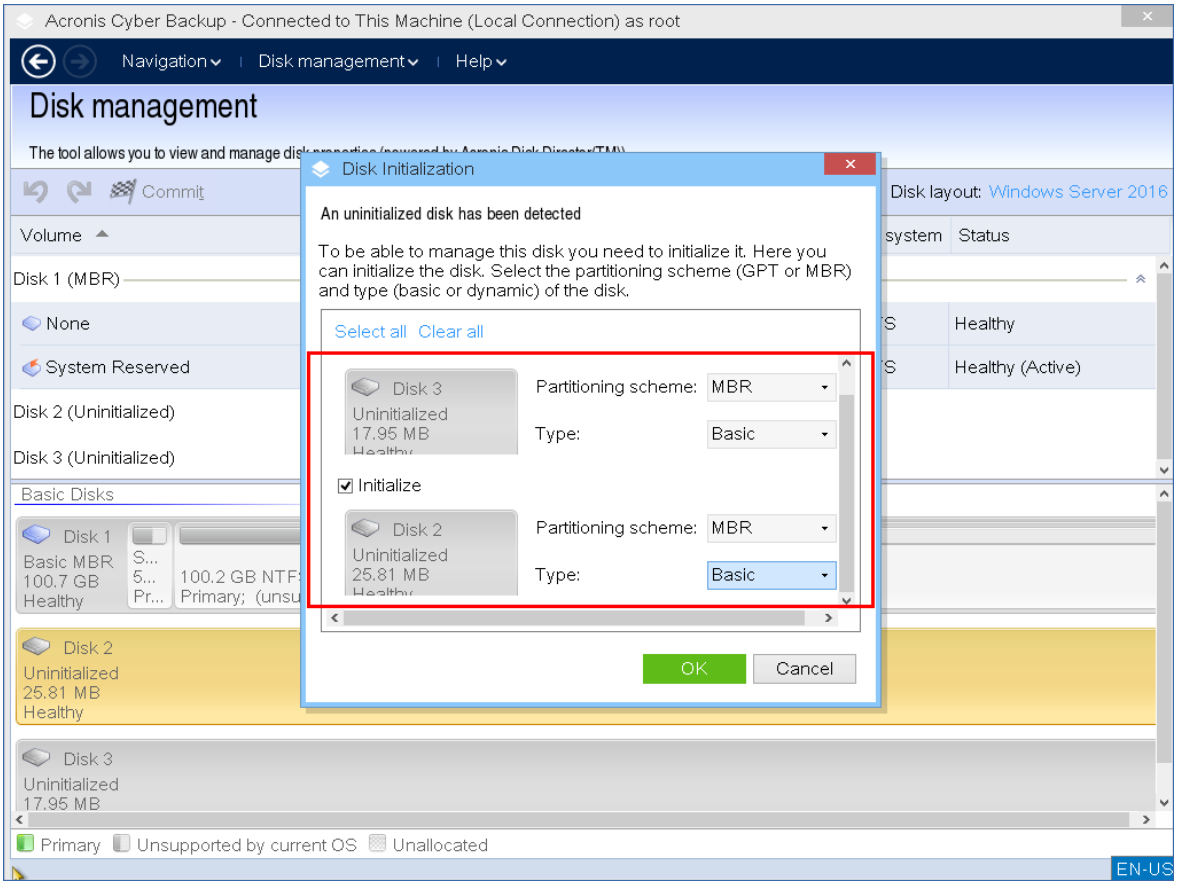
- Laufwerksinitialisierung – Initialisiert eine neue Hardware, die dem System hinzugefügt wurde
- Basis-Laufwerk klonen – Überträgt die kompletten Daten einer Quell- auf eine Zielplatte (gilt für Basisdatenträger vom MBR-Typ)
- Laufwerk konvertieren: MBR zu GPT – Konvertiert eine MBR-Partitionstabelle zu GPT
- Laufwerk konvertieren: GPT zu MBR – Konvertiert eine GPT-Partitionstabelle zu MBR
- Laufwerk konvertieren: Basis zu Dynamisch – Konvertiert einen Basis- zu einem dynamischen Datenträger
- Laufwerk konvertieren: Dynamisch zu Basis – Konvertiert einen dynamischen zu einem Basisdatenträger

## Laufwerksinitialisierung

Das Boot-Medium stellt ein nicht initialisiertes Laufwerk als grauen Block mit einem grauen Symbol dar und zeigt damit an, dass das Laufwerk nicht vom System verwendet werden kann.

***So können Sie ein Laufwerk initialisieren:***

1. Klicken Sie mit der rechten Maustaste auf das gewünschte Laufwerk und wählen Sie den Befehl **Initialisieren**.
2. Sie können im Fenster **Laufwerksinitialisierung** das Laufwerk-Partitionierungsschema (MBR oder GPT) und den Laufwerkstyp (Basis oder Dynamisch) einstellen.
3. Indem Sie auf **OK** klicken, fügen Sie die Laufwerksinitialisierung der Liste ausstehender Aktionen hinzu.
4. Um die hinzugefügte Aktion abschließen zu können, müssen Sie diese noch ausführen lassen. Wenn Sie das Programm ohne Ausführung der Aktion beenden, wird diese verworfen.
5. Nach der Initialisierung ist der Laufwerksspeicherplatz erst einmal nicht zugeordnet. Wenn Sie diesen verwenden wollen, müssen Sie auf dem Laufwerk ein Volume erstellen.




## Klonen von Basis-Laufwerken

Mit einem voll ausgestatteten Linux-basierten Boot-Medium können Sie MBR-Laufwerke vom Typ 'Basis' klonen. Die Funktion 'Laufwerk klonen' ist nicht verfügbar, wenn Sie ein vorgefertigtes Boot-

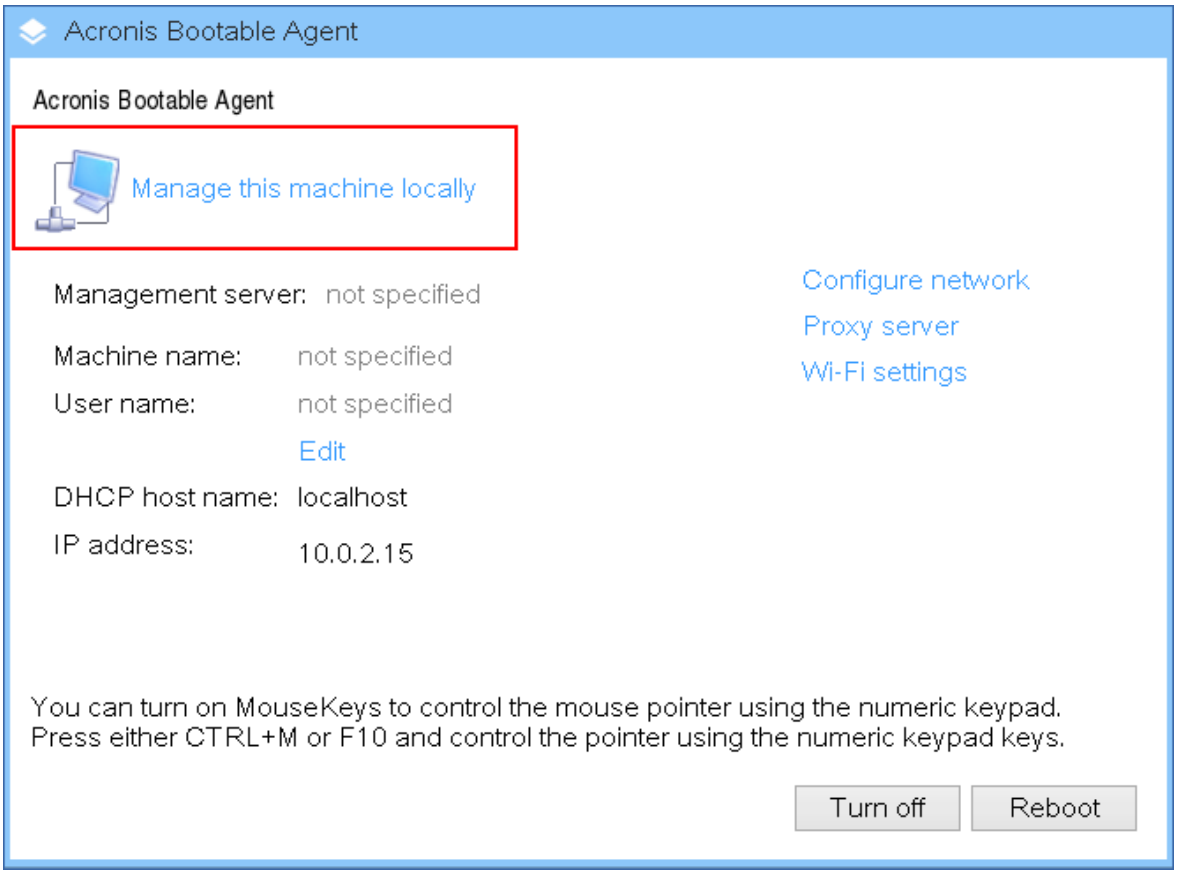
Medium verwenden (das Sie herunterladen können) – oder mit einem Boot-Medium, welches Sie ohne Lizenzschlüssel erstellt haben.

**Hinweis**
Sie können Laufwerke auch über das Acronis Cyber Protect Befehlszeilenwerkzeug klonen.

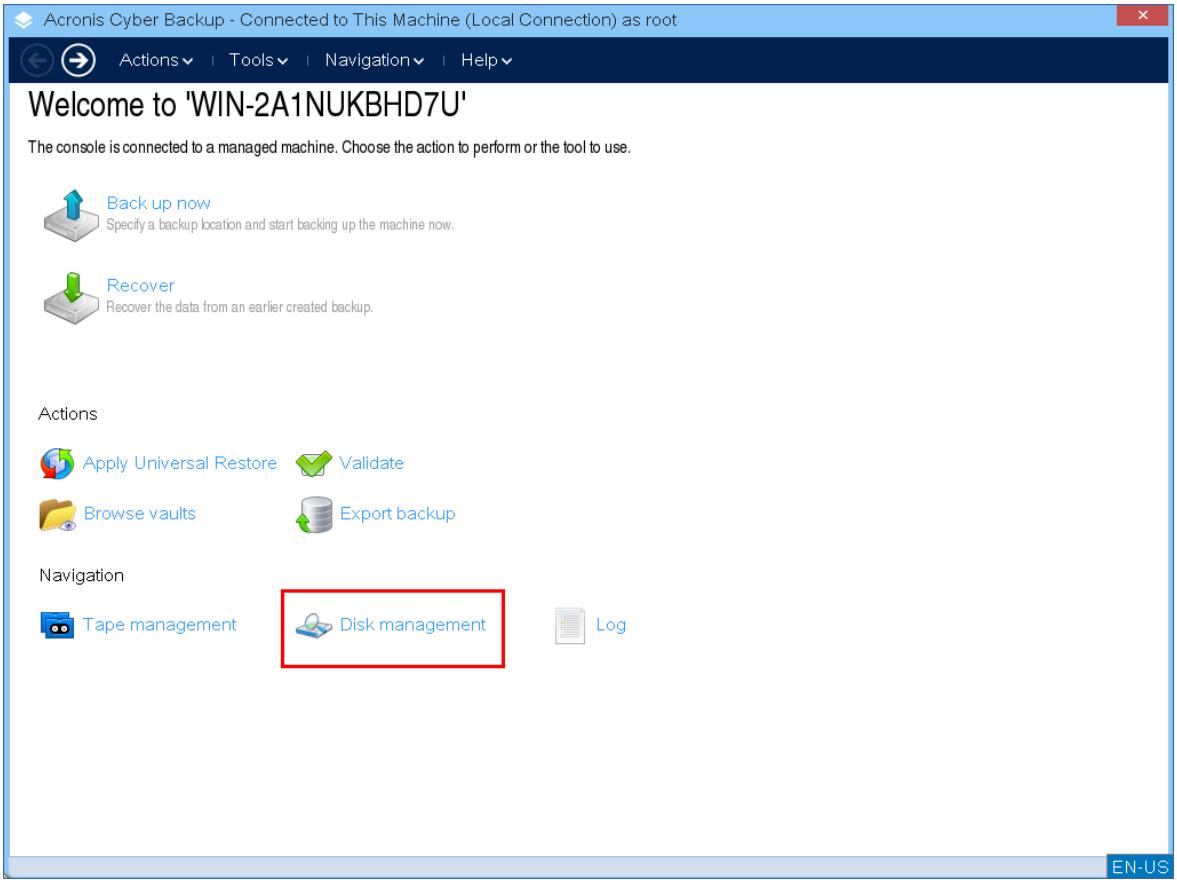
***So können Sie Laufwerke vom Typ 'Basis' mit einem Boot-Medium klonen***

1. Booten Sie mit einem Acronis Boot-Medium.


2. Klicken Sie auf **Diese Maschine lokal verwalten**, wenn Sie ein Laufwerk der lokalen Maschine klonen wollen. Anweisungen für Remote-Verbindungen finden Sie im Abschnitt 'Medien auf dem Management Server registrieren'.

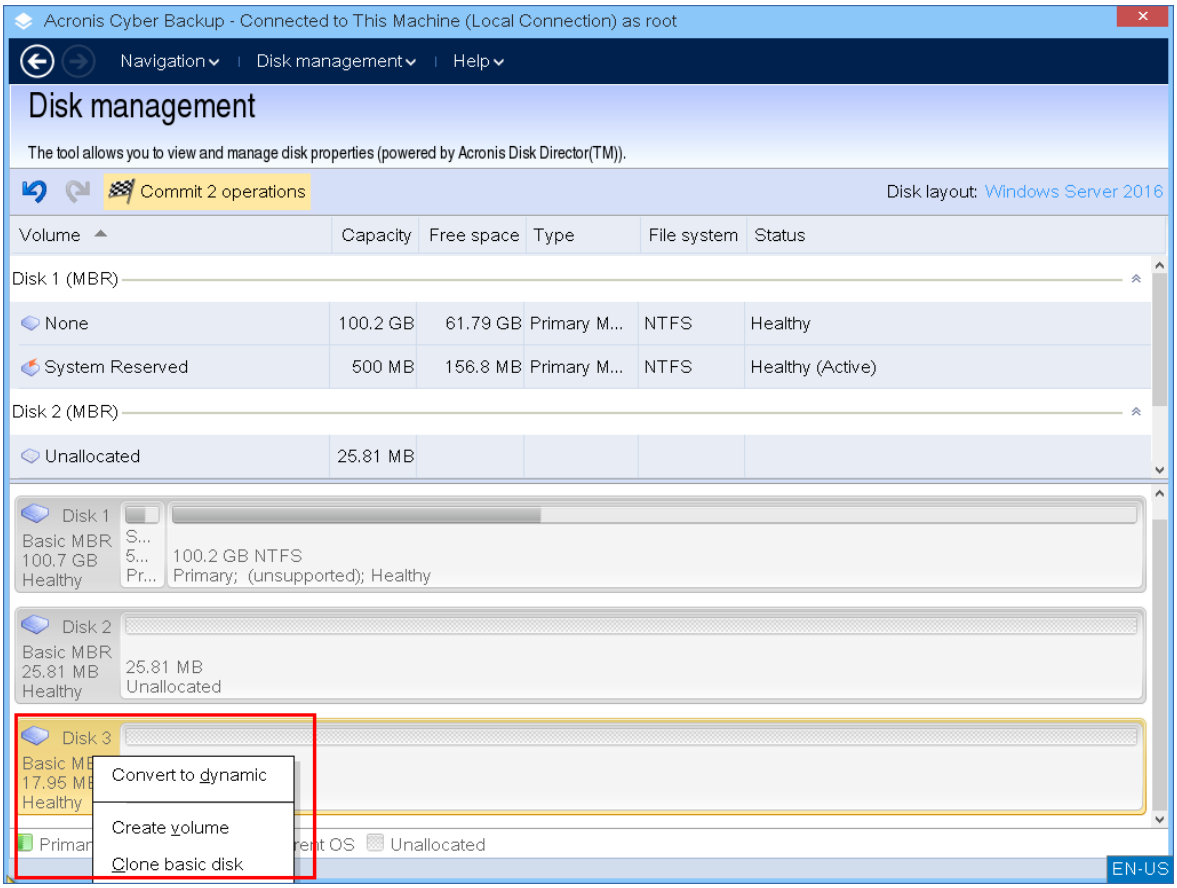



3. Klicken Sie auf **Laufwerksverwaltung**.

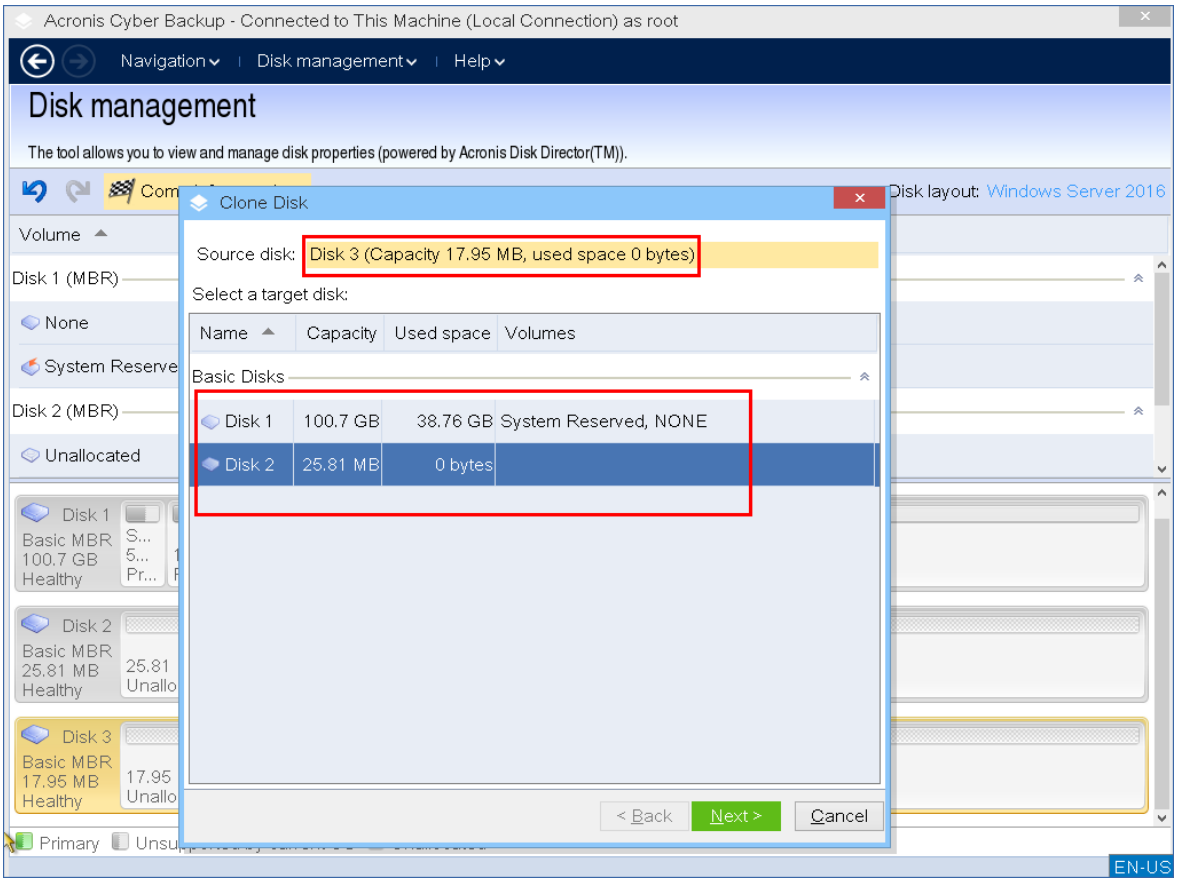


4. Die verfügbaren Laufwerke werden angezeigt. Klicken Sie mit der rechten Maustaste auf das Laufwerk, welches Sie klonen wollen, und klicken Sie dann auf **Basis-Laufwerk klonen**.

**Hinweis**
Sie können nur komplette Laufwerke klonen. Ein Klonen von Volumes (Partitionen) ist nicht verfügbar.

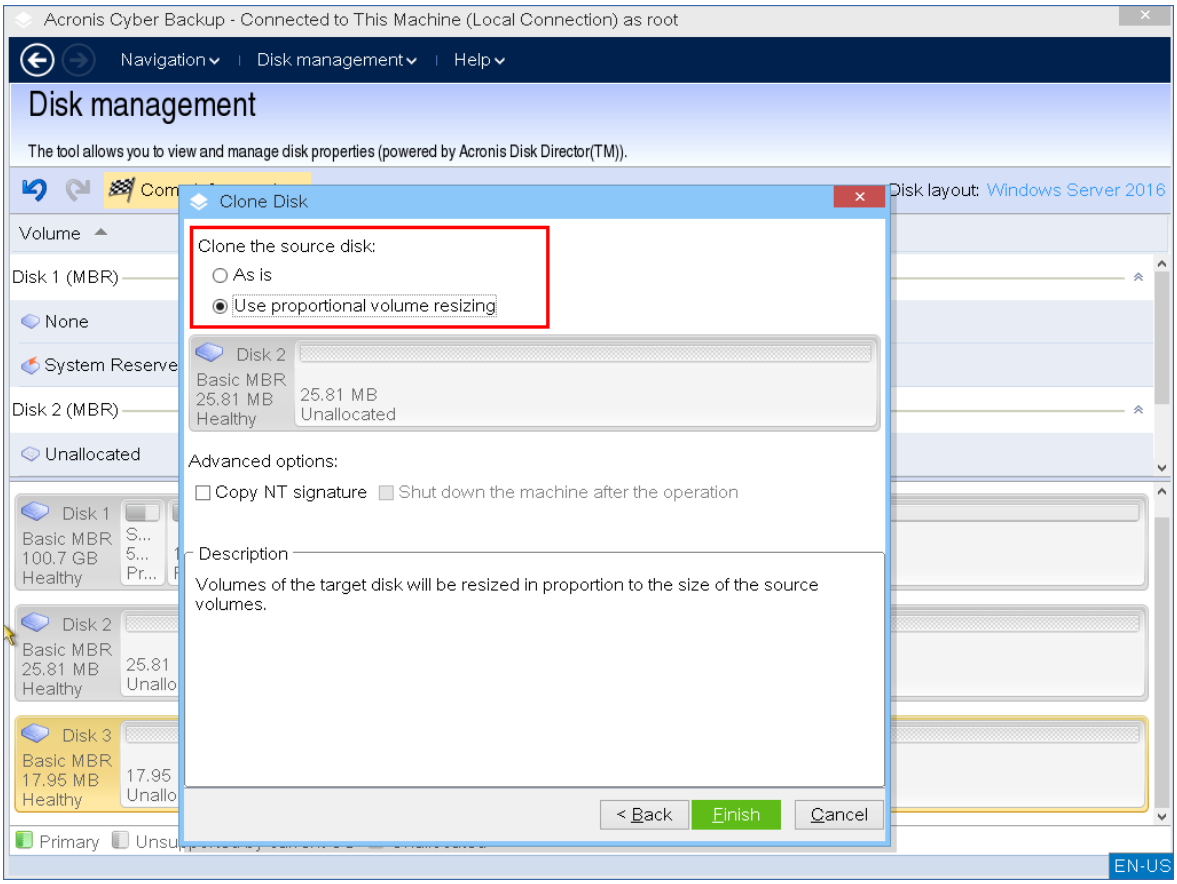



5. Es wird eine Liste der verfügbaren Laufwerke angezeigt. Das Programm erlaubt es Ihnen, ein Ziellaufwerk auszuwählen, wenn dieses groß genug ist, um alle Daten des Quelllaufwerks ohne Verlust aufzunehmen. Wählen Sie ein Ziellaufwerk und klicken Sie dann auf **Weiter**.

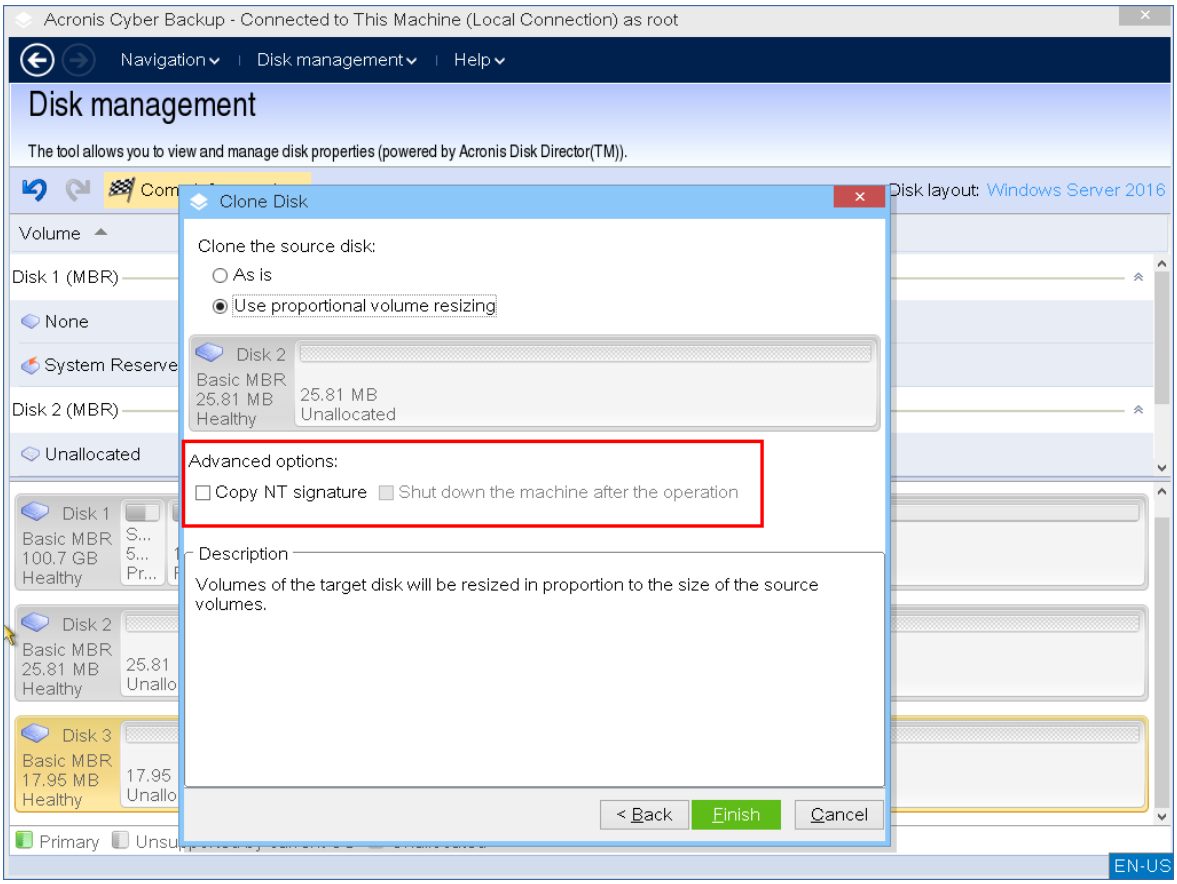



Wenn das Ziellaufwerk größer ist, können Sie das Laufwerk wie vorliegend klonen – oder die Größe der Volumes des Quelllaufwerks proportional so anpassen (Standardoption), dass auf dem Ziel nicht zugeordneter Speicherplatz vermieden wird.
Wenn das Ziellaufwerk kleiner ist, ist nur eine proportionale Größenanpassung möglich. Wenn selbst mit proportionaler Größenänderung kein sicheres Klonen möglich ist, können Sie die Aktion nicht fortsetzen.

**Wichtig**
Wenn sich Daten auf dem Ziellaufwerk befinden, wird Ihnen folgende Warnungmeldung angezeigt: "*Das gewählte Ziellaufwerk ist nicht leer. Die Daten seiner Volumes werden überschrieben.*" Wenn Sie fortfahren, werden alle Daten, die sich derzeit auf dem Zielaufwerk befinden, unwiederbringlich verloren gehen.




6. Bestimmen Sie, ob die NT-Signatur des Quelllaufwerks kopiert werden soll oder nicht.




Wenn Sie ein Laufwerk klonen, das ein System-Volume enthält, müssen Sie auch die Bootfähigkeit des Betriebssystems für das Ziellaufwerk bewahren. Das bedeutet, dass das Betriebssystem System-Laufwerks-Informationen (z.B. Laufwerksbuchstaben) erhalten muss, die zur NT-Festplatten-Signatur passen (welche im Master Boot Record hinterlegt ist). Zwei Laufwerke mit der gleichen NT-Signatur können jedoch nicht korrekt unter ein und demselben Betriebssystem arbeiten.

Wenn auf einer Maschine zwei Laufwerke, die ein System-Volume enthalten, dieselbe NT-Signatur haben, so startet das Betriebssystem vom ersten Laufwerk, erkennt dabei die identische Signatur des zweiten Laufwerks, erzeugt automatisch eine neue eindeutige NT-Signatur und weist diese dann dem zweiten Laufwerk zu. Als Konsequenz verlieren daraufhin alle Volumes des zweiten Laufwerks ihre früheren Laufwerksbuchstaben, werden Verzeichnispfade ungültig und können Programme ihre Dateien nicht mehr finden. Das Betriebssystem auf diesem Laufwerk kann daher auch nicht mehr booten.

Sie können Folgendes tun, um die Bootfähigkeit des Systems auf dem Ziellaufwerk zu bewahren:

a. **Die NT-Signatur kopieren** – versehen Sie das Ziellaufwerk mit der NT-Signatur des Quelllaufwerks, die zu den entsprechenden Registry-Schlüsseln passt, die ebenfalls auf das Ziellaufwerk kopiert werden.

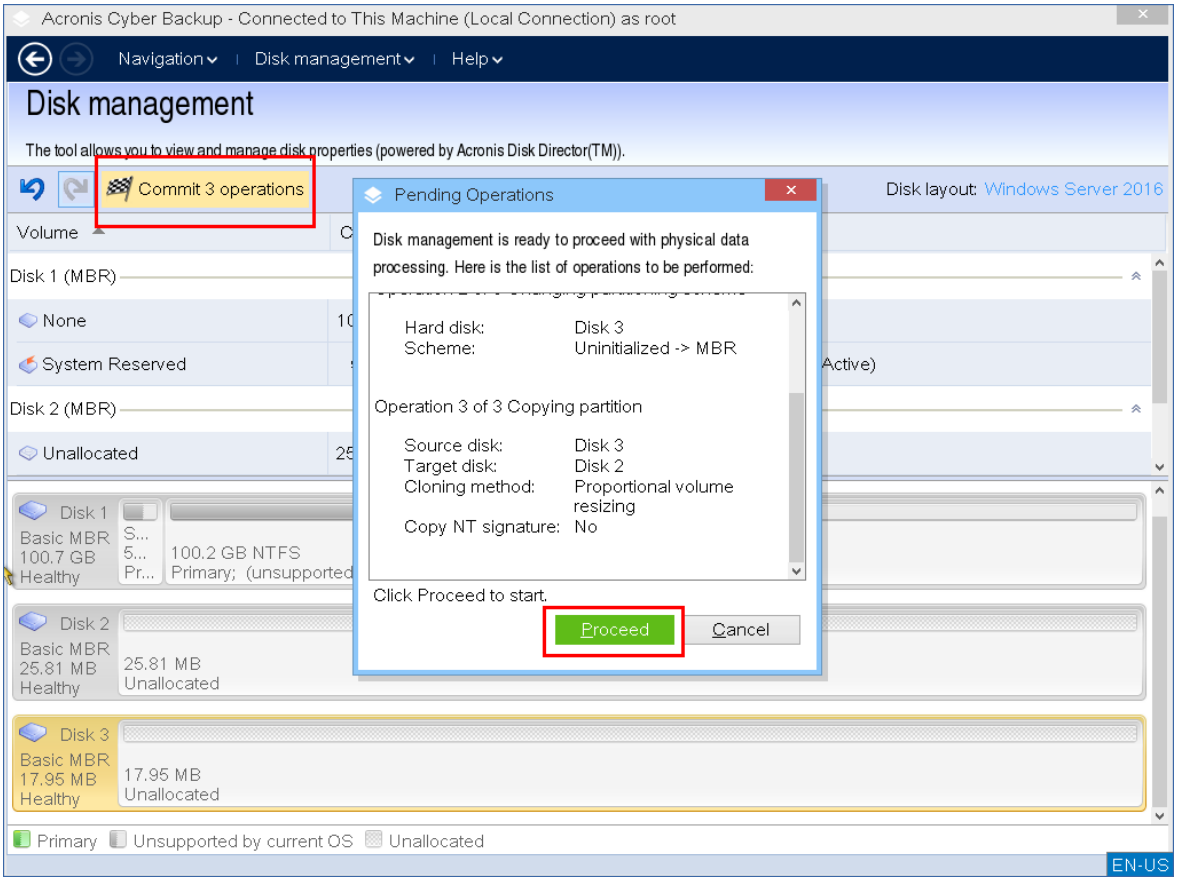
   Aktivieren Sie dafür das Kontrollkästchen **NT-Signatur kopieren**.

   Sie erhalten diese Warnungmeldung: *„Wenn sich auf der Festplatte ein Betriebssystem befindet, so entfernen Sie entweder die Quell- oder Zielfestplatte aus dem Computer, bevor Sie diesen erneut starten. Anderenfalls wird das Betriebssystem von der ersten der beiden Festplatten starten und*

*das Betriebssystem der zweiten Platte seine Bootfähigkeit verlieren."*
Das Kontrollkästchen **Maschine nach Abschluss der Aktion automatisch herunterfahren** wird automatisch ausgewählt und deaktiviert.

b. **Die NT-Signatur belassen** – übernehmen Sie die alte Signatur des Ziellaufwerks und aktualisieren Sie das Betriebssystem entsprechend der Signatur.
Deaktivieren Sie dafür das Kontrollkästchen **NT-Signatur kopieren**.
Das Kontrollkästchen **Maschine nach Abschluss der Aktion automatisch herunterfahren** wird automatisch deaktiviert.

7. Klicken Sie auf **Abschluss**, um die Klon-Aktion zur Liste der ausstehenden Aktionen hinzuzufügen.
8. Klicken Sie zuerst auf **Ausführen** und dann im Fenster **Ausstehende Aktionen** auf **Fortsetzen**.
Wenn Sie das Programm ohne Ausführung der Aktion beenden, wird diese verworfen.




9. Wenn Sie sich für das Kopieren der NT-Signatur entschieden haben, warten Sie, bis der Vorgang abgeschlossen und der Computer ausgeschaltet wurde. Trennen Sie dann entweder das Quell- oder Ziellaufwerk von der Maschine.

## Laufwerk konvertieren: MBR zu GPT

Ein Basis-Laufwerk von MBR zu GPT zu konvertieren, kann angebracht sein, wenn Sie Folgendes benötigen:

- Mehr als vier primäre Volumes auf einem Laufwerk.
- Eine größere Laufwerkszuverlässigkeit gegen möglichen Datenbeschädigungen.

**Wichtig**
Das Basis-MBR-Laufwerk, welches das Boot-Volume des aktuell laufenden Betriebssystems enthält, kann nicht zu GPT konvertiert werden.

***So können Sie ein Basis-Laufwerk von MBR zu GPT konvertieren***

1. Klicken Sie mit der rechten Maustaste auf das entsprechende Laufwerk und wählen Sie dann den Befehl **Zu GPT konvertieren**.
2. Wenn Sie auf **OK** klicken, wird die Aktion 'Laufwerk von MBR zu GPT konvertieren' zur Liste der ausstehenden Aktionen hinzugefügt.
3. Um die hinzugefügte Aktion abschließen zu können, müssen Sie diese noch ausführen lassen. Wenn Sie das Programm ohne Ausführung der Aktion beenden, wird diese verworfen.

**Hinweis**
Ein GPT-partitioniertes Laufwerk reserviert am Ende des partitionierten Bereiches Speicherplatz für einen benötigten Backup-Bereich, der Kopien des GPT-Headers und der Partitionstabelle speichert. Sollte das Laufwerk so voll sein, dass die Volume-Größe nicht automatisch verkleinert werden kann, so wird die 'Konvertierung von MBR zu GPT' fehlschlagen.
Die Aktion kann nicht rückgängig gemacht werden. Wenn Sie ein MBR-Laufwerk mit einem primären Volume haben und dieses Laufwerk zuerst zu GPT und dann wieder zurück zu MBR konvertieren, so erhalten Sie ein logisches Volume, welches Sie nicht mehr als System-Volume verwenden können.

## Dynamischen Datenträger konvertieren: MBR zu GPT

Das Boot-Medium unterstützt bei dynamischen Laufwerken keine direkte Konvertierung von MBR zu GPT. Sie können jedoch folgende Konvertierungen durchführen, um dieses Ziel zu erreichen:

1. MBR Laufwerk konvertieren: Dynamisch zu Basis unter Verwendung der Aktion **Zu Basis konvertieren**.
2. Basis-Laufwerk konvertieren: MBR zu GPT, unter Verwendung der Aktion **Zu GPT konvertieren**.
3. GPT Laufwerk konvertieren: Basis zu Dynamisch durch Verwendung der Aktion **Zu Dynamisch konvertieren**.

## Laufwerk konvertieren: GPT zu MBR

Wenn Sie ein Betriebssystem installieren wollen, das keine GPT-Laufwerke unterstützt, können Sie ein Laufwerk von GPT zu MBR konvertieren.

**Wichtig**
Das Basis-GPT-Laufwerk, welches das Boot-Volume des aktuell laufenden Betriebssystems enthält, kann nicht zu MBR konvertiert werden.

***So konvertieren Sie ein Laufwerk von GPT zu MBR***

1. Klicken Sie mit der rechten Maustaste auf das entsprechende Laufwerk und wählen Sie dann den Befehl **Zu MBR konvertieren**.
2. Wenn Sie auf **OK** klicken, wird die Aktion 'Laufwerk von GPT zu MBR konvertieren' zur Liste der ausstehenden Aktionen hinzugefügt.
3. Um die hinzugefügte Aktion abschließen zu können, müssen Sie diese noch ausführen lassen. Wenn Sie das Programm ohne Ausführung der Aktion beenden, wird diese verworfen.

**Hinweis**
Nach der Aktion werden die Volumes auf diesem Laufwerk zu logischen Volumes. Diese Änderung kann nicht rückgängig gemacht werden.

## Laufwerk konvertieren: Basis zu Dynamisch

Die Konvertierung von einem Basis-Laufwerk zu einem dynamischen Laufwerk kann angebracht sein, wenn Sie:

- Das Laufwerk als Teil einer dynamischen Laufwerksgruppe verwenden wollen
- Eine erhöhte Laufwerkszuverlässigkeit zur Datenspeicherung erreichen wollen

***So können Sie ein Basis-Laufwerk zu einem dynamischen Laufwerk konvertieren***

1. Klicken Sie mit der rechten Maustaste auf zu konvertierende Laufwerk und wählen Sie dann den Befehl **Zu 'Dynamisch' konvertieren**.
2. Klicken Sie auf **OK**.

Die Konvertierung wird umgehend durchgeführt und Ihre Maschine dabei (falls notwendig) neu gestartet.

**Hinweis**
Ein dynamisches Laufwerk belegt das letzte Megabyte des physischen Laufwerks mit einer Datenbank, die eine sogenannte Four-Level-Beschreibung (Volume-Component-Partition-Disk) für jedes dynamische Volume enthält. Sollte sich während der Konvertierung zu 'Dynamisch' herausstellen, dass das Basis-Laufwerk voll ist und daher die Laufwerksgröße nicht automatisch reduziert werden kann, so wird die Konvertierungsaktion fehlschlagen.
Die Konvertierung von Laufwerken, die System-Volumes enthalten, kann einige Zeit dauern – und jeder Stromausfall, jedes unbeabsichtigte Ausschalten oder versehentliche Drücken des Reset-Schalters während der Aktion kann zum Verlust der Bootfähigkeit führen.

Anders als die Datenträgerverwaltung von Windows gewährleistet das Programm die Bootfähigkeit eines **Offline-Betriebssystems** nach der Aktion.

## Laufwerk konvertieren: Dynamisch zu Basis

Eine Rückkonvertierung von dynamischen Laufwerken zu Basis-Laufwerken kann beispielsweise dann angebracht sein, wenn Sie ein Betriebssystem verwenden wollen, welches keine dynamischen

Laufwerke unterstützt.

***So können Sie ein dynamisches Laufwerk zu einem Basis-Laufwerk konvertieren***

1. Klicken Sie mit der rechten Maustaste auf zu konvertierende Laufwerk und wählen Sie dann den Befehl **Zu 'Basis' konvertieren**.
2. Klicken Sie auf **OK**.

Die Konvertierung wird umgehend durchgeführt und Ihre Maschine dabei (falls notwendig) neu gestartet.

**Hinweis**
Diese Aktion ist nicht für dynamische Laufwerke verfügbar, die übergreifende, Stripeset- oder RAID-5-Volumes enthalten.

Nach der Umwandlung werden 8 MB des Laufwerksspeichers für zukünftige Konvertierungen von Basis zu Dynamisch reserviert. Der resultierende 'nicht zugeordnete' Speicherplatz und die anvisierte maximale Volume-Größe können von Fall zu Fall variieren (weil beispielsweise die Größe einer Spiegelung die Größe einer anderen Spiegelung bedingt oder weil die letzten 8 MB Speicherplatz für zukünftige Konvertierungen von Basis zu Dynamisch reserviert werden).

**Hinweis**
Die Konvertierung von Laufwerken, die System-Volumes enthalten, kann einige Zeit dauern – und jeder Stromausfall, jedes unbeabsichtigte Ausschalten oder versehentliche Drücken des Reset-Schalters während der Aktion kann zum Verlust der Bootfähigkeit führen.

Anders als die Datenträgerverwaltung von Windows gewährleistet das Programm:

- Die sichere Konvertierung eines dynamischen Laufwerks zu einem Basis-Laufwerk, sofern dieses Laufwerk Volumes **mit Daten** für einfache und gespiegelte Volumes enthält.
- In Multiboot-Systemen die Bootfähigkeit eines Systems, das während der Aktion **offline** war.

## Volume-Aktionen

Mit einem Boot-Medium können Sie folgende Aktionen mit Volumes durchführen:

- Volume erstellen – Erstellt ein neues Volume
- Volume löschen – Löscht das ausgewählte Volume
- Aktiv setzen – Kennzeichnet das ausgewählte Volume als 'Aktiv', sodass ein hier installiertes Betriebssystem gebootet werden kann.
- Laufwerksbuchstabe ändern – wechselt den Laufwerksbuchstaben des ausgewählten Volumes
- Bezeichnung ändern – ändert die Bezeichnung des ausgewählten Volumes
- Volume formatieren – Formatiert ein Volume mit einem gewünschten Dateisystem

Verschiedene Arten dynamischer Volumes

## Einfaches Volume (Simple)

Ein Volume, das aus freien Speicherplatz eines einzelnen physischen Laufwerks erstellt wurde. Es kann aus einer oder auch mehreren Regionen auf dem Laufwerk bestehen, die durch den LDM (Logical Disk Manager) von Windows virtuell vereint werden. Es bietet keine Vorteile bezüglich Zuverlässigkeit, Geschwindigkeit oder Speicherplatz.

## Übergreifendes Volume (Spanned)

Ein Laufwerk, basierend auf dem freien Speicher mehrerer physischer Laufwerke, die durch den LDM miteinander verbunden sind. Es können bis zu 32 Laufwerke zu einem Volume zusammengefasst werden, um Größenbeschränkungen durch die Hardware zu überwinden. Aber wenn auch nur eines der Laufwerke ausfällt, gehen alle Daten auf dem Volume verloren. Außerdem kann kein Teil eines übergreifenden Volumes entfernt werden, ohne dass das komplette Volume zerstört wird. Daher bietet ein übergreifendes Volume keine bessere Zuverlässigkeit oder bessere E/A-Rate.

## Stripeset-Volume

Ein solches Volume wird auch RAID-0-Volume genannt. Es besteht aus gleichgroßen 'Datenstreifen' (Stripesets), die über jedes Laufwerk, das zum Volume gehört, geschrieben werden. Um ein Stripeset-Volume erstellen zu können, benötigen Sie also zwei oder mehr dynamische Laufwerke. Die Laufwerke in einem Volume vom Typ 'Stripeset' müssen nicht identisch sein, aber auf jedem Laufwerk, das Sie in das Volume aufnehmen wollen, muss ungenutzter Speicher vorhanden sein. Die Größe des Volumes wird durch die Größe des kleinsten Speicherplatzes bestimmt. Der Datenzugriff bei einem Volume vom Typ 'Stripeset' ist üblicherweise schneller als der vergleichbare Zugriff auf ein einzelnes physisches Laufwerk, weil die Eingabe/Ausgabe-Operationen über mehr als ein Laufwerk verteilt werden.

Laufwerke vom Typ 'Stripeset' werden zur Performance-Steigerung und nicht wegen besserer Zuverlässigkeit erstellt, da sie keine redundanten Informationen enthalten.

## Gespiegeltes Volume (Mirrored)

Ein fehlertoleranter Volume-Typ, der auch RAID-1 genannt wird, und dessen Daten auf zwei identischen physischen Laufwerken dupliziert werden. Alle Daten des einen Laufwerks werden zur Schaffung der Datenredundanz auf das andere Laufwerk kopiert. Nahezu jedes Volume kann gespiegelt werden, System- und Boot-Volumes eingeschlossen. Falls eines der Laufwerke ausfällt, kann immer noch auf die Daten der verbliebenen Laufwerke zugegriffen werden. Leider gibt es starke Hardware-Begrenzungen bezüglich Größe und Geschwindigkeit bei der Verwendung von gespiegelten Volumes.

## Gespiegeltes Stripeset-Volume

Ein auch RAID-1+0 genanntes, fehlertolerantes Volume, welches die Vorteile erhöhter E/A-Geschwindigkeit des Typs 'Stripeset' mit der Redundanz beim Typ 'Gespiegelt' kombiniert. Die Spiegelungsarchitektur bedingt jedoch einen Nachteil: ein schlechtes Laufwerk-zu-Volume-Größenverhältnis.

## RAID-5

Ein fehlertolerantes Stripeset-Volume, dessen Daten über eine Zusammenstellung (Array) von drei oder noch mehr Laufwerken quer verteilt sind. Die Laufwerke müssen nicht identisch sein, aber des Laufwerk des Volumes muss über gleich große Blöcke an nicht zugeordnetem Speicherplatz verfügen. Außerdem werden über das Laufwerk-Array auch Paritätsdaten (speziell berechnete Werte, die im Fehlerfall zur Datenrekonstruktion verwendet werden können) verteilt gespeichert. Und diese Paritätsdaten werden immer auf einem anderen Laufwerk als die eigentlichen Daten gespeichert. Sollte eine physische Platte ausfallen, so kann der Anteil des RAID-5-Laufwerks, der auf dieser Festplatte lag, aus den verbliebenen Daten und den Paritätsdaten wiederhergestellt werden. Ein RAID-5-Volume bietet erhöhte Zuverlässigkeit und ermöglicht die Speicherbegrenzungen physischer Laufwerke zu überwinden, wobei das Disk-zu-Volume-Größenverhältnis besser ist als bei Laufwerken vom Typ 'Gespiegelt' (Mirrored).

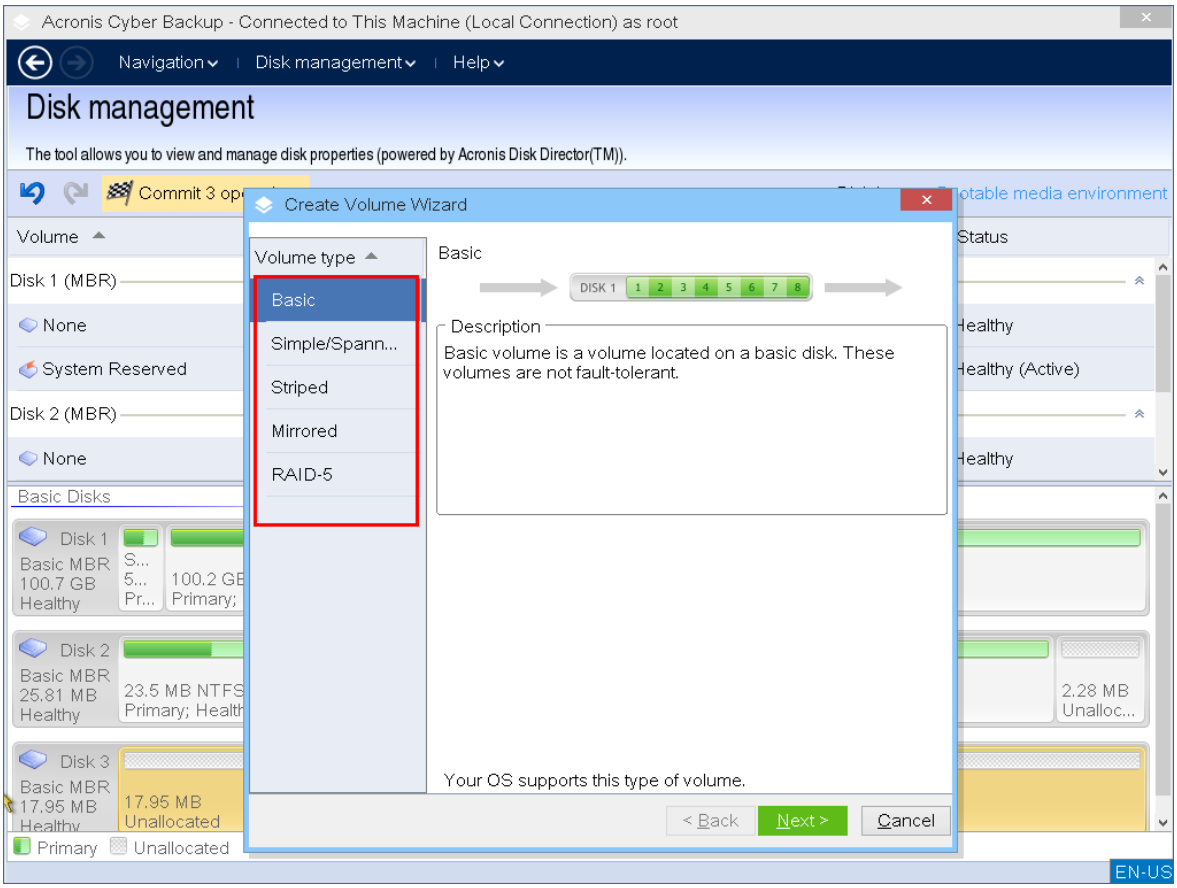
### Ein Volume erstellen

Beispiele, für die Sie ein neues Volume benötigen könnten:

- Um Daten (z.B. ein System) in einem früher erstellten Backup mit exakt derselben Konfiguration wiederherzustellen, wie sie früher vorlagen
- Um Dateien mit ähnlichen Inhalten gemeinsam zu speichern – z.B. Sammlungen von MP3- oder Videodateien auf einem eigenen Volume
- Um Backups (Images) von anderen Laufwerke/Volumes auf einem speziellen Volume zu speichern
- Um ein neues Betriebssystem (oder eine Auslagerungsdatei) auf einem neuen Volume zu speichern
- Um einer Maschine neue Hardware hinzuzufügen

***So können Sie ein Volume erstellen***

1. Klicken Sie bei einem Laufwerk mit der rechten Maustaste auf einen nicht zugewiesenen Speicherplatz – und anschließend auf den Befehl **Volume erstellen**. Der Assistent **Volume erstellen** wird geöffnet.




2. Wählen Sie den gewünschten Volume-Typ. Folgende Optionen sind verfügbar:
   - Basis
   - Einfach/Übergreifend
   - Stripeset
   - Gespiegelt
   - RAID-5

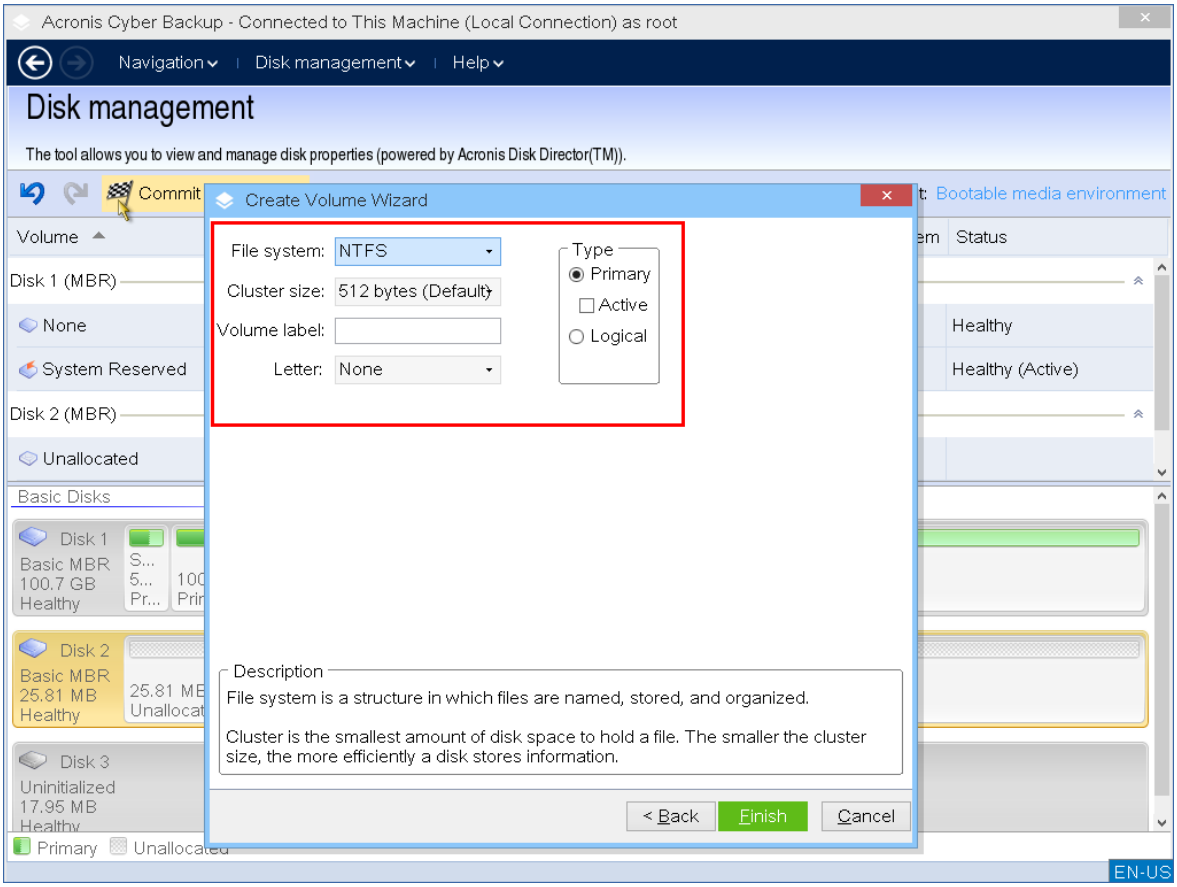
   Sollte das aktuelle Betriebssystem den gewählten Volume-Typ nicht unterstützen, erhalten Sie eine Warnung und die Schaltfläche **Weiter** wird deaktiviert. Sie müssen dann einen anderen Volume-Typ auswählen, um fortfahren zu können.
3. Spezifizieren Sie den nicht zugewiesenen Speicherplatz oder wählen Sie Ziellaufwerke aus.
   - Für ein Basis-Volume: spezifizieren Sie den nicht zugewiesenen Speicherplatz auf dem ausgewählten Laufwerk.
   - Für ein einfaches/übergreifendes Volume: wählen Sie ein oder mehrere Laufwerke aus.
   - Für ein gespiegeltes Volume: wählen Sie zwei Ziellaufwerke aus.
   - Für ein Stripeset-Volume: wählen Sie zwei oder mehr Ziellaufwerke aus.
   - Für ein RAID-5-Volume: wählen Sie drei Ziellaufwerke aus.

   Wenn Sie versuchen, ein **dynamisches** Volume auf einem oder mehreren **Basis**-Laufwerken zu erstellen, erhalten Sie eine Warnmeldung, dass die ausgewählten Laufwerke automatisch zum Typ 'Dynamisch' konvertiert werden.

4. Bestimmen Sie die Volume-Größe.

   Der maximale Wert entspricht normalerweise dem maximal verfügbaren nicht zugeordneten Speicherplatz. In einigen Fällen kann der vorgeschlagene Maximalwert davon abweichen – beispielsweise, wenn die Größe einer Spiegelung die Größe der anderen Spiegelung bestimmt oder wenn die letzten 8 MB des Laufwerks für eine zukünftige Konvertierung des Laufwerks vom Typ 'Basis' zum Typ 'Dynamisch' reserviert wurden.

   Sie können die Position eines neuen Basis-Volumes auf dem Laufwerk festlegen, wenn der nicht zugeordnete Speicherplatz auf dem Laufwerk größer als das betreffende Volume ist.
5. Legen Sie die Volume-Optionen fest.




   Sie können einen **Laufwerksbuchstaben** zuweisen (Standard ist der erste freie Buchstabe im Alphabet) und optional eine **Bezeichnung** für das Volume vergeben (Standard ist: keine Bezeichnung). Sie müssen außerdem das **Dateisystem** und die **Clustergröße** spezifizieren.

   Folgende Dateisystem-Optionen sind verfügbar:

   - FAT16 (deaktiviert, wenn die Volume-Größe auf mehr als 2 GB festgelegt wurde)
   - FAT32 (deaktiviert, wenn die Volume-Größe auf mehr als 2 TB festgelegt wurde)
   - NTFS
   - Volume unformatiert lassen.

   Bei der Wahl der Clustergröße können Sie eine Zahl aus den vorgegebenen Größen auswählen, die für das jeweilige Dateisystem vorgegeben wurden. Die Clustergröße, die standardmäßig vorgeschlagen wird, ist am besten für das Volume und dem ausgewählten Dateisystem geeignet.

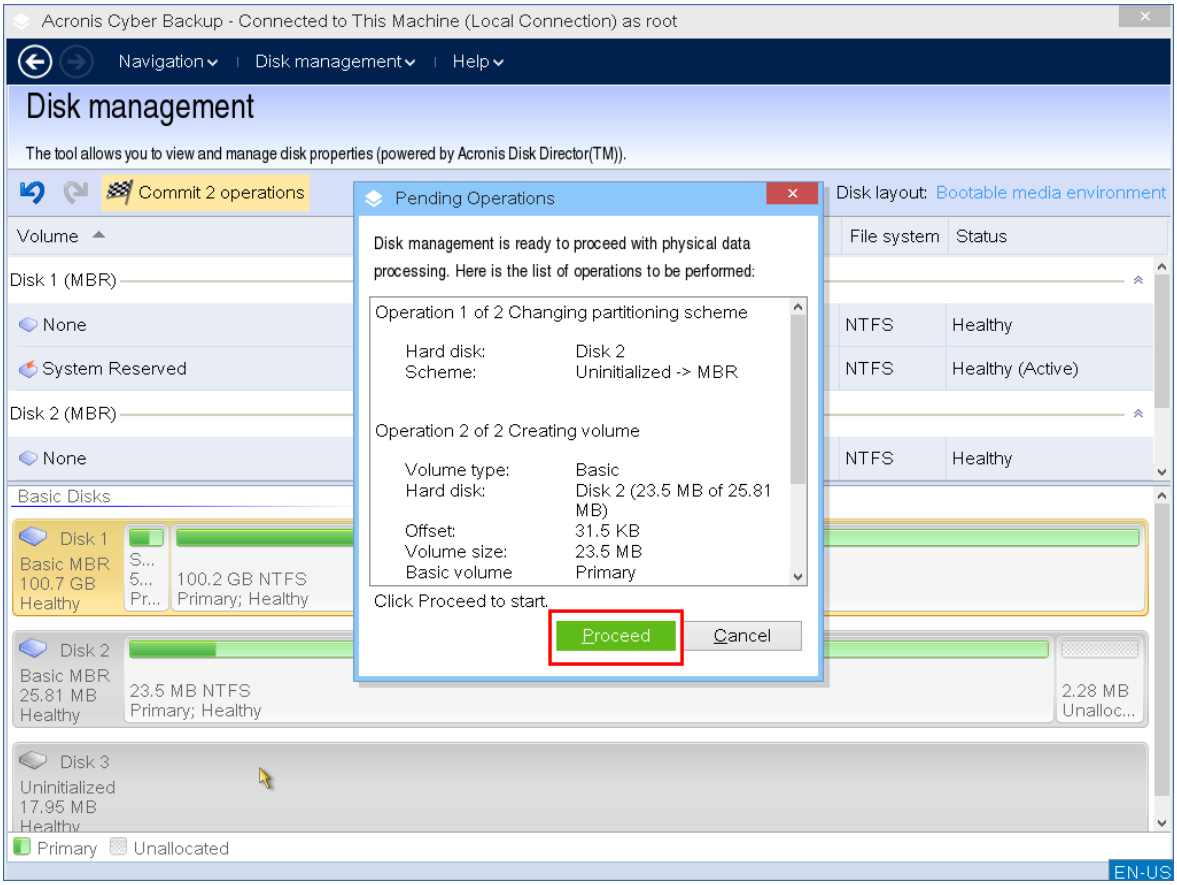
Sollten Sie bei FAT16/FAT32 eine Clustergröße von 64K oder bei NTFS eine Größe von 8-64KB eingestellt haben, so kann Windows das Volume zwar mounten, aber bei manchen Anwendungen (z.B. Setup-Programmen) kann es zu Fehlkalkulationen bei der Laufwerksgrößenberechnung kommen.

Wenn Sie ein Basis-Volume erstellen, das auch zu einem System-Volume gemacht werden kann, können Sie außerdem den Volume-Typ auswählen – **Primär** (**Aktiv primär**) oder **Logisch**. **Primär** ist die übliche Wahl, wenn ein Betriebssystem auf dem Volume installiert werden soll. Wählen Sie **Aktiv** (Standardeinstellung), wenn Sie auf dem Volume ein Betriebssystem installieren wollen, von dem der Computer beim Start direkt bootet. Wenn die Einstellung **Primär** nicht ausgewählt ist, so ist auch die Option **Aktiv** ausgeschaltet. Soll das Volume nur zum Speichern von Daten verwendet werden, so wählen Sie **Logisch**.

**Hinweis**

Ein Basis-Laufwerk kann bis zu vier primäre Volumes enthalten. Sollten diese schon existieren, so muss das Laufwerk zur Erstellung weiterer primärer Volumes in ein dynamisches Volume konvertiert werden – anderenfalls werden die Optionen **Aktiv** und **Primär** deaktiviert und werden Sie nur den Volume-Typ **Logisch** auswählen können.

6. Klicken Sie zuerst auf **Ausführen** und dann im Fenster **Ausstehende Aktionen** auf **Fortsetzen**. Wenn Sie das Programm ohne Ausführung der Aktion beenden, wird diese verworfen.



## Ein Volume löschen

***So können Sie ein Volume löschen***

1. Klicken Sie mit der rechten Maustaste auf das Volume, das Sie löschen wollen.
2. Klicken Sie auf **Volume löschen**.

   **Hinweis**
   Alle Informationen auf diesem Volume werden unwiderruflich verloren gehen.

3. Wenn Sie auf **OK** klicken, wird der Befehl zur Liste ausstehender Aktionen hinzugefügt.
4. Um die hinzugefügte Aktion abschließen zu können, müssen Sie diese noch ausführen lassen. Wenn Sie das Programm ohne Ausführung der Aktion beenden, wird diese verworfen.

Nachdem ein Volume gelöscht wurde, wird dessen Speicherplatz zum nicht zugeordneten Speicherplatz hinzugefügt. Sie können diesen verwenden, um ein neues Volume zu erstellen oder Typ eines anderen Volumes zu ändern.

## Aktives Volume setzen

Wenn Sie über mehrere primäre Volumes verfügen, dann müssen Sie eines davon als Boot-Volume spezifizieren. Dafür müssen Sie das Volume als 'Aktiv' festlegen. Ein Laufwerk darf jeweils nur ein aktives Volume haben.

***So können Sie ein Volume als 'Aktiv' festlegen:***

1. Klicken Sie bei einem MBR-Basis-Laufwerk mit der rechten Maustaste auf das gewünschte primäre Volume und anschließend auf den Befehl **Als 'Aktiv' markieren**.
   Sofern im System kein anderes aktives Volume vorliegt, wird die Kennzeichnung des Volumes als 'aktiv' zur Liste der ausstehenden Aktionen hinzugefügt. Sollte im System ein anderes Volume aktiv sein, so erhalten Sie eine Warnmeldung, dass das bisherige Volume zuerst als passiv ('Nicht aktiv') markiert werden muss.

   **Hinweis**
   Wenn Sie das neue Volume auf 'aktiv' setzen, ändert sich möglicherweise der Laufwerksbuchstabe des bisherigen aktiven Volumes und werden einige installierte Programme möglicherweise nicht mehr ausgeführt.

2. Wenn Sie auf **OK** klicken, wird der Befehl zur Liste ausstehender Aktionen hinzugefügt.

   **Hinweis**
   Selbst wenn ein Betriebssystem auf dem neuen aktiven Volume liegt, kann es unter Umständen sein, dass der Computer dennoch nicht von diesem booten kann. Sie müssen Ihre Entscheidung bestätigen, das neue Volume als aktiv einzustellen, bestätigen.

3. Um die hinzugefügte Aktion abschließen zu können, müssen Sie diese noch ausführen lassen. Wenn Sie das Programm ohne Ausführung der Aktion beenden, wird diese verworfen.

## Laufwerksbuchstaben ändern

Windows-Betriebssysteme weisen Laufwerken ihre Buchstaben während des Startvorgangs zu. Diese Laufwerksbuchstaben werden vom Betriebssystem und Anwendungsprogrammen verwendet, um Dateien und Ordner auf den Volumes zu finden. Das Hinzufügen neuer Laufwerke sowie das Erstellen oder Löschen von Volumes auf existierenden Laufwerken kann Ihre Systemkonfiguration ändern. Das kann zur Folge haben, dass manche Anwendungsprogramme nicht mehr normal funktionieren oder Benutzerdateien nicht mehr automatisch gefunden bzw. geöffnet werden können. Um dies zu verhindern, können Sie die Buchstaben, die den Volumes vom Betriebssystem automatisch zugeordnet wurden, manuell ändern.

***So können Sie einen Laufwerksbuchstaben ändern, der einem Volume vom Betriebssystem zugewiesen wurde***

1. Klicken Sie mit der rechten Maustaste auf das gewünschte Volume und wählen Sie den Befehl **Laufwerksbuchstabe ändern**.
2. Wählen Sie im Dialog **Laufwerksbuchstabe ändern** einen neuen Laufwerksbuchstaben aus.
3. Wenn Sie auf **OK** klicken, wird der Befehl für die Laufwerksbuchstaben-Zuweisung zur Liste der ausstehenden Aktionen hinzugefügt.
4. Um die hinzugefügte Aktion abschließen zu können, müssen Sie diese noch ausführen lassen. Wenn Sie das Programm ohne Ausführung der Aktion beenden, wird diese verworfen.

## Volume-Bezeichnung ändern

Die Volume-Bezeichnung ist ein optionales Attribut. Es handelt sich um einen Namen, der dem Volume zur leichteren Erkennung zugewiesen wird.

***So ändern Sie eine Volume-Bezeichnung***

1. Klicken Sie mit der rechten Maustaste auf das gewünschte Volume und wählen Sie den Befehl **Bezeichnung ändern**.
2. Geben Sie in das Textfeld des Dialoges **Bezeichnung ändern** den neuen Laufwerksnamen ein.
3. Wenn Sie auf **OK** klicken, wird der Befehl zur Änderung der Volume-Bezeichnung zur Liste der ausstehenden Aktionen hinzugefügt.
4. Um die hinzugefügte Aktion abschließen zu können, müssen Sie diese noch ausführen lassen. Wenn Sie das Programm ohne Ausführung der Aktion beenden, wird diese verworfen.

