Synology

# Admin-Handbuch für ActiveProtect-Gerät für APM 1.0

Last updated: Feb 11,2025

# Kennenlernen von ActiveProtect

**ActiveProtect** ist eine umfassende Lösung für den Datenschutz, die für verschiedene Unternehmensumgebungen entwickelt wurde. Von nahtlosen Backups und schnellen Wiederherstellungen bis hin zur langfristigen Datenspeicherung ist es Ihre bevorzugte Lösung zum Schutz Ihrer wertvollen Vermögenswerte. Egal, ob Ihre Organisation aus mehreren einzelnen Standorten, entfernten Büros oder weitläufigen Unternehmenskomplexen besteht, ActiveProtect bietet Ihnen Schutz.

Richten Sie Ihren Backup-Standort mit **Synology ActiveProtect Appliances** (DP-Serie) ein. Diese Geräte sind mit dem zuverlässigen Betriebssystem **ActiveProtect Manager (APM)** ausgestattet, das mühelose Backups und Wiederherstellungen ermöglicht und Ihren Datenschutzprozess vereinfacht.

Zusätzlich können Sie **ActiveProtect Vault** nutzen, ein integriertes Paket auf Ihrem Synology NAS, das sich ideal für die Remote-Speicherung eignet, um eine langfristige Datenspeicherung zu gewährleisten.

Dieser Abschnitt wird Sie in ActiveProtect einführen und Ihnen helfen, den Datenschutz an die spezifischen Bedürfnisse Ihres Unternehmens anzupassen.

## In diesem Abschnitt

# Übersicht über den Datenschutz

## Schützen Sie Ihre Daten aktiv

ActiveProtect schützt eine breite Palette von Workloads in Ihrer Geschäftsumgebung, einschließlich Personalcomputern, physischen Servern, Dateiservern, virtuellen Maschinen, Datenbanken und Microsoft 365.

Um umfassende Datensicherheit und -wiederherstellung zu gewährleisten, folgt ActiveProtect der **3-2-1-1-Backup-Strategie**:

- Schutz von **3** Kopien von Daten: Originaldaten, Sicherungen und Sicherungskopien.
- Speicherung von Daten auf **2** verschiedenen Medien.
- Aufrechterhaltung von **1** externen Kopie, geografisch getrennt für die Notfallwiederherstellung.
- Beibehaltung von **1** unveränderlichen Kopie, die gegen Ransomware-Angriffe unempfindlich ist.

## Lösungs-Highlights

ActiveProtect bietet die folgenden Funktionen, um Ihre Datenschutzstrategie zu vereinfachen und zu verbessern:

### Sicherung

- Erstellen Sie flexible Schutzpläne, die auf Ihre Bedürfnisse zugeschnitten sind, und optimieren Sie Sicherungsstrategien durch angepasste Zeitpläne, Bereiche, Aufbewahrungsfristen und Sicherungskopien.
- Identifizieren und schützen Sie neu hinzugefügte Workloads automatisch mit Auto-Backup-Regeln, um mühelosen Datenschutz zu gewährleisten.
- Optimieren Sie den Speicherplatz und minimieren Sie Redundanzen durch Deduplizierung während der Sicherungen.

### Wiederherstellung

- Bieten Sie verschiedene Wiederherstellungsoptionen an, die zu Ihren Workloads passen, einschließlich Datei-Ebene, Bare-Metal und Cross-Hypervisor-Wiederherstellung.
- Zentralisieren Sie gesicherte Daten für einfaches Durchsuchen und Selbstbedienungswiederherstellung.
- Führen Sie Testwiederherstellungen durch, um die Datenwiederherstellbarkeit zu testen, indem Sie verwenden:
  - Eingebauter Hypervisor-Test: Starten Sie virtuelle Maschinen direkt auf dem integrierten Hypervisor, um Daten und Dienste schnell zu überprüfen.
  - Sicherungsüberprüfung: Zeichnen Sie den gesamten Startvorgang als Video auf, um sicherzustellen, dass die gesicherte Maschine ordnungsgemäß startet.

## Datenmanagement

- Vereinfachen Sie Ihr Datenmanagement mit einer einheitlichen Plattform, die es Ihnen ermöglicht, Daten von allen Sicherungsservern und Remote-Speichern zu durchsuchen und zu verwalten.
- Bieten Sie Echtzeit-Einblicke in Datenströme aus allen Quellen für eine effiziente Analyse.

## Sicherheit und Zuverlässigkeit

- Stellen Sie die Integrität der Sicherung durch Btrfs-Prüfsummenverifizierung und RAID-Speichermechanismen sicher.
- Schützen Sie gesicherte Daten vor unbefugten Änderungen durch Unveränderlichkeit.
- Verwenden Sie Air Gaps, um sich gegen Ransomware-Bedrohungen zu schützen.
- Implementieren Sie ein sicheres Identitätsmanagement, einschließlich Domain/LDAP-Integration, Single Sign-On (SSO) und mehreren Zugriffskontrollmaßnahmen.

## Infrastrukturmanagement

- Bieten Sie ein zentrales Dashboard mit Echtzeit-Einblicken in die Systemleistung, den Sicherungsstatus und die allgemeine Infrastrukturgesundheit.
- Vereinfachen Sie die Verwaltung und Überwachung von Backup-Servern und Remote-Speicher, um die volle Kontrolle über Ihre Standortinfrastruktur zu erhalten.
- Sorgen Sie für Katastrophenresilienz mit einem primär-sekundären Failover-Mechanismus für ununterbrochenen Datenschutz.
- Nutzen Sie ein umfassendes Protokollierungssystem, um vergangene Ereignisse zu verfolgen, bei der Fehlerbehebung zu unterstützen und Verantwortlichkeit sicherzustellen.
- Halten Sie sich mit rechtzeitigen E-Mail-Benachrichtigungen über kritische Ereignisse auf dem Laufenden.

# Infrastrukturkomponenten

ActiveProtect gewährleistet die Datensicherheit durch einen Server-Cluster, der **Site** genannt wird. Innerhalb dieser Site arbeiten mehrere Server zusammen, um Workloads zu sichern, Daten zu speichern und Wiederherstellungslösungen bereitzustellen.

Dieser Artikel beschreibt die einzelnen Servertypen und ihre Funktionen. Um zu erfahren, wie Sie eine Site bereitstellen, lesen Sie Infrastruktur.

## Sicherungsserver

Sicherungsserver sind das Herzstück einer ActiveProtect-Site und umfassen zwei Servertypen: **Synology ActiveProtect-Gerät** und **Synology NAS**.[1] Sie schützen die Daten Ihrer Organisation durch folgende Mechanismen:

- **Workloads sichern**: Sichern Sie Ihre Daten zur Aufbewahrung und bedarfsgerechten Wiederherstellung.
- **Sicherungsversionen kopieren**: Erstellen Sie zusätzliche Kopien der Sicherungsdaten, um die Sicherheit zu erhöhen.
- **Daten speichern**: Bewahren Sie Sicherungsdaten und deren Kopien auf.[2]
- **Datenaufbewahrung implementieren**: Löschen Sie frühere Sicherungsversionen, um Speicherplatz freizugeben.
- **Schutz für neue Workloads automatisieren**: Identifizieren und sichern Sie automatisch Workloads, die Ihren Kriterien entsprechen, um einen nahtlosen Datenschutz zu gewährleisten.
- **Geschützte Maschinen ausführen**: Starten Sie gesicherte virtuelle Maschinen und physische Server mit einem integrierten Hypervisor, um die Wiederherstellbarkeit Ihrer Sicherungsdaten zu überprüfen.
- **Gesamte Workloads oder Dateien wiederherstellen**: Stellen Sie Sicherungsdaten wieder her, um Datenverlust und -beschädigung zu verhindern.

Erfahren Sie mehr darüber, wie Sie Sicherungsserver bereitstellen.

## Verwaltungsserver

Um Server und deren Aktivitäten zu überwachen, können Sie einen Sicherungsserver als **Verwaltungsserver**[3] für Ihre Site zuweisen. Wenn Sie nur einen Sicherungsserver haben, übernimmt dieser automatisch diese Rolle.

Wählen Sie ein ActiveProtect-Gerät, das die Verwaltung Ihrer Site über den **ActiveProtect Manager (APM)**, eine lokale Konsole für den Datenschutz, ermöglicht. Sie können auch ein weiteres Sicherungsgerät als Failover-Server festlegen, um unterbrechungsfreie Serveraktivitäten sicherzustellen.

Ein Verwaltungsserver ermöglicht Ihnen die Durchführung verschiedener administrativer Aufgaben, wie zum Beispiel:

- Überwachen der Site-Infrastruktur
- Verwalten von Workloads und Schutzplänen

- Durchführen der Datenwiederherstellung
- Anzeigen von Sicherungsinformationen und Dateien
- Zuweisen von Zugriffsberechtigungen
- Überprüfen der Site-Aktivitäten

## Remote-Speicher

Um Daten für längere Zeiträume aus rechtlichen oder regulatorischen Gründen aufzubewahren, sollten Sie in Betracht ziehen, Ihre Sicherungskopien in den **Remote-Speicher** zu verschieben. Sie können hoch skalierbare **Synology NAS** oder **Objektspeicherdienste** (z. B. C2 Object Storage) als Remote-Speicher Ihrer Site hinzufügen.

Wenn Sie Synology NAS als Remote-Speicher einrichten möchten, installieren Sie zuerst das Paket **ActiveProtect Vault** (siehe die Kompatibilitätsliste).

Erfahren Sie mehr darüber, wie Sie Remote-Speicher bereitstellen.

## Hypervisoren

Richten Sie Hypervisoren als Sandbox-Umgebung für Wiederherstellungsübungen oder Softwaretests ein. Das Hinzufügen dieser Hypervisoren zu einer Site ermöglicht es Ihnen, virtuelle Maschinen, die darauf laufen, effizient zu schützen.

ActiveProtect unterstützt derzeit die Integration mit **VMware vSphere** und **Microsoft Hyper-V**.

Erfahren Sie mehr darüber, wie Sie Hypervisoren bereitstellen.

**Hinweis:**

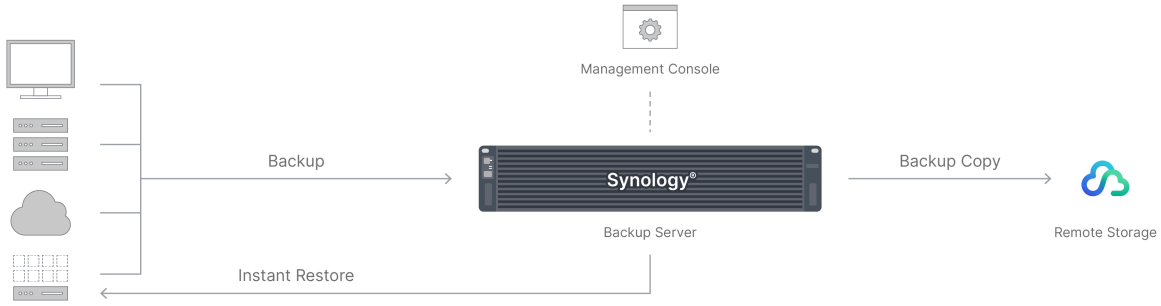
1. Um einen NAS als Backup-Server einzurichten, müssen Sie das Paket **Active Backup for Business** installieren.
2. Das Speichern von Backup-Kopien wird von Synology NAS nicht unterstützt.
3. Jede ActiveProtect-Site kann nur **einen** Management-Server haben.

# Bereitstellungsszenarien

ActiveProtect bietet Flexibilität bei der Serverbereitstellung, um den Anforderungen Ihrer Organisation gerecht zu werden. Dieser Artikel stellt drei Strategien für die Bereitstellung eines ActiveProtect-Standorts vor, die jeweils auf unterschiedliche Organisationsgrößen zugeschnitten sind.

Für Schritt-für-Schritt-Anleitungen zur Standortbereitstellung können Sie sich auf Infrastruktur beziehen.

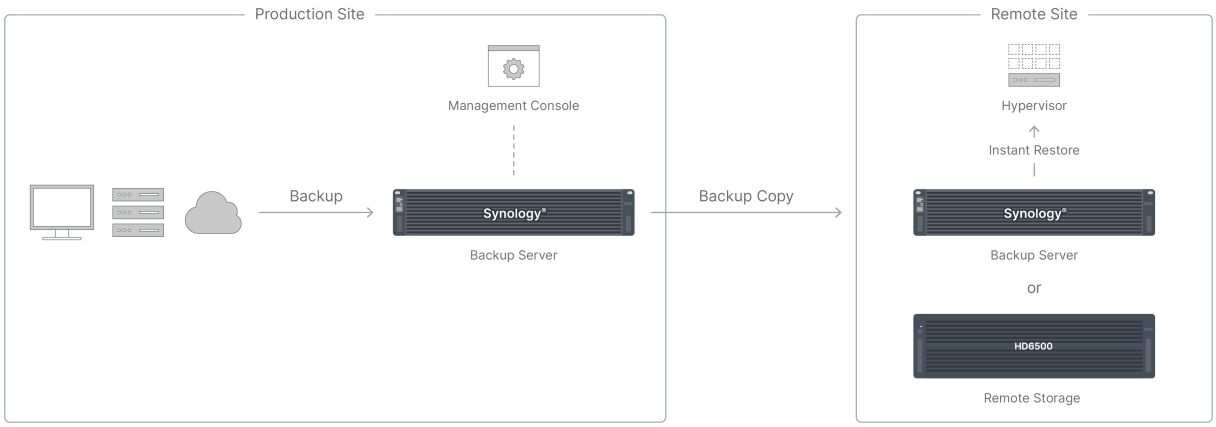
## Einzelstandortbereitstellung




Wenn Ihre Organisation nur ein Büro hat, können Sie ein einzelnes Set aus Backup-Server und Remote-Speicher bereitstellen, um Arbeitslasten zu minimalen Kosten zu schützen:

- **1 Backup-Server**: Richten Sie ein ActiveProtect-Gerät ein, um Ihre Arbeitslasten zu sichern, wiederherzustellen und zu speichern. Dieses Backup-Gerät dient auch als Verwaltungsserver Ihres Standorts.
- **1 Cloud-Remote-Speicher**: Implementieren Sie die 3-2-1-1-Backup-Strategie, indem Sie Sicherungskopien extern speichern, um die Auswirkungen einzelner Ausfallpunkte zu reduzieren. Wir empfehlen die Verwendung von C2 Object Storage als Ihren Remote-Speicher aufgrund seiner nativen Datenunveränderlichkeit und Objektversionierung.