## Volume formatieren

Fälle, in denen es angebracht sein kann, ein Volume mit einem neuen Dateisystem zu formatieren:

- Um zusätzlichen Speicherplatz zu gewinnen, der zuvor durch eine ungünstige Clustergröße auf FAT16- oder FAT32-Dateisystemen verloren ging.
- Um auf dem Volume befindliche Daten auf schnelle und relativ zuverlässige Art zu zerstören

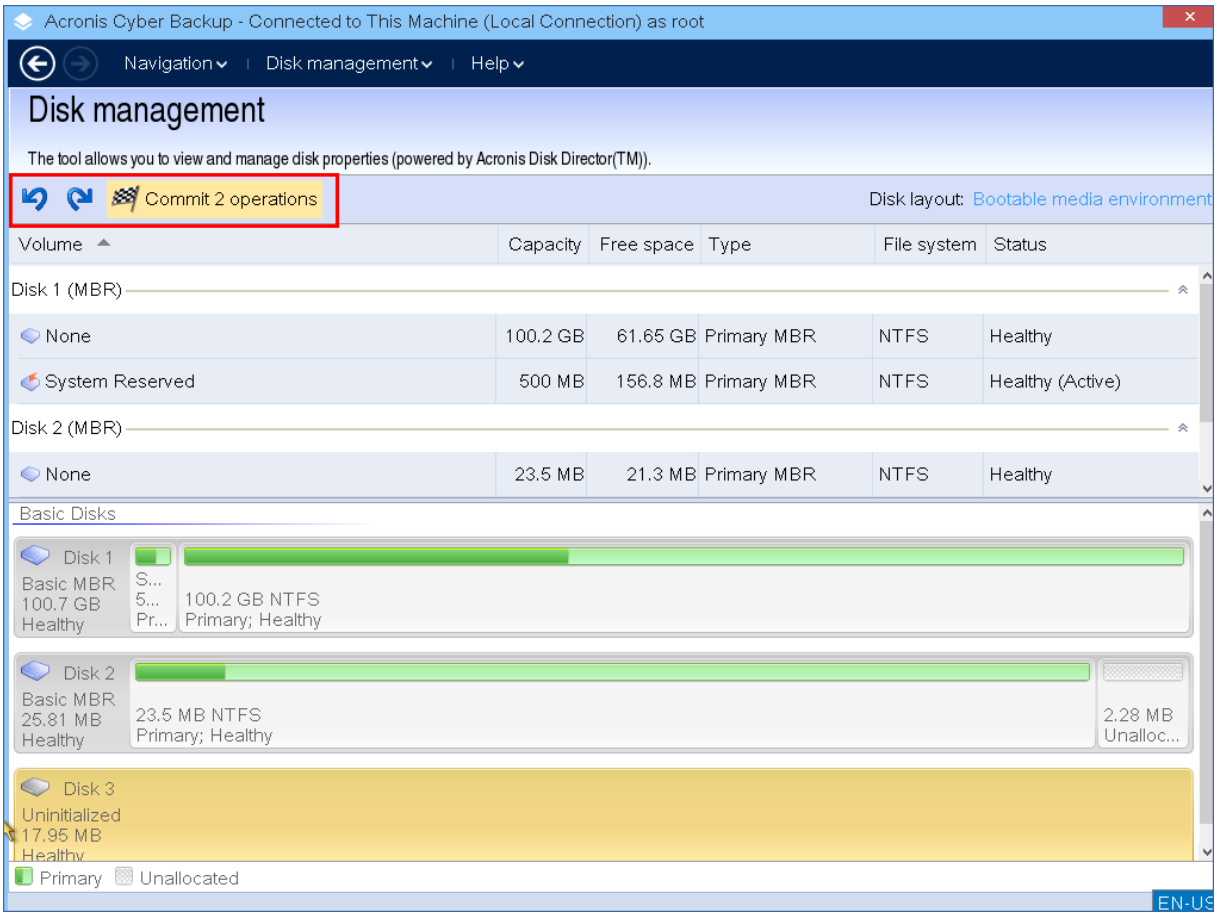
***So können Sie ein Volume formatieren:***

1. Klicken Sie mit der rechten Maustaste auf das gewünschte Volume und wählen Sie den Befehl **Formatieren**.
2. Wählen Sie die Clustergröße und das Dateisystem aus. Folgende Dateisystem-Optionen sind verfügbar:
   - FAT16 (deaktiviert, wenn die Volume-Größe auf mehr als 2 GB festgelegt wurde)
   - FAT32 (deaktiviert, wenn die Volume-Größe auf mehr als 2 TB festgelegt wurde)
   - NTFS
3. Wenn Sie auf **OK** klicken, wird der Befehl zum Formatieren des Volumes zur Liste ausstehender Aktionen hinzugefügt.
4. Um die hinzugefügte Aktion abschließen zu können, müssen Sie diese noch ausführen lassen. Wenn Sie das Programm ohne Ausführung der Aktion beenden, wird diese verworfen.

## Ausstehende Aktionen

Alle Aktionen gelten solange als ausstehend, bis Sie auf den Befehl **Ausführen** klicken und dessen Durchführung noch einmal bestätigen. Auf diese Weise können Sie alle geplanten Aktionen kontrollieren, die gewünschten Änderungen noch einmal überprüfen und – sofern erforderlich – jede Aktion vor der Ausführung wieder abbrechen.

Sie finden in der Ansicht **Laufwerksverwaltung** eine Symbolleiste, die Icons für die Befehle **Rückgängig**, **Wiederherstellen** und **Ausführen** enthält, welche speziell für die ausstehenden Aktionen gedacht sind. Sie können diese Befehle auch über das Menü **Laufwerksverwaltung** starten.




Alle geplanten Operationen werden zur Liste der ausstehenden Aktionen hinzugefügt.

Über den Befehl **Rückgängig** können Sie je den letzten Befehl in dieser Liste zurücksetzen. Solange die Liste nicht leer ist, steht dieser Befehl zur Verfügung.

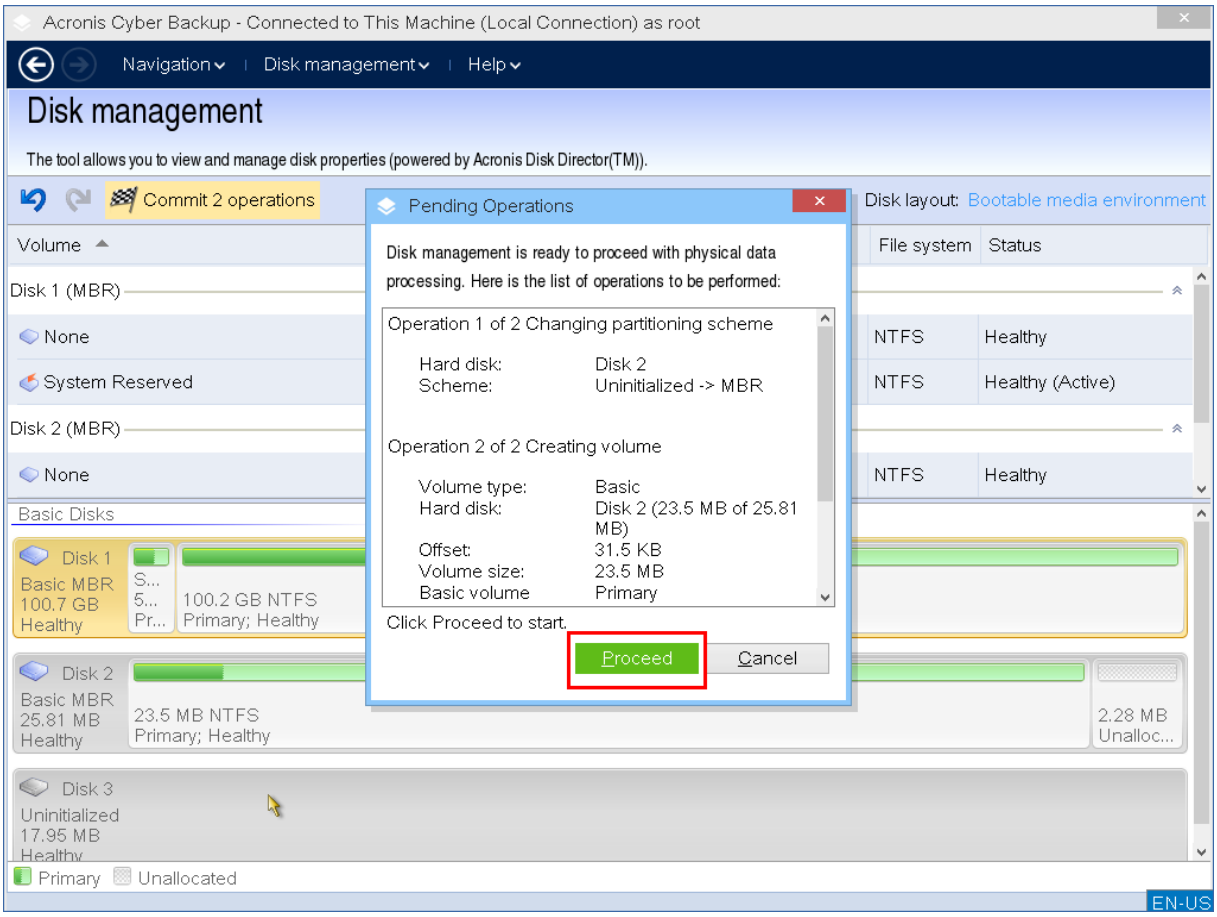
Über den Befehl **Wiederherstellen** können Sie die letzte ausstehende und zuvor rückgängig gemachte Aktion wieder zurückholen.

Der Befehl **Ausführen** bringt Sie zum Fenster **Ausstehende Aktionen**, in dem Sie die Liste dieser ausstehenden Aktionen noch einmal einsehen können.

Wenn Sie die Ausführung der Befehle starten wollen, klicken Sie auf **Fertig stellen**.

**Hinweis**
Sobald Sie den Befehl **Fertig stellen** gewählt haben, können Sie keinen der Befehle bzw. Aktionen mehr rückgängig machen!

Wenn Sie die Ausführung nicht umsetzen wollen, klicken Sie auf **Abbrechen**. In dem Fall wird die Liste der ausstehenden Aktionen nicht verändert. Wenn Sie das Programm ohne Ausführung der ausstehenden Aktionen beenden, werden diese alle endgültig verworfen.




# Remote-Aktionen mit einem Boot-Medium

Um das Boot-Medium in der Cyber Protect-Konsole sehen zu können, müssen Sie es zuerst registrieren (wie im Abschnitt '"Medien auf dem Management Server registrieren" (S. 409)' beschrieben).

Wenn Sie das Medium in der Cyber Protect-Konsole registriert haben, wird es unter **Geräte** –> **Boot-Medium** angezeigt.

Sie können das Medium dann über die Weboberfläche remote verwalten. Sie können beispielsweise Daten wiederherstellen. die Maschine (die mit dem Medium gebootet wurde) neu starten oder herunterfahren oder sich Informationen, Aktivitäten und Alarmmeldungen zu dem Medium anzeigen lassen.

***So können Sie Dateien oder Ordner mit einem Boot-Medium aus der Ferne wiederherstellen***

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte** –> **Boot-Medium**.
1. Wählen Sie das Medium aus, das Sie für die Datenwiederherstellung verwenden wollen.
2. Klicken Sie auf **Recovery**.
3. Wählen Sie zuerst den Speicherort und dann das gewünschte Backup aus. Beachten Sie dabei, dass die Backups nach Speicherorten gefiltert werden.

4. Wählen Sie den Recovery-Punkt aus und klicken Sie dann auf **Dateien/Ordner wiederherstellen**.
5. Wechseln Sie zum benötigten Ordner oder verwenden Sie die Suchleiste, um eine Liste der gewünschten Dateien und Ordner abzurufen.

   Sie können ein oder mehrere Platzhalterzeichen (* und ?) verwenden. Ausführlichere Informationen über die Verwendung von Platzhalterzeichen finden Sie im Abschnitt '"Dateifilter" (S. 291)'.
6. Wählen Sie die wiederherzustellenden Dateien aus und klicken Sie dann auf **Recovery**.
7. Wählen Sie bei **Pfad** das gewünschte Ziel für die Wiederherstellung.
8. [Optional] Wenn Sie erweiterte Konfigurationsmöglichkeiten für die Wiederherstellung benötigen, klicken Sie auf **Recovery-Optionen**. Weitere Informationen dazu finden Sie im Abschnitt '"Recovery-Optionen" (S. 352)'.
9. Klicken Sie auf **Recovery starten**.
10. Wählen Sie eine der folgenden Optionen zum Überschreiben:
    - **Vorhandene Dateien überschreiben**
    - **Vorhandene Datei überschreiben, wenn diese älter ist**
    - **Vorhandene Dateien nicht überschreiben**

    Bestimmen Sie, ob ein automatischer Neustart der Maschine erfolgen soll.
11. Klicken Sie auf **Fortsetzen**, um die Wiederherstellung zu starten. Der Recovery-Fortschritt wird auf der Registerkarte **Aktivitäten** angezeigt.

***So können Sie Laufwerke, Volumes oder komplette Maschinen mit einem Boot-Medium aus der Ferne wiederherstellen***

1. Gehen Sie auf der Registerkarte **Geräte** zur Gruppe **Boot-Medium** und wählen Sie dann das Medium aus, das Sie für die Datenwiederherstellung verwenden wollen.
2. Klicken Sie auf **Recovery**.
3. Wählen Sie zuerst den Speicherort und dann das gewünschte Backup aus. Beachten Sie dabei, dass die Backups nach Speicherorten gefiltert werden.
4. Wählen Sie den Recovery-Punkt aus und klicken Sie dann auf **Recovery** –> **Komplette Maschine**.

   Bei Bedarf können Sie die Zuordnung der Zielmaschinen bzw. ihrer Volumes konfigurieren, wie im Abschnitt '"Eine physische Maschine wiederherstellen" (S. 330)' beschrieben.
5. Wenn Sie erweiterte Konfigurationsmöglichkeiten für die Wiederherstellung benötigen, klicken Sie auf **Recovery-Optionen**. Weitere Informationen dazu finden Sie im Abschnitt '"Recovery-Optionen" (S. 352)'.
6. Klicken Sie auf **Recovery starten**.
7. Bestätigen Sie, dass die Daten auf den Laufwerken durch die Datenversionen überschrieben werden sollen, die im Backup vorliegen. Bestimmen Sie, ob ein automatischer Neustart der Maschine erfolgen soll.
8. Der Recovery-Fortschritt wird auf der Registerkarte **Aktivitäten** angezeigt.

***So können Sie die gebootete Maschine aus der Ferne neu starten***

1. Gehen Sie auf der Registerkarte **Geräte** zur Gruppe **Boot-Medium** und wählen Sie dann das Medium aus, das Sie für die Datenwiederherstellung verwenden wollen.
2. Klicken Sie auf **Neustart**.
3. Bestätigen Sie, dass Sie die Maschine, die mit dem Medium gebootet wurde, neu starten wollen.

***So können Sie die gebootete Maschine aus der Ferne herunterfahren***

1. Gehen Sie auf der Registerkarte **Geräte** zur Gruppe **Boot-Medium** und wählen Sie dann das Medium aus, das Sie für die Datenwiederherstellung verwenden wollen.
2. Klicken Sie auf **Herunterfahren**.
3. Bestätigen Sie, dass Sie die Maschine, die mit dem Medium gebootet wurde, herunterfahren wollen.

***So können Sie sich Informationen über das Boot-Medium anzeigen lassen***

1. Gehen Sie auf der Registerkarte **Geräte** zur Gruppe **Boot-Medium** und wählen Sie dann das Medium aus, das Sie für die Datenwiederherstellung verwenden wollen.
2. Klicken Sie auf **Details**, **Aktivitäten** oder **Alarmmeldungen**, um die entsprechenden Informationen einzusehen.

***So können Sie ein Boot-Medium aus der Ferne löschen***

1. Gehen Sie auf der Registerkarte **Geräte** zur Gruppe **Boot-Medium** und wählen Sie dann das Medium aus, das Sie für die Datenwiederherstellung verwenden wollen.
2. Klicken Sie auf **Löschen**, um das Boot-Medium aus der Cyber Protect-Konsole zu entfernen.
3. Bestätigen Sie, dass Sie das Boot-Medium löschen wollen.

# iSCSI-Geräte konfigurieren

Dieser Abschnitt beschreibt, wie iSCSI-Geräte (Internet Small Computer System Interface) bei der Arbeit mit bootfähigen Medien konfiguriert werden. Nachdem Sie die unteren Schritte durchgeführt haben, können Sie die Geräte so verwenden, als wären sie lokal an der per Boot-Medium gestarteten Maschine angeschlossen.

Ein **iSCSI-Zielserver** (oder **Zielportal**) ist ein Server, der ein iSCSI-Gerät hostet. Ein **iSCSI-Ziel** ist eine Komponente auf einem Zielserver. Sie gibt das Gerät frei und listet die iSCSI-Initiatoren auf, die auf das Gerät zugreifen dürfen. Ein **iSCSI-Initiator** ist eine Komponente auf einer Maschine. Sie ermöglicht das Zusammenspiel zwischen der Maschine und einem iSCSI-Ziel. Wenn Sie auf einer per Boot-Medium gestarteten Maschine den Zugriff auf ein iSCSI-Gerät konfigurieren wollen, müssen Sie das iSCSI-Zielportal des Geräts und einen der im Ziel aufgelisteten iSCSI-Initiatoren spezifizieren. Wenn sich das Ziel mehrere Geräte teilt, erhalten Sie Zugriff auf alle diese Geräte.

***So fügen Sie ein iSCSI-Gerät in einem Linux-basierten Boot-Medium hinzu***

1. Klicken Sie auf **Extras** –> **iSCSI/NDAS-Geräte konfigurieren**.
2. Klicken Sie auf **Host hinzufügen**.
3. Spezifizieren Sie die IP-Adresse und den Port des iSCSI-Zielportals sowie den Namen eines iSCSI-Initiators, der auf das Gerät zugreifen darf.
4. Benötigt der Host eine Authentifizierung, dann geben Sie Benutzernamen und Kennwort ein.
5. Klicken Sie auf **OK**.
6. Wählen Sie das iSCSI-Ziel aus der Liste und klicken Sie dann auf **Verbinden**.
7. Wenn in den Einstellungen des iSCSI-Ziels eine CHAP-Authentifizierung aktiviert ist, werden Sie aufgefordert, Anmeldedaten für den Zugriff auf das iSCSI-Ziel einzugeben. Spezifizieren Sie denselben Benutzernamen und geheimen Zielschlüssel wie in den Einstellungen des iSCSI-Ziels. Klicken Sie auf **OK**.
8. Klicken Sie auf **Schließen**, um das Fenster zu schließen.

***So fügen Sie ein iSCSI-Gerät in einem PE-basierten Boot-Medium hinzu***

1. Klicken Sie auf **Extras** –> **iSCSI-Setup ausführen**.
2. Klicken Sie auf die Registerkarte **Suche**.
3. Klicken Sie unter **Zielportale** auf **Hinzufügen** und spezifizieren Sie die IP-Adresse und den Port des iSCSI-Zielportals. Klicken Sie auf **OK**.
4. Klicken Sie in der Registerkarte **Allgemein** auf **Ändern** und spezifizieren Sie den Namen eines iSCSI-Initiators, der auf das Gerät zugreifen darf.
5. Klicken Sie in der Registerkarte **Ziele** auf **Aktualisieren**, wählen Sie das iSCSI-Gerät Ziel aus der Liste aus und klicken Sie dann auf **Verbinden**. Klicken Sie auf **OK**, um eine Verbindung mit dem iSCSI-Ziel herzustellen.
6. Wenn in den Einstellungen des iSCSI-Ziels eine CHAP-Authentifizierung aktiviert ist, wird Ihnen ein **Authentifizierungfehler** angezeigt. Klicken Sie in diesem Fall zuerst auf **Verbinden** und dann auf **Erweitert**. Aktivieren Sie anschließend das Kontrollkästchen **CHAP-Anmeldung aktivieren** und spezifizieren Sie dann denselben Benutzernamen und geheimen Zielschlüssel wie in den Einstellungen des iSCSI-Ziels. Klicken Sie auf **OK**, um das Fenster zu schließen, und dann erneut auf **OK**, um die Verbindung mit dem iSCSI-Ziel herzustellen.
7. Klicken Sie auf **OK**, um das Fenster zu schließen.

# Startup Recovery Manager

Der Startup Recovery Manager ist eine bootfähige Komponente, die auf Ihrem Festplattenlaufwerk gespeichert ist. Mit dem Startup Recovery Manager können Sie eine spezielle bootfähige Notfallumgebung starten, ohne ein klassisches physisches Boot-Medium zu benötigen.

Der Startup Recovery Manager ist besonders für Benutzer nützlich, die häufiger auf Reisen sind. Wenn ein Fehler auftritt, booten Sie die Maschine einfach neu und drücken Sie die Taste 'F11', sobald die Meldung '**F11 druecken, um den Acronis Startup Recovery Manager zu starten...**' erscheint. Das Programm wird daraufhin gestartet und Sie können mit einer Wiederherstellung

beginnen. 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 während des Boot-Vorgangs zu drücken.

Sie können mit dem Startup Recovery Manager natürlich auch Backups erstellen (wenn Sie unterwegs sind).

Um den Startup Recovery Manager verwenden zu können, müssen Sie ihn zuerst aktivieren. Dadurch aktivieren Sie die Anzeige '**F11 druecken, um den Acronis Startup Recovery Manager zu starten**' während des Boot-Vorgangs (oder fügen Sie das Element '**Startup Recovery Manager**' dem GRUB-Menü hinzu, wenn Sie den GRUB-Boot-Loader verwenden).

**Hinweis**
Wenn Sie den Startup Recovery Manager auf einer Maschine mit unverschlüsseltem System-Volume aktivieren wollen, muss die Maschine über mindestens 100 MB an freiem Speicherplatz verfügen. Wiederherstellungsaktionen, bei denen ein Neustart der Maschine erforderlich ist, benötigen zusätzliche 100 MB.

Sie können das Startup Recovery Manager auf einer Maschine aktivieren, die ein per BitLocker verschlüsseltes Volume hat, sofern diese Maschine mindestens noch ein weiteres, nicht verschlüsseltes Volume hat. Dieses unverschlüsselte Volume muss über mindestens 500 MB an freiem Speicherplatz verfügen. Für Wiederherstellungsaktionen, bei denen auch ein Neustart der Maschine erforderlich ist, muss die Maschine ebenfalls über weitere 500 MB an freiem Speicherplatz verfügen.

**Wichtig**
Wenn der Startup Recovery Manager nicht aktiviert werden kann, werden Backup-Aktionen, die One-Click-Recovery-Backups erstellen, fehlschlagen.

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 Drittanbietern) installiert haben, müssen Sie diese möglicherweise reaktivieren.

Wenn Sie unter Linux einen anderen Boot-Loader als GRUB verwenden (wie beispielsweise 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.

## Startup Recovery Manager aktivieren

Auf einer Maschine, auf welcher der Agent für Windows oder der Agent für Linux ausgeführt wird, können Sie den Startup Recovery Manager über die Cyber Protect-Webkonsole aktivieren.

***So können Sie den Startup Recovery Manager in der Cyber Protect Webkonsole 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 **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.

## Startup Recovery Manager deaktivieren

Wenn Sie Startup Recovery Manager deaktivieren wollen, müssen Sie die Aktivierungsprozedur wiederholen und dann die jeweils entgegengesetzten Aktionen auswählen. Mit der Deaktivierung wird die Boot-Meldung '**F11 druecken, um den Acronis Startup Recovery Manager zu starten**' (oder der entsprechende Menü-Eintrag von GRUB) wieder entfernt.

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

# Acronis PXE Server

Der Acronis PXE Server ermöglicht es, auf entsprechenden Maschinen die bootfähigen Komponenten von Acronis über das Netzwerk zu booten.

Netzwerk-Booten:

- eliminiert die Notwendigkeit eines Technikers vor Ort, um das bootfähige Medium in das zu bootende System einzulegen
- reduziert bei Gruppen-Operationen die zum Booten mehrerer Maschinen benötigte Zeit (im Vergleich zu physischen Bootmedien).

Die bootfähigen Komponenten werden mithilfe des Acronis Bootable Media Builders zum Acronis PXE Server hochgeladen. Um eine bootfähige Komponente hochzuladen, starten Sie den Bootable Media Builder und befolgen Sie dann die im Abschnitt 'Linux-basiertes Boot-Medium' aufgeführten Schritt-für-Schritt-Anweisungen.

Das Booten mehrerer Maschinen über den Acronis PXE Server ist sinnvoll, wenn im Netzwerk ein DHCP-Server (Dynamic Host Control Protocol) vorhanden ist. Dann erhalten die Netzwerkadapter der gebooteten Maschinen automatisch eine IP-Adresse.

**Beschränkung:**

Der Acronis PXE Server unterstützt keine UEFI-Boot-Loader.

## Den Acronis PXE Server installieren

***So können Sie den Acronis PXE Server installieren***

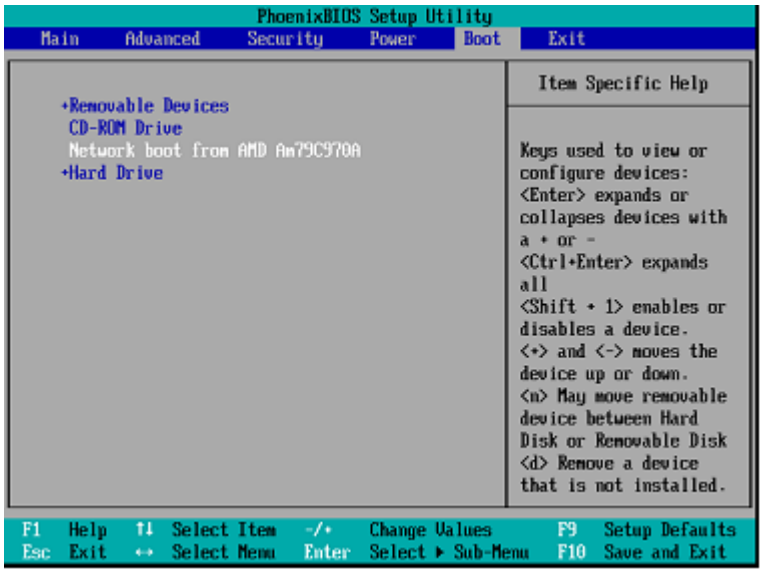
1. Melden Sie sich als Administrator an und starten Sie das Acronis Cyber Protect Setup-Programm.
2. [Optional] Wenn Sie die Sprache des Setup-Programms ändern wollen, klicken Sie auf **Sprache einrichten**.
3. Akzeptieren Sie die Bedingungen der Lizenzvereinbarung sowie die Datenschutzerklärung und klicken Sie anschließend auf **Fertigstellen**.
4. Klicken Sie auf **Installationseinstellungen anpassen**.
5. Klicken Sie neben **Zu installierende Komponenten** auf **Ändern**.
6. Aktivieren Sie das Kontrollkästchen **PXE Server**. Falls Sie keine anderen Komponenten auf dieser Maschine installieren wollen, deaktivieren Sie die entsprechenden Kontrollkästchen. Klicken Sie auf **Fertig**, um fortzufahren.
7. [Optional] Ändern Sie weitere Installationseinstellungen.
8. Klicken Sie auf **Installation**, um mit der Einrichtung fortzufahren.
9. Klicken Sie nach Abschluss der Installation auf **Schließen**.

Der Acronis PXE Server wird direkt nach der Installation als Dienst ausgeführt. Später wird er automatisch nach jedem System-Neustart ausgeführt. Sie können den Acronis PXE Server wie jeden anderen Windows-Dienst starten oder stoppen.

## Eine Maschine für das Booten von PXE konfigurieren

Für fabrikneue Maschinen reicht es aus, dass ihr BIOS das Booten von Netzwerk unterstützt.

Auf einer Maschine, die ein Betriebssystem auf ihrer Festplatte hat, muss das BIOS so konfiguriert werden, dass der Netzwerkadapter entweder das erste Boot-Gerät ist – oder zumindest vor der Festplatte aufgelistet ist. Das Beispiel zeigt eine typische BIOS-Konfiguration. Wenn Sie kein bootfähiges Medium einlegen, wird die Maschine vom Netz booten.




In einigen BIOS-Versionen müssen Sie die geänderten BIOS-Einstellungen, nach Aktivierung des Netzwerkadapters, erst abspeichern, damit die Netzwerkkarte in der Liste der Boot-Geräte erscheint.

Sollte Ihre Hardware mehrere Netzwerkadapter haben, so stellen Sie sicher, dass das Netzwerkkabel auch in der vom BIOS unterstützten Karte steckt.

## Über Subnetze hinweg arbeiten

Damit der Acronis PXE Server auch in anderen Subnetzen arbeiten kann (über einen Switch hinweg), muss der Switch PXE-Netzwerkverkehr weiterreichen können. Die IP-Adressen des PXE Servers sind auf Pro-Netzwerkadapter-Basis konfiguriert, unter Verwendung von IP-Helfer-Funktionalität wie bei DHCP-Server-Adressen. Weitere Informationen finden Sie unter: https://docs.microsoft.com/de-de/troubleshoot/mem/configmgr/boot-from-pxe-server.

# 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 Cyber Protect Webkonsole 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 Cyber Protect Webkonsole auf einem Computer oder Tablet verwenden.
- [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

1. Öffnen Sie auf dem Mobilgerät einen Webbrowser und gehen Sie zu https://backup.acronis.com/.
2. Melden Sie sich mit Ihrem Konto an.
3. Klicken Sie auf **Alle Geräte** –> **Hinzufügen**.
4. Wählen Sie unter **Mobilgeräte** den Gerätetyp.

   Abhängig vom Gerätetyp werden Sie entweder zum Apple App Store oder zum Google Play Store weitergeleitet.
5. [Nur auf iOS-Geräten] Klicken Sie auf **Laden**.
6. Klicken Sie auf **Installieren**, damit die Backup-App eingerichtet wird.

## So können Sie die Sicherung Ihrer Daten starten

1. Öffnen Sie die App.
2. Melden Sie sich mit Ihrem Konto an.

Tippen Sie auf **Einrichten**, um Ihr erstes Backup zu erstellen.

1. Wählen Sie die Datenkategorien aus, die Sie sichern wollen. Standardmäßig sind alle Kategorien ausgewählt.
2. [Optionaler Schritt] Aktivieren Sie **Backup verschlüsseln**, um Ihr Backup durch Verschlüsselung zu schützen. In diesem Fall müssen Sie außerdem:
   a. Ein Verschlüsselungskennwort zweimal eingeben.

      **Hinweis**
      Stellen Sie sicher, dass Sie sich das Kennwort merken, weil ein vergessenes Kennwort weder wiederhergestellt noch geändert werden kann.

   b. Tippen Sie auf **Verschlüsseln**.
3. Tippen Sie auf **Backup**.
4. 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

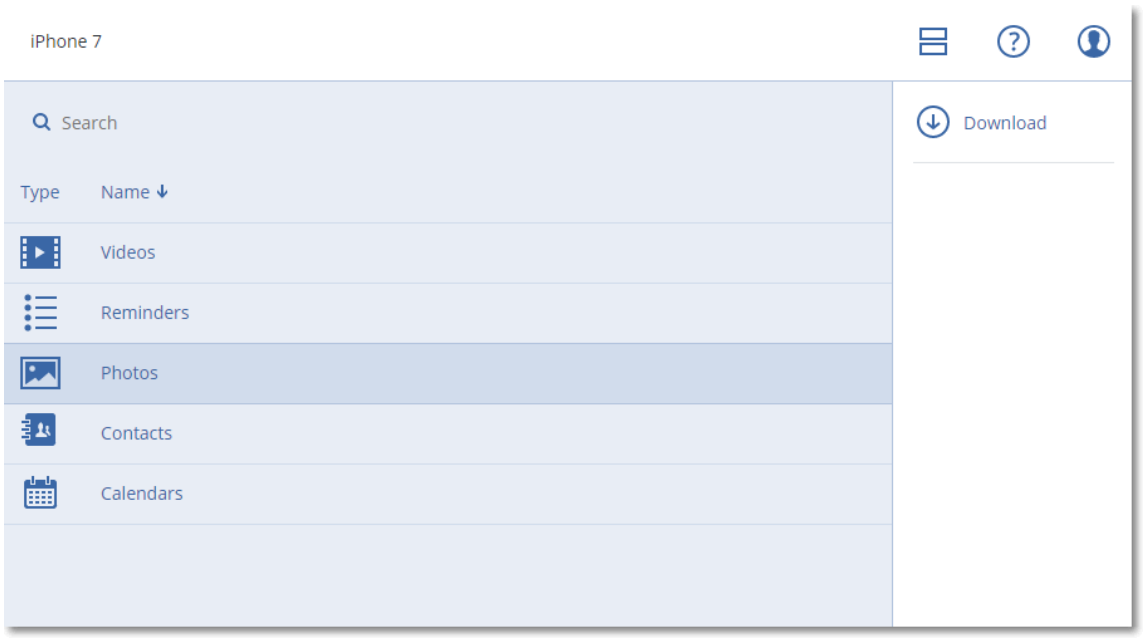
1. Öffnen Sie die Backup-App.
2. Tippen Sie auf den Befehl **Durchsuchen**.
3. Tippen Sie auf den Gerätenamen.
4. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Wenn Sie alle gesicherten Daten wiederherstellen wollen, müssen Sie auf **Alle wiederherstellen** tippen. Es sind keine weiteren 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.

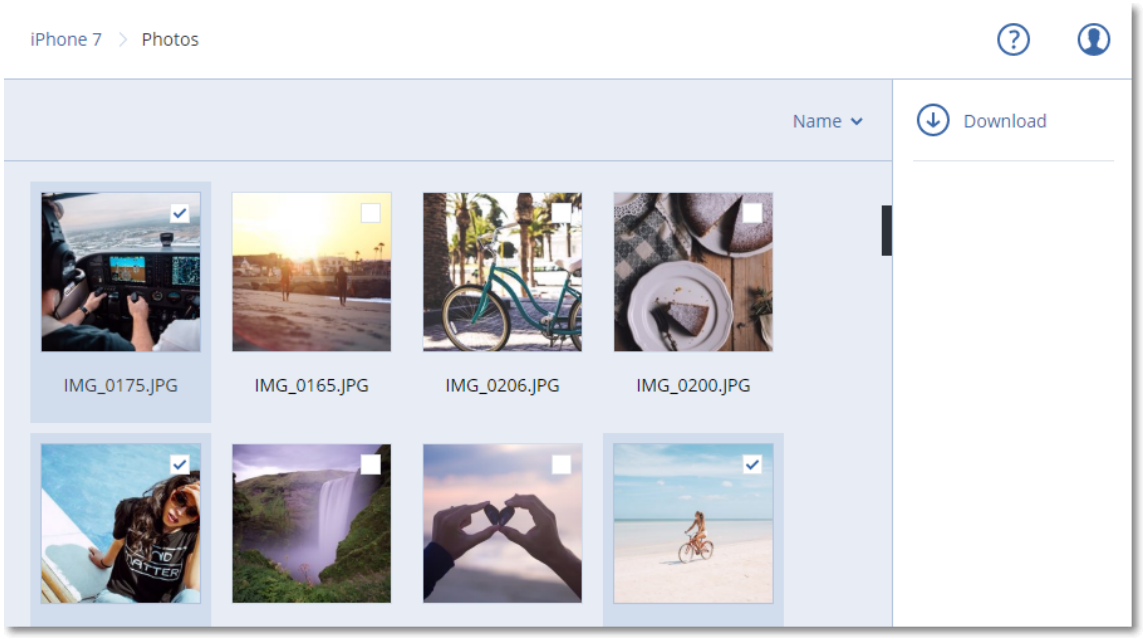
6. Tippen Sie auf den Befehl **Recovery**.

# So können Sie Daten über die Cyber Protect Webkonsole überprüfen

1. Öffnen Sie auf einem Computer einen Webbrowser und geben Sie die URL der Cyber Protect Webkonsole 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.

# Microsoft-Applikationen sichern

**Wichtig**
Einige der in diesem Abschnitt beschriebenen Funktionen stehen nur bei On-Premise-Bereitstellungen zur Verfügung.

## 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 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<br>Datenbanken als Dateien | Komplette Maschine<br>Datenbanken zu einer aktiven SQL Server-Instanz<br>Datenbanken als Dateien | Komplette Maschine |
| Microsoft Exchange Server | Datenbanken zu einem aktiven Exchange Server<br>Datenbanken als Dateien<br>Granulares Recovery zu einem aktiven Exchange Server oder zu Microsoft 365* | Komplette Maschine<br>Datenbanken zu einem aktiven Exchange Server<br>Datenbanken als Dateien<br>Granulares Recovery zu einem aktiven Exchange Server oder zu Microsoft 365* | Komplette Maschine |
| Microsoft SharePoint-Datenbank-Server | Datenbanken zu einer aktiven SQL Server-Instanz<br>Datenbanken als Dateien<br>Granulares Recovery mithilfe des SharePoint Explorers | Komplette Maschine<br>Datenbanken zu einer aktiven SQL Server-Instanz<br>Datenbanken als Dateien<br>Granulares Recovery mithilfe des SharePoint Explorers | Komplette Maschine |
| Microsoft SharePoint-Front-End-Webserver | - | - | Komplette Maschine |

| | | | |
|---|---|---|---|
| Active Directory-Domänendienste | - | Komplette Maschine | - |

* Granulares Recovery ist auch für Postfach-Backups möglich.

# Voraussetzungen

Bevor Sie das applikationskonforme Backup konfigurieren, sollten Sie sicherstellen, dass die nachfolgenden Voraussetzungen bzw. Anforderungen erfüllt sind.

Verwenden Sie zum Überprüfen des VSS-Writer-Stadiums den Befehl `vssadmin list writers`.

## Allgemeine Anforderungen

**Für Microsoft SQL Server müssen folgende Anforderungen erfüllt sein:**

- Mindestens eine Microsoft SQL Server-Instanz ist gestartet.
- Der SQL Writer für VSS ist aktiviert.

**Für Microsoft Exchange Server müssen folgende Anforderungen erfüllt sein:**

- Der Microsoft Exchange-Informationsspeicherdienst ist gestartet.
- Windows PowerShell ist installiert. Für Exchange 2010 (und höher) muss es mindestens Windows PowerShell-Version 2.0 sein.
- Microsoft .NET Framework ist installiert.
  Für Exchange 2007 muss es mindestens Microsoft .NET Framework-Version 2.0 sein.
  Für Exchange 2010 (und höher) muss es mindestens Microsoft .NET Framework-Version 3.5 sein.
- Der Exchange Writer für VSS ist aktiviert.

---

**Hinweis**
Der Agent für Exchange benötigt einen temporären Speicher, um arbeiten zu können. Diese temporären Dateien liegen standardmäßig im Ordner `%ProgramData%\Acronis\Temp`. Überprüfen Sie, dass der freie Speicherplatz des Volumes, auf dem der Ordner `%ProgramData%` liegt, mindestens 15% der Größe einer Exchange-Datenbank entspricht. Alternativ können Sie vor der Erstellung von Exchange-Backups den Speicherort der temporären Dateien ändern. Die Vorgehensweise ist hier beschrieben: https://kb.acronis.com/content/40040.

---

**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 ist die Backup-Option 'VSS (Volume Shadow Copy Service)' aktiviert.
- Für virtuelle Maschinen ist die Backup-Option 'VSS (Volume Shadow Copy Service) für virtuelle Maschinen' aktiviert.

## Zusätzliche Anforderungen für applikationskonforme Backups

Überprüfen Sie bei Erstellung eines Schutzplans, dass die '**Komplette Maschine**' zum Backup ausgewählt wurde. Die Backup-Option **Sektor-für-Sektor** muss im Schutzplan deaktiviert sein, ansonsten können aus solchen Backups keine Applikationsdaten wiederhergestellt werden. Wenn der Plan im **Sektor-für-Sektor**-Modus ausgeführt wird, weil automatisch auf diesen Modus umgeschaltet wird, dann werden keine Applikationsdaten wiederherstellbar sein.

### Anforderungen für virtuelle ESXi-Maschinen

Falls die Applikation auf einer virtuellen Maschine läuft, die vom Agenten für VMware gesichert wird, müssen folgende Anforderungen erfüllt sein:

- Die zu sichernde virtuelle Maschine erfüllt die Anforderungen für applikationskonsistente Backups und Wiederherstellungen, wie sie im englischsprachigen Artikel „Windows Backup Implementations“ der VMware-Dokumentation unter folgender Adresse aufgeführt sind: https://code.vmware.com/docs/1674/virtual-disk-programming-guide/doc/vddkBkupVadp.9.6.html
- Die VMware Tools sind auf der Maschine installiert und aktuell.
- Die Benutzerkontensteuerung (UAC) ist auf der Maschine deaktiviert. Wenn Sie die Benutzerkontensteuerung (UAC) nicht ausschalten wollen, müssen Sie die Anmeldedaten 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**).

# Datenbank-Backup

Bevor Sie ein Datenbank-Backup durchführen, sollten Sie sicherstellen, dass die unter 'Voraussetzungen' aufgeführten Anforderungen erfüllt sind.

Wählen Sie die Datenbanken wie nachfolgend beschrieben aus – und spezifizieren Sie die anderen Einstellungen des Schutzplans je nach Bedarf.

## SQL-Datenbanken auswählen

Das Backup einer SQL-Datenbank enthält die entsprechenden Datenbankdateien (.mdf, .ndf), Protokolldateien (.ldf) und andere zugeordnete Dateien. Die Dateien werden mithilfe des SQL-Writer-Dienstes gesichert. Der Dienst muss dann laufen, wenn der Volume Shadow Copy Service (VSS, Volumenschattenkopie-Dienst) ein Backup oder eine Wiederherstellung anfordert.

Die SQL-Transaktionsprotokolle werden nach jedem erfolgreichen Backup abgeschnitten. Die SQL-Protokollabschneidung kann in den Schutzplan-Optionen deaktiviert werden.

***So können Sie SQL-Datenbanken auswählen***

1. Klicken Sie auf **Geräte** –> **Microsoft SQL**.
   Die Software zeigt einen Verzeichnisbaum mit SQL Server-AlwaysOn-Verfügbarkeitsgruppen (AAG), Maschinen, die den Microsoft SQL Server ausführen, SQL Server-Instanzen und Datenbanken an.
2. Bestimmen Sie (per 'Durchsuchen') die Daten, die Sie sichern wollen.
   Erweitern Sie die Verzeichnisknoten oder klicken Sie rechts neben dem Verzeichnis doppelt auf einzelne Elemente in der Liste.
3. Wählen Sie Daten aus, die Sie sichern wollen. Sie können AAGS, den SQL Server ausführende Maschinen, SQL Server-Instanzen oder bestimmte Datenbanken auswählen.
   - Wenn Sie eine AAG auswählen, werden alle in der ausgewählten AAG enthaltenen Datenbanken per Backup gesichert. Weitere Informationen über das Backup von AAGs oder einzelnen AAG-Datenbanken finden Sie im Abschnitt 'AlwaysOn-Verfügbarkeitsgruppen (AAG) sichern'.
   - Wenn Sie eine Maschine auswählen, auf welcher ein SQL Server läuft, so werden alle Datenbanken gesichert, die an allen (auf der ausgewählten Maschine laufenden) SQL Server-Instanzen angefügt sind.
   - Wenn Sie eine bestimmte SQL Server-Instanz auswählen, werden alle Datenbanken gesichert, die an diese ausgewählte Instanz angefügt sind.

- Wenn Sie die gewünschten Datenbanken direkt auswählen, werden dagegen nur diese Datenbanken gesichert.

4. Klicken Sie auf den Befehl **Schützen**. Geben Sie bei Aufforderung die benötigten Anmeldedaten ein, um auf die SQL Server-Daten zugreifen zu können.

   Wenn Sie die Windows-Authentifizierung verwenden, muss das Konto auf der betreffenden Maschine ein Mitglied der Gruppe **Sicherungs-Operatoren** oder der Gruppe **Administratoren** sein – und auf jeder Instanz, die Sie sichern wollen, ein Mitglied der **SysAdmin**-Rolle.

   Wenn Sie die SQL Server-Authentifizierung verwenden, muss das Konto auf jeder Instanz, die Sie sichern wollen, ein Mitglied der **SysAdmin**-Rolle sein.

## Exchange Server-Daten auswählen

Die nachfolgende Tabelle gibt Ihnen einen Überblick über die Microsoft Exchange Server-Daten, die Sie für ein Backup verwenden können – und die (mindestens benötigten) Benutzerrechte, die zum Sichern dieser Daten erforderlich sind.

| Exchange-Version | Datenelemente | Benutzerrechte |
|---|---|---|
| 2007 | Speichergruppen | Mitglied in der Rollengruppe **Exchange-Organisationsadministratoren** |
| 2010/2013/2016/2019 | Datenbanken, Datenbankverfügbarkeitsgruppen (DAG) | Mitglied in der Rollengruppe **Serververwaltung**. |

Ein Voll-Backup enthält alle ausgewählten Exchange Server-Daten.

Ein inkrementelles Backup enthält die geänderten Datenblöcke der Datenbankdateien, die Prüfpunktdateien und eine kleinere Anzahl von Protokolldateien, die neuer als der korrespondierende Datenbank-Prüfpunkt sind. Da im Backup alle Änderungen an den Datenbankdateien enthalten sind, ist es nicht notwendig, alle Transaktionsprotokoll-Datensätze seit dem letzten (vorherigen) Backup zu sichern. Es muss nur dasjenige Protokoll nach einer Wiederherstellung zurückgespielt werden, welches neuer (jünger) als der Prüfpunkt ist. Dies ermöglicht eine schneller Wiederherstellung und gewährleistet ein erfolgreiches Datenbank-Backup auch bei aktivierter Umlaufprotokollierung.

Die Transaktionsprotokolldateien werden nach jedem erfolgreichen Backup abgeschnitten.

***So können Sie Exchange-Server-Daten auswählen***

1. Klicken Sie auf **Geräte** –> **Microsoft Exchange**.

   Die Software zeigt den Verzeichnisbaum der Exchange Server Datenbankverfügbarkeitsgruppen (DAG) sowie der Maschinen an, die den Microsoft Exchange Server und Exchange Server-Datenbanken ausführen. Wenn Sie den Agenten für Exchange so konfiguriert haben, wie es im Abschnitt 'Postfach-Backup' 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' 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**.

# AlwaysOn-Verfügbarkeitsgruppen (AAG) sichern

## 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.

   **Hinweis**
   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 AAG oder den Datenbanksatz für das Backup wie im Abschnitt 'SQL-Datenbanken auswählen' beschrieben aus.
   Sie müssen die AAG selbst auswählen, um alle Datenbanken der AAG sichern zu können. Wenn Sie einen Satz von Datenbanken sichern wollen, müssen Sie diesen Datenbanksatz in allen Knoten der AAG definieren.

   **Warnung!**
   Der Datenbanksatz muss in allen Knoten exakt gleich sein. Wenn auch nur ein Satz unterschiedlich ist oder nicht auf allen Knoten definiert wurde, wird das Cluster-Backup nicht richtig funktionieren.

3. Konfigurieren Sie die Backup-Option 'Cluster-Backup-Modus'.

## Datenbanken in einer AAG wiederherstellen

1. Wählen Sie zuerst die wiederherzustellenden Datenbanken und dann den Recovery-Punkt, von dem aus die Wiederherstellung der Datenbanken erfolgen soll.
   Wenn Sie eine geclusterte Datenbank unter **Geräte** –> **Microsoft SQL** –> **Datenbanken** ausgewählt haben und anschließend auf **Recovery** klicken, zeigt die Software nur die Recovery-Punkte an, die mit den Zeitpunkten korrespondieren, wenn die ausgewählte Kopie der Datenbank gesichert wurde.
   Die einfachste Möglichkeit, alle Recovery-Punkte einer geclusterten Datenbank einzusehen, besteht darin, das Backup der kompletten AAG in der Registerkarte 'Backup Storage' auszuwählen. Die Namen der AAG-Backups basieren auf folgender Vorlage: `<AAG-Name> - <Schutzplan-Name>` und haben ein spezielles Symbol.
2. Befolgen Sie zur Konfiguration der Wiederherstellung die im Abschnitt 'SQL-Datenbanken wiederherstellen' beschriebene Anleitung (beginnend mit Schritt 5).

Die Software definiert automatisch einen Cluster-Knoten, wohin die Daten wiederhergestellt werden. Der Name des Knotens wird im Feld **Recovery zu** angezeigt. Sie können den Zielknoten manuell ändern.

**Wichtig**
Eine in einer AlwaysOn-Verfügbarkeitsgruppe (AAG) enthaltene Datenbank kann während einer Wiederherstellung nicht überschrieben werden, weil der Microsoft SQL Server dies verhindert. Sie müssen die Zieldatenbank daher von der AAG ausschließen, bevor Sie die Wiederherstellung durchführen. Oder Sie stellen die Datenbank einfach als 'Nicht-AGG'-Datenbank wieder her. Nach Abschluss der Wiederherstellung können Sie die ursprüngliche AAG-Konfiguration wieder aufbauen.

# Datenbankverfügbarkeitsgruppen (DAG) sichern

## Exchange Server-Cluster – eine Übersicht

Der Leitgedanke von Exchange-Cluster ist, eine hohe Datenbankverfügbarkeit bereitzustellen – bei schneller Ausfallsicherung (Failover) und ohne Datenverlust. Üblicherweise wird dies erreicht, indem eine oder mehrere Kopien von Datenbanken oder Speichergruppen auf den Mitgliedern des Clusters (Cluster-Knoten) vorgehalten werden. Fällt der die aktive Datenbankkopie vorhaltende Cluster-Knoten oder die aktive Datenbankkopie selbst aus, dann springt der andere, die passive Kopie vorhaltende Knoten ein, übernimmt die Aktionen des fehlerhaften Knotens und ermöglicht so mit minimaler Ausfallszeit einen weiteren Zugriff auf die Exchange-Dienste. Auf diese Weise dienen die Cluster selbst bereits als eine Art von Disaster Recovery-Lösung.

Es gibt jedoch Fälle, in denen 'Failover Cluster'-Lösungen keinen Schutz für die Daten bereitstellen können: Beispielsweise bei logischer Beschädigung einer Datenbank, wenn eine bestimmte Datenbank in einem Cluster keine Kopie (Replikat) hat oder wenn der komplette Cluster ausgefallen ist. Cluster-Lösungen schützen außerdem nicht vor schädlichen Inhaltsänderungen, da diese üblicherweise sofort auf alle Cluster-Knoten repliziert werden.

## Cluster-konformes Backup

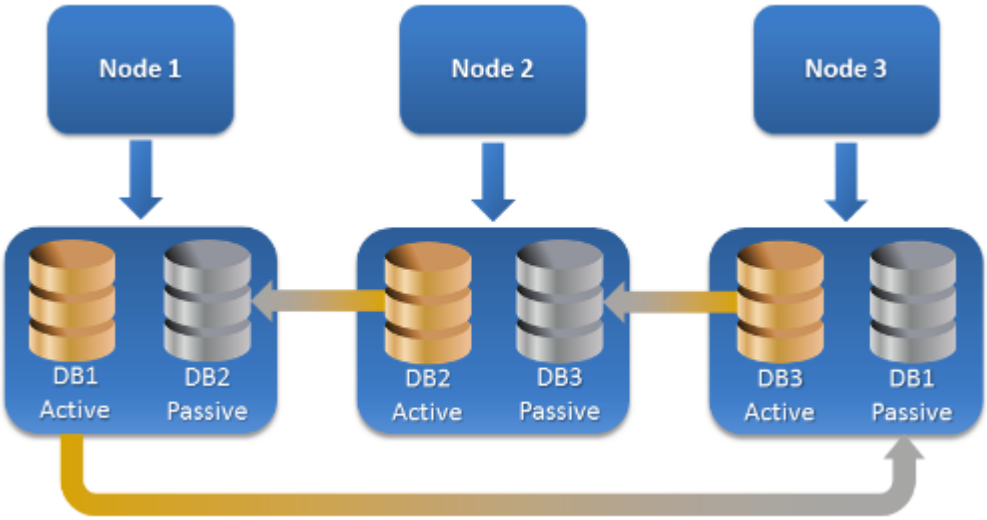
Bei einem Cluster-konformen Backup wird nur eine Kopie der geclusterten Daten gesichert. Wenn die Daten ihren Speicherort im Cluster ändern (aufgrund eines Switchovers oder Failovers), kann die Software alle Verlagerungen dieser Daten verfolgen und diese zuverlässig per Backup sichern.

## Unterstützte Cluster-Konfigurationen

Cluster-konformes Backup wird *nur* für Datenbankverfügbarkeitsgruppen (DAG) in Exchange Server 2010 oder höher unterstützt. Andere Cluster-Konfigurationen – wie Einzelkopiencluster (Single Copy Cluster, SCC) und fortlaufende Cluster-Replikation (Cluster Continuous Replication, CCR) für Exchange Server 2007 – werden *nicht* unterstützt.

Eine DAG besteht aus einer Gruppe von bis zu 16 Exchange-Postfachservern. Jeder Knoten kann eine Kopie der Postfachdatenbank von jedem anderen Knoten hosten. Jeder Knoten kann passive

und aktive Datenbankkopien hosten. Es können bis zu 16 Kopien von jeder Datenbank erstellt werden.




## Wie viele Agenten sind für Cluster-konforme Backups und Wiederherstellungen erforderlich?

Um geclusterte Datenbanken erfolgreich sichern und wiederherstellen zu können, muss der Agent für Exchange auf jedem Knoten des Exchange-Clusters installiert sein.

**Hinweis**
Nachdem Sie den Agenten auf einem der Knoten installiert haben, zeigt die Cyber Protect Webkonsole 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' beschrieben ist.
2. Konfigurieren Sie die Backup-Option 'Cluster-Backup-Modus'.
3. Spezifizieren Sie bei Bedarf noch weitere Einstellungen des Schutzplans.

**Wichtig**
Stellen Sie bei einem Cluster-konformen Backup sicher, dass Sie die DAG selbst auswählen. Wenn Sie einzelne Knoten oder Datenbanken innerhalb der DAG auswählen, werden nur die ausgewählten Elemente gesichert und die Option **Cluster-Backup-Modus** ignoriert.

## Exchange-Cluster-Daten wiederherstellen

1. Wählen Sie den Recovery-Punkt für die Datenbank aus, die Sie wiederherstellen wollen. Einen kompletten Cluster zur Wiederherstellung auszuwählen, ist jedoch nicht möglich.

   Wenn Sie die Kopie einer geclusterten Datenbank unter **Geräte** –> **Microsoft Exchange** –> **Datenbanken** –> `<Cluster-Name>` –> `<Knoten-Name>` auswählen und dann auf **Recovery** klicken, zeigt die Software nur solche Recovery-Punkte an, die mit den Zeitpunkten korrespondieren, wenn die Kopie dieser Datenbank gesichert wurde.

   Die einfachste Möglichkeit, alle Recovery-Punkte einer geclusterten Datenbank einzusehen, besteht darin, deren Backup in der Registerkarte 'Backup Storage' auszuwählen.
2. Befolgen Sie die im Abschnitt 'Exchange-Datenbanken wiederherstellen' 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.

# Applikationskonformes Backup

Applikationskonformes Backup auf Laufwerksebene ist für physische Maschinen sowie 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 deaktiviert werden. Die Exchange-Transaktionsprotokolle werden nur auf virtuellen Maschinen abgeschnitten. Sie können die Option 'VSS-Voll-Backup' aktivieren, falls Sie wollen, dass die Exchange-Transaktionsprotokolle auf einer physischen Maschine abgeschnitten werden.

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.

**Hinweis**
Bei virtuellen Hyper-V-Maschinen, auf denen der Windows Server 2022 ausgeführt wird, werden keine applikationskonformen Backups im agentenlosen Modus unterstützt (also wenn das Backup durch den Agenten für Hyper-V durchgeführt wird). Wenn Sie Microsoft-Applikationen auf diesen Maschinen schützen wollen, müssen Sie daher den Agenten für Windows innerhalb des Gastbetriebssystems installieren.

Der Agent für VMware (Virtuelle Appliance) und der Agent für VMware (Linux) können applikationskonforme Backups erstellen, aber keine Applikationsdaten aus diesen Backups wiederherstellen. Wenn Sie Applikationsdaten aus Backups wiederherstellen wollen, die von diesen 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.

Die allgemeinen Anforderungen sind in den Abschnitten '"Voraussetzungen" (S. 469)' und '"Erforderliche Benutzerrechte für applikationskonforme Backups" (S. 478)' aufgeführt.

## Erforderliche Benutzerrechte für applikationskonforme Backups

Ein applikationskonformes Backup enthält die Metadaten von VSS-kompatiblen Applikationen, die auf dem Laufwerk vorliegen. Um auf diese Metadaten zugreifen zu können, benötigt der Agenten ein Konto mit passenden Berechtigungen, die nachfolgend aufgeführt sind. Wenn Sie ein applikationskonformes Backup aktivieren, werden Sie aufgefordert, ein solches Konto zu spezifizieren.

- Für SQL Server:
  Wenn Sie die Windows-Authentifizierung verwenden, muss das Konto auf der betreffenden Maschine ein Mitglied der Gruppe **Sicherungs-Operatoren** oder der Gruppe **Administratoren** sein – und auf jeder Instanz, die Sie sichern wollen, ein Mitglied der **SysAdmin**-Rolle. Wenn Sie die

SQL Server-Authentifizierung verwenden, muss das Konto auf jeder Instanz, die Sie sichern wollen, ein Mitglied der **SysAdmin**-Rolle sein.

- 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.

### Zusätzliche Anforderungen für Maschinen mit Windows

Um applikationskonforme Backups zu ermöglichen, müssen Sie bei allen Windows-Versionen die Richtlinien für die Benutzerkontensteuerung (UAC) deaktivieren. Wenn Sie die UAC-Richtlinien nicht ausschalten wollen, müssen Sie die Anmeldedaten eines integrierten Domain-Administrators (DOMAIN\Administrator) bereitstellen, wenn Sie applikationskonforme Backups konfigurieren.

***So können Sie die UAC-Richtlinien in Windows deaktivieren***

1. Suchen Sie im Registrierungs-Editor den folgenden Registrierungsschlüssel:
   `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System`
2. Ändern Sie den Wert für **EnableLUA** auf **0**.
3. Starten Sie die Maschine neu.

# Postfach-Backup

Das Postfach-Backup wird für Microsoft Exchange Server 2010 Service Pack 1 (SP1) oder höher unterstützt.

Die Möglichkeit zur Sicherung von Postfächern ist dann verfügbar, wenn auf dem Management Server mindestens ein Agent für Exchange registriert ist. Die Agent muss auf einer Maschine installiert sein, die zu derselben Active Directory-Gesamtstruktur (Forest) gehört wie der Microsoft Exchange Server.

Bevor Sie Postfächer sichern können, müssen Sie den Agenten für Exchange mit der Maschine verbinden, auf welcher die Server-Rolle **Clientzugriff** (CAS) des Microsoft Exchange Servers ausgeführt wird. In Exchange 2016 oder höher ist die CAS-Rolle nicht als separate Installationsoption verfügbar. Es wird automatisch als Teil der Postfachserverrolle installiert. Auf

diese Weise können Sie den Agenten mit jedem Server verbinden, auf dem die **Postfachrolle** ausgeführt wird.

***So verbinden Sie den Agenten mit der Clientzugriffsrolle***

1. Klicken Sie auf **Geräte** –> **Hinzufügen**.
2. Klicken Sie auf **Microsoft Exchange Server**.
3. Klicken Sie auf **Exchange-Postfächer**.
   Wenn auf dem Management Server kein Agent für Exchange registriert ist, wird Ihnen die Software vorschlagen, dass Sie den Agenten installieren sollen. Wiederholen Sie nach der Installation diese Prozedur ab Schritt 1.
4. [Optional] Sollten auf dem Management Server mehrere Agenten für Exchange registriert sein, dann klicken Sie auf **Agent** und ändern Sie den Agenten, der das Backup durchführen soll.
5. Spezifizieren Sie bei **Clientzugriffsserver (CAS)** den vollqualifizierten Domain-Namen (FQDN) derjenigen Maschine, auf welcher die Rolle '**Clientzugriff**' des Microsoft Exchange Servers aktiviert ist.
   In Exchange 2016 oder höher werden die Clientzugriffsdienste automatisch als Teil der Postfachserverrolle installiert. Auf diese Weise können Sie jeden Server spezifizieren, auf dem die **Postfachrolle** ausgeführt wird. Wir werden diesen Server später in diesem Abschnitt einfach als „CAS“ bezeichnen.
6. Bestimmen Sie bei **Authentifizierungstyp** den Authentifizierungstyp, der für die Clientzugriffsrolle verwendet werden soll. Sie können **Kerberos** (Standard) oder **Basis** auswählen.
7. [Nur bei Basisauthentifizierung] Bestimmen Sie, welches Protokoll verwendet werden soll. Sie können **HTTPS** (Standard) oder **HTTP** auswählen.
8. [Nur bei Basisauthentifizierung mit HTTPS-Protokoll] Falls die Clientzugriffsrolle ein SSL-Zertifikat verwendet, welches von einer offiziellen Zertifizierungsstelle ausgestellt wurde, und Sie wollen, dass die Software das Zertifikat bei Verbindung mit der Clientzugriffsrolle (CAS) überprüft, dann aktivieren Sie das Kontrollkästchen **SSL-Zertifikat überprüfen**. Ansonsten können Sie diesen Schritt überspringen.
9. Geben Sie die Anmeldedaten eines Kontos ein, welches für den Zugriff auf die Clientzugriffsrolle verwendet werden soll. Die Anforderungen für dieses Konto sind im Abschnitt 'Erforderliche Benutzerrechte' aufgeführt.
10. Klicken Sie auf **Hinzufügen**.

Als Ergebnis erscheinen die Postfächer anschließend unter **Geräte** –> **Microsoft Exchange** –> **Postfächer**.

## Exchange Server-Postfächer auswählen

Wählen Sie die Postfächer wie nachfolgend beschrieben aus – und spezifizieren Sie dann die anderen Einstellungen des Schutzplans nach Bedarf.

***So können Sie Exchange-Postfächer auswählen***

1. Klicken Sie auf **Geräte** –> **Microsoft Exchange**.
   Die Software zeigt den Verzeichnisbaum der Exchange-Datenbanken und -Postfächer.
2. Klicken Sie auf **Postfächer** und wählen Sie die Postfächer, die Sie per Backup sichern wollen.
3. Klicken Sie auf **Backup**.

## Erforderliche Benutzerrechte

Um auf Postfächer zugreifen zu können, benötigt der Agent für Exchange ein Konto mit passenden Berechtigungen. Sie werden aufgefordert, dieses Konto zu spezifizieren, wenn Sie Aktionen mit Postfächern konfigurieren.

Die Mitgliedschaft des Kontos in der Rollengruppe **Organisationsverwaltung** ermöglicht den Zugriff auf alle Postfächer (auch solche, die in Zukunft erstellt werden).

Die mindestens erforderlichen Benutzerrechte sind:

- Das Konto muss Mitglied in den Rollengruppen **Serververwaltung** und **Empfängerverwaltung** sein.
- Das Konto muss die Verwaltungsrolle **ApplicationImpersonation** für alle Benutzer oder Benutzergruppen aktiviert haben, auf deren Postfächer der Agent zugreifen wird.
  Genauere Informationen zur Konfiguration der Verwaltungsrolle **ApplicationImpersonation** finden Sie im folgenden Microsoft Knowledge Base-Artikel: https://msdn.microsoft.com/de-de/library/office/dn722376.aspx.

# SQL-Datenbanken wiederherstellen

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.

Wenn Sie die Windows-Authentifizierung verwenden, müssen Sie außerdem die Anmeldedaten für ein Konto angeben, welches auf der Maschine ein Mitglied der Gruppe **Sicherungs-Operatoren** oder der Gruppe **Administratoren** ist – und zudem auf der Zielinstanz ein Mitglied der **SysAdmin**-Rolle ist. Wenn Sie die SQL Server-Authentifizierung verwenden, müssen Sie die Anmeldedaten für ein Konto angeben, das auf der Zielinstanz ein Mitglied der **SysAdmin**-Rolle ist.

Sie können die Datenbanken alternativ auch als Dateien wiederherstellen. Das kann nützlich sein, falls Sie Daten zur Überwachung oder weiteren Verarbeitung durch Drittthersteller-Tools extrahieren müssen. Wie Sie SQL-Datenbankdateien an eine SQL Server-Instanz anfügen, ist im Abschnitt 'SQL Server-Datenbanken anfügen' 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' 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'.

   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:
   - **Einsatzbereit (Mit RECOVERY wiederherstellen)** (Standardeinstellung)
     Die Datenbank ist nach Abschluss der Wiederherstellung direkt einsatzbereit. Benutzer haben vollen Zugriff auf sie. Die Software wird für alle Transaktionen der wiederhergestellten Datenbank ein Rollback ausführen, für die kein 'Commit' ausgeführt wurde und die in den Transaktionsprotokollen gespeichert sind. Sie können keine zusätzlichen Transaktionsprotokolle von systemeigenen Microsoft SQL-Backups wiederherstellen.
   - **Nicht betriebsbereit (Mit NORECOVERY wiederherstellen)**
     Die Datenbank ist nach Abschluss der Wiederherstellung nicht betriebsbereit. Benutzer haben keinen Zugriff auf sie. Die Software behält alle nicht übernommenen Transaktionen (ohne 'Commit') der wiederhergestellten Datenbank. Sie können zusätzliche Transaktionsprotokolle von systemeigenen Microsoft SQL-Backups wiederherstellen und auf diese Weise den notwendigen Recovery-Punkt erreichen.
   - **Schreibgeschützt (Mit STANDBY wiederherstellen)**
     Benutzer haben nach Abschluss der Wiederherstellung einen Nur-Lesen-Zugriff auf die Datenbank. Die Software wird alle nicht übernommenen Transaktionen (ohne 'Commit') rückgängig machen. Die Rückgängigaktionen werden jedoch in einer temporären Standby-Datei gespeichert, sodass die Recovery-Effekte zurückgestellt werden werden können.
     Dieser Wert wird primär verwendet, um den Zeitpunkt eines SQL Server-Fehlers zu ermitteln.
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'.

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.

## Systemdatenbanken wiederherstellen

Alle Systemdatenbanken einer Instanz werden gleichzeitig wiederhergestellt. Bei der Wiederherstellung von Systemdatenbanken führt die Software einen automatischen Neustart der Zielinstanz im Einzelbenutzermodus aus. Nach Abschluss der Wiederherstellung startet die Software die Instanz neu und stellt andere Datenbanken (sofern vorhanden) wieder her.

Weitere Punkte, die bei der Wiederherstellung von Systemdatenbanken beachtet werden sollten:

- Systemdatenbanken können nur zu einer Instanz wiederhergestellt werden, die dieselbe Version wie die ursprüngliche Instanz hat.
- Systemdatenbanken können nur im Stadium 'Einsatzbereit' (ready to use) wiederhergestellt werden.

### Die master-Datenbank wiederherstellen

Zu den Systemdatenbanken gehört auch die sogenannte **master**-Datenbank. Die **master**-Datenbank erfasst allgemeine Informationen über alle Datenbanken einer Instanz. Die **master**-Datenbank in einem Backup enthält daher genau die Informationen über die Datenbanken, die zum Zeitpunkt des Backups in der Instanz vorlagen. Nach der Wiederherstellung der **master**-Datenbank müssen Sie möglicherweise Folgendes tun:

- Datenbanken, die in der Instanz aufgetaucht sind, nachdem das Backup erstellt wurde, sind für die Instanz nicht sichtbar. Um diese Datenbanken zurück in die Produktion zu bringen, müssen Sie diese manuell mithilfe des Microsoft SQL Server Management Studios an die Instanz anschließen.

- Datenbanken, die nach Erstellung des Backups gelöscht wurden, werden in der Instanz als offline angezeigt. Löschen Sie diese Datenbanken mithilfe des SQL Server Management Studios.

## SQL Server-Datenbanken anfügen

Dieser Abschnitt beschreibt, wie Sie eine Datenbank im SQL Server mithilfe des SQL Server Management Studios anfügen können. Es kann immer nur eine Datenbank gleichzeitig angefügt werden.

Das Anfügen einer Datenbank erfordert eine der folgenden Berechtigungen: **Datenbank erstellen**, **Beliebige Datenbank erstellen** oder **Beliebige Datenbank ändern**. Normalerweise verfügt auf der Instanz die Rolle **SysAdmin** über diese Berechtigungen.

***So fügen Sie eine Datenbank an***

1. Führen Sie Microsoft SQL Server Management Studio aus.
2. Verbinden Sie sich mit der benötigten SQL Server-Instanz und erweitern Sie dann die Instanz.
3. Klicken Sie mit der rechten Maustaste auf **Datenbanken** und klicken Sie dann auf **Anfügen**.
4. Klicken Sie auf **Hinzufügen**.
5. Lokalisieren und Wählen Sie im Dialogfenster **Datenbankdateien suchen** die .mdf-Datei der Datenbank.
6. Stellen Sie im Bereich **Datenbankdetails** sicher, dass die restlichen Datenbankdateien (.ndf- und .ldf-Dateien) gefunden werden.

   **Details**: SQL Server-Datenbankdateien werden möglicherweise nicht automatisch gefunden, falls:
   - Sie sich nicht am Standardspeicherort befinden – oder sie nicht im selben Ordner wie die primäre Datenbankdatei (.mdf) sind. Lösung: Spezifizieren Sie den Pfad zu den benötigten Dateien manuell in der Spalte **Aktueller Dateipfad**.
   - Sie haben einen unvollständigen Satz an Dateien wiederhergestellt, der die Datenbank bildet. Lösung: Stellen Sie die fehlenden SQL Server-Datenbankdateien aus dem Backup wieder her.
7. Klicken Sie, wenn alle Dateien gefunden sind, auf **OK**.

# Exchange-Datenbanken wiederherstellen

Dieser Abschnitt beschreibt die Wiederherstellung von Datenbank-Backups und applikationskonformen Backups.

Sie können Exchange Server-Daten zu einem aktiv laufenden Exchange Server wiederherstellen. Dies kann der ursprüngliche Exchange Server sein – oder ein Exchange Server mit derselben Version, der auf einer Maschine mit demselben vollqualifizierten Domain-Namen (FQDN) läuft. Der Agent für Exchange muss auf der Zielmaschine installiert sein.

Die nachfolgende Tabelle gibt Ihnen einen Überblick über die Exchange Server-Daten, die Sie für eine Wiederherstellung verwenden können – und die (mindestens benötigten) Benutzerrechte, die zur Wiederherstellung dieser Daten erforderlich sind.

| Exchange-Version | Datenelemente | Benutzerrechte |
|---|---|---|
| 2007 | Speichergruppen | Mitglied in der Rollengruppe **Exchange-Organisationsadministratoren**. |
| 2010/2013/2016/2019 | Datenbanken | Mitglied in der Rollengruppe **Serververwaltung**. |

Sie können die Datenbanken (Speichergruppen) alternativ auch als Dateien wiederherstellen. Die Datenbankdateien werden (zusammen mit den Transaktionsprotokolldateien) aus dem Backup in einem von Ihnen spezifizierten Ordner extrahiert. Das kann nützlich sein, falls Sie Daten für eine Überwachung oder zur weiteren Verarbeitung durch Tools von Drittherstellern extrahieren müssen – oder wenn eine Wiederherstellung aus irgendeinem Grund fehlschlägt und Sie nach einem Workaround suchen, die Datenbanken manuell zu mounten.

Falls Sie lediglich den Agenten für VMware (Windows) verwenden, ist nur eine Recovery-Methode verfügbar, nämlich Datenbanken als Dateien wiederherzustellen. Eine Wiederherstellung von Datenbanken über den Agenten für VMware (Virtual Appliance) ist nicht möglich.

Wir werden bei den unteren Prozeduren die Datenbanken und Speichergruppen einheitlich nur als 'Datenbanken' bezeichnen.

***So können Sie Exchange-Datenbanken zu einem aktiv laufenden Exchange Server wiederherstellen***

1. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Wenn Sie eine Wiederherstellung aus einem applikationskonformen Backup durchführen, wählen Sie unter **Geräte** diejenige Maschine aus, auf der sich die wiederherzustellenden Daten ursprünglich befunden haben.
   - Wenn Sie eine Wiederherstellung aus einem Datenbank-Backup durchführen, klicken Sie auf **Geräte** –> **Microsoft Exchange** –> **Datenbanken** – und wählen Sie dann die Datenbanken, die Sie wiederherstellen wollen.
2. Klicken Sie auf **Recovery**.
3. Wählen Sie einen Recovery-Punkt. Beachten Sie dabei, dass Recovery-Punkte nach Speicherorten gefiltert werden.

   Falls die Maschine offline ist, werden keine Recovery-Punkte angezeigt. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - [Nur bei Wiederherstellung aus einem applikationskonformen Backup] Sollte sich das Backup im Cloud Storage oder einem freigegebenen Storage befinden (d.h., dass andere Agenten auf diesen zugreifen können), dann klicken Sie zuerst auf den Befehl **Maschine auswählen**. Wählen Sie anschließend eine Maschine aus, die online ist und auf welcher der Agent für Exchange installiert ist, und dann den gewünschten Recovery-Punkt.
   - Wählen Sie einen Recovery-Punkt auf der Registerkarte 'Backup Storage'.

   Die in einer der oberen Aktionen zum Durchsuchen ausgewählte Maschine wird als Zielmaschine für die Wiederherstellung der Exchange-Daten verwendet.
4. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:

- Wenn Sie eine Wiederherstellung aus einem applikationskonformen Backup durchführen, klicken Sie auf **Recovery** –> **Exchange-Datenbanken**, wählen Sie die wiederherzustellende Datenbank aus und klicken Sie dann auf **Recovery**.
- Wenn Sie eine Wiederherstellung aus einem Datenbank-Backup durchführen, klicken Sie auf **Recovery** –> **Datenbanken zu einem Exchange Server**.

5. Die Datenbanken werden standardmäßig zu den ursprünglichen Datenbanken wiederhergestellt. Falls die ursprüngliche Datenbank nicht existiert, wird sie automatisch neu erstellt.

   So können Sie eine Datenbank zu einer anderen Datenbank wiederherstellen:

   a. Klicken Sie auf den Datenbanknamen.

   b. Wählen Sie bei **Recovery zu** die Option **Neue Datenbank**.

   c. Spezifizieren Sie den Namen für die neue Datenbank.

   d. Spezifizieren Sie den Pfad für die neue Datenbank und den Pfad für die Protokolle. Der von Ihnen spezifizierte Ordner darf keine ursprüngliche Datenbank oder Protokolldateien enthalten.

6. Klicken Sie auf **Recovery starten**.

Der Recovery-Fortschritt wird auf der Registerkarte **Aktivitäten** angezeigt.

***So können Sie Exchange-Datenbanken als Dateien wiederherstellen***

1. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Wenn Sie eine Wiederherstellung aus einem applikationskonformen Backup durchführen, wählen Sie unter **Geräte** diejenige Maschine aus, auf der sich die wiederherzustellenden Daten ursprünglich befunden haben.
   - Wenn Sie eine Wiederherstellung aus einem Datenbank-Backup durchführen, klicken Sie auf **Geräte** –> **Microsoft Exchange** –> **Datenbanken** – und wählen Sie dann die Datenbanken, die Sie wiederherstellen wollen.
2. Klicken Sie auf **Recovery**.
3. Wählen Sie einen Recovery-Punkt. Beachten Sie dabei, dass Recovery-Punkte nach Speicherorten gefiltert werden.

   Falls die Maschine offline ist, werden keine Recovery-Punkte angezeigt. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - [Nur bei Wiederherstellung aus einem applikationskonformen Backup] Sollte sich das Backup im Cloud Storage oder einem freigegebenen Storage befinden (d.h., dass andere Agenten auf diesen zugreifen können), dann klicken Sie zuerst auf den Befehl **Maschine auswählen**. Wählen Sie anschließend eine Maschine aus, die online ist und auf welcher der Agent für Exchange oder der Agent für VMware installiert ist, und dann den gewünschten Recovery-Punkt.
   - Wählen Sie einen Recovery-Punkt auf der Registerkarte 'Backup Storage'.

   Die in einer der oberen Aktionen zum Durchsuchen ausgewählte Maschine wird als Zielmaschine für die Wiederherstellung der Exchange-Daten verwendet.
4. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:

- Wenn Sie eine Wiederherstellung aus einem applikationskonformen Backup durchführen, klicken Sie auf **Recovery** –> **Exchange-Datenbanken**, wählen Sie die wiederherzustellende Datenbank aus und klicken Sie dann auf **Als Dateien wiederherstellen**.
- Wenn Sie eine Wiederherstellung aus einem Datenbank-Backup durchführen, klicken Sie auf **Recovery** –> **Datenbanken als Dateien**

5. Klicken Sie auf **Durchsuchen** und wählen Sie einen lokalen Ordner oder Netzwerkordner aus, in dem die Dateien gespeichert werden sollen.
6. Klicken Sie auf **Recovery starten**.

Der Recovery-Fortschritt wird auf der Registerkarte **Aktivitäten** angezeigt.

## Exchange-Server-Datenbanken mounten

Sie können die Datenbanken nach Wiederherstellung der Datenbankdateien dadurch wieder online bringen, dass Sie sie mounten. Das Mounten wird mithilfe der Exchange-Verwaltungskonsole, dem Exchange-System-Manager oder der Exchange-Verwaltungsshell durchgeführt.

Die wiederhergestellte Datenbank wird sich im Stadium 'Dirty Shutdown' befinden. Eine Datenbank, die sich im Zustand 'Dirty Shutdown' befindet, kann vom System gemountet werden, falls sie zu ihrem ursprünglichen Speicherort wiederhergestellt wurde (vorausgesetzt, die Information über die ursprüngliche Datenbank ist im Active Directory vorhanden). Wenn Sie eine Datenbank zu einem anderen Speicherort wiederherstellen (beispielsweise eine neue Datenbank oder die Wiederherstellungsdatenbank), dann kann die Datenbank solange gemountet werden, bis Sie sie mithilfe des Befehls `Eseutil /r <Enn>` in das Stadium 'Clean Shutdown' bringen. `<Enn>` gibt den Logdatei-Präfix für die Datenbank an (bzw. die Speichergruppe, welche die Datenbank enthält), auf die Sie die Transaktionsprotokolldateien anwenden müssen.

Das Konto, welches Sie zum Anfügen einer Datenbank verwenden, muss an eine Exchange-Server-Administratorrolle und an eine lokalen Administratorengruppe des Zielservers delegiert sein.

Weitere Details zum Mounten von Datenbanken finden Sie in folgenden Artikeln:

- Exchange 2010 oder höher: http://technet.microsoft.com/de-de/library/aa998871.aspx
- Exchange 2007: http://technet.microsoft.com/de-de/library/aa998871(v=EXCHG.80).aspx

# Exchange-Postfächer und Postfachelemente wiederherstellen

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 365 wiederhergestellt werden.

Folgende Elemente können wiederhergestellt werden:

- Postfächer (ausgenommen archivierte Postfächer)
- Öffentliche Ordner

  **Hinweis**
  Nur für Datenbank-Backups verfügbar. Siehe "Exchange Server-Daten auswählen" (S. 472)

- 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 for VMware (Windows) durchgeführt werden. Der als Ziel verwendete Exchange Server und die Maschine, auf welcher der Agent läuft, müssen derselben Active Directory-Gesamtstruktur (Forest) angehören.

Wenn bei einer Postfach-Wiederherstellung ein vorhandenes Postfach als Ziel ausgewählt wird, werden alle dort vorliegenden Elemente, die übereinstimmende IDs haben, überschrieben.

Bei einer Wiederherstellung von Postfachelementen werden keinerlei Elemente überschrieben. Stattdessen wird der vollständige Pfad zu einem Postfachelement im Zielordner neu erstellt.

### Anforderungen an Benutzerkonten

Ein von einem Backup aus wiederhergestelltes Postfach muss ein assoziiertes Benutzerkonto im Active Directory haben.

Benutzerpostfächer und deren Inhalte können nur dann wiederhergestellt werden, wenn die mit ihnen assoziierten Benutzerkonten *aktiviert* sind. Raum-, Geräte- oder freigegebene Postfächer können nur dann wiederhergestellt werden, wenn ihre assoziierten Benutzerkonten *deaktiviert* sind.

Ein Postfach, welches die oberen Bedingungen nicht erfüllt, wird während einer Wiederherstellung übersprungen.

Falls einige Postfächer übersprungen werden, die Wiederherstellung mit dem Status 'Mit Warnungen' abgeschlossen. Sollten alle Postfächer übersprungen werden, schlägt die Wiederherstellung fehl.

## Wiederherstellungen zu Microsoft 365

Wiederherstellungen können aus Backups von Microsoft Exchange Server 2010 (oder höher) durchgeführt werden.

Wenn ein Postfach zu einem vorhandenen Microsoft 365-Postfach wiederhergestellt wird, bleiben dort bereits vorhandene Elemente erhalten. Die wiederhergestellten Elemente werden neben den vorhandenen gespeichert.

Wenn Sie ein einzelnes Postfach wiederherstellen, müssen Sie das Microsoft 356-Postfach auswählen, das als Ziel dienen soll. Wenn Sie mehrere Postfächer mit einer Recovery-Aktion wiederherstellen wollen, wird die Software versuchen, jedes Postfach zu dem Postfach desjenigen Benutzers wiederherzustellen, der denselben Benutzernamen hat. Wenn dieser Benutzer nicht gefunden werden kann, wird das Postfach übersprungen. Falls einige Postfächer übersprungen werden, die Wiederherstellung mit dem Status 'Mit Warnungen' abgeschlossen. Sollten alle Postfächer übersprungen werden, schlägt die Wiederherstellung fehl.

Weitere Informationen über Wiederherstellungen in Microsoft 365 finden Sie im Abschnitt '"Microsoft 365-Postfächer sichern" (S. 497)'

## Postfächer wiederherstellen

***So können Sie Postfächer aus einem applikationskonformen Backup oder einem Datenbank-Backup wiederherstellen***

1. [Nur bei Wiederherstellung eines Datenbank-Backups zu Microsoft 365] Wenn der Agent für Microsoft 365 auf der Maschine, die den Exchange Server ausführt und per Backup gesichert wurde, nicht installiert ist, gehen Sie folgendermaßen vor:
   - Falls Sie keinen Agenten für 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'.
2. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Bei Wiederherstellung aus einem applikationskonformen Backup: Wählen Sie unter **Geräte** diejenige Maschine aus, auf der sich die wiederherzustellenden Daten ursprünglich befunden haben.

- Wenn Sie eine Wiederherstellung aus einem Datenbank-Backup durchführen, klicken Sie auf **Geräte** –> **Microsoft Exchange** –> **Datenbanken** – und wählen Sie dann diejenige Datenbank aus, in der sich die wiederherzustellenden Daten ursprünglich befunden haben.

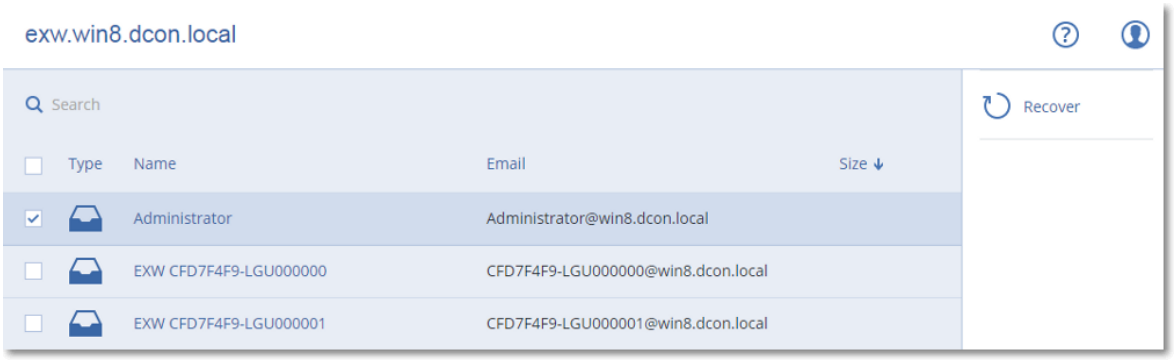
3. Klicken Sie auf **Recovery**.
4. Wählen Sie einen Recovery-Punkt. Beachten Sie dabei, dass Recovery-Punkte nach Speicherorten gefiltert werden.

   Falls die Maschine offline ist, werden keine Recovery-Punkte angezeigt. Andere Wiederherstellungsmöglichkeiten verwenden:

   - [Nur bei Wiederherstellung aus einem applikationskonformen Backup] Sollte sich das Backup im Cloud Storage oder einem freigegebenen Storage befinden (d.h., dass andere Agenten auf diesen zugreifen können), dann klicken Sie zuerst auf den Befehl **Maschine auswählen**. Wählen Sie anschließend eine Maschine aus, die online ist und auf welcher der Agent für Exchange oder der Agent für VMware installiert ist, und dann den gewünschten Recovery-Punkt.
   - Wählen Sie einen Recovery-Punkt auf der Registerkarte 'Backup Storage'.

   Die in einer der oberen Aktionen zum Durchsuchen ausgewählte Maschine wird dann die Wiederherstellung durchführen (statt der ursprünglichen Maschine, die offline ist).
5. Klicken Sie auf **Recovery** –> **Exchange-Postfächer**.
6. Wählen Sie die Postfächer aus, die Sie wiederherstellen wollen.

   Sie können die Postfächer nach einem Namen durchsuchen. Platzhalterzeichen (Wildcards) werden nicht unterstützt.




7. Klicken Sie auf **Recovery**.
8. [Nur bei Wiederherstellung zu Microsoft 365]:
   a. Wählen Sie bei **Recovery zu** den Eintrag **Microsoft 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. 481)' aufgeführt.

10. [Optional] Klicken Sie auf **Datenbank zur Neuerstellung fehlender Postfächer**, wenn Sie die automatisch ausgewählte Datenbank ändern wollen.
11. Klicken Sie auf **Recovery starten**.

Der Recovery-Fortschritt wird auf der Registerkarte **Aktivitäten** angezeigt.

***So können Sie ein Postfach aus einem Postfach-Backup wiederherstellen***

1. Klicken Sie auf **Geräte** –> **Microsoft Exchange** –> **Postfächer**.
2. Wählen Sie das wiederherzustellende Postfach und klicken Sie dann auf **Recovery**.

   Sie können die Postfächer nach einem Namen durchsuchen. Platzhalterzeichen (Wildcards) werden nicht unterstützt.

   Falls das Postfach gelöscht wurde, wählen Sie es in der Registerkarte 'Backup Storage' aus – und klicken Sie dann auf **Backups anzeigen**.
3. Wählen Sie einen Recovery-Punkt. Beachten Sie dabei, dass Recovery-Punkte nach Speicherorten gefiltert werden.
4. Klicken Sie auf **Recovery** –> **Postfach**.
5. Führen Sie die Schritte 8-11 der oberen Prozedur durch.

## Postfachelemente wiederherstellen

***So können Sie Postfachelemente aus einem applikationskonformen Backup oder einem Datenbank-Backup wiederherstellen***

1. [Nur bei Wiederherstellung eines Datenbank-Backups zu Microsoft 365] Wenn der Agent für Microsoft 365 auf der Maschine, die den Exchange Server ausführt und per Backup gesichert wurde, nicht installiert ist, gehen Sie folgendermaßen vor:
   - Falls Sie keinen Agenten für 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'.
2. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:

- Bei Wiederherstellung aus einem applikationskonformen Backup: Wählen Sie unter **Geräte** diejenige Maschine aus, auf der sich die wiederherzustellenden Daten ursprünglich befunden haben.
- Wenn Sie eine Wiederherstellung aus einem Datenbank-Backup durchführen, klicken Sie auf **Geräte** –> **Microsoft Exchange** –> **Datenbanken** – und wählen Sie dann diejenige Datenbank aus, in der sich die wiederherzustellenden Daten ursprünglich befunden haben.

3. Klicken Sie auf **Recovery**.
4. Wählen Sie einen Recovery-Punkt. Beachten Sie dabei, dass Recovery-Punkte nach Speicherorten gefiltert werden.

   Falls die Maschine offline ist, werden keine Recovery-Punkte angezeigt. Andere Wiederherstellungsmöglichkeiten verwenden:
   - [Nur bei Wiederherstellung aus einem applikationskonformen Backup] Sollte sich das Backup im Cloud Storage oder einem freigegebenen Storage befinden (d.h., dass andere Agenten auf diesen zugreifen können), dann klicken Sie zuerst auf den Befehl **Maschine auswählen**. Wählen Sie anschließend eine Maschine aus, die online ist und auf welcher der Agent für Exchange oder der Agent für VMware installiert ist, und dann den gewünschten Recovery-Punkt.
   - Wählen Sie einen Recovery-Punkt auf der Registerkarte 'Backup Storage'.

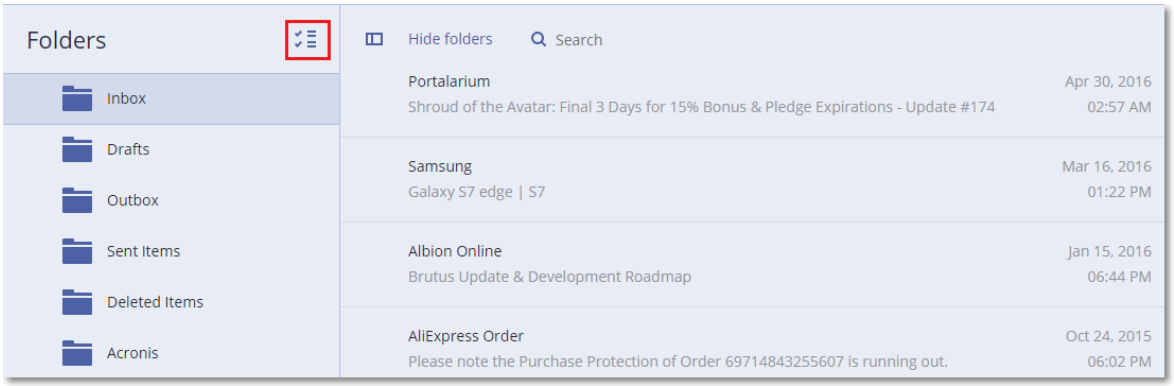
   Die in einer der oberen Aktionen zum Durchsuchen ausgewählte Maschine wird dann die Wiederherstellung durchführen (statt der ursprünglichen Maschine, die offline ist).
5. Klicken Sie auf **Recovery** –> **Exchange-Postfächer**.
6. Klicken Sie auf dasjenige Postfach, in dem sich die wiederherzustellenden Elemente ursprünglich befunden haben.
7. Wählen Sie die Elemente aus, die Sie wiederherstellen wollen.

   Folgende Suchoptionen sind verfügbar. Platzhalterzeichen (Wildcards) werden nicht unterstützt.
   - Für E-Mail-Nachrichten: Suche per Betreff, Absender, Empfänger und Datum.
   - Für Ereignisse: Suche nach Titel und Datum.
   - Für Tasks: Suche per Betreff und Datum.
   - Für Kontakte: Suche nach Namen, E-Mail-Adresse und Telefonnummer.

   Bei Auswahl einer E-Mail-Nachricht können Sie auf **Inhalt anzeigen** klicken, damit Ihnen die Nachricht (inkl. Anhänge) angezeigt wird.

   **Hinweis**
   Sie können eine angehängte Datei herunterladen, indem Sie auf deren Namen klicken.

   Wenn Sie Ordner auswählen wollen, klicken Sie auf das Symbol zum Wiederherstellen von Ordnern.




8. Klicken Sie auf **Recovery**.
9. Wenn Sie eine Wiederherstellung zu Microsoft 365 durchführen 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. 481)' aufgeführt.
11. Bei **Zielpostfach** können Sie das gewünschte Zielpostfach anzeigen lassen, ändern oder spezifizieren.

    Das ursprüngliche Postfach wird automatisch vorausgewählt. Wenn dieses Postfach nicht existiert oder Sie eine andere als die ursprüngliche Maschine als Ziel ausgewählt haben, müssen Sie das Zielpostfach spezifizieren.
12. [Nur bei Wiederherstellung von E-Mail-Nachrichten] Bei **Zielordner** können Sie den Zielordner im Zielpostfach einsehen oder ändern. Standardmäßig ist der Ordner **Wiederhergestellte Elemente** vorausgewählt. Aufgrund von Microsoft Exchange-Beschränkungen werden Kalendereereignisse, Aufgaben und Notizen immer zu ihrem ursprünglichen Ordner wiederhergestellt, unabhängig davon, ob ein anderer **Zielordner** spezifiziert wurde.
13. Klicken Sie auf **Recovery starten**.

Der Recovery-Fortschritt wird auf der Registerkarte **Aktivitäten** angezeigt.

***So können Sie ein Postfachelement aus einem Postfach-Backup wiederherstellen***

1. Klicken Sie auf **Geräte** –> **Microsoft Exchange** –> **Postfächer**.
2. Wählen Sie dasjenige Postfach aus, in dem sich die wiederherzustellenden Elemente ursprünglich befunden haben – und klicken Sie dann auf **Recovery**.
   Sie können die Postfächer nach einem Namen durchsuchen. Platzhalterzeichen (Wildcards) werden nicht unterstützt.
   Falls das Postfach gelöscht wurde, wählen Sie es in der Registerkarte 'Backup Storage' aus – und klicken Sie dann auf **Backups anzeigen**.
3. Wählen Sie einen Recovery-Punkt. Beachten Sie dabei, dass Recovery-Punkte nach Speicherorten gefiltert werden.
4. Klicken Sie auf **Recovery** –> **E-Mail-Nachrichten**.
5. Wählen Sie die Elemente aus, die Sie wiederherstellen wollen.
   Folgende Suchoptionen sind verfügbar. Platzhalterzeichen (Wildcards) werden nicht unterstützt.
   - Für E-Mail-Nachrichten: Suche per Betreff, Absender, Empfänger und Datum.
   - Für Ereignisse: Suche nach Titel und Datum.
   - Für Tasks: Suche per Betreff und Datum.
   - Für Kontakte: Suche nach Namen, E-Mail-Adresse und Telefonnummer.

   Bei Auswahl einer E-Mail-Nachricht können Sie auf **Inhalt anzeigen** klicken, damit Ihnen die Nachricht (inkl. Anhänge) angezeigt wird.

   **Hinweis**
   Sie können eine angehängte Datei herunterladen, indem Sie auf deren Namen klicken.

   Wenn eine E-Mail-Nachricht ausgewählt wurde, können Sie auf **Als E-Mail senden** klicken, damit die Nachricht an eine bestimmte E-Mail-Adresse gesendet wird. Als Absender der Nachricht wird die E-Mail-Adresse Ihres Administrator-Kontos verwendet.

   Wenn Sie Ordner auswählen wollen, klicken Sie auf das Symbol 'Ordner wiederherstellen': 
6. Klicken Sie auf **Recovery**.
7. Führen Sie die Schritte 9-13 der oberen Prozedur durch.

## Microsoft Exchange-Bibliotheken kopieren

Wenn Sie Exchange-Postfächer oder Postfach-Elemente zu Microsoft 365 wiederherstellen wollen, müssen Sie möglicherweise die folgenden Bibliotheken von der Maschine, die per Backup gesichert wurde (oder von einer anderen Maschine mit derselben Microsoft Exchange Server-Version), zu derjenigen Maschine kopieren, auf welcher sich der Agent für Microsoft 365 befindet.

Kopieren Sie – entsprechend der gesicherten Microsoft Exchange Server-Version – die folgenden Dateien:

| Microsoft Exchange Server-Version | Bibliotheken | Standardspeicherort |
|---|---|---|

| | | |
|---|---|---|
| Microsoft Exchange Server 2010 | ese.dll<br>esebcli2.dll<br>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<br>msvcp110.dll | %WINDIR%\system32 |

Die Bibliotheken sollten in diesem Ordner gespeichert werden: **%ProgramData%\Acronis\ese**. Wenn dieser Ordner noch nicht existiert, müssen Sie ihn manuell erstellen.

# Die SQL Server- oder Exchange Server-Zugriffsanmeldedaten ändern

Sie können die Zugriffsanmeldedaten für einen SQL Server oder Exchange Server ändern, ohne den entsprechenden Agenten neu installieren zu müssen.

***So ändern Sie die Anmeldedaten für einen SQL Server oder Exchange Server***

1. Klicken Sie auf **Geräte** und anschließend auf **Microsoft SQL** oder **Microsoft Exchange**.
2. Wählen Sie die AlwaysOn-Verfügbarkeitsgruppe, Datenbankverfügbarkeitsgruppe, SQL Server-Instanz oder den Exchange Server, für die/den Sie die Anmeldedaten ändern wollen.
3. Klicken Sie auf **Anmeldedaten spezifizieren**.
4. Spezifizieren Sie die neuen Anmeldedaten und klicken Sie abschließend auf **OK**.

***So ändern Sie die Anmeldedaten eines Exchange Servers bei einem Postfach-Backup***

1. Klicken Sie auf **Geräte** –> **Microsoft Exchange**und erweiteren Sie dann **Postfächer**.
2. Wählen Sie den Exchange Server aus, dessen Anmeldedaten Sie ändern wollen.
3. Klicken Sie auf **Einstellungen**.
4. Spezifizieren Sie bei **Exchange-Administratorkonto** die neuen Zugriffsanmeldedaten und klicken Sie anschließend auf **Speichern**.

# Microsoft 365-Postfächer sichern

**Wichtig**
Dieser Abschnitt gilt für On-Premise-Bereitstellungen von Acronis Cyber Protect. Wenn Sie eine Cloud-Bereitstellung verwenden, sollten Sie sich unter https://www.acronis.com/support/documentation/CyberProtectionService/#protecting-microsoft-365-data.html informieren.

Weitere Informationen zu den Lizenzierungsoptionen finden Sie im Abschnitt 'Acronis Cyber Backup für Microsoft 365-Lizenzierung'.

## Warum sollten Sie Microsoft 365-Postfächer per Backup sichern?

Microsoft 365 ist zwar ein Cloud-Dienst, ein regelmäßiges Backup bietet jedoch eine zusätzliche Schutzebene gegen Anwenderfehler und vorsätzliche böswillige Angriffe. Sie können gelöschte Elemente auch dann noch aus einem Backup wiederherstellen, wenn die offizielle Microsoft 365-Aufbewahrungsdauer abgelaufen ist. Zusätzlich können Sie eine lokale Kopie Ihrer Microsoft 365-Postfächer speichern, falls Sie dies aufgrund von gesetzlichen oder firmeninternen Vorschriften tun müssen.

## Recovery

Folgende Elemente können aus einem Postfach-Backup wiederhergestellt werden:

- Postfächer
- E-Mail-Ordner
- E-Mail-Nachrichten
- Kalenderereignisse
- Aufgaben
- Kontakte
- Journal-Einträge
- Hinweise

Sie können eine Suchfunktion verwenden, um bestimmte Elemente zu finden.

Wiederherstellungen können zu Microsoft 365 oder zu einem aktiv laufenden Exchange Server durchgeführt werden.

Wenn bei einer Postfach-Wiederherstellung ein vorhandenes Microsoft 365-Postfach als Ziel ausgewählt wird, werden alle dort vorliegenden Elemente, die übereinstimmende IDs haben, überschrieben. Wenn ein Postfach zu einem vorhandenen Exchange Server-Postfach

wiederhergestellt wird, bleiben dort bereits vorhandene Elemente erhalten. Die wiederhergestellten Elemente werden neben den vorhandenen gespeichert.

Bei einer Wiederherstellung von Postfachelementen werden keinerlei Elemente überschrieben. Stattdessen wird der vollständige Pfad zu einem Postfachelement im Zielordner neu erstellt.

# Einschränkungen

- Einen Schutzplan auf mehr als 500 Postfächer anzuwenden, kann die Backup-Performance verschlechtern. Wenn Sie besonders viele Postfächer schützen wollen, erstellen Sie mehrere Schutzpläne und lassen Sie diese per Planung zu unterschiedlichen Zeiten ausführen.
- Archivpostfächer (**In-Situ-Archiv**) können nicht gesichert werden.
- 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.
- Wiederherstellungen zu einem neuen Microsoft 365-Postfach sind nicht möglich. Sie müssen zuerst einen neuen Microsoft 365-Benutzer manuell erstellen und dann die gewünschten Elemente zum Postfach dieses Benutzers wiederherstellen.
- Wiederherstellungen zu einer anderen Microsoft 365-Organisation werden nicht unterstützt.
- Einige Element-Typen oder -Eigenschaften, die von Microsoft 365 unterstützt werden, werden möglicherweise nicht vom Exchange Server unterstützt. Bei einer Wiederherstellung zum Exchange Server werden diese dann übersprungen.

# Eine Microsoft 365-Organisation hinzufügen

Wenn Sie eine Microsoft-Organisation hinzufügen wollen, müssen Sie Ihre Anwendungs-ID, das Anwendungsgeheimnis und die Microsoft 365-Mandanten-ID kennen. Weitere Informationen dazu, wie Sie diese Informationen finden können, sind im Abschnitt 'Anwendungs-ID und Anwendungsgeheimnis abrufen' aufgeführt.

***So können Sie eine Microsoft 365-Organisation hinzufügen***

1. Installieren Sie den Agenten für Office 365 auf einer Windows-Maschine, die über eine Internetverbindung verfügt. Innerhalb einer Organisation darf es nur einen Agenten für Office 365 geben.
2. Klicken Sie in der Cyber Protect Webkonsole auf **Microsoft Office 365**.
3. Geben Sie in dem sich öffnenden Fenster Ihre Anwendungs-ID, Ihr Anwendungsgeheimnis und die Microsoft 365-Mandanten-ID ein.
4. Klicken Sie auf **Anmelden**.

Als Ergebnis erscheinen die Datenelemente Ihrer Organisation in der Cyber Protect-Webkonsole auf der Registerkarte **Microsoft Office 365**.

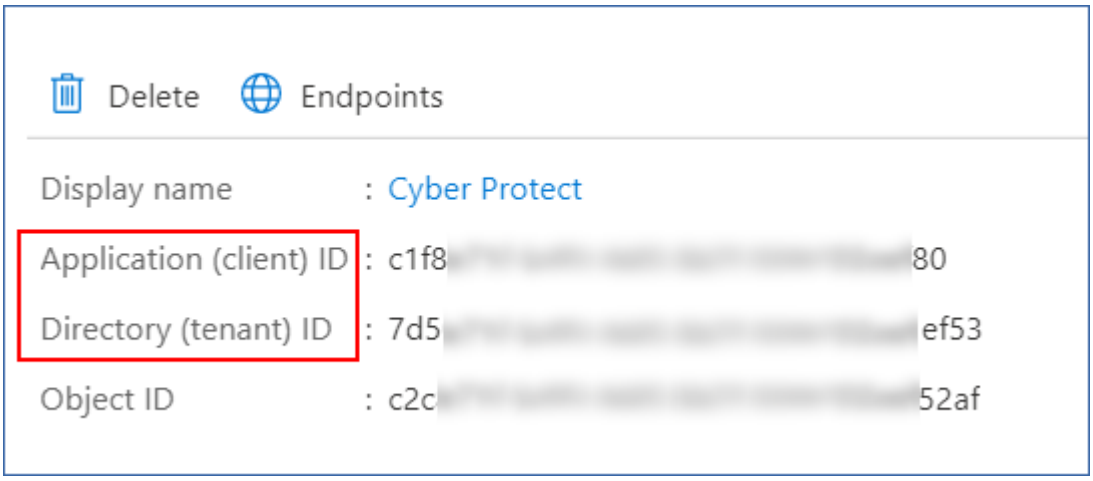
# Anwendungs-ID und Anwendungsgeheimnis abrufen

Um die moderne Authentifizierung für Microsoft 365 verwenden zu können, müssen Sie eine benutzerdefinierte Anwendung im Azure Active Directory erstellen und dieser spezifische API-Berechtigungen gewähren. Dadurch erhalten Sie die **Anwendungs-ID**, das **Anwendungsgeheimnis** und **Verzeichnis-(Mandanten)-ID**, die Sie in die Cyber Protect-Webkonsole eingeben müssen.

***So können Sie eine Anwendung im Azure Active Directory erstellen***

1. Melden Sie sich am Azure-Portal als Administrator an.
2. Gehen Sie zu **Azure Active Directory** –> **App-Registrierungen** und klicken Sie dann auf **Neue Registrierung**.
3. Spezifizieren Sie einen Namen für Ihre benutzerdefinierte Anwendung – beispielsweise: Cyber Protect.
4. Wählen Sie bei **Unterstützte Kontotypen** die Option **Nur Konten in diesem Organisationsverzeichnis**.
5. Klicken Sie auf **Registrieren**.

Ihr Anwendung ist nun erstellt. Gehen Sie im Azure-Portal zur **Übersichtsseite** der Anwendung und überprüfen Sie die ID Ihrer Anwendung (Client-ID) und des Verzeichisses (Mandanten-ID).




Weitere Informationen darüber, wie Sie eine Anwendung im Azure-Portal erstellen, finden Sie in der Microsoft-Dokumentation.

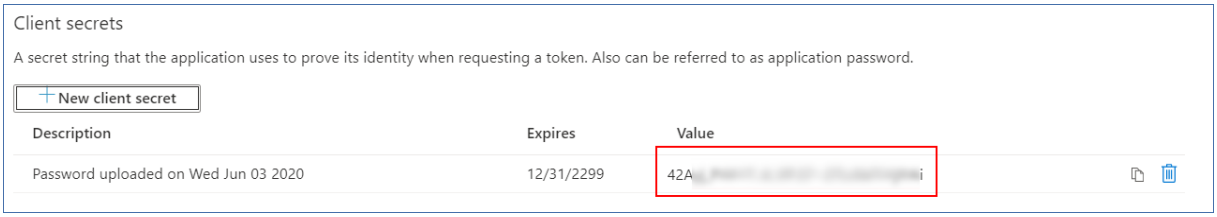
***So können Sie Ihrer Anwendung die erforderlichen API-Berechtigungen erteilen***

1. Gehen Sie im Azure-Portal zu den **API-Berechtigungen** der Anwendung und klicken Sie auf **Eine Berechtigung hinzufügen**.
2. Wählen Sie die Registerkarte **APIs, die mein Unternehmen verwendet** aus und suchen Sie dann nach **Office 365 Exchange Online**.
3. Klicken Sie zuerst auf **Office 365 Exchange Online** und anschließend auf **Anwendungsberechtigungen**.

4. Aktiveren Sie das Kontrollkästchen **full_access_as_app** (Vollzugriff_als_App) und klicken Sie dann auf **Berechtigungen hinzufügen**.
5. Klicken Sie bei **API-Berechtigungen** auf **Eine Berechtigung hinzufügen**.
6. Wählen Sie **Microsoft Graph**.
7. Wählen Sie **Anwendungsberechtigungen**.
8. Erweitern Sie die Registerkarte **Verzeichnis** und aktivieren Sie das Kontrollkästchen **Directory.Read.All** (Verzeichnis.Lesen.Alles). Klicken Sie auf **Berechtigungen hinzufügen**.
9. Aktivieren Sie alle Berechtigungen und klicken Sie dann auf **Administratoreinwilligung gewähren für <Name Ihrer Anwendung>**.
10. Bestätigen Sie Ihre Wahl durch Klicken auf **Ja**.

***So können Sie ein Anwendungsgeheimnis erstellen***

1. Gehen Sie im Azure-Portal zum Bereich **Zertifikate & Geheimnisse** –> **Neuer geheimer Clientschlüssel** für Ihre Anwendung.
2. Wählen Sie in dem sich öffnenden Dialogfeld die Option 'Gültig bis': **Nie** – und klicken Sie dann auf **Hinzufügen**.
3. Überprüfen Sie Ihr Anwendungsgeheimnis im Feld **Wert** und stellen Sie sicher, dass Sie sich dieses merken.




Weitere Informationen über das Anwendungsgeheimnis finden Sie in der Microsoft-Dokumentation.

# Die Microsoft 365-Zugriffsanmeldedaten ändern

Sie können die Zugriffsanmeldedaten für Microsoft 365 ändern, ohne den Agenten neu installieren zu müssen.

***So können Sie die Anmeldedaten für Microsoft 365 ändern***

1. Gehen Sie in der Cyber Protect-Webkonsole zu **Geräte** –> **Microsoft Office 365**.
2. Wählen Sie die Microsoft 365-Organisation aus.
3. Klicken Sie auf **Anmeldedaten spezifizieren**.
4. Geben Sie Ihre Anwendungs-ID, das Anwendungsgeheimnis und die Microsoft 365-Mandanten-ID ein. Weitere Informationen dazu, wie Sie diese finden, sind im Abschnitt 'Anwendungs-ID und Anwendungsgeheimnis abrufen' aufgeführt.
5. Klicken Sie auf **Anmelden**.

# Postfächer auswählen

Wählen Sie die Postfächer wie nachfolgend beschrieben aus – und spezifizieren Sie dann die anderen Einstellungen des Schutzplans nach Bedarf.

***So können Sie Postfächer auswählen***

1. Gehen Sie in der Cyber Protect-Webkonsole zu **Geräte** –> **Microsoft Office 365**.
2. Wählen Sie die Postfächer aus, die Sie per Backup sichern wollen.
3. Klicken Sie auf **Backup**.

# Postfächer und Postfachelemente wiederherstellen

## Postfächer wiederherstellen

1. [Nur bei Wiederherstellung zu einem Exchange Server] Stellen Sie sicher, dass es einen Exchange-Benutzer gibt, dessen Anmeldenamen dem Benutzernamen des Benutzers entspricht, dessen Postfach wiederhergestellt werden soll. Wenn dies nicht der Fall ist, erstellen Sie den Benutzer. Eine vollständige Liste der Anforderungen für diesen Benutzer finden Sie im Abschnitt '"Anforderungen an Benutzerkonten" (S. 489)'.
2. Gehen Sie in der Cyber Protect-Webkonsole zu **Geräte** –> **Microsoft Office 365**.
3. Wählen Sie das wiederherzustellende Postfach und klicken Sie dann auf **Recovery**.
   Sie können die Postfächer nach einem Namen durchsuchen. Platzhalterzeichen (Wildcards) werden nicht unterstützt.
   Falls das Postfach gelöscht wurde, wählen Sie es in der Registerkarte 'Backup Storage' aus – und klicken Sie dann auf **Backups anzeigen**.
4. Wählen Sie einen Recovery-Punkt. Beachten Sie dabei, dass Recovery-Punkte nach Speicherorten gefiltert werden.
5. Klicken Sie auf **Recovery** –> **Postfach**.
6. Wenn Sie eine Wiederherstellung zu einem Exchange Server durchführen wollen, wählen Sie bei **Recovery zu** den Eintrag **Microsoft Exchange**. Fahren Sie mit der Wiederherstellung so fort, wie es im Abschnitt '"Postfächer wiederherstellen" (S. 490)' (beginnend mit Schritt 9) beschrieben wurde. Weitere Schritte dieser Prozedur sind nicht erforderlich.
   Wenn Sie eine Wiederherstellung zu Microsoft 365 durchführen wollen, übernehmen Sie bei **Recovery zu** den Eintrag **Microsoft Office 365**.
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**.

## Postfachelemente wiederherstellen

1. [Nur bei Wiederherstellung zu einem Exchange Server] Stellen Sie sicher, dass es einen Exchange-Benutzer gibt, dessen Anmeldenamen dem Benutzernamen des Benutzers entspricht, dessen Postfach wiederhergestellt werden soll. Wenn dies nicht der Fall ist, erstellen Sie den Benutzer. Eine vollständige Liste der Anforderungen für diesen Benutzer finden Sie im Abschnitt '"Anforderungen an Benutzerkonten" (S. 489)'.
2. Gehen Sie in der Cyber Protect-Webkonsole zu **Geräte** –> **Microsoft Office 365**.
3. Wählen Sie dasjenige Postfach aus, in dem sich die wiederherzustellenden Elemente ursprünglich befunden haben – und klicken Sie dann auf **Recovery**.
   Sie können die Postfächer nach einem Namen durchsuchen. Platzhalterzeichen (Wildcards) werden nicht unterstützt.
   Falls das Postfach gelöscht wurde, wählen Sie es in der Registerkarte 'Backup Storage' aus – und klicken Sie dann auf **Backups anzeigen**.
4. Wählen Sie einen Recovery-Punkt. Beachten Sie dabei, dass Recovery-Punkte nach Speicherorten gefiltert werden.
5. Klicken Sie auf **Recovery** –> **E-Mail-Nachrichten**.
6. Wählen Sie die Elemente aus, die Sie wiederherstellen wollen.
   Folgende Suchoptionen sind verfügbar. Platzhalterzeichen (Wildcards) werden nicht unterstützt.
   - Für E-Mail-Nachrichten: Suche per Betreff, Absender, Empfänger und Datum.
   - Für Ereignisse: Suche nach Titel und Datum.
   - Für Tasks: Suche per Betreff und Datum.
   - Für Kontakte: Suche nach Namen, E-Mail-Adresse und Telefonnummer.

   Bei Auswahl einer E-Mail-Nachricht können Sie auf **Inhalt anzeigen** klicken, damit Ihnen die Nachricht (inkl. Anhänge) angezeigt wird.

   **Hinweis**
   Sie können eine angehängte Datei herunterladen, indem Sie auf deren Namen klicken.

   Wenn eine E-Mail-Nachricht ausgewählt wurde, können Sie auf **Als E-Mail senden** klicken, damit die Nachricht an eine bestimmte E-Mail-Adresse gesendet wird. Als Absender der Nachricht wird die E-Mail-Adresse Ihres Administrator-Kontos verwendet.

   Wenn Sie Ordner auswählen wollen, klicken Sie auf das Symbol 'Ordner wiederherstellen'. 
7. Klicken Sie auf **Recovery**.
8. Wenn Sie eine Wiederherstellung zu einem Exchange Server durchführen wollen, wählen Sie bei **Recovery zu** den Eintrag **Microsoft Exchange**.
   Wenn Sie eine Wiederherstellung zu Microsoft 365 durchführen wollen, übernehmen Sie bei **Recovery zu** den Eintrag **Microsoft Office 365**.

9. [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**' des Microsoft Exchange Servers 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. 481)' aufgeführt.
10. 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.
11. [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.
12. Klicken Sie auf **Recovery starten**.

# Google Workspace-Daten schützen

Dieses Feature ist nur bei den Cloud-Bereitstellungen von Acronis Cyber Protect verfügbar. Eine detaillierte Beschreibung dieser Funktionalität finden Sie unter https://www.acronis.com/support/documentation/CyberProtectionService/#protecting-google-workspace-data.html.

# Oracle Database sichern

Die Sicherung von Oracle Database wird in einem separaten Dokument erläutert, welches unter der Adresse https://dl.managed-protection.com/u/pdf/AcronisCyberProtect_15_OracleBackup_whitepaper.pdf verfügbar ist.

# Spezielle Aktionen mit virtuellen Maschinen

## Eine virtuelle Maschine aus einem Backup heraus ausführen (Instant Restore)

Sie können eine virtuelle Maschine aus einem Laufwerk-Backup heraus ausführen, welches ein Betriebssystem enthält. Mit dieser Aktion, die auch 'sofortige Wiederherstellung' oder 'Instant Restore' genannt wird, können Sie einen virtuellen Server innerhalb von Sekunden hochfahren. Die virtuellen Laufwerke werden direkt aus dem Backup heraus emuliert und belegen daher keinen Speicherplatz im Datenspeicher (Storage). Zusätzlicher Speicherplatz wird lediglich benötigt, um Änderungen, die an den virtuellen Laufwerken durchgeführt werden, zu speichern.

Wir empfehlen, 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.

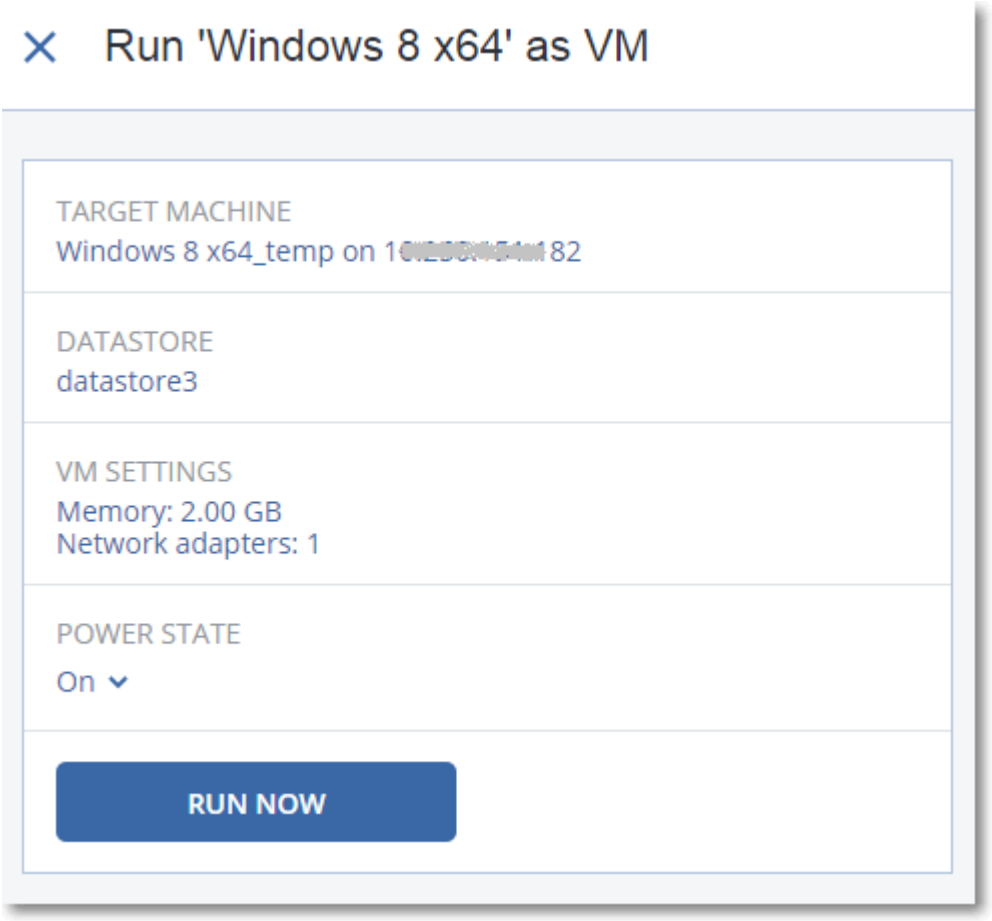
### Voraussetzungen

- Mindestens ein Agent für VMware oder Agent für Hyper-V muss für den Cyber Protection Service registriert sein.
- Das Backup kann in einem Netzwerkordner, auf einem Storage Node 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. Eine virtuelle Maschine kann nicht aus einem Backup ausgeführt werden, welches auf einem SFTP-Server, einem Bandgerät oder in der Secure Zone gespeichert ist.

- Das Backup muss eine komplette Maschine enthalten oder doch zumindest alle Volumes, die zur Ausführung des Betriebssystems notwendig sind.
- Es können sowohl die Backups von physischen wie auch virtuellen Maschinen verwendet werden. Die Backups von Virtuozzo-*Containern* können nicht verwendet werden.
- Backups, die logische Linux-Volumes (LVMs) enthalten, müssen mit dem Agenten für VMware oder Agenten für Hyper-V erstellt werden. Die virtuelle Maschine muss denselben Typ wie die Originalmaschine (ESXi oder Hyper-V) haben.

## Eine Maschine ausführen

1. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Wählen Sie eine zu sichernde Maschine, klicken Sie auf **Recovery** und wählen Sie dann einen Recovery-Punkt.
   - Wählen Sie einen Recovery-Punkt auf der Registerkarte 'Backup Storage'.
2. Klicken Sie auf **Als VM ausführen**.
   Die Software wählt den Host und die anderen benötigten Parameter automatisch aus.




3. [Optional] Klicken Sie auf **Zielmaschine** und ändern Sie den Typ der virtuellen Maschine (ESXi oder Hyper-V), den Host oder den Namen der virtuellen Maschine.
4. [Optional] Klicken Sie auf **Datenspeicher** für ESXi oder **Pfad** für Hyper-V – und bestimmten Sie dann den Datenspeicher für die neue virtuelle Maschine.

Während die Maschine ausgeführt wird, werden die (möglichen) Änderungen gesammelt, die an den virtuellen Laufwerken erfolgen. Stellen Sie sicher, dass der ausgewählte Datenspeicher genügend freien Speicherplatz hat. Wenn Sie diese Änderungen dadurch bewahren wollen, dass Sie die virtuelle Maschine zu einer 'dauerhaften' Maschine machen, müssen Sie einen Datenspeicher wählen, der für den Produktionsbetrieb der Maschine geeignet ist.

5. [Optional] Klicken Sie auf **VM-Einstellungen**, um die Größe des Arbeitsspeichers und die Netzwerkverbindungen der virtuellen Maschine zu ändern.
6. [Optional] Bestimmen Sie den Betriebszustand der VM (**An**/**Aus**).
7. Klicken Sie auf **Jetzt ausführen**.

Als Ergebnis dieser Aktion wird die Maschine in der Weboberfläche mit einem dieser Symbole angezeigt:  oder 

. Von solchen virtuellen Maschinen kann kein Backup erstellt werden.

## 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.

## 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.

# Mit VMware vSphere arbeiten

Dieser Abschnitt beschreibt Aktionen, die spezifisch für VMware vSphere-Umgebungen sind.

## Replikation von virtuellen Maschinen

Die Möglichkeit zur Replikation ist nur für virtuelle VMware ESXi-Maschinen verfügbar.

Unter Replikation wird (hier) ein Prozess verstanden, bei dem von einer virtuellen Maschine zuerst eine exakte Kopie (Replikat) erstellt wird – und dieses Replikat dann mit der ursprünglichen Maschine fortlaufend synchronisiert wird. Wenn Sie eine wichtige virtuelle Maschine replizieren, haben Sie immer eine Kopie dieser Maschine in einem startbereiten Zustand verfügbar.

Eine Replikation kann entweder manuell oder auf Basis einer (von Ihnen spezifizierten) Planung gestartet werden. Die erste Replikation ist vollständig, was bedeutet, dass die komplette Maschine kopiert wird. Alle nachfolgenden Replikationen erfolgen dann inkrementell und werden mithilfe von 'CBT (Changed Block Tracking)' durchgeführt (außer diese Option wird extra deaktiviert).

### Replikation vs. Backup

Anders als bei geplanten Backups wird bei einem Replikat immer nur der letzte (jüngste) Zustand der virtuellen Maschine aufbewahrt. Ein Replikat belegt Platz im Datenspeicher, während für Backups ein kostengünstigerer Storage verwendet werden kann.

Das Aktivieren eines Replikats geht jedoch deutlich schneller als eine klassische Wiederherstellung aus einem Backup – und ist auch schneller als die Ausführung einer virtuellen Maschine aus einem Backup. Ein eingeschaltetes Replikat arbeitet schneller als eine VM, die aus einem Backup ausgeführt wird, und es muss kein Agent für VMware geladen werden.

### Anwendungsbeispiele

- **Sie replizieren virtuelle Maschinen zu einem Remote-Standort.**
  Die Replikation ermöglicht Ihnen, teilweise oder vollständige Datacenter-Ausfälle zu überstehen, indem Sie die virtuellen Maschinen von einem primären zu einem sekundären Standort klonen. Als sekundärer Standort wird üblicherweise eine entfernt gelegene Einrichtung verwendet, die normalerweise nicht von denselben Störereignissen (Katastrophen in der Umgebung, Infrastrukturprobleme etc.) wie der primäre Standort betroffen wird/werden kann.
- **Sie replizieren virtuelle Maschinen innerhalb eines Standortes (von einem Host/Datenspeicher zu einem anderen).**
  Eine solche Onsite-Replikation kann zur Gewährleistung einer hohen Verfügbarkeit und für Disaster Recovery-Szenarien verwendet werden.

## Das können Sie mit einem Replikat tun

- **Ein Replikat testen**

  Das Replikat wird für den Test eingeschaltet. Verwenden Sie den vSphere Client oder andere Tools, um die korrekte Funktion des Replikats zu überprüfen. Die Replikation wird angehalten, solange der Test läuft.
- **Failover auf ein Replikat**

  Bei einem Failover wird der Workload der ursprünglichen virtuellen Maschine auf ihr Replikat verschoben. Die Replikation wird angehalten, solange die Failover-Aktion läuft.
- **Das Replikat sichern**

  Backup und Replikation erfordern beide einen Zugriff auf virtuelle Laufwerke, wodurch wiederum der Host, auf dem die virtuelle Maschine läuft, in seiner Performance beeinflusst wird. Wenn Sie von einer virtuellen Maschine sowohl Backups als auch ein Replikat haben wollen, der Produktions-Host dadurch aber nicht zusätzlich belastet werden soll, dann replizieren Sie die Maschine zu einem anderen Host. Dieses Replikat können Sie anschließend per Backup sichern.

## Einschränkungen

Folgende Arten von virtuellen Maschinen können nicht repliziert werden:

- Fehlertolerante Maschinen, die auf ESXi 5.5 (und niedriger) laufen.
- Maschine, die aus Backups ausgeführt werden.
- Die Replikate von virtuellen Maschinen.

## Einen Replikationsplan erstellen

Ein Replikationsplan muss für jede Maschine individuell erstellt werden. Es ist nicht möglich, einen vorhandenen Plan auf andere Maschinen anzuwenden.

***So erstellen Sie einen Replikationsplan***

1. Wählen Sie eine virtuelle Maschine aus, die repliziert werden soll.
2. Klicken Sie auf **Replikation**.

   Die Software zeigt eine Vorlage für den neuen Replikationsplan an.
3. [Optional] Wenn Sie den Namen des Replikationsplans ändern wollen, klicken Sie auf den vorgegebenen Standardnamen.
4. Klicken Sie auf **Zielmaschine** – und gehen Sie dann folgendermaßen vor:
   a. Bestimmen Sie, ob ein neues Replikat erstellt werden oder ein bereits vorhandenes Replikat der Maschine verwendet werden soll.
   b. Wählen Sie den ESXi-Host und spezifizieren Sie einen Namen für das neue Replikat – oder wählen Sie eine bereits vorhandenes Replikat aus.

      Der Standardname für ein neues Replikat ist **[Name der ursprünglichen Maschine]_**

**replica**.

c. Klicken Sie auf **OK**.

5. [Nur bei Replikation zu einer neuen Maschine] Klicken Sie auf **Datenspeicher** und bestimmten Sie dann den Datenspeicher für die neue virtuelle Maschine.
6. [Optional] Klicken Sie auf **Planung**, wenn Sie die Planung für die Replikation ändern wollen.

   Die Replikation erfolgt standardmäßig einmal am Tag – und zwar von Montag bis Freitag. Sie können den genauen Zeitpunkt festlegen, an dem die Replikation ausgeführt werden soll.

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

   Sie außerdem noch Folgendes tun:

   - Sie können einen Datumsbereich für die Planung festlegen, zu dem die entsprechende Operation ausgeführt werden soll. Aktivieren Sie das Kontrollkästchen **Den Plan in einem Datumsbereich ausführen** und spezifizieren Sie anschließend den gewünschten Datumsbereich.
   - Sie können die Planung deaktivieren. In diesem Fall kann die Replikation manuell gestartet werden.
7. [Optional] Klicken Sie auf das Zahnradsymbol, wenn Sie die Replikationsoptionen anpassen wollen.
8. Klicken Sie auf **Anwenden**.
9. [Optional] Wenn Sie den Plan manuell ausführen wollen, klicken im Fensterbereich für die Planung auf **Jetzt ausführen**.

Wenn ein Replikationsplan ausgeführt wird, erscheint das virtuelle Maschinen-Replikat in der Liste '**Alle Geräte**' und wird mit diesem Symbol gekennzeichnet: 


## Ein Replikat testen

***So bereiten Sie ein Replikat für einen Test vor***

1. Wählen Sie ein Replikat aus, das getestet werden soll.
2. Klicken Sie auf **Replikat testen**.
3. Klicken Sie auf **Test starten**.
4. Bestimmen Sie, ob das eingeschaltete Replikat mit dem Netzwerk verbunden werden soll. Die Standardvorgabe ist, dass das Replikat nicht mit dem Netzwerk verbunden wird.
5. [Optional] Falls Sie das Replikat mit dem Netzwerk verbinden wollen, müssen Sie das Kontrollkästchen **Ursprüngliche virtuelle Maschine stoppen** aktivieren, damit die ursprüngliche Maschine angehalten wird, bevor das Replikat eingeschaltet wird.
6. Klicken Sie auf **Start**.

***So stoppen Sie den Test eines Replikats***

1. Wählen Sie das Replikat aus, welches gerade getestet wird.
2. Klicken Sie auf **Replikat testen**.
3. Klicken Sie auf **Test stoppen**.
4. Bestätigen Sie Ihre Entscheidung.

## Ein Failover auf ein Replikat durchführen

***So führen Sie einen Failover von einer Maschine auf ein Replikat durch***

1. Wählen Sie ein Replikat aus, auf welches der Failover erfolgen soll.
2. Klicken Sie auf **Replikat-Aktionen**.
3. Klicken Sie auf **Failover**.
4. Bestimmen Sie, ob das eingeschaltete Replikat mit dem Netzwerk verbunden werden soll. Als Standardvorgabe wird das Replikat mit demselben Netzwerk wie die ursprüngliche Maschine verbunden.
5. [Optional] Falls Sie das Replikat mit dem Netzwerk verbinden wollen, müssen Sie das Kontrollkästchen **Ursprüngliche virtuelle Maschine stoppen** deaktivieren, wenn die ursprüngliche Maschine online bleiben soll.
6. Klicken Sie auf **Start**.

Während sich das Replikat im Failover-Stadium befindet, können Sie eine der folgenden Aktionen wählen:

- **Failover stoppen**

  Stoppen Sie das Failover, wenn die ursprüngliche Maschine repariert wurde. Das Replikat wird ausgeschaltet. Die Replikation wird fortgesetzt.
- **Permanentes Failover auf das Replikat durchführen**

  Diese sofortige Aktion entfernt die 'Replikat'-Kennzeichnung von der virtuellen Maschine, sodass diese nicht mehr als Replikationsziel verwendet werden kann. Wenn Sie die Replikation wieder aufnehmen wollen, bearbeiten Sie den Replikationsplan, um diese Maschine als Quelle auszuwählen.
- **Failback**

  Führen Sie einen Failback aus, falls Sie einen Failover zu einer Site gemacht haben, die nicht für den Dauerbetrieb gedacht ist. Das Replikat wird zu der ursprünglichen oder einer neuen virtuellen Maschine wiederhergestellt. Sobald die Wiederherstellung zu der ursprünglichen Maschine abgeschlossen ist, wird diese eingechaltet und die Replikation fortgesetzt. Wenn Sie die Wiederherstellung zu einer neuen Maschine durchgeführt haben, bearbeiten Sie den Replikationsplan, um diese Maschine als Quelle auszuwählen.

## Failover 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.

## Einen permanenten Failover durchführen

***So können Sie einen permanenten Failover durchführen***

1. Wählen Sie ein Replikat, das sich im Failover-Stadium befindet.
2. Klicken Sie auf **Replikat-Aktionen**.
3. Klicken Sie auf **Permanentes Failover**.
4. [Optional] Ändern Sie den Namen der virtuellen Maschine.
5. [Optional] Aktivieren Sie das Kontrollkästchen **Ursprüngliche virtuelle Maschine stoppen**.
6. Klicken Sie auf **Start**.

## Ein Failback durchführen

***So führen Sie einen Failback von einem Replikat durch***

1. Wählen Sie ein Replikat, das sich im Failover-Stadium befindet.
2. Klicken Sie auf **Replikat-Aktionen**.
3. Klicken Sie auf **Failback vom Replikat**.
   Die Software wählt automatisch die ursprüngliche Maschine als Zielmaschine aus.
4. [Optional] Klicken Sie auf **Zielmaschine** – und gehen Sie dann folgendermaßen vor:
   a. Bestimmen Sie, ob der Failback zu einer neuen oder einer bereits vorhandenen Maschine durchgeführt werden soll.
   b. Wählen Sie den ESXi-Host und spezifizieren Sie einen Namen für die neue Maschine – oder wählen Sie eine bereits vorhandene Maschine aus.
   c. Klicken Sie auf **OK**.
5. [Optional] Wenn Sie eine neue Maschine als Failback-Ziel verwenden, können Sie außerdem noch Folgendes tun:
   - Klicken Sie auf **Datenspeicher**, um den Datenspeicher für die virtuelle Maschine festzulegen.
   - Klicken Sie auf **VM-Einstellungen**, um die Größe des Arbeitsspeichers, die Anzahl der Prozessoren und die Netzwerkverbindungen für die virtuelle Maschine zu ändern.
6. [Optional] Klicken Sie auf **Recovery-Optionen**, wenn Sie die Failback-Optionen ändern wollen.
7. Klicken Sie auf **Recovery starten**.
8. Bestätigen Sie Ihre Entscheidung.

## Replikationsoptionen

Wenn Sie die Replikationsoptionen ändern wollen, klicken Sie auf das Zahnradsymbol neben dem Namen des Replikationsplans und dann auf das Element **Replikationsoptionen**.

### Changed Block Tracking (CBT)

Diese Option entspricht im Wesentlichen der Backup-Option 'CBT (Changed Block Tracking)'.

### Laufwerk-Provisioning

Diese Option definiert den Laufwerk-Provisioning-Modus für das Replikat.

Die Voreinstellung ist: **Thin Provisioning**.

Folgende Werte sind verfügbar: **Thin Provisioning**, **Thick Provisioning**, **Ursprüngliche Einstellung behalten**.

### Fehlerbehandlung

Diese Option entspricht im Wesentlichen der Backup-Option 'Fehlerbehandlung'.

### Vor-/Nach-Befehle

Diese Option entspricht im Wesentlichen der Backup-Option 'Vor-/Nach-Befehle'.

### VSS (Volume Shadow Copy Service) für virtuelle Maschinen

Diese Option entspricht im Wesentlichen der Backup-Option 'VSS (Volume Shadow Copy Service) für virtuelle Maschinen'.

## Failback-Optionen

Wenn Sie die Failback-Optionen ändern wollen, klicken Sie während der Failbackup-Konfiguration auf **Recovery-Optionen**.

### Fehlerbehandlung

Diese Option entspricht im Wesentlichen der Recovery-Option 'Fehlerbehandlung'.

### Performance

Diese Option entspricht im Wesentlichen der Recovery-Option 'Performance'.

### Vor-/Nach-Befehle

Diese Option entspricht im Wesentlichen der Recovery-Option 'Vor-/Nach-Befehle'.

### VM-Energieverwaltung

Diese Option entspricht im Wesentlichen der Recovery-Option 'VM-Energieverwaltung'.

## Seeding eines anfänglichen Replikats

Um die Replikation zu einem Remote-Standort zu beschleunigen und Netzwerkbandbreite einzusparen, können Sie ein Replikat-Seeding durchführen.

**Wichtig**
Um ein Replikat-Seeding durchführen zu können, muss der Agent für VMware (Virtuelle Appliance) auf dem ESXi-Zielhost ausgeführt werden.

***So führen Sie das Seeding eines anfänglichen Replikats durch***

1. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Wenn die ursprüngliche Maschine ausgeschaltet werden kann, tun Sie dies – und springen sie dann zu Schritt 4.
   - Wenn die ursprüngliche virtuelle Maschine nicht ausgeschaltet werden kann, fahren Sie mit dem nächsten Schritt fort.
2. Erstellen Sie einen Replikationsplan.

   Wählen Sie beim Erstellen des Plans bei **Zielmaschine** die Option **Neues Replikat** sowie den ESXi, der die ursprüngliche Maschine hostet.
3. Führen Sie den Plan einmal aus.

   Auf dem ursprünglichen ESXi wird ein Replikat erstellt.
4. Exportieren Sie die Dateien der virtuellen Maschine (oder des Replikats) auf ein externes Festplattenlaufwerk.
   a. Verbinden Sie das externe Laufwerk mit der Maschine, auf welcher der vSphere Client ausgeführt wird.
   b. Verbinden Sie den vSphere Client mit dem ursprünglichen vCenter/ESXi.
   c. Wählen Sie das neu erstellte Replikat in der Bestandsliste (Inventory) aus.
   d. Klicken Sie auf **Datei** –> **Exportieren** –> **OVF-Vorlage exportieren**.
   e. Spezifizieren Sie im **Verzeichnis** den entsprechenden Ordner auf dem externen Laufwerk.
   f. Klicken Sie auf **OK**.
5. Senden Sie das Festplattenlaufwerk zum Remote-Standort.
6. Importieren Sie das Replikat in den ESXi-Zielhost.
   a. Verbinden Sie das externe Laufwerk mit der Maschine, auf welcher der vSphere Client ausgeführt wird.
   b. Verbinden Sie den vSphere Client mit dem Ziel-vCenter/-ESXi.
   c. Klicken Sie auf **Datei** –> **OVF-Vorlage bereitstellen**.
   d. Spezifizieren Sie bei **Von einer Datei oder URL bereitstellen** die Vorlage, die Sie in Schritt 4 exportiert haben.
   e. Schließen Sie die Import-Prozedur ab.

7. Bearbeiten Sie den Replikationsplan, den Sie in Schritt 2 erstellt haben. Wählen Sie bei **Zielmaschine** die Option **Vorhandenes Replikat** und wählen Sie dann das importierte Replikat aus.

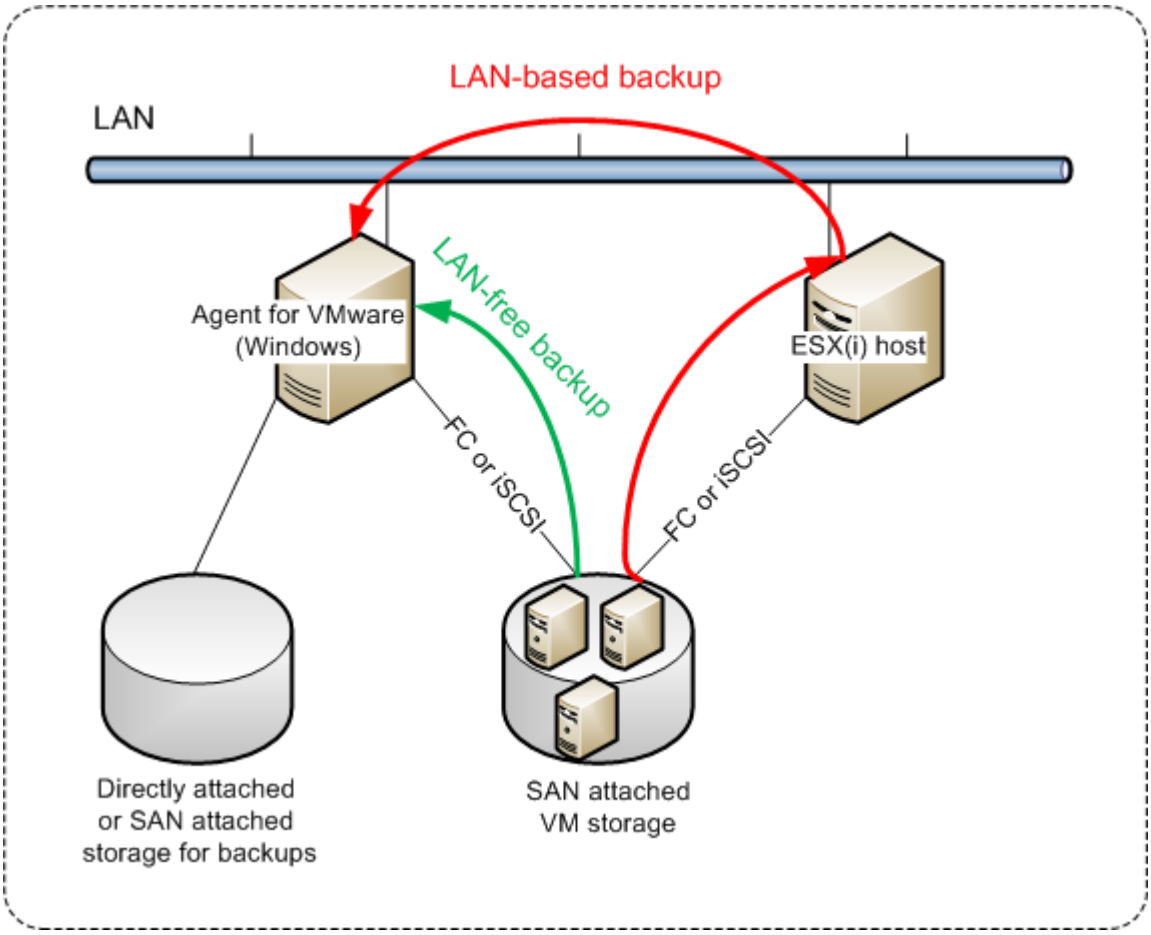
Die Software wird daraufhin die Aktualisierung des Replikats fortsetzen. Alle Replikationen werden inkrementell sein.