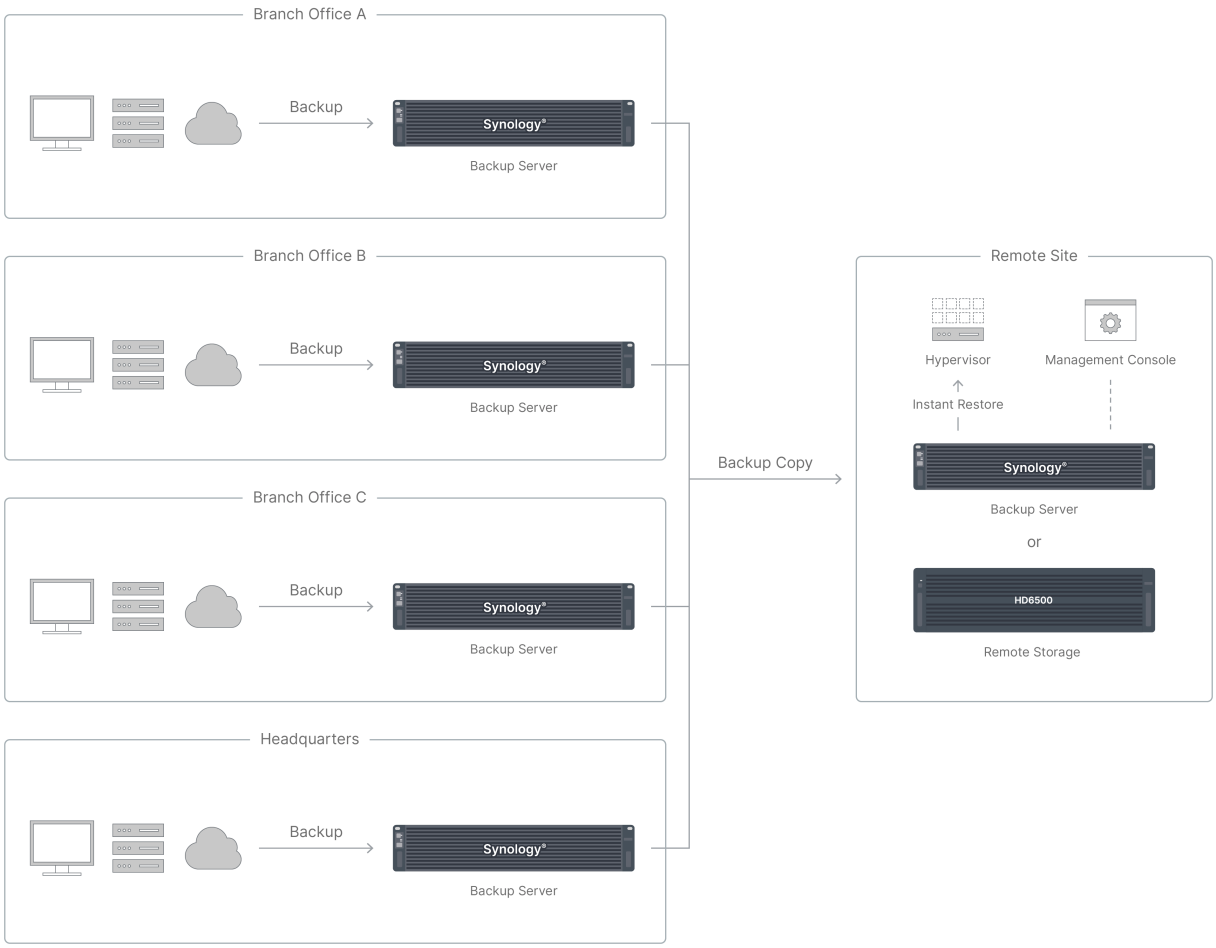
# Allgemeine Bereitstellung




Neben der Sicherung von Arbeitslasten ist es wichtig, Wiederherstellungsübungen durchzuführen, um sicherzustellen, dass Ihre Organisation auf die Notfallwiederherstellung vorbereitet ist. Die Zentralisierung all dieser Aufgaben auf einem Server kann die Leistung beeinträchtigen. Um sowohl die Leistung als auch die Datenwiederherstellbarkeit zu gewährleisten, empfehlen wir, einen Standort wie folgt einzurichten:

- **2 Backup-Server**: Richten Sie zwei ActiveProtect-Geräte ein, eines als primären Backup-Server und das andere zur Speicherung von Sicherungskopien[1] extern und zur Durchführung regelmäßiger Wiederherstellungsübungen.
    - **Verwaltungsserver und Failover-Server**: Weisen Sie einen Backup-Server als Verwaltungsserver zur Überwachung des Standortstatus und der Aktivitäten zu, während Sie den anderen als Failover-Server konfigurieren, um eine unterbrechungsfreie Verwaltung zu gewährleisten.
- **1 Hypervisor**: Stellen Sie physische Server und virtuelle Maschinen auf einem externen Hypervisor wieder her. Dies hilft Ihnen, regelmäßige Wiederherstellungsübungen und Labortests durchzuführen, ohne Ihre ursprünglichen Maschinen zu beeinträchtigen.

# Verteilte Bereitstellung




Große Unternehmen besitzen große Mengen an Daten und Maschinen und benötigen daher eine Backup-Lösung, die Leistung, Skalierbarkeit und hohe Verfügbarkeit garantiert. Um Daten umfassend zu schützen und diese Kriterien zu erfüllen, empfehlen wir die Einführung eines verteilten Bereitstellungsansatzes: Richten Sie mehrere Backup-Server ein und verteilen Sie die Arbeitslasten auf diese:

- **Mehrere Backup-Server**: Richten Sie mehrere ActiveProtect-Geräte ein, die mit Ihrer Datengröße und Netzwerkarchitektur übereinstimmen, und platzieren Sie sie in jedem Büro für optimale Backup-Effizienz. Außerdem können Sie einen Backup-Server an einem Notfallwiederherstellungsstandort einrichten, um Sicherungskopien[1] zu speichern und Wiederherstellungsübungen durchzuführen.
  - **Verwaltungsserver und Failover-Server**: Weisen Sie einen Backup-Server als Verwaltungsserver zur Überwachung des Standortstatus und der Aktivitäten zu, während Sie den Remote-Backup-Server als Failover konfigurieren, um eine unterbrechungsfreie Verwaltung zu gewährleisten.
- **1 Hypervisor**: Stellen Sie physische Server und virtuelle Maschinen auf einem externen Hypervisor wieder her, um sicherzustellen, dass regelmäßige Wiederherstellungsübungen und Labortests durchgeführt werden, ohne die ursprünglichen Arbeitslasten zu beeinträchtigen.

### Hinweis:

1. Sicherungskopien können auf externen ActiveProtect-Geräten oder Remote-Speicher (wie HD6500) gespeichert werden. Setzen Sie sie als Backup-Kopierserver basierend auf Ihren Bedürfnissen ein:
   - **Allgemeine Nutzung**: Verwenden Sie ActiveProtect-Geräte für die direkte Datenwiederherstellung, im Gegensatz zu Remote-Speicher, der das Streamen von Daten über Backup-Server für

Wiederherstellungsaufgaben erfordert.

- **Längerfristige Aufbewahrung**: Wählen Sie Remote-Speicher, wenn Sie Daten über einen längeren Zeitraum speichern müssen.

# ActiveProtect-Navigation

**ActiveProtect Manager(APM)** ist das webbasierte Betriebssystem für Synology ActiveProtect-Geräte. Die intuitive Benutzeroberfläche erleichtert den Schutz Ihrer Daten, optimiert sowohl die Sicherungs- als auch die Wiederherstellungsleistung und bietet eine benutzerfreundliche Erfahrung.

## APM-Portale

APM verfügt über die folgenden Webportale, mit denen Sie ActiveProtect-Geräte umfassend verwalten können:

| Portal | Funktionen |
| --- | --- |
| Verwaltungscenter | • Ein ActiveProtect-Standort bereitstellen und überwachen (siehe Infrastruktur)<br>• Workloads und Pläne verwalten (siehe Sicherung & Sicherungskopie)<br>• Benutzer und Berechtigungen verwalten (siehe Benutzerverwaltung)<br>• Standortstatus und Aktivitäten prüfen (siehe Überwachung)<br>• Sicherungsdaten wiederherstellen (siehe Datenwiederherstellung) |
| Wiederherstellungsportal | • Benutzern erlauben, die Sicherungsdaten selbstständig wiederherzustellen |
| Gerätekonsole | • Systemwartungseinstellungen für Ihr ActiveProtect-Gerät verwalten, wie z.B. Netzwerk- und Ressourcennutzung |

## Anmelden beim ActiveProtect Manager

1. Stellen Sie sicher, dass Ihr Computer und das ActiveProtect-Gerät sich im selben lokalen Netzwerk befinden.
2. Melden Sie sich bei den Portalen mit einer der folgenden URLs an:

| Portal | Zugriffsmethode | Beispiel |
| --- | --- | --- |
| Verwaltungscenter | • *https://Management-IP oder FQDN des Geräts*[1] | • https://backup-1.synology.com |
| Wiederherstellungsportal | • *https://IP oder FQDN des Geräts*/portal | • https://backup-1.synology.com/portal |
| Gerätekonsole | • *https://Management-IP oder FQDN des Geräts*[1]:5001 | • https://backup-1.synology.com:5001 |

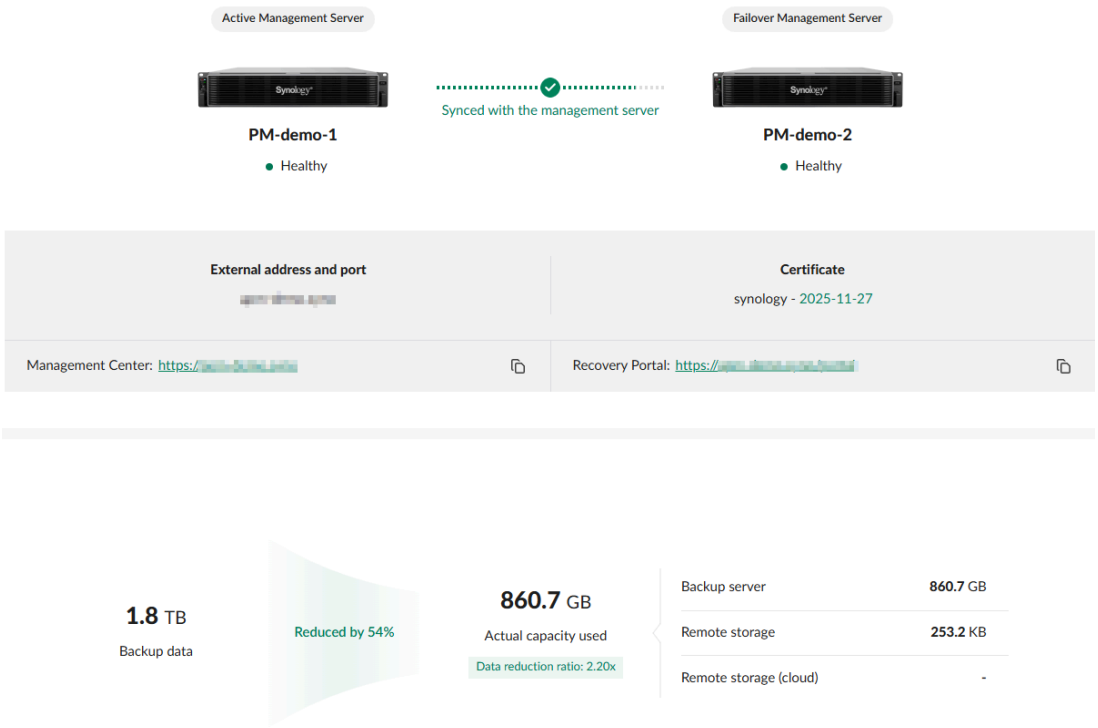
**Hinweis:**

1. Standardmäßig können Verwaltungscenter und Gerätekonsole nur über die **Management-Schnittstelle** zugegriffen werden. Erfahren Sie mehr
2. Wenn Sie weiterhin Schwierigkeiten haben, Ihre Serveradresse zu finden, versuchen Sie, Ihr Gerät mit find.synology.com oder Synology Assistant zu finden. Erfahren Sie mehr

# Infrastruktur

In diesem Abschnitt erfahren Sie, wie Sie Ihre Backup-Infrastruktur für Ihre ActiveProtect-Website einrichten und verwalten. Sie lernen, wie Sie wichtige Komponenten wie Backup-Server, Remote-Speicher und Hypervisoren bereitstellen, um den Anforderungen Ihrer Arbeitsumgebung gerecht zu werden.

Sobald Ihre Infrastruktur eingerichtet ist, können Sie den Status Ihrer Management- und Failover-Server, die Datennutzung und die Lizenzdetails von einem einzigen Dashboard aus überwachen.




## In diesem Abschnitt

- ActiveProtect-Geräte verwalten
- Synology NAS verwalten
- Remote-Speicher bereitstellen
- Hypervisoren bereitstellen
- Failover konfigurieren und initiieren

# ActiveProtect-Geräte verwalten

Mit dem ActiveProtect Manager (APM) können Sie mehrere Sicherungsgeräte zentral von einer einzigen Konsole aus verwalten, was die Verwaltung vereinfacht und die Betriebseffizienz maximiert.

Sobald Sie Sicherungsgeräte zu einer ActiveProtect-Site hinzufügen:

- Sicherungsgeräte können auf Site-Ressourcen zugreifen und diese gemeinsam nutzen, einschließlich Hypervisoren und Remote-Speicher, und als Sicherungs- oder Sicherungskopieziel für PCs/Macs, physische und virtuelle Maschinen sowie SaaS-Anwendungen dienen.
- Alle Aktivitäten der Sicherungsgeräte können zentral auf dem Verwaltungsserver überwacht werden.
- Konfigurationen und Systemaktualisierungen der Sicherungsgeräte können vom Verwaltungsserver aus verwaltet werden.

## In diesem Abschnitt

# ActiveProtect-Geräte hinzufügen

Sie können mehrere ActiveProtect-Geräte zu einer ActiveProtect-Site hinzufügen. Sobald das Sicherungsgerät der Site beitritt:

- Workload-Details und Versionen auf dem Sicherungsgerät werden mit dem Verwaltungsserver synchronisiert.
- Auf dem Sicherungsgerät konfigurierte Schutzpläne werden auf den Verwaltungsserver repliziert.
- Remote-Speicher und Hypervisoren, die mit dem Sicherungsgerät verbunden sind, werden automatisch zu gemeinsamen Ressourcen innerhalb der Site.
- Domain- und LDAP-Einstellungen des Sicherungsgeräts werden nach dem Beitritt zur Site zurückgesetzt.
- Alle lokalen Benutzer auf dem Sicherungsgerät, mit Ausnahme des Superadministrators, werden deaktiviert.

## Bevor Sie beginnen

### Externe Adresse einrichten

Wir empfehlen dringend, die externe Adresse Ihres Verwaltungsservers als vollständig qualifizierten Domainnamen (FQDN) zu konfigurieren, damit alle Sicherungsserver eine Verbindung herstellen können. Dies verhindert die Notwendigkeit, die Verbindung jedes Sicherungsservers neu zu konfigurieren, wenn sich die IP-Adresse ändert, und sorgt für reibungslose Failovers.