## LAN-freies Backup

Falls Ihre produktiven ESXi-Hosts so stark ausgelastet sind, dass eine Ausführung der virtuellen Appliances nicht wünschenswert ist, dann sollten Sie die Installation des Agenten für VMware (Windows) auf einer physischen Maschine außerhalb der ESXi-Infrastruktur erwägen.

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.

     Um eine LUN-Initialisierung zu vermeiden, ist die **SAN-Richtlinie** während der Installation des Agenten für VMware (Windows) automatisch auf **Offline – Alle** eingestellt.

Als Ergebnis wird der Agent den SAN-Transportmodus nutzen, um auf die virtuelle Laufwerke zuzugreifen. Das bedeutet, es werden nur die blanken ('raw') LUN-Sektoren über iSCSI/FC gelesen, ohne dass das VMFS-Dateisystem erkannt wird (welches von Windows nicht unterstützt wird).

## Einschränkungen

- In vSphere 6.0 (und höher) kann der Agent den SAN-Transportmodus nicht verwenden, wenn sich einige der VM-Laufwerke auf einem „VMware Virtual Volume“ (VVol) befinden und einige nicht. Die Backups solcher virtuellen Maschinen werden daher fehlschlagen.
- Verschlüsselte virtuelle Maschinen, die mit VMware vSphere 6.5 eingeführt wurden, werden via LAN gesichert – und zwar auch dann, wenn Sie den SAN-Transportmodus für den Agenten konfiguriert haben. Der Agent wird stattdessen auf den NBD-Transportmodus zurückgreifen, weil VMware den SAN-Transportmodus beim Backup verschlüsselter virtueller Laufwerke nicht unterstützt.

## Beispiel

Falls Sie ein iSCSI-SAN verwenden, konfigurieren Sie den iSCSI-Initiator auf einer unter Windows laufenden Maschine, auf welcher der Agent für VMware installiert ist.

***So konfigurieren Sie die SAN-Richtlinie***

1. Melden Sie sich als Administrator an, öffnen Sie die Eingabeaufforderung, geben Sie den Befehl `diskpart` ein und drücken Sie dann auf die **Eingabetaste**.
2. Geben Sie `san` und drücken Sie dann die **Eingabetaste**. Überprüfen Sie, dass **SAN-Richtlinie: Offline – Alle** angezeigt wird.
3. Falls ein anderer Wert für die SAN-Richtlinie eingestellt ist:
   a. Geben Sie `san policy=offlineall` ein.
   b. Drücken Sie die **Eingabetaste**.
   c. Führen Sie Schritt 2. aus, um zu überprüfen, dass die Einstellung korrekt angewendet wurde.
   d. Starten Sie die Maschine neu.

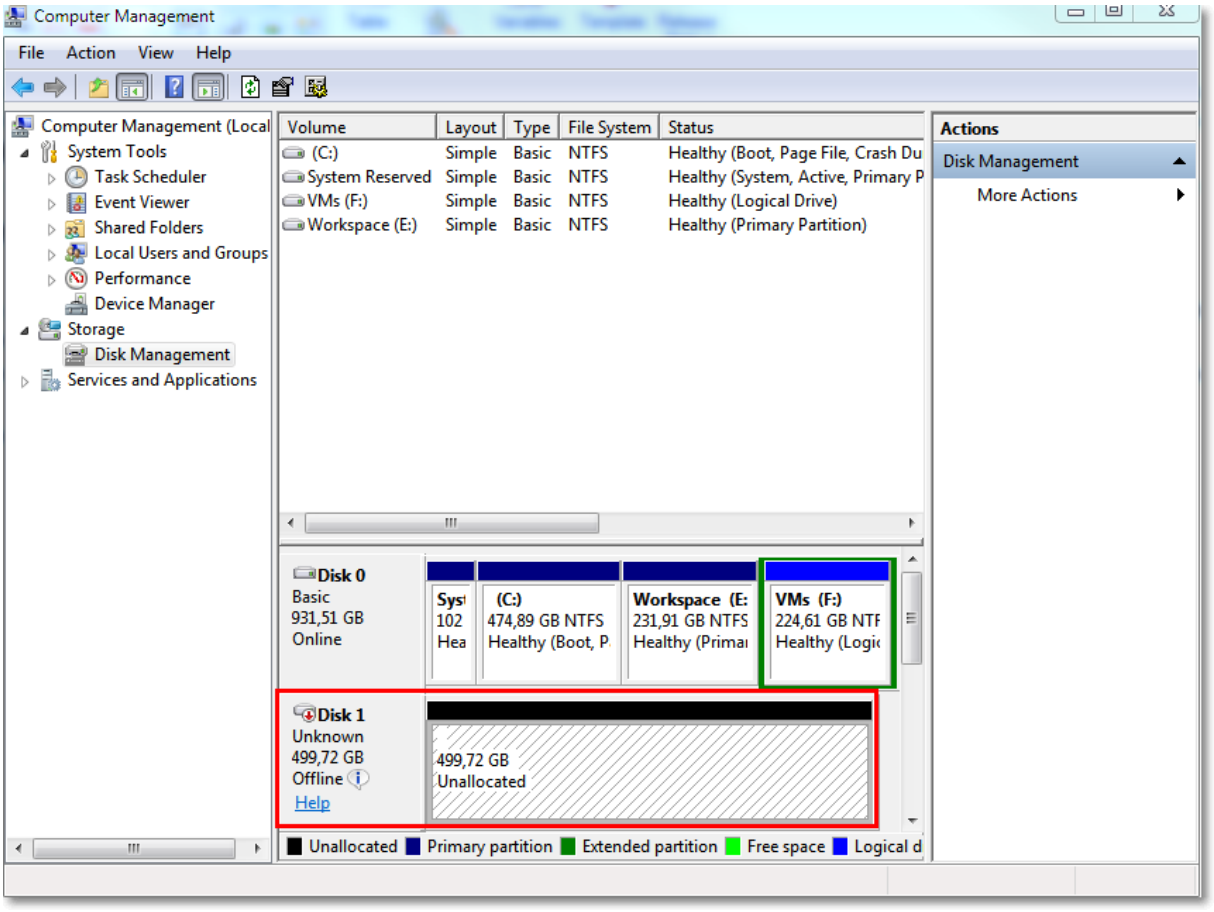
***So konfigurieren Sie einen iSCSI-Initiator***

1. Gehen Sie zu **Systemsteuerung** –> **Verwaltung** –> **iSCSI-Initiator**.

   **Hinweis**
   Wenn Sie das Systemsteuerungsmodul **Verwaltung** nicht finden können, müssen Sie evtl. die Ansicht der **Systemsteuerung** von **Start** oder **Kategorie** auf eine andere Ansicht umstellen – oder die Suchfunktion verwenden.

2. Wenn Sie den Microsoft iSCSI-Initiator das erste Mal aufrufen, müssen Sie bestätigen, dass Sie den Microsoft iSCSI-Initiator-Dienst starten wollen.
3. Geben Sie in der Registerkarte **Ziele** den vollqualifizierten Domain-Namen (FQDN) oder die IP-Adresse des SAN-Zielgerätes ein und klicken Sie dann auf **Schnell verbinden**.
4. Wählen Sie die LUN aus, die den Datenspeicher hostet, und klicken Sie dann auf **Verbinden**.
   Sollte die LUN nicht angezeigt werden, dann überprüfen Sie, dass die Zonenzuweisung auf dem iSCSI-Ziel der Maschine, die den Agenten ausführt, ermöglicht, auf die LUN zuzugreifen. Die Maschine muss in die Liste der erlaubten iSCSI-Initiatoren auf diesem Ziel aufgenommen sein.
5. Klicken Sie auf **OK**.

Die betriebsbereite SAN-LUN sollte in der **Datenträgerverwaltung** so wie im unterem Screenshot angezeigt werden.



# SAN-Hardware-Snapshots verwenden

Wenn Ihr VMwar vSphere ein SAN-Storage-System (Storage Area Network) als Datenspeicher verwendet, können Sie dem Agenten für VMware (Windows) ermöglichen, bei der Backup-Durchführung SAN-Hardware-Snapshots zu verwenden.

**Wichtig**
Nur NetApp-SAN-Storage wird unterstützt.

## Warum sollten Sie SAN-Hardware-Snapshots verwenden?

Der Agent für VMware benötigt einen Snapshot von einer virtuellen Maschine, um von dieser ein konsistentes Backup erstellen zu können. Da der Agent die Inhalte der virtuellen Laufwerke aus dem Snapshot ausliest, muss der Snapshot über die komplette Dauer des Backup-Prozesses aufbewahrt werden.

Standardmäßig verwendet der Agent die VMware-eigenen Snapshots (native VMware-Snapshots), die der ESXi-Host erstellt. Solange der Snapshot aufbewahrt wird, befinden sich die virtuellen Laufwerksdateien im 'Nur-Lesen'-Stadium – und der Host schreibt alle derweil an den Laufwerken durchgeführten Änderungen in separate Delta-Dateien. Sobald der Backup-Prozess abgeschlossen wurde, löscht der Host den Snapshot, was bedeutet, dass die Delta-Dateien mit den virtuellen Laufwerksdateien vereint werden.

Sowohl die Aufbewahrung wie auch die Löschung der Snapshots beeinflusst die Performance der virtuellen Maschinen. Bei großen virtuellen Laufwerken und schnellen Datenänderungen können diese Aktionen eine längere Zeit benötigen, in der die Performance leidet. In extremen Fällen, wenn mehrere Maschinen gleichzeitig gesichert werden, können die anwachsenden Delta-Dateien den kompletten Datenspeicher belegen und ein Ausschalten aller virtuellen Maschinen bewirken.

Sie können die Ressourcen-Belastung des Hypervisors aber reduzieren, indem Sie die Snapshots zu einem SAN auslagern. In diesem Fall sieht die Abfolge der Aktionen folgendermaßen aus:

1. Der ESXi erstellt zu Beginn des Backup-Prozesses einen VMware-Snapshot, um die virtuellen Laufwerke in einen konsistenten Zustand zu bringen.
2. Das SAN erstellt einen Hardware-Snapshot des Volumes oder der LUN, wo die virtuelle Maschine und ihr VMware-Snapshot vorliegt. Diese Aktion benötigt normalerweise nur wenige Sekunden.
3. Der ESXi löscht den VMware-Snapshot. Der Agent für VMware liest die Inhalte der virtuellen Laufwerke aus dem SAN-Hardware-Snapshot aus.

Da der VMware-Snapshot nur für ein paar Sekunden aufbewahrt wird, wird die Virtuelle-Maschinen-Performance nur mimal beeinflusst.

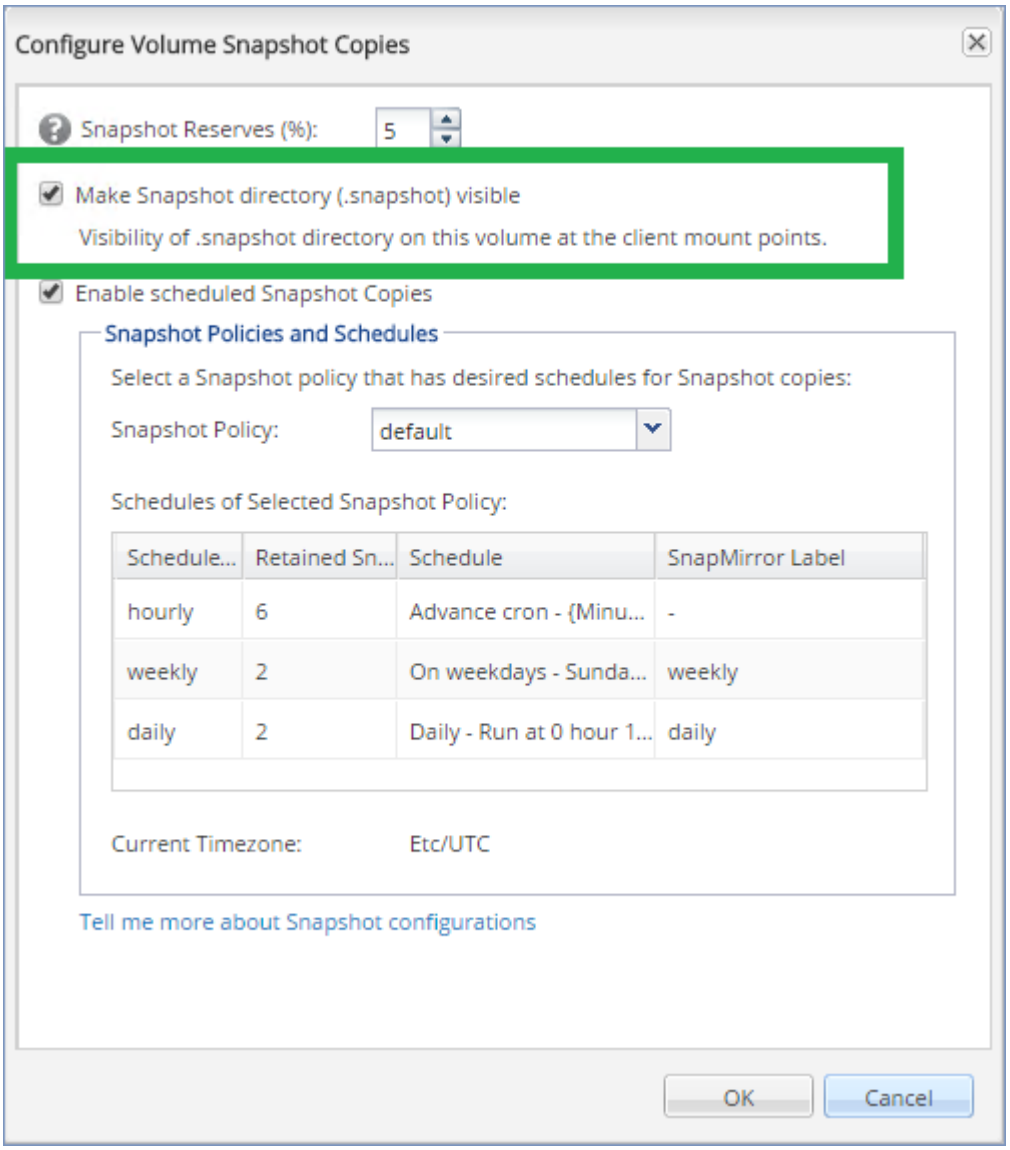
## Was benötigte ich, um SAN-Hardware-Snapshots verwenden zu können?

Wenn Sie SAN-Hardware-Snapshots beim Backup von virtuellen Maschinen verwenden wollen, sollten Sie überprüfen, dass folgende Bedingungen erfüllt sind:

- Der NetApp-SAN-Storage erfüllt die im Abschnitt 'NetApp-SAN-Storage-Anforderungen' beschriebenen Voraussetzungen.
- Die Maschine, die den Agenten für VMware (Windows) ausführt, ist wie im Abschnitt 'Die Maschine mit dem Agenten für VMware konfigurieren' beschrieben konfiguriert.
- Der SAN-Storage ist auf dem Management Server registriert.
- [Wenn es Agenten für VMware gibt, die an der oberen Registrierung nicht teilgenommen haben] Die auf dem SAN-Storage liegenden virtuellen Maschinen sind wie im Abschnitt 'Virtuelle Maschinen anbinden' beschrieben den SAN-fähigen Agenten zugewiesen.
- Die Backup-Option SAN-Hardware-Snapshots in den Schutzplan-Optionen ist aktiviert.

## NetApp-SAN-Storage-Anforderungen

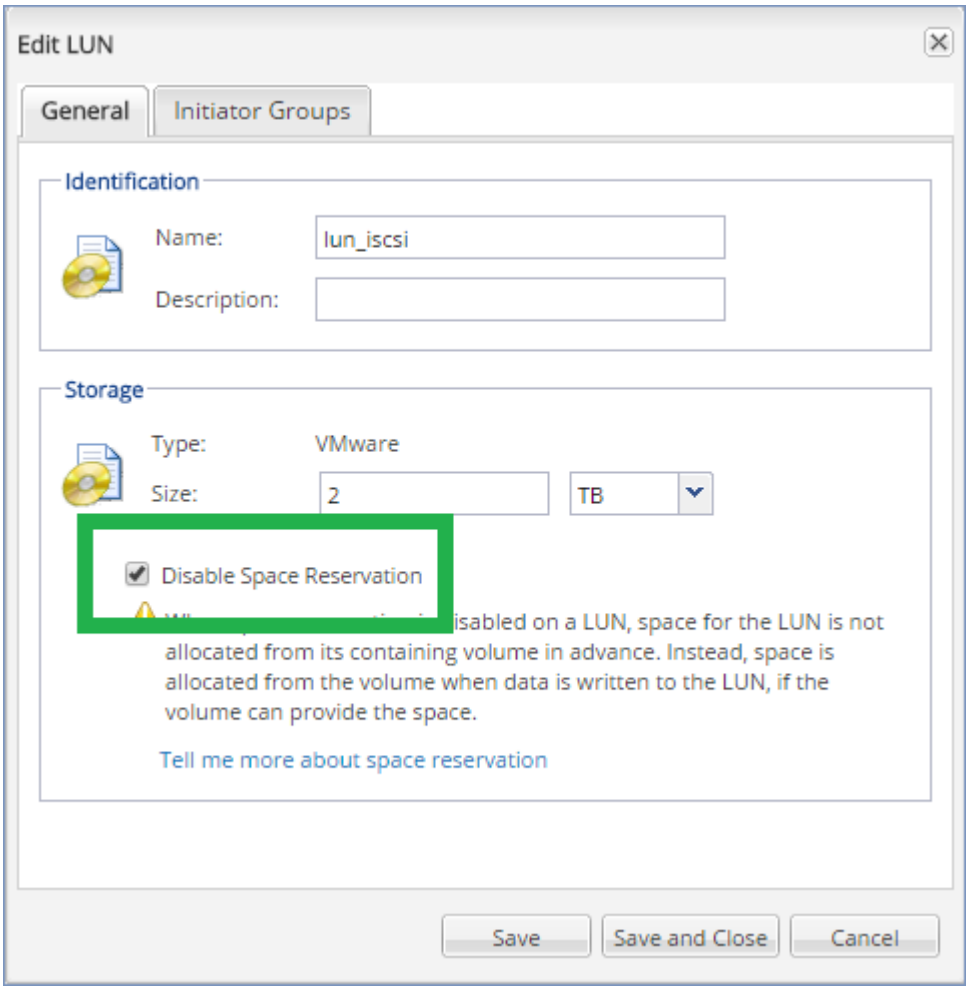
- Ein SAN-Storage mus als NFS- oder iSCSI-Datenspeicher verwendet werden.
- Das SAN muss Data ONTAP 8.1 (oder später) im **(cDOT)**-Modus (**Clustered Data ONTAP**) ausführen. Der Modus **7-Mode** wird nicht unterstützt.
- Im NetApp OnCommand System Manager muss das Kontrollkästchen **Snapshot-Kopien** –> **Konfigurieren** –> **Snapshot-Verzeichnis (.snapshot) sichtbar machen** für das Volume aktiviert sein, auf dem sich der Datenspeicher befindet.




- [Für NFS-Datenspeicher] Auf der SVM (Storage Virtual Machine), die beim Erstellen des Datenspeichers spezifiziert wurde, muss der Zugriff auf NFS-Freigaben von Windows NFSv3-Clients aktiviert sein. Der Zugriff kann mit folgendem Befehl aktiviert werden:

  ```
  vserver nfs modify -vserver [SVM name] -v3-ms-dos-client enable
  ```

  Weitere Informationen finden Sie im „Best Practices“-Dokument von NetApp: https://kb.netapp.com/support/s/article/ka21A0000000k89QAA/top-windows-nfsv3-0-issues-workarounds-and-best-practices
- [Für iSCSI-Datenspeicher] Im NetApp OnCommand System Manager muss das Kontrollkästchen **Platzreservierung deaktivieren** für die iSCSI-LUN aktiviert sein, wo der Datenspeicher vorliegt.




## Die Maschine mit dem Agenten für VMware konfigurieren

Gehen Sie in Abhängigkeit davon, ob der SAN-Storage als NFS- oder iSCSI-Datenspeicher verwendet wird, zu dem jeweils entsprechenden unteren Abschnitt.

### Den iSCSI-Initiator konfigurieren

Überprüfen Sie, dass die folgenden Punkte alle zutreffen:

- Der Microsoft iSCSI-Initiator ist installiert.
- Der Starttyp des Microsoft iSCSI-Initiator-Dienst ist auf **Automatisch** oder **Manuell** eingestellt. Diese Einstellung kann bei Bedarf über das Snap-In **Dienste** überprüft bzw. konfiguriert werden.
- Der iSCSI-Initiator ist so konfiguriert, wie es im Beispielabschnitt 'LAN-freies Backup' beschrieben ist.

### Den NFS-Client konfigurieren

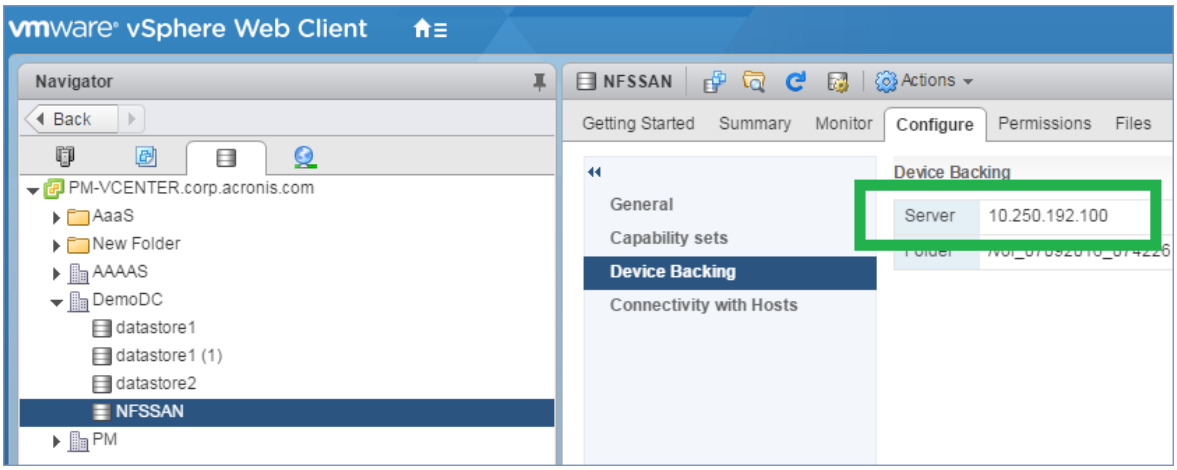
Überprüfen Sie, dass die folgenden Punkte alle zutreffen:

- Die Microsoft **Dienste für NFS** (im Windows Server 2008) oder der **Client für NFS** (im Windows Server 2012 oder später) ist installiert.

- Der NFS-Client ist für anonymen Zugriff konfiguriert. Das kann folgendermaßen erfolgen:
  a. Öffnen Sie den Registrierungseditor.
  b. Suchen Sie folgenden Registry-Schlüssel: **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ClientForNFS\CurrentVersion\Default**
  c. Erstellen Sie in diesem Schlüssel einen neuen **DWORD**-Wert mit der Bezeichnung **AnonymousUID** und legen Sie dessen Wert mit '0' fest.
  d. Erstellen Sie in demselben Schlüssel noch einen neuen **DWORD**-Wert – und zwar mit der Bezeichnung **AnonymousGID**. Legen Sie auch dessen Wert mit '0' fest.
  e. Starten Sie die Maschine neu.

## Einen SAN-Storage auf dem Management Server registrieren

1. Klicken Sie auf **Einstellungen** –> **SAN-Storage**.
2. Klicken Sie auf **Storage hinzufügen**.
3. [Optional] Ändern Sie bei **Name** die Bezeichnung für den Storage.
   Dieser Name wird später in der Registerkarte **SAN-Storage** angezeigt.
4. Spezifizieren Sie bei **Host-Name oder IP-Adresse** die NetApp-SVM (Storage Virtual Machine, auch als Filer bezeichnet), welche bei Erstellung des Datenspeichers spezifiziert wurde.
   Sie können die benötigten Informationen finden, wenn Sie im VMware vSphere Web Client den Datenspeicher wählen und dann auf **Konfigurieren** –> **Geräteunterstützung** (Device backing) klicken. Der Host-Name oder die IP-Adresse werden im Feld **Server** angezeigt.




5. Spezifizieren Sie bei **Benutzername** und **Kennwort** die SVM-Administrator-Anmeldedaten.

**Wichtig**
Das spezifizierte Konto muss ein lokaler Administrator auf der SVM sein und kein NetApp-System-Management-Administrator.

Sie können einen vorhandenen Benutzer spezifizieren oder einen neuen erstellen. Gehen Sie zum Erstellen eines neuen Benutzers im NetApp OnCommand System Manager zu **Konfiguration** –> **Sicherheit** –> **Benutzer** und erstellen Sie dann einen neuen Benutzer.

6. Wählen Sie einen oder mehrere Agenten für VMware (Windows), die Leserechte für das SAN-Gerät erhalten.
7. Klicken Sie auf **Hinzufügen**.

## Einen lokal angeschlossenen Storage verwenden

Sie können an einen Agenten für VMware (Virtuelle Appliance) ein zusätzliches Laufwerk anschließen, sodass der Agent seine Backups zu diesem lokal angeschlossenen Storage durchführen kann. Mit diesem Ansatz wird Netzwerkverkehr zwischen dem Agenten und dem Backup-Speicherort vermieden.

Eine virtuelle Appliance, die auf demselben Host oder Cluster mit den gesicherten virtuellen Maschinen ausgeführt wird, hat direkten Zugriff auf den/die Datenspeicher, wo sich die Maschinen befinden. Das bedeutet, dass die Appliance die gesicherten Laufwerke per HotAdd-Transport anschließen kann und der Backup-Verkehr daher von einem lokalen Laufwerk zu einem anderen weitergeleitet wird. Wenn der Datenspeicher als **Festplatte/LUN** (statt per **NFS**) verbunden ist, wird das Backup komplett 'LAN-frei' sein. Bei einem NFS-Datenspeicher kommt es dagegen zum Netzwerkverkehr zwischen dem Datenspeicher und dem Host.

Die Verwendung eines lokal angeschlossenen Storages setzt voraus, dass der Agent immer dieselben Maschinen sichert. Sie müssen, falls mehrere Agenten innerhalb der vSphere arbeiten – und einer oder mehrere davon lokal angeschlossene Storages verwenden – jeden Agenten manuell an alle Maschinen binden, die er sichern soll. Falls die Maschinen stattdessen vom Management Server zwischen den Agenten verteilt werden, können die Backups einer Maschine über mehrere Storages zerstreut werden.

Sie können den Storage zu einem bereits arbeitenden Agenten hinzufügen oder wenn Sie den Agenten über eine OVF-Vorlage bereitstellen.

***So können Sie einen Storage an einen bereits arbeitenden Agenten anschließen***

1. Klicken Sie in der VMware vSphere-Bestandsliste (Inventory) mit der rechten Maustaste auf den Agenten für VMware (Virtuelle Appliance).
2. Fügen Sie das Laufwerk hinzu, indem Sie die Einstellungen der virtuellen Maschine bearbeiten. Die Laufwerksgröße muss mindestens 10 GB betragen.

   **Warnung!**
   Seien Sie vorsichtig, wenn Sie ein bereits existierendes Laufwerk hinzufügen. Sobald der Storage erstellt wird, gehen alle zuvor auf dem Laufwerk enthaltenen Daten verloren.

3. Gehen Sie zur Konsole der virtuellen Appliance. Der Link **Storage erstellen** ist im unteren Bereich der Anzeige verfügbar. Wenn nicht, klicken Sie auf **Aktualisieren**.
4. Klicken Sie auf den Link **Storage erstellen**, wählen Sie das Laufwerk und spezifizieren Sie eine Bezeichnung für dieses. Die Länge der Bezeichnung ist aufgrund von Dateisystembeschränkungen auf 16 Zeichen limitiert.

***So können Sie einen lokal angeschlossen Storage als Backup-Ziel auswählen***

Wählen Sie beim Erstellen eines Schutzplans unter **Backup-Ziel** die Option **Lokale Ordner** – Sie dann den mit dem lokal angeschlossenen Storage korrespondierenden Laufwerksbuchstaben an, beispielsweise **D:**.

# Virtuelle Maschinen anbinden

Dieser Abschnitt gibt Ihnen einen Überblick darüber, wie der Management Server die Aktionen mehrerer Agenten innerhalb des VMware vCenters organisiert.

Der untere Verteilungsalgorithmus gilt für die virtuellen Appliances und die unter Windows installierten Agenten.

## Verteilungsalgorithmus

Die virtuellen Maschinen werden automatisch gleichmäßig zwischen den Agenten für VMware verteilt. Mit 'gleichmäßig' ist gemeint, dass jeder Agent eine gleiche Anzahl von Maschinen verwaltet. Die Menge an Speicherplatz, die eine virtuelle Maschine belegt, wird nicht gezählt.

Wenn Sie jedoch einen Agenten für eine Maschine auswählen, versucht die Software die Gesamt-Performance des Systems zu optimieren. Das bedeutet, dass die Software den Speicherort des Agenten und der virtuellen Maschine berücksichtigt. Ein Agent, der auf demselben Host vorliegt, wird bevorzugt. Falls es keinen Agenten auf demselben Host gibt, wird ein Agent aus demselben Cluster bevorzugt.

Sobald eine virtuelle Maschine einem Agenten zugewiesen wurde, werden alle Backups dieser Maschine an diesen Agenten delegiert.

## Neuverteilung

Wenn eine aufgebaute Verteilung nicht (mehr) funktioniert, weil es bei der Auslastung zwischen den Agenten zu einem Ungleichgewicht von über 20% gekommen ist, erfolgt eine automatische Neuverteilung. Dazu kann es kommen, wenn eine Maschine oder ein Agent hinzugefügt oder entfernt wird – oder eine Maschine zu einem anderen Host bzw. Cluster migriert – oder wenn Sie eine Maschine manuell an einen Agenten anbinden. Wenn das passiert, teilt der Management Server 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 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. Diese passiert jedoch nicht, wenn ein Agent beschädigt wird oder manuell aus vSphere gelöscht wird. Eine Neuverteilung wird in diesem Fall nur dann gestartet, wenn Sie einen solchen Agenten über die Weboberfläche entfernen.

## Die Verteilungsergebnisse einsehen

Sie können das Ergebnis der automatischen Verteilung einsehen:

- für jede virtuelle Maschine in der Spalte **Agent** im Bereich **Alle Geräte**
- im Abschnitt **Zugewiesene virtuelle Maschinen** des Fensterbereichs **Details**, wenn ein Agent im Bereich **Einstellungen** –> **Agenten** ausgewählt wurde

## Manuelle Anbindung

Durch die Option 'Anbindung des Agenten für VMware' können Sie eine virtuelle Maschine von diesem Verteilungsprozess ausschließen, indem Sie einen Agenten spezifizieren, der die Backups dieser Maschine immer durchführen muss. Die Gesamtbalance bleibt erhalten, aber diese spezielle Maschine kann nur dann zu einem anderen Agenten weitergereicht werden, wenn der der ursprüngliche Agent entfernt wurde.

***So können Sie eine Maschine an einen Agenten binden***

1. Wählen Sie die Maschine aus.
2. Klicken Sie auf **Details**.
   Die Software zeigt im Bereich **Zugewiesener Agent** den Agenten an, der die ausgewählte Maschine derzeit verwaltet.
3. Klicken Sie auf **Ändern**.
4. Wählen Sie **Manuell**.
5. Bestimmen Sie den Agenten, den Sie an die Maschine anbinden wollen.
6. Klicken Sie auf **Speichern**.

***So können Sie eine Maschine von einem Agenten trennen***

1. Wählen Sie die Maschine aus.
2. Klicken Sie auf **Details**.
   Die Software zeigt im Bereich **Zugewiesener Agent** den Agenten an, der die ausgewählte Maschine derzeit verwaltet.
3. Klicken Sie auf **Ändern**.
4. Wählen Sie **Automatisch**.
5. Klicken Sie auf **Speichern**.

## Die automatische Zuweisung für einen Agenten deaktivieren

Sie können die automatische Zuweisung für einen Agenten für VMware deaktivieren und ihn so vom Verteilungsprozess ausschließen, indem Sie eine Liste der Maschinen spezifizieren, die dieser Agent sichern muss. Die Gesamtbalance zwischen den anderen Agenten bleibt erhalten.

Die Automatische Zuweisung für einen Agenten kann nicht deaktiviert werden, wenn es keine anderen/weiteren registrierten Agenten gibt oder wenn die automatische Zuweisung für alle anderen Agenten deaktiviert ist.

***So können Sie die automatische Zuweisung für einen Agenten deaktivieren***

1. Klicken Sie auf **Einstellungen** –> **Agenten**.
2. Wählen Sie den Agenten für VMware aus, für den Sie die automatische Zuweisung deaktivieren wollen.
3. Klicken Sie auf **Details**.
4. Deaktivieren Sie den Schalter für **Automatische Zuweisung**.

### Anwendungsbeispiele

- Die manuelle Anbindung kann nützlich sein, falls Sie eine bestimmte (sehr große) Maschine durch den Agenten für VMware (Windows) über eine 'Fibre Channel'-Verbindung sichern wollen, während das Backup anderer Maschinen durch virtuelle Appliances erfolgt.
- Eine manuelle Anbindung ist auch notwendig, wenn Sie SAN-Hardware-Snapshots verwenden. Verbinden Sie den Agenten für VMware (Windows), für den SAN-Hardware-Snapshots konfiguriert sind, mit den Maschinen, die auf dem SAN-Datenspeicher liegen.
- 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.

## 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.

## Virtualisierungsumgebungen verwalten

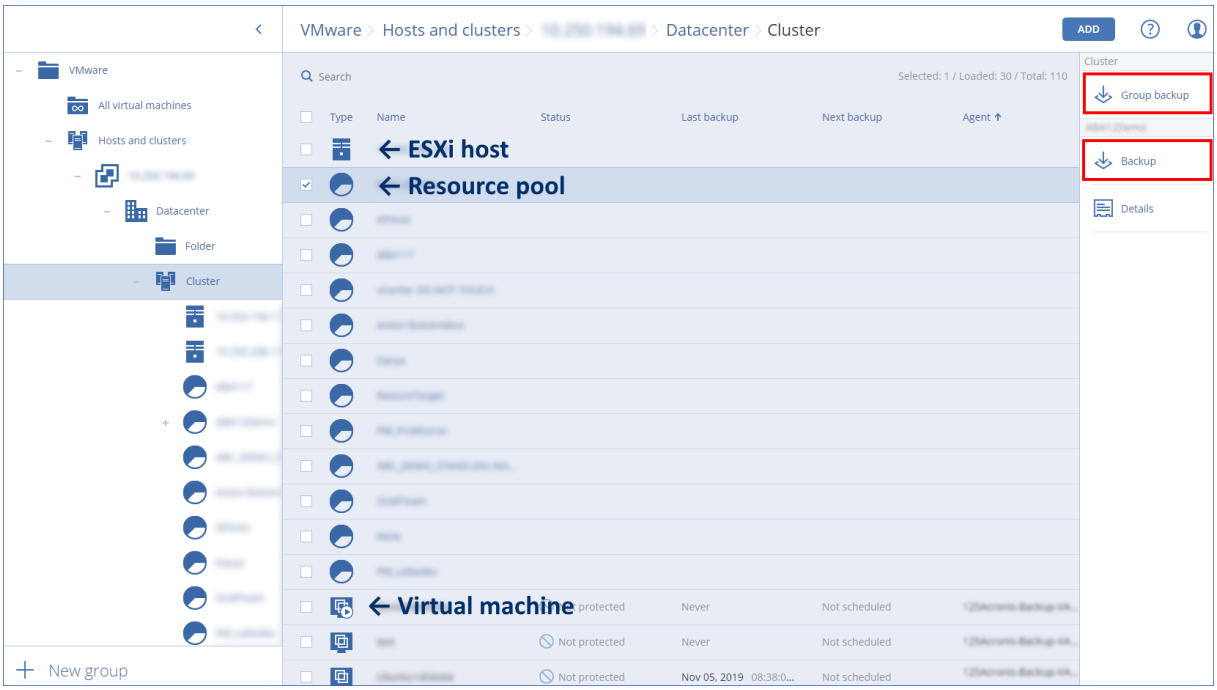
Sie können vSphere-, Hyper-V- und Virtuozzo-Umgebungen in ihrer nativen Darstellung anzeigen lassen. Sobald der entsprechende Agent installiert und registriert ist, werden die Registerkarten **VMware**, **Hyper-V** oder **Virtuozzo** unter **Geräte** angezeigt.

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 **Backup** klicken – oder die übergeordnete Maschinengruppe, zu der die ausgewählte Gruppe gehört, indem Sie auf **Gruppen-Backup** klicken.

Beispiel: Sie haben den Cluster ausgewählt und in diesem dann einen Ressourcenpool. Wenn Sie auf **Backup** klicken, werden alle virtuellen Maschinen per Backup gesichert, die zu dem ausgewählten Ressourcenpool gehören. Wenn Sie auf **Gruppen-Backup** klicken, werden alle virtuellen Maschinen per Backup gesichert, die sich im Cluster befinden.




Sie können die Zugriffsanmeldedaten für einen vCenter Server oder eigenständigen ESXi-Host ändern, ohne den Agenten neu installieren zu müssen.

***So ändern Sie die Zugriffsanmeldedaten für einen vCenter Server oder eigenständigen ESXi-Host***

1. Klicken Sie bei **Geräte** auf **VMware**.
2. Klicken Sie auf **Hosts und Cluster**.
3. Wählen Sie in der '**Hosts und Cluster**'-Liste (rechts neben dem '**Hosts und Cluster**'-Verzeichnisbaum) denjenigen vCenter Server oder eigenständigen ESXi-Host aus, der bei der Installation des Agenten für VMware spezifiziert wurde.
4. Klicken Sie auf **Details**.
5. Klicken Sie unter **Anmeldedaten** auf den Benutzernamen.
6. Spezifizieren Sie die neuen Anmeldedaten und klicken Sie abschließend auf **OK**.

## Den Backup-Status im vSphere Client einsehen

Sie können den Backup-Status und den letzte Backup-Zeitpunkt einer virtuellen Maschine im vSphere Client einsehen.

Diese Informationen erscheinen in der Übersicht der virtuellen Maschine (**Übersicht** –> **Benutzerdefinierte Attribute/Anmerkungen/Hinweise**, in Abhängigkeit vom Client-Typ und der vSphere-Version). Sie können außerdem die Spalten **Letztes Backup** und **Backup-Status** auf der Registerkarte **Virtuelle Maschinen** für jedes Datacenter, jeden Host, Ordner, Ressourcenpool oder gesamten vCenter Server aktivieren.

Um diese Attribute bereitzustellen, muss der Agent für VMware neben den in Abschnitt 'Agent für VMware – notwendige Berechtigungen' beschriebenen Berechtigungen noch über folgende Berechtigungen verfügen:

- **Global** –> **Benutzerdefinierte Attribute verwalten**
- **Global** –> **Benutzerdefinierte Attribute festlegen**

## Agent für VMware – notwendige Berechtigungen

Dieser Abschnitt beschreibt die Berechtigungen, die für Aktionen mit virtuellen ESXi-Maschinen sowie für die Bereitstellung der virtuellen Appliance erforderlich sind.

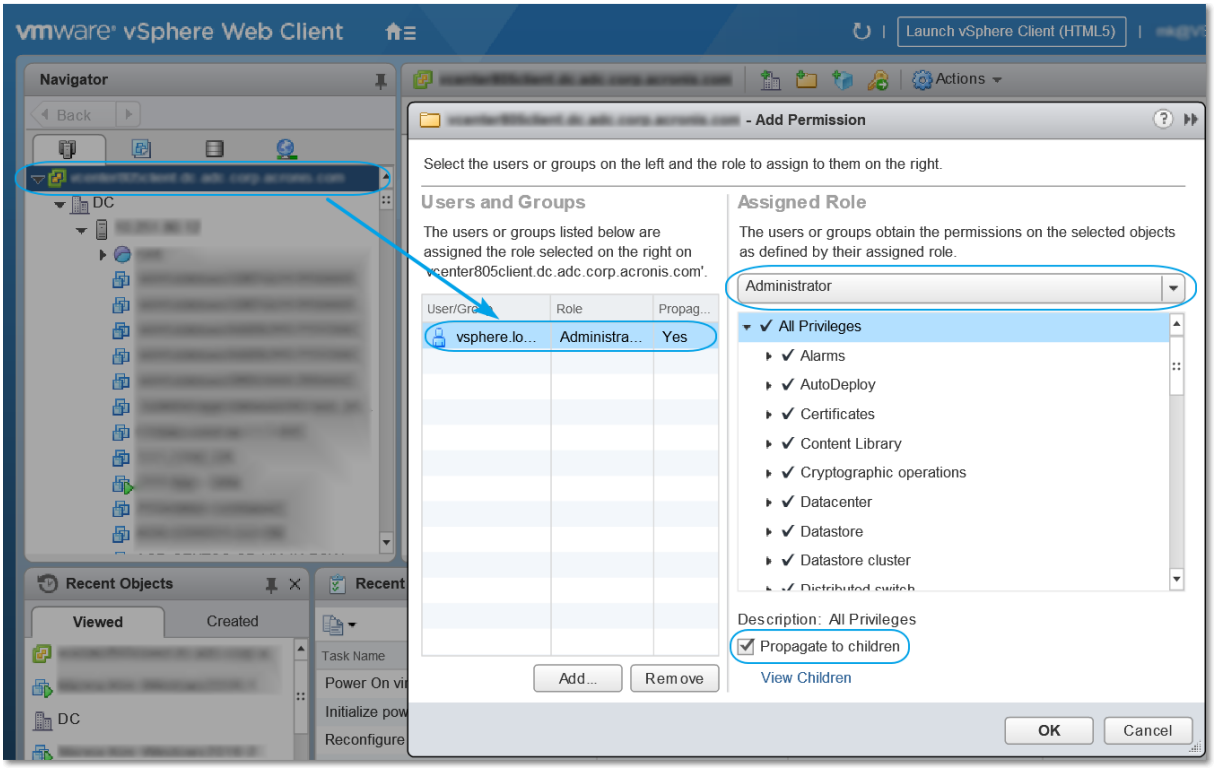
**Hinweis**
vStorage APIs muss auf dem ESXi-Host installiert sein, um Backups von virtuellen Maschinen aktivieren zu können. Siehe: https://kb.acronis.com/de/content/14931.

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'.

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**.




| Objekt | Recht | Aktion | | | | |
|---|---|---|---|---|---|---|
| | | Backup einer VM | Recovery zu einer neuen VM | Recovery zu einer existierenden VM | VM von Backup ausführen | VA-Deployment |
| **Kryptografische Operationen** (ab vSphere 6.5) | **Laufwerk hinzufügen** | +* | | | | |
| | **Direktzugriff** | +* | | | | |
| **Datenspeicher** | **Speicher zuweisen** | | + | + | + | + |
| | **Datenspeicher durchsuchen** | | | | + | + |
| | **Datenspeicher konfigurieren** | + | + | + | + | + |
| | **Dateivorgänge auf niedriger Ebene** | | | | + | + |
| **Global** | **Lizenzen** | + | + | + | + | |
| | **Methoden deaktivieren** | + | + | + | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | **Methoden aktivieren** | + | + | + | | |
| | **Benutzerdefinierte Attribute verwalten** | + | + | + | | |
| | **Benutzerdefinierte Attribute festlegen** | + | + | + | | |
| **Host –> Konfiguration** | **Autostart-Konfiguration für virtuelle Maschine** | | | | | + |
| | **Konfiguration für Speicherpartition** | | | | + | |
| **Host > Bestandsliste** | **Cluster ändern** | | | | | + |
| **Host > Lokale Operationen** | **VM erstellen** | | | | + | + |
| | **VM löschen** | | | | + | + |
| | **Virtuelle Maschine rekonfigurieren** | | | | + | + |
| **Netzwerk** | **Netzwerk zuweisen** | | + | + | + | + |
| **Ressource** | **Virtuelle Maschine zu Ressourcenpool zuweisen** | | + | + | + | + |
| | **Importieren** | | | | | + |
| **Virtuelle Maschine –> Konfiguration** | **Vorhandenes Laufwerk hinzufügen** | + | + | | + | |
| | **Neues Laufwerk hinzufügen** | | + | + | + | + |
| | **Gerät hinzufügen oder entfernen** | | + | | + | + |
| | **Advanced** | + | + | + | | + |
| | **CPU-Anzahl ändern** | | + | | | |
| | **Festplattenänderungsverfolgung** | + | | + | | |
| | **Festplatten-Lease** | + | | + | | |
| | **Arbeitsspeicher** | | + | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | **Laufwerk entfernen** | + | + | + | + | |
| | **Umbenennen** | | + | | | |
| | **Anmerkung festlegen** | | | | + | |
| | **Einstellungen** | | + | + | + | |
| **Virtuelle Maschine** –> **Gastbetriebssystem** | **Programmausführung im Gastbetriebssystem** | +** | | | | + |
| | **Gastvorgangsabfragen** | +** | | | | + |
| | **Änderungen des Gastbetriebssystems** | +** | | | | |
| **Virtuelle Maschine** –> **Interaktion** | **Ticket zur Steuerung durch Gast abrufen** (in vSphere 4.1 und 5.0) | | | | + | + |
| | **CD-Medien konfigurieren** | | + | + | | |
| | **Konsoleninteraktion** | | | | | + |
| | **Gastbetriebssystem-Verwaltung über VIX API** (in vSphere 5.1 und höher) | | | | + | + |
| | **Ausschalten** | | | + | + | + |
| | **Einschalten** | | + | + | + | + |
| **Virtuelle Maschine** –> **Bestandsliste** | **Aus vorhandener erstellen** | | + | + | + | |
| | **Neu erstellen** | | + | + | + | + |
| | **Verschieben** | | | | | + |
| | **Registrieren** | | | | + | |
| | **Entfernen** | | + | + | + | + |
| | **Registrierung aufheben** | | | | + | |
| **Virtuelle Maschine** –> **Provisioning** | **Laufwerkszugriff erlauben** | | + | + | + | |
| | **Lesezugriff auf Laufwerk erlauben** | + | | + | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | **Download virtueller Maschine zulassen** | + | + | + | + | |
| **Virtuelle Maschine** –> **Status**<br>**Virtuelle Maschine** –> **Snapshot-Verwaltung**<br>(vSphere 6.5 und höher) | **Snapshot erstellen** | + | | + | + | + |
| | **Snapshot entfernen** | + | | + | + | + |
| **vApp** | **Virtuelle Maschine hinzufügen** | | | | + | |

* Diese Berechtigung ist nur zum Backup von verschlüsselten Maschinen erforderlich.

** Diese Berechtigung ist nur für applikationskonforme Backups erforderlich.

# Backup von geclusterten Hyper-V-Maschinen

In einem Hyper-V-Cluster können virtuelle Maschinen zwischen den Cluster-Knoten migrieren. Folgen Sie diesen Anweisungen, um ein korrektes Backup von geclusterten Hyper-V-Maschinen einzurichten:

1. Eine Maschine muss für Backups verfügbar sein, egal zu welchem Knoten sie migriert wird. Um zu gewährleisten, dass der Agent für Hyper-V auf jedem Knoten auf eine Maschine zugreifen kann, muss der Agenten-Dienst (Agent Service) unter einem Domain-Benutzerkonto ausgeführt werden, welches auf jedem der Cluster-Knoten über administrative Berechtigungen verfügt.
   Wir empfehlen, dass Sie ein solches Konto für den Agenten-Dienst während der Installation des Agenten für Hyper-V spezifizieren.
2. Installieren Sie den Agenten für Hyper-V auf jedem Knoten des Clusters.
3. Registrieren Sie alle Agenten auf dem Management Server.

## 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 auf einer *neuen* virtuellen Hyper-V-Maschine wiederherstellen oder eine Konvertierung zu einer virtuellen Hyper-V-Maschine innerhalb eines Schutzplans durchführen, ist die resultierende Maschine nicht hochverfügbar. Sie wird als Reserve-Maschine (Spare Machine) betrachtet und ist normalerweise ausgeschaltet. Falls Sie die Maschine in einer

Produktionsumgebung einsetzen müssen, können Sie deren Hochverfügbarkeit über das **Failovercluster-Verwaltungs-**-Snap-in konfigurieren.

# Die Gesamtzahl der gleichzeitig gesicherten virtuellen Maschinen begrenzen

Die Backup-Option **Planung** 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 ein Agent für VMware (Virtuelle Appliance) oder Agent für VMware (Linux) gleichzeitig sichern kann***

1. Starten Sie auf der Maschine, die den Agenten ausführt, die Befehlseingaben-Oberfläche (Konsole):
   - **Agent für VMware (Virtuelle Appliance):** Drücken Sie die Tastenkombination Strg+Umschalt+F2, während Sie sich in der Benutzeroberfläche der virtuellen Appliance befinden.
   - **Agent für VMware (Linux):** Melden Sie sich auf der Maschine, die die Acronis Cyber Protect Appliance ausführt, als Benutzer 'root' an. Das Kennwort ist dasselbe wie für die Cyber Protect Webkonsole.
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. Starten Sie den Agenten neu:
   - **Agent für VMware (Virtuelle Appliance):** Führen Sie den Befehl `reboot` aus.
   - **Agent für VMware (Linux):** Führen Sie folgende Befehl aus:

     ```
     sudo service acronis_mms restart
     ```

# 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* | Virtuelle Virtuozzo Hybrid Infrastructure-Maschine* | Virtuelle Scale Computing HC3-Maschine | Virtuelle RHV/oVirt-Maschine* |
| Physische Maschine | + | + | + | - | - | + | + | + |
| Virtuelle | + | + | + | - | - | + | + | + |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| VMware ESXi-Maschine | | | | | | | | |
| Virtuelle Hyper-V-Maschine | + | + | + | - | - | + | + | + |
| Virtuelle Virtuozzo-Maschine* | + | + | + | + | - | + | + | + |
| Virtuozzo-Container* | - | - | - | - | + | - | - | - |
| Virtuelle Virtuozzo Hybrid Infrastructure-Maschine* | + | + | + | - | - | + | + | + |
| Virtuelle Scale Computing HC3-Maschine | + | + | + | - | - | + | + | + |
| Virtuelle Red Hat Virtualization/oVirt-Maschine* | + | + | + | - | - | + | + | + |

* Nur bei der Cloud-Bereitstellung verfügbar

Anleitungen zur Durchführung von Migrationen finden Sie in folgenden Abschnitten:

- Physisch-zu-virtuell (P2V) – "Eine physische Maschine zu einer virtuellen Maschine wiederherstellen" (S. 333)
- Virtuell-zu-virtuell (V2V) – "Eine virtuelle Maschine wiederherstellen" (S. 335)
- Virtuell-zu-physisch (V2P) – "Eine virtuelle Maschine wiederherstellen" (S. 335) oder "Laufwerke und Volumes mithilfe eines Boot-Mediums wiederherstellen" (S. 339)

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- und V2P-Migrationen 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.

# 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 sie jedoch als virtuelle Maschine gezählt, wenn Sie in einer Cloud-Bereitstellung 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' wieder her. Wählen Sie die neue Maschine als Zielmaschine aus, wenn Sie die Wiederherstellung konfigurieren.

## Netzwerk-Anforderungen

Die auf den zu sichernden Maschinen installierten Agenten müssen in der Lage sein, mit dem Management Server über das Netzwerk zu kommunizieren.

### On-Premise-Bereitstellung

- Wenn sowohl die Agenten als auch der Management Server in der Azure/EC2-Cloud installiert sind, befinden sich alle Maschinen bereits im selben Netzwerk. Es sind keine weiteren Aktionen erforderlich.
- Wenn sich der Management Server außerhalb der Azure/EC2-Cloud befindet, haben die Maschinen in der Cloud keinen (direkten) Zugriff auf das lokale Netzwerk, in dem der Management Server installiert ist. Damit die Agenten, die auf solchen Maschinen installiert sind, mit dem Management Server kommunizieren können, muss eine VPN-Verbindung (Virtual Private Network) zwischen dem lokalen (on-premise) Netzwerk und dem Cloud-Netzwerk (Azure/EC2)

hergestellt werden. Anweisungen zur Erstellung dieser VPN-Verbindung finden Sie in den folgenden Artikeln:

Amazon EC2: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html#vpn-create-cgw

Windows Azure: https://docs.microsoft.com/de-de/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal

## Cloud-Bereitstellung

Bei einer Cloud-Bereitstellung befindet sich der Management Server in einem der Acronis Datacenter und ist daher für die Agenten erreichbar. Es sind keine weiteren Aktionen erforderlich.

# 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/AcronisCyberProtect_15_SAP_HANA_whitepaper_en-US.pdf

# Antimalware Protection und Web Protection

Die Antimalware Protection in Cyber Protect 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.

## 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.

Acronis Cyber Protect wird vom Windows-Sicherheitscenter unterstützt und in diesem registriert.

Wenn das Antivirus & Antimalware Protection-Modul auf eine Maschine angewendet wird und diese Maschine zu diesem Zeitpunkt bereits durch die Antivirus-Lösung eines Drittanbieters geschützt wird, wird das System eine Alarmmeldung generieren und den Echtzeitschutz stoppen, um mögliche Kompatibilitäts- und Performance-Probleme zu verhindern. Sie müssen dann die Antivirus-Lösung des Drittanbieters entweder deaktivieren oder deinstallieren, damit die Acronis Cyber Protect Antivirus & Antimalware Protection vollumfänglich funktionieren kann.

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 schädliche URLs (für Windows)
- Verschieben von gefährlichen Dateien in eine Quarantäne
- Verwalten einer Whitelist mit vertrauenswürdigen Unternehmensapplikationen

Das Antivirus & Antimalware Protection-Modul bietet Ihnen zwei verschiedene Scanning-Methoden:

- Echtzeitschutz-Scan
- On-Demand-Malware-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.

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-Malware-Scan

Das Antimalware-Scanning wird auf Basis eines Zeitplans durchgeführt.

Sie können die Ergebnisse des Antimalware-Scannings im Widget **Dashboard** –> **Überblick** –> Kürzlich betroffen überwachen.

## Antivirus & Antimalware Protection-Einstellungen

Eine Anleitung zum Erstellen eines Schutzplans mit aktiviertem Antivirus & Antimalware Protection-Modul finden Sie im Abschnitt 'Einen Schutzplan erstellen'.

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.

In den Cyber Backup-Editionen von Acronis Cyber Protect ist die Active Protection-Funktionalität ein separates Modul innerhalb eines Schutzplans. So kann sie separat konfiguriert und auf verschiedene Geräte oder Geräte-Gruppen angewendet werden. Bei den Protect-Editionen von Acronis Cyber Protect ist die Active Protection-Funktionalität ein Bestandteil des Antivirus & Antimalware Protection-Moduls.

Active Protection ist für Maschinen mit folgenden Betriebssystemen verfügbar:

- Desktop-Betriebssysteme: Windows 7 Service Pack 1 und höher
  Stellen Sie bei Maschinen, die unter Windows 7 laufen, sicher, dass dieses Update für Windows 7 (KB2533623) installiert ist.
- Server-Betriebssysteme: Windows Server 2008 R2 und höher.

Auf der zu schützenden Maschine muss der Agent für Windows laufen.

### 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**.

## Netzwerkordnerschutz

Die Option **Als lokale Laufwerke zugeordnete Netzwerkordner schützen** bestimmt, ob die Antivirus & Antimalware Protection auch Netzwerkordner, die als lokale Laufwerke gemounted wurden, vor lokalen Schadprozessen schützen soll.

Diese Option gilt für Ordner, die per SMB- oder NFS-Protokoll freigegeben/zugeordnet wurden.

Wenn sich eine Datei ursprünglich auf einem solchen Netzlaufwerk befand, kann diese nicht an ihrem ursprünglichen Speicherort wiederhergestellt werden, wenn die Datei aufgrund des Befehls **Aus Cache wiederherstellen** aus dem Cache extrahiert wird. Stattdessen wird die Datei aus dem

Cache in demjenigen Ordner wiederhergestellt, der in 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, müssen Sie 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 müssen den Benutzernamen und die IP-Adressen spezifizieren.

Auf der Registerkarte **Blockiert** können Sie Verbindungen spezifizieren, die keine Daten modifizieren dürfen. Sie müssen den Benutzernamen und die IP-Adressen spezifizieren.

## Selbstschutz

Der **Selbstschutz** (Self-Protection) verhindert, dass die Prozesse, Registry-Einträge, ausführbaren Dateien, Konfigurationsdateien und die Einer Secure Zone der Backup-Software sowie die 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**.

## 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 die 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**.

## Quarantäne

Die Quarantäne 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**.

## Verhaltenserkennung

Acronis Cyber Protect schützt Ihr System vor Malware, indem es mithilfe einer verhaltensbasierten Heuristik bösartige Prozesse identifiziert: Die Funktion vergleicht 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.

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**.

## Echtzeitschutz

Der **Echtzeitschutz** (Realtime Protection, RTP) überprüft das System Ihrer Maschine kontinuierlich auf Viren und andere Bedrohungen. Dies erfolgt während der gesamten Betriebszeit Ihres Systems.

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 Ihre Maschine nach Malware überprüft wird, wenn Sie die Einstellung **Scan planen** aktivieren.

**Aktion bei Erkennung:**

- **Quarantäne**
  Die Software generiert einen Alarm und verschiebt die entsprechende ausführbare Datei in den Quarantäne-Ordner
- **Nur benachrichtigen**
  Die Software generiert einen Alarm über den Prozess, bei dem der Verdacht auf Malware-Aktivität besteht, dass es sich um eine Malware handelt.

Standardeinstellung: **Quarantäne**.

**Scan-Typ**:

- **Vollständig**
  Der vollständige Scan 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.
- **Benutzerdefiniert**
  Der benutzerdefinierte Scan überprüft die Dateien/Ordner, die vom Administrator für den Schutzplan ausgewählt wurden.

Sie können alle drei Scan-Typen – **Schnell**, **Vollständig** und **Benutzerdefiniert** – in einem Schutzplan planen.

Standardeinstellungen:

- Es ist ein Scan vom Typ **Schnell** und **Vollständig** geplant.
- die Scan-Option **Benutzerdefiniert** ist standardmäßig deaktiviert.

**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 (beliebigen) Benutzers ausgelöst. Sie können diese Einstellung so ändern, dass nur ein bestimmtes Benutzerkonto den Task auslösen kann.
- **Wenn sich ein Benutzer vom System abmeldet** – Die Task-Ausführung wird standardmäßig durch die Abmeldung eines (beliebigen) Benutzers ausgelöst. Sie können diese Einstellung so ändern, dass nur ein bestimmtes Benutzerkonto den Task auslösen kann.

**Hinweis**
Der Task wird daher nicht beim Herunterfahren des Systems ausgeführt. Herunterfahren und Abmelden sind unterschiedliche Ereignisse in der Planungskonfiguration.

- **Beim Systemstart** – Der Task wird ausgeführt, wenn das Betriebssystem startet.
- **Beim Herunterfahren des Systems** – Der Task wird ausgeführt, wenn das Betriebssystem herunterfährt.

Standardeinstellung: **Planung nach Zeit**.

**Planungstyp**:

- **Monatlich** – Wählen Sie die Monate und dann die jeweiligen Wochen oder Tage des Monats, in denen der Task ausgeführt werden soll.
- **Täglich** – Wählen Sie die Wochentage aus, an denen der Task ausgeführt werden soll.
- **Stündlich** – Wählen Sie die Wochentage, die Anzahl der Wiederholungen sowie das Zeitintervall aus, in dem der Task ausgeführt werden soll.

Standardeinstellung: **Täglich**.

**Starten um** – Bestimmen Sie den genauen Zeitpunkt, an dem der Task ausgeführt werden soll.

**Innerhalb eines Zeitraums ausführen** – Bestimmten Sie einen Datumsbereich, innerhalb dessen die konfigurierte Planung gültig sein soll.

**Startbedingungen** – Definieren Sie alle Bedingungen, die gleichzeitig zutreffen müssen, damit der Task ausgeführt werden kann.

Die Startbedingungen für Antimalware-Scans sind ähnlich wie die Startbedingungen für das Backup-Modul, die wiederum im Abschnitt '"Startbedingungen" (S. 254)' beschrieben sind. Sie können folgende zusätzliche Startbedingungen definieren:

- **Task-Startzeit innerhalb eines Zeitfensters verteilen**– Diese Option ermöglicht es Ihnen, einen Zeitrahmen für den Task festzulegen, um Netzwerkengpässe zu vermeiden. Sie können die Verzögerung in Stunden oder Minuten spezifizieren. Wenn beispielsweise die Standardstartzeit 10:00 Uhr morgens ist und die Verzögerung 60 Minuten beträgt, dann beginnt der Task zwischen 10:00 und 11:00 Uhr morgens.
- **Task bei Neustart der Maschine ausführen, wenn die Maschine zur geplanten Zeit ausgeschaltet war**

- **Standby- oder Ruhezustandsmodus während der Task-Ausführung verhindern** – Diese Option gilt nur für Maschinen, die unter Windows laufen.
- **Wenn die Startbedingungen nicht erfüllt sind, Task trotzdem ausführen nach:** – Spezifizieren Sie einen Zeitraum, nach dem der Task unabhängig von anderen Startbedingungen auf jeden Fall gestartet werden soll.

**Nur neue und geänderte Dateien scannen** – Es werden nur neu erstellte und/oder geänderte Dateien überprüft.

Standardeinstellung: **Aktiviert**.

Wenn Sie einen **vollständigen Scan** planen, haben Sie zwei zusätzliche Optionen:

- **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**

## Ausschlüsse

Um die Ressourcen zu minimieren, die durch die heuristische Analyse belegt werden, und sogenannte Falsch-Positiv-Erkennungen zu vermeiden, können Sie folgende Einstellungen festlegen, wenn ein vertauenswürdiges Programm als Ransomware eingestuft wird:

Auf der Registerkarte **Vertrauenswürdig** können Sie Folgendes spezifizieren:

- Prozesse, die niemals als Malware eingestuft werden. Prozesse, die von Microsoft signiert wurden, werden immer als vertrauenswürdig eingestuft.
- Ordner, in denen keine Dateiänderungen überwacht werden.
- Dateien und Ordner, in denen kein geplanter Scan durchgeführt wird.

Auf der Registerkarte **Blockiert** können Sie Folgendes spezifizieren:

- Prozesse, die immer geblockt werden. Solange Active Protection auf der Maschine aktiviert ist, können diese Prozesse nicht gestartet werden.

- Ordner, in denen jeder Prozess blockiert wird.

Spezifizieren Sie den vollständigen Pfad zur ausführbaren Datei des Prozesses (mit dem Laufwerksbuchstaben beginnend). Beispiel: `C:\Windows\Temp\er76s7sdkh.exe`.

Sie können die Platzhalterzeichen (* und ?) verwenden, um Ordner zu spezifizieren. Der Asterisk (*) ersetzt null bis mehrere Zeichen. Das Fragezeichen (?) steht für exakt ein Zeichen. Umgebungsvariablen (wie etwa `%AppData%`) können nicht verwendet werden.

Standardeinstellung: Standardmäßig sind keine Ausnahmen definiert.

### URL-Filterung

Eine ausführlichere Beschreibung finden Sie im Abschnitt 'URL-Filterung'.

## Active Protection

In den Cyber Backup-Editionen von Acronis Cyber Protect ist die Active Protection-Funktionalität ein separates Modul innerhalb eines Schutzplans. Dieses Modul hat folgende Einstellungen:

- Aktion bei Erkennung
- Selbstschutz
- Netzwerkordnerschutz
- Serverseitiger Schutz
- Erkennung von Cryptomining-Prozessen
- Ausschlüsse

Bei den Protect-Editionen von Acronis Cyber Protect ist die Active Protection-Funktionalität ein Bestandteil des Antivirus & Antimalware Protection-Moduls.

Active Protection ist für Maschinen mit folgenden Betriebssystemen verfügbar:

- Desktop-Betriebssysteme: Windows 7 Service Pack 1 und höher
  Stellen Sie bei Maschinen, die unter Windows 7 laufen, sicher, dass dieses Update für Windows 7 (KB2533623) installiert ist.
- Server-Betriebssysteme: Windows Server 2008 R2 und höher.

Auf der zu schützenden Maschine muss der Agent für Windows laufen.

Weitere Informationen über Active Protection und dessen Einstellungen finden Sie im Abschnitt '"Antivirus & Antimalware Protection-Einstellungen" (S. 543)'.

## 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-Modul ermöglicht Ihnen, eine Windows Defender Antivirus-Sicherheitsrichtlinie zu konfigurieren und deren Status über die Cyber Protect Webkonsole 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 Elementen, die bei einem Schnellscan gescannt werden). 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 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 Windows Defender Antivirus-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 Standardeinstellungen für Windows Defender Antivirus-Aktionen finden Sie unter der Adresse https://docs.microsoft.com/de-de/sccm/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 Einstellungen für den Windows Defender Antivirus-Echtzeitschutz finden Sie unter der Adresse https://docs.microsoft.com/de-de/sccm/protect/deploy-use/endpoint-antimalware-policies#real-time-protection-settings.

## Erweitert

Spezifizieren Sie die erweiterten Scan-Einstellungen:

- **Archivdateien scannen** – auch Archivdateien (wie .zip- oder .rar-Dateien) werden in den Scan-Vorgang mit einbezogen.
- **Wechsellaufwerke scannen** – auch entfernbare Laufwerke werden bei einem vollständigen Scan überprüft
- **Systemwiederherstellungspunkt erstellen** – es kann gelegentlich vorkommen, dass eine wichtige Datei oder ein Registry-Eintrag als 'falsch positiv' erkannt und dann entfernt wird. Mit einem Wiederherstellungspunkt können Sie Ihr System auf den entsprechenden Zustand davor zurücksetzen.
- **Dateien aus der Quarantäne entfernen nach:** – definiert einen Zeitraum, nach dessen Ablauf die entsprechenden Dateien aus der Quarantäne gelöscht werden.
- **Beispiele automatisch senden, wenn eine weitere Untersuchung erforderlich ist:**

    - **Immer auffordern** – Sie werden vor dem Versenden der Datei aufgefordert, die Aktion zu bestätigen.
    - **Automatisch sichere Beispiele senden** – die meisten Beispiele werden automatisch gesendet. Ausgenommen davon sind Dateien, die persönliche Informationen enthalten könnten. Für solche Dateien ist eine zusätzliche Bestätigung erforderlich.
    - **Automatisch alle Beispiele senden** – alle Beispiele werden automatisch gesendet.
- **Windows Defender Antivirus-Benutzeroberfläche deaktivieren** – wenn diese Option ausgewählt ist, wird die Windows Defender Antivirus-Benutzeroberfläche nicht für den Benutzer verfügbar sein. Sie können die Windows Defender Antivirus-Richtlinien über die Cyber Protect Webkonsole verwalten.
- **MAPS (Microsoft Active Protection Service)** – eine Online-Community, die Ihnen bei der Entscheidung hilft, wie Sie auf potenzielle Bedrohungen reagieren sollten.
    - **Ich möchte MAPS nicht verwenden** – es werden keine Informationen über die erkannte Software an Microsoft gesendet.
    - **Basis-Mitgliedschaft** – es werden grundlegende Informationen über die erkannte Software an Microsoft gesendet.
    - **Premium-Mitgliedschaft** – es werden ausführlichere Informationen über die erkannte Software an Microsoft gesendet.

    Weitere Informationen dazu finden Sie unter der Adresse https://www.microsoft.com/security/blog/2015/01/14/maps-in-the-cloud-how-can-it-help-your-enterprise.

Weitere Informationen über die erweiterten Windows Defender Antivirus-Einstellungen finden Sie unter der Adresse https://docs.microsoft.com/de-de/sccm/protect/deploy-use/endpoint-antimalware-policies#advanced-settings.

## Ausschlüsse

Sie können folgende Dateien und Ordner definieren, die vom Scannen ausgeschlossen werden sollen:

- **Prozesse** – jede Datei, die von einem hier spezifizierten Prozess gelesen oder geschrieben wird, wird aus dem Scanvorgang ausgeschlossen. Sie müssen einen vollständigen Pfad zur ausführbaren Datei des entsprechenden Prozesses definieren.
- **Dateien und Ordner** – die hier spezifizierten Dateien und Ordner werden aus dem Scanvorgang ausgeschlossen. Sie müssen einen vollständigen Pfad zu einem Ordner/einer Datei spezifizieren – oder (eine) Datei-Erweiterung(en) definieren.

Weitere Informationen über die Windows Defender Antivirus-Ausschlusseinstellungen finden Sie unter der Adresse https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#exclusion-settings.

# Microsoft Security Essentials

Microsoft Security Essentials ist eine integrierte Antimalware-Komponente von Microsoft Windows, die mit Windows-Betriebssystemen vor Windows 8 ausgeliefert wurde.

Das Microsoft Security Essentials-Modul ermöglicht Ihnen, eine Microsoft Security Essentials-Sicherheitsrichtlinie zu konfigurieren und deren Status über die Cyber Protect Webkonsole 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 Protect Webkonsole definieren zu können.

# URL-Filterung

Malware wird häufig über bösartige oder infizierte Websites verbreitet und verwendet dafür eine Angriffsmethode, die auch Drive-by-Download-Infektion genannt wird. Mit der URL-Filterung können Sie Maschinen vor Bedrohungen wie Malware und Phishing schützen, die aus dem Internet kommen. Sie können Benutzerzugriffe auf bestimmte Websites blockieren, die bösartige/schädliche Inhalte haben können.

Sie können mit der URL-Filterung auch die Nutzung des Webs (WWWs) kontrollieren, um beispielsweise externe Vorschriften (wie gesetzliche Bestimmungen) oder interne Unternehmensrichtlinien einzuhalten. Sie können verschiedene Zugriffsrichtlinien für mehr als 40 Website-Kategorien konfigurieren.

Derzeit werden nur von Windows-Maschinen ausgehende HTTP- und HTTPS-Verbindungen vom entsprechenden Protection Agenten überprüft.

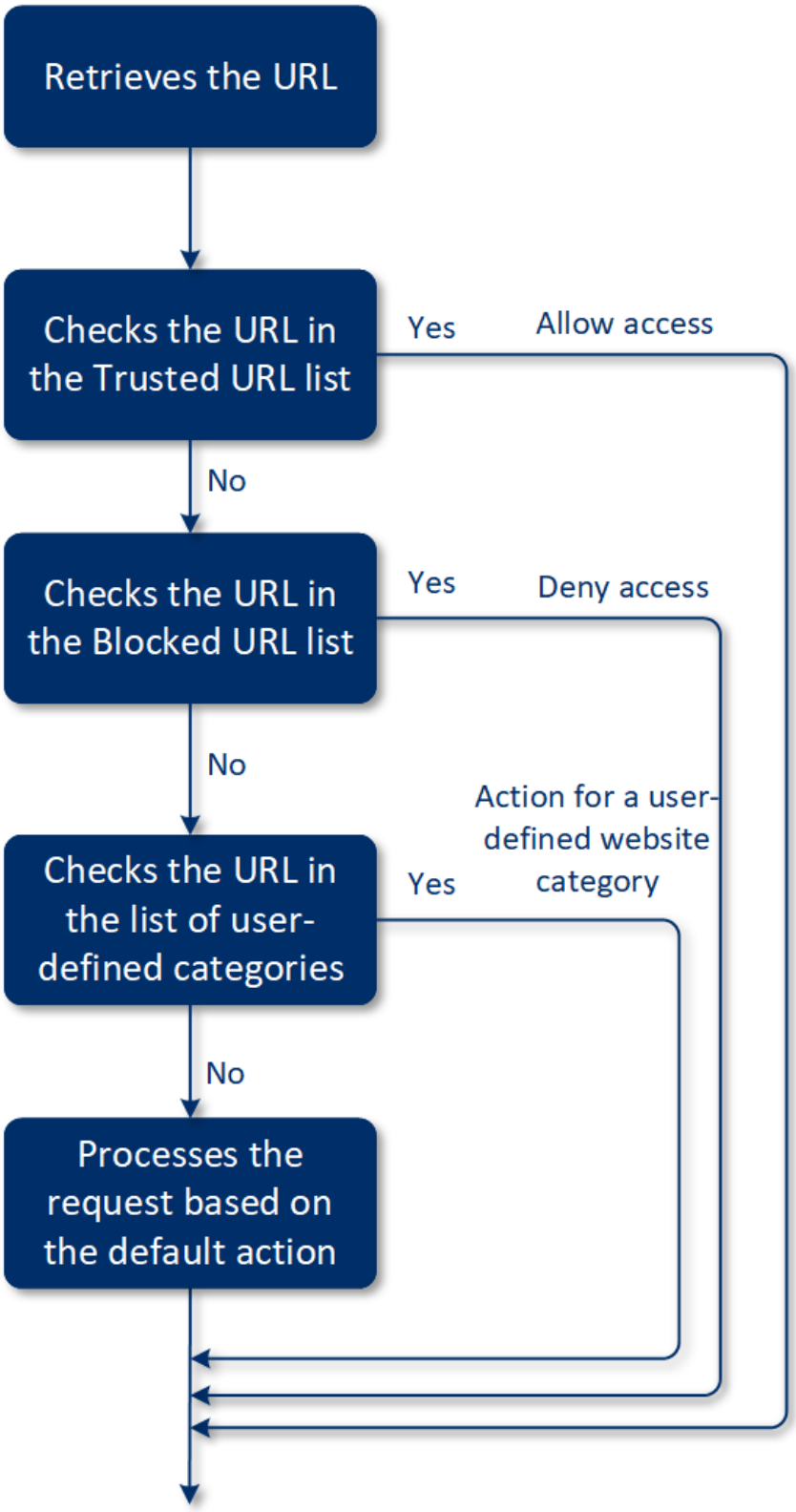
Für die URL-Filterungsfunktion ist eine Internetverbindung erforderlich.

**Hinweis**
Es kann zu Konflikten kommen, wenn die URL-Filterung parallel zu der Antivirus-Lösung eines Drittanbieters verwendet wird, die ebenfalls URL-Filterungsfunktionen verwendet. Sie können die Statuszustände von anderen installierten Antivirus-Lösungen über das Windows Sicherheitscenter ermitteln.
Wenn es zu Kompatibilitäts- oder Performance-Problemen kommt, können Sie die Drittanbieter-Lösung deinstallieren oder das URL-Filterungsmodul in Ihren Schutzplänen deaktivieren.

## Und so funktioniert es

Ein Benutzer folgt einem Link oder gibt eine URL in die Adressleiste eines Webbrowsers ein. Der sogenannte Interceptor fängt die URL ab und sendet diese an den Protection Agenten. Der

Protection Agent analysiert die URL, überprüft die Datenbank und meldet dann eine Bewertung an den Interceptor zurück. Wenn die URL verboten ist, blockiert der Interceptor den Zugriff auf diese und teilt dem Benutzer mit, dass er den entsprechenden Inhalt nicht sehen darf.




***So können Sie die URL-Filterung konfigurieren:***

1. Erstellen Sie einen Schutzplan, in dem das URL-Filterungsmodul aktiviert ist.
2. Spezifizieren Sie die URL-Filter-Einstellungen (siehe unten).
3. Weisen Sie den gewünschten 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 konfiguriert werden:

### Zugriff auf schädliche Website

Spezifizieren Sie, welche Aktionen ausgeführt werden, wenn ein Benutzer eine bösartige Website öffnen möchte:

- **Blockieren** – Der Zugriff auf die schädliche Website wird blockiert 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 die Zugriffsrichtlinie konfigurieren können: Standardmäßig ist der Zugriff auf Websites aus allen Kategorien erlaubt.

| | 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.<br><br>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.<br><br>Folgende Websites werden nicht von dieser Kategorie erfasst:<br>• Offizielle Websites von Unternehmen, die Videospiele/Videogames entwickeln (außer, sie produzieren Online-Spiele)<br>• Diskussions-Websites, auf denen Spiele/Games diskutiert werden<br>• Websites, auf denen Nicht-Online-Spiele heruntergeladen werden |

| | | |
|---|---|---|
| | | können (einige von diesen werden über die die Kategorie „Illegal" erfasst)<br>• 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:<br>• Websites von terroristischen Organisationen<br>• Websites mit rassistischen oder fremdenfeindlichen Inhalten<br>• 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:<br>• 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<br>• Warez-Websites (für raubkopierte kommerzielle Software) und entsprechende Diskussionsforen<br>• Also Websites, die Benutzern sogenannte Cracks, Schlüsselgeneratoren und Seriennummern bereitstellen, um die illegale Nutzung von Software zu ermöglichen |

| | | |
|---|---|---|
| | | Einige dieser Websites können auch über die Kategorien Pornografie oder Alkohol/Zigarren erkannt werden, da sie häufig entsprechende Werbungen verwenden, um Geld zu verdienen. |
| 20 | **Instant Messaging** | Diese Kategorie umfasst Instant Messaging- und Chat-Websites, über die Benutzer in Echtzeit chatten können. Sie erkennt auch „yahoo.com“ und „gmail.com“, weil diese Portale einen eingebetteten Instant Messenger Service enthalten. |
| 21 | **Jobs/Anstellung** | Diese Kategorie umfasst Websites, die Jobbörsen, Stellenanzeigen und Informationen zu Karrieremöglichkeiten präsentieren (das umfasst auch die Aggregatoren solcher Dienste/Angebote). Sie umfasst aber weder Personalvermittlungsagenturen noch die „Jobs“-Unterseiten von normalen Unternehmens-Websites. |
| 22 | **Anstößige Inhalte** | Diese Kategorie umfasst Inhalte, die der Website-Ersteller mit „für Erwachsene“ gekennzeichnet hat. Sie deckt ein breites Spektrum von Websites ab – vom Kama-Sutra-Buch über Websites zur Sexualerziehung bis hin zu harter Pornografie. |
| 23 | **Betäubungsmittel** | Diese Kategorie umfasst Websites, die Informationen über illegale und Freizeit-Drogen bereitstellen. Zu dieser Kategorie gehören auch Websites, die sich mit der Entwicklung oder dem Anbau von Drogen befassen. |
| 24 | **News** | Diese Kategorie umfasst News-Websites, die Nachrichten in Text- oder Videoform bereitstellen. Sie versucht, globale und lokale News-Websites abzudecken. Einige kleinere Lokalzeitungen werden jedoch möglicherweise nicht abgedeckt. |
| 25 | **Online-Dating** | Diese Kategorie umfasst kostenlose oder kommerzielle Online-Dating-Websites, auf denen Benutzer mit bestimmten Kriterien nach Kontakten/Partnern suchen können. Oder die Benutzer stellen eigene Profile von sich ein, um gefunden zu werden. Zu dieser Kategorie gehören kostenlose und zahlungspflichtige Online-Dating-Websites.<br><br>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.<br><br>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.<br><br>Dieser Website-Typ wird erkannt, weil er für folgende Zwecke verwendet wird (und daher evtl. auch blockiert werden sollte):<br>• 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).<br>• 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.<br>• 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.<br><br>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. |

Wenn Sie das Kontrollkästchen **Alle Benachrichtigungen für blockierte URLs nach Kategorien anzeigen** aktivieren, 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.

## Ausschlüsse

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.

***So können Sie eine URL zu einer Liste hinzufügen***

1. Klicken Sie im URL-Filterungsmodul eines Schutzplans auf **Ausschlüsse**.
2. Wählen Sie die gewünschte Liste aus: **Vertrauenswürdig** oder **Blockiert**.
3. Klicken Sie auf **Hinzufügen**.
4. Spezifizieren Sie die URL oder IP-Adresse, und aktivieren Sie dann das Kontrollkästchen.

**Beispiele für URL-Ausschlüsse**:

- Wenn Sie 'xyz.com' als vertrauenswürdig/nicht vertrauenswürdig hinzufügen, werden alle Adressen in der Domain 'xyz.com' als vertrauenswürdig bzw. nicht vertrauenswürdig behandelt (je nachdem, wo Sie die Domain hinzufügen wollen).
- Wenn Sie eine bestimmte Subdomain hinzufügen wollen, können Sie **mail.xyz.com** als vertrauenswürdig/nicht vertrauenswürdig hinzufügen. Dadurch werden nicht alle **xyz.com**-Adressen als vertrauenswürdig oder nicht vertrauenswürdig eingestuft.
- Wenn Sie IPv4-Adressen als vertrauenswürdig/nicht vertrauenswürdig hinzufügen wollen, müssen Sie folgendes Format verwenden, damit sie gültig sind: **20.53.203.50**.
- Wenn Sie mehrere URL-Ausschlüsse gleichzeitig hinzufügen wollen, müssen Sie jeden Eintrag in einer neuen Zeile einfügen:

**acronis.com**

**mail.xyz.com**

**20.53.203.50**

# 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.

## Quarantäne-Speicherort auf den Maschinen

Der Standardspeicherort für die Quarantäne von verdächtigen Dateien ist:

Bei Windows-Maschinen: `%ProgramData%\%Produkt_Name%\Quarantine`

Bei Mac-/Linux-Maschinen: `/usr/local/share/%Produkt_Name%/quarantine`

# Positivliste für Unternehmensapplikationen

**Wichtig**
Eine Positivliste für Unternehmensapplikationen setzt voraus, dass der Scan Service auf dem Management Server installiert ist.

Eine Antivirus-Lösung könnte zulässige unternehmensspezifische Applikationen als verdächtig identifizieren. Um solche Falsch-Positiv-Erkennungen zu vermeiden, werden vertrauenswürdige Applikationen manuell zu einer Positivliste hinzugefügt, was zeitaufwendig sein kann.

Cyber Protect kann diese Prozess automatisieren: vorhandene Backups werden vom Antivirus & Antimalware Protection-Modul gescannt und die gescannten Daten analysiert, sodass diese Applikationen in die Positivliste aufgenommen werden und somit zukünftige Falsch-Positiv-Erkennungen unterbunden werden. Die unternehmensweite Positivliste verbessert außerdem die Performance zukünftiger Scans.

Die Positivliste kann jederzeit aktiviert und deaktiviert werden. Wenn sie deaktiviert wird, werden die hinzugefügten Dateien vorübergehend ausgeblendet.

## Automatisches Hinzufügen zur Positivliste

1. Führen Sie ein Cloud-Scanning von Backups auf mindestens zwei Maschinen durch. Sie können dafür die Funktion '"Backup-Scanning-Plan" (S. 372)' verwenden.
2. Aktivieren Sie in den Einstellungen der Positivliste den Schalter **Positivliste automatisch generieren**.

## Manuelles Hinzufügen zur Positivliste

Wenn der Schalter **Positivliste automatisch generieren** deaktiviert ist, können Sie Dateien dennoch weiterhin manuell zur Positivliste hinzufügen.

1. Gehen Sie in der Cyber Protect Webkonsole zu **Antimalware Protection** –> **Positivliste**.
2. Klicken Sie auf **Datei hinzufügen**.
3. Spezifizieren Sie den Pfad zu der Datei und klicken Sie dann auf **Hinzufügen**.

## Unter Quarantäne stehende Dateien zur Positivliste hinzufügen

Sie können Dateien, die sich in der Quarantäne befinden, zur Positivliste hinzufügen.

1. Gehen Sie in der Cyber Protect Webkonsole zu **Antimalware Protection** –> **Quarantäne**.
2. Wählen Sie eine unter Quarantäne stehende Datei aus und klicken Sie dann auf **Zur Positivliste hinzufügen**.

## Einstellungen für die Positivliste

Wenn Sie den Schalter **Positivliste automatisch generieren** aktivieren, müssen Sie eine der folgenden Stufen des Heuristikschutzes spezifizieren:

- **Niedrig**
  Die Unternehmensapplikationen werden erst nach einer längeren Zeit und einigen Überprüfungen in die Positivliste aufgenommen. Solche Applikationen sind vertrauenswürdiger. Dieser Ansatz erhöht jedoch die Möglichkeit von Falsch-Positiv-Erkennungen. Die Kriterien, nach denen eine Datei als sauber und vertrauenswürdig eingestuft wird, sind hoch.
- **Standard**
  Die Unternehmensapplikationen werden der Positivliste entsprechend der empfohlenen Schutzstufe hinzugefügt, um mögliche falsch-positive Erkennungen zu reduzieren. Die Kriterien, nach denen eine Datei als sauber und vertrauenswürdig eingestuft wird, sind mittelstark.
- **Hoch**
  Unternehmensapplikationen werden der Whitelist 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.

## Details zu Elementen in der Positivliste anzeigen

Sie können auf ein Element in der Positivliste klicken, um weitere Informationen zu diesem Element zu erhalten und es online zu analysieren.

Wenn Sie sich bei einem Element, welches Sie hinzugefügt haben, unsicher sind, können Sie es im VirusTotal Analyzer überprüfen. Wenn Sie auf **Auf VirusTotal überprüfen** klicken, wird die Website

verdächtige Dateien und URLs analysieren, um Malware-Typen zu erkennen, wobei der Datei-Hash des von Ihnen hinzugefügten Elements verwendet wird. Sie können den Hash in der Zeichenfolge **Datei-Hash (MD5)** einsehen.

Der Wert **Maschinen** steht für die Anzahl der Maschinen, bei denen ein solcher Hash beim Backup-Scannen gefunden wurde. Dieser Wert wird nur angegeben, wenn ein Element aus dem Backup-Scanning oder der Quarantäne stammt. Dieses Feld bleibt leer, wenn die Datei manuell zur Positivliste hinzugefügt wurde.

# Antimalware-Scan von Backups

Um zu verhindern, dass infizierte Dateien aus Backups wiederhergestellt werden, können Sie Backups nach Malware durchsuchen lassen. Die Backup-Scanning-Funktionalität wird nur für Windows-Betriebssysteme unterstützt. Sie ist nur verfügbar, wenn der Scan Service auf dem Cyber Protect Management Server installiert ist.

Um Backups nach Malware durchsuchen zu lassen, erstellen Sie einen Backup-Scanning-Plan.

**Hinweis**
Aus Sicherheits- und Performance-Gründen empfehlen wir, dass Sie zum Scannen eine speziell dafür vorgesehene Maschine verwenden. Diese Maschine muss Zugriff auf alle Backups haben, die gescannt werden.

Sie können die Ergebnisse des Scans im 'Widget für die Backup-Scanning-Details' auf dem Dashboard überprüfen. Sie können außerdem den Backup-Status unter **Backup Storage** –> **Speicherorte** –> **<Backup-Name>** einsehen. Wenn kein Backup-Scan durchgeführt wurde, haben die Backups den Status **Nicht gescannt**. Nachdem ein Backup-Scan durchgeführt wurde, haben die Backups einen der folgenden Statuszustände:

- **Keine Malware**
- **Malware erkannt**

## Einschränkungen

- Nur Backups vom Typ **Komplette Maschine** oder **Laufwerke/Volumes** können nach Malware durchsucht werden.
- Es werden nur Volumes mit NTFS-Dateisystem und GPT- oder MBR-Partitionierung gescannt.
- Die unterstützten Backup-Speicherorte sind: **Cloud Storage**, **Lokaler Ordner** und **Netzwerkordner**.
- Backups mit Recovery-Punkten aus der kontinuierlichen Datensicherung (CDP) können zwar Scannen ausgewählt werden. Diese speziellen Recovery-Punkte werden dann beim Scan jedoch ausgeschlossen. Nur die regulären Recovery-Punkte werden gescannt.
- 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** ausführen.

# 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. Cyber Protect 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 einen Protection Agenten auf derjenigen Maschine, auf welcher die jeweilige Kollaborationsapplikation installiert ist.
2. Melden Sie sich an der Cyber Protect Webkonsole an und wenden Sie einen Schutzplan an, für den eines der folgenden Module aktiviert ist:
   - **Antivirus & Antimalware Protection** (wo die Einstellungen **Selbschutz** und and **Active Protection** aktiviert sind) – wenn Sie eine der Cyber Protect-Editionen haben:
   - **Active Protection** (wo die Einstellung **Selbstschutz** aktiviert ist) – wenn Sie eine der Cyber Backup-Editionen haben.
3. [Optional] Konfigurieren Sie das Modul **Patch-Verwaltung** im Schutzplan, wenn Sie die automatische Installation von Updates nutzen wollen.

Als Ergebnis wird Ihre Zoom-Applikation geschützt, was folgende Aktivitäten umfasst:

- Zoom-Client-Updates automatisch installieren
- Zoom-Prozesse vor Schadcode-Einschleusung schützen
- Verdächtige Aktionen durch Zoom-Prozesse verhindern
- Die Datei 'hosts' davor schützen, dass Domains hinzugefügt werden, die sich auf Zoom beziehen

# Schwachstellenbewertung und Patch-Verwaltung

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 in einem Schutzplan können Sie Ihre Maschinen auf Schwachstellen scannen lassen und so überprüfen, ob die Betriebssysteme und installierten Applikationen aktuell sind und ordnungsgemäß funktionieren.

Schwachstellenbewertungsscans werden für Maschinen mit folgenden Betriebssystemen unterstützt:

- Windows. Weitere Informationen finden Sie im Abschnitt '"Unterstützte Microsoft- und Drittanbieter-Produkte" (S. 571)'.
- Linux-Maschinen (CentOS 7/Virtuozzo/Acronis Cyber Infrastructure). Weitere Informationen finden Sie im Abschnitt '"Unterstützte Linux-Produkte" (S. 572)'.

Verwenden Sie die **Patch-Verwaltungs**-Funktionalität (PV), um Patches (Updates) für die Betriebssysteme und Applikationen zu verwalten, die auf Ihren Maschinen installiert sind, und Ihre Systeme so auf dem neuesten Stand zu halten. Im Patch-Verwaltungsmodul können Sie automatisch oder manuell genehmigen, welche Updates auf Ihren Maschinen installiert werden sollen.

Die Patch-Verwaltung wird für Maschinen unterstützt, die unter Windows laufen. Weitere Informationen finden Sie im Abschnitt '"Unterstützte Microsoft- und Drittanbieter-Produkte" (S. 571)'.

## Schwachstellenbewertung

Der Schwachstellenbewertungsprozess besteht aus folgenden Schritten:

1. Sie erstellen einen Schutzplan mit aktiviertem Schwachstellenbewertungsmodul, spezifizieren die Einstellungen für die Schwachstellenbewertung und weisen den Plan den gewünschten Maschinen zu.
2. Das System sendet (per Planung oder manuell ausgelöst) einen Befehl an die Protection Agenten, die Schwachstellenbewertungsscans auszuführen.
3. Die Agenten empfangen den Befehl, starten mit dem Scannen nach Schwachstellen und generieren die Scan-Aktivität.
4. Wenn der Schwachstellenbewertungsscan abgeschlossen wurde, generieren die Agenten die entsprechenden Ergebnisse und senden diese an den Monitoring Service.
5. Der Monitoring Service verarbeitet die Daten von den Agenten, zeigt die Ergebnisse im Widget für Schwachstellenbewertung an und listet die gefundenen Schwachstellen auf.
6. Mithilfe dieser Informationen können Sie entscheiden, welche der gefundenen Schwachstellen behoben werden sollen.

Sie können die Ergebnisse des Scannens nach Schwachstellen im Widget **Dashboard** –> **Überblick** –> **Schwachstellen / Gefundene Schwachstellen** überwachen.

## Unterstützte Microsoft- und Drittanbieter-Produkte

Folgende Microsoft-Produkte und Produkte von Drittanbietern für Windows-Betriebssysteme werden für die Schwachstellenbewertung unterstützt:

### Unterstützte Microsoft-Produkte

Desktop-Betriebssysteme

- Windows 7 (Enterprise, Professional, Ultimate)
- Windows 8
- Windows 8.1
- Windows 10

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 Drittanbieter-Produkte für Windows

Cyber Protect unterstützt die Schwachstellenbewertung und das Patchen einer breiten Palette von Dritthersteller-Applikationen – Kollaborationstools und VPN-Clients eingeschlossen, die bei Remote-Arbeitsszenarien von entscheidender Bedeutung sind.

Eine vollständige Liste der unterstützten Drittanbieter-Produkte für Windows finden Sie unter https://kb.acronis.com/content/62853.

## Unterstützte Linux-Produkte

Folgende Linux-Distributionen/-Versionen werden für die Schwachstellenbewertung 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

## Einstellungen für die Schwachstellenbewertung

Eine Anleitung zum Erstellen eines Schutzplans mit aktiviertem Schwachstellenbewertungsmodul finden Sie im Abschnitt '"Einen Schutzplan erstellen" (S. 214)'. Sie können Schwachstellenbewertungsscans per Planung oder bei Bedarf/manuell (mit der Aktion **Jetzt ausführen** in einem Schutzplan) durchführen lassen.

Sie können folgende Einstellungen im Schwachstellenbewertungsmodul spezifizieren.

## Scan-Umfang

Definieren Sie, welche Software-Produkte nach Schwachstellen gescannt werden sollen:

- Windows-Maschinen:
  - **Microsoft-Produkte**
  - **Windows-Produkte von Drittanbietern**
    Weitere Informationen über unterstützte Drittanbieter-Produkte für Windows 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 (beliebigen) Benutzers ausgelöst. Sie können diese Einstellung so ändern, dass nur ein bestimmtes Benutzerkonto den Task auslösen kann.
- **Wenn sich ein Benutzer vom System abmeldet** – Die Task-Ausführung wird standardmäßig durch die Abmeldung eines (beliebigen) Benutzers ausgelöst. Sie können diese Einstellung so ändern, dass nur ein bestimmtes Benutzerkonto den Task auslösen kann.

  **Hinweis**
  Der Task wird daher nicht beim Herunterfahren des Systems ausgeführt. Herunterfahren und Abmelden sind unterschiedliche Ereignisse in der Planungskonfiguration.

- **Beim Systemstart** – Der Task wird ausgeführt, wenn das Betriebssystem startet.
- **Beim Herunterfahren des Systems** – Der Task wird ausgeführt, wenn das Betriebssystem herunterfährt.

Standardeinstellung: **Planung nach Zeit**.

**Planungstyp**:

- **Monatlich** – Wählen Sie die Monate und dann die jeweiligen Wochen oder Tage des Monats, in denen der Task ausgeführt werden soll.
- **Täglich** – Wählen Sie die Wochentage aus, an denen der Task ausgeführt werden soll.
- **Stündlich** – Wählen Sie die Wochentage, die Anzahl der Wiederholungen sowie das Zeitintervall aus, in dem der Task ausgeführt werden soll.

Standardeinstellung: **Täglich**.

**Starten um** – Bestimmen Sie den genauen Zeitpunkt, an dem der Task ausgeführt werden soll.

**Innerhalb eines Zeitraums ausführen** – Bestimmten Sie einen Datumsbereich, innerhalb dessen die konfigurierte Planung gültig sein soll.

**Startbedingungen** – Definieren Sie alle Bedingungen, die gleichzeitig zutreffen müssen, damit der Task ausgeführt werden kann.

Die Startbedingungen für Antimalware-Scans sind ähnlich wie die Startbedingungen für das Backup-Modul, die wiederum im Abschnitt '"Startbedingungen" (S. 254)' beschrieben sind. Sie können folgende zusätzliche Startbedingungen definieren:

- **Task-Startzeit innerhalb eines Zeitfensters verteilen**– Diese Option ermöglicht es Ihnen, einen Zeitrahmen für den Task festzulegen, um Netzwerkengpässe zu vermeiden. Sie können die Verzögerung in Stunden oder Minuten spezifizieren. Wenn beispielsweise die Standardstartzeit 10:00 Uhr morgens ist und die Verzögerung 60 Minuten beträgt, dann beginnt der Task zwischen 10:00 und 11:00 Uhr morgens.
- **Task bei Neustart der Maschine ausführen, wenn die Maschine zur geplanten Zeit ausgeschaltet war**
- **Standby- oder Ruhezustandsmodus während der Task-Ausführung verhindern** – Diese Option gilt nur für Maschinen, die unter Windows laufen.
- **Wenn die Startbedingungen nicht erfüllt sind, Task trotzdem ausführen nach:** – Spezifizieren Sie einen Zeitraum, nach dem der Task unabhängig von anderen Startbedingungen auf jeden Fall gestartet werden soll.

**Hinweis**
Für Linux werden keine Startbedingungen unterstützt.

## Schwachstellenbewertung für Windows-Maschinen

Sie können Windows-Maschinen und Drittanbieter-Produkte für Windows auf Schwachstellen scannen.

1. Erstellen Sie in der Cyber Protect Webkonsole einen Schutzplan und aktivieren Sie das Modul für die **Schwachstellenbewertung**.
2. Spezifizieren Sie die Einstellungen für die Schwachstellenbewertung:
   - **Scan-Umfang** – wählen Sie **Microsoft-Produkte**, **Windows-Produkte von Drittanbietern** oder beides.
   - **Planung** – definieren Sie die Planung, auf deren Basis die Schwachstellenbewertung ausgeführt wird.
     Weitere Informationen über die **Planungs**-Optionen finden Sie im Abschnitt '"Einstellungen für die Schwachstellenbewertung" (S. 572)'.
3. Weisen Sie den Windows-Maschinen den Plan zu.

Nach einem Schwachstellenbewertungsscan wird Ihnen eine Liste der gefundenen Schwachstellen angezeigt. Sie können die Informationen bearbeiten und entscheiden, welche der gefundenen Schwachstellen behoben werden sollen.

Wenn Sie die Ergebnisse der Schwachstellenbewertung einsehen bzw. überwachen wollen, nutzen Sie die Widgets **Dashboard** –> **Überblick** –> **Schwachstellen / Gefundene Schwachstellen**.

## Schwachstellenbewertung für Linux-Maschinen

Sie können Linux-Maschinen nach Schwachstellen auf Applikations- und Kernel-Ebene scannen lassen.

***So können Sie die Schwachstellenbewertung für Linux-Maschinen konfigurieren***

1. Erstellen Sie in der Cyber Protect Webkonsole einen Schutzplan und aktivieren Sie das Modul für die **Schwachstellenbewertung**.
2. Spezifizieren Sie die Einstellungen für die Schwachstellenbewertung:
   - **Scan-Umfang** – wählen Sie **Linux-Pakete scannen**.
   - **Planung** – definieren Sie die Planung, auf deren Basis die Schwachstellenbewertung ausgeführt wird.
     Weitere Informationen über die **Planungs**-Optionen finden Sie im Abschnitt '"Einstellungen für die Schwachstellenbewertung" (S. 572)'.
3. Weisen Sie den Linux-Maschinen den Plan zu.

Nach einem Schwachstellenbewertungsscan wird Ihnen eine Liste der gefundenen Schwachstellen angezeigt. Sie können die Informationen bearbeiten und entscheiden, welche der gefundenen Schwachstellen behoben werden sollen.

Wenn Sie die Ergebnisse der Schwachstellenbewertung einsehen bzw. überwachen wollen, nutzen Sie die Widgets **Dashboard** –> **Überblick** –> **Schwachstellen / Gefundene Schwachstellen**.

## Gefundene Schwachstellen verwalten

Wenn die Schwachstellenbewertung mindestens einmal durchgeführt wurde und Schwachstellen gefunden wurden, können Sie diese unter **Software-Verwaltung** –> **Schwachstellen** einsehen. Die Liste der Schwachstellen enthält sowohl welche, für die Patches verfügbar sind, als auch solche ohne vorgeschlagene Patches. Sie können einen Filter verwenden, um nur Schwachstellen mit verfügbaren 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:<br>• **Kritisch**: 9 - 10 CVSS<br>• **Hoch**: 7 - 9 CVSS<br>• **Mittel**: 3 - 7 CVSS<br>• **Niedrig**: 0 - 3 CVSS<br>• **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 zu einer gefundenen Schwachstelle einsehen, wenn Sie auf deren Namen in der Liste klicken.

***So können Sie den Prozess zur Schwachstellenbehebung starten***

1. Gehen Sie in der Cyber Protect Webkonsole zum Bereich **Software-Verwaltung** –> **Schwachstellen**.
2. Wählen Sie die Schwachstellen aus der Liste aus und klicken Sie dann auf **Patches installieren**. Der Assistent zur Schwachstellenbehebung wird geöffnet.
3. Wählen Sie die zu installierenden Patches aus. Klicken Sie auf **Weiter**.
4. Wählen Sie die Maschinen aus, auf denen Patches installiert werden sollen.
5. Bestimmen Sie, ob die Maschinen nach der Patch-Installation neu gestartet werden sollen:
   - **Nein** – es wird kein Neustart nach der Patch-Installation initiiert.
   - **Bei Bedarf** – es wird nur dann ein Neustart initiiert, wenn dies für die Anwendung der Updates erforderlich ist.
   - **Ja** – es wird immer ein Neustart nach der Patch-Installation initiiert. Sie können jedoch eine Verzögerung spezifizieren.

   **Nicht neu starten, bevor das Backup abgeschlossen wurde** – wenn ein Backup-Prozess läuft, wird der Neustart der Maschine solange verzögert, bis das Backup abgeschlossen wurde.
6. Klicken Sie auf **Patches installieren**.

Als Ergebnis werden die ausgewählten Patches auf den ausgewählten Maschinen installiert.

# Patch-Verwaltung

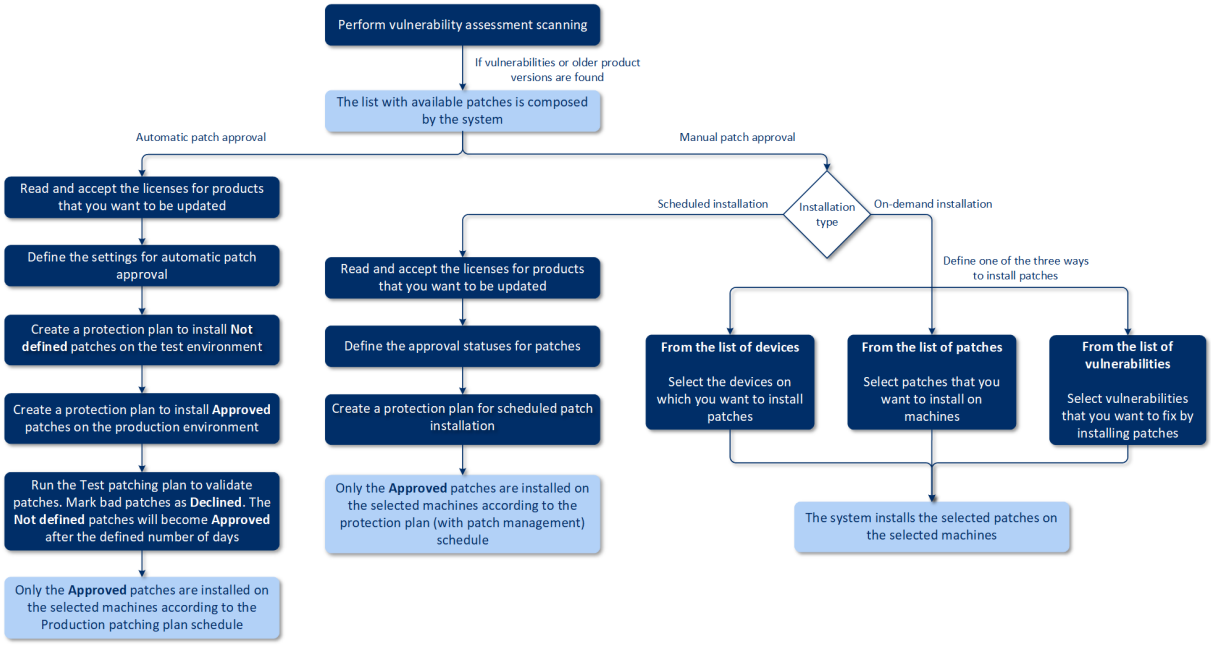
Sie können mit der Patch-Verwaltungsfunktionalität Folgendes tun:

- Updates auf Betriebssystem- und Applikationsebene installieren
- Patches manuell oder automatisch genehmigen
- Patches bei Bedarf (manuell) und per Planung installieren
- Genau definieren, welche Patches nach welchen unterschiedlichen Kriterien angewendet werden sollen: Schweregrad, Kategorie und Genehmigungsstatus
- Ein Vor-Update-Backup durchführen, um sich dagegen abzusichern, dass Updates fehlerhaft oder erfolglos sind
- Eine Option definieren, die regelt, ob es nach der Patch-Installation einen Neustart gibt

Mit Cyber Protect 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 mithilfe eines Schutzplans durchführen, bei dem das Modul **Schwachstellenbewertung** aktiviert wurde. Nach erfolgtem Scan stellt das System die Listen der gefundenen Schwachstellen und der verfügbaren Patches zusammen.
2. Anschließend können Sie die automatische Patch-Genehmigung konfigurieren oder die manuelle Patch-Genehmigung 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.

## Einstellungen für die Patch-Verwaltung

Eine Anleitung zum Erstellen eines Schutzplans mit aktiviertem Patch-Verwaltungsmodul finden Sie im Abschnitt 'Einen Schutzplan erstellen'. 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.

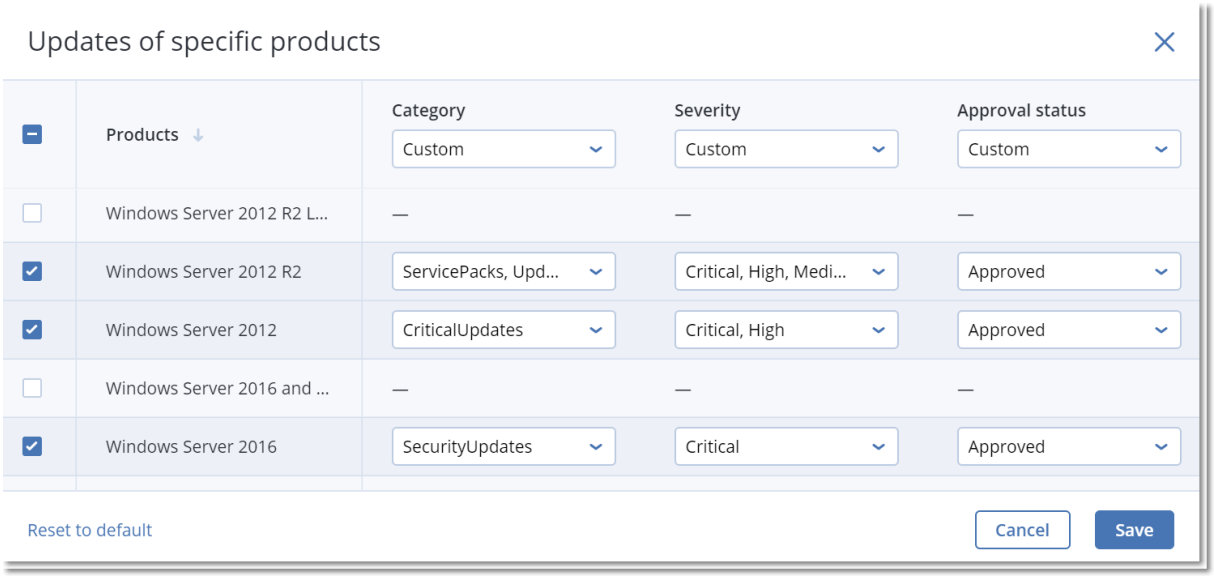
Für das Patch-Verwaltungsmodul können folgende Einstellungen spezifiziert werden:

### 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.

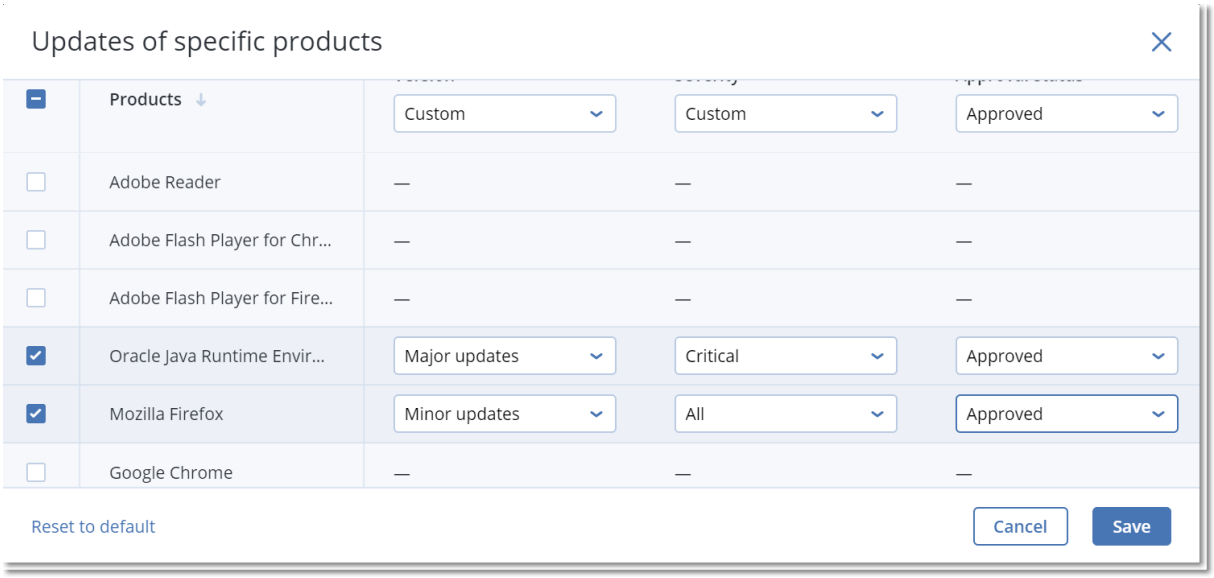



## Windows-Produkte von Drittherstellern

Wenn Sie Drittherstellers-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 größere Updates** – ermöglicht Ihnen, die letzte (jüngste) verfügbare Version eines Updates zu installieren.
- **Nur 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 (beliebigen) Benutzers ausgelöst. Sie können diese Einstellung so ändern, dass nur ein bestimmtes Benutzerkonto den Task auslösen kann.
- **Wenn sich ein Benutzer vom System abmeldet** – Die Task-Ausführung wird standardmäßig durch die Abmeldung eines (beliebigen) Benutzers ausgelöst. Sie können diese Einstellung so ändern, dass nur ein bestimmtes Benutzerkonto den Task auslösen kann.

  **Hinweis**
  Der Task wird daher nicht beim Herunterfahren des Systems ausgeführt. Herunterfahren und Abmelden sind unterschiedliche Ereignisse in der Planungskonfiguration.

- **Beim Systemstart** – Der Task wird ausgeführt, wenn das Betriebssystem startet.
- **Beim Herunterfahren des Systems** – Der Task wird ausgeführt, wenn das Betriebssystem herunterfährt.

Standardeinstellung: **Planung nach Zeit**.

**Planungstyp**:

- **Monatlich** – Wählen Sie die Monate und dann die jeweiligen Wochen oder Tage des Monats, in denen der Task ausgeführt werden soll.
- **Täglich** – Wählen Sie die Wochentage aus, an denen der Task ausgeführt werden soll.
- **Stündlich** – Wählen Sie die Wochentage, die Anzahl der Wiederholungen sowie das Zeitintervall aus, in dem der Task ausgeführt werden soll.

Standardeinstellung: **Täglich**.

**Starten um** – Bestimmen Sie den genauen Zeitpunkt, an dem der Task ausgeführt werden soll.

**Innerhalb eines Zeitraums ausführen** – Bestimmten Sie einen Datumsbereich, innerhalb dessen die konfigurierte Planung gültig sein soll.

**Startbedingungen** – Definieren Sie alle Bedingungen, die gleichzeitig zutreffen müssen, damit der Task ausgeführt werden kann.

Die Startbedingungen für Antimalware-Scans sind ähnlich wie die Startbedingungen für das Backup-Modul, die wiederum im Abschnitt '"Startbedingungen" (S. 254)' beschrieben sind. Sie können folgende zusätzliche Startbedingungen definieren:

- **Task-Startzeit innerhalb eines Zeitfensters verteilen**– Diese Option ermöglicht es Ihnen, einen Zeitrahmen für den Task festzulegen, um Netzwerkengpässe zu vermeiden. Sie können die Verzögerung in Stunden oder Minuten spezifizieren. Wenn beispielsweise die Standardstartzeit 10:00 Uhr morgens ist und die Verzögerung 60 Minuten beträgt, dann beginnt der Task zwischen 10:00 und 11:00 Uhr morgens.
- **Task bei Neustart der Maschine ausführen, wenn die Maschine zur geplanten Zeit ausgeschaltet war**
- **Standby- oder Ruhezustandsmodus während der Task-Ausführung verhindern** – Diese Option gilt nur für Maschinen, die unter Windows laufen.
- **Wenn die Startbedingungen nicht erfüllt sind, Task trotzdem ausführen nach:** – Spezifizieren Sie einen Zeitraum, nach dem der Task unabhängig von anderen Startbedingungen auf jeden Fall gestartet werden soll.

### 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. Dies ermöglicht es Ihnen, im Falle eines Patch-Installationsfehlers die betreffende Maschine auf ihren ursprünglichen Zustand zurücksetzen zu können. Damit die Option **Vor-Update-Backup** funktionieren kann, muss den entsprechenden Maschinen ein Schutzplan mit aktiviertem Patch-Verwaltungs- und Backup-Modul zugewiesen sein und in letzterem als Backup-Quelle entweder die komplette Maschine oder die Boot- und System-Volumes festgelegt sein. Wenn Sie ungeeignete Elemente für das Backup auswählen, wird das System verhindern, dass Sie die Option **Vor-Update-Backup** aktivieren können.

## Die Liste der Patches verwalten

Nachdem die Schwachstellenbewertung abgeschlossen wurde, können Sie die verfügbaren Patches im Bereich **Software-Verwaltung** –> **Patches** finden.

| Name | Beschreibung |
|---|---|
| **Name** | Der Name des Patches |
| **Schweregrad** | Der Schweregrad des Patches:<br>• **Kritisch**<br>• **Hoch**<br>• **Mittel**<br>• **Niedrig**<br>• **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:<br>• **Kritisches Update** – allgemein veröffentlichte Fixes für spezifische Probleme, die kritische, nicht sicherheitsbezogene Fehler beheben.<br>• **Sicherheitsupdate** – allgemein veröffentlichte Fixes für spezifische Produkte, die Sicherheitsprobleme beheben.<br>• **Definitionsupdates** – Updates für Viren-Definitionen oder andere Definitionsdateien.<br>• **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.<br>• **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.<br>• **Tools** – Hilfsprogramme (Utilities) oder Funktionen, die der Bewältigung einzelner oder mehrerer Aufgaben dienen.<br>• **Feature Packs** – neue Funktionen, die zumeist auch in die nächste Produktversion integriert werden.<br>• **Updates** – allgemein veröffentlichte Fixes für spezifische Probleme, die nicht kritische, nicht sicherheitsbezogene Fehler beheben.<br>• **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.<br><br>Sie können folgende Statuszustände für einen Patch definieren:<br><br>• **Genehmigt** – der Patch wurde auf mindestens einer Maschine installiert und mit 'Ok' eingestuft.<br>• **Abgelehnt** – der Patch ist nicht sicher und kann das System einer Maschine beschädigen<br>• **Nicht definiert** – der Patch-Status ist unklar und sollte validiert werden |
| **Lizenzvereinbarung** | • Lesen und akzeptieren<br>• 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 |

# Automatische Patch-Genehmigung

Die automatische Patch-Genehmigung ermöglicht Ihnen, den Prozess der Update-Installation auf den Maschinen zu vereinfachen. Betrachten wir an einem Beispiel, wie dies funktioniert.

## 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 (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 (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 Cyber Protect Webkonsole zum 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 Cyber Protect Webkonsole zum 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.

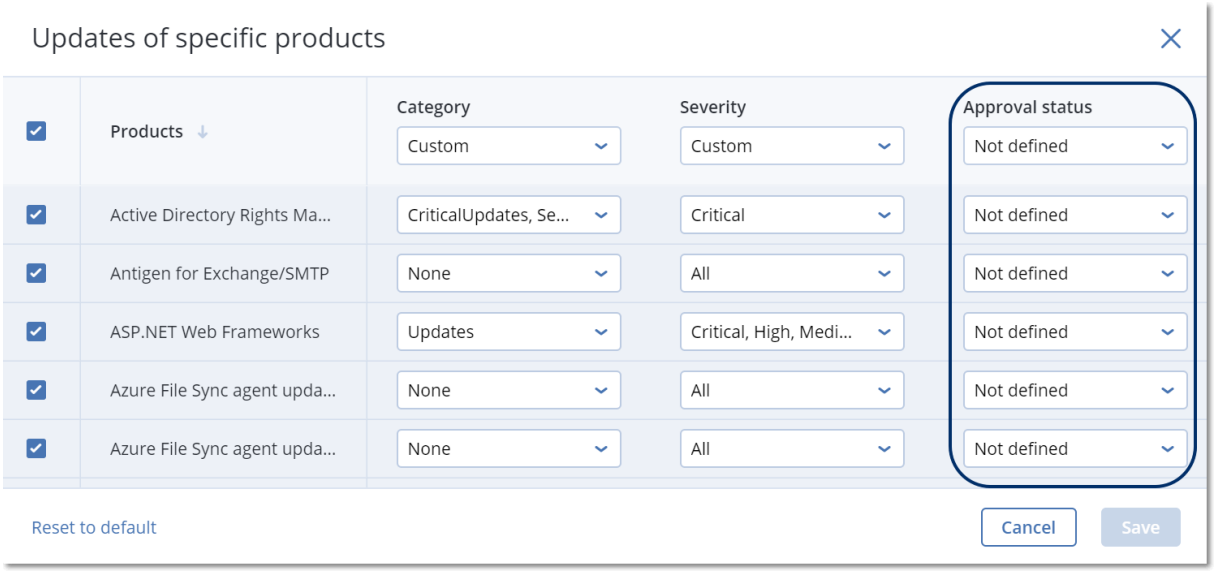
   Nehmen wir beispielsweise an, Sie spezifizieren 10 Tage. Sie haben den Schutzplan 'Patch-Test' für die Testmaschinen durchgeführt und die Patches wurden installiert. Diejenigen Patches, die die Maschinen offensichtlich beschädigt haben, wurden von Ihnen mit **Abgelehnt** gekennzeichnet, während die übrigen Patches den Status **Nicht definiert** behalten. Nach 10 Tage 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 Cyber Protect Webkonsole 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'.

   **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.



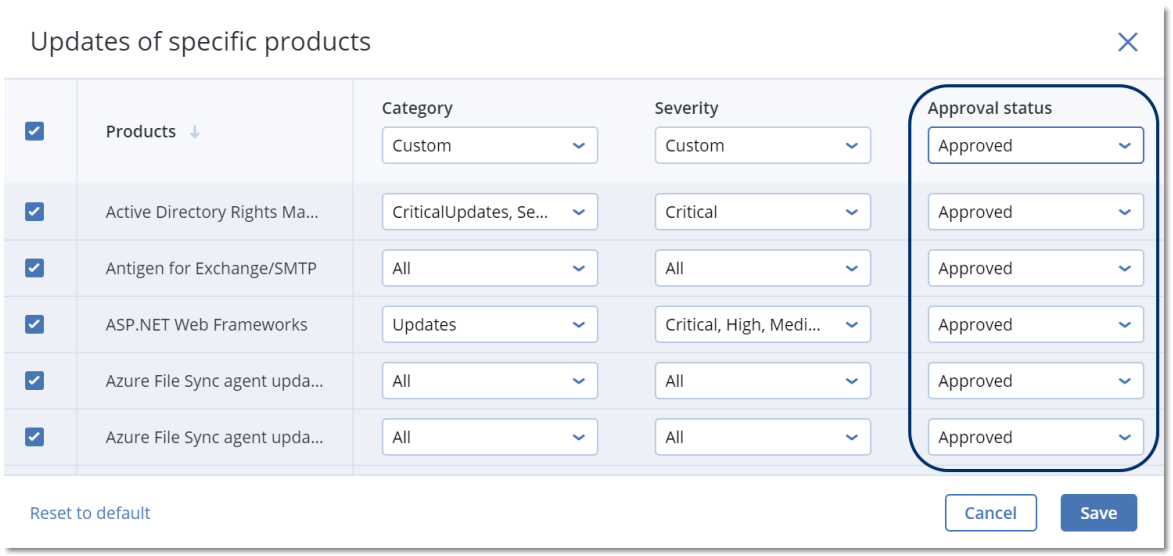

## Schritt 4: Erstellen Sie den Schutzplan zum Patchen der Produktionsumgebung

1. Gehen Sie in der Cyber Protect Webkonsole 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'.

**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.

**Hinweis**




## 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.

# Manuelle Patch-Genehmigung

Der Prozess einer manuellen Patch-Genehmigung verläuft folgendermaßen:

1. Gehen Sie in der Cyber Protect Webkonsole zum 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. 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.

## 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 Cyber Protect Webkonsole zum 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.
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.

## 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 sieben Tage nach seiner ersten Installation entfernt.
  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 30 Tage nach seiner ersten Installation entfernt.

# Smart Protection

## Bedrohungsfeed

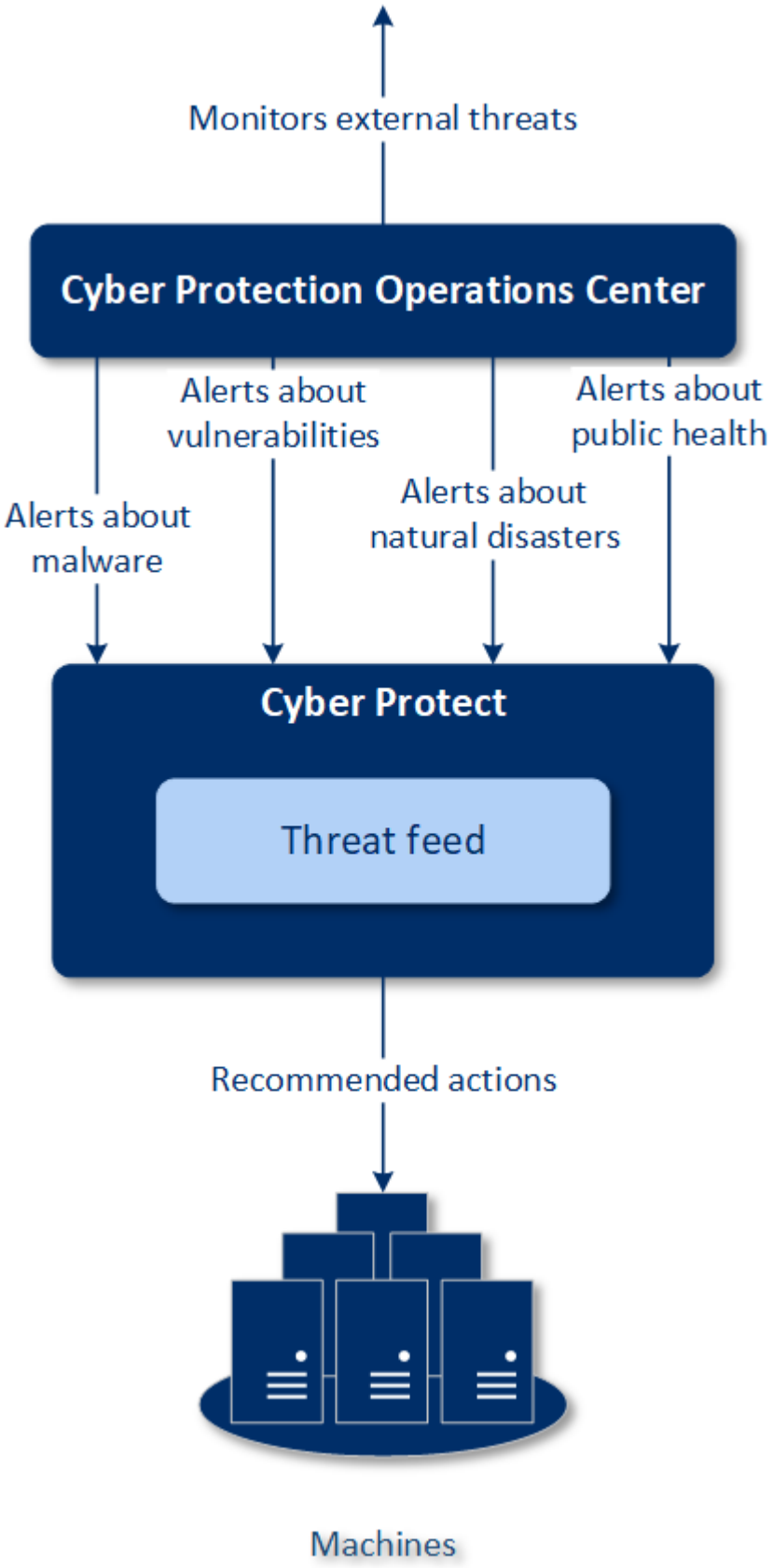
Das Acronis Cyber Protection Operations Center (CPOC) generiert Sicherheitsalarmmeldungen, die nur zu entsprechenden geographischen Regionen gesendet werden. Diese Sicherheitsmeldungen liefern Informationen über Malware, Schwachstellen, Naturkatastrophen, zu relevanten Aspekten der öffentlichen Gesundheit und anderen Arten von globalen Ereignissen, die Ihre Data Protection beeinträchtigen können. Der Bedrohungsfeed informiert Sie über potenzielle Bedrohungen und ermöglicht Ihnen so, diese abzuwenden.

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 Cyber Protect Webkonsole einsehen. Abhängig von der Art des Alarms können Sie empfohlene Aktionen zur Behebung des Problems durchführen.

Der Hauptablauf des Bedrohungsfeeds ist in der nachfolgenden Abbildung dargestellt.



Gehen Sie folgendermaßen vor, um bei einem Alarm, den Sie über das Acronis Cyber Protection Operations Center empfangen haben, die empfohlenen Aktionen durchzuführen:

1. Gehen Sie in der Cyber Protect Webkonsole zu **Dashboard** –> **Bedrohungsfeed**, um dort zu überprüfen, es es Sicherheitsalarmmeldungen gibt.

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 ausgewählten 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

Die Bedrohungsfeed-Alarmmeldungen werden nach folgenden Zeiträumen automatisch bereinigt:

- Natürliche Disaster – 1 Woche
- Schwachstellen – 1 Monat
- Malware – 1 Monat
- Öffentliche Gesundheit – 1 Woche

## Data Protection-Karte

Die Funktionalität 'Data Protection-Karte' ermöglicht Ihnen:

- Ausführliche Informationen über die auf Ihren Maschinen gespeicherten Daten (Klassifizierung, Speicherorte, Sicherungsstatus und weitere Informationen) zu erhalten.
- Zu ermitteln, ob Daten geschützt sind oder nicht. Daten werden als 'geschützt' angesehen, wenn diese per Backup (über einen Schutzplan mit aktiviertem Backup-Modul) gesichert wurden.
- Data Protection-Aktionen durchzuführen.

## Und so funktioniert es

1. Zuerst müssen Sie einen Schutzplan erstellen, in dem das Modul Data Protection-Karte aktiviert ist.
2. Nachdem dieser Plan ausgeführt wurde und Ihre Daten erkannt und analysiert wurden, erhalten Sie im Widget Data Protection-Karte eine visuelle Darstellung der Data Protection-Analyse.
3. Alternativ können Sie auch zu **Geräte** –> **Data Protection-Karte** gehen, wo Ihnen Informationen über ungeschützte Dateien pro Gerät angezeigt werden.
4. Sie können Aktionen vornehmen, um die ungeschützten Dateien, die auf den Geräten gefunden wurden, zu schützen.

## Erkannte ungeschützte Dateien verwalten

Gehen Sie folgendermaßen vor, um wichtige Dateien, die als ungeschützt erkannt wurden, zu sichern:

1. Gehen Sie in der Cyber Protect Webkonsole 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 ausführliche Informationen über die ungeschützten Dateien auf einem bestimmten Gerät erhalten wollen, klicken Sie auf den Namen des entsprechenden Gerätes.

   Ihnen wird eine Liste mit ungeschützten Dateien angezeigt – aufgeschlüsselt nach Erweiterungen und Speicherort. Sie können diese Liste nach Dateierweiterungen filtern.
3. Wenn Sie alle ungeschützten Dateien sichern wollen, klicken Sie auf **Alle Dateien schützen**. Sie werden zur Liste der Pläne weitergeleitet, wo Sie einen Schutzplan mit aktiviertem Backup-Modul erstellen können.

Wenn Sie die Informationen über die ungeschützten Dateien in Form eines Berichts erhalten wollen, können Sie auf den Befehl **Ausführlichen Bericht im CSV-Format herunterladen** klicken.

## Einstellungen für die Data Protection-Karte

Eine Anleitung zum Erstellen eines Schutzplans mit aktiviertem Modul für die Data Protection-Karte finden Sie im Abschnitt 'Einen Schutzplan erstellen'.

Für das Data Protection-Karten-Modul können folgende Einstellungen spezifiziert werden:

## Planung

Sie können verschiedene Einstellungen für einen Zeitplan definieren, auf dessen Basis der Task für die Data Protection-Karte ausgeführt wird.

**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 (beliebigen) Benutzers ausgelöst. Sie können diese Einstellung so ändern, dass nur ein bestimmtes Benutzerkonto den Task auslösen kann.
- **Wenn sich ein Benutzer vom System abmeldet** – Die Task-Ausführung wird standardmäßig durch die Abmeldung eines (beliebigen) Benutzers ausgelöst. Sie können diese Einstellung so ändern, dass nur ein bestimmtes Benutzerkonto den Task auslösen kann.

  **Hinweis**
  Der Task wird daher nicht beim Herunterfahren des Systems ausgeführt. Herunterfahren und Abmelden sind unterschiedliche Ereignisse in der Planungskonfiguration.

- **Beim Systemstart** – Der Task wird ausgeführt, wenn das Betriebssystem startet.
- **Beim Herunterfahren des Systems** – Der Task wird ausgeführt, wenn das Betriebssystem herunterfährt.

Standardeinstellung: **Planung nach Zeit**.

**Planungstyp**:

- **Monatlich** – Wählen Sie die Monate und dann die jeweiligen Wochen oder Tage des Monats, in denen der Task ausgeführt werden soll.
- **Täglich** – Wählen Sie die Wochentage aus, an denen der Task ausgeführt werden soll.
- **Stündlich** – Wählen Sie die Wochentage, die Anzahl der Wiederholungen sowie das Zeitintervall aus, in dem der Task ausgeführt werden soll.

Standardeinstellung: **Täglich**.

**Starten um** – Bestimmen Sie den genauen Zeitpunkt, an dem der Task ausgeführt werden soll.

**Innerhalb eines Zeitraums ausführen** – Bestimmten Sie einen Datumsbereich, innerhalb dessen die konfigurierte Planung gültig sein soll.

**Startbedingungen** – Definieren Sie alle Bedingungen, die gleichzeitig zutreffen müssen, damit der Task ausgeführt werden kann.

Die Startbedingungen für Antimalware-Scans sind ähnlich wie die Startbedingungen für das Backup-Modul, die wiederum im Abschnitt '"Startbedingungen" (S. 254)' beschrieben sind. Sie können folgende zusätzliche Startbedingungen definieren:

- **Task-Startzeit innerhalb eines Zeitfensters verteilen**– Diese Option ermöglicht es Ihnen, einen Zeitrahmen für den Task festzulegen, um Netzwerkengpässe zu vermeiden. Sie können die Verzögerung in Stunden oder Minuten spezifizieren. Wenn beispielsweise die Standardstartzeit 10:00 Uhr morgens ist und die Verzögerung 60 Minuten beträgt, dann beginnt der Task zwischen 10:00 und 11:00 Uhr morgens.
- **Task bei Neustart der Maschine ausführen, wenn die Maschine zur geplanten Zeit ausgeschaltet war**
- **Standby- oder Ruhezustandsmodus während der Task-Ausführung verhindern** – Diese Option gilt nur für Maschinen, die unter Windows laufen.
- **Wenn die Startbedingungen nicht erfüllt sind, Task trotzdem ausführen nach:** – Spezifizieren Sie einen Zeitraum, nach dem der Task unabhängig von anderen Startbedingungen auf jeden Fall gestartet werden soll.

## 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.

# Remote-Desktop-Zugriff

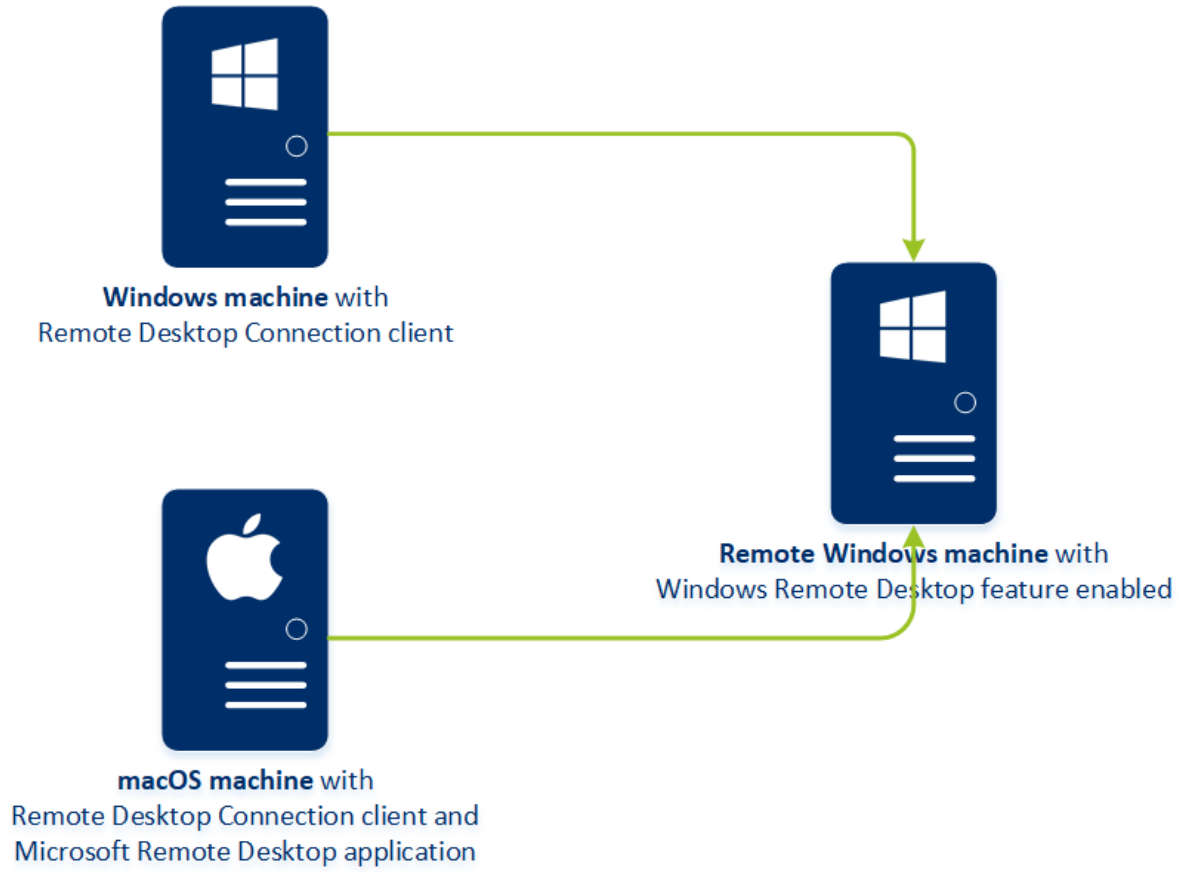
## Remote-Zugriff (RDP- und HTML5-Clients)

Cyber Protect ermöglicht Ihnen Remote-Zugriffe auf Maschinen. Sie können sich direkt über die Webkonsole remote (aus der Ferne) mit Ihren Benutzer-Maschinen verbinden, um diese zu verwalten. Dies ermöglicht Ihnen, Ihren Benutzern bei der Lösung von Problemen auf deren Maschinen zu helfen.

Voraussetzungen:

- Ein Protection Agent ist auf der Remote-Maschine installiert und auf dem Management Server registriert.
- Der Maschine wurde eine passende Cyber Protect-Lizenz zugewiesen.
- Der Remote-Desktop-Verbindungsclient ist auf der Maschine installiert, von der aus die Verbindung initialisiert wird.
- Die Maschine, von der die RDP-Verbindung initialisiert wird, muss über ihren Host-Namen auf den Management Server zugreifen können. Die DNS-Einstellungen müssen entsprechend konfiguriert sein – oder der Host-Name des Management Servers muss in der Datei 'hosts' eingetragen werden.

Eine Remote-Verbindung kann von Windows- und macOS-Maschinen aus hergestellt werden.



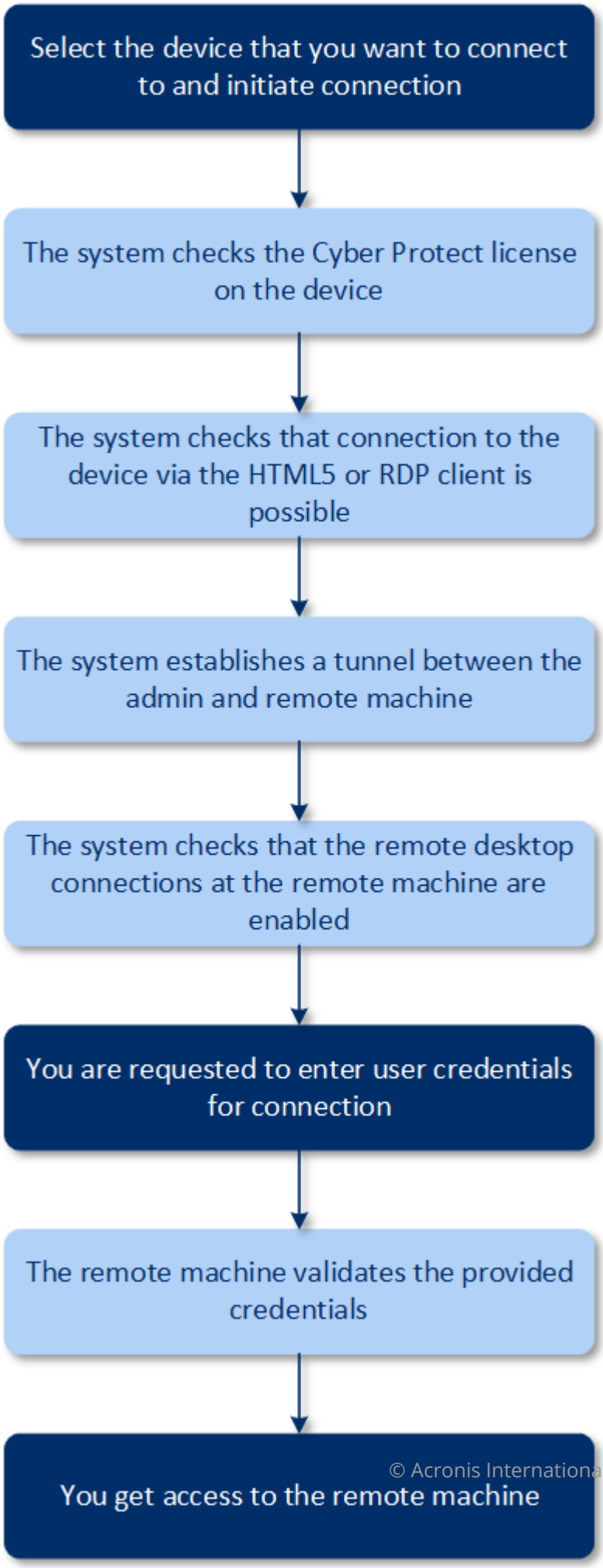
Die Remote-Zugriffsfunktionalität kann nur für Verbindungen mit Windows-Maschinen verwendet werden, auf denen die Windows-Remote-Desktop-Unterstützung aktiviert ist. Deshalb ist beispielsweise kein Remote-Zugriff auf ein Windows 10 Home- oder macOS-System möglich.