1. Gehen Sie auf Ihrem Verwaltungsserver zu **Infrastruktur** > **Site-Management**.
2. Klicken Sie unter **Externe Adresse und Port** auf **Einrichten**:
   - **Externe Adresse**: Standardmäßig ist dies die IP-Adresse der Out-of-band (OOB)-Schnittstelle. Wenn Sie sie als FQDN festlegen, stellen Sie sicher, dass der FQDN auf die OOB-Schnittstellenadresse auf Ihrem DNS-Server verweist.
   - **Port**: Standardmäßig ist dies 443. Wenn der verwaltete Server und der Verwaltungsserver in unterschiedlichen Netzwerken sind, stellen Sie sicher, dass der externe Port auf Port 443 auf Ihrem Gateway oder Router umgeleitet wird.

### Zertifikate importieren

Standardmäßig verwendet das System ein selbstsigniertes Zertifikat, um Verbindungen für das Site-Management zu sichern. Sie können auch Zertifikate manuell importieren, damit andere Server dem Verwaltungsserver vertrauen. Erfahren Sie, wie Sie Zertifikate für das Site-Management importieren

### Sicherungsserver-Kontingent prüfen und Lizenzen aktivieren

Um mehrere ActiveProtect-Geräte zu verwalten, stellen Sie sicher, dass Sie über genügend Sicherungsserver-Kontingent verfügen.

Um Ihr Kontingent zu überprüfen, melden Sie sich bei Ihrem Verwaltungsserver an und gehen Sie zu **Infrastruktur** > **Site-Management**. Wenn das Kontingent nicht ausreicht, müssen Sie eine Lizenz für Ihre

ActiveProtect-Site aktivieren. Erfahren Sie, wie Sie Lizenzen aktivieren

### Zeit zwischen Servern synchronisieren

Um die Datenkonsistenz zu gewährleisten, synchronisieren Sie die Zeit auf beiden Servern:

1. Gehen Sie zu **Infrastruktur** > **Sicherungsserver** und wählen Sie Ihren Server aus.
2. Klicken Sie auf **Mehr** > **Gerätekonsole öffnen**.
3. Gehen Sie zu **Systemsteuerung** > **Regionale Optionen** > **Zeit** und wählen Sie **Mit NTP-Server synchronisieren**.
4. Stellen Sie sicher, dass beide Server mit demselben NTP-Server synchronisiert sind.

**Hinweis:**

- Wenn der verwaltete Server und der Verwaltungsserver nicht im selben Netzwerk sind, stellen Sie sicher, dass die Firewall Port 8443 zulässt.
- ActiveProtect-Gerät Tower-Serie **kann nicht** als Verwaltungs- oder Failover-Server eingerichtet werden.

## Sicherungsgeräte hinzufügen

### Auf dem Verwaltungsserver

1. Führen Sie eine der folgenden Aktionen aus, um den Assistenten zu starten:
   - Gehen Sie zu **Infrastruktur** > **Site-Management** > **Site-Einstellungen** > **Sicherungsserver hinzufügen** und klicken Sie auf **Hinzufügen**.
   - Gehen Sie zu **Infrastruktur** > **Sicherungsserver** und klicken Sie auf **Hinzufügen**.
2. Kopieren Sie die Serveradresse und den Verbindungsschlüssel.

### Auf dem zu verwaltenden Backup-Gerät

1. Gehen Sie zu **Infrastruktur** > **Standortverwaltung** > **Standorteinstellungen** > **ActiveProtect-Site beitreten** und klicken Sie auf **Beitreten**.
2. Fügen Sie die externe Adresse und den Verbindungsschlüssel ein, die vom Verwaltungsserver kopiert wurden.
3. Folgen Sie dem Assistenten, um den Vorgang abzuschließen.

**Hinweis:**

- Um der Site beizutreten, muss der Backup-Server mit der Version des Verwaltungsservers kompatibel sein. Erfahren Sie mehr über die Serverkompatibilität
- Workloads benötigen einige Zeit, um sich zu synchronisieren, selbst nachdem das Backup-Gerät erfolgreich der ActiveProtect-Site beigetreten ist. Vermeiden Sie es, die Workloads zu verwalten, bis der Synchronisierungsprozess abgeschlossen ist.
- Nach dem Beitritt zur ActiveProtect-Site können Sie weiterhin den Verbindungs- und Gesundheitsstatus des verwalteten Servers anzeigen:

- Wenn **Kritisch** oder **Aufmerksamkeit** angezeigt wird, melden Sie sich bei Ihrem Verwaltungsserver an, gehen Sie zu **Infrastruktur** > **Backup-Server** und wählen Sie den verwalteten Server aus, um dessen Details anzuzeigen.
- Wenn **Getrennt** angezeigt wird, können Sie zur **Gerätekonsole** des verwalteten Servers gehen, um den Laufwerkszustand zu überprüfen.

# Details des Backup-Geräts anzeigen

Sie können zu **Infrastruktur** > **Backup-Server** gehen und auf Ihr Backup-Gerät klicken, um dessen Details und Einstellungen anzuzeigen.

## Informationen

Unter **Informationen** können Sie die folgenden Details anzeigen:

- **Informationen**: Allgemeine Informationen des Backup-Geräts, einschließlich des Status und der Speichernutzung des Backup-Geräts.
- **Zusammenfassung der Datenreduktion:**
  - **Logische Schutzdatengröße**: Gesamte Größe der durch das Backup-Gerät geschützten Daten vor der Deduplizierung.
  - **Physische Schutzdatengröße:** Gesamte Größe der auf dem Backup-Gerät gespeicherten Daten nach der Deduplizierung.
  - **Deduplizierungsverhältnis:** Verhältnis der logischen Schutzgröße zur physischen Schutzgröße.
- **Speichernutzungstrend:** Gesamte Größe der auf dem Backup-Gerät gespeicherten Daten nach der Deduplizierung.
- **Übertragene Datenmenge**: Die Menge der ein- und ausgehenden Daten, gemessen in Megabyte.

## Konnektivität

Unter **Konnektivität** können Sie die folgenden Einstellungen anzeigen und anpassen:

- **Externer Zugriff**: Bearbeiten Sie FQDN, IP-Adresse und Portinformationen. Hier können Sie auch auf **Zertifikat verwalten** klicken, um Zertifikate zu erstellen, zu bearbeiten, zu exportieren und zu löschen.
- **Netzwerkschnittstelle**: Anzeigen der Netzwerkkonfiguration des Backup-Geräts.
- **Datenport-Einstellung**: Stellen Sie sicher, dass die folgenden Dienste verfügbar sind, wenn Sie über den Datenport eine Verbindung zum Backup-Gerät herstellen:
  - Verwaltungscenter
  - Gerätekonsole
  - Standortauthentifizierung für Backup-Server und Agenten, die dem Standort beitreten
  - Zugänglichkeit der Datenoberfläche zu Verwaltungsdiensten

## Speicher

Unter **Speicher** > **Laufwerksinformationen** können Sie die folgenden Details anzeigen:

- Steckplatz
- Laufwerksmodell

- Seriennummer
- Kapazität
- Zuweisungsrolle
- Gesundheitsstatus

## Bandbreitenkontrolle

Unter **Bandbreitenkontrolle** können Sie Regeln festlegen, um den ein- und ausgehenden Datenverkehr zum und vom Backup-Server zu begrenzen. Erfahren Sie mehr über die Bandbreitenkontrolle

## Air Gap

Unter **Air Gap** können Sie die Firewall- und Isolierungseinstellungen für Ihr ActiveProtect-Gerät anzeigen und anpassen. Erfahren Sie mehr über Air Gap

# Bandbreitenkontrolle konfigurieren

Durch effektives Management des eingehenden und ausgehenden Datenverkehrs auf Sicherungsgeräten wird verhindert, dass Sicherungs- oder Datenübertragungsaktivitäten die Bandbreite Ihrer Organisation verbrauchen.

## Bandbreitenkontrolle im ActiveProtect Manager

ActiveProtect ermöglicht es Ihnen, die gesamten eingehenden und ausgehenden Bandbreitengrenzen für jedes Sicherungsgerät anzupassen. Um die Auswirkungen der Datenübertragung auf die Produktionsnetzwerkbandbreite zu minimieren, können Sie externe Netzwerkverbindungen einschränken, wenn Sie Sicherungsdaten extern oder in die Cloud kopieren. Sie können auch bestimmte Segmente einschränken, um Endpunktsicherungen auf das Sicherungsgerät über Wi-Fi oder VPN zu optimieren.

Die konfigurierte Bandbreite wird gleichmäßig auf alle gleichzeitig verarbeiteten Jobs innerhalb des Sicherungsgeräts verteilt. Bandbreitenbeschränkungen gelten für alle Netzwerkschnittstellen und Ports und beschränken den gesamten eingehenden und ausgehenden Datenverkehr. Dies umfasst UI-Operationen, Sicherungen, Sicherungskopien, Wiederherstellungen und Download-Jobs.

Zusätzlich können Sie mehrere Bandbreitenkontrollregeln für jedes Sicherungsgerät festlegen, um verschiedene Verkehrsanforderungen in unterschiedlichen Segmenten zu adressieren.

## Bandbreitenkontrollregel hinzufügen

1. Gehen Sie zu **Infrastruktur** > **Sicherungsserver**.
2. Wählen Sie ein Sicherungsgerät > **Bandbreitenkontrolle** > **Regel hinzufügen**.
3. Geben Sie die folgenden Informationen ein:
    - **Name**
    - **Typ**: Eingehend oder ausgehend
    - **Regel anwenden auf**:
        - **Spezifische IP-Adressen**
        - **Spezifischer IP-Bereich**
        - **Spezifisches Subnetz**
        - **Öffentliche IP-Adressen**[1]
    - **Bandbreitengrenze**
4. Klicken Sie auf **Hinzufügen**.

**Hinweis:**

1. Jede IPv4-Adresse außerhalb der folgenden Bereiche wird als öffentliche IP-Adresse betrachtet:
    - 10.0.0.0/8
    - 172.16.0.0/12

- 169.254.0.0/16

## Szenario zur Konfiguration von Bandbreitenkontrollregeln

Sie können mehrere Bandbreitenkontrollregeln hinzufügen. Bei Regelkonflikten haben höher gelistete Regeln Vorrang. Wenn mehrere Geräte derselben Regel folgen, wird die Bandbreite während gleichzeitiger Aktivitäten gleichmäßig auf diese Geräte verteilt.

### Beispiel:

**Regel A**: Begrenzt den gesamten eingehenden Datenverkehr von 10.17.1.1-10.17.1.100 auf 100 MB/s

**Regel B**: Begrenzt den gesamten eingehenden Datenverkehr von 10.17.1.50-10.17.1.155 auf 200 MB/s

- **Regel A** hat Vorrang vor **Regel B**.
- Wenn Gerät A (befindet sich bei 10.17.1.20) sichert, wird **Regel A** angewendet.
- Wenn Gerät B (befindet sich bei 10.17.1.70) sichert, wird **Regel A** angewendet.
- Wenn Gerät C (befindet sich bei 10.17.1.110) sichert, wird **Regel B** angewendet.
- Da sowohl Gerät A als auch Gerät B **Regel A** folgen, werden jedem Gerät 50 MB/s zugewiesen, wenn sie gleichzeitig sichern.

# Luftspalt konfigurieren

Ein Luftspalt ist eine Sicherheitsmaßnahme, die Ihren Sicherungsserver isoliert und das Risiko von Ransomware-Angriffen erheblich reduziert, indem die Bedrohungsexposition begrenzt wird. Sie können einen Luftspalt für jedes ActiveProtect-Gerät auf der Site einrichten, indem Sie unbefugten Zugriff einschränken und das Sicherungsgerät während bestimmter Zeiträume entweder logisch oder physisch isolieren.

Bevor Sie beginnen, lesen Sie Einen Luftspalt einrichten für Bereitstellungs- und Netzwerkanforderungen. Wir empfehlen **den Luftspalt auf Sicherungskopierserver anzuwenden** anstatt auf primäre Sicherungsserver für optimalen Schutz.

Um einen Luftspalt zu konfigurieren, gehen Sie zu **Infrastruktur** > **Sicherungsserver**, wählen Sie Ihren Server aus und wählen Sie dann **Luftspalt**.

## Unbefugten Zugriff einschränken

Sie können den Zugriff auf Ihr ActiveProtect-Gerät einschränken, indem Sie zulässige IP-Adressen angeben. Gehen Sie wie folgt vor:

1. Gehen Sie zu **Luftspalt** > **Firewall-Einstellungen**.
2. Wählen Sie **Nur bestimmte IP-Adressen zulassen**. Diese Option verweigert alle eingehenden Verbindungen außer denen auf der Freigabeliste.

**Hinweis:**

- Die Firewall-Einstellungen gelten nur für die Datenschnittstellen. Die Verwaltungsschnittstelle ist nicht eingeschränkt, da empfohlen wird, sie in einem separaten Netzwerk einzurichten. Mehr erfahren
- Um ununterbrochene Sicherungskopien zu gewährleisten, werden die IP-Adressen der Datenschnittstellen aller Sicherungsserver auf der Site automatisch zur Standard-Freigabeliste hinzugefügt. Die Standard-Freigabeliste kann nicht geändert werden.

## Isolationszeitplan und -methode festlegen

Sie können den Isolationszeitplan und die Methode für Ihr ActiveProtect-Gerät konfigurieren, indem Sie diese Schritte befolgen:

1. Gehen Sie zu **Luftspalt** > **Isolationseinstellungen**.
2. Klicken Sie auf **Alle Verbindungen verweigern** und richten Sie den Isolationszeitplan mit dem Zeitplan ein.[1]
3. Um die Isolationsmethode anzupassen, klicken Sie auf das Zahnradsymbol neben **Alle Verbindungen verweigern** und wählen Sie eine der folgenden Optionen:
    - **Alle Verbindungen verweigern**: Dies blockiert alle eingehenden Verbindungen über die Firewall während der Isolationsperiode, einschließlich IP-Adressen in der Freigabeliste.
    - **Netzwerkschnittstellenkarten (NICs) deaktivieren**: Dies deaktiviert die Datennetzwerkschnittstelle, was zu fehlgeschlagenen eingehenden und ausgehenden Verbindungen während der

Isolationsperiode führt.

- **Server herunterfahren**: Das Sicherungsgerät wird während der Isolationsperiode automatisch heruntergefahren und startet neu, wenn sie endet. Um ununterbrochene Dienste zu gewährleisten, empfehlen wir nicht, einen Luftspalt auf die Verwaltungs- oder Failover-Server anzuwenden.