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 eine Cyber Protect-Lizenz 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 Anmeldedaten ein und erhalten Sie, nachdem die Anmeldedaten überprüft wurden, Zugriff auf die Remote-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 Cyber Protect Webkonsole zu **Geräte** –> **Alle Geräte**.
2. Klicken Sie auf die Maschine, auf die Sie aus der Ferne zugreifen wollen, und klicken Sie dann auf **Cyber Protection Desktop** –> **Über RDP-Client verbinden** oder **Über HTML5-Client verbinden**.

   **Hinweis**
   Verbindungen über einen HTML5-Client sind nur verfügbar, wenn der Management Server auf einer Linux-Maschine installiert ist.

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 Remote-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.

# Eine Remote-Verbindung freigeben

Mitarbeiter, die im Home-Office arbeiten, benötigen manchmal Zugriff auf ihre(n) Computer im Büro. Es kann jedoch vorkommen, dass Ihr Unternehmen kein konfiguriertes VPN oder andere Tools für Remote-Verbindungen hat. Cyber Protect bietet Ihnen die Möglichkeit, eine RDP-Link für Endbenutzer freizugeben und diesen so einen Remote-Zugriff auf ihre Maschinen zu ermöglichen.

***So können Sie die Funktionalität zur Freigabe von Remote-Verbindungen aktivieren***

1. Gehen Sie in der Cyber Protect Webkonsole zu **Einstellungen** –> **Schutz** –> **Remote-Verbindung**.
2. Aktivieren Sie das Kontrollkästchen **Remote-Desktop-Verbindung freigeben**.

Wenn Sie anschließend ein Gerät in der Cyber Protect Webkonsole auswählen, wird dort die neue Option **Remote-Verbindung freigeben** angezeigt.

***So können Sie eine Remote-Verbindung für Ihre Benutzer freigeben***

1. Gehen Sie in der Cyber Protect Webkonsole zu **Geräte** –> **Alle Geräte**.
2. Wählen Sie das Gerät aus, zu dem Sie eine Remote-Verbindung bereitstellen wollen.
3. Klicken Sie auf **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.

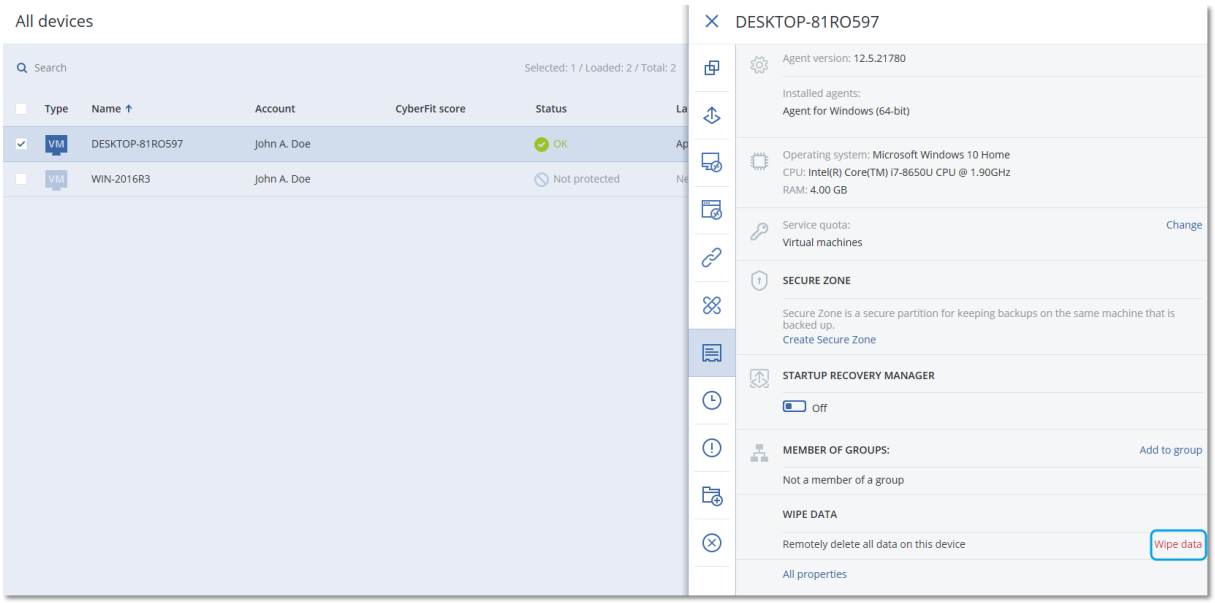
Nachdem Sie den Link abgerufen haben, können Sie diesen per E-Mail oder über andere Kommunikationsmittel teilen. Der Benutzer, für den der Link freigegeben wurde, muss darauf klicken und dann den Verbindungstyp auswählen:

- 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 entsprechenden Anmeldefenster weitergeleitet, wo er die Anmeldedaten für den Zugriff auf die Maschine eingeben muss.

# Remote-Löschung

Über die Remote-Löschung kann ein Cyber Protect 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 Cyber Protect Webkonsole zu **Geräte** –> **Alle Geräte**.
2. Wählen Sie die Maschine aus, deren Daten Sie vollständig löschen wollen.

   **Hinweis**
   Sie können nur jeweils die Daten einer Maschine gleichzeitig löschen.

3. Klicken Sie auf **Details** und dann auf den Befehl **Daten löschen**.
   Die Option **Daten löschen** ist nicht verfügbar, wenn die von Ihnen ausgewählte Maschine offline ist.
4. Bestätigen Sie Ihre Wahl.
5. Geben Sie die Anmeldedaten des lokalen Administrators dieser Maschine ein und klicken Sie dann auf den Befehl **Daten löschen**.

   **Hinweis**
   Über **Dashboard** –> **Aktivitäten** können Sie Details zum Löschvorgang und wer diesen gestartet einsehen.

# Gerätegruppen

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).

## 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.

## 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. Ansonsten 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.

# 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 Attribute und Operatoren verwenden (wie unten beschrieben).
3. Klicken Sie neben dem Suchfeld auf **Speichern unter**.

**Hinweis**
Bei der Gruppenerstellung werden einige Attribute nicht unterstützt. Siehe die Tabelle im unteren Abschnitt 'Suchabfragen'.

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

## Suchabfragen

In der nachfolgenden Tabelle finden Sie eine Übersicht der verfügbaren Attribute, die Sie in Ihren Suchabfragen verwenden können.

| Attribut | Bedeutung | Beispiele für Suchanfragen | Für Gruppenerstellung unterstützt |
|---|---|---|---|
| `name` | • Host-Name für physische Maschinen<br>• Name für virtuelle Maschinen<br>• Datenbankname<br>• E-Mail-Adresse für Postfächer | `name = 'en-00'` | Ja |
| `parameters.MacAddress` | MAC-Adresse. | `parameters.MacAddress LIKE '00-22-4D-50-25-E5'` | Ja |
| `comment` | Kommentar für ein Gerät. Er kann | `comment = 'important machine'` | Ja |

| Attribut | Bedeutung | Beispiele für Suchanfragen | Für Gruppenerstellung unterstützt |
|---|---|---|---|
| | automatisch oder manuell spezifiziert werden.<br><br>Standardwert:<br><br>• Bei physischen Maschinen, die unter Windows laufen, wird die Computer-Beschreibung in Windows automatisch als Kommentar übernommen. Dieser Wert wird alle 15 Minuten synchronisiert.<br>• Leer für andere Geräte.<br><br>**Hinweis**<br>Wenn Sie Text manuell in das Kommentarfeld eingeben, wird die automatische Synchronisierung der Windows-Beschreibung deaktiviert. Wenn Sie diese wieder aktivieren wollen, müssen Sie den von Ihnen hinzugefügten Kommentar löschen.<br><br>Um die automatisch synchronisierten Kommentare für Ihre Geräte aktualisieren zu können, müssen Sie den Managed Machine Service in den **Windows-Diensten** neu starten oder folgende | `comment = ''` (alle Maschinen ohne Kommentar) | |

| Attribut | Bedeutung | Beispiele für Suchanfragen | Für Gruppenerstellung unterstützt |
|---|---|---|---|
| | Befehle in der Eingabeaufforderung ausführen:<br>`net stop mms`<br>`net start mms`<br>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**.<br>Wenn Sie einen Kommentar hinzufügen oder ändern wollen, klicken Sie auf **Hinzufügen** oder **Bearbeiten**.<br>Bei Geräten, auf denen ein Protection Agent installiert ist, gibt es zwei separate Kommentarfelder:<br>• Agenten-Kommentar<br>◦ Bei physischen Maschinen, die unter Windows laufen, wird die Computer-Beschreibung in Windows automatisch als Kommentar übernommen. Dieser Wert wird alle 15 Minuten | | |

| Attribut | Bedeutung | Beispiele für Suchanfragen | Für Gruppenerstellung unterstützt |
|---|---|---|---|
| | synchronisiert.<br>◦ Leer für andere Geräte.<br><br>**Hinweis**<br>Wenn Sie Text manuell in das Kommentarfeld eingeben, wird die automatische Synchronisierung der Windows-Beschreibung deaktiviert. Wenn Sie diese wieder aktivieren wollen, müssen Sie den von Ihnen hinzugefügten Kommentar löschen.<br><br>• Geräte-Kommentar<br>◦ Wenn der Agenten-Kommentar automatisch spezifiziert wird, wird er als Geräte-Kommentar kopiert. Manuell hinzugefügte Agenten-Kommentare werden nicht als Geräte-Kommentare kopiert.<br>◦ Geräte-Kommentare werden nicht als Agenten-Kommentare kopiert.<br><br>Für ein Gerät können einer oder beide | | |

| Attribut | Bedeutung | Beispiele für Suchanfragen | Für Gruppenerstellung unterstützt |
|---|---|---|---|
| | Kommentare spezifiziert werden – oder beide können auch leer bleiben. Wenn beide Kommentare spezifiziert sind, hat der Geräte-Kommentar die höhere Priorität.<br><br>Wenn Sie einen Agenten-Kommentar einsehen wollen, wählen Sie unter **Einstellungen** – > **Agenten** das Geräte mit dem Agenten aus, klicken Sie dann auf **Details** und suchen Sie anschließend den Bereich **Kommentar**.<br><br>Wenn Sie einen Gerätekommentar einsehen wollen, wählen Sie unter **Geräte** das entsprechende Geräte aus, klicken Sie dann auf **Details** und suchen Sie anschließend den Abschnitt**Kommentar**.<br><br>Wenn Sie einen Kommentar manuell hinzufügen oder ändern wollen, klicken Sie auf **Hinzufügen** oder **Bearbeiten**. | | |
| `ip` | IP-Adresse (nur für physische Maschinen). | `ip RANGE ('10.250.176.1','10.250.176.50')` | Ja |
| `cpuArch` | CPU-Architektur.<br><br>Mögliche Werte: | `cpuArch = 'x64'` | Ja |

| Attribut | Bedeutung | Beispiele für Suchanfragen | Für Gruppenerstellung unterstützt |
|---|---|---|---|
| | • `'x64'`<br>• `'x86'` | | |
| `memorySize` | RAM-Größe in Megabyte (MiB). | `memorySize < 1024` | Ja |
| `cpuName` | CPU-Name. | `cpuName LIKE '%XEON%'` | Ja |
| `insideVm` | Virtuelle Maschine, die einen Agenten enthält.<br>Mögliche Werte:<br>• `true`<br>• `false` | `insideVm = true` | Ja |
| `tzOffset` | Zeitzonenversatz der Maschine in Minuten. | `tzOffset = 120` | Ja |
| `parameters.Architecture` | Betriebssystem-Architektur.<br>Mögliche Werte:<br>• `'x86'`<br>• `'x64'` | `parameters.Architecture = 'x86'` | Ja |
| `osName` | Betriebssystemname. | `osName LIKE '%Windows XP%'` | Ja |
| `osType` | Betriebssystemtyp.<br>Mögliche Werte:<br>• `'windows'`<br>• `'linux'`<br>• `'macosx'` | `osType IN ('linux', 'macosx')` | Ja |
| `osProductType` | Der Betriebssystemprodukttyp.<br>Mögliche Werte:<br>• `'dc'`<br>Steht für Domain Controller.<br>• `'server'`<br>• `'workstation'` | `osProductType = 'server'` | Ja |
| `virtualType` | Typ der virtuellen | `virtualType = 'vmwesx'` | Ja |

| Attribut | Bedeutung | Beispiele für Suchanfragen | Für Gruppenerstellung unterstützt |
|---|---|---|---|
| | Maschine.<br>Mögliche Werte:<br>• `'vmwesx'` Virtuelle VMware-Maschinen.<br>• `'mshyperv'` Virtuelle Hyper-V-Maschinen.<br>• `'pcs'` Virtuelle Virtuozzo-Maschinen.<br>• `'hci'` Virtuelle Virtuozzo Hybrid Infrastructure-Maschinen.<br>• `'scale'` Virtuelle Scale Computing HC3-Maschinen.<br>• `'ovirt'` Virtuelle oVirt-Maschinen | | |
| `osSp` | Service-Paket des Betriebssystems. | `osSp = 1` | Ja |
| `osVersionMajor` | Hauptversion des Betriebssystems. | `osVersionMajor = 1` | Ja |
| `osVersionMinor` | Nebenversion des Betriebssystems. | `osVersionMminor = 1` | Ja |
| `isOnline` | Maschinenverfügbarkeit.<br>Mögliche Werte:<br>• `true`<br>• `false` | `isOnline = true` | Nein |
| `tenant` | Der Name der Abteilung, zu welcher das Gerät gehört. | `tenant = 'Unit 1'` | Ja |

| Attribut | Bedeutung | Beispiele für Suchanfragen | Für Gruppenerstellung unterstützt |
|---|---|---|---|
| `tenantId` | Die ID der Abteilung, zu welcher das Gerät gehört.<br>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 |
| `state` | Gerätestadium.<br>Mögliche Werte:<br>• `'idle'`<br>• `'interactionRequired'`<br>• `'canceling'`<br>• `'backup'`<br>• `'recover'`<br>• `'install'`<br>• `'reboot'`<br>• `'failback'`<br>• `'testReplica'`<br>• `'run_from_image'`<br>• `'finalize'`<br>• `'failover'`<br>• `'replicate'`<br>• `'createAsz'`<br>• `'deleteAsz'`<br>• `'resizeAsz'` | `state = 'backup'` | Nein |
| `status` | Ressourcenstatus.<br>Mögliche Werte:<br>• `'notProtected'`<br>• `'ok'`<br>• `'warning'`<br>• `'error'` | `status = 'ok'` | Nein |

| Attribut | Bedeutung | Beispiele für Suchanfragen | Für Gruppenerstellung unterstützt |
|---|---|---|---|
| | • `'critical'` | | |
| `protectedByPlan` | Geräte, die durch einen Schutzplan mit einer bestimmten ID gesichert werden.<br><br>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 |

| Attribut | Bedeutung | Beispiele für Suchanfragen | Für Gruppenerstellung unterstützt |
|---|---|---|---|
| `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 |
| `ou` | Maschinen, die zu der spezifizierten Active Directory-Organisationseinheit gehören. | `ou IN ('RnD', 'Computers')` | Ja |
| `id` | Geräte-ID.<br>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 erfolgreichen Backups.<br>Das Format ist `'YYYY-MM-DD HH:MM'`. | `lastBackupTime > '2022-03-11'`<br>`lastBackupTime <= '2022-03-11 00:15'`<br>`lastBackupTime is null` | Nein |
| `lastBackupTryTime` | Zeitpunkt des letzten Backup-Versuchs.<br>Das Format ist `'YYYY-MM-DD HH:MM'`. | `lastBackupTryTime >= '2022-03-11'` | Nein |
| `nextBackupTime` | Zeitpunkt des nächsten Backups.<br>Das Format ist `'YYYY-MM-DD HH:MM'`. | `nextBackupTime >= '2022-08-11'` | Nein |
| `agentVersion` | Version des installierten Protection Agenten. | `agentVersion LIKE '12.0.*'` | Ja |

| Attribut | Bedeutung | Beispiele für Suchanfragen | Für Gruppenerstellung unterstützt |
|---|---|---|---|
| `hostId` | Interne ID des Protection Agenten.<br><br>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.<br><br>Mögliche Werte:<br>• `'machine'`<br>• `'virtual_machine.vmwesx'`<br>• `'virtual_machine.mshyperv'`<br>• `'virtual_machine.rhev'`<br>• `'virtual_machine.kvm'`<br>• `'virtual_machine.xen'` | `resourceType = 'machine'`<br><br>`resourceType in ('mssql_aag_database', 'mssql_database')` | Ja |
| `hasAsz` | Protection Agent auf einer physischen Maschine mit AcronisEiner Secure Zone.<br><br>Mögliche Werte:<br>• `true`<br>• `false` | `hasAsz=true` | Ja |
| `chassis` | Maschinen-Gehäusetyp.<br><br>Mögliche Werte:<br>• unknown | `chassis='laptop'` | Ja |

| Attribut | Bedeutung | Beispiele für Suchanfragen | Für Gruppenerstellung unterstützt |
|---|---|---|---|
| | • laptop<br>• desktop<br>• server<br>• other | | |

**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'` |
| `IN (<wert1>,... <wertN>)` | Dieser Operator wird verwendet, um zu testen, ob ein Ausdruck mit irgendeinem Wert in einer Liste von Werten übereinstimmt. | `osType IN ('windows', 'linux')` |
| `NOT` | Operator für logische Negation. | `NOT(osProductType = 'workstation')` |
| `NOT IN (<value1>,... <valueN>)` | Dieser Operator ist das Gegenteil des Operators `IN`. | `NOT osType IN ('windows', 'linux')` |
| `LIKE 'wildcard pattern'` | Dieser Operator wird verwendet, um zu testen, ob ein Ausdruck mit dem Platzhalter-Muster übereinstimmt.<br>Die folgenden Platzhalteroperatoren können verwendet werden:<br>• * oder %. Der Asterisk und das Prozentzeichen stehen für kein, ein oder oder mehrere Zeichen.<br>• _. Das Unterstrichzeichen repräsentiert ein | `name LIKE 'en-00'`<br>`name LIKE '*en-00'`<br>`name LIKE '*en-00*'`<br>`name LIKE 'en-00_'` |

| Operator | Bedeutung | Beispiele |
|---|---|---|
| | einzelnes Zeichen | |
| `RANGE (<starting_value>, <ending_value>)` | 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')` |
| `= or ==` | *Ist gleich*-Operator. | `osProductType = 'server'` |
| `!=` oder `<>` | *Ist nicht gleich*-Operator. | `id != '4B2A7A93-A44F-4155-BDE3-A023C57C9431'` |
| `<` | *Kleiner als*-Operator. | `memorySize < 1024` |
| `>` | *Größer als*-Operator | `diskSize > 300GB` |
| `<=` | *Kleiner als- oder Ist gleich*-Operator. | `lastBackupTime <= '11.05.22 00:15'` |
| `>=` | *Größer als- oder Ist gleich*-Operator. | `nextBackupTime >= '11.09.22'` |

# 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 'Backup' beschrieben – einen neuen Schutzplan.

# Überwachung und Berichterstellung

Das Dashboard **Überblick** ermöglicht Ihnen, den aktuellen Status Ihrer geschützten Infrastruktur zu überwachen.

Der Bereich **Berichte** ermöglicht Ihnen, Berichte über Ihre geschützte Infrastruktur generieren zu lassen (je nach Bedarf oder nach Planung). Dieser Abschnitt ist nur mit einer Advanced-Lizenz verfügbar.

## Das Dashboard 'Überblick'

Das Dashboard **Überblick** enthält eine Reihe benutzerdefinierbarer Widgets, die Ihnen einen Überblick über Ihre geschützte Infrastruktur geben. Sie können aus mehr als 20 Widgets wählen, die als Diagramme (z.B. Torten oder Balken), Tabellen oder Listen angezeigt werden. Die Widgets haben anklickbare Elemente, über die Sie Probleme untersuchen und beheben können. Die Informationen in den Widgets werden alle fünf Minuten aktualisiert.

Mit einer Advanced-Lizenz können Sie den aktuellen Zustand des Dashboards auch in Form einer .pdf- und/oder .xlsx-Datei herunterladen oder als E-Mail versenden. Bevor Sie das Dashboard per E-Mail versenden, sollten Sie überprüfen, dass die **E-Mail-Server**-Einstellungen konfiguriert wurden.

Die verfügbaren Widgets hängen davon ab, welche Edition von Cyber Protect Sie haben. Die vorgegebenen Widgets sind nachfolgend aufgelistet:

| Widget | Verfügbarkeit | Beschreibung |
|---|---|---|
| Cyber Protection | Nicht verfügbar in den Cyber Backup-Editionen | Zeigt allgemeine Informationen über blockierte Malware, blockierte URLs, gefundene Schwachstellen, installierte Patches und die Größe von Backups an. |
| Schutzstatus | In allen Editionen verfügbar | Zeigt den aktuellen Schutzstatus für alle Maschinen an. |
| Aktivitäten | In allen Editionen verfügbar | Zeigt eine Übersicht über diejenigen Aktivitäten an, die während eines bestimmten Zeitraums durchgeführt wurden. |
| Aktive Alarmmeldungen – Übersicht | In allen Editionen verfügbar | Zeigt eine Übersicht der aktiven Alarmmeldungen nach Alarmtyp und Schweregrad an. |
| Status der Patch-Installation | Nicht verfügbar in den Cyber Backup-Editionen | Zeigt die Anzahl der Maschinen gruppiert nach dem Status des Patch-Installation an. |
| Fehlende Updates nach | Nicht verfügbar | Zeigt die Anzahl der fehlenden Updates nach Kategorie |

| | | |
|---|---|---|
| Kategorie | in den Cyber Backup-Editionen | an. |
| Laufwerksintegritätsstatus | Nicht verfügbar in den Cyber Backup-Editionen | Zeigt die Anzahl der Laufwerke nach ihrem Status an. |
| Geräte | In allen Editionen verfügbar | Zeigt ausführliche Informationen über die Geräte in Ihrer Umgebung an. |
| Details 'Aktive Alarmmeldungen' | In allen Editionen verfügbar | Zeigt ausführliche Informationen über die aktiven Alarmmeldungen an. |
| Vorhandene Schwachstellen | In allen Editionen verfügbar | Zeigt die vorhandenen Schwachstellen für die Betriebssysteme und Applikationen in Ihrer Umgebung sowie die betroffenen Maschinen an. |
| Verlauf der Patch-Installation | Nicht verfügbar in den Cyber Backup-Editionen | Zeigt ausführliche Informationen über die installierten Patches an. |
| Kürzlich betroffen | In allen Editionen verfügbar | Zeigt ausführliche Informationen über die kürzlich infizierten Maschinen an. |
| Speicherorte-Übersicht | In allen Editionen verfügbar | Zeigt ausführliche Informationen über die Backup-Speicherorte an. |

***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 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 entfernen***

Klicken Sie neben dem Widget-Namen auf das X-Symbol.

## Cyber Protection

Dieses Widget zeigt allgemeine Informationen über blockierte Malware, blockierte URLs, gefundene Schwachstellen, installierte Patches und die Größe von Backups an.

Die obere Zeile zeigt die aktuellen Statistiken an:

- **Heute gesichert** – die summierte Größe aller Recovery-Punkte für die letzten 24 Stunden
- **Malware blockiert** – die Anzahl der derzeit aktiven Alarmmeldungen über blockierte Malware
- **URLs blockiert** – die Anzahl der derzeit aktiven Alarmmeldungen über blockierte URLs
- **Vorhandene Schwachstellen** – die Anzahl der derzeit vorhandenen Schwachstellen
- **Patches bereit zur Installation** – die Anzahl der derzeit verfügbaren Patches, die installiert werden sollen

Die untere Zeile zeigt die Gesamtstatistiken an:

- Die komprimierte Größe aller Backups
- Die akkumulierte Anzahl der blockierten Malware auf allen Maschinen
- Die akkumulierte Anzahl der blockierten URLs auf allen Maschinen
- Die akkumulierte Anzahl der erkannten Schwachstellen auf allen Maschinen
- Die akkumulierte Anzahl der installierten Updates/Patches auf allen Maschinen

## Schutzstatus

### 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.

# Überwachung der Laufwerksintegrität

Die Überwachung der Laufwerksintegrität liefert Informationen über den aktuellen Laufwerksintegritätsstatus sowie eine Vorhersage über diesen. Dadurch können Sie Datenverluste vorab verhindern, die durch einen Laufwerksausfall verursacht werden könnten. Es werden sowohl Laufwerke vom Typ HDD (klassische Festplatten) als auch SSD (Flash-Speicher basierte Laufwerke) unterstützt.

## Beschränkungen:

- Die Vorhersage zur Laufwerksintegrität wird nur für Maschinen unterstützt, die unter Windows laufen.
- Es können nur Laufwerke von physischen Maschinen überwacht werden. Die Laufwerke von virtuellen Maschinen können nicht überwacht werden und werden daher auch nicht in den Laufwerksintegrität-Widgets angezeigt.
- RAID-Konfigurationen werden nicht unterstützt.
- Bei NVMe-Laufwerken wird die Überwachung der Laufwerksintegrität nur für solche Laufwerke unterstützt, die ihre SMART-Daten über die Windows-API kommunizieren. Bei NVMe-Laufwerken, bei denen die SMART-Daten direkt aus dem Laufwerk ausgelesen werden müssen, wird die Überwachung der Laufwerksintegrität nicht unterstützt.

Die Laufwerksintegrität wird durch folgende Statuszustände dargestellt:

- **OK**
  Die Laufwerksintegrität liegt zwischen 70% und 100%.
- **Warnung**
  Die Laufwerksintegrität liegt zwischen 30% und 70%.
- **Kritisch**
  Die Laufwerksintegrität liegt zwischen 0% und 30%.
- **Laufwerksdaten werden berechnet**
  Der aktuelle Laufwerksstatus und die Vorhersage werden ermittelt

## Und so funktioniert es

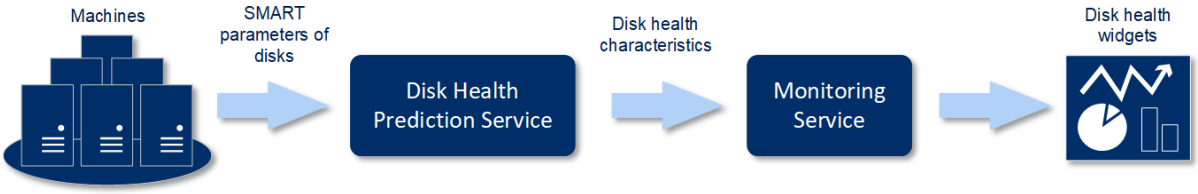
Der Disk Health Prediction Service verwendet ein auf künstlicher Intelligenz (KI) basierendes Vorhersagemodell.

1. Der Protection Agent sammelt die SMART-Parameter der Laufwerke und übermittelt diese Daten an den Disk Health Prediction Service:

- SMART 5 – Wiederzugewiesene Sektoren (Reallocated Sectors Count).
- 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 – Aktuell ausstehende Sektoren (Current Pending Sector Count)
- SMART 198 – Nicht korrigierbare Sektoren (Offline Uncorrectable Sector Count).
- 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 Laufwerksintegritätsstatus: 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 empfängt diese Merkmale und zeigt die entsprechenden Informationen dann in den Laufwerksintegrität-Widgets der Cyber Protect Webkonsole an.




## Laufwerksintegrität-Widgets

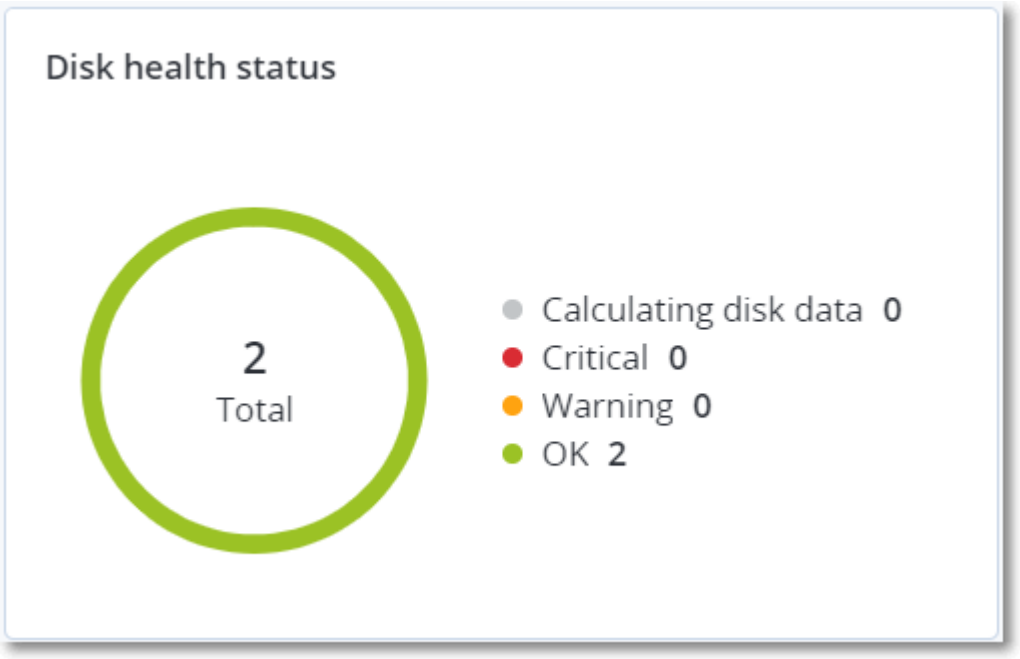
Die Ergebnisse der Laufwerksintegritätsüberwachung werden in folgenden Widgets dargestellt, die in der Cyber Protect Webkonsole verfügbar sind.

- **Überblick der Laufwerksintegrität** ist ein Treemap-Widget (Kacheldiagramm mit Baumstruktur) mit zwei Detailebenen, zwischen denen umgeschaltet werden kann.
  - Maschinenebene
    Zeigt zusammengefasste Informationen über den Laufwerkstatus aller Maschinen in der ausgewählten Organisationseinheit (Abteilung) an. Es werden nur die kritischsten Laufwerkstatuszustände angezeigt. Die anderen Statuszustände werden in einem Tooltip angezeigt, wenn Sie mit dem Mauszeiger über einen bestimmten Block fahren. Die Blockgröße der Maschine hängt von der Gesamtgröße aller Laufwerke dieser Maschine ab. Die Blockfarbe der Maschine hängt vom kritischsten Laufwerksstatus ab, der gefunden wurde.


- Laufwerksebene
  Zeigt den aktuellen Laufwerksintegritätsstatus aller Laufwerke für die ausgewählte Maschine an. Jeder Laufwerksblock zeigt eine der nachfolgenden Vorhersagen zur Laufwerksintegrität sowie die dazugehörige Wahrscheinlichkeit (in Prozent) an:
  - Wird heruntergestuft
  - Wird stabil bleiben

- Wird verbessert


- **Laufwerksintegritätsstatus** ist ein Kreisdiagramm-Widget, welches die Anzahl der Laufwerke für jeden Status anzeigt.



## Alarmmeldungen zum Laufwerksintegritätsstatus

Die Laufwerksintegritätsprüfung wird alle 30 Minuten durchgeführt, während die entsprechende Alarmmeldung nur einmal täglich generiert wird. Wenn sich der Laufwerksintegritätsstatus von **Warnung** zu **Kritisch** ändert, wird immer ein Alarm generiert.

| Alarmbezeichnung | Schweregrad | Laufwerksintegritätsstatus | Beschreibung |
|---|---|---|---|
| Laufwerksausfall ist möglich | Warnung | (30 – 70) | Das Laufwerk <Laufwerksname> auf dieser Maschine wird wahrscheinlich demnächst ausfallen. Sichern Sie das Laufwerk möglichst bald mit einem vollständigen Image-Backup. Bauen Sie dann ein Ersatzlaufwerk ein und stellen Sie das Image auf diesem wieder her. |
| Laufwerksausfall steht unmittelbar bevor | Kritisch | (0 – 30) | Das Laufwerk <Laufwerksname> auf dieser Maschine befindet sich in einem kritischen Zustand und wird höchstwahrscheinlich sehr bald ausfallen. 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. |

## 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 Sicherungsstatus aller wichtigen Dateien in Form einer skalierbaren Treemap-Anzeige (Kacheldiagramm mit Baumstruktur) zu erhalten.

Jede Blockgröße hängt von der Gesamtzahl/Größe aller wichtigen Dateien ab, die zu einer Organisationseinheit/Maschine gehören.

Dateien können einen der folgenden Schutzstatus-Zustände haben:

- **Kritisch** – es gibt 1-20% ungeschützte Dateien mit den von Ihnen spezifizierten Erweiterungen, die für die/den ausgewählte(n) Maschine/Speicherort nicht per Backup gesichert wurden und mit den vorhandenen Backup-Einstellungen nicht gesichert werden.
- **Niedrig** – es gibt 21-50% ungeschützte Dateien mit den von Ihnen spezifizierten Erweiterungen, die für die/den ausgewählte(n) Maschine/Speicherort nicht per Backup gesichert wurden und mit den vorhandenen Backup-Einstellungen nicht gesichert werden.
- **Mittel** – es gibt 1-20% ungeschützte Dateien mit den von Ihnen spezifizierten Erweiterungen, die für die/den ausgewählte(n) Maschine/Speicherort nicht per Backup gesichert wurden und mit den vorhandenen Backup-Einstellungen nicht gesichert werden.
- **Hoch** – alle Dateien mit den von Ihnen spezifizierten Erweiterungen wurden für die/den ausgewählte(n) Maschine/Speicherort per Backup gesichert.

Alle Ergebnisse der Data Protection-Untersuchtung können auf dem Dashboard im Data Protection-Karten-Widget gefunden werden – einem Treemap-Widget, welches die Details auf Maschinenebene anzeigt.

Fahren Sie mit der Maus über den farbigen Block, um weitere Informationen über die Anzahl der ungeschützten Dateien und deren Speicherort zu erhalten. Wenn Sie diese sichern wollen, klicken Sie auf **Alle Dateien schützen**.

# Widget für Schwachstellenbewertung

## Verwundbare Maschinen

Dieses Widget zeigt die verwundbaren Maschinen nach dem Verwundbarkeitsgrad an.

Die gefundene Schwachstelle kann gemäß CVSS v3.0 (Common Vulnerability Scoring System) einen der folgenden Schweregrade haben:

- Gesichert: es wurden keine Schwachstellen gefunden
- Kritisch: 9.0 - 10.0 CVSS
- Hoch: 7.0 - 8.9 CVSS
- Mittel: 4.0 - 6.9 CVSS

- Niedrig: 0.1 - 3.9 CVSS
- Ohne: 0.0 CVSS

### Vorhandene Schwachstellen

Dieses Widget zeigt die derzeit vorhandenen Schwachstellen auf Maschinen an. Im Widget **Vorhandene Schwachstellen** gibt es zwei Spalten mit Zeitstempeln:

- **Zuerst erkannt** – Datum und Uhrzeit, als die Schwachstelle erstmals auf der Maschine erkannt wurde.
- **Zuletzt erkannt** – Datum und Uhrzeit, als die Schwachstelle das letzte Mal auf der Maschine erkannt wurde.

## Widgets für Patch-Installation

Es gibt vier Widgets im Zusammenhang mit der Patch-Verwaltungsfunktionalität.

### Status der Patch-Installation

Dieses Widget zeigt die Anzahl der Maschinen gruppiert nach dem Status des Patch-Installation an.

- **Installiert** – alle verfügbaren Patches sind auf einer Maschine installiert
- **Neustart erforderlich** – nach einer Patch-Installation muss eine Maschine neu gestartet werden
- **Fehlgeschlagen** – die Patch-Installation ist auf einer Maschine fehlgeschlagen

### Übersicht der Patch-Installation

Dieses Widget zeigt eine Übersicht der Patches an, gruppiert nach Installationsstatus.

### Verlauf der Patch-Installation

Dieses Widget zeigt ausführliche Informationen über die Patches an, die auf den Maschinen installiert wurden.

### Fehlende Updates nach Kategorie

Dieses Widget zeigt die Anzahl der fehlenden Updates nach Kategorie an. Folgende Kategorien werden angezeigt:

- Sicherheitsupdates
- Kritische Updates
- Andere

## Backup-Scanning-Details

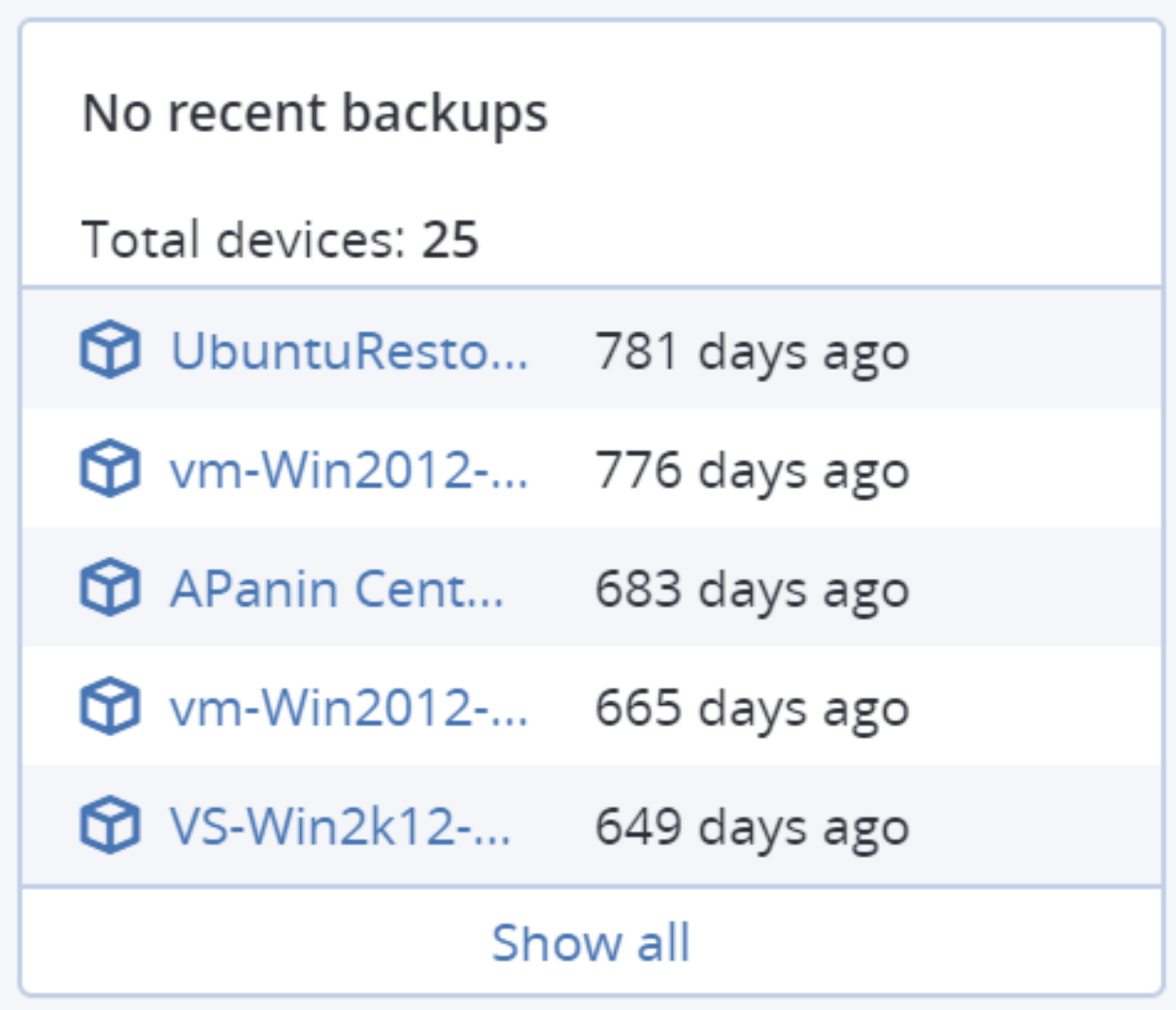
Dieses Widget ist nur dann verfügbar, wenn der Scan Service auf dem Management Server installiert wurde. Das Widget zeigt ausführliche Informationen über die Bedrohungen an, die in den Backups erkannt wurden.

## Kürzlich betroffen

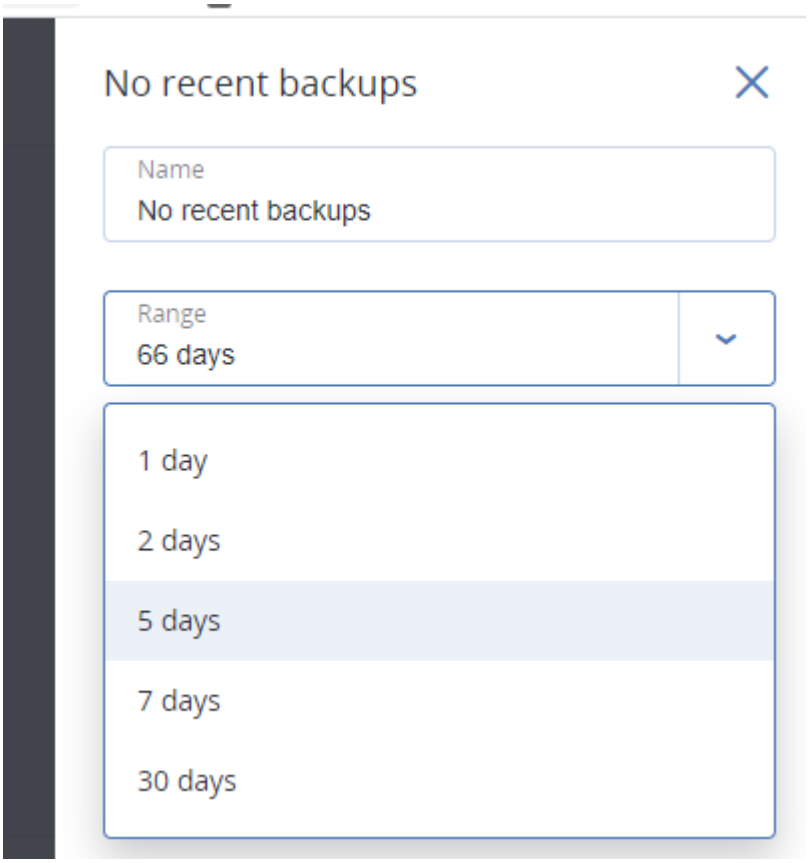
Dieses Widget zeigt ausführliche Informationen über kürzlich infizierte Maschinen an. Sie können hier Informationen darüber finden, welche Bedrohung erkannt wurde und wie viele Dateien infiziert wurden.

## Keine neueren Backups

Dieses Widget zeigt Workloads mit angewendeten Schutzplänen an, deren letztes erfolgreiches Backup-Datum vor dem Zeitraum lag, der in den Widget-Einstellungen spezifiziert wurde.



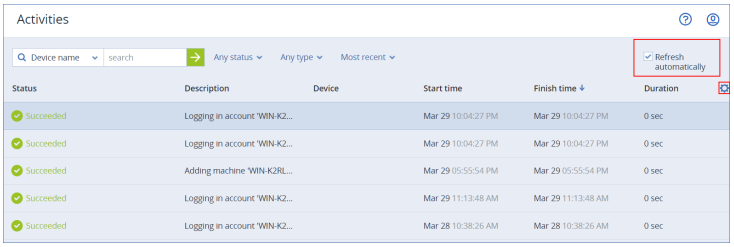
Wenn Sie dieses Widget hinzufügen, zeigt es standardmäßig die entsprechenden Informationen für die letzten 5 Tage an. Sie können über das Listenfeld einen anderen Zeitraum auswählen oder eine Anzahl von Tagen manuell eingeben. Die maximale Anzahl der Tage, die Sie eingeben können, beträgt 180.




# Die Registerkarte 'Aktivitäten'

Die Registerkarte **Aktivitäten** bietet einen Überblick über die Aktivitäten der letzten 90 Tage.

Wenn Sie die Darstellung der Registerkarte **Aktivitäten** anpassen wollen, können Sie auf das Zahnradsymbol klicken und die Spalten auswählen, die angezeigt werden sollen. Wenn Sie den Aktivitätsfortschritt in Echtzeit sehen wollen, aktivieren Sie das Kontrollkästchen **Automatisch aktualisieren**. Beachten Sie, dass häufige Aktualisierungen vieler Aktivitäten die Performance des Management Servers beeinträchtigen können.




Sie können die aufgelisteten Aktivitäten nach den folgenden Kriterien durchsuchen:

- **Gerätename**
  Dies ist die Maschine, auf welcher die Aktivität durchgeführt wird.
- **Gestartet von**
  Dies ist das Konto, welches die Aktivität gestartet hat.

Sie können die Aktivitäten auch nach folgenden Eigenschaften filtern:

- **Status**
  Zum Beispiel: erfolgreich, fehlgeschlagen, wird ausgeführt oder abgebrochen.
- **Typ**
  Zum Beispiel: Plan wird angewendet, Backups werden gelöscht, Software-Updates werden installiert.
- **Zeit**
  Zum Beispiel: die jüngsten Aktivitäten, die Aktivitäten der letzten 24 Stunden oder die Aktivitäten während eines bestimmten Zeitraums innerhalb der vorgegebenen Aufbewahrungsdauer.

Bearbeiten Sie die Konfigurationsdatei task_manager.yaml, wenn Sie die standardmäßige Aufbewahrungsdauer ändern wollen.

***So können Sie die Aufbewahrungsdauer ändern***

1. Öffnen Sie auf dier Maschine, die den Management Server ausführt, die nachfolgende Konfigurationsdatei in einem Text-Editor:
   - Unter Windows: `%Program Files%\Acronis\TaskManager\task_manager.yaml`
   - Unter Linux: `/usr/lib/Acronis/TaskManager/task_manager.yaml`
2. Suchen Sie den folgenden Abschnitt:

```
database:
  connection-string: ""
  run-cleanup-at: "23:59"
  cleanup-batch-size: 10
  max-cleanup-retries: 10
  log-queries: false
  max-transaction-retries: 10
  shards:
   - connection-string: sqlite://task-manager.sqlite
     days-to-keep: 90
     space: "default"
     key: "00000000-0000-0000-0000-000000000000"
```

3. Sie können die Zeile `days-to-keep` an Ihre Anforderungen anpassen:
   Zum Beispiel:

```
days-to-keep: 30
```

**Hinweis**
Sie können die Aufbewahrungsdauer an Ihre Anforderungen anpassen. Eine Erhöhung der Aufbewahrungsdauer verschlechtert die Performance des Management Servers.

4. Starten Sie den **Acronis Service Manager Service** neu (wie im Abschnitt '"So können Sie den Acronis Service Manager Service neu starten" (S. 209)' beschrieben).

# Berichte

Sie können Berichte außerdem vordefinieren oder einen benutzerdefinierten Bericht erstellen. Ein Bericht kann einen beliebigen Satz von Dashboard-Widgets enthalten.

Sie können Berichte nur für die Abteilungen konfigurieren, die Sie verwalten.

Die Berichte können per E-Mail gesendet oder nach einer Planung heruntergeladen werden. Bevor Sie die Berichte per E-Mail versenden, sollten Sie überprüfen, dass die **E-Mail-Server**-Einstellungen konfiguriert wurden. Wenn Sie einen Bericht mit Drittanbieter-Programmen verarbeiten wollen, sollten Sie in die Planung aufnehmen, dass der Bericht im .xlsx-Format in einem bestimmten Ordner gespeichert wird.

Die verfügbaren Berichte hängen davon ab, welche Edition von Cyber Protect Sie haben. Die Standardberichte sind nachfolgend aufgelistet:

| Berichtsname | Verfügbarkeit | Beschreibung |
|---|---|---|
| Alarmmeldungen | Cyber Backup Advanced<br>Cyber Protect Advanced | Zeigt Alarmmeldungen an, die während eines bestimmten Zeitraums aufgetreten sind. |
| Backup-Scanning-Details | Cyber Protect Advanced | Zeigt ausführliche Informationen über erkannte Bedrohungen in den Backups an. |
| Backups | Cyber Backup Advanced<br>Cyber Protect Advanced | Zeigt Details über aktuelle Backups und Recovery-Punkten an. |
| Aktueller Status | Cyber Backup Advanced<br>Cyber Protect Advanced | Zeigt den aktuellen Status Ihrer Umgebung an. |
| Tägliche Aktivitäten | Cyber Backup Advanced | Zeigt eine Übersicht über diejenigen Aktivitäten an, die während eines bestimmten Zeitraums durchgeführt wurden. |

| | | |
|---|---|---|
| | Cyber Protect Advanced | |
| Data Protection-Karte | Cyber Protect Advanced | Zeigt ausführliche Informationen über Anzahl, Größe, Speicherort und Sicherungsstatus aller wichtigen Dateien auf den Maschinen an. |
| Erkannte Bedrohungen | Cyber Backup Advanced<br>Cyber Protect Advanced | Zeigt Details über die betroffenen Maschinen anhand der Anzahl der blockierten Bedrohungen sowie anhand von Informationen über die fehlerfreien und verwundbaren Maschinen an. |
| Erkannte Maschinen | Cyber Backup Advanced<br>Cyber Protect Advanced | Zeigt alle Maschinen an, die im Organisationsnetzwerk erkannt wurden. |
| Vorhersage der Laufwerksintegrität | Cyber Protect Advanced | Zeigt den aktuellen Laufwerksstatus an sowie eine Prognose darüber, wann Ihre HDD/SSD vermutlich ausfallen wird. |
| Vorhandene Schwachstellen | Cyber Backup Advanced<br>Cyber Protect Advanced | Zeigt die vorhandenen Schwachstellen für die Betriebssysteme und Applikationen in Ihrer Umgebung sowie die betroffenen Maschinen an. |
| Lizenzen | Cyber Backup Advanced<br>Cyber Protect Advanced | Zeigt eine Übersicht zu den verfügbaren Lizenzen an. |
| Speicherorte | Cyber Backup Advanced<br>Cyber Protect Advanced | Zeigt Nutzungsstatistiken für die Backup-Speicherorten an (für einen bestimmten Zeitraum). |
| Übersicht zur Patch-Verwaltung | Cyber Protect Advanced | Zeigt die Anzahl der fehlenden, installierten und anwendbaren Patches an. Sie können sich Detailinformationen zu dem Bericht anzeigen lassen, um Informationen und Details zu den fehlenden/installierten Patches für alle Systeme zu erhalten. |
| Übersicht | Cyber Backup Advanced<br>Cyber Protect Advanced | Zeigt eine Übersicht zu den geschützten Geräten an (für einen bestimmten Zeitraum). |

| | | |
|---|---|---|
| Band-Aktivitäten | Cyber Backup Advanced<br>Cyber Protect Advanced | Zeigt eine Liste von Bändern an, die während der letzten 24 Stunden verwendet wurden. |
| Wöchentliche Aktivitäten | Cyber Backup Advanced<br>Cyber Protect Advanced | Zeigt eine Übersicht über diejenigen Aktivitäten an, die während eines bestimmten Zeitraums durchgeführt wurden. |

## Basis-Aktionen mit Berichten

- Wenn Sie einen Bericht einsehen wollen, klicken Sie auf dessen Namen.
- Wenn Sie weitere Aktionen mit einem Bericht durchführen wollen, klicken Sie auf das Drei-Punkte-Symbol (...).

  Dieselben Aktionen sind aus dem Bericht heraus verfügbar.

***So können Sie eine 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.
   - Klicken Sie auf **Benutzerdefiniert**, um einen angepassten Bericht hinzuzufügen. Es wird ein neuer Bericht mit der Bezeichnung **Benutzerdefiniert** in die Liste der Berichte aufgenommen. Öffnen Sie diesen Bericht und fügen Sie Widgets hinzu.
3. [Optional] Ordnen Sie die Widgets per Drag & Drop nach Ihren Vorstellungen neu an.
4. [Optional] Bearbeiten Sie den Bericht wie nachfolgend beschrieben.

***So können Sie eine Bericht bearbeiten***

1. Klicken Sie neben dem Namen des Berichts auf das Drei-Punkte-Symbol (...) und anschließend auf **Einstellungen**.
2. Bearbeiten Sie den Bericht. Sie können:
   - 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
3. Klicken Sie auf **Speichern**.

***So können Sie eine Bericht planen***

1. Wählen Sie einen Bericht aus und klicken Sie dann auf **Planung**.
2. Aktivieren Sie den Schalter **Einen geplanten Bericht senden**.

3. Bestimmen Sie, ob der Bericht per E-Mail versendet werden soll, in einem Ordner gespeichert werden soll – oder beides. Spezifizieren Sie – abhängig von Ihrer Entscheidung – die E-Mail-Adressen, den Ordnerpfad oder beides.
4. Bestimmen Sie das Format für den Bericht: .pdf, .xlsx oder beides.
5. Bestimmen Sie den Berichtszeitraum: 1 Tag, 7 Tage oder 30 Tage.
6. Bestimmen Sie die Tage und den Zeitpunkt, an dem der Bericht gesendet oder gespeichert werden soll.
7. Klicken Sie auf **Speichern**.

### Die Berichtsstruktur exportieren und importieren

Sie können die Berichtsstruktur (die Zusammenstellung der Widgets und die Planungseinstellungen) als .json-Datei exportieren oder importieren. Dies kann nützlich sein, wenn Sie den Management Server neu installieren müssen oder die Berichtsstruktur zu einem anderen Management Server kopieren wollen.

Um die Berichtstruktur exportieren zu können, müssen Sie den Bericht zuerst auswählen und dann auf **Exportieren** klicken.

Wenn Sie die Berichtsstruktur importieren wollen, müssen Sie zuerst auf **Bericht erstellen** klicken und anschließend auf **Importieren**.

### Die Berichtsdaten sichern

Sie können eine Abbild (Dump) der Berichtsdaten als .csv-Datei speichern. Die Abbildsicherung enthält alle Berichtsdaten (ungefiltert) für einen bestimmten Zeitraum.

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. Wählen Sie einen Bericht aus und klicken Sie dann auf **Öffnen**.
2. Klicken Sie in der rechten oberen Ecke auf das Drei-Punkte-Symbol (...) und anschließend auf **Sicherungsdaten**.
3. Spezifizieren Sie bei **Speicherort** den Pfad zu dem Ordner, wo die .csv-Datei gespeichert werden soll.
4. Spezifizieren Sie bei **Zeitraum** den gewünschten Zeitrahmen.
5. Klicken Sie auf **Speichern**.

## Den Schweregrad von Alarmmeldungen konfigurieren

Ein Alarm ist eine Nachricht, die vor gegenwärtigen oder potentiellen Problemen warnt. Sie können Alarmmeldungen auf vielfältige Weise verwenden:

- Im Bereich **Alarmmeldungen** der Registerkarte **Überblick** können Sie Probleme schnell erkennen und lösen, indem Sie die aktuellen Alarmmeldungen überwachen.
- Bei **Geräte** wird der jeweilige Gerätestatus aus den Alarmmeldungen abgeleitet. Über die Spalte **Status** können Sie Geräte mit Problemen herausfiltern.
- Bei der Konfiguration von E-Mail-Benachrichtigungen können Sie bestimmen, welche Alarmmeldungen eine Benachrichtigung auslösen sollen.

Ein Alarm kann einen der folgenden Schweregrade haben:

- **Kritisch**
- **Fehler**
- **Warnung**

Sie können den Schweregrad eines Alarms ändern oder einen Alarm über die unten beschriebene Alarmkonfigurationsdatei komplett deaktivieren. Diese Aktion erfordert einen Neustart des Management Servers.

Eine Änderung des Schweregrads für einen Alarm hat keinen Effekt auf Alarmmeldungen, die bereits generiert wurden.

## Alarmkonfigurationsdatei

Die Konfigurationsdatei befindet sich auf der Maschine, auf welcher der Management Server ausgeführt wird.

- Unter Windows: `<Installationspfad>`**\AlertManager\alert_manager.yaml**
  Wobei `<Installationspfad>` für den Installationspfad des Management Servers steht. Standardmäßig ist dies der Ordner '**%ProgramFiles%\Acronis**'.
- Unter Linux: **/usr/lib/Acronis/AlertManager/alert_manager.yaml**

Die Datei ist als YAML-Dokument strukturiert. Jeder Alarm ist ein Element in der Liste `alertTypes`.

Der Schlüssel `name` identifiziert die Alarmmeldung.

Der Schlüssel `severity` bestimmt den Schweregrad des Alarms. Es darf einer der folgenden Werte vergeben sein: `critical`, `error` oder `warning`.

Der optionale Schlüssel `enabled` bestimmt, ob der Alarm aktiviert oder deaktiviert ist. Zulässige Werte sind entweder `true` oder `false`. Standardmäßig (ohne diesen Schlüssel) sind alle Alarmmeldungen aktiviert.

***So können Sie einen Alarm deaktivieren oder seinen Schweregrad ändern***

1. Öffnen Sie auf der Maschine, auf welcher der Management Server installiert ist, die Datei **alert_manager.yaml** in einem Texteditor.
2. Suchen Sie den Alarm, den Sie ändern oder deaktivieren möchten.
3. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:

- Wenn Sie den Schweregrad eines Alarms ändern wollen, ändern Sie den Wert des Schlüssels `severity`.
- Wenn Sie den Alarm deaktivieren wollen, fügen Sie den Schlüssel `enabled` hinzu und legen Sie dessen Wert dann mit `false` fest.

4. Speichern Sie die Datei.
5. Starten Sie wie nachfolgend beschrieben den Management Server-Dienst neu.

***So können Sie den Management Server-Dienst unter Windows neu starten***

1. Klicken Sie im **Start**-Menü auf **Ausführen** und geben Sie ein: **cmd**
2. Klicken Sie auf **OK**.
3. Führen Sie folgende Befehle aus:

```
net stop acrmngsrv
net start acrmngsrv
```

***So können Sie den Management Server-Dienst unter Linux neu starten***

1. Öffnen Sie die Applikation **Terminal**.
2. Führen Sie folgenden Befehl (in einem beliebigen Verzeichnis) aus:

```
sudo service acronis_ams restart
```

# Erweiterte Storage-Optionen

## Bandgeräte

Die folgenden Abschnitte erläutern ausführlich, wie Bandgeräte zur Speicherung von Backups verwendet werden.

### Was ist ein Bandgerät?

Ein **Bandgerät** ist ein Oberbegriff für eine Bandbibliothek oder ein autonomes Bandlaufwerk.

Eine **Bandbibliothek** (Roboterbibliothek) ist eine Speichereinrichtung mit hoher Kapazität, die aus den folgenden Komponenten besteht:

- einem oder mehreren Bandlaufwerken
- mehreren (bis zu mehreren Tausend) Schächten zur Aufnahme von Bändern
- einem oder mehreren Wechslern (Robotermechanismen), deren Aufgabe im Wechseln der Bänder zwischen den Schächten und den Bandlaufwerken besteht.

Es können noch weitere Komponenten enthalten sein, etwa ein Barcode-Leser oder Barcode-Drucker.

Ein **Autoloader** ist ein spezieller Fall einer Bandbibliothek. Er enthält ein Laufwerk, mehrere Schächte, einen Wechsler und (optional) einen Barcode-Leser.

Ein **autonomes Bandlaufwerk** (auch **Streamer** genannt) hat einen Schacht und kann jeweils nur ein Band aufnehmen.

### Überblick der Band-Unterstützung

Die Protection Agenten können Daten entweder direkt oder über einen Storage Node zu einem Bandgerät sichern. In beiden Fällen ist eine vollautomatische Steuerung des Bandgerätes gewährleistet. Wenn ein Bandgerät mit mehreren Laufwerken an einen Storage Node angeschlossen wird, können mehrere Agenten gleichzeitig Backups auf Bänder erstellen.

#### Kompatibilität mit RSM und Drittthersteller-Software

##### Koexistenz mit Drittthersteller-Software

Auf einer Maschinen, auf der eine Drittanbieter-Software mit proprietären Tools zur Bandverwaltung installiert ist, kann nicht mit Bändern gearbeitet werden. Um auf einer solchen Maschine Bändern nutzen zu können, müssen Sie die Bandverwaltungssoftware des Drittherstellers daher deinstallieren oder deaktivieren.

### Interaktion mit dem Windows Removable Storage Manager (RSM)

Der RSM wird weder von den Protection Agenten noch Storage Nodes verwendet. Wenn sie ein Bandgerät erkennen, deaktivieren sie das Gerät vom RSM (außer es wird gerade von einer anderen Software verwendet). Solange Sie mit dem Bandgerät arbeiten wollen, sollten Sie sicherstellen, dass weder ein Benutzer noch eine Drittanbieter-Software das Gerät wieder für den RSM aktiviert. Sollte das Bandgerät für den RSM aktiviert worden sein, dann wiederholen Sie die Bandgeräterkennung.

## Unterstützte Hardware

Acronis Cyber Protect unterstützt externe SCSI-Geräte. Das sind Geräte, die per Fibre Channel angebunden sind oder SCSI, iSCSI bzw. Serial Attached SCSI (SAS) als Schnittstelle verwenden. Acronis Cyber Protect unterstützt außerdem per USB angeschlossene Bandgeräte.

Unter Windows kann Acronis Cyber Protect Backups auch dann auf ein Bandgerät erstellen, wenn die Treiber für den Wandler des Gerätes nicht installiert sind. Ein solches Bandgerät wird im **Geräte-Manager** als **Unbekannter Medienwechsler** angezeigt. Treiber für die Laufwerke des Gerätes müssen jedoch installiert sein. Unter Linux und bootfähigen Medien sind Backups auf ein Bandgerät ohne Treiber nicht möglich.

Eine Erkennung von per IDE oder SATA angebunden Geräten wird nicht garantiert. Sie hängt davon ab, ob im Betriebssystem die korrekten Treiber installiert wurden.

Um zu ermitteln, ob Ihr jeweiliges Gerät unterstützt wird, können Sie das Hardware-Kompatibilitätstool verwenden. Eine entsprechende Beschreibung finden Sie unter http://kb.acronis.com/content/57237. Sie können einen Bericht über die Testergebnisse auch gerne an Acronis senden. Hardware mit bestätigter Unterstützung finden Sie in der Hardware-Kompatibilitätsliste aufgeführt: https://go.acronis.com/acronis-cyber-protect-advanced-tape-hcl.

## Bandverwaltungsdatenbank

Die Informationen über alle Bandgeräte, die eine Maschine angeschlossen sind, werden in der Bandverwaltungsdatenbank gespeichert. Der Standardpfad für die Datenbank lautet folgendermaßen:

- In Windows XP/Server 2003: `%ALLUSERSPROFILE%\Application Data\Acronis\BackupAndRecovery\ARSM\Database`.
- In Windows 7 und höheren Versionen von Windows: `%PROGRAMDATA%\Acronis\BackupAndRecovery\ARSM\Database`.
- Unter Linux: `/var/lib/Acronis/BackupAndRecovery/ARSM/Database`.

Die Datenbankgröße hängt von der Zahl der auf den Bändern gespeicherten Backups ab – wobei etwa 10 MB auf einhundert Backups kommen. Die Datenbank kann recht groß werden, wenn die Bandbibliothek tausende Backups enthält. In diesem Fall könnten Sie erwägen, die Band-Datenbank auf einem anderen Volume zu speichern.

***So verlagern Sie die Datenbank unter Windows:***

1. Stoppen Sie den Removable Storage Management Service.
2. Verschieben Sie alle Dateien vom vorgegebenen Speicherort zum neuen Speicherort.
3. Suchen Sie folgenden Registry-Schlüssel: `HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\ARSM\Settings`.
4. Spezifizieren Sie den Pfad zum neuen Speicherort im Registry-Wert `ArsmDmlDbProtocol`. Der String darf bis zu 32765 Zeichen enthalten.
5. Starten Sie den Removable Storage Management Service.

***So verlagern Sie die Datenbank unter Linux:***

1. Stoppen Sie den Dienst `acronis_rsm`.
2. Verschieben Sie alle Dateien vom vorgegebenen Speicherort zum neuen Speicherort.
3. Öffnen Sie die Konfigurationsdatei `/etc/Acronis/ARSM.config` in einem Text-Editor.
4. Suchen Sie nach der Zeile `<value name="ArsmDmlDbProtocol" type="TString">`.
5. Ändern Sie den Pfad unter dieser Ziele.
6. Speichern Sie die Datei.
7. Starten Sie den Dienst `acronis_rsm`.

### Der Ordner `TapeLocation`

Der Ordner `TapeLocation` enthält einen Cache der Dateisystem-Metadaten von allen Volumes, die auf Bändern gesichert wurden.

Der Standardpfad des Ordners `TapeLocation` lautet:

- In Windows XP/Server 2003: `%ALLUSERSPROFILE%\Application Data\Acronis\BackupAndRecovery\TapeLocation`
- Unter Windows 7 (und höher): `%PROGRAMDATA%\Acronis\BackupAndRecovery\TapeLocation`
- Unter Linux: `/var/lib/Acronis/BackupAndRecovery/TapeLocation`

Die Größe des Ordners `TapeLocation` entspricht ca. 0,5-1% der Größe aller Backups, die auf Bändern gespeichert wurden. Bei Backups auf Laufwerksebene, für die die Option zur Dateiwiederherstellung aktiviert wurde, kann die Größe des Ordners `TapeLocation` auch etwas größer sein (abhängig von der genauen Anzahl der gesicherten Dateien).

## Parameter zum Schreiben auf Bänder

Mit den Parametern zum Schreiben auf Bändern (Block- und Cache-Größe) können Sie die Software zur Erreichung einer maximalen Performance konfigurieren. Zum Schreiben auf Bänder sind eigentlich beide Parameter erforderlich, normalerweise muss aber nur die Blockgröße angepasst werden. Der optimale Wert hängt von der Art des Bandgerätes und den zu sichernden Daten ab – beispielsweise deren Anzahl und Größe.

**Hinweis**
Beim Lesen von Bändern verwendet die Software dieselbe Blockgröße, die auch beim Schreiben auf das Band verwendet wurde. Sollte das Bandgerät diese Blockgröße nicht unterstützen, schlägt der Lesevorgang fehl.

Die Parameter werden auf jeder Maschine festgelegt, an der ein Bandgerät angeschlossen ist. Es kann sich um eine Maschine handeln, auf der ein Agent oder ein Storage Node installiert ist. Auf einer unter Windows laufenden Maschine erfolgt die Konfiguration in der Registry. Auf einer unter Linux laufenden Maschine wird die Konfigurationsdatei **/etc/Acronis/BackupAndRecovery.config** verwendet.

In Windows müssen Sie die entsprechenden Registry-Schlüssel und deren DWORD-Werte erstellen. In Linux müssen Sie folgenden Text an das Ende der Konfigurationsdatei einfügen, direkt vor dem Tag `</registry>`:

```
<key name="TapeLocation">
     <value name="WriteCacheSize" type="Dword">
          "value"
     </value>
     <value name=DefaultBlockSize" type="Dword">
          "value"
     </value>
</key>
```

### DefaultBlockSize

Dies ist die Blockgröße (in Byte), die beim Schreiben auf die Bänder verwendet wird.

*Mögliche Werte:* 0, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 16384, 32768, 65536, 131072, 262144, 524288, 1048576.

Falls der Wert 0 beträgt oder der Parameter fehlt, wird die Blockgröße folgendermaßen bestimmt:

- In Windows wird der Wert vom Treiber des Bandgerätes abgerufen.
- In Linux wird **64 KB** als Wert verwendet.

*Registry-Schlüssel (auf einer unter Windows laufenden Maschine):* **HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\BackupAndRecovery\TapeLocation\DefaultBlockSize**

*Die Befehlszeile in '/etc/Acronis/BackupAndRecovery.config' (auf einer unter Linux laufenden Maschine):*

```
     <value name=DefaultBlockSize" type="Dword">
          "value"
     </value>
```

Falls das Bandlaufwerk den spezifizierten Wert nicht akzeptiert, teilt die Software den Wert durch 2, bis ein passender Wert oder bis 32 Byte als Wert erreicht ist. Sollte dabei kein passender Wert gefunden werden, multipliziert die Software den spezifizierten Wert mit 2, bis ein passender Wert

oder 1 MB als Wert erreicht ist. Wenn das Laufwerk keinen dieser Werte akzeptiert, schlägt das Backup fehl.

### WriteCacheSize

Dies ist die Puffergröße (in Byte), die beim Schreiben auf die Bänder verwendet wird.

*Mögliche Werte:* 0, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 16384, 32768, 65536, 131072, 262144, 524288, 1048576 – aber nicht geringer als der Parameterwert für **DefaultBlockSize**.

Falls der Wert 0 beträgt oder der Parameter fehlt, wird **1 MB** als Puffergröße verwendet. Sollte das Betriebssystem diesen Wert nicht unterstützen, wird die Software den Wert solange durch 2 teilen, bis ein passender Wert gefunden oder der Parameterwert für **DefaultBlockSize** erreicht wurde. Falls kein vom Betriebssystem unterstützter Wert gefunden wird, schlägt das Backup fehl.

*Registry-Schlüssel (auf einer unter Windows laufenden Maschine):*
**HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\BackupAndRecovery\TapeLocation\WriteCacheSize**

*Die Befehlszeile in '/etc/Acronis/BackupAndRecovery.config' (auf einer unter Linux laufenden Maschine):*

```
<value name="WriteCacheSize" type="Dword">
     "value"
</value>
```

Falls Sie einen Wert ungleich 'Null' (0) spezifizieren, der vom Betriebssystem nicht unterstützt wird, schlägt das Backup fehl.

## Band-bezogene Backup-Optionen

Sie können die Backup-Optionen für die **Bandverwaltung** konfigurieren, um festzulegen:

- Ob das Datei-Recovery für auf Bändern gespeicherte Laufwerk-Backups aktiviert werden soll.
- Ob Bänder nach Schutzplan-Abschluss zurück in die Slots verschoben werden sollen.
- Ob Bänder nach einem Backup-Abschluss ausgeworfen werden sollen.
- Ob ein freies Band für jedes vollständige Backup verwendet werden soll.
- Ob ein Band überschrieben werden soll, wenn ein neues Voll-Backup erstellt wird (nur für autonome Bandlaufwerke).
- Ob Bandsätze zur Unterscheidung verwendeter Bänder genutzt werden sollen – beispielsweise für Backups, die an unterschiedlichen Tagen der Woche erstellt wurden, oder für Backups von unterschiedlichen Maschinentypen.

## Parallele Aktionen

Acronis Cyber Protect kann Aktionen mit verschiedenen Komponenten eines Bandgerätes gleichzeitig durchführen. Sie können während einer Aktion (Backup, Recovery, erneutes Scannen oder Löschen), die ein Bandlaufwerk verwendet, eine Aktion starten, die einen Wechsler verwendet

(ein Band zu einem anderen Schacht verschieben oder ein Band auswerfen). Falls Ihre Bandbibliothek mehr als ein Laufwerk hat, können Sie zudem eine Aktion starten, die eines der Laufwerke nutzt, während eine Aktion mit einem anderen abläuft. Mehrere Maschinen können beispielsweise gleichzeitig sichern oder wiederherstellen – unter Verwendung verschiedener Laufwerke derselben Bandbibliothek.

Die Aktion zur Erkennung neuer Bandgeräte kann gleichzeitig mit jeder anderen Aktion durchgeführt werden. Während einer Inventarisierung ist – mit Ausnahme der Aktion 'Neue Bandgeräte ermitteln' – keine andere Aktion verfügbar.

Aktionen, die nicht parallel ausgeführt werden können, werden in eine Warteschlange gestellt.

## Einschränkungen

Bei Verwendung von Bandgeräten gelten folgende Beschränkungen:

1. Es werden keine Bandgeräte unterstützt, wenn eine Maschine mit einem Boot-Medium gestartet wird, welches auf einem 32-Bit-Linux-Kernel basiert.
2. Folgende Datentypen können nicht auf Bändern gesichert werden: Microsoft 365-Postfächer, Microsoft Exchange-Postfächer.
3. Sie können keine applikationskonformen Backups von physischen und virtuellen Maschinen erstellen.
4. Unter macOS werden nur Datei-Backups zu einem verwalteten bandbasierten Speicherort unterstützt.
5. Eine Konsolidierung von auf Bändern gespeicherten Backups ist nicht möglich. Das Backup-Schema **Nur Inkrementell** ist daher nicht verfügbar, wenn Sie Bänder als Backup-Ziel verwenden.
6. Eine Deduplizierung von auf Bändern gespeicherten Backups ist nicht möglich.
7. Die Software kann ein Band nicht automatisch überschreiben, wenn auf dem Band noch nicht gelöschte Backups vorliegen oder wenn es auf anderen Bändern noch abhängige Backups gibt. Die einzige Ausnahme von dieser Regel ist, wenn die Option 'Band im autonomen Bandlaufwerk bei Erstellung eines Voll-Backups überschreiben' aktiviert wurde.
8. Sie können unter einem Betriebssystem keine auf Bändern gespeicherten Backups wiederherstellen, wenn für die Recovery-Aktion ein Neustart des Betriebssystems erforderlich ist. Verwenden Sie zur Durchführung einer solchen Wiederherstellung ein Boot-Medium.
9. Sie können jedes auf Bändern gespeicherte Backup validieren, aber Sie können keine Validierung für einen kompletten, bandbasierten Speicherort oder ein Bandgerät auswählen.
10. Ein verwalteter bandbasierter Speicherort kann nicht per Verschlüsselung geschützt werden. Verschlüsseln Sie stattdessen Ihre Backups.
11. Die Software kann ein Backup nicht gleichzeitig auf mehrere Bänder schreiben – oder mehrere Backups mittels desselben Laufwerks auf dasselbe Band.
12. Es werden keine Geräte unterstützt, die das 'Network Data Management Protocol' (NDMP) verwenden.

13. Es werden keine Barcode-Drucker unterstützt.
14. Bänder, die mit LTFS (Linear Tape File System) formatiert sind, werden nicht unterstützt.

## Die Lesbarkeit von Bändern, die von älteren Acronis Produkten beschrieben wurden

Die nachfolgende Tabelle fasst die Lesbarkeit von Bändern in Acronis Cyber Protect, die durch die Produktfamilie Acronis True Image Echo, Acronis True Image 9.1, Acronis Backup & Recovery 10, Acronis Backup & Recovery 11, Acronis Backup 11.5, 11.7 und 12.5 beschrieben wurden. Die Tabelle illustriert außerdem die Kompatibilität von Bändern, die durch verschiedene Komponenten von Acronis Cyber Protect beschrieben wurden.

Sie können inkrementelle und differentielle Backups an erneut gescannte Backups anhängen, die von Acronis Backup 11.5, 11.7 und 12.5 erstellt wurden.

| | **... ist lesbar auf einem Bandgerät, angeschlossen an eine Maschine mit...** | | | |
|---|---|---|---|---|
| | Acronis Cyber Protect Bootable Media | Acronis Cyber Protect Agent für Windows | Acronis Cyber Protect Agent für Linux | Acronis Cyber Protect Storage Node |

| | | | | | | |
|---|---|---|---|---|---|---|
| **Band, beschrieben auf einem lokal angeschlossenen Bandgerät (Bandlaufwerk oder -bibliothek), durch...** | Boot-Medium | 9.1 | + | + | + | + |
| | | Echo | + | + | + | + |
| | | ABR10 | + | + | + | + |
| | | ABR11/ Acronis Backup 11.5/11.7/12.5 | + | + | + | - |
| | Agent für Windows | 9.1 | + | + | + | + |
| | | Echo | + | + | + | + |
| | | ABR10 | + | + | + | + |
| | | ABR11/ Acronis Backup 11.5/11.7/12.5 | + | + | + | - |
| | Agent für Linux | 9.1 | + | + | + | + |
| | | Echo | + | + | + | + |
| | | ABR10 | + | + | + | + |
| | | ABR11/ Acronis Backup 11.5/11.7/12.5 | + | + | + | - |
| **Band, beschrieben auf einem Bandgerät, durch...** | Backup Server | 9.1 | - | - | - | - |
| | | Echo | - | - | - | - |
| | Storage Node | ABR10 | + | + | + | + |
| | | ABR11/ Acronis Backup 11.5/11.7/12.5 | + | + | + | + |

# Erste Schritte bei Verwendung eines Bandgeräts

## Eine Maschine per Backup zu einem lokal angeschlossenen Bandgerät sichern

### Voraussetzungen

- Das Bandgerät ist gemäß den Herstelleranweisungen mit der Maschine verbunden.
- Der Protection Agent ist auf der Maschine installiert.

### Vor dem Backup

1. Beladen Sie das Bandgerät mit Bändern.
2. Melden Sie sich an der Cyber Protect Webkonsole an.
3. Erweitern Sie unter **Einstellungen** –> **Bandverwaltung** den Maschinenknoten – und klicken Sie dann auf **Bandgeräte**.
4. Überprüfen Sie, dass das angeschlossene Bandgerät angezeigt wird. Wenn nicht, klicken Sie auf **Geräte erkennen**.
5. Führen Sie die Band-Inventarisierung durch:
   a. Klicken Sie auf den Namen des Bandgeräts.
   b. Klicken Sie auf **Inventarisierung**, damit die geladenen Bänder erkannt werden. Lassen Sie die Option **Vollständige Inventarisierung** eingeschaltet. Schalten Sie die Option **Unbekannte oder importierte Bänder in den Pool 'Freie Bänder' verschieben** nicht aus. Klicken Sie auf **Inventarisierung jetzt starten**.
   **Ergebnis:** Die geladenen Bänder wurden zu den passenden Pools verschoben, so wie im Abschnitt 'Inventarisierung' spezifiziert.

   **Hinweis**
   Die vollständige Inventarisierung eines kompletten Bandgerätes kann viel Zeit benötigen.

   c. Falls die geladenen Bänder an den Pool **Unbekannte Bänder** oder **Importierte Bänder** übertragen wurden und Sie diese für Backups nutzen wollen, dann verschieben Sie diese Bänder manuell zum Pool **Freie Bänder**.

   **Hinweis**
   Bänder, die an den Pool **Importierte Bänder** übertragen wurden, enthalten Backups, die von Acronis Software geschrieben wurden. Bevor Sie solche Bänder in den Pool **Freie Bänder** verschieben, sollten Sie sicherstellen, dass Sie diese Backups nicht mehr benötigen.

### Backup

Erstellen Sie einen Schutzplan, wie im Abschnitt 'Backup' beschrieben. Wenn Sie den Backup-Speicherort festlegen, wählen Sie **Band-Pool 'Acronis'**.

### Ergebnis

- Wenn Sie auf den Speicherort zugreifen wollen, wo die Backups erstellt werden, dann klicken Sie auf **Backup Storage** –> **Band-Pool 'Acronis'**.
- Die Bänder mit den Backups werden in den Pool '**Acronis**' verschoben.

## Backups zu einem Bandgerät erstellen, das an einen Storage Node angeschlossen ist

### Voraussetzungen

- Ein Storage Node ist auf dem Management Server registriert.
- Das Bandgerät ist gemäß den Herstelleranweisungen mit dem Storage Node verbunden.

### Vor dem Backup

1. Beladen Sie das Bandgerät mit Bändern.
2. Melden Sie sich an der Cyber Protect Webkonsole an.
3. Erweitern Sie unter **Einstellungen** –> **Bandverwaltung** den Knoten mit dem Storage Node-Name – und klicken Sie dann auf **Bandgeräte**.
4. Überprüfen Sie, dass das angeschlossene Bandgerät angezeigt wird. Wenn nicht, klicken Sie auf **Geräte erkennen**.
5. Führen Sie die Band-Inventarisierung durch:
   a. Klicken Sie auf den Namen des Bandgeräts.
   b. Klicken Sie auf **Inventarisierung**, damit die geladenen Bänder erkannt werden. Lassen Sie die Option **Vollständige Inventarisierung** eingeschaltet. Schalten Sie die Option **Unbekannte oder importierte Bänder in den Pool 'Freie Bänder' verschieben** nicht aus. Klicken Sie auf **Inventarisierung jetzt starten**.

      **Ergebnis:** Die geladenen Bänder wurden zu den passenden Pools verschoben, so wie im Abschnitt 'Inventarisierung' spezifiziert.

      **Hinweis**
      Die vollständige Inventarisierung eines kompletten Bandgerätes kann viel Zeit benötigen.

   c. Falls die geladenen Bänder an den Pool **Unbekannte Bänder** oder **Importierte Bänder** übertragen wurden und Sie diese für Backups nutzen wollen, dann verschieben Sie diese Bänder manuell zum Pool **Freie Bänder**.

**Hinweis**
Bänder, die an den Pool **Importierte Bänder** übertragen wurden, enthalten Backups, die von Acronis Software geschrieben wurden. Bevor Sie solche Bänder in den Pool **Freie Bänder** verschieben, sollten Sie sicherstellen, dass Sie diese Backups nicht mehr benötigen.

d. Entscheiden Sie, ob Ihre Backups auf Bänder erfolgen sollen, die sich im Pool '**Acronis**' befinden – oder ob Sie einen neuen Pool erstellen wollen.

   **Details:** Wenn Sie mehrere Pools haben, dann können Sie damit auch für jede Maschine oder Unternehmensabteilung einen separaten Bandsatz verwenden. Durch die Verwendung mehrerer Pools können Sie verhindern, dass Backups, die von unterschiedlichen Schutzpläne erstellt wurden, auf einem Band gemischt werden.

e. Überspringen Sie diesen Schritt, wenn der ausgewählte Pool bei Bedarf Bänder aus dem Pool '**Freie Bänder**' nehmen kann.

   Verschieben Sie anderenfalls Bänder vom Pool '**Freie Bänder**' zu dem ausgewählten Pool.

   **Tipp:** Um zu erfahren, ob ein Pool Bänder aus dem Pool '**Freie Bänder**' entnehmen kann, klicken Sie auf den entsprechenden Pool und wählen dann den Befehl **Info**.

### Backup

Erstellen Sie einen Schutzplan, wie im Abschnitt 'Backup' beschrieben. Wenn Sie den Backup-Speicherort festlegen, wählen Sie den erstellten Band-Pool.

### Ergebnis

- Wenn Sie auf den Speicherort zugreifen wollen, wo die Backups erstellt werden, dann klicken Sie auf **Backups** und anschließend auf den Namen des erstellten Band-Pools.
- Bänder mit Backups werden zum ausgewählten Pool verschoben.

### Tipps zur weiteren Nutzung der Bandbibliothek

- Sie müssen nicht jedes Mal, wenn Sie ein neues Band laden, eine vollständige Inventarisierung durchführen. Folgen Sie zur Zeitersparnis der im Abschnitt 'Inventarisierung' beschriebenen Prozedur (unter 'Schnelle und vollständige Inventarisierung kombinieren').
- Sie können auch andere Pools auf derselben Bandbibliothek erstellen und jede davon als Backup-Ziel auswählen.

## Wiederherstellung unter einem Betriebssystem von einem Bandgerät

***So führen Sie eine Recovery-Aktion unter einem Betriebssystem von einem Bandgerät aus:***

1. Melden Sie sich an der Cyber Protect Webkonsole an.
2. Klicken Sie auf **Geräte** und wählen Sie dann die per Backup gesicherte Maschine aus.
3. Klicken Sie auf **Recovery**.

4. Wählen Sie einen Recovery-Punkt. Beachten Sie dabei, dass Recovery-Punkte nach Speicherorten gefiltert werden.
5. Die Software zeigt Ihnen eine Liste mit all den Bändern an, die für die Wiederherstellung erforderlich sind. Fehlende Bänder sind ausgegraut dargestellt. Sollte Ihr Bandgerät noch leere Slots (Schächte) haben, dann laden Sie diese Bänder in das Gerät.
6. Konfigurieren Sie andere Recovery-Einstellungen.
7. Klicken Sie auf **Recovery starten**, damit die Wiederherstellung beginnt.
8. Sollte eines der benötigten Bänder aus irgendeinem Grund nicht geladen sein, dann wird Ihnen die Software eine Nachricht mit dem Identifier des erforderlichen Bandes anzeigen. Gehen Sie folgendermaßen vor:
   a. Laden Sie das Band.
   b. Führen Sie eine schnelle Inventarisierung durch.
   c. Klicken Sie auf **Überblick** –> **Aktivitäten** und anschließend auf die Recovery-Aktivität mit dem Status **Benutzereingriff erforderlich**.
   d. Klicken Sie zuerst auf **Details anzeigen** und dann auf **Wiederholen**, um mit der Wiederherstellung fortzufahren.

### Was, wenn ich keine auf Bändern gespeicherten Backups sehen kann?

Das kann bedeuten, dass die Datenbank mit den Bandinhalten aus irgendeinem Grund verloren gegangen ist oder beschädigt wurde.

Gehen Sie folgendermaßen vor, um die Datenbank wiederherzustellen:

1. Führen Sie eine schnelle Inventarisierung durch.

   **Warnung!**
   Schalten Sie während der Inventarisierung *nicht* die Option **Unbekannte oder importierte Bänder in den Pool 'Freie Bänder' verschieben** ein. Falls der Schalter eingeschaltet ist, können Sie möglicherweise alle Ihre Backups verlieren.

2. Lassen Sie den Pool **Unbekannte Bänder** erneut scannen. Als Ergebnis erhalten Sie die Inhalte des geladenen Bandes (bzw. der Bänder).
3. Falls irgendwelche der ermittelten Backups auf anderen Bändern fortgesetzt werden, die bisher noch nicht neu eingescannt wurden, dann laden Sie diese Bänder bei entsprechender Aufforderung und scannen Sie auch diese neu ein.

## Wiederherstellung mit einem Boot-Medium von einem lokal angebundenen Bandgerät

***So führen Sie eine Wiederherstellung mit einem Boot-Medium von einem lokal angebundenen Bandgerät aus:***

1. Laden Sie die für die Wiederherstellung benötigten Bänder in das Bandgerät.
2. Booten Sie die Maschine mithilfe eines Boot-Mediums.
3. Klicken Sie entweder auf **Diese Maschine lokal verwalten** oder zweimal auf **Rescue Bootable Media** (abhängig vom verwendeten Typ des Mediums).
4. Sollte das Bandgerät per iSCSI-Schnittstelle angebunden sein, dann konfigurieren Sie das Gerät wie im Abschnitt 'iSCSI- und NDAS-Geräte konfigurieren' beschrieben.
5. Klicken Sie auf **Bandverwaltung**.
6. Klicken Sie auf **Inventarisierung**.
7. Wählen Sie bei **Zu inventarisierende Objekte** das gewünschte Bandgerät.
8. Klicken Sie auf **Start**, damit die Inventarisierungsaktion beginnt.
9. Klicken Sie nach Abschluss der Inventarisierung auf **Schließen**.
10. KlickenSie auf **Aktionen** –> **Recovery**.
11. Klicken Sie auf **Daten wählen** und dann auf **Durchsuchen**.
12. Erweiteren Sie die Anzeige für die **Bandgeräte** und wählen Sie dann das benötigte Gerät aus. Das System erfragt eine Bestätigung der Aktion 'Erneut scannen'. Klicken Sie auf **Ja**.
13. Wählen Sie den Pool **Unbekannte Bänder**.
14. Wählen Sie die erneut zu scannenden Bänder. Aktivieren Sie zur Wahl aller Bänder des Pools das Kontrollkästchen neben dem Spaltenkopf **Bandname**.
15. Sollten die Bänder ein kennwortgeschütztes Backup enthalten, dann aktivieren Sie das entsprechende Kontrollkästchen und spezifizieren Sie das Kennwort des Backups im Feld **Kennwort**. Bei einer fehlenden oder falschen Angabe des Kennworts wird das Backup nicht erkannt. Denken Sie daran, falls nach dem erneuten Scannen keine Backup angezeigt werden.

    **Tipp**: Sollten die Bänder mehrere kennwortgeschützte Backups enthalten, die wiederum verschiedene Kennwörter verwenden, dann müssen Sie das erneute Scannen mehrfach wiederholen, um jedes Kennwort entsprechend einzugeben.
16. Klicken Sie auf **Start**, damit das erneute Scannen beginnt. Als Ergebnis erhalten Sie die Inhalte des geladenen Bandes (bzw. der Bänder).
17. Falls irgendwelche der ermittelten Backups auf anderen Bändern fortgesetzt werden, die bisher noch nicht neu eingescannt wurden, dann laden Sie diese Bänder bei entsprechender Aufforderung und scannen Sie auch diese neu ein.
18. Klicken Sie auf **OK**, nachdem das erneute Scannen abgeschlossen ist.
19. Wählen Sie in der **Archiv-Anzeige** das Backup für die Recovery-Aktion aus und wählen Sie dann die wiederherzustellenden Daten. Nachdem Sie auf **OK** geklickt haben, wird Ihnen auf der Seite **Daten wiederherstellen** eine Liste der für die Wiederherstellung benötigten Bänder angezeigt. Fehlende Bänder sind ausgegraut dargestellt. Sollte Ihr Bandgerät noch leere Slots (Schächte) haben, dann laden Sie diese Bänder in das Gerät.
20. Konfigurieren Sie andere Recovery-Einstellungen.
21. Wählen Sie **OK**, um die Wiederherstellung zu starten.

22. Sollte eines der benötigten Bänder aus irgendeinem Grund nicht geladen sein, dann wird Ihnen die Software eine Nachricht mit dem Identifier des erforderlichen Bandes anzeigen. Gehen Sie folgendermaßen vor:
    a. Laden Sie das Band.
    b. Führen Sie eine schnelle Inventarisierung durch.
    c. Klicken Sie auf **Überblick** –> **Aktivitäten** und anschließend auf die Recovery-Aktivität mit dem Status **Benutzereingriff erforderlich**.
    d. Klicken Sie zuerst auf **Details anzeigen** und dann auf **Wiederholen**, um mit der Wiederherstellung fortzufahren.

## Wiederherstellung mit einem Boot-Medium von einem Bandgerät, das an einem Storage Node angeschlossen ist

***So führen Sie mit einem Boot-Medium eine Wiederherstellung von einem Bandgerät aus, welches an einem Storage Node angeschlossen ist:***

1. Laden Sie die für die Wiederherstellung benötigten Bänder in das Bandgerät.
2. Booten Sie die Maschine mithilfe eines Boot-Mediums.
3. Klicken Sie entweder auf **Diese Maschine lokal verwalten** oder zweimal auf **Rescue Bootable Media** (abhängig vom verwendeten Typ des Mediums).
4. Klicken Sie auf **Recovery**.
5. Klicken Sie auf **Daten wählen** und dann auf **Durchsuchen**.
6. Geben Sie im Feld **Pfad** die Zeichenfolge '`bsp://<Storage Node-Adresse>/<Pool-Name>/`' ein – wobei `<Storage Node-Adresse>` der IP-Adresse des Storage Nodes entspricht, der das benötigte Backup enthält, und `<Pool-Name>` für die Bezeichnung des Pools steht. Klicken Sie auf **OK** und spezifizieren Sie die Anmeldedaten für den Pool.
7. Wählen Sie zuerst das Backup und dann die Daten, die Sie wiederherstellen wollen. Nachdem Sie auf **OK** geklickt haben, wird Ihnen auf der Seite **Daten wiederherstellen** eine Liste der für die Wiederherstellung benötigten Bänder angezeigt. Fehlende Bänder sind ausgegraut dargestellt. Sollte Ihr Bandgerät noch leere Slots (Schächte) haben, dann laden Sie diese Bänder in das Gerät.
8. Konfigurieren Sie andere Recovery-Einstellungen.
9. Wählen Sie **OK**, um die Wiederherstellung zu starten.
10. Sollte eines der benötigten Bänder aus irgendeinem Grund nicht geladen sein, dann wird Ihnen die Software eine Nachricht mit dem Identifier des erforderlichen Bandes anzeigen. Gehen Sie folgendermaßen vor:
    a. Laden Sie das Band.
    b. Führen Sie eine schnelle Inventarisierung durch.
    c. Klicken Sie auf **Überblick** –> **Aktivitäten** und anschließend auf die Recovery-Aktivität mit dem Status **Benutzereingriff erforderlich**.

d. Klicken Sie zuerst auf **Details anzeigen** und dann auf **Wiederholen**, um mit der Wiederherstellung fortzufahren.

# Bandverwaltung

## Bandgeräte erkennen

Beim Erkennen von Bandgeräten findet die Backup-Software die Bandgeräte, die an die Maschine angeschlossen sind, und schreibt die dazugehörigen Informationen in die Bandverwaltungsdatenbank. Bandgeräte, die erkannt wurden, werden vom RSM (Removable Storage Manager) deaktiviert.

Normalerweise wird ein Bandgerät automatisch erkannt, sobald es an eine Maschine angeschlossen wird, auf dem das Produkt installiert ist. In folgenden Fällen kann es jedoch notwendig sein, die Erkennung von Bandgeräten manuell anzustoßen:

- Nachdem Sie ein Bandgerät (erneut) angeschlossen haben.
- Nachdem Sie die Backup-Software (erneut) auf der Maschine installiert haben, an die ein Bandgerät angeschlossen ist.

***So lassen Sie Bandgeräte erkennen***

1. Klicken Sie auf **Einstellungen** –> **Bandverwaltung**.
2. Wählen Sie die Maschine aus, an welcher das Bandgerät angeschlossen ist.
3. Klicken Sie auf **Geräte erkennen**. Sie sehen die angeschlossener Bandgeräte, deren Laufwerke und Slots (Schächte).

## Band-Pools

Die Backup-Software verwendet sogenannte Band-Pools, bei denen es sich um logische Gruppen von Bändern handelt. Die Software enthält bereits folgende vordefinierte Band-Pools: **Unbekannte Bänder**, **Importierte Bänder**, **Freie Bänder** und **Acronis**. Sie können außerdem auch Ihre eigenen, benutzerdefinierten Pools erstellen.

Der Pool **Acronis** sowie benutzerdefinierte Pools werden ebenfalls als Backup-Speicherorte verwendet.

### Vordefinierte Pools

**Unbekannte Bänder**

Der Pool enthält Bänder, die durch Anwendungen von Drittherstellern beschrieben wurden. Um auf diese Bänder schreiben zu können, müssen sie von Ihnen explizit in den Pool **Freie Bänder** verschoben werden. Sie können Bändern von diesem Pool zu keinem anderen Pool verschieben – mit Ausnahme des Pools **Freie Bänder**.

**Importierte Bänder**

Der Pool enthält Bänder, die von Acronis Cyber Protect in einem Bandgerät beschrieben wurden, das aber an einen anderen Storage Node oder Agenten angeschlossen war. Um auf diese Bänder schreiben zu können, müssen sie von Ihnen explizit in den Pool **Freie Bänder** verschoben werden. Sie können Bändern von diesem Pool zu keinem anderen Pool verschieben – mit Ausnahme des Pools **Freie Bänder**.

**Freie Bänder**

Der Pool enthält freie (leere) Bänder. Sie können Bänder von anderen Pools manuell zu diesem Pool verschieben.

Wenn Sie ein Band zum Pool **Freie Bänder** verschieben, kennzeichnet die Software diese als leer. Falls das Band Backups enthält, so sind diese mit dem Symbol  gekennzeichnet. Wenn die Software mit dem Überschreiben des Bandes beginnt, werden die mit den Backups verbundenen Daten aus der Datenbank entfernt.

**Acronis**

Der Pool wird standardmäßig für Backups verwendet, wenn Sie keine eigenen Pools erstellen wollen. Das trifft üblicherweise bei Bandlaufwerken mit einer kleinen Zahl von Bändern zu.

### Benutzerdefinierte Pools

Sie müssen mehrere Pools erstellen, falls Sie Backups mit unterschiedlichen Daten separieren wollen. Sie können benutzerdefinierte Pools beispielsweise erstellen, um folgende Daten zu trennen:

- Backups aus unterschiedlichen Abteilungen Ihrer Firma
- Backups von verschiedenen Maschinen
- Backups von System-Volumes und Benutzerdaten.

## Aktionen mit Pools

### Einen Pool erstellen

***So erstellen Sie einen Pool:***

1. Klicken Sie auf **Einstellungen** –> **Bandverwaltung**.
2. Wählen Sie die Maschine oder den Storage Node, an welche(n) Ihr Bandgerät angeschlossen ist, und klicken Sie dann unterhalb dieser Maschine auf **Band-Pools**.
3. Klicken Sie auf **Pool erstellen**.
4. Spezifizieren Sie den Pool-Namen.
5. [Optional] Deaktivieren Sie das '**Bänder automatisch vom Pool 'Freie Bänder' nehmen...**'-Kontollkästchen. Wenn es deaktiviert ist, werden nur solche Bänder für Backups verwendet, die zu einem bestimmten Moment in den neuen Pool aufgenommen wurden.
6. Klicken Sie auf **Erstellen**.

### Einen Pool bearbeiten

Sie können die Parameter des Pools **Acronis** oder Ihres eigenen, benutzerdefinierten Pools bearbeiten.

***So können Sie einen Pool bearbeiten:***

1. Klicken Sie auf **Einstellungen** –> **Bandverwaltung**.
2. Wählen Sie die Maschine oder den Storage Node, an welche(n) Ihr Bandgerät angeschlossen ist, und klicken Sie dann unterhalb dieser Maschine auf **Band-Pools**.
3. Wählen Sie den gewünschten Pool aus und klicken Sie dann auf **Pool bearbeiten**.
4. Sie können den Namen des Pools oder dessen Einstellungen ändern. Zu weiteren Informationen über Pool-Einstellungen siehe den Abschnitt 'Einen Pool erstellen'.
5. Klicken Sie auf **Speichern**, um die Änderungen zu übernehmen.

### Einen Pool löschen

Sie können nur benutzerdefinierte Pools löschen. Vordefinierte Band-Pools (**Unbekannte Bänder**, **Importierte Bänder**, **Freie Bänder** und **Acronis**) können nicht gelöscht werden.

**Hinweis**
Vergessen Sie nach dem Löschen eines Pools nicht, all die Schutzpläne zu bearbeiten, die diesen Pool als Backup-Speicherort verwenden. Ansonsten werden diese Schutzpläne fehlschlagen.

***So löschen Sie einen Pool:***

1. Klicken Sie auf **Einstellungen** –> **Bandverwaltung**.
2. Wählen Sie die Maschine oder den Storage Node, an welche(n) Ihr Bandgerät angeschlossen ist, und klicken Sie dann unterhalb dieser Maschine auf **Band-Pools**.
3. Wählen Sie den gewünschten Pool und klicken Sie dann auf **Löschen**.
4. Wählen Sie den neuen Pool, zu dem die Bänder des alten (zu löschenden) Pools verschoben werden sollen, nachdem der alte Pool gelöscht wurde.
5. Klicken Sie auf **OK**, um den Pool zu löschen.

## Aktionen mit Bändern

### Zu einem anderen Slot verschieben

Verwenden Sie die Aktion in folgenden Situationen:

- Sie müssen mehrere Bänder gleichzeitig aus einem Bandgerät herausnehmen.
- Ihr Bandgerät hat keinen 'Mail-Slot' (Schacht) und die herauszunehmenden Bänder befinden sich in Slots von fest angeschlossenen Magazinen.

Sie müssen Bänder zu den Slots von Ein-Slot-Magazinen verschieben und das Magazin dann manuell herausnehmen.

***So können Sie ein Band zu einem anderen Slot (Schacht) verschieben***

1. Klicken Sie auf **Einstellungen** –> **Bandverwaltung**.
2. Wählen Sie die Maschine oder den Storage Node, an welche(n) Ihr Bandgerät angeschlossen ist, und klicken Sie dann unterhalb dieser Maschine auf **Band-Pools**.
3. Klicken Sie auf den Pool, der das gewünschte Band enthält, und wählen Sie dann das erforderliche Band.
4. Klicken Sie auf **Zu Slot verschieben**.
5. Wählen Sie einen neuen Slot, zu dem das gewählte Band verschoben werden soll.
6. Klicken Sie auf **Verschieben**, damit die Aktion gestartet wird.

## Zu einem anderen Pool verschieben

Diese Aktion ermöglicht Ihnen, ein Band oder mehrere Bänder von einem Pool zu einem anderen zu verschieben.

Wenn Sie ein Band zum Pool **Freie Bänder** verschieben, kennzeichnet die Software diese als leer.

Falls das Band Backups enthält, so sind diese mit dem Symbol  gekennzeichnet. Wenn die Software mit dem Überschreiben des Bandes beginnt, werden die mit den Backups verbundenen Daten aus der Datenbank entfernt.

**Anmerkungen zu besonderen Bandtypen**

- Sie können keine schreibgeschützten Bänder und keine einmal beschreibbaren WORM-Bänder (Write-Once-Read-Many) in den Pool **Freie Bänder** verschieben.
- Reinigungsbänder werden immer im Pool **Unbekannte Bänder** angezeigt; diese können von Ihnen zu keinem anderen Pool verschoben werden.

***So können Sie Bänder zu einem anderen Pool verschieben***

1. Klicken Sie auf **Einstellungen** –> **Bandverwaltung**.
2. Wählen Sie die Maschine oder den Storage Node, an welche(n) Ihr Bandgerät angeschlossen ist, und klicken Sie dann unterhalb dieser Maschine auf **Band-Pools**.
3. Klicken Sie auf den Pool, der die notwendigen Bänder enthält und wählen Sie dann die benötigten Bänder.
4. Klicken Sie auf **Zu Pool verschieben**.
5. [Optional] Klicken Sie auf **Neuen Pool erstellen**, falls Sie für die gewählten Bänder einen anderen Pool erstellen wollen. Führen Sie die im Abschnitt „Einen Pool erstellen“ beschriebenen Aktionen aus.
6. Wählen Sie den Pool, zu dem die Bänder verschoben werden sollen.
7. Klicken Sie auf **Verschieben**, um die Änderungen zu übernehmen.

**Hinweis**
Wenn Sie wiederherstellbare Backups auf dem Band haben und das Band zu einem anderen Pool verschieben, sollten Sie sicherstellen, dass Sie das Depot unter 'Backup Storage' aktualisieren, sobald Sie die Verschieben-Aktion abgeschlossen haben. Die Backups werden, unabhängig vom ursprünglichen Backup-Ziel, im zweiten Pool verfügbar sein.

## Inventarisierung

Die Inventarisierungsaktion ermittelt in ein Bandgerät geladene Bänder und weist denjenigen Bändern Namen zu, die keine haben.

### Inventarisierungsmethoden

Es gibt zwei Methoden der Inventarisierung.

**Schnelle Inventarisierung**

Der Agent oder der Storage scannt die Bänder nach Barcodes. Durch die Verwendung von Barcodes kann die Software ein Band schnell zu dem Pool zurückgeben, wo es zuvor vorlag.

Verwenden Sie diese Methode, um Bänder zu erkennen, die von demselben und an dieselbe Maschine angeschlossenen Bandgerät verwendet wurden. Andere Bänder werden an den Pool **Unbekannt Bänder** gesendet.

Sollte Ihre Bandbibliothek keinen Barcode-Leser enthalten, dann werden alle Bänder an den Pool **Unbekannte Bänder** gesendet. Führen Sie zur Erkennung Ihrer Bänder eine vollständige Inventarisierung durch – oder kombinieren Sie (wie weiter unten beschrieben) eine schnelle und eine vollständige Inventarisierung.

**Vollständige Inventarisierung**

Der Agent oder der Storage Node lesen früher geschriebene Tags und analysieren weitere Informationen über die Inhalte der geladenen Bänder. Verwenden Sie diese Methode, um leere Bänder zu erkennen – sowie Bänder, die durch dieselbe Software auf beliebigen Bandgeräten und Maschinen beschrieben wurden.

Die nachfolgende Tabelle zeigt Pools an, zu denen Bänder als Ergebnis der vollständigen Inventarisierung gesendet werden.

| Band wurde verwendet von... | Band wird gelesen von... | Band wird gesendet zu Pool... |
|---|---|---|
| Agent | Derselbe Agent | Wo das Band zuvor war |
| | Ein anderer Agent | **Importierte Bänder** |
| | Storage Node | **Importierte Bänder** |

| | | |
|---|---|---|
| Storage Node | Derselbe Storage Node | Wo das Band zuvor war |
| | Ein anderer Storage Node | **Importierte Bänder** |
| | Agent | **Importierte Bänder** |
| Drittanbieter-Backup-Applikation | Agent oder Storage Node | **Unbekannte Bänder** |

Bänder bestimmter Typen werden zu besonderen Pools gesendet:

| Bandtyp | Band wird gesendet zu Pool... |
|---|---|
| Leere Bänder | **Freie Bänder** |
| Leeres, schreibgeschütztes Band | **Unbekannte Bänder** |
| Reinigungsband | **Unbekannte Bänder** |

Die schnelle Inventarisierung kann auf komplette Bandgeräte angewendet werden. Die vollständige Inventarisierung kann auf komplette Bandgeräte, einzelne Laufwerke oder Slots angewendet werden. Bei autonomen Bandlaufwerken wird die vollständige Inventarisierung immer durchgeführt, selbst wenn die schnelle Inventarisierung ausgewählt wurde.

**Schnelle und vollständige Inventarisierung kombinieren**

Die vollständige Inventarisierung eines kompletten Bandgerätes kann viel Zeit benötigen. Sollten Sie nur einige wenige Bänder inventarisieren müssen, dann können Sie folgendermaßen vorgehen:

1. Führen Sie eine schnelle Inventarisierung des Bandgerätes durch.
2. Klicken Sie auf den Pool **Unbekannte Bänder**. Ermitteln Sie die Bänder, die Sie inventarisieren wollen, und notieren Sie sich die Slots (Schächte), die diese Bänder belegen.
3. Führen Sie für diese Slots eine vollständige Inventarisierung durch.

## Aktionen nach der Inventarisierung

Falls Sie Backups auf Bänder durchführen wollen, die in den Pools **Unbekannte Bänder** oder **Importierte Bänder** vorliegen, dann verschieben Sie diese in den Pool **Freie Bänder** und dann zum Pool **Acronis** oder einen benutzerdefinierten Pool. Falls der Pool, zu dem die Backups erfolgen sollen, vom Typ 'wiederauffüllbar' ist, können Sie die Bänder im Pool **Freie Bänder** belassen.

Falls Sie eine Wiederherstellung von einem Band ausführen wollen, das im Pool **Unbekannte Bänder** oder **Importierte Bänder** vorliegt, so müssen Sie es erneut scannen. Das Band wird zu dem Pool verschoben, den Sie beim erneuten Scannen ausgewählt haben – und die auf dem Band gespeicherten Backups erscheinen in diesem Speicherort.

### Abfolge der Aktionen

1. Klicken Sie auf **Einstellungen** –> **Bandverwaltung**.
2. Wählen Sie die Maschine mit dem angeschlossenen Bandgerät aus – und dann das Bandgerät, welches Sie inventarisieren wollen.
3. Klicken Sie auf **Inventarisierung**.
4. [Optional] Um die schnelle Inventarisierung auszuwählen, müssen Sie die **Vollständige Inventarisierung** ausschalten.
5. [Optional] Schalten Sie die Option **Unbekannte und importierte Bänder in den Pool 'Freie Bänder' verschieben** ein.

   **Warnung!**
   Aktivieren Sie diesen Schalter nur dann, wenn Sie absolut sicher sind, dass die auf Ihren Bändern gespeicherten Daten überschrieben werden können.

6. Klicken Sie auf **Inventarisierung jetzt starten**, damit die Inventarisierung gestartet wird.

## Erneut scannen

Die Informationen über den Inhalt der Bänder werden in einer dedizierten Datenbank gespeichert. Die Aktion 'Erneut scannen' liest den Inhalt der Bänder ein und aktualisiert die Datenbank, falls die dort befindlichen Informationen nicht mit den auf den Bändern gespeicherten Daten übereinstimmen. Die als Folge der Aktion ermittelten Backups werden in dem spezifizierten Pool platziert.

Sie können innerhalb einer Aktion die Bänder eines Pools erneut scannen lassen. Nur 'online' Bänder können für die Aktion ausgewählt werden.

Wenn Sie Bänder mit einem Multistream- oder Multistream- und Multiplex-Backup erneut scannen wollen, benötigen Sie mindestens die gleiche Anzahl von Laufwerken, die zum Erstellen dieses Backups verwendet wurden. Ein solches Backup kann nicht durch ein autonomes Bandlaufwerk erneut gescannt werden.

Führen Sie 'Erneut scannen' aus:

- Falls die Datenbank eines Storages Nodes oder einer verwalteten Maschine verloren ging oder beschädigt wurde.
- Falls die Informationen über ein Band in der Datenbank nicht mehr aktuell sind (beispielsweise, weil der Inhalt eines Bandes durch einen anderen Storage Node oder Agenten modifiziert wurde).
- Um auf die auf Bändern gespeicherten Backups zugreifen zu können, wenn Sie unter einem Boot-Medium arbeiten.
- Falls Sie die Informationen über ein Band versehentlich von der Datenbank entfernt haben. Wenn Sie ein zuvor entferntes Band erneut scannen, erscheinen die auf diesem gespeicherten Backups erneut in der Datenbank und werden für Recovery-Aktionen verfügbar.

- Falls Backups von einem Band entweder manuell oder durch Aufbewahrungsregeln gelöscht wurden, Sie diese aber wieder für Recovery-Aktionen verfügbar haben wollen. Bevor Sie ein solches Band erneut scannen, sollten Sie es zuerst auswerfen, seine Information aus der Datenbank entfernen und das Band danach wieder in das Bandgerät einlegen.

***So können Sie Bänder neu scannen***

1. Klicken Sie auf **Einstellungen** –> **Bandverwaltung**.
2. Wählen Sie die Maschine oder den Storage Node, an welche(n) Ihr Bandgerät angeschlossen ist, und klicken Sie dann unterhalb dieser Maschine auf **Bandgeräte**.
3. Wählen Sie das Bandgerät, wo Sie die Bänder geladen haben.
4. Führen Sie eine schnelle Inventarisierung durch.

   **Hinweis**
   Aktivieren Sie während der Inventarisierung *nicht* die Option **Unbekannte oder importierte Bänder in den Pool 'Freie Bänder' verschieben**.

5. Wählen Sie den Pool **Unbekannte Bänder**. Das ist der Pool, zu dem die Mehrheit der Bänder als Ergebnis einer schnellen Inventarisierung gesendet wird. Sie können auch jeden anderen Pool neu scannen.
6. [Optional] Wenn Sie nur einzelne Bänder neu scannen wollen, müssen Sie diese auswählen.
7. Klicken Sie auf **Erneut scannen**.
8. Bestimmen Sie den Pool, wo die neu ermittelten Backups platziert werden sollen.
9. Aktivieren Sie bei Bedarf das Kontrollkästchen **Datei-Recovery für auf Bändern gespeicherte Laufwerk-Backups aktivieren**.

   **Details**: Falls das Kontrollkästchen aktiviert ist, erstellt die Software zusätzliche Dateien auf einem Festplattenlaufwerk der Maschine, an der das Bandgerät angeschlossen ist. Datei-Recovery von Laufwerk-Backups ist möglich, solange diese zusätzlichen Dateien intakt sind. Stellen Sie sicher, dass das Kontrollkästchen aktiviert ist, falls die Bänder applikationskonformen Backups enthalten. Anderenfalls werden Sie nicht in der Lage sein, Applikationsdaten von diesen Backups wiederherzustellen.
10. Sollten die Bänder kennwortgeschützte Backups enthalten, dann aktivieren Sie das entsprechende Kontrollkästchen und spezifizieren Sie das Kennwort für die Backups. Ohne oder bei falscher Angabe des Kennwortes werden die Backups nicht erkannt. Denken Sie daran, falls nach dem erneuten Scannen keine Backup angezeigt werden.

    **Tipp**: Sollten die Bänder Backups mit unterschiedlichen Kennwörtern enthalten, dann müssen Sie das erneute Scannen mehrfach wiederholen und bei jedem Durchlauf das jeweils passende Kennwort eingeben.
11. Klicken Sie auf **Erneutes Scannen starten**, damit die Aktion beginnt.

**Ergebnis:** Die ausgewählten Bänder werden zu dem ausgewählten Pool verschoben. Die auf diesen Bändern gespeicherten Backups können in diesem Pool gefunden werden. Ein über mehrere

Bänder verteiltes Backup erscheint solange nicht im Pool, bis alle entsprechenden Bänder erneut gescannt wurden.

## Umbenennung

Falls die Software ein neues Band ermittelt, weist sie diesem automatisch einen Namen im folgenden Format zu: **Band XXX**, wobei **XXX** eine eindeutige Nummer ist. Bändern werden fortlaufend nummeriert. Die Umbenennungsaktion ermöglicht Ihnen, den Namen eines Bandes manuell zu ändern.

***So können Sie Bänder umbenennen***

1. Klicken Sie auf **Einstellungen** –> **Bandverwaltung**.
2. Wählen Sie die Maschine oder den Storage Node, an welche(n) Ihr Bandgerät angeschlossen ist, und klicken Sie dann unterhalb dieser Maschine auf **Band-Pools**.
3. Klicken Sie auf den Pool, der das gewünschte Band enthält, und wählen Sie dann das erforderliche Band.
4. Klicken Sie auf **Umbenennen**.
5. Geben Sie den neuen Namen für das ausgewählte Band ein.
6. Klicken Sie auf **Umbenennen**, um die Änderungen zu übernehmen.

## Löschen

Wird ein Band physisch gelöscht, so werden auch alle auf dem Band gespeicherten Backups gelöscht und die dazugehörigen Informationen aus der Datenbank. Die Information über das Band selbst verbleibt jedoch in der Datenbank.

Nach dem Löschen wird ein Band, das sich im Pool **Unbekannte Bänder** oder **Importierte Bänder** befand, in den Pool **Freie Bänder** verschoben. Ein in einem anderen Pool befindliches Band wird nicht verschoben.

***So können Sie Bänder löschen***

1. Klicken Sie auf **Einstellungen** –> **Bandverwaltung**.
2. Wählen Sie die Maschine oder den Storage Node, an welche(n) Ihr Bandgerät angeschlossen ist, und klicken Sie dann unterhalb dieser Maschine auf **Band-Pools**.
3. Klicken Sie auf den Pool, der die notwendigen Bänder enthält und wählen Sie dann die benötigten Bänder.
4. Klicken Sie auf **Löschen**. Das System erfragt eine Bestätigung der Aktion.
5. Bestimmen Sie die Löschmethode: schnell oder vollständig.
6. Klicken Sie auf **Löschen**, damit die Aktion gestartet wird.
   **Details:** Sie können die Lösch-Aktion nicht abbrechen.

## Auswerfen

Zum erfolgreichen Auswerfen eines Bandes aus einer Bandbibliothek muss diese den 'Mail-Slot' (Schacht) haben und dieser darf nicht durch einen Benutzer oder eine andere Software gesperrt sein.

***So können Sie Bänder auswerfen***

1. Klicken Sie auf **Einstellungen** –> **Bandverwaltung**.
2. Wählen Sie die Maschine oder den Storage Node, an welche(n) Ihr Bandgerät angeschlossen ist, und klicken Sie dann unterhalb dieser Maschine auf **Band-Pools**.
3. Klicken Sie auf den Pool, der die notwendigen Bänder enthält und wählen Sie dann die benötigten Bänder.
4. Klicken Sie auf **Auswerfen**. Die Software fordert Sie auf, die Bandbeschreibung bereitzustellen. Wir empfehlen, dass Sie den physischen Ort beschreiben, wo die Bänder aufbewahrt werden. Die Software zeigt während einer Wiederherstellung diese Beschreibung an, sodass Sie die Bänder leichter finden können.
5. Klicken Sie auf **Auswerfen**, damit die Aktion gestartet wird.

Nachdem ein Band manuell oder automatisch ausgeworfen wurde, empfiehlt es sich, den entsprechenden Namen auf das Band zu schreiben.

## Entfernen

Durch die Aktion 'Entfernen' werden die Informationen über die auf dem gewählten Band gespeicherten Backups sowie die Informationen über das Band selbst aus der Datenbank gelöscht.

Sie können nur ein offline (ausgeworfenes) Band entfernen.

***So können Sie ein Band entfernen***

1. Klicken Sie auf **Einstellungen** –> **Bandverwaltung**.
2. Wählen Sie die Maschine oder den Storage Node, an welche(n) Ihr Bandgerät angeschlossen ist, und klicken Sie dann unterhalb dieser Maschine auf **Band-Pools**.
3. Klicken Sie auf den Pool, der das gewünschte Band enthält, und wählen Sie dann das erforderliche Band.
4. Klicken Sie auf **Entfernen**. Das System erfragt eine Bestätigung der Aktion.
5. Klicken Sie auf **Entfernen**, um das Band zu entfernen.

***Was sollen Sie tun, wenn Sie ein Band versehentlich entfernt haben?***

Anders als bei einem gelöschten Band wurden die Daten eines entfernten Bandes nicht physisch gelöscht. Sie können daher die auf einem solchen Band gespeicherten Backups wieder verfügbar machen. Gehen Sie folgendermaßen vor:

1. Laden Sie das Band in Ihr Bandgerät.
2. Führen Sie eine schnelle Inventarisierung durch, um das Band erkennen zu lassen.

   **Hinweis**
   Aktivieren Sie während der Inventarisierung *nicht* die Option **Unbekannte oder importierte Bänder in den Pool 'Freie Bänder' verschieben**.

3. Führen Sie die Aktion 'Erneut scannen' durch, um die auf den Bändern gespeicherten Daten mit der Datenbank abzugleichen.

## Einen Bandsatz spezifizieren

Mit dieser Aktion können Sie einen Bandsatz für Bänder spezifizieren.

Ein **Bandsatz** ist eine Gruppe von Bändern innerhalb eines Pools.

Anders als bei den Bandsätzen in den Backup-Optionen, wo Sie Variablen verwenden können, können Sie hier nur einen String-Wert spezifizieren.

Führen Sie diese Aktion aus, wenn die Software Backups zu *spezifischen* Bändern und gemäß einer bestimmten Regel durchführen soll (beispielsweise, wenn Sie die Backups an Montagen auf Band 1 speichern wollen, die von Dienstagen auf Band 2 usw.). Spezifizieren Sie einen bestimmten Bandsatz für jedes der erforderlichen Bänder und spezifizieren Sie denselben Bandsatz oder verwenden Sie geeignete Variablen in den Backup-Optionen.

Spezifizieren Sie beispielsweise den Bandsatz `Monday` für Band 1, `Tuesday` für Band 2 usw. In den Backup-Optionen spezifizieren Sie `[Weekday]`. Auf diese Weise wird am jeweiligen Wochentag das entsprechende Band verwendet.

***So können Sie einen Bandsatz für ein oder mehrere Bänder spezifizieren***

1. Klicken Sie auf **Einstellungen** –> **Bandverwaltung**.
2. Wählen Sie die Maschine oder den Storage Node, an welche(n) Ihr Bandgerät angeschlossen ist, und klicken Sie dann unterhalb dieser Maschine auf **Band-Pools**.
3. Klicken Sie auf den Pool, der die notwendigen Bänder enthält und wählen Sie dann die benötigten Bänder.
4. Klicken Sie auf **Bandsatz**.
5. Geben Sie einen Namen für den Bandsatz ein. Wenn für die ausgewählten Bänder bereits ein anderer Bandsatz spezifiziert wurde, wird er überschrieben. Wenn Sie die Bänder von dem Bandsatz ausschließen wollen, ohne einen anderen zu spezifizieren, dann löschen Sie den vorhandenen Bandsatznamen.
6. Klicken Sie auf **Speichern**, um die Änderungen zu übernehmen.

# Storage Nodes

Ein Storage Node ist ein Server, der zur optimalen Nutzung verschiedener Ressourcen (z.B. Storage-Kapazitäten, Netzwerkbandbreiten oder CPU-Last der Produktionsserver) entwickelt wurde, die zur Sicherung der Unternehmensdaten erforderlich sind. Dieses Ziel wird durch Organisation und Verwaltung von Standorten erreicht, die als dedizierte Speicherorte für die Backups des Unternehmens dienen (verwaltete Standorte).

Der Hauptzweck des Acronis Storage Node besteht darin, einen zentralen Zugriff auf Bandlaufwerke bzw. -bibliotheken zu ermöglichen, beispielsweise, um Daten von mehreren Geräten auf demselben Bandlaufwerk oder derselben Bandbibliothek sichern bzw. von diesen wiederherstellen zu können (verwaltetes Depot auf Band).

Ein weiterer Einsatzzweck ist die Nutzung von erweiterten Deduplizierungsfähigkeiten, bei denen Daten über mehrere Geräte hinweg gemeinsam dedupliziert und an einem einzigen Ort gespeichert werden müssen (verwaltetes Depot mit aktivierter Deduplizierung).

## Einen Storage Node und Katalogdienst installieren

Stellen Sie vor der Installation eines Storage Nodes sicher, dass die Maschine die Systemanforderungen erfüllt.

Wir empfehlen, dass Sie Storage Nodes und Katalogdienste auf getrennten Maschinen installieren. Die Systemanforderungen an eine Maschine, auf der ein Katalogdienst läuft, sind im Abschnitt '"Optimale Vorgehensweisen bei der Katalogisierung" (S. 670)' beschrieben.

***So können Sie einen Storage Node und/oder einen Katalogdienst installieren***

1. Melden Sie sich als Administrator an und starten Sie das Acronis Cyber Protect Setup-Programm.
2. [Optional] Wenn Sie die Sprache des Setup-Programms ändern wollen, klicken Sie auf **Sprache einrichten**.
3. Akzeptieren Sie die Bedingungen der Lizenzvereinbarung sowie die Datenschutzerklärung und klicken Sie anschließend auf **Fertigstellen**.
4. Klicken Sie auf **Einen Protection Agenten installieren**.
5. Klicken Sie auf **Installationseinstellungen anpassen**.
6. Klicken Sie neben **Zu installierende Komponenten** auf **Ändern**.
7. Bestimmen Sie, welche Komponenten installiert werden sollen:
   - Wenn Sie einen Storage Node installieren wollen, aktivieren Sie das Kontrollkästchen **Storage Node**. Das Kontrollkästchen **Agent für Windows** wird automatisch ausgewählt.
   - Wenn Sie einen Katalogdienst installieren wollen, aktivieren Sie das Kontrollkästchen **Katalogdienst**.
   - Falls Sie keine anderen Komponenten auf dieser Maschine installieren wollen, deaktivieren Sie die entsprechenden Kontrollkästchen.

Klicken Sie auf **Fertig**, um fortzufahren.

8. Spezifizieren Sie den Management Server, auf dem die Komponenten registriert werden sollen:
   a. Klicken Sie neben **Acronis Cyber Protect Management Server** auf **Spezifizieren**.
   b. Spezifizieren Sie den Host-Namen oder die IP-Adresse derjenigen Maschine, auf welcher der Management Server installiert ist.
   c. Spezifizieren Sie die Anmeldedaten eines Management Server-Administrators oder ein Registrierungstoken.
      Weitere Informationen über die Generierung eines Registrierungstokens finden Sie im Abschnitt '"Schritt 1: Ein Registrierungstoken generieren" (S. 187)'.
   d. Klicken Sie auf **Fertig**.
9. Bestimmen Sie bei Aufforderung, ob die Maschine mit dem Storage Node und/oder Katalogdienst dem Unternehmen oder einer der Abteilungen hinzugefügt werden soll.
   Die Aufforderung erscheint, wenn Sie mehr als eine Abteilung oder ein Unternehmen mit mindestens einer Abteilung verwalten. Anderenfalls wird die Maschine unaufgefordert der von Ihnen verwalteten Abteilung oder dem Unternehmen hinzugefügt. Weitere Informationen finden Sie im Abschnitt 'Administratoren und Abteilungen'.
10. [Optional] Ändern Sie bei Bedarf andere Installationseinstellungen. Informationen dazu finden Sie im Abschnitt 'Installationseinstellungen anpassen'.
11. Klicken Sie auf **Installation**, um mit der Einrichtung fortzufahren.
12. Klicken Sie nach Abschluss der Installation auf **Schließen**.

## Update des Katalogdienstes mit Acronis Cyber Protect 15 Update 4

Acronis Cyber Protect 15 Update 4 verwendet eine neue Version des Katalogdienstes. Die neue Version ist nicht direkt mit den Katalogdaten kompatibel, die von früheren Versionen erstellt wurden.

Während der Aktualisierung auf Acronis Cyber Protect 15 Update 4 können Sie diese Daten manuell auf die neue Version des Katalogdienstes migrieren. Alternativ können Sie die Migration auch überspringen und die Katalogdaten später neu erstellen. Eine Neuerstellung der Katalogdaten nimmt mehr Zeit in Anspruch als ihre Migration.

***So können Sie die Katalogdaten migrieren***

1. Führen Sie auf der Maschine, auf welcher der Katalogdienst installiert ist, das Setup-Programm von Acronis Cyber Protect aus.
2. Akzeptieren Sie die Bedingungen der Lizenzvereinbarung sowie die Datenschutzerklärung und klicken Sie anschließend auf **Fertigstellen**.
3. Aktivieren Sie das Kontrollkästchen **Ich verstehe** und klicken Sie dann auf **Update**.
4. Aktivieren Sie das Kontrollkästchen für die Option **Spezifizieren Sie einen temporären Ordner**.
5. Spezifizieren Sie den Ordner, wohin die Katalogdaten exportiert werden sollen.
   Die exportierte Daten werden verschlüsselt. Der temporäre Ordner wird automatisch gelöscht,

sobald die Migration abgeschlossen wurde.

6. Klicken Sie auf **Fertig**.

***So können Sie die Migration der Katalogdaten überspringen***

1. Führen Sie auf der Maschine, auf welcher der Katalogdienst installiert ist, das Setup-Programm von Acronis Cyber Protect aus.
2. Akzeptieren Sie die Bedingungen der Lizenzvereinbarung sowie die Datenschutzerklärung und klicken Sie anschließend auf **Fertigstellen**.
3. Aktivieren Sie das Kontrollkästchen **Ich verstehe** und klicken Sie dann auf **Update**.
4. Deaktivieren Sie das Kontrollkästchen für die Option **Spezifizieren Sie einen temporären Ordner**.
5. Klicken Sie auf **Fertig**.
6. Bestätigen Sie Ihre Wahl.

Das hat zur Folge, dass die bisherigen Katalogdaten nach der Aktualisierung auf Acronis Cyber Protect 15 Update 4 nicht mehr verfügbar sind. Wenn Sie die Katalogdaten wiederherstellen wollen, müssen Sie ein Backup durchführen.

---

**Hinweis**
Wenn der Katalogdienst, der Storage Node und der Management Server auf unterschiedlichen Maschinen laufen, müssen Sie sicherstellen, dass Sie diese in folgender Reihenfolge auf Acronis Cyber Protect 15 Update 4 aktualisieren:

1. Management Server
2. Storage Node
3. Katalogdienst

---

## Einen verwalteten Speicherort hinzufügen

Ein verwalteter Speicherort kann auf folgenden Storages organisiert werden:

- In einem lokalen Ordner:
  - Auf einem Festplattenlaufwerk, welches lokal an den Storage Node angeschlossen ist
  - Auf einem SAN-Storage, der dem Betriebssystem wie ein lokal angeschlossenes Gerät erscheint
- in einem Netzwerkordner:
  - In einer SMB-/CIFS-Freigabe
  - Auf einem SAN-Storage, der dem Betriebssystem wie ein Netzwerkordner erscheint
  - Auf einem NAS-Gerät
- Auf einem Bandgerät, welches lokal an den Storage Node angeschlossen ist.

Band-basierte Speicherorte werden in Form von Band-Pools erstellt. Standardmäßig ist ein Band-Pool vorhanden. Bei Bedarf können Sie weitere Band-Pools erstellen (wie später in diesem Abschnitt beschrieben).

***So können Sie einen verwalteten Speicherort in einem lokalen Ordner oder Netzwerkordner erstellen***

1. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Klicken Sie zuerst auf **Backup Storage** –> **Speicherort hinzufügen** und dann auf **Storage Node**.
   - Klicken Sie bei Erstellung eines Schutzplans auf **Backup-Ziel** –> **Speicherort hinzufügen** und dann auf **Storage Node**.
   - Klicken Sie auf **Einstellungen** –> **Storage Nodes**, bestimmen Sie den Storage Node, der den Speicherort verwalten soll, und klicken Sie anschließend auf **Speicherort hinzufügen**.
2. Spezifizieren Sie bei **Name** eine eindeutige Bezeichnung für den Speicherort. Eindeutig meinte dabei, dass es kein anderer Speicherort, der vom selben Storage Node verwaltet wird, den gleichen Namen haben darf.
3. [Optional] Wählen Sie den Storage Node, der den Speicherort verwalten soll. Wenn Sie im Schritt 1 die letzte Option auswählen, können Sie den Storage Node nicht mehr ändern.
4. Wählen Sie den Name/die IP-Adresse des Storage Nodes, den/die der Agent verwenden soll, um auf den Speicherort zuzugreifen

   Standardmäßig wird der Name des Storage Nodes vorausgewählt. Sie müssen diese Einstellung möglicherweise ändern, wenn der DNS-Server nicht in der Lage ist, den Namen in die IP-Adresse aufzulösen (wodurch der Zugriff dann fehlschlagen wird). Wenn Sie diese Einstellung zu einem späteren Zeitpunkt ändern wollen, klicken Sie auf **Backup Storage** –> den Speicherort –> **Bearbeiten** und ändern Sie dann den Wert im Feld **Adresse**.
5. Geben Sie den Pfad zum Ordner ein oder wählen Sie den gewünschen Ordner per 'Durchsuchen'.
6. Klicken Sie auf **Fertig**. Die Software überprüft, ob auf den spezifizierten Ordner zugegriffen werden kann.
7. [Optional] Aktivieren Sie die Backup-Deduplizierung für den Speicherort.

   Eine Deduplizierung reduziert den Backup-Datentransfer und die Größe der am Speicherort gesicherten Backups, indem redundante Laufwerksdatenblöcke nur einmalig gespeichert werden.

   Weiter Informationen über Deduplizierungsbeschränkungen finden Sie im Abschnitt 'Deduplizierungsbeschränkungen'.
8. [Nur bei aktivierter Deduplizierung] Spezifizieren oder ändern Sie den Wert des Feldes **Pfad zur Deduplizierungsdatenbank**.

   Dabei muss es sich um einen Ordner oder eine Festplatte handeln, die für den Storage Node lokal verfügbar sind. Zur Verbesserung der System-Performance empfehlen wir, die Deduplizierungsdatenbank und den verwalteten Speicherort auf unterschiedlichen Laufwerken zu erstellen.

Weiter Informationen über die Deduplizierungsdatenbank finden Sie im Abschnitt 'Optimale Vorgehensweisen bei der Deduplizierung'.

9. [Optional] Bestimmen Sie, ob der Speicherort per Verschlüsselung geschützt werden soll. Alle Daten, die zum Speicherort geschrieben werden, werden verschlüsselt – und alle Daten, die von dort gelesenen werden, werden transparent entschlüsselt (unter Verwendung eines Speicherort-spezifischen, auf dem Storage Node hinterlegten Codierungsschlüssels).
   Weitere Informationen zum Thema Verschlüsselung finden Sie im Abschnitt 'Speicherort-Verschlüsselung'.
10. [Optional] Wählen Sie, ob die am Speicherort verwalteten Backups katalogisiert werden sollen. Der Datenkatalog ermöglicht Ihnen, benötigte Versionen von bestimmten Daten leicht zu finden und diese für eine Recovery-Aktion auszuwählen.
    Wenn mehrere Katalogdienste auf dem Management Server registriert sind, können Sie den Dienst auswählen, der die am Speicherort verwalteten Backups katalogisieren soll.
    Die Katalogisierung kann auch zu einem späteren Zeitpunkt aktiviert oder deaktiviert werden. Weitere Informationen dazu finden Sie im Abschnitt 'So können Sie die Katalogisierung (de)aktivieren'.
11. Klicken Sie auf **Fertig**, damit der Speicherort erstellt wird.

***Sie erstellen Sie einen verwalteten Speicherort auf einem Bandgerät***

1. Klicken Sie auf **Backup Storage** –> **Speicherort hinzufügen** – oder klicken Sie bei Erstellung eines Schutzplans auf **Backup-Ziel** –> **Speicherort hinzufügen**.
2. Klicken Sie auf **Bänder**.
3. [Optional] Wählen Sie den Storage Node, der den Speicherort verwalten soll.
4. Befolgen Sie die im Abschnitt 'Einen Pool erstellen' beschriebenen Aktionen (beginnend mit Schritt 4.).

**Hinweis**
Standardmäßig verwenden die Agenten den Namen des Storage Nodes, um auf einen verwalteten bandbasierten Speicherort zuzugreifen. Wenn Sie wollen, dass die Agenten die IP-Adresse des Storage Nodes verwenden sollen, klicken Sie auf **Backup Storage** –> den Speicherort –> **Bearbeiten** und ändern Sie dann den entsprechenden Wert im Feld **Adresse**.

# Deduplizierung

## Deduplizierungsbeschränkungen

### Allgemeine Einschränkungen

Verschlüsselte Backups können nicht dedupliziert werden. Wenn Sie Deduplizierung und Verschlüsselung gleichzeitig verwenden wollen, lassen Sie die Backups unverschlüsselt und leiten Sie zu einem Speicherort, für den sowohl Deduplizierung als auch Verschlüsselung aktiviert sind.

### Backup auf Laufwerksebene

Eine Deduplizierung von Laufwerksdatenblöcken erfolgt nicht, falls die Größe der Zuordnungseinheit des Volumes – auch als Cluster-Größe oder Block-Größe bekannt – nicht durch 4 KB teilbar ist.

**Hinweis**
Die Größe der Zuordnungseinheit der meisten NTFS- und ext3-Volumes beträgt 4 KB. Dies erlaubt also eine Deduplizierung auf Block-Ebene. Andere Größen von Zuordnungseinheiten, die eine Deduplizierung auf Block-Ebene ermöglichen, sind z.B. 8 KB, 16 KB und 64 KB.

### Backup auf Dateiebene

Eine Datei wird nicht dedupliziert, wenn die Datei verschlüsselt ist.

**Deduplizierung und NTFS-Datenströme**

Im NTFS-Dateisystem kann eine Datei mit einem oder mehreren zusätzlichen Datensätzen assoziiert sein – meist (englisch) *Alternate Data Streams* genannt.

Beim Backup einer solchen Datei werden auch all ihre alternativen Datenströme (Alternate Data Streams) mit gesichert. Diese Streams werden jedoch auch dann nie dedupliziert, wenn die Datei selbst es wird.

## Optimale Vorgehensweisen bei der Deduplizierung

Deduplizierung ist ein komplexer Prozess, der von vielen Faktoren abhängt.

Die wichtigsten Faktoren, die die Deduplizierungsgeschwindigkeit beeinflussen, sind:

- Die Zugriffsgeschwindigkeit auf die Deduplizierungsdatenbank
- Die RAM-Kapazität des Storage Nodes
- Die Anzahl der deduplizierenden Speicherorte, die auf dem Storage Node erstellt wurden.

Folgen Sie den unteren Empfehlungen, um die Deduplizierungsperformance zu verbessern.

### Platzieren Sie die Deduplizierungsdatenbank und den deduplizierenden Speicherort auf unterschiedlichen physischen Geräten

Die Deduplizierungsdatenbank enthält Hash-Werte für alle am Speicherort gesicherten Elemente – mit Ausnahme solcher, die nicht dedupliziert werden können (z.B. verschlüsselte Dateien).

Um die Zugriffsgeschwindigkeit auf eine Deduplizierungsdatenbank verbessern zu können, sollten die Datenbank und der Speicherort auf unterschiedlichen physischen Geräten liegen.

Es ist am besten, dem Speicherort und der Datenbank je eigene, dedizierte (also nur für diese Aufgabe bestimmte) Geräte zuzuweisen. Falls dies nicht möglich ist, sollten Sie zumindest weder den Speicherort noch die Datenbank auf ein gemeinsames Laufwerk zusammen mit dem

Betriebssystem legen. Der Grund ist, dass das Betriebssystem häufige Lese-/Schreib-Aktionen auf dem Laufwerk durchführt, was die Deduplizierung deutlich verlangsamen kann.

**Ein Laufwerk für eine Deduplizierungsdatenbank auswählen**

- Die Datenbank muss auf einem fest eingebauten Laufwerk liegen. Versuchen Sie nicht, die Deduplizierungsdatenbank auf ein externes, entfernbares Laufwerk zu legen.
- Um eine niedrige Zugriffszeit für die Datenbank zu gewährleisten, sollten Sie diese auf einem direkt angeschlossenen Laufwerk speichern (statt beispielsweise auf einem Netzwerk-Volume). Eine netzwerkbedingte Latenz kann eine deutliche Reduzierung der Deduplizierungsperformance bewirken.
- Der für eine Deduplizierungsdatenbank erforderliche Speicherplatz kann mit folgender Formel abgeschätzt werden:

$$G = E * 90 / 65536 + 10$$

Wobei:

G die Laufwerksgröße in GB ist,

E die geplante Menge an 'einmaligen' (nur einmal vorkommenden) Daten im Deduplizierungsdatenspeicher in GB ist.

Falls beispielsweise für die geplante Menge der einmaligen Daten im Deduplizierungsdatenspeicher 'E=5 TB' gilt, dann erfordert die Deduplizierungsdatenbank einen freien Speicherplatz mit folgender Größe:

$$G = 5000 * 90 / 65536 +10 = 17 GB$$

**Ein Laufwerk für einen deduplizierenden Speicherort bestimmen**

Zum Schutz gegen Datenverlust empfehlen wir die Verwendung von RAID 10, 5 oder 6. RAID 0 wird nicht empfohlen, da es nicht fehlertolerant ist. RAID 1 ist aufgrund seiner geringen Geschwindigkeit nicht empfehlenswert. Es gibt keine Bevorzugung von lokalen Laufwerken gegenüber SAN, beide sind gut.

## 40 to 160 MB an RAM pro 1 TB an einmaligen Daten

Wenn der Grenzwert erreicht ist, wird die Deduplizierung gestoppt. Backups und Wiederherstellungen sind davon aber nicht direkt betroffen und funktionieren weiterhin. Wenn Sie den Storage Node mit mehr RAM erweitern, wird die Deduplizierung wieder aufgenommen und fortgesetzt. Grundsätzlich gilt: je mehr RAM Sie haben, desto mehr einmalige Daten können Sie speichern.

## Nur ein deduplizierender Speicherort auf jedem Storage Node

Es wird dringend empfohlen, auf einem Storage Node nur je einen deduplizierenden Speicherort zu erstellen. Anderenfalls wird möglicherweise der komplette verfügbare Arbeitsspeicher (RAM) proportional unter den Speicherorten aufgeteilt.

### Applikationen vermeiden, die um Ressourcen konkurrieren

Auf der Maschine mit dem Storage Node sollten keine weiteren Applikationen ausgeführt werden, die viele Systemressourcen benötigen – wie beispielsweise Datenbankverwaltungssysteme (DBMS) oder Enterprise Resource Planning-Systeme (ERP).

### Ein Mehrkern-Prozessor mit einer Taktrate von mindestens 2,5 GHz

Wir empfehlen die Verwendung eines Prozessors mit wenigstens vier Kernen und einer Taktfrequenz nicht unter 2,5 GHz.

### Ausreichend freier Speicherplatz für den Speicherort

Für eine Deduplizierung am Ziel ist genauso viel freier Speicherplatz erforderlich, wie die gesicherten Daten belegen, direkt nachdem diese zum Speicherort geschrieben wurden. Ohne Komprimierung oder Deduplizierung an der Quelle entspricht dieser Wert der Größe der ursprünglich gesicherten Daten während einer gegebenen Backup-Aktion.