Um minimale Unterbrechungen der Sicherungsaktivitäten zu gewährleisten, empfehlen wir, einen Luftspalt auf Sicherungskopierserver anzuwenden. Sehen Sie in der folgenden Tabelle nach, wie sich jede Isolations-Einstellung auf Sicherungskopien auswirkt, die auf den luftgesperrten Server übertragen werden:

| | Alle Verbindungen verweigern | Netzwerkschnittstellenkarten deaktivieren | Server herunterfahren |
|---|---|---|---|
| **Sicherungskopien, die auf den luftgesperrten Server übertragen werden** | • Sicherungskopien werden vorübergehend über die Verwaltungsnetzwerkschnittstelle übertragen. | | • Unvollständige Sicherungskopien werden fortgesetzt, sobald die Isolation endet. |

Wir empfehlen nicht, einen Luftspalt auf die primären Sicherungsserver anzuwenden, da dies die Sicherungsaktivitäten beeinträchtigen könnte. Sehen Sie in der folgenden Tabelle nach, wie Aktivitäten auf dem primären Sicherungsserver durch Isolations-Einstellungen beeinflusst werden können:

| | Alle Verbindungen verweigern | Netzwerkschnittstellenkarten deaktivieren | Server herunterfahren |
|---|---|---|---|
| **Agentenbasierte Sicherungen** | • Alle laufenden Sicherungen versuchen, bis zu 72 Stunden lang eine Verbindung zum Server herzustellen. Wenn dies nicht erfolgreich ist, werden die Sicherungen abgebrochen.<br>• Aufgaben, die noch nicht gestartet wurden, beginnen, sobald der Server wieder online ist. Wenn mehrere Sicherungsversionen verpasst wurden, wird nur die neueste Version erstellt. | | |

<table>
<tr><td>Virtuelle Maschinen-Sicherungen (Hyper-V)</td><td colspan="2"><ul><li>Alle laufenden Sicherungen werden versuchen, sich bis zu 72 Stunden lang mit dem Server zu verbinden. Wenn dies nicht erfolgreich ist, werden die Sicherungen abgebrochen.</li><li>Aufgaben, die noch nicht gestartet wurden, beginnen, sobald der Server wieder online ist. Wenn mehrere Sicherungsversionen verpasst wurden, wird nur die neueste Version erstellt.</li></ul></td><td rowspan="4"><ul><li>Laufende Sicherungen werden abgebrochen.</li><li>Sicherungen können während der Isolation nicht geplant oder ausgelöst werden.</li></ul></td></tr>
<tr><td>Virtuelle Maschinen-Sicherungen (VMware)</td><td rowspan="3"><ul><li>Sicherungen sind nicht betroffen.</li></ul></td><td rowspan="3"><ul><li>Laufende und geplante Sicherungen werden fehlschlagen.</li></ul></td></tr>
<tr><td>Dateiserver-Sicherungen</td></tr>
<tr><td>Microsoft 365-Sicherungen</td></tr>
<tr><td>Sicherungskopien, die auf andere ActiveProtect-Geräte übertragen werden</td><td><ul><li>Sicherungskopien sind nicht betroffen.</li></ul></td><td colspan="2"><ul><li>Laufende und geplante Sicherungskopien werden fortgesetzt, sobald die Isolation endet.</li></ul></td></tr>
</table>

**Hinweis:**

1. Der Isolationszeitplan wird nicht durch laufende Sicherungen oder Sicherungskopien verzögert.

# Luftspaltintervalle planen

Um sicherzustellen, dass Ihr Sicherungsgerät genügend Zeit hat, um notwendige Aufgaben abzuschließen, bevor ein Luftspalt angewendet oder erneut angewendet wird, müssen Sie die Zeit bestimmen, die das Sicherungsgerät zugänglich bleiben sollte. Dies kann anhand der Datenmenge geschätzt werden, die während der Sicherung kopiert werden muss.

Verwenden Sie die folgende Formel, um die insgesamt zu kopierenden Daten zu schätzen:

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Gesamtdatenmenge, die kopiert werden soll** | = | Jede Workload-Datengröße | x | Änderungsrate | x | Deduplizierungsrate (Normalerweise 50%) | x | Workload-Anzahl |

Die Netzwerkgeschwindigkeit sollte ebenfalls berücksichtigt werden, wenn die Zeit für jede Sicherungskopie berechnet wird.

# ActiveProtect-Geräte ausschalten und neu starten

Um ein Backup-Gerät auszuschalten oder neu zu starten, gehen Sie zu **Verwaltung** > **Infrastruktur** > **Backup-Server**. Wählen Sie ein Backup-Gerät aus und klicken Sie auf **Mehr**, dann wählen Sie, ob Sie **Neustart** oder **Herunterfahren** möchten.

**Hinweis:**

- Ein Verwaltungsserver, der ausgeschaltet oder neu gestartet wird, kann vorübergehend keine anderen Server verwalten.
- Verwaltete Backup-Geräte, die ausgeschaltet oder neu gestartet werden, verlieren vorübergehend die Fähigkeit, mit dem Verwaltungsserver zu synchronisieren oder von ihm verwaltet zu werden.

# ActiveProtect-Geräte aktualisieren

ActiveProtect Manager ruft automatisch die neuesten Updates vom Download-Zentrum ab, um sicherzustellen, dass Ihr Sicherungsgerät immer für die Installation bereit ist.

Sie können automatische Updates planen, um Sicherungsgeräte auf dem neuesten Stand zu halten, oder manuelle Updates wählen, um mehr Flexibilität und Kontrolle über den Zeitpunkt zu haben.

Um Kompatibilität und ununterbrochene Dienste zu gewährleisten, empfehlen wir, dass alle Server auf der Site dieselbe Version verwenden.

**Hinweis:**

- Konfigurationen, die auf dem Verwaltungsserver vorgenommen werden, werden auf alle Sicherungsgeräte angewendet und überschreiben deren ursprüngliche Einstellungen.

## Sicherungsgeräte automatisch aktualisieren

1. Gehen Sie zu **Infrastruktur** > **Site-Management** > **Site-Einstellungen** > **Server-Update-Richtlinie konfigurieren**.
2. Klicken Sie auf das Bearbeitungssymbol neben **Automatisch aktualisieren um** und wählen Sie eine der folgenden Optionen:
   - **Updates nicht automatisch installieren**: Diese Option ermöglicht es Ihnen dennoch, Benachrichtigungen zu erhalten, wenn das neueste Update verfügbar ist.
   - **Neueste Updates automatisch installieren** (empfohlen): Nach Abschluss der laufenden Aufgaben wird das Update gemäß dem konfigurierten Zeitplan auf alle Sicherungsgeräte innerhalb der Site installiert.

**Hinweis:**

- Updates werden nicht fortgesetzt, wenn der Verwaltungsserver Dienste ausführt, heruntergefahren oder offline ist. Sie müssen auf das nächste geplante Update warten.
- Wenn einige Sicherungsserver die Update-Dateien (.pat) nicht abgerufen haben, werden automatische Updates nicht fortgesetzt. In diesem Fall müssen Sie die Update-Dateien (.pat) für alle Server innerhalb der Site erneut hochladen.

## Alle Sicherungsgeräte manuell aktualisieren

1. Gehen Sie zu **Infrastruktur** > **Site-Management** > **Site-Einstellungen** > **Server-Update-Richtlinie konfigurieren**.
2. Wenn Ihre Server in einem internen Netzwerk sind, werden sie die Update-Dateien (.pat) nicht automatisch abrufen. In diesem Fall müssen Sie die Dateien vom Download-Zentrum beziehen und manuell hochladen.
3. Klicken Sie auf **Jetzt alle Server aktualisieren**.

**Hinweis:**

- ActiveProtect Manager kann nicht auf eine ältere Version zurückgesetzt werden. Es können nur neuere Versionen installiert werden.
- Stellen Sie sicher, dass dieselbe APM-Version für alle Server innerhalb der Site hochgeladen wird.

# Ein einzelnes Sicherungsgerät manuell aktualisieren

Wenn Sie neue Funktionen testen oder einen kritischen Sicherheitspatch auf einen gefährdeten Server anwenden müssen, können Sie ein einzelnes Sicherungsgerät manuell aktualisieren, bevor Sie die gesamte Site aktualisieren.

Das unabhängige Aktualisieren eines Servers wird jedoch im Allgemeinen nicht empfohlen, da es zu Kompatibilitätsproblemen mit anderen Diensten innerhalb der Site führen kann, was möglicherweise zu unvollständigen Aufgaben oder Dateninkonsistenzen führt.

1. Gehen Sie zu **Infrastruktur** > **Sicherungsserver** und wählen Sie das Sicherungsgerät aus, das Sie aktualisieren möchten.
2. Klicken Sie auf **Mehr** > **Manuelles Update**.
3. Laden Sie die Update-Datei (.pat) hoch, die Sie vom Download-Zentrum erhalten haben.

# Inkompatible Versionen aktualisieren

Sie können einen Versionsinkompatibilitätsstatus sehen, wenn der Sicherungsserver für ein Update in der Warteschlange steht oder sich noch im Aktualisierungsprozess befindet. Wir empfehlen, zu warten, bis das Update abgeschlossen ist, bevor Sie das Problem angehen.

Wenn das Sicherungsgerät nach Abschluss des Updates in einem inkompatiblen Zustand bleibt, können Sie den Server manuell aktualisieren.

**Hinweis:**

- Wenn der Sicherungsserver mit dem Verwaltungsserver inkompatibel ist, werden Schutz- und Archivierungspläne weiterhin wie geplant ausgeführt. Der Verwaltungsserver kann jedoch den Sicherungsserver nicht mehr verwalten, was zur Unfähigkeit führt, Workloads wiederherzustellen oder zu verwalten, einschließlich der Anpassung von Schutzplänen.

# Aktualisierungsprobleme beheben

## Unterbrochene Aktualisierungen

Wenn die Aktualisierung durch Benutzeraktionen oder unerwartete Ereignisse wie Stromausfälle unterbrochen wurde, können Sie den Server neu starten und es erneut versuchen.

## Beschädigte Aktualisierungsdateien

Das Hochladen einer beschädigten Aktualisierungsdatei (.pat) kann ebenfalls zu Aktualisierungsfehlern führen. Sie können zum Download-Zentrum gehen, um die Aktualisierungsdatei (.pat) zu erhalten und sie erneut hochzuladen.

Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support von Synology zur Unterstützung.

# ActiveProtect-Geräte entfernen

Um auf eigenständige Verwaltung umzuschalten, können Sie Ihren Sicherungsserver von der ActiveProtect-Site entfernen.

Bevor Sie Ihren Server entfernen, beachten Sie die folgenden Änderungen:

### ActiveProtect-Site

- Alle Sicherungsdaten auf diesem Server, einschließlich Workloads, Versionen und Aktivitäten, werden von der Site entfernt.
- Wenn Sicherungen auf diesem Server auf einen anderen Sicherungsserver oder Remote-Speicher kopiert wurden, werden Sie aufgefordert, während der Entfernung einen Archivierungsplan für die kopierten Daten anzuwenden.

### Entfernter Sicherungsserver

- **Workloads**: Workloads, die auf diesem Server gesichert wurden, verbleiben auf dem Server.
- **Schutzpläne**: Schutzpläne, die auf die Workloads auf diesem Server angewendet werden, werden mit dem Server synchronisiert, aber die Einstellungen für Sicherungskopien werden automatisch deaktiviert.
- **Remote-Speicher**: Remote-Speicher wird nicht mit dem Server synchronisiert, was bedeutet, dass Sicherungskataloge, die ursprünglich damit verknüpft waren, nicht mehr angezeigt oder wiederhergestellt werden können.
- **Hypervisoren**: Hypervisoren für virtuelle Maschinen, die auf diesem Server gesichert wurden, werden mit dem Server synchronisiert, aber ihre Anmeldeinformationen werden nicht gespeichert.
- **Cloud-Anwendungen**: Mandanten von Cloud-Anwendungen, die auf diesem Server gesichert wurden, werden mit dem Server synchronisiert, aber ihre Anmeldeinformationen werden nicht gespeichert.
- **Benutzer- und Gruppenberechtigungen**: Benutzer- und Gruppenberechtigungseinstellungen werden nicht mit dem Server synchronisiert. Nach der Entfernung kann sich nur der Super-Admin beim Sicherungsserver anmelden, während andere lokale Benutzer und Gruppen deaktiviert bleiben.
- **Sicherungskopien von anderen Servern**: Sicherungskopien von anderen Workloads innerhalb der Site, die auf diesem Server gespeichert wurden, werden unverwaltet.

## Sicherungsserver von der Site entfernen

Stellen Sie sicher, dass Ihre Internetverbindung stabil ist. Wenn der Sicherungsserver während der Entfernung die Verbindung zum Verwaltungsserver verliert, wechselt er erst in den eigenständigen Modus, wenn die Verbindung wiederhergestellt ist.

1. Gehen Sie zu **Infrastruktur** > **Sicherungsserver**.
2. Wählen Sie Ihren Sicherungsserver aus und klicken Sie auf **Mehr** > **Entfernen**.
3. Wählen Sie gegebenenfalls einen Archivierungsplan für verbleibende Sicherungskopiedaten aus.
4. Geben Sie den Servernamen ein, um den Server zu löschen.

**Hinweis:**

- Sicherungsserver können nicht entfernt werden, wenn:
  - Der Server ein Ziel für Sicherungskopien ist.
  - Der Server ein automatisches Sicherungsziel für Microsoft 365 Workloads ist.
  - Der Server als Failover-Server konfiguriert ist.
- Sie können die ActiveProtect-Site nicht vom Sicherungsserver aus verlassen.

# Synology NAS verwalten

Mit dem ActiveProtect Manager (APM) können Sie mehrere Synology NAS-Server zentral von einer einzigen Konsole aus verwalten, was die Verwaltung vereinfacht und die Betriebseffizienz maximiert.

Sobald Sie Synology NAS zur ActiveProtect-Site hinzufügen:

- Backups und Wiederherstellungen für Personal Computer, physische Server und virtuelle Maschinen werden zentral vom Verwaltungsserver aus durchgeführt und überwacht.
- Der grundlegende Systemstatus (z. B. Speicher) und Systeminformationen können auf dem Verwaltungsserver überwacht werden.

Weitere Informationen finden Sie im Active Backup for Business Admin Guide für ActiveProtect Manager.

**Hinweis:**

- Synology NAS kann nicht als Ziel für Backup-Kopien verwendet werden.
- Remote-Speicher ist für Synology NAS-Backups nicht verfügbar.

## In diesem Abschnitt

# Synology NAS hinzufügen

Sie können Synology NAS, die Active Backup for Business ausführen, als Sicherungsserver zur ActiveProtect-Site hinzufügen.

Verweisen Sie auf den Active Backup for Business Admin Guide für ActiveProtect Manager, um mehr über Anforderungen, Einschränkungen und Änderungen an Active Backup for Business nach dem Beitritt zu erfahren.

**Hinweis:**

- Aufgrund struktureller Unterschiede kann der ActiveProtect Manager keine Synology NAS- oder Dateiserver-Workloads verwalten. Sicherungen und Wiederherstellungen für diese Workloads werden weiterhin über Active Backup for Business verwaltet.

## Bevor Sie beginnen

### Externe Adresse einrichten

Wir empfehlen dringend, die externe Adresse Ihres Verwaltungsservers als vollständig qualifizierten Domainnamen (FQDN) zu konfigurieren, damit alle Sicherungsserver eine Verbindung herstellen können. Dies verhindert die Notwendigkeit, die Verbindung jedes Sicherungsservers neu zu konfigurieren, wenn sich die IP-Adresse ändert, und sorgt für reibungslose Failovers.

1. Gehen Sie auf Ihrem Verwaltungsserver zu **Infrastruktur** > **Site-Management**.
2. Klicken Sie unter **Externe Adresse und Port** auf **Einrichten**:
   - **Externe Adresse**: Standardmäßig ist dies die IP-Adresse der Out-of-band (OOB)-Schnittstelle. Wenn Sie es als FQDN festlegen, stellen Sie sicher, dass der FQDN auf die OOB-Schnittstellenadresse auf Ihrem DNS-Server verweist.
   - **Port**: Standardmäßig ist dies 443. Wenn der verwaltete Server und der Verwaltungsserver in verschiedenen Netzwerken sind, stellen Sie sicher, dass der externe Port auf Port 443 auf Ihrem Gateway oder Router umgeleitet wird.

### Zertifikate importieren

Standardmäßig verwendet das System ein selbstsigniertes Zertifikat, um Verbindungen für das Site-Management zu sichern. Sie können auch Zertifikate manuell importieren, damit andere Server dem Verwaltungsserver vertrauen. Erfahren Sie, wie Sie Zertifikate für das Site-Management importieren

### Sicherungsserver-Kontingent überprüfen und Lizenzen aktivieren

Um Synology NAS-Server zu verwalten, die Active Backup for Business ausführen, stellen Sie sicher, dass Sie über genügend Sicherungsserver-Kontingent verfügen.

Um Ihr Kontingent zu überprüfen, melden Sie sich bei Ihrem Verwaltungsserver an und gehen Sie zu **Infrastruktur** > **Site-Management**. Wenn das Kontingent nicht ausreicht, müssen Sie eine Lizenz für Ihre

ActiveProtect-Site aktivieren. Erfahren Sie, wie Sie Lizenzen aktivieren

### Zeit zwischen Servern synchronisieren

Um die Datenkonsistenz zu gewährleisten, synchronisieren Sie die Zeit auf beiden Servern:

1. Gehen Sie zu **Infrastruktur** > **Sicherungsserver** und wählen Sie Ihren Server aus.
2. Klicken Sie auf **Mehr** > **Gerätekonsole öffnen**.
3. Gehen Sie zu **Systemsteuerung** > **Regionale Optionen** > **Zeit** und wählen Sie **Mit NTP-Server synchronisieren**.
4. Stellen Sie sicher, dass beide Server mit demselben NTP-Server synchronisiert sind.

**Hinweis:**

- Wenn der verwaltete Server und der Verwaltungsserver nicht im selben Netzwerk sind, stellen Sie sicher, dass die Firewall Port 8443 zulässt.
- Synology NAS kann nicht als Verwaltungs- oder Failover-Server verwendet werden.

## Synology NAS hinzufügen

### Auf dem Verwaltungsserver

1. Führen Sie eine der folgenden Aktionen aus, um den Assistenten zu starten:
   - Gehen Sie zu **Infrastruktur** > **Site-Management** > **Site-Einstellungen** > **Sicherungsserver hinzufügen** und klicken Sie auf **Hinzufügen**.
   - Gehen Sie zu **Infrastruktur** > **Sicherungsserver** und klicken Sie auf **Hinzufügen**.
2. Kopieren Sie die Serveradresse und den Verbindungsschlüssel.

### Auf dem zu verwaltenden Synology NAS

1. Gehen Sie zu **Active Backup for Business** > **Zentralisierte Verwaltung**.
2. Fügen Sie die externe Adresse und den Verbindungsschlüssel ein, die vom Verwaltungsserver kopiert wurden.
3. Folgen Sie dem Assistenten, um den Vorgang abzuschließen.

**Hinweis:**

- Um der Site beizutreten, muss der Backup-Server mit der Manager-Server-Version kompatibel sein. Erfahren Sie mehr über die Serverkompatibilität
- Erfahren Sie, wie Sie mehrere Synology NAS-Server zu einer ActiveProtect-Site hinzufügen.
- Sobald das Synology NAS der ActiveProtect-Site beitritt, synchronisiert es automatisch alle 10 Minuten seine Einstellungen, wie Verbindungsdetails, mit dem Verwaltungsserver.
- Workloads benötigen einige Zeit zur Synchronisierung, selbst nachdem das Synology NAS erfolgreich der ActiveProtect-Site beigetreten ist. Vermeiden Sie die Verwaltung der Workloads, bis der Synchronisierungsprozess abgeschlossen ist.

- Um sicherzustellen, dass das Synology NAS erfolgreich der ActiveProtect-Site beitritt, stellen Sie sicher, dass **Proxy-Server für lokale Adressen überbrücken** ausgewählt ist, wenn Sie über einen Proxy-Server verbinden.

# Details des Synology NAS anzeigen

Sie können zu **Infrastruktur** > **Backup-Server** gehen und auf Ihr Synology NAS klicken, um dessen Details und Einstellungen anzuzeigen.

## Informationen

Unter **Informationen** können Sie die folgenden Details einsehen:

- **Serverinformationen**: Allgemeine Informationen des Servers, einschließlich des Serverstatus und der Speichernutzung.
- **Sicherungsdatenübersicht**:
  - **Übertragene Datenmenge**: Gesamte Größe der durch das Synology NAS geschützten Daten vor der Deduplizierung.
  - **Tatsächlich genutzter Speicher**: Gesamte Größe der auf dem Synology NAS gespeicherten Daten nach der Deduplizierung.
  - **Deduplizierungsverhältnis**: Verhältnis der übertragenen Datenmenge zum tatsächlich genutzten Speicher.
- **Übertragene Datenmenge**: Die Menge der ein- und ausgehenden Daten, gemessen in Megabyte.

## Netzwerk

Unter **Netzwerk** können Sie die DDNS- und Zertifikatseinstellungen Ihres Synology NAS einsehen.

## Speicher

Unter **Speicher** können Sie Informationen zu Speicherpools und Volumes Ihres Synology NAS einsehen.

## Vorlage

Unter **Vorlage** können Sie Active Backup for Business-Vorlagen erstellen, anzeigen, bearbeiten und löschen. Weitere Informationen finden Sie unter Sicherungs-Vorlagen konfigurieren.

# Sicherungs-Vorlagen konfigurieren

Sobald Ihr Synology NAS einem ActiveProtect-Standort beitritt, werden alle Active Backup for Business-Vorlageneinstellungen[1] für PCs, Macs und physische Server in Schutzpläne zusammengeführt und können nur vom Verwaltungsserver verwaltet werden.

Um Sicherungsvorlagen im ActiveProtect Manager zu verwalten, führen Sie die folgenden Schritte aus:

1. Gehen Sie zu **Infrastruktur** > **Sicherungsserver**.
2. Wählen Sie Ihr Synology NAS aus.
3. Gehen Sie zu **Vorlage**, um Vorlagen zu erstellen, zu bearbeiten oder zu löschen.

**Hinweis:**

1. Plattform, Standardgerätetyp, Sicherungsziel und angewendete Benutzer- oder Gruppeneinstellungen bleiben unverändert.

# Synology NAS entfernen

Um auf eigenständige Verwaltung umzuschalten, können Sie Ihren Sicherungsserver von der ActiveProtect-Site entfernen.

Bevor Sie Ihren Server entfernen, beachten Sie die folgenden Änderungen:

### ActiveProtect-Site

- Alle Sicherungsdaten auf diesem Server, einschließlich Workloads, Versionen und Aktivitäten, werden von der Site entfernt.
- Wenn Sicherungen auf diesem Server auf einen anderen Sicherungsserver kopiert wurden, werden Sie aufgefordert, während der Entfernung einen Archivierungsplan für die kopierten Daten anzuwenden.

### Entfernter Sicherungsserver

- **Workloads**: Workloads, die auf diesem Server gesichert wurden, verbleiben auf dem Synology NAS und werden von Active Backup for Business verwaltet.
- **Schutzpläne**: Schutzpläne, die auf die Workloads auf diesem Server angewendet wurden, werden mit Active Backup for Business synchronisiert und in Aufgaben umgewandelt. Alle Einstellungen, die von Active Backup for Business nicht unterstützt werden, werden automatisch entfernt.
- **Hypervisoren**: Hypervisoren für virtuelle Maschinen, die auf diesem Server gesichert wurden, werden mit Active Backup for Business synchronisiert, aber ihre Anmeldeinformationen werden nicht gespeichert.
- **Benutzer- und Gruppenberechtigungen**: Benutzer- und Gruppenberechtigungseinstellungen werden nicht mit Active Backup for Business synchronisiert. Berechtigungseinstellungen, die ursprünglich auf Active Backup for Business konfiguriert wurden, werden wiederhergestellt.

## Synology NAS von der Site entfernen

Stellen Sie sicher, dass Ihre Internetverbindung stabil ist. Wenn der Sicherungsserver während der Entfernung die Verbindung zum Verwaltungsserver verliert, wechselt er nicht in den eigenständigen Modus, bis die Verbindung wiederhergestellt ist.

1. Gehen Sie zu **Infrastruktur** > **Sicherungsserver**.
2. Wählen Sie Ihren Sicherungsserver aus und klicken Sie auf Mehr > **Entfernen**.
3. Wählen Sie gegebenenfalls einen Archivierungsplan für verbleibende Sicherungskopiedaten aus.
4. Geben Sie den Servernamen ein, um den Server zu löschen.

### Hinweis:

- Sie können die ActiveProtect-Site auch über Active Backup for Business verlassen.
- Um Sicherungen nach dem Wechsel in den eigenständigen Modus weiterlaufen zu lassen, authentifizieren Sie die Anmeldeinformationen für Hypervisoren erneut.

# Remote-Speicher bereitstellen

Um die 3-2-1-Strategie der Datensicherung effektiv umzusetzen, empfehlen wir die Verwendung skalierbarer Speichergeräte oder -dienste als Ziel für Ihre Sicherungskopie. Wenn Ihr Sicherungsserver seine Speicherkapazität erreicht, sollten Sie in Betracht ziehen, die Daten auf Remote-Speicher zu kopieren, um eine erweiterte und effiziente langfristige Aufbewahrung zu gewährleisten.

In **Infrastruktur** > **Remote-Speicher** können Sie die folgenden Remote-Speichertypen hinzufügen und verwalten:

- Synology NAS mit installiertem ActiveProtect Vault (globale Deduplizierungsfunktion enthalten)
- Objektspeicherdienste wie Amazon S3 und Synology C2 Object Storage

Bevor Sie Ihren Remote-Speicher einrichten, ist es hilfreich, die folgenden Begriffe und Konzepte zu verstehen:

- **Bucket**: Beim Einrichten von Amazon S3 oder C2 Object Storage als Remote-Speicher müssen Sie einen Bucket als Ziel für Ihre Daten auswählen. Ein Bucket ist ein Container für Objekte, die in Amazon S3 oder C2 Object Storage gespeichert sind. Sie können so viele Objekte oder Daten wie erforderlich im Bucket speichern.
- **Tresor**: Beim Einrichten von Synology NAS als Remote-Speicher müssen Sie einen Tresor als Ziel für Ihre Daten auswählen. Ein Tresor ist ein dedizierter freigegebener Ordner auf dem NAS. Daten, die im selben Tresor oder freigegebenen Ordner gespeichert sind, werden gemeinsam dedupliziert. Wir empfehlen, separate Tresore für verschiedene Standorte zu erstellen, um die Daten unabhängig zu halten. Erfahren Sie, wie Sie ActiveProtect Vault einrichten
- **Sicherungskatalog**: Sicherungskataloge werden automatisch unter Tresoren oder Buckets generiert, sobald der Kopiervorgang beginnt. Jeder Sicherungskatalog ist mit einem Sicherungsserver innerhalb des Standorts verbunden und speichert Daten, die von diesem spezifischen Sicherungsserver kopiert wurden. Der Zugriff und das Löschen von Daten im Sicherungskatalog sind ausschließlich dem zugehörigen Sicherungsserver vorbehalten.

## In diesem Abschnitt

# ActiveProtect Vault hinzufügen

Sie können Synology NAS, auf dem ActiveProtect Vault läuft, zu einer ActiveProtect-Site hinzufügen.

## Bevor Sie beginnen

- Stellen Sie sicher, dass das ActiveProtect Vault-Paket auf Ihrem Synology NAS installiert ist.
- Richten Sie freigegebene Ordner als Tresore ein. Ein Standardfreigabeordner wird bei der Installation von ActiveProtect Vault erstellt.

## Neue Tresore hinzufügen

Um Tresore hinzuzufügen, die noch nie mit einer ActiveProtect-Site verbunden waren, folgen Sie diesen Schritten:

1. Gehen Sie zu **Infrastruktur** > **Remote-Speicher** > **Hinzufügen**.
2. Wählen Sie **ActiveProtect Vault**.
3. Geben Sie die Informationen für ActiveProtect Vault ein.
4. Wenn keine Zertifikate eingerichtet sind, wird das Standardzertifikat verwendet.
5. Wählen Sie, ob Sie die clientseitige Verschlüsselung aktivieren möchten. Wir empfehlen, sie zu aktivieren oder einen verschlüsselten freigegebenen Ordner oder ein verschlüsseltes Volume für den Tresor zu verwenden.[1]

**Hinweis:**

1. Wenn die clientseitige Verschlüsselung aktiviert ist, wird der Verschlüsselungsschlüssel automatisch auf Ihren Computer heruntergeladen. Stellen Sie sicher, dass Sie den Verschlüsselungsschlüssel sicher aufbewahren, da er benötigt wird, um den Tresor mit einer anderen Site zu verknüpfen oder hinzuzufügen.

## Zuvor verwendete Tresore hinzufügen

Um Tresore hinzuzufügen, die zuvor mit einer ActiveProtect-Site verbunden waren, folgen Sie diesen Schritten:

1. Gehen Sie zu **Infrastruktur** > **Remote-Speicher** > **Hinzufügen**.
2. Wählen Sie **ActiveProtect Vault**.
3. Geben Sie die Informationen für ActiveProtect Vault ein.
4. Wenn keine Zertifikate eingerichtet sind, wird das Standardzertifikat verwendet.
5. Geben Sie den Verschlüsselungsschlüssel ein, wenn der Tresor die **Client-seitige Verschlüsselung** aktiviert hat. Wenn Sie den Schlüssel verlieren, können Sie ihn von einer ActiveProtect-Site abrufen, die derzeit mit dem Tresor unter **Infrastruktur** > **Remote-Speicher** verbunden ist.

# C2 Object Storage hinzufügen

Sie können Synology C2 Object Storage zur ActiveProtect-Site hinzufügen.

## Bevor Sie beginnen

- Stellen Sie sicher, dass ein Bucket mit aktiviertem Object Lock eingerichtet ist und die Standardaufbewahrungszeit nicht festgelegt ist. Dies ermöglicht es dem ActiveProtect Manager, die Sperrzeit basierend auf seiner Aufbewahrungsrichtlinie festzulegen.
- Stellen Sie sicher, dass der Zugriffsschlüssel für den Bucket Lese- und Schreibberechtigungen hat.
- Stellen Sie sicher, dass der Verwaltungsserver für die anfängliche Authentifizierung eine Verbindung zu "**https://s3.synologyc2.net**" herstellen kann. Nachdem Sie C2 Object Storage hinzugefügt haben, stellen Sie sicher, dass alle Backup-Server innerhalb der Site eine Verbindung zum Endpunkt des Buckets herstellen können.
- Führen Sie einen Geschwindigkeitstest durch, wenn Sie langsame Datenübertragungsraten beim Übertragen von Daten zu C2 Object Storage feststellen.

## Neue Buckets hinzufügen

Um Buckets hinzuzufügen, die noch nie mit einer ActiveProtect-Site verbunden waren, gehen Sie wie folgt vor:

1. Gehen Sie zu **Infrastruktur** > **Remote-Speicher** > **Hinzufügen**.
2. Wählen Sie **C2 Object Storage**.
3. Geben Sie die Informationen für C2 Object Storage ein.
4. Wenn keine Zertifikate eingerichtet sind, wird das Standardzertifikat verwendet.
5. Wählen Sie, ob die clientseitige Verschlüsselung aktiviert werden soll. Wir empfehlen, diese Option zu aktivieren.[1]

**Hinweis:**

1. Wenn die clientseitige Verschlüsselung aktiviert ist, wird der Verschlüsselungsschlüssel automatisch auf Ihren Computer heruntergeladen. Stellen Sie sicher, dass Sie den Verschlüsselungsschlüssel sicher aufbewahren, da er erforderlich ist, um den Bucket mit einer anderen Site zu verknüpfen oder hinzuzufügen.

## Zuvor verwendete Buckets hinzufügen

Um Buckets hinzuzufügen, die zuvor mit einer ActiveProtect-Site verbunden waren, gehen Sie wie folgt vor:

1. Gehen Sie zu **Infrastruktur** > **Remote-Speicher** > **Hinzufügen**.
2. Wählen Sie **C2 Object Storage**.

3. Geben Sie die Informationen für C2 Object Storage ein.
4. Wenn keine Zertifikate eingerichtet sind, wird das Standardzertifikat verwendet.
5. Geben Sie den Verschlüsselungsschlüssel ein, wenn der Bucket **Client-seitige Verschlüsselung** aktiviert hat. Wenn Sie den Schlüssel verlieren, können Sie ihn von einer ActiveProtect-Site abrufen, die derzeit mit dem Bucket unter **Infrastruktur** > **Remote-Speicher** verbunden ist.

# Amazon S3 hinzufügen

Sie können Amazon S3 zur ActiveProtect-Site hinzufügen.

## Bevor Sie beginnen

- Stellen Sie sicher, dass Sie einen Bucket mit aktiviertem S3 Object Lock einrichten und die standardmäßige Aufbewahrungszeit deaktiviert lassen. Dies ermöglicht es dem ActiveProtect Manager, die Sperrfrist basierend auf seiner Aufbewahrungsrichtlinie festzulegen.
- Daten im Bucket werden ausschließlich vom ActiveProtect Manager verwaltet, einschließlich Aufbewahrung und Datenmanagement. Die Aktivierung von Lebenszyklusregeln wird nicht unterstützt, da sie zu Sicherungs- und Wiederherstellungsfehlern führen können.
- Beachten Sie, dass nur **S3 Standard**-Speicherklassen unterstützt werden. Weitere Informationen finden Sie unter Amazon S3 Storage Classes.
- Stellen Sie sicher, dass der Zugriffsschlüssel für den Bucket die erforderlichen Berechtigungen hat, indem Sie die bereitgestellte JSON-Richtlinienvorlage anwenden. Weitere Informationen finden Sie unter Manage Access Keys for IAM Users von Amazon.
- Stellen Sie sicher, dass der Verwaltungsserver für die anfängliche Authentifizierung eine Verbindung zu https://s3.amazonaws.com oder https://s3.cn-north-1.amazonaws.com.cn herstellen kann. Nachdem Sie Amazon S3 hinzugefügt haben, stellen Sie sicher, dass alle Sicherungsserver innerhalb der Site eine Verbindung zum Endpunkt des Buckets herstellen können.
- Führen Sie einen Geschwindigkeitstest durch, wenn Sie langsame Datenübertragungsraten beim Sichern von Daten auf Amazon S3 feststellen.

## JSON-Richtlinienvorlage

Verwenden Sie die folgende Vorlage, um IAM-Benutzerberechtigungen und Zugriffskontrollen für den Bucket zu definieren. Ersetzen Sie "**bucket-name**" durch den Namen des S3-Buckets, den Sie hinzufügen möchten:

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Action": [
    "s3:AbortMultipartUpload",
    "s3:CompleteMultipartUpload",
    "s3:CopyObject",
    "s3:CreateMultipartUpload",
```

```
        "s3:DeleteObject",
        "s3:GetBucketLocation",
        "s3:GetBucketVersioning",
        "s3:GetObject",
        "s3:GetObjectLockConfiguration",
        "s3:GetObjectRetention",
        "s3:HeadObject",
        "s3:ListBuckets",
        "s3:ListObjectVersions",
        "s3:ListObjectsV2",
        "s3:PutObject",
        "s3:PutObjectRetention",
        "s3:UploadPart",
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::bucket-name"
    }
  ]
}
```

# Neue Buckets hinzufügen

Um Buckets hinzuzufügen, die noch nie mit einer ActiveProtect-Site verbunden waren, gehen Sie wie folgt vor:

1. Gehen Sie zu **Infrastruktur** > **Remote-Speicher** > **Hinzufügen**.
2. Wählen Sie **Amazon S3** oder **Amazon S3 China-Region**.
3. Geben Sie die Informationen für Amazon S3 ein.
4. Wenn keine Zertifikate eingerichtet sind, wird das Standardzertifikat verwendet.
5. Wählen Sie, ob Sie die clientseitige Verschlüsselung aktivieren möchten. Wir empfehlen, sie zu aktivieren oder die AWS S3 serverseitige Verschlüsselung anzuwenden.[1]

**Hinweis:**

1. Wenn die clientseitige Verschlüsselung aktiviert ist, wird der Verschlüsselungsschlüssel automatisch auf Ihren Computer heruntergeladen. Stellen Sie sicher, dass Sie den Verschlüsselungsschlüssel sicher aufbewahren, da er erforderlich ist, um den Bucket mit einer anderen Site zu verknüpfen oder hinzuzufügen.

# Zuvor verwendete Buckets hinzufügen

Um Buckets hinzuzufügen, die zuvor mit einer ActiveProtect-Site verbunden waren, gehen Sie wie folgt vor:

1. Gehen Sie zu **Infrastruktur** > **Remote-Speicher** > **Hinzufügen**.
2. Wählen Sie **Amazon S3** oder **Amazon S3 China-Region**.
3. Geben Sie die Informationen für Amazon S3 ein.
4. Wenn keine Zertifikate eingerichtet sind, wird das Standardzertifikat verwendet.
5. Geben Sie den Verschlüsselungsschlüssel ein, wenn der Bucket die **Client-seitige Verschlüsselung** aktiviert hat. Wenn Sie den Schlüssel verlieren, können Sie ihn von einer ActiveProtect-Site abrufen, die derzeit mit dem Bucket unter **Infrastruktur** > **Remote-Speicher** verbunden ist.

# Details des Remote-Speichers anzeigen

Sie können zu **Infrastruktur** > **Remote-Speicher** gehen und auf Ihren Remote-Speicher klicken, um dessen Details und Einstellungen anzuzeigen.

## Grundlegende Informationen

Unter **Allgemein** > **Grundlegende Informationen** können Sie die folgenden Details einsehen:

- **Name**: Name des Tresors oder Buckets.
- **Dienst**: ActiveProtect Vault, C2 Object Storage oder Amazon S3.
- **Clientseitige Verschlüsselung**: Verschlüsselt oder unverschlüsselt.
- **Status**:
  - **Verbunden**: Der Tresor oder Bucket ist mit dem Verwaltungsserver verbunden. Wenn es nicht verwaltete Sicherungskataloge gibt, wird deren Anzahl neben dem Status angezeigt.
  - **Getrennt**: Der Tresor oder Bucket ist vom Verwaltungsserver getrennt.
  - **Erneute Authentifizierung erforderlich**: Die Authentifizierungsdaten müssen aktualisiert werden, um eine Verbindung zum Remote-Speicher herzustellen.
  - **Fehlerhafte Tresoreinrichtung**: Dieses Problem könnte durch einen fehlenden freigegebenen Ordner oder falsche Tresoreinstellungen verursacht werden. Gehen Sie zum ActiveProtect Vault, um das Problem zu lösen.
  - **Daten beschädigt**: Daten in diesem Bucket sind beschädigt oder gelöscht. Wenden Sie sich an den technischen Support von Synology, um das Problem zu lösen.
  - **Unbekannt**: Ein unbekannter Fehler ist aufgetreten. Wenden Sie sich an den technischen Support von Synology, um das Problem zu lösen.
  - **Löschen**: Der Tresor oder Bucket wird derzeit entfernt.
- **Speicher**: Die gesamte Speicherkapazität, die vom Tresor oder Bucket genutzt wird.

## Verbindungsinformationen (nur ActiveProtect Vault)

Die Adressen der Remote-Speicherserver werden unter **Allgemein** > **Verbindungsinformationen** angezeigt. Sie können auf **Verbindung bearbeiten** klicken, um die Adresse, die Portnummer und die Zugangsschlüssel zu ändern.

## Verschlüsselungsschlüssel

Um die Datensicherheit zu gewährleisten, benötigen Sie den Verschlüsselungsschlüssel, um Ihren Remote-Speicher zu entsperren oder der ActiveProtect-Site wieder beizutreten. Bewahren Sie Ihren Verschlüsselungsschlüssel sicher auf, um den Zugriff auf Ihre Daten nicht zu verlieren.

Unter **Allgemein** > **Verschlüsselungsschlüssel** können Sie Folgendes tun:

- **Kopieren** und **Herunterladen** Sie den Verschlüsselungsschlüssel, um auf Ihren Remote-Speicher zuzugreifen.
- Klicken Sie auf **Neu generieren**, wenn Sie den Verschlüsselungsschlüssel widerrufen oder erneuern müssen. Sobald ein neuer Schlüssel generiert wird, wird der aktuelle Schlüssel deaktiviert und kann den Remote-Speicher nicht mehr entsperren. Diese Aktion hat keinen Einfluss auf Tresore oder Buckets, die mit anderen Sites verbunden sind.

## Sicherungskatalog

Jeder Sicherungskatalog wird ausschließlich von einem Sicherungsserver verwaltet. Im **Sicherungskatalog** können Sie die Details des Sicherungskatalogs einsehen. Beachten Sie die folgenden Status:

- **Verwaltet**: Der Katalog wird von einem Sicherungsserver innerhalb dieser Site verwaltet.
- **Von einer anderen Site verwaltet**: Der Katalog wird von einem Sicherungsserver einer anderen Site verwaltet.
- **Nicht verwaltet**: Der Katalog wurde zuvor von einem Sicherungsserver in einer ActiveProtect-Site verwaltet, ist aber jetzt nicht mehr verknüpft. Dieser Status tritt typischerweise auf, wenn ein Sicherungsserver entfernt wird oder wenn der Remote-Speicher der Site wieder beitritt. Auf Sicherungsdaten in nicht verwalteten Katalogen kann nicht zugegriffen werden.

  **Hinweis:**

- Der Katalog wird automatisch entfernt, wenn alle darin enthaltenen Daten gemäß den Aufbewahrungseinstellungen gelöscht werden.

# Remote-Speicher entfernen

Wenn Sie den Remote-Speicher nicht mehr benötigen, können Sie ihn von der ActiveProtect-Website entfernen.

Bevor Sie Ihren Remote-Speicher entfernen, beachten Sie die folgenden Änderungen:

- Sicherungsdaten im Remote-Speicher werden nicht gelöscht, können jedoch auch nach dem erneuten Verknüpfen nicht mehr angezeigt oder wiederhergestellt werden.
- Alle laufenden Wiederherstellungsaufgaben, die Daten aus dem Remote-Speicher abrufen, werden abgebrochen.

## Remote-Speicher entfernen

1. Gehen Sie zu **Infrastruktur** > **Remote-Speicher**.
2. Wählen Sie den Remote-Speicher aus und klicken Sie auf **Entfernen**.

**Hinweis:**

- Remote-Speicher, die als Sicherungskopieziel verwendet werden, können nicht entfernt werden.
- Um Daten dauerhaft aus einem Bucket oder Vault zu löschen, gehen Sie zu C2 Object Storage, Amazon S3 oder ActiveProtect Vault.

# Hypervisor bereitstellen

Fügen Sie Hypervisoren hinzu, um Ihre Workloads auf einer ActiveProtect-Site zu schützen. Neben der Sicherung von virtuellen Maschinen (VM) können Sie sowohl physische als auch virtuelle Maschinen als VMs auf Ihren Hypervisoren wiederherstellen.

Dieser Artikel zeigt Ihnen, wie Sie Hypervisoren hinzufügen, bearbeiten und entfernen.

## Bevor Sie beginnen

- **VMware vSphere**: Erlauben Sie erforderliche Dienste und Berechtigungen auf Ihren VM-Hosts.
- **Hyper-V**: Konfigurieren Sie die erforderlichen Einstellungen auf Ihren VM-Hosts.

## Hypervisoren hinzufügen

1. Gehen Sie zu **Infrastruktur** > **Hypervisoren** und klicken Sie auf **Hinzufügen**.
2. Wählen Sie einen Hypervisor-Typ aus.
3. Geben Sie die Serveradresse und die Kontoinformationen ein.[1]

Nach der Bereitstellung von Hypervisoren auf Ihrer Site können Sie mit dem Schutz von VMs unter **Maschinen** > **Virtuelle Maschinen** beginnen. Physische Server können ebenfalls als VMs auf Ihren Hypervisoren wiederhergestellt werden.

## Hypervisoren bearbeiten

Klicken Sie auf einen Hypervisor, um seine Kontoinformationen und Verbindungseinstellungen zu bearbeiten. Für Hyper-V-Hypervisoren, die keine Verbindung zu Sicherungsservern herstellen können, gehen Sie zur Seite **Benutzerdefinierte Verbindungen** und passen Sie die Serveradressen und Ports an.

## Hypervisoren entfernen

1. Gehen Sie zu **Maschinen** > **Virtuelle Maschinen**.
2. Löschen oder archivieren Sie alle VMs, die zu Ihrem Ziel-Hypervisor gehören.
3. Wechseln Sie zu **Infrastruktur** > **Hypervisoren**.
4. Fahren Sie mit der Maus über Ihren Hypervisor und klicken Sie auf ⋮ > **Entfernen**. Beachten Sie, dass dieser Vorgang nicht rückgängig gemacht werden kann.

**Hinweis:**

1. Um SCVMM zu sichern, stellen Sie sicher, dass die Anmeldeinformationen Ihres SCVMM verwendet werden können, um sich bei allen von ihm verwalteten Hypervisoren anzumelden.

# Failover konfigurieren und initiieren

Richten Sie ein Synology ActiveProtect-Gerät als Failover-Server ein, um die Betriebszeit für Ihr Standortmanagement zu maximieren. Wenn Ihr Verwaltungsserver ausgefallen oder offline ist, wechseln Sie manuell zum Failover, um den Betrieb aufrechtzuerhalten.

**Wichtig:**

- Die Sicherungsdaten auf dem Verwaltungsserver **werden nicht** mit dem Failover-Server synchronisiert.

## Bevor Sie beginnen

- **Stellen Sie mindestens zwei ActiveProtect-Geräte bereit:** Konfigurieren Sie eines als Verwaltungsserver und das andere als Failover-Server. Beachten Sie, dass nur ein ActiveProtect-Gerät als Failover-Server eingerichtet werden kann.[1]
- **Überprüfen Sie die Betriebssystemversionen:** Stellen Sie sicher, dass Ihr Failover-Server und Verwaltungsserver dieselbe Version von APM haben.
- **Überprüfen Sie die Modelle:** Um eine stabile Leistung zu gewährleisten, überprüfen Sie, dass das Modell Ihres Failover-Servers mit dem des Verwaltungsservers identisch ist oder dieses übertrifft.
- **Treten Sie einem Verzeichnisdienst bei:** Nur Benutzer, Gruppen und Berechtigungen aus einem Verzeichnisdienst können vom Verwaltungsserver zum Failover-Server synchronisiert werden. Daher sollten Sie Ihren Verwaltungsserver einer Domain oder einem LDAP-Verzeichnis beitreten lassen, bevor Sie den Failover-Server einrichten.
- **Synchronisieren Sie die Zeit zwischen den Servern:** Um eine konsistente Zeit zwischen Ihrem Verwaltungsserver und dem Failover-Server sicherzustellen, folgen Sie diesen Schritten:
  1. Gehen Sie zu Ihrem Verwaltungsserver > Gerätekonsole > **Systemsteuerung** > **Regionale Optionen** > **Uhrzeit**.
  2. Aktivieren Sie die Option **Mit NTP-Server synchronisieren** und geben Sie eine Serveradresse an.
  3. Wiederholen Sie die obigen Schritte auf Ihrem Failover-Server.

## Failover-Server festlegen

1. Melden Sie sich bei Ihrem Verwaltungsserver an.
2. Gehen Sie zu **Infrastruktur** > **Standortverwaltung** und klicken Sie auf **Standorteinstellungen**.
3. Klicken Sie im Abschnitt **Failover-Server einrichten** auf **Einrichten**.
4. Wählen Sie ein ActiveProtect-Gerät aus und speichern Sie die Einstellungen.
5. Ihr Sicherungsgerät ist jetzt ein Failover-Server, der regelmäßig Systemkonfigurationen vom Verwaltungsserver synchronisiert.

Nach der Servereinrichtung können Sie Ihren Failover-Server auf derselben Seite auch ändern oder entfernen.

# Failover initiieren

Die folgenden Schritte hängen davon ab, wie Ihre Sicherungsserver mit dem Verwaltungsserver verbunden sind:

### Wenn Ihre Sicherungsserver über einen FQDN verbunden sind (empfohlen)

1. Gehen Sie zu Ihrem DNS-Server. Weisen Sie die externe Adresse des Verwaltungsservers der IP-Adresse Ihres Failover-Servers zu.
2. Melden Sie sich beim Failover-Server mit einem APM-Administratorkonto an.
3. Klicken Sie im Abschnitt **Failover** auf **Übernehmen**.
4. Der Failover-Server ist jetzt ein Verwaltungsserver, während der ursprüngliche Verwaltungsserver die Rolle des Failover-Servers übernimmt.

### Wenn Ihre Server über eine IP-Adresse verbunden sind

1. Melden Sie sich beim Failover-Server mit einem APM-Administratorkonto an.
2. Klicken Sie im Abschnitt **Failover** auf **Übernehmen**.
3. Melden Sie sich bei jedem Ihrer verwalteten Backup-Server an. Klicken Sie auf das Stiftsymbol neben **Management-Server** und geben Sie die IP-Adresse Ihres Failover-Servers ein.
4. Der Failover-Server ist jetzt ein Management-Server, während der ursprüngliche Management-Server die Rolle des Failover-Servers übernimmt.

# Synchronisierte Konfigurationen

Der Failover-Server synchronisiert die folgenden Informationen vom Management-Server:

- Das FQDN und das Zertifikat des Management-Servers
- Liste der Backup-Server
- Liste der Remote-Speicher
- Speicheranmeldeinformationen
- Planliste
- Workload-Liste
- Listen der Sicherungsversionen
- Domain/LDAP-Informationen
- Berechtigungen für Domain/LDAP-Benutzer
- Anmeldestile
- Benachrichtigungseinstellungen
- Protokolleinstellungen

**Hinweis:**

1. ActiveProtect-Gerät Tower-Serie **kann nicht** als Management- oder Failover-Server eingerichtet werden.

2. Wir empfehlen, den Failover-Server an einem externen oder entfernten Standort zu installieren, um die Auswirkungen von Einzelpunktausfällen wie Festplattenfehlern oder Stromausfällen zu verringern.
3. Ein ActiveProtect-Gerät muss mit dem Management-Server synchronisiert werden, nachdem es als Failover-Server zugewiesen wurde. Vermeiden Sie die Verwaltung der Workloads, bis der Synchronisierungsprozess abgeschlossen ist.
4. Nachdem Ihr Management-Server einem Verzeichnisdienst beigetreten ist, wird der Failover-Server bestimmte Dienste neu starten und die folgenden Aufgaben abbrechen:
    - Sicherung von virtuellen Maschinen und physischen Servern
    - Wiederherstellung und Migration von virtuellen Maschinen
    - Wiederherstellung und Migration von physischen Servern als virtuelle Maschinen
5. Die Zeit, die benötigt wird, um Konfigurationen auf einen Failover-Server zu synchronisieren, hängt von den folgenden Faktoren ab:
    - Lese-/Schreibgeschwindigkeit des Laufwerks
    - Verfügbare CPU- und RAM-Ressourcen
    - Netzwerkübertragungsgeschwindigkeit
    - Größe der Konfigurationsdaten

    Zum Beispiel dauert die Synchronisierung von Standortkonfigurationen für 150.000 Workloads (jeweils mit 30 Sicherungsversionen) auf einen Failover-Server etwa 30 Minuten.

# Sicherheit

Da Cyberangriffe immer häufiger werden und weitreichende Störungen und Datenverluste verursachen, müssen Organisationen ihre Abwehrmaßnahmen gegen diese wachsende Bedrohung verstärken. Im **Sicherheits**-Abschnitt bieten wir einen umfassenden Überblick über bewährte Sicherheitspraktiken und zeigen, wie Sie Ihre ActiveProtect-Geräte und digitalen Vermögenswerte schützen können.

## In diesem Abschnitt

# Halten Sie das Betriebssystem auf dem neuesten Stand

Der wichtigste und direkteste Weg, Ihr ActiveProtect-Gerät zu schützen, besteht darin, sein Betriebssystem, den **ActiveProtect Manager (APM)**, regelmäßig zu aktualisieren. Synologys dediziertes Sicherheitsteam überwacht aktiv Schwachstellen und veröffentlicht Software-Updates, die oft Sicherheitskorrekturen und Leistungsverbesserungen enthalten.

Standardmäßig ist APM so konfiguriert, dass es die neuesten Updates automatisch vom Synology Download-Zentrum abruft. Wenn Sie mehrere ActiveProtect-Geräte haben, empfehlen wir, automatische Updates für Ihre gesamte Site zu planen, um sicherzustellen, dass APM auf allen Ihren Backup-Geräten auf dem neuesten Stand bleibt.

**Hinweis:**

- Um Ports und Domains für automatische Systemupdates zu überprüfen, siehe Sicherer Netzwerkzugang.

# Sicheren Netzwerkzugang

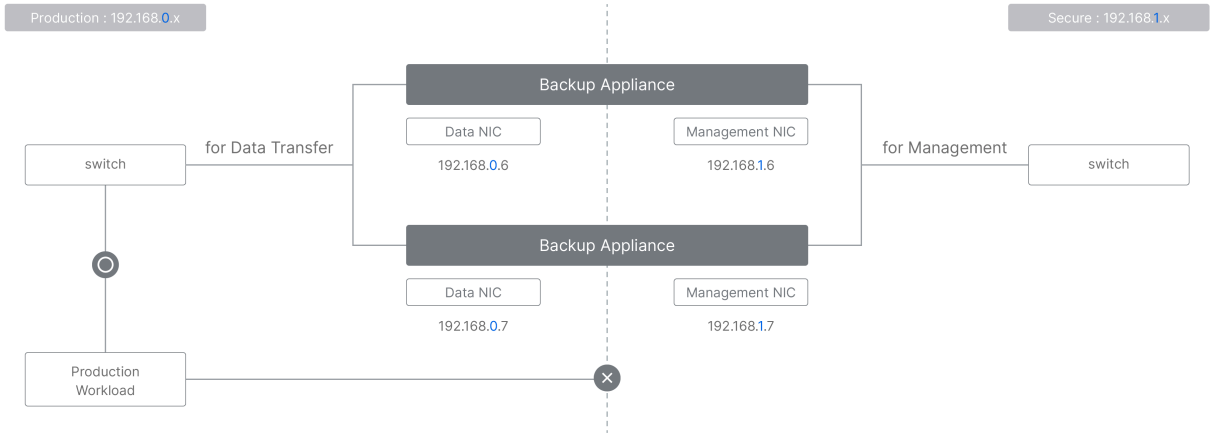
Netzwerkkonfigurationen sind entscheidend für den Schutz Ihres ActiveProtect-Geräts. Dieser Artikel stellt die Netzwerk-Schnittstellen, Ports und Netzwerksicherheitseinstellungen des Geräts vor.

## Getrennte Netzwerksegmente für Verwaltung und Datentransfer

Ein ActiveProtect-Gerät verfügt über zwei Arten von Netzwerkschnittstellen: die **Verwaltungsschnittstelle** für Systemoperationen und die **Datenschnittstelle** für die Übertragung von Sicherungsdaten:

| Netzwerkschnittstelle | Funktionen |
|---|---|
| Verwaltungsschnittstelle | • Dient standardmäßig zur Verwaltung einer ActiveProtect-Site.<br>• Zugriff auf Verwaltungscenter und Gerätekonsole.<br>• Stellt initiale Authentifizierungsverbindungen zu Sites her, wenn Sicherungsserver zu Sites hinzugefügt werden, und synchronisiert Ereignisse zwischen dem Verwaltungsserver und den Sicherungsservern.<br>• Bietet Out-of-Band (OOB) Management. |
| Datenschnittstelle | • Dient zur Datenübertragung während Sicherungen, Sicherungskopien und Wiederherstellungen.<br>• Zugriff auf Wiederherstellungsportal. |

Um diese Netzwerkschnittstellen optimal zu nutzen und gleichzeitig eine sichere Systemverwaltung zu gewährleisten, empfehlen wir, sie mit getrennten Netzwerksegmenten zu verbinden. Setzen Sie die Verwaltungsschnittstelle in ein isoliertes Netzwerk für eine sichere Systemverwaltung ein, während Datenschnittstellen mit der Produktionsumgebung verbunden werden sollten, damit alle Daten ordnungsgemäß gesichert und wiederhergestellt werden können.



**Hinweis:**

- Um die Funktionen der Verwaltungsschnittstelle (außer OOB) auf Ihre Datenschnittstellen anzuwenden, klicken Sie auf **Zugriff auf Gerätekonsole und Verwaltungscenter über Datenports erlauben** bei Gerätekonsole > **Systemsteuerung** > **Netzwerk** > **Konnektivität**. Wir empfehlen jedoch, diese Option deaktiviert zu lassen, um eine sichere Systemverwaltung zu gewährleisten.
- Die Verwaltungsschnittstelle kann auf das Wiederherstellungsportal zugreifen und Sicherungsdaten übertragen, ist jedoch auf die maximale Übertragungsrate von 1 GbE beschränkt. Für eine verbesserte Leistung empfehlen wir die Verwendung von Datenschnittstellen für Sicherungs- und Wiederherstellungsaufgaben.

# Erlauben Sie Ports und Domains, die vom ActiveProtect Manager verwendet werden

Die folgenden Tabellen geben einen Überblick über die erforderlichen Ports und Domains für den ActiveProtect Manager (APM). Standardmäßig erlaubt APM diese automatisch und blockiert diejenigen, die nicht unten aufgeführt sind. Wenn Sie jedoch eine Firewall eines Drittanbieters verwenden, müssen Sie diese manuell konfigurieren, um diese Ports und Domains ordnungsgemäß zuzulassen.

Beachten Sie, dass die in der folgenden Tabelle erwähnten Verwaltungsserver, Sicherungsserver und Sicherungskopierserver **ActiveProtect-Geräte** sind.

## Netzwerkports

| Verwendung | Von | Zu | Port | Protokoll |
|---|---|---|---|---|
| APM Verwaltungscenter UI | Benutzergeräte | ActiveProtect-Geräte | 443 | TCP |
| APM Wiederherstellungsportal UI | Benutzergeräte | ActiveProtect Geräte | 443 | TCP |
| APM Gerätekonsole UI[1] | Benutzergeräte | ActiveProtect Geräte | 5001 | TCP |
| OOB-Modul | Benutzergeräte | ActiveProtect Geräte | 57 | TCP |
| Authentifizieren von Backup-Servern oder ActiveProtect-Agenten[2] | Backup-Server oder ActiveProtect-Agenten | Verwaltungsserver | 443, 8443 | TCP |
| Synchronisieren von Standortereignissen[3] | Backup-Server | Verwaltungsserver | 8443 | TCP |
| Backups über ActiveProtect-Agenten durchführen | ActiveProtect-Agenten | Backup-Server | 443, 8443 | TCP |

| | | | | |
|---|---|---|---|---|
| Wiederherstellungen über das ActiveProtect Wiederherstellungstool durchführen[4] | ActiveProtect Wiederherstellungstool | Backup-Server oder Backup-Kopierserver | 443, 8443 | TCP |
| Daten auf ActiveProtect-Geräte kopieren | Backup-Server | Backup-Kopierserver | 8443 | TCP |
| Sofortige Wiederherstellung zu Hyper-V oder VMware[4] | Hyper-V- oder VMware-Hosts | Backup-Server oder Backup-Kopierserver | 111, 829, 2049 | TCP |
| Hyper-V sichern oder wiederherstellen | Hyper-V-Hosts | ActiveProtect-Geräte | 5510 | TCP |
| | ActiveProtect-Geräte | Hyper-V-Hosts | 445 (SMB), 5986 (HTTPS)[5] | TCP |
| VMware sichern oder wiederherstellen[5] | ActiveProtect-Geräte | vCenter Server | 443 | TCP |
| | | ESXi-Hosts | 443, 902 | TCP |
| Sichern oder Wiederherstellen von Dateiservern[5] | ActiveProtect-Geräte | SMB-Server | 445 | TCP |
| Sichern oder Wiederherstellen von Microsoft 365 | ActiveProtect-Geräte | Microsoft 365 | 443 (API) | TCP |
| Daten in C2 Object Storage kopieren oder daraus wiederherstellen | ActiveProtect-Geräte | C2 Object Storage | 443 | TCP |
| Daten in Amazon S3 kopieren oder daraus wiederherstellen | ActiveProtect-Geräte | Amazon S3 | 443 | TCP |
| Daten in ActiveProtect Vault kopieren oder daraus wiederherstellen | ActiveProtect-Geräte | ActiveProtect Vault | 8444 | TCP |
| Lizenzinformationen synchronisieren | Verwaltungsserver | Synology-Server | 443 | HTTPS |
| Automatische Updates für APM | ActiveProtect-Geräte | Synology Download-Zentrum | 443 | TCP |
| Benachrichtigungs-E-Mails senden[5] | ActiveProtect-Geräte | SMTP-Server | 25 | TCP |

| | | | | |
|---|---|---|---|---|
| Zeit synchronisieren[5] | ActiveProtect-Geräte | NTP-Server | 123 | UDP |
| Protokolle weiterleiten[5] | ActiveProtect-Geräte | Protokollserver | 514 | TCP/UDP |
| SNMP-Kommunikation[5] | ActiveProtect-Geräte | SNMP-Server | 161 | TCP/UDP |
| Support-Center | ActiveProtect-Geräte | Synology-Server | 443 | TCP |
| Automatische Updates für die Laufwerksdatenbank | ActiveProtect-Geräte | Synology-Server | 443 | TCP |

## Domänen

| Verwendung | Domänen |
|---|---|
| Microsoft 365 sichern oder wiederherstellen | • synooauth.synology.com<br>• microsoft.com<br>• microsoftonline.com<br>• office365.com<br>• sharepoint.com<br>• chinacloudapi.cn (nur China)<br>• outlook.cn (nur China) |
| Daten in C2 Object Storage kopieren oder daraus wiederherstellen | • https://s3.synologyc2.net |
| Daten in Amazon S3 kopieren oder daraus wiederherstellen | • https://s3.amazonaws.com<br>• https://s3.cn-north-1.amazonaws.com.cn (nur China) |
| Lizenzinformationen synchronisieren | • apm-license.synology.com |
| Automatische Updates für APM | • global.download.synology.com<br>• global.synologydownload.com<br>• utyautoupdate.synology.com<br>• utyupdate.synology.com<br>• update7.synology.com<br>• autoupdate7.synology.com<br>• autoupdate7.synology.cn (nur China) |
| Zeit synchronisieren | • Die Domäne Ihres NTP-Servers, wie z.B. die Standarddomäne: time.google.com |

| | |
|---|---|
| Support-Center | • account.synology.com<br>• kb.synology.com<br>• www.synology.com/company/legal/Services_Data_Collection Disclosure#technical-support<br>• www.synology.com/company/legal/privacy |
| Automatische Updates für die Laufwerksdatenbank | • diskupdate.synology.com<br>• diskdownload.synology.com<br>• dataupdate7.synology.com<br>• dataautoupdate7.synology.com<br>• dataautoupdate7.synology.cn (nur China) |

**Hinweis:**

1. Der Port für die Gerätekonsole kann angepasst werden.
2. Dieser Port wird für die Authentifizierung verwendet, wenn Backup-Server oder physische Workloads zu einem Standort hinzugefügt werden.
3. Dieser Port wird verwendet, um die Kommunikation zwischen dem Verwaltungsserver und den Backup-Servern sicherzustellen.
4. Das Wiederherstellungstool und die Wiederherstellungs-Hosts sollten sich mit den Backup-Kopierservern verbinden, wenn Backup-Kopien wiederhergestellt werden.
5. Dies sind die Standardports für Drittanbieterdienste. Passen Sie sie an die Einstellungen Ihrer Organisation an.

## DoS-Schutz aktivieren

Denial-of-Service (DoS)-Angriffe überlasten ein Computersystem mit zahlreichen Anfragen, die die Kapazität des Ziels überschreiten. Infolgedessen kann der angegriffene Computer wichtige Daten oder Dienstanfragen (wie E-Mails) von externen Quellen verpassen und unter begrenzter Bandbreite leiden.

Um den DoS-Schutz zu aktivieren, gehen Sie zu jedem Ihrer ActiveProtect-Geräte > Gerätekonsole > **Systemsteuerung** > **Sicherheit** > **Schutz**.

# Zertifikate einrichten

Zertifikate schaffen Vertrauen und Sicherheit, indem sie sicherstellen, dass die Datenübertragung auf Ihrer ActiveProtect-Website ordnungsgemäß verschlüsselt und verifiziert wird. Sie können standardmäßig selbstsignierte Zertifikate verwenden oder Drittanbieterzertifikate importieren, um Ihre Datensicherungsumgebung zu sichern.

## Zertifikat für die Standortverwaltung importieren

Standardmäßig verwendet der ActiveProtect Manager (APM) ein selbstsigniertes Zertifikat, um die folgenden Dienste auf dem Verwaltungsserver zu schützen:

- Verwaltungscenter-Benutzeroberfläche
- Wiederherstellungsportal-Benutzeroberfläche
- Standortauthentifizierung zum Hinzufügen von Sicherungsservern und physischen Workloads

Wenn Sie ein Zertifikat von einer anderen Zertifizierungsstelle verwenden möchten, importieren Sie es über die folgenden Schritte, damit Ihr Verwaltungsserver von anderen Geräten als vertrauenswürdig angesehen wird:

1. Gehen Sie zu Ihrem Verwaltungsserver > **Infrastruktur** > **Standortverwaltung**.
2. Klicken Sie im Abschnitt **Verwaltungscenter** > **Zertifikat** auf das Zahnradsymbol ⚙.
3. Laden Sie die folgenden Zertifikatsdateien hoch:
   - **Privater Schlüssel**: Unterstützt ECC- oder RSA-Schlüssel. Beachten Sie, dass RSA-Schlüssel nicht durch ein Passwort geschützt werden können.
   - **Zertifikat**: Muss im X.509-, PEM- oder DER-Format vorliegen. Stellen Sie sicher, dass der Domainname dieses Zertifikats mit der externen Adresse Ihres Servers (FQDN oder Hostname) übereinstimmt.
   - **Zwischenzertifikat (Optional)**

## Zertifikate für Backup-Appliance-Benutzeroberflächen importieren

Selbstsignierte Zertifikate werden standardmäßig verwendet, um das Verwaltungscenter, das Wiederherstellungsportal und die Gerätekonsole für jedes verwaltete ActiveProtect-Gerät zu schützen. Sie können auch Ihre eigenen Zertifikate importieren, damit Ihre Geräte von anderen Geräten als vertrauenswürdig angesehen werden:

1. Gehen Sie zu Ihrem Verwaltungsserver > **Infrastruktur** > **Backup-Server** und klicken Sie auf einen Backup-Server.
2. Klicken Sie auf der Registerkarte **Konnektivität** auf **Zertifikat verwalten** > **Erstellen**.
3. Laden Sie den privaten Schlüssel, das Zertifikat und das Zwischenzertifikat hoch (siehe Formatanforderungen). Klicken Sie auf **Erstellen**.[1]

4. Wählen Sie Ihr neu erstelltes Zertifikat als Systemstandardzertifikat aus.

## Daten durch ein internes Zertifikat schützen

Sobald Backup-Server und physische Workloads einem ActiveProtect-Standort beitreten, interagieren Benutzer in den meisten Fällen nicht direkt mit ihnen. Alle Kommunikationen zwischen diesen Geräten werden mit dem selbstsignierten Zertifikat von APM verschlüsselt und als vertrauenswürdig angesehen. Daher hat das Ersetzen oder Erneuern des Zertifikats für einen Standort oder ein Gerät keinen Einfluss auf die Ereignissynchronisation, Backups oder andere Datenübertragungen zwischen diesen Geräten.

**Hinweis:**

1. Wenn das ausgewählte Backup-Gerät Ihr **Verwaltungsserver** ist, wird dieses Zertifikat nur auf die Gerätekonsole angewendet. Um das Zertifikat für das Verwaltungscenter und das Wiederherstellungsportal des Verwaltungsservers zu ändern, folgen Sie den Schritten im Abschnitt Zertifikat für die Standortverwaltung importieren.

# Benutzerauthentifizierung verwalten

ActiveProtect Manager (APM) wird über Benutzerkonten verwaltet. Um Ihre Daten sicher zu halten, ist es wichtig sicherzustellen, dass Benutzer starke Authentifizierungsmethoden beim Anmelden verwenden.

## Mit einem Domain/LDAP-Dienst integrieren

Wir empfehlen, Ihre ActiveProtect-Geräte einem Verzeichnisdienst beizutreten für eine vereinfachte Benutzerverwaltung. Mit einem Domain/LDAP-Dienst können IT-Administratoren Benutzerkonten auf einer einzigen Plattform verwalten. Außerdem können Ihre Teammitglieder sicher auf ihre Sicherungsdaten und andere Dienste mit nur einem Satz Anmeldeinformationen zugreifen.

## Single Sign-On einrichten

Um Domain/LDAP-Benutzeranmeldungen zu sichern, empfehlen wir auch die Aktivierung von Single Sign-On (SSO). SSO-Dienstanbieter bieten eine Vielzahl von Anmeldeoptionen, wie z.B. Multi-Faktor-Authentifizierung. Durch die Integration von SSO mit ActiveProtect Manager können Sie diese Sicherheitsfunktionen nutzen, um Benutzeranmeldeinformationen zu schützen und unbefugten Zugriff zu verhindern.

ActiveProtect Manager unterstützt eine breite Palette von SSO-Protokollen, wie OIDC und SAML 2.0. Lesen Sie diesen Artikel, um zu erfahren, wie Sie SSO aktivieren.

## Kennwortrichtlinien durchsetzen

Stellen Sie sicher, dass die Kennwortrichtlinien auf Ihrem Domain/LDAP-Dienst ordnungsgemäß konfiguriert sind. Für lokale Benutzer verwalten Sie diese Richtlinien unter **Benutzerverwaltung** > **Lokale Benutzer** > **Kennwortsicherheit**.

## Ihr Anmeldeportal anpassen

ActiveProtect Manager ermöglicht es Ihnen, Webportale anzupassen, die Benutzer beim Anmelden sehen. Sie können diese Portale personalisieren und wichtige Nachrichten wie rechtliche Hinweise, Warnungen oder Unternehmensrichtlinien anzeigen. Außerdem stärkt das Hinzufügen des Logos Ihrer Organisation Ihre Markenidentität und sorgt für ein einheitliches Erscheinungsbild auf der Plattform.

Um Ihre Anmeldeportale anzupassen, gehen Sie zu **Einstellungen** > **Anmeldestile**.

# Automatische Blockierung konfigurieren

Die Funktion „Automatische Blockierung“ verbessert die Sicherheit Ihres APM, indem die IP-Adressen von Clients mit zu vielen fehlgeschlagenen Anmeldeversuchen blockiert werden. Dies hilft, das Risiko zu verringern, dass Konten durch Brute-Force-Angriffe kompromittiert werden.

**Wichtig:**

- Die folgenden Einstellungen sollten auf **jedem** Ihrer ActiveProtect-Geräte konfiguriert werden.

## Automatische Blockierung aktivieren

1. Gehen Sie zu Gerätekonsole > **Systemsteuerung** > **Sicherheit** > **Schutz**.
2. Wählen Sie **Automatische Blockierung aktivieren**.
3. Konfigurieren Sie die Felder **Anmeldeversuche** und **Innerhalb von (Minuten)**. Eine IP-Adresse wird blockiert, wenn die Anzahl der fehlgeschlagenen Anmeldeversuche innerhalb des angegebenen Zeitraums überschritten wird.
4. Wählen Sie **Blockablauf aktivieren** und konfigurieren Sie das Feld **Blockierung aufheben nach (Tagen)**, um eine blockierte IP-Adresse nach der angegebenen Anzahl von Tagen zu entfernen.
5. Klicken Sie auf **Übernehmen**, um die Einstellungen zu speichern.

## Freigabe-/Blockierungsliste erstellen

1. Gehen Sie zu Gerätekonsole > **Systemsteuerung** > **Sicherheit** > **Schutz**.
2. Klicken Sie auf **Freigabe-/Blockierungsliste** und gehen Sie zur **Freigabeliste** oder **Blockierungsliste**.[1]
3. Wählen Sie eine der folgenden Optionen aus dem Dropdown-Menü **Erstellen**:
   - **IP-Adresse hinzufügen**
   - **IP-Adressliste importieren**: Importieren Sie eine .txt-Datei, die mehrere IP-Adressen enthält.[2] Aktivieren Sie das Kontrollkästchen, wenn Sie bestehende IP-Adressen überschreiben möchten. Wenn diese Option nicht ausgewählt ist, werden doppelte IP-Adressen übersprungen.

**Hinweis:**

1. Wenn sich Ihre ActiveProtect-Geräte hinter einem Reverse-Proxy-Server befinden, stellen Sie sicher, dass dieser zur Freigabeliste hinzugefügt wird.
2. Die importierte Datei muss die folgenden Kriterien erfüllen:
   - Die Datei muss eine reine Textdatei sein.
   - Jede Zeile der Datei darf nur entweder eine IP-Adresse, einen IP-Bereich (wie 192.168.1.1~192.168.1.10), ein Subnetz (wie 192.168.1.1/255.255.0.0 oder 192.168.1.1/16), oder einen Domainnamen enthalten.
   - Reine Textnotizen sollten mit einem Hashtag (#) beginnen.

# Benutzerberechtigungen verwalten

ActiveProtect Manager (APM) bietet granulare Zugriffskontrolle, die es Ihnen ermöglicht, Berechtigungen für jeden Benutzer und jede Gruppe anzupassen. Beim Gruppieren von Benutzern und Zuweisen von Berechtigungen sollten Sie besonders auf die Verwendung der folgenden Arten von lokalen Benutzern und Gruppen achten.

Für Schritt-für-Schritt-Anleitungen zur Benutzerautorisierung siehe Verwaltungsberechtigungen delegieren.

## Superadministrator

Das Superadmin[1]-Konto wird während der Erstinstallation von APM erstellt. Nur dieses Konto hat vollen Zugriff auf das gesamte Betriebssystem, einschließlich Verwaltungscenter, Wiederherstellungsportal, Gerätekonsole und Out-of-Band-Management (OOB).[2] Stellen Sie sicher