### High-Speed LAN

1-Gbit-LAN wird empfohlen. Dadurch kann die Software 5-6 Backups mit Deduplizierung parallel durchführen, ohne dass die Geschwindigkeit deutlich heruntergeht.

### Backup einer typischen Maschine, bevor Sie mehrere Maschinen mit ähnlichem Inhalt sichern

Wenn Sie mehrere Maschinen mit ähnlichem Inhalt sichern wollen, empfiehlt es sich, zuerst nur das Backup einer Maschine zu erstellen und dann zu warten, bis die Indizierung der gesicherten Daten abgeschlossen ist. Danach werden die Backups der anderen Maschinen schneller verlaufen, was der effizienten Deduplizierung zu verdanken ist. Da das Backup der ersten Maschine bereits indiziert wurde, befinden sich die meisten Daten bereits im Deduplizierungsdatenspeicher.

### Backups von verschiedenen Maschinen zu unterschiedlichen Zeiten

Falls Sie eine größere Anzahl an Maschinen sichern wollen, sollten Sie die Backup-Aktionen zeitlich verteilen. Erstellen Sie dazu mehrere Schutzpläne mit unterschiedlichen Planungen.

## Speicherort-Verschlüsselung

Wenn Sie einen Speicherort durch Verschlüsselung schützen, werden alle zu diesem Speicherort geschriebenen Daten verschlüsselt – und alle von dort gelesenen Daten durch den Storage Node wieder transparent entschlüsselt (unter Verwendung eines Speicherort-spezifischen, auf dem Storage Node hinterlegten Codierungsschlüssels). Falls das Speichermedium gestohlen wird oder eine unbefugte Person darauf zugreift, wird der Übeltäter den Inhalt des Speicherortes ohne Zugriff auf den Storage Node nicht entschlüsseln können.

Diese Verschlüsselung hat nichts mit der üblichen Verschlüsselung von Backups zu tun, die über einen Schutzplan spezifiziert und durch einen Agenten ausgeführt wird. Sollte ein Backup bereits verschlüsselt sein, so wird die Verschlüsselung aufseiten des Storage Nodes noch einmal über die durch den Agenten ausgeführte Verschlüsselung quasi drübergelegt.

***So schützen Sie einen Speicherort per Verschlüsselung***

1. Spezifizieren (und bestätigen) Sie ein Kennwort, welches zur Generierung des Codierungsschlüssels werden soll.

   Beim Kennwort wird nach Groß-/Kleinschreibung unterschieden. Das Kennwort wird nur abgefragt, wenn Sie den Speicherort an einen anderen Storage Node anschließen.
2. Wählen Sie einen der folgenden Verschlüsselungsalgorithmen:
   - **AES 128** – die Inhalte des Speicherortes werden mit dem AES-Algorithmus (Advanced Encryption Standard) und einer Tiefe von 128 Bit verschlüsselt.
   - **AES 192** – die Inhalte des Speicherortes werden mit dem AES-Algorithmus und einer Tiefe von 192 Bit verschlüsselt.
   - **AES 256** – die Inhalte des Speicherortes werden mit dem AES-Algorithmus und einer Tiefe von 256 Bit verschlüsselt.
3. Klicken Sie auf **OK**.

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 höher die Schlüsselgröße, desto länger wird das Programm zur Verschlüsselung der am Speicherort gesicherten Backups benötigen, aber desto sicherer sind die Daten dann auch.

Der Codierungsschlüssel wird dann mit AES-256 verschlüsselt, wobei ein SHA-256-Hash-Wert des gewählten Kennworts als Schlüssel dient. Das Kennwort selbst wird nirgendwo auf dem Laufwerk gespeichert, es wird nur der Kennwort-Hash-Wert für Bestätigungszwecke verwendet. Mit dieser zweistufigen Methode sind die Backups vor jedem unberechtigten Zugriff geschützt, aber ein verlorenes Kennwort kann unmöglich wiederhergestellt werden.

# Katalogisierung

## Datenkatalog

Der Datenkatalog ermöglicht Ihnen, benötigte Versionen von bestimmten Daten leicht zu finden und diese für eine Recovery-Aktion auszuwählen. Der Datenkatalog zeigt die Daten an, die in verwalteten Speicherorten, für die eine Katalogisierung aktiviert ist oder war, vorliegen.

Der Fensterbereich **Katalog** wird nur dann in der Registerkarte **Backup Storage** angezeigt, wenn auf dem Management Server mindestens ein Katalogdienst registriert ist. Informationen zur Installation des Katalogdienstes finden Sie im Abschnitt 'Einen Storage Node und Katalogdienst installieren'.

Der Fensterbereich **Katalog** ist nur für Organisationsadministratoren sichtbar.

## Einschränkungen

Nur Laufwerk- und Datei-Backups von physischen Maschinen sowie Backups von virtuellen Maschinen können katalogisiert werden.

Folgende Daten können nicht im Katalog angezeigt werden:

- Daten aus verschlüsselten Backups
- Daten, die auf Bandgeräte gesichert wurden
- Daten, die in den Cloud Storage gesichert wurden
- Daten, die mithilfe früherer Versionen von Acronis Cyber Protect (älter als Version 12.5) erstellt wurden.

## Gespeicherte Daten für eine Recovery-Aktion auswählen

1. Klicken Sie auf **Backup Storage** –> **Katalog**.
2. Wenn mehrere Katalogdienste auf dem Management Server registriert sind, wählen Sie den Dienst aus, der die am Speicherort verwalteten Backups katalogisiert.

   **Hinweis**
   Um einzusehen, welcher Dienst einen Speicherort katalogisiert, müssen Sie den entsprechenden Speicherort bei **Backup Storage** –> **Speicherorte** –> **Speicherorte** auswählen und anschließend auf **Details** klicken.

3. Die Software zeigt als die Maschinen an, die zu den verwalteten Speicherorten gesichert wurden, welche wiederum von dem ausgewählten Katalogdienst katalogisiert werden.
   Wählen Sie die Daten, die Sie wiederherstellen wollen, mithilfe der Funktion 'Durchsuchen' aus oder indem Sie die Suchfunktion verwenden.
   - **Durchsuchen**
     Klicken Sie doppelt auf eine Maschine, um die gesicherten Laufwerke, Volumes, Ordner und Dateien einsehen zu können.
     Wenn Sie ein Laufwerk wiederherstellen wollen, wählen das Laufwerk aus, welches mit dem folgenden Symbol gekennzeichnet ist: 
     Wenn Sie ein Volume wiederherstellen wollen, müssen Sie zuerst doppelt auf das Laufwerk klicken, welches das Volume enthält. Anschließend können Sie das Volume auswählen.
     Wenn Sie Dateien/Ordner wiederherstellen wollen, müssen Sie das Volume durchsuchen, in dem sich die Dateien/Ordner befinden. Sie können die Volumes durchsuchen, die mit dem folgenden Symbol gekennzeichnet sind: 
   - **Suchen**

Geben Sie im Suchfeld diejenigen Informationen ein, die Ihnen helfen, die benötigten Datenelemente (das kann ein Maschinenname, ein Ordnername oder eine Laufwerksbezeichnung sein) zu identifizieren – und klicken Sie dann auf den Befehl **Suchen**.

Sie können Platzhalterzeichen (* und ?) verwenden.

Als Suchergebnis wird Ihnen eine Liste mit allen gesicherten Datenelementen angezeigt, deren Namen komplett oder teilweise mit dem eingegebenen Wert übereinstimmt.

4. Die Daten werden standardmäßig auf den spätestmöglichen (neuesten) Zeitpunkt zurückgesetzt. Wenn Sie ein einzelnes Element ausgewählt haben, können Sie die Schaltfläche **Versionen** verwenden, um einen bestimmten Zeitpunkt (Recovery-Punkt) auszuwählen.
5. Gehen Sie nach Auswahl der gewünschten Daten folgendermaßen vor:
   - Klicken Sie auf **Recovery** und konfigurieren Sie anschließend die Parameter der Wiederherstellungsaktion wie im Abschnitt ''Recovery' beschrieben.
   - [Nur bei Dateien/Ordnern] Wenn Sie die Dateien als .zip-Archiv speichern wollen, müssen Sie zuerst auf **Download** klicken, dann den Zielspeicherort wählen und abschließend auf **Speichern** klicken.

## Optimale Vorgehensweisen bei der Katalogisierung

Folgen Sie den unteren Empfehlungen, um die Katalogisierungsperformance zu verbessern.

### Installation

Wir empfehlen, dass Sie Katalogdienste und Storage Nodes auf getrennten Maschinen installieren. Ansonsten werden diese Komponenten um CPU- und RAM-Ressourcen konkurrieren.

Wenn mehrere Storage Nodes auf einem Management Server registriert sind, reicht ein Katalogdienst zumeist aus – außer die Indizierungs- oder Suchperformance nimmt zu stark ab. Wenn Sie beispielsweise feststellen, dass die Katalogisierung ständig arbeitet (es also keinerlei Pausen mehr zwischen den Katalogisierungsaktivitäten gibt), sollten Sie einen zusätzlichen Katalogdienst auf einer weiteren, separaten Maschine installieren. Entfernen Sie dann einige der verwalteten Speicherorte und erstellen Sie diese mit dem zusätzlichen Katalogdienst neu. Die an diesen Speicherorten vorliegenden Backups sind davon nicht betroffen und bleiben intakt.

### Systemanforderungen

| Parameter | Minimalwert | Empfohlener Wert |
|---|---|---|
| Anzahl der CPU-Kerne | 2 | 4 und mehr |
| RAM | 8 GB | 16 GB und mehr |
| Festplatte | HDD mit 7200 U/min (RPM) | SSD |
| Netzwerkverbindung zwischen der Maschine mit dem Storage Node und der Maschine mit dem Katalogdienst | 100 Mbit/s | 1 Gbit/s |

## So können Sie die Katalogisierung (de)aktivieren

Wenn für einen verwalteten Speicherort die Katalogisierungsfunktion aktiviert ist, wird der Inhalt eines jeden Backups, welches diesen Speicherort als Backup-Ziel verwendet, dem Datenkatalog hinzugefügt – und zwar, sobald das Backup erstellt wurde.

Sie können die Katalogisierung aktivieren, wenn Sie einen verwalteten Speicherort hinzufügen – oder dies auch zu einem späteren Zeitpunkt nachholen. Sobald die Katalogisierung aktiviert ist, werden alle Backups katalogisiert, die am Speicherort vorliegen und nicht zuvor katalogisiert wurden, sobald das nächste Backup zu diesem Speicherort erfolgt.

Der Katalogisierungsprozess kann zeitaufwendig sein, insbesondere wenn eine große Anzahl von Maschinen zu demselben Speicherort gesichert werden. Sie können die Katalogisierung jederzeit deaktivieren. Die Katalogisierung von Backups, die vor der Deaktivierung erstellt wurden, wird fertiggestellt. Neu erstellte Backups werden nicht katalogisiert.

***So können Sie die Katalogisierung für einen vorhandenen Speicherort konfigurieren***

1. Klicken Sie auf **Backup Storage** –> **Speicherorte**.
2. Klicken Sie auf **Speicherorte** und wählen Sie dann den verwalteten Speicherort aus, für den Sie die Katalogisierung konfigurieren wollen.
3. Klicken Sie auf **Bearbeiten**.
4. Aktivieren oder deaktivieren Sie den Schalter für den **Katalogdienst**.
5. Klicken Sie auf **Fertig**.

# Systemeinstellungen

Diese Einstellungen sind nur bei On-Premise-Bereitstellungen verfügbar.

Klicken Sie auf **Einstellungen** –> **Systemeinstellungen**, um auf diese Optionen zugreifen zu können.

Der Fensterbereich **Systemeinstellungen** ist nur für Organisationsadministratoren sichtbar.

## E-Mail-Benachrichtigungen

Sie können globalen Einstellungen konfigurieren, die dann für alle E-Mail-Benachrichtungen gelten, die vom Management Server gesendet werden.

Sie können diese Einstellungen in den Standardoptionen für Backups für alle Ereignisse überschreiben, die bei Backup-Aktionen auftreten. In diesem Fall gelten die globalen Einstellungen weiterhin für alle anderen Aktionen – außer für Backups (die dann ihre eigenen Einstellungen haben).

Wenn Sie einen Schutzplan erstellen, können Sie wählen, welche der Einstellungen verwendet werden sollen: die globalen Einstellungen oder die Einstellungen, die in den 'Standardoptionen für Backups' festgelegt wurden. Sie können diese auch mit benutzerdefinierten Werten überschreiben, die nur für den Plan spezifisch sind.

**Wichtig**
Wenn die globalen Einstellungen für E-Mail-Benachrichtigungen geändert werden, sind davon alle Schutzpläne betroffen, die die globalen Einstellungen verwenden.

Überprüfen Sie beim Konfigurieren der Einstellungen, dass die **E-Mail-Server**-Einstellungen konfiguriert werden.

***So konfigurieren Sie die globalen Einstellungen für E-Mail-Benachrichtigungen***

1. Klicken Sie auf **Einstellungen** –> **Systemeinstellungen** –> **E-Mail-Benachrichtigungen**.
2. Geben Sie im Feld **E-Mail-Adressen der Empfänger** die Ziel-E-Mail-Adressen ein. Sie können mehrere Adressen eingeben, müssen diese aber je per Semikolon trennen.
3. [Optional] Ändern Sie bei **Betreff** den Inhalt der Betreffzeile für die E-Mail-Benachrichtigungen.
   Sie können dafür folgende Variablen verwenden:
   - `[Alert]` – Alarmübersicht
   - `[Device]` – Gerätename.
   - `[Plan]` – der Name des Plans, der den Alarm generiert hat.
   - `[ManagementServer]` – der Host-Name der Maschine, auf welcher der Management Server installiert ist.
   - `[Unit]` – der Name der Abteilung, zu welcher die Maschine gehört.

   Die Standard-Betreffszeile für Benachrichtigungen lautet: `[Alert]` **Gerät:** `[Device]` **Plan:** `[Plan]`

4. [Optional] Aktivieren Sie das Kontrollkästchen **Tägliche Zusammenfassung über aktive Alarmmeldungen** – und gehen Sie dann folgendermaßen vor:
   a. Spezifizieren Sie den Zeitpunkt, wann die Zusammenfassung versendet werden soll.
   b. [Optional] Aktivieren Sie das Kontrollkästchen **Nachrichten mit 'Keine aktiven Alarmmeldungen' nicht senden**.
5. [Optional] Bestimmen Sie die Sprache, die in den E-Mail-Benachrichtigungen verwendet werden soll.
6. Aktivieren Sie die Kontrollkästchen für diejenigen Ereignisse, zu denen Sie Benachrichtigungen erhalten wollen. Sie können aus einer Liste aller Alarmmeldungen auswählen, die auftreten können (nach Schweregrad gruppiert).
7. Klicken Sie auf **Speichern**.

# E-Mail-Server

Sie können einen E-Mail-Server spezifizieren, der verwendet wird, um E-Mail-Benachrichtigungen vom Management Server zu versenden.

***So spezifizieren Sie den E-Mail-Server***

1. Klicken Sie auf **Einstellungen** –> **Systemeinstellungen** –> **E-Mail-Server**.
2. Wählen Sie bei **E-Mail-Dienst** einen der folgenden Anbieter:
   - **Benutzerdefiniert**
   - **Gmail**
   - **Yahoo Mail**
   - **Outlook.com**
3. [Nur bei einem benutzerdefinierten E-Mail-Dienst] Spezifizieren Sie folgende Einstellungen:
   - Geben Sie bei **SMTP-Server** den Namen des Postausgangsservers (SMTP) ein.
   - Legen Sie bei **SMTP-Port** den Port für den Postausgangsserver fest. Standardmäßig ist der Port 25 festgelegt.
   - Bestimmen Sie, ob eine SSL- oder TSL-Verschlüsselung verwendet werden soll. Wählen Sie **Ohne**, um die Verschlüsselung zu deaktivieren.
   - Falls der SMTP-Server eine Authentifizierung erfordert, aktivieren Sie das Kontrollkästchen **SMTP-Server erfordert Authentifizierung** und spezifizieren Sie dann die Anmeldedaten eines Kontos, welches zum Versenden der Nachrichten verwendet werden soll. Falls Sie nicht sicher sind, ob Ihr SMTP-Server eine Authentifizierung erfordert, dann kontaktieren Sie Ihren Netzwerkadministrator oder bitten Sie Ihren E-Mail-Dienstanbieter um Hilfe.
4. [Nur für Gmail, Yahoo Mail und Outlook.com] Spezifizieren Sie die Anmeldedaten eines Kontos, welches zum Versenden der Nachrichten verwendet werden soll.
5. [Nur bei einem benutzerdefinierten E-Mail-Dienst] Geben Sie bei **Absender** ein, welcher Name als Absender angezeigt werden soll. Dieser Name wird im Feld **Von** der E-Mail-

Benachrichtigungen (beim Empfänger) angezeigt. Falls Sie das Feld leer lassen, wird in den Nachrichten hier das Konto angezeigt, welches Sie in Schritt 3 oder 4 angegeben haben.

6. [Optional] Klicken Sie auf **Testnachricht senden**, um zu überprüfen, ob die E-Mail-Benachrichtigungen mit den spezifizierten Einstellungen korrekt funktionieren. Geben Sie eine E-Mail-Adresse an, an welche die Testnachricht gesendet werden soll.

# Sicherheit

Verwenden Sie diese Optionen, um die Sicherheit zu erhöhen, wenn Sie Acronis Cyber Protect mit einer On-Premise-Bereitstellung verwenden.

## Inaktive Benutzer abmelden nach:

Mit dieser Option können Sie eine Zeitüberschreitung zur automatischen Abmeldung festlegen, wenn ein Benutzer zu lange inaktiv war. Wenn noch eine Minute der festgelegten Zeitüberschreitung übrig ist, wird der Benutzer von der Software gefragt, ob er angemeldet bleiben möchte. Wenn er weiterhin nicht reagiert, wird der Benutzer abgemeldet und alle nicht gespeicherten Änderungen gehen verloren.

Die Voreinstellung ist: **Aktiviert. Zeitlimit. 10 Minuten.**

## Benachrichtigung über die letzte Anmeldung des aktuellen Benutzers anzeigen

Mit dieser Option können folgende Informationen angezeigt werden: der Zeitpunkt der letzten erfolgreichen Anmeldung des Benutzers, die Anzahl der Authentifizierungsfehler seit der letzten erfolgreichen Anmeldung und die IP-Adresse der letzten erfolgreichen Anmeldung. Die Informationen werden bei jeder Anmeldung des Benutzers am unteren Bildschirmrand angezeigt.

Die Voreinstellung ist: **Deaktiviert**.

## Bei Ablauf des lokalen oder Domain-Kennworts warnen

Mit dieser Option wird angezeigt, wann das Kennwort abläuft, mit dem der Benutzer auf Acronis Cyber Protect Management Server zugreifen kann. Es handelt sich um das lokale Kennwort oder das Domain-Kennwort, mit dem sich der Benutzer an der Maschine anmeldet, auf welcher der Management Server installiert ist. Die verbleibende Zeit bis zum Kennwortablauf wird unten auf dem Bildschirm und rechts oben im Konto-Menü angezeigt.

Die Voreinstellung ist: **Deaktiviert**.

# Updates

Diese Option bestimmt, ob Acronis Cyber Protect jedes Mal, wenn sich ein Organisationsadministrator an der Cyber Protect Webkonsole anmeldet, nach einer neuen Version sucht.

Die Voreinstellung ist: **Aktiviert**.

Wenn diese Option deaktiviert ist, kann der Administrator – wie im Abschnitt 'Auf Software-Updates prüfen' beschrieben – manuell nach Updates suchen.

# Standardoptionen für Backup

Die Standardwerte der Backup-Optionen gelten für alle Schutzpläne auf dem Management Server. Ein Organisationsadministrator kann einen Standardoptionswert gegen einen vordefinierten Wert ersetzen. Der neue Wert wird dann als Vorgabe in allen Schutzplänen verwendet, die nach Durchführung der Änderung 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. Melden Sie sich an der Cyber Protect Webkonsole als Organisationsadministrator an.
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**.

# Schutzeinstellungen

Wenn Sie die Schutzeinstellungen konfigurieren wollen, gehen Sie in der für Cyber Protect-Webkonsole zu **Einstellungen** –> **Schutz**.

Wenn Sie weitere Informationen zu bestimmten Einstellungen und Prozeduren benötigen, informieren Sie sich bitte unter dem entsprechenden Thema in diesem Abschnitt.

## Die Schutzdefinitionen aktualisieren

Standardmäßig können sich alle Protection Agenten mit dem Internet verbinden und Updates für folgende Komponenten herunterladen:

- Antimalware
- Schwachstellenbewertung
- Patch-Verwaltung

### Agenten mit der Updater-Rolle

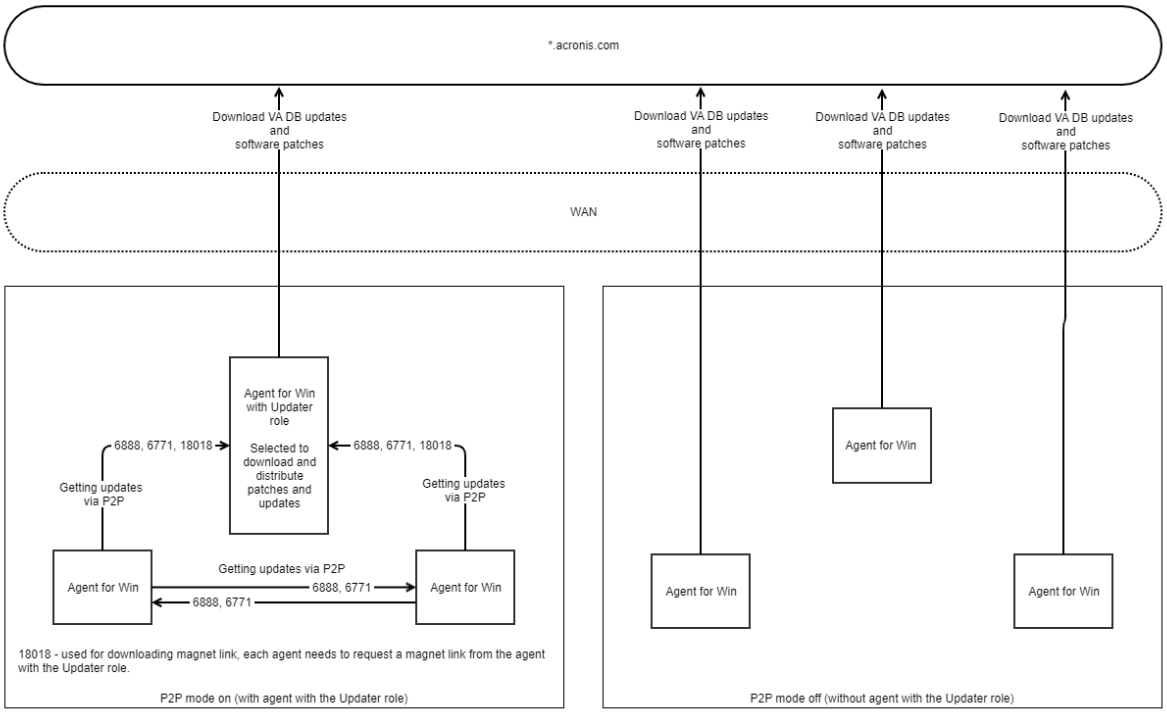
Ein Administrator kann die Bandbreite des Netzwerkverkehrs minimieren, indem er einen oder mehrere Agenten in der Umgebung auswählt und diesen die Updater-Rolle zuweist. Dadurch werden sich die dedizierten Agenten mit dem Internet verbinden und die Updates herunterladen. Alle anderen Agenten werden sich mithilfe der Peer-zu-Peer-Technologie mit den dedizierten Updater-Agenten verbinden und dann die Updates von diesen herunterladen.

Die Agenten ohne die Updater-Rolle werden sich mit dem Internet verbinden, wenn kein dedizierter Updater-Agent in der Umgebung vorhanden ist – oder wenn die Verbindung zu einem dedizierten Updater-Agenten für ca. fünf Minuten nicht hergestellt werden konnte.

Bevor Sie einem Agenten die Updater-Rolle zuweisen, sollten Sie sicherstellen, dass die Maschine mit diesem Agenten ausreichend leistungsfähig ist, einen stabilen und schnellen Internetzugang hat und über genügend freien Speicherplatz verfügt.

Sie können die Updater-Rolle mehreren Agenten in der Umgebung zuweisen. Wenn dann ein Agent mit der Updater-Rolle offline ist, können andere Agenten mit dieser Rolle als Quelle für die aktualisierten Schutzdefinitionen dienen.

Das nachfolgende Diagramm verdeutlicht die Möglichkeiten beim Herunterladen von Schutz-Updates. Auf der linken Seite wird einem Agenten die Updater-Rolle zugewiesen. Dieser Agent verbindet sich mit dem Internet, um die Schutz-Updates herunterzuladen. Dessen Peer-Agenten verbinden sich wiederum mit dem Updater-Agenten, um die neuesten Updates zu erhalten. Auf der rechten Seite ist keinem Agenten die Rolle Updater zugewiesen. Daher verbinden sich alle Agenten selbst mit dem Internet, um die Schutz-Updates herunterzuladen.




***So können Sie eine Maschine für die Updater-Rolle vorbereiten***

1. Wenden Sie auf der Maschine, auf der ein Agent mit der Updater-Rolle ausgeführt werden soll, folgende Firewall-Regeln an:
   - Eingehend (ankommend) "updater_incoming_tcp_ports": erlaube die Verbindung zu den TCP-Ports 18018 und 6888 für alle Firewall-Profile (öffentlich, privat und Domain).
   - Eingehend (ankommend) "updater_incoming_udp_ports": erlaube die Verbindung zu den UDP-Ports 6888 für alle Firewall-Profile (öffentlich, privat und Domain).
2. Starten Sie den Dienst 'Acronis Agent Core Service' neu.
3. Starten Sie den Firewall-Dienst neu.

Wenn Sie diese Regeln nicht anwenden und die Firewall aktiviert ist, werden die Peer-Agenten die Updates aus der Cloud heruntergeladen.

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

1. Gehen Sie in der Cyber Protect Webkonsole zu **Einstellungen** –> **Agenten**.
2. Wählen Sie die Maschine mit demjenigen Agenten aus, dem Sie die Updater-Rolle zuweisen wollen.
3. Klicken Sie auf **Details** und aktivieren Sie dann den Schalter **Diesen Agenten verwenden, um Patches und Updates herunterzuladen und zu verteilen**.

# Updates planen

Sie können entweder eine automatische Aktualisierung der Schutzdefinitionen auf allen Agenten planen oder die Aktualisierung auf ausgewählten Agenten manuell vornehmen.

***So können Sie automatische Updates planen***

1. Gehen Sie in der Cyber Protect-Webkonsole zu **Einstellungen** –> **Schutz** –> **Update der Schutzdefinitionen**.
2. Wählen Sie **Planung**.
3. Wählen Sie bei **Planungstyp** eine der folgenden Möglichkeiten:
   - **Täglich**

     Bestimmen Sie die Wochentage, an denen die Schutzdefinitionen aktualisiert werden sollen.

     Wählen Sie bei **Starten um**, den Zeitpunkt, an dem die Aktualisierungen beginnen soll.
   - **Stündlich**

     Legen Sie eine genauere Planung für die Aktualisierungen fest.

     Definieren Sie bei **Ausführen alle/jede(n)** eine Periodizität für die Aktualisierungen.

     Definieren Sie über **Von** ... **Bis** einen bestimmten Zeitraum für die Aktualisierungen.

***So können Sie die Schutzdefinitionen manuell aktualisieren***

1. Gehen Sie in der Cyber Protect Webkonsole zu **Einstellungen** –> **Agenten**.
2. Wählen Sie die Maschinen aus, für deren Agenten Sie die Schutzdefinitionen aktualisieren wollen, und klicken Sie dann auf **Definitionen aktualisieren**.

# Den Download-Speicherort ändern

Die Schutzdefinitionen werden in den standardmäßigen Ordner für temporäre Dateien auf Ihrer Maschine heruntergeladen und dann im Programmordner von Acronis gespeichert.

***So können Sie den temporären Ordner für den Download ändern***

1. Öffnen Sie auf der Maschine mit dem Management Server die Datei `atp-database-mirror.json` zur Bearbeitung.

   Sie können diese Datei an folgenden Speicherorten finden:
   - Windows: `%programdata%\Acronis\AtpDatabaseMirror\`
   - Linux: `/var/lib/Acronis/AtpDatabaseMirror/`
2. Ändern Sie den Wert für `"enable_user_config"` auf `true`.

```
{
"sysconfig":
{
...
"enable_user_config": true
```

```
}
...
}
```

3. Öffnen Sie auf der Maschine mit dem Management Server die Datei `config.json` zur Bearbeitung.
   Sie können diese Datei an folgenden Speicherorten finden:
   - Windows: `%programdata%\Acronis\AtpDatabaseMirror\`
   - Linux: `/var/lib/Acronis/AtpDatabaseMirror/`
4. Fügen Sie folgende Zeile hinzu: `"mirror_temp_dir": "<Pfad_zum_neuen_Download_Speicherort>"`
   Zum Beispiel:

   ```
   {
           "mirror_temp_dir": "C:\\temp"
   }
   ```

   Der Pfad kann absolut oder relativ zum Ordner `AppData` sein.
   Wenn der Ordner nicht erstellt werden kann oder der Management Server keine Schreibrechte für das ausgewählte Verzeichnis hat, wird wieder der Standardspeicherort verwendet.

# Cache Storage-Optionen

Die zwischengespeicherten Daten werden an folgenden Orten gespeichert:

- Windows: `C:\ProgramData\Acronis\Agent\var\atp-downloader\Cache`
- Linux: `/opt/acronis/var/atp-downloader/Cache`
- macOS: `/Library/Application Support/Acronis/Agent/var/atp-downloader/Cache`

Sie können eine Planung zur Bereinigung veralteter Cache-Daten konfigurieren und einen Grenzwert für deren Größe festlegen. Sie können verschiedene Grenzwerte für Maschinen mit Nicht-Updater-Agenten und Maschinen mit Updater-Agenten festlegen.

# Die Quelle für die neuesten Schutzdefinitionen

Folgende Quellen können für das Herunterladen der neuesten Schutzdefinitionen verwendet werden:

- **Die Cloud**
  Die Protection Agenten verbinden sich mit dem Internet und laden die neuesten Schutzdefinitionen aus der Acronis Cloud herunter. Standardmäßig suchen alle Agenten, die auf dem Management Server registriert sind, nach Updates und verteilen diese. Weitere Informationen über Agenten mit der Updater-Rolle finden Sie im Abschnitt '"Die Schutzdefinitionen aktualisieren" (S. 676)'.
- **Cyber Protect Management Server**

Bei dieser Option benötigen die Agenten keinen Zugriff auf das Internet. Sie verbinden sich nur mit dem Management Server, auf dem die Schutzdefinitionen gespeichert sind. Jedoch muss der Management Server mit dem Internet verbunden sein, um selbst die neuesten Schutzdefinitionen herunterladen zu können.

- **Benutzerdefinierte Webserver**

  Diese Option ist für Fehlerbehebungen, zu Testzwecken oder für den Einsatz in Air-Gap-Umgebungen vorgesehen. Weitere Informationen dazu finden Sie im Abschnitt '"Die Schutzdefinitionen in einer Air-Gap-Umgebung aktualisieren" (S. 680)'. Sie müssen diese Option normalerweise nur dann auswählen, wenn Sie vom Acronis Support dazu aufgefordert werden.

# Remote-Verbindung

Wenn Sie die Remote-Verbindung aktivieren, werden in der Cyber Protect-Webkonsole unter **Cyber Protection Desktop** im rechtsliegenden Menü die Optionen **Über RDP-Client verbinden** und **Über HTML5-Client verbinden** angezeigt. Das rechtsliegende Menü wird geöffnet, wenn Sie einen Workload auf der Registerkarte **Geräte** auswählen.

Wenn Sie die Remote-Verbindung aktivieren oder deaktivieren, wirkt sich dies auf alle Anwender in Ihrer Organisation aus.

***So können Sie die Remote-Verbindung aktivieren***

1. Gehen Sie in der Cyber Protect Webkonsole zu **Einstellungen** –> **Schutz**.
2. Klicken Sie auf **Remote-Verbindung** und aktivieren Sie den Schalter **Remote-Desktop-Verbindung**.

Außerdem können Sie die Freigabe der Remote-Verbindung aktivieren. Mit dieser Option können Sie einen Link generieren, der einen Remote Zugriff auf den ausgewählten Workload ermöglicht. Sie können diese Links dann mit anderen Nutzern teilen.

***So können Sie die Freigabe von Remote-Verbindungen aktivieren***

1. Gehen Sie in der Cyber Protect Webkonsole zu **Einstellungen** –> **Schutz**.
2. Aktivieren Sie das Kontrollkästchen **Remote-Desktop-Verbindung freigeben**.

Daraufhin wird in der Cyber Protect-Webkonsole unter **Cyber Protection Desktop** im rechtsliegenden Menü die Option **Remote-Verbindung freigeben** angezeigt.

# Die Schutzdefinitionen in einer Air-Gap-Umgebung aktualisieren

Acronis Cyber Protect unterstützt eine Aktualisierung der Schutzdefinitionen in Air-Gap-Umgebungen.

***So können Sie die Schutzdefinitionen in einer Air-Gap-Umgebung aktualisieren***

1. Installieren Sie außerhalb Ihrer Air-Gap-Umgebung einen zweiten Management Server, der Zugriff auf das Internet hat.
   Weitere Informationen über die entsprechende Durchführung finden Sie im Abschnitt '"Den Management Server installieren" (S. 87)'.
2. Kopieren Sie die Schutzdefinitionen von dem Management Server, der online ist, zuerst auf ein Wechsellaufwerk – und übertragen Sie die Definitionen dann auf einen HTTP-Server in der Air-Gap-Umgebung.
   Weitere Informationen zu diesem Schritt finden Sie in den Abschnitten '"Die Definitionen auf einen Online Management-Server herunterladen" (S. 681)' und '"Die Definitionen an einen HTTP-Server übertragen" (S. 682)'.
3. Konfigurieren Sie auf dem per Air-Gap abgesicherten Management Server den HTTP-Server als Quelle für aktualisierte Schutzdefinitionen.
   Weitere Informationen zu diesem Schritt finden Sie im Abschnitt '"Die Quelle für Definitionen auf einem per Air-Gap abgesicherten Management Server konfigurieren" (S. 683)'.

## Die Definitionen auf einen Online Management-Server herunterladen

aden Sie nach der Installation eines zweiten Management Servers, der auf das Internet zugreifen kann, die neuesten Schutzdefinitionen herunter und kopieren Sie diese auf ein Wechsellaufwerk (wie z.B. einen USB-Stick oder eine externe Festplatte).

***können Sie die Schutzdefinitionen herunterladen und kopieren***

1. Kopieren Sie auf der Maschine mit dem Online Management Server den Ordner `AtpDatabaseMirror` zu einem Ort Ihrer Wahl – beispielsweise auf den Desktop oder in den `Temp`-Ordner.
   Sie können den Ordner `AtpDatabaseMirror` an folgenden Speicherorten finden:
   - Windows: `%ProgramData%\Acronis\`
   - Linux: `/usr/lib/Acronis/`
2. Öffnen Sie die Datei `atp_database_mirror.json` zur Bearbeitung. Sie können die Datei an folgenden Speicherorten finden:
   - Windows: `%Program Files%\Acronis\AtpDatabaseMirror`

     **Hinweis**
     Unter Windows ist dieser Ordner nicht mit dem Ordner aus dem vorherigen Schritt identisch.

   - Linux: `/usr/lib/Acronis/AppDatabaseMonitor`
3. Gehen Sie folgendermaßen vor, um die Datei `atp_database_mirror.json` zu bearbeiten:
   a. Ändern Sie den Wert `"enable_appdata_as_root"` zu `false`.
   b. Ändern Sie die Werte aller Einträge von `"local_path"` zu dem absoluten Pfad des Ortes, wo Sie die Schutzdefinitionen speichern wollen.

4. Speichern Sie die Änderungen in der Datei `atp_database_mirror.json`.
5. Stoppen Sie auf der Maschine mit dem Online Management Server den Dienst **Acronis Management Server** mit folgendem Befehl:
   - Windows (Eingabeaufforderung):
     ```
     sc stop AcrMngSrv
     ```
   - Linux (Terminal):
     ```
     sudo systemctl stop acronis_ams.service
     ```
6. Starten Sie im Ordner `AtpDatabaseMirror`, den Sie zu einem Speicherort Ihrer Wahl kopiert haben, das Tool `AtpDatabaseMirror` mit folgendem Befehl:
   - Windows (Eingabeaufforderung):
     ```
     atp_database_mirror.exe -config atp_database_mirror.json
     ```
   - Linux (Terminal):
     ```
     sudo ./atp_database_mirror -config atp_database_mirror.json
     ```

   Wenn alle Updates zu dem Ordner heruntergeladen wurden, den Sie unter `"local_path"` spezifiziert haben, wird folgende Zeile in der Eingabeaufforderung oder im Terminal-Fenster angezeigt:
   ```
   standing by for 1m0s
   ```
7. Beenden Sie das Tool `AtpDatabaseMirror` durch Drücken der Tastenkombination STRG+C.
8. Kopieren Sie die Dateien aus dem Ordner, den Sie unter `"local_path"` spezifiziert haben, auf ein Wechsellaufwerk.

Anschließend müssen Sie die Dateien vom Wechsellaufwerk zu einem HTTP-Server in Ihrer Air-Gap-Umgebung kopieren. Sie können diesen per Air-Gap abgesicherten Management Server als HTTP-Server verwenden. Weitere Informationen dazu finden Sie im Abschnitt '"Die Definitionen an einen HTTP-Server übertragen" (S. 682)'.

## Die Definitionen an einen HTTP-Server übertragen

Wenn Sie die Schutzdefinitionen in Ihrer Air-Gap-Umgebung verteilen wollen, benötigen Sie einen dedizierten HTTP-Server. Sie können Ihren per Air-Gap abgesicherten Management Server als HTTP-Server verwenden.

***So können Sie die Schutzdefinitionen zu einem HTTP-Server übertragen***

1. Kopieren Sie auf der Maschine, auf der Sie den HTTP-Server ausführen werden, die Schutzdefinitionen in einen Ordner Ihrer Wahl.

2. Starten Sie aus dem Ordner heraus, in den Sie die Schutzdefinitionen kopiert haben, einen HTTP-Server.

   Sie können beispielsweise Python verwenden und folgenden Befehl ausführen:

   ```
   python -m http.server 8080
   ```

   **Hinweis**
   Sie können jeden beliebigen HTTP-Server verwenden, den Sie bevorzugen.

3. Öffnen Sie in dem Ordner, wohin Sie die Schutzdefinitionen kopiert haben, folgende `update-index.json`-Dateien zur Bearbeitung:
   - `./ngmp/update-index.json`
   - `./vapm/update-index.json`
4. Bearbeiten Sie in beiden `update-index.json`-Dateien alle Felder bei `products > os > arch > components > versions > url` – und zwar folgendermaßen:
   a. Legen Sie die IP-Adresse und den Port Ihres HTTP-Servers als Werte für die Felder `IP` bzw. `port` fest.
   b. Ändern Sie nicht den anderen Teil des Pfades.

   Zum Beispiel: `"url": "http://192.168.1.10:8080/ngmp/win64/ngmp.zip"` – wobei 192.168.1.10 die IP-Adresse des HTTP-Servers und 8080 dessen Port ist. Ändern Sie nicht den Teil `/ngmp/win64/ngmp.zip`.
5. Speichern Sie Ihre Bearbeitungen in beiden `update-index.json`-Dateien.

Als nächstes müssen Sie die Quelle der Schutzdefinitionen auf dem per Air-Gap-Umgebung abgesicherten Management Server konfigurieren. Weitere Informationen dazu finden Sie im Abschnitt '"Die Quelle für Definitionen auf einem per Air-Gap abgesicherten Management Server konfigurieren" (S. 683)'.

## Die Quelle für Definitionen auf einem per Air-Gap abgesicherten Management Server konfigurieren

Nach der Konfiguration des HTTP-Servers müssen Sie diesen auf dem per Air-Gap abgesicherten Management Server als Quelle für die Schutzdefinitionen konfigurieren.

***So können Sie die Quelle für Schutzdefinitionen auf einem per Air-Gap abgesicherten Management Server konfigurieren***

1. Gehen Sie in der Cyber Protect-Webkonsole des per Air-Gap abgesicherten Management Servers zu **Einstellungen** –> **Schutz** –> **Update der Schutzdefinitionen**.
2. Wählen Sie **Definitionen** aus.
3. Wählen Sie **Benutzerdefiniert** und spezifizieren Sie folgende Pfade:

- Für **Antivirus & Antimalware-Definitionen**:

  `http://<IP address of your HTTP server>:8080/scanner`
- Für **Definitionen für die erweiterte Erkennung**:

  `http://<IP address of your HTTP server>:8080/ngmp`
- Für **Definitionen für die Schwachstellenbewertung und die Patch-Verwaltung**:

  `http://<IP address of your HTTP server>:8080/vapm`

Als Ergebnis werden die Agenten in der Air-Gap-Umgebung die Schutzdefinitionen von Ihrem HTTP-Server herunterladen.

# Benutzerkonten und Organisationseinheiten (Abteilungen) verwalten

## On-Premise-Bereitstellung

Die in diesem Abschnitt beschriebene Funktionalität ist nur für Organisationsadministratoren verfügbar.

Klicken Sie auf **Einstellungen** –> **Konten**, um auf diese Einstellungen zugreifen zu können.

### Abteilungen und administrative Konten

Wenn Sie Abteilungen und administrative Konten verwalten wollen, gehen Sie in der Cyber Protect Webkonsole zu **Einstellungen** –> **Konten**. Im Fensterbereich **Konten** wird die Gruppe **Organisation** mit einem Verzeichnisbaum der Abteilungen (sofern vorhanden) angezeigt – sowie die Liste der administrativen Konten auf der ausgewählten Hierarchieebene.

#### Abteilungen

Wenn Sie den Management Server installieren, wird die Gruppe **Organisation** automatisch erstellt. Mit einer Acronis Cyber Protect Advanced-Lizenz können Sie Untergruppen erstellen, die 'Abteilungen' genannt werden und denen administrative Konten hinzugefügt werden können. Diese Abteilungen entsprechen typsicherweise bestimmten Untereinheiten bzw. Bereichen eines Unternehmens. Auf diese Weise können Sie die Schutzverwaltung an andere Personen delegieren, deren Zugriffsberechtigungen streng auf die entsprechenden Abteilungen begrenzt sind. Informationen über die Erstellung einer Abteilung finden Sie im Abschnitt '"Abteilungen erstellen" (S. 690)'.

Jede Abteilung (Organisationseinheit) kann Unterabteilungen haben. Die administrativen Konten der übergeordneten Abteilung haben in allen Unterabteilungen dieselben Berechtigungen. Die Gruppe **Organisation** ist die übergeordnete Abteilung mit der höchsten Ebene – und administrative Konten auf dieser Ebene haben die gleichen Berechtigungen in allen Abteilungen.

#### Administrative Konten

Jedes Konto, das sich an der Cyber Protect Webkonsole anmelden kann, ist ein administratives Konto.

In der Cyber Protect Webkonsole kann jedes administrative Konto alles einsehen oder verwalten, was sich auf oder unterhalb der Hierarchie-Ebene seiner Abteilung befindet. Ein administratives Konto in der *Organization*' hat beispielsweise Zugriff auf diese höchste Ebene und damit Zugriff auf alle Abteilungen dieser Organisation – während ein administratives Konto in einer bestimmten *Abteilung* nur auf diese Abteilung und deren Unterabteilungen zugreifen kann.

## Welche Konten können administrativ sein?

Falls der Management Server auf einer Windows-Maschine installiert ist, die einer Active Directory-Domain angehört, können Sie lokalen Benutzern oder Benutzern und Benutzergruppen innerhalb der Active Directory-Domänengesamtstruktur administrative Rechte gewähren.

Standardmäßig stellt der Management Server eine SSL/TLS-geschützte Verbindung zum Active Directory Domain Controller her. Wenn dies nicht möglich ist, wird gar keine Verbindung hergestellt. Sie können jedoch auch unsichere Verbindungen zulassen, indem Sie die Datei `auth-connector.json5` bearbeiten.

Wenn Sie eine sichere Verbindung verwenden wollen, stellen Sie sicher, dass LDAPS (LDAP-über-SSL) für Ihr Active Directory konfiguriert ist.

***So können Sie LDAPS für Active Directory konfigurieren***

1. Erstellen und installieren Sie auf dem Domain Controller ein LDAPS-Zertifikat, das die Microsoft-Anforderungen erfüllt.
   Weitere Informationen zur Durchführung dieser Aktionen finden Sie im Artikel 'Aktivieren von LDAP über SSL mit einer Zertifizierungsstelle eines Drittanbieters' in der Microsoft-Dokumentation.
2. Öffnen Sie auf dem Domain Controller die **Microsoft Management Console** und überprüfen Sie, ob das Zertifikat unter **Zertifikate (Lokaler Computer)** –> **Persönlich** –> **Zertifikate** vorhanden ist.
3. Starten Sie den Domain-Controller neu.
4. Überprüfen Sie, ob LDAPS aktiviert ist.

***So können Sie unsichere Verbindungen zum Domain Controller zulassen***

1. Melden Sie sich an der Maschine an, auf welcher der Management Server installiert ist.
2. Öffnen Sie die Datei `auth-connector.json5` zur Bearbeitung.
   Die Datei `auth-connector.json5` befindet sich im Verzeichnis `%APPDATA%\Acronis\AuthConnector`.
3. Gehen Sie zum Abschnitt **sync** und ersetzen Sie dann in jeder **"connectionMode"**-Zeile den Eintrag **"ssl_only"** durch **"auto"**.
   Im Modus **auto** wird dann eine unsichere Verbindung aufgebaut, wenn keine TLS-Verbindung möglich ist.
4. Starten Sie den **Acronis Service Manager Service** neu (wie im Abschnitt '"So können Sie den Acronis Service Manager Service neu starten" (S. 209)' beschrieben).

**Hinweis**
Wenn der Management Server in keiner Active Directory-Domain enthalten ist oder wenn er auf einer Linux-Maschine installiert ist, können Sie nur lokalen Benutzern und Gruppen administrative Rechte gewähren.

Wie Sie dem Management Server ein administratives Konto hinzufügen können, wird im Abschnitt '"Administrative Konten hinzufügen" (S. 689)' erläutert.

## Administrative Konto-Rollen

Jedem administrativen Konto wird eine Rolle mit den vordefinierten Berechtigungen zugewiesen, die für bestimmte Aufgaben erforderlich sind. Es gibt folgende administrative Konto-Rollen:

- **Administrator**
  Diese Rolle ermöglicht den vollen administrativen Zugriff auf die Organisation oder eine Abteilung.
- **Nur Lesen**
  Diese Rolle ermöglicht einen schreibgeschützten Zugriff auf die Cyber Protect Webkonsole. Sie ermöglicht nur das Sammeln von Diagnoseinformationen (wie z.B. Systemberichte). Mit der Nur-Lesen-Rolle können weder Backups noch die Inhalte von gesicherten Postfächern durchsucht werden.
- **Auditor**
  Diese Rolle ermöglicht einen Nur-Lesen-Zugriff auf die Registerkarte **Aktivitäten** in der Cyber Protect Webkonsole. Weitere Informationen zu dieser Registerkarte finden Sie im Abschnitt '"Die Registerkarte 'Aktivitäten'" (S. 627)'. Mit dieser Rolle können keine Daten (auch nicht die Systeminformationen des Management Servers) gesammelt oder exportiert werden.

Alle Änderungen in den Rollen werden auf der Registerkarte **Aktivitäten** angezeigt.

## Vererbung von Rollen

Die Rollen in einer übergeordneten Abteilung werden an ihre Unterabteilungen weitergegeben. Wenn demselben Benutzerkonto in der übergeordneten und in einer untergeordneten Abteilung unterschiedliche Rollen zugewiesen wurden, verfügt es über beide Rollen.

Rollen können außerdem einem bestimmten Benutzerkonto explizit zugewiesen oder von einer Benutzergruppe geerbt werden. Ein Benutzerkonto kann daher sowohl eine spezifisch zugewiesene als auch eine vererbte Rolle haben.

Wenn ein Benutzerkonto verschiedene Rollen hat (zugewiesen und/oder vererbt), kann es auf alle Objekte zugreifen und alle Aktionen ausführen, die durch diese Rollen erlaubt werden. So erhält beispielweise ein Benutzerkonto, dem die Rolle 'Nur Lesen' zugewiesen wurde und das gleichzeitig die Rolle 'Administrator' geerbt hat, volle administrative Berechtigungen.

**Wichtig**
In der Cyber Protect Webkonsole werden nur explizit zugewiesene Rollen für die aktuelle Abteilung angezeigt. Eventuelle Unstimmigkeiten mit vererbten Rollen werden nicht angezeigt. Wir empfehlen dringend, dass Sie die Rollen 'Administrator', 'Nur-Lesen' und 'Auditor' nur jeweils separaten Konten oder Gruppen zuweisen, um mögliche Probleme mit vererbten Rollen zu vermeiden.

## Standard-Administratoren

### Unter Windows:

Wenn ein Management Server auf einer Maschine installiert wird, passiert Folgendes:

- Es wird die Benutzergruppe **Acronis Centralized Admins** auf der Maschine erstellt.
  Auf einem Domain Controller wird die Gruppe folgendermaßen bezeichnet: *DCNAME* **$ Acronis Centralized Admins**. Wobei *DCNAME* für den NetBIOS-Namen des Domain Controllers steht.
- Alle Mitglieder der Gruppe **Administratoren** werden der Gruppe **Acronis Centralized Admins** hinzugefügt. Wenn sich die Maschine in einer Domain befindet, aber kein Domain Controler ist, werden lokale (Nicht-Domain-)Benutzer ausgeschlossen. Auf einem Domain Controller gibt es keine Nicht-Domain-Benutzer.
- Die Gruppen **Acronis Centralized Admins** und **Administratoren** werden dem Management Server **Organisationsadministratoren** hinzugefügt. Wenn sich die Maschine in einer Domäne befindet, aber kein Domain Controller ist, wird die Gruppe **Administratoren** nicht hinzugefügt, sodass lokale (Nicht-Domain-)Benutzer keine Organisationsadministratoren werden.

Sie können die Gruppe **Administratoren** aus der Liste der Organisationsadministratoren löschen. Die Gruppe **Acronis Centralized Admins** kann jedoch nicht gelöscht werden. Für den unwahrscheinlichen Fall, dass alle Organisationsadministratoren gelöscht wurden, können Sie der Gruppe **Acronis Centralized Admins** in Windows ein Konto hinzufügen – und sich dann über dieses Konto an der Cyber Protect Webkonsole anmelden.

### Unter Linux:

Wenn der Management Server auf einer Maschine installiert wird, wird der Benutzer **root** dem Management Server als **Organisationsadministrator** hinzugefügt.

Sie können der Liste der Management Server-Administratoren weitere Linux-Benutzer hinzufügen (wie weiter unten beschrieben) und dann auch den Benutzer **root** von dieser Liste wieder entfernen. Für den unwahrscheinlichen Fall, dass alle Organisationsadministratoren gelöscht wurden, können Sie den Dienst `acronis_asm` neu starten. Der Benutzer **root** wird dadurch automatisch wieder als Organisationsadministrator hinzugefügt.

## Administratives Konto in mehreren Abteilungen

Einem Konto können in beliebig vielen Abteilungen administrative Berechtigungen erteilt werden. Für ein solches Konto (genauso wie für administrative Konten auf der Organisationsebene) wird in der Cyber Protect Webkonsole eine Abteilungsauswahl angezeigt. Mit diesem Auswahlelement kann der Besitzer des Kontos jede Abteilung separat einsehen oder verwalten.

Ein Konto, das über Berechtigungen für alle Abteilungen in einer Organisation verfügt, hat keine Berechtigungen für die Organisation selbst. Administrative Konten auf der Organisationsebene müssen der Gruppe **Organization** explizit hinzugefügt werden.

## So können Sie Abteilungen mit Maschinen befüllen

Wenn ein Administrator eine Maschine über die Weboberfläche hinzufügt, wird diese Maschine der Abteilung hinzugefügt, die von diesem Administrator verwaltet wird. Wenn der Administrator mehrere Abteilungen verwaltet, wird die Maschine derjenigen Abteilung hinzugefügt, die in der Abteilungsauswahl angewählt ist. Der Administrator muss die Abteilung daher schon vorher auswählen, bevor er auf **Hinzufügen** klickt.

Wenn Agenten lokal installiert werden, muss ein Administrator deren Anmeldedaten bereitstellen. Die Maschine wird der Abteilung hinzugefügt, die vom Administrator verwaltet wird. Wenn der Administrator mehrere Abteilungen verwaltet, wird er vom Installer aufgefordert, eine Abteilung auszuwählen, der die Maschine hinzugefügt werden soll.

# Administrative Konten hinzufügen

**Hinweis**
Diese Funktion ist in den Standard- und Essentials-Editionen nicht verfügbar.

***So können Sie Konten hinzufügen***

1. Klicken Sie auf **Einstellungen** –> **Konten**.
   Die Software zeigt eine Liste mit den Administratoren des Management Servers an und (sofern vorhanden) den Verzeichnisbaum der Abteilungen.
2. Wählen Sie **Organisation** oder wählen Sie die Abteilung aus, wo Sie einen Administrator hinzufügen wollen.
3. Klicken Sie auf **Konto hinzufügen**.
4. Wählen Sie bei **Domain** die Domain aus, welche die Benutzerkonten enthält, die Sie hinzufügen wollen. Falls der Management Server keiner Active Directory-Domain angehört oder unter Linux installiert ist, können nur lokale Benutzer hinzugefügt werden.
5. Suchen Sie nach dem Benutzernamen oder dem Namen einer Benutzergruppe.
6. Klicken Sie auf das '+'-Zeichen, welches neben dem Benutzer- oder Gruppennamen liegt.
7. Wählen Sie die Rolle für das Konto aus.
8. Wiederholen Sie die Schritte 4-6 für alle Benutzer oder Gruppen, die Sie hinzufügen wollen.
9. Klicken Sie zum Abschluss auf **Fertig**.
10. [Nur unter Linux] Fügen Sie die Benutzernamen wie nachfolgend beschrieben zur PAM-Konfiguration (Pluggable Authentication Module) für die Acronis Module hinzu.

***So können Sie Benutzernamen zur PAM-Konfiguration für Acronis hinzufügen***

Diese Prozedur gilt für Management Server, die auf Linux-Maschinen und in der Acronis Cyber Protect All-in-one-Appliance laufen.

1. Öffnen Sie als Benutzer 'root' auf der Maschine, die den Management Server ausführt, die Datei **/etc/security/acronisagent.conf** in einem Text-Editor.
2. Geben Sie in dieser Datei die Benutzernamen ein, die Sie als Management Server-Administratoren hinzugefügt haben – und zwar einen pro Zeile.
3. Speichern und schließen Sie die Datei.

## Abteilungen erstellen

1. Klicken Sie auf **Einstellungen** –> **Konten**.
2. Die Software zeigt eine Liste mit den Administratoren des Management Servers an und (sofern vorhanden) den Verzeichnisbaum der Abteilungen.
3. Wählen Sie **Organisationen** oder wählen Sie die übergeordnete Abteilung für die neue Abteilung aus.
4. Klicken Sie auf **Abteilung erstellen**.
5. Spezifizieren Sie einen Namen für die neue Abteilung und klicken Sie dann auf **Erstellen**.

# Cloud-Bereitstellung

Die Verwaltung von Benutzerkonten und Organisationseinheiten (Abteilungen) erfolgt über das Management-Portal. Auf dieses können Sie zugreifen, indem Sie nach der Anmeldung am Cyber Protection Service auf **Management-Portal** klicken. Alternativ können Sie in der rechten oberen Ecke auch auf das Symbol  klicken und anschließend auf **Management-Portal**. Nur Benutzer mit administrativen Berechtigungen können auf das Portal zugreifen.

Weitere Informationen über die Verwaltung von Benutzerkonten und Organisationseinheiten (Abteilungen) finden Sie in der Management-Portal-Administrator-Anleitung. Sie können auf dieses Dokument zugreifen, wenn Sie im Management-Portal auf das Fragezeichen-Symbol klicken.

Dieser Abschnitt enthält zusätzliche Informationen zur Verwaltung des Cyber Protection Service.

## Quotas

Mit Quotas können Sie einschränken, ob und wie Benutzer den Service verwenden können. Um Quotas festlegen zu können, müssen Sie in der Registerkarte **Benutzer** den gewünschten Benutzer auswählen und anschließend im Bereich **Quotas** auf das Stiftsymbol klicken.

Wenn eine Quota überschritten wird, wird an den Benutzer (bzw. seine E-Mail-Adresse) eine entsprechende Benachrichtigung gesendet. Wenn Sie keine Quota-Überschreitung festlegen, wird die Quota als 'weich' angesehen. Das bedeutet, dass keine Beschränkungen für die Nutzung des Cyber Protection Service gelten.

Sie können außerdem Quota-Überschreitungen spezifizieren. Eine Überschreitung erlaubt es dem Benutzer, die Quota um den spezifizierten Wert zu überschreiten. Wird die Überschreitung überschritten, werden Nutzungsbeschränkungen auf den Cyber Protection Service angewendet.

## Backup

Sie können die Cloud Storage-Quota, die Quota für lokale Backups und die maximale Anzahl an Maschinen/Geräten/Postfächern spezifizieren, die ein Benutzer sichern darf. Folgende Quotas sind verfügbar:

- **Cloud Storage**
- **Workstations**
- **Server**
- **Windows Server Essentials**
- **Virtuelle Hosts**
- **Universal**
  Diese Quota kann anstelle einer der vier oben aufgeführten Quotas verwendet werden: Workstations, Server, Windows Server Essentials, virtuelle Hosts.
- **Mobilgeräte**
- **Microsoft 365-Postfächer**
- **Lokales Backup**

Ein(e) Maschine/Gerät/Postfach wird als 'geschützt' betrachtet, wenn auf diese(s) mindestens ein Schutzplan angewendet wurde. Ein Mobilgerät wird nach Durchführung des ersten Backups als 'geschützt' betrachtet.

Wird die Cloud Storage-Quota-Überschreitungsgrenze erreicht, schlägt das Backup fehl. Wenn die Überschreitungsgrenze für eine bestimmte Anzahl von Geräten erreicht ist, kann der Benutzer keinen weiteren Geräten mehr einen Schutzplan zuweisen.

Die Quota '**Lokales Backup**' beschränkt die Gesamtgröße der lokalen Backups, die mithilfe der Cloud-Infrastruktur erstellt werden können. Für diese Quota kann keine Überschreitung festgelegt werden.

## Disaster Recovery

Diese Quotas werden vom Service-Provider auf die komplette Firma angewendet. Firmenadministratoren können die Quotas und Nutzungsinformationen im Management-Portal einsehen, jedoch keine Quotas für bestimmte Benutzer festlegen.

- **Disaster Recovery Storage**
  Dieser Storage wird von primären Servern und Recovery-Servern verwendet. Wenn die Überschreitungsgrenze für diese Quota erreicht ist, können keine primären Server oder Recovery-Server erstellt oder Laufwerke zu vorhandenen primären Servern hinzufügt/erweitert werden. Wenn die Überschreitungsgrenze für diese Quota erreicht ist, kann kein Failover initiiert oder ein gestoppter Server gestartet werden. Die Ausführung laufender Server wird aber fortgesetzt.

Wenn die Quota deaktiviert wird, werden alle Server gelöscht. Die Registerkarte **Cloud-Recovery-Site** wird nicht mehr in der Cyber Protect Webkonsole angezeigt.

- **Berechnungspunkte**

  Diese Quota begrenzt die CPU- und RAM-Ressourcen, die die primären Server und Recovery-Server während eines Abrechnungszeitraums verbrauchen dürfen. Wenn die Überschreitungsgrenze für diese Quota erreicht ist, werden alle primären Server und Recovery-Server heruntergefahren. Diese Server können erst wieder verwendet werden, wenn der nächste Abrechnungszeitraum beginnt. Der vorgegebene Abrechnungszeitraum ist ein voller Kalendermonat.

  Wenn die Quota deaktiviert ist, können die Server überhaupt nicht verwendet werden (unabhängig vom Abrechnungszeitraum).

- **Öffentliche IP-Adressen**

  Mit dieser Quota wird die Anzahl der öffentlichen IP-Adressen beschränkt, die primären Servern und Recovery-Servern zugewiesen werden können. Wenn die Überschreitungsgrenze für diese Quota erreicht ist, können keine öffentlichen IP-Adressen mehr für weitere Server aktiviert werden. Sie können einem Server die Verwendung öffentlicher IP-Adressen verbieten, wenn Sie in den Server-Einstellungen das Kontrollkästchen **Öffentliche IP-Adressen** deaktivieren. Anschließend können Sie einem anderen Server die Verwendung einer öffentlichen IP-Adresse (die normalerweise nicht dieselbe ist) erlauben.

  Wenn die Quota deaktiviert wird, hören alle Server auf, öffentliche IP-Adressen zu verwenden, und sind anschließend nicht mehr über das Internet erreichbar.

- **Cloud Server**

  Diese Quota ermöglicht es, die Gesamtzahl der primären Server und Recovery-Server zu beschränken. Wenn die Überschreitungsgrenze für diese Quota erreicht ist, können keine primären Server oder Recovery-Server erstellt werden.

  Wenn die Quota deaktiviert wird, sind die Server zwar noch in der Cyber Protect Webkonsole sichtbar, aber die einzige auf sie anwendbare Aktion ist **Löschen**.

- **Internetzugriff**

  Diese Quota (de)aktiviert den Internetzugriff für primäre Server und Recovery-Server.

  Wenn die Quota deaktiviert wird, verlieren die primären Server und Recovery-Server sofort ihre Internetverbindung. Der Schalter **Internetzugriff** in den Server-Eigenschaften wird zurückgesetzt und deaktiviert.

## Benachrichtigungen

Wenn Sie die Benachrichtigungseinstellungen für einen Benutzer ändern wollen, müssen Sie in der Registerkarte **Benutzer** den gewünschten Benutzer auswählen und anschließend im Bereich **Einstellungen** auf das Stiftsymbol klicken. Es stehen folgende Benachrichtigungseinstellungen zur Verfügung:

- **Benachrichtigungen über Quota-Überbenutzung** (standardmäßig aktiviert)

  Die Benachrichtigungen zu überschrittenen Quotas.

- **Geplante Nutzungsberichte**

Die nachfolgend beschriebenen Nutzungsberichte, die am ersten Tag eines jeden Monats gesendet werden.

- **Benachrichtigungen über Fehler**, **Benachrichtigungen über Warnungen** und **Benachrichtigungen über erfolgreiche Aktionen** (standardmäßig deaktiviert)
  Die Benachrichtigungen über die Ausführungsergebnisse von Schutzplänen und die Ergebnisse von Disaster Recovery-Aktionen für jedes Gerät.
- **Tägliche Zusammenfassung über aktive Alarmmeldungen** (standardmäßig aktiviert)
  Die Zusammenfassung informiert Sie über fehlgeschlagene Backups, verpasste Backups und andere Probleme. Die Zusammenfassung wird um 10:00 Uhr morgens (nach der Zeit des Datacenters) versendet. Wenn zum betreffenden Zeitpunkt keine Probleme vorliegen, wird auch keine Zusammenfassung gesendet.

Alle Benachrichtigungen werden an die E-Mail-Adresse gesendet, die für den entsprechenden Benutzer spezifiziert wurde.

## Berichte

Ein Bericht über die Nutzung des Cyber Protection Service enthält folgende Daten über das Unternehmen oder eine Abteilung:

- Die Größe von Backups pro Abteilung, pro Benutzer, pro Gerätetyp.
- Die Anzahl von geschützten Geräten pro Abteilung, pro Benutzer, pro Gerätetyp.
- Der Preis pro Abteilung, pro Benutzer, pro Gerätetyp.
- Die Gesamtgröße der Backups.
- Die Gesamtzahl der geschützten Geräte.
- Der Gesamtpreis.

# Befehlszeilenreferenz

Die Befehlszeilenreferenz ist als eigenständiges Dokument unter folgender Adresse verfügbar: https://www.acronis.com/de-de/support/documentation/AcronisCyberProtect_15_Command_Line_Reference/index.html.

# 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. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Wählen Sie bei **Geräte** die Maschine aus, deren Protokolle Sie sammeln wollen. Klicken Sie anschließend auf **Aktivitäten**.
   - Wählen Sie bei **Einstellungen** –> **Agenten** die Maschine aus, deren Protokolle Sie sammeln wollen. Klicken Sie anschließend auf **Details**.
2. Klicken Sie auf **Systeminformationen sammeln**.
3. Spezifizieren Sie bei Aufforderung durch Ihren Webbrowser, wo die Datei gespeichert werden soll.

# Glossar

## B

**Backup-Format 'Einzeldatei'**

Ein neues Backup- Format, in dem das anfängliche Voll- Backup sowie die nachfolgenden inkrementellen Backups gemeinsam in Form einer einzigen .tib- Datei (statt einer Kette von Dateien) gespeichert werden. Dieses Format nutzt die Geschwindigkeit der inkrementellen Backup-Methode und vermeidet dabei gleichzeitig deren größten Nachteil: das schwierige Löschen veralteter Backups. Die Software kennzeichnet diejenigen Blöcke, die von veralteten Backups verwendet werden, als 'frei' und schreibt neue Backups in diese neuen Blöcke. Dies führt zu einer extrem schnellen Bereinigung, bei gleichzeitig minimalem Ressourcenverbrauch. Das Backup- Format 'Einzeldatei' ist nicht verfügbar, wenn als Backup- Ziel ein Storage (wie etwa ein SFTP-Server) 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- Sätze den Backup-Methoden ('Vollständig', 'Differentiell' und 'Inkrementell'). In allen anderen Fällen sind die Backups- Sätze 'Monatlich', 'Täglich', 'Wöchentlich' und 'Stündlich'. Ein 'monatliches' Backup ist dasjenige Backup, das als erstes in einem bestimmten Monat erstellt wird. Ein 'wöchentliches' Backup ist das erste Backup, welches an demjenigen Wochentag erstellt wird, wie er über die Option 'Wöchentliches Backup' festgelegt wurde (klicken Sie auf das Zahnradsymbol und dann auf die Befehle 'Backup-Optionen' –> 'Wöchentliche Backups'). Wenn ein 'wöchentliches' Backup das erste Backup ist, welches seit Anbruch eines Monats erstellt wurde, so wird dieses Backup als 'monatliches' Backup betrachtet. In diesem Fall wird ein wöchentliches Backup an dem ausgewählten Tag der nächsten Woche erstellt. Ein 'tägliches' Backup ist das erste Backup, welches nach Anbruch eines Tages erstellt wird – es sei denn, dieses Backup fällt unter die Definition eines monatlichen oder wöchentlichen Backups. Ein 'stündliches' Backup ist das erste Backup, welches nach Anbruch einer Stunde erstellt wird – es sei denn, dieses Backup fällt unter die Definition eines 'monatlichen', 'wöchentlichen' oder 'täglichen' Backups.

## D

**Differentielles Backup**

Ein differentielles Backup speichert Änderungen an den Daten im Vergleich zum letzten vorangegangenen Voll- Backup. Sie müssen auf das entsprechende Voll- Backup zugreifen können, um Daten aus einem differentiellen Backup wiederherstellen zu können.

## 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.

# S

**Startup Recovery Manager**

Eine Modifikation des bootfähigen Agenten, der auf dem Systemlaufwerk gespeichert wird und so konfiguriert ist, dass er gestartet werden kann, wenn beim Booten auf die Taste F11 gedrückt wird. Der Startup Recovery Manager ist eine alternative Möglichkeit, eine bootfähige Notfallumgebung zu starten, ohne dass dafür ein Boot- Medium oder eine Netzwerkverbindung benötigt wird. Der Startup Recovery Manager ist besonders für Anwender mobiler Geräte (wie Notebooks) nützlich. Wenn ein schwerwiegender Fehler auftritt, kann der Benutzer die Maschine neu starten und auf die F11-Taste drücken, wenn die Meldung „Druecken Sie F11 zum Ausfuehren des Startup Recovery Managers...“ erscheint. Anschließend kann er eine Datenwiederherstellung auf dieselbe Art durchführen, wie es Verwendung eines herkömmlichen Boot-Mediums der Fall wäre. Einschränkung: Erfordert die Möglichkeit, einen anderen Boot- Loader als den von Windows oder GRUB aktivieren zu können.

# V

**Verwalteter Speicherort**

Ein Backup-Speicherort, der von einem Storage Node verwaltet wird. Physisch können sich verwaltete Speicherorte auf einem freigegebenen Netzlaufwerk, einem SAN, NAS, auf einer lokalen Festplatte des Storage Nodes oder auf einer Bandbibliothek befinden, die lokal an den Storage Node angeschlossen ist. Der Storage Node bereinigt und validiert die am verwalteten Speicherort gesicherten Backups – sofern dies in einem entsprechenden Schutzplan so festgelegt wurde. Sie können zudem noch weitere Aktionen spezifizieren, die der Storage Node durchführen soll (wie Deduplizierung oder Verschlüsselung).

**Voll-Backup**

Ein selbstständiges Backup, das alle für ein Backup ausgewählten Daten enthält. Sie benötigen kein weiteres Backup, um die Daten aus einem Voll-Backup wiederherzustellen.

# Index

**B**

**S**

**T**

**U**

**V**

**W**

**Z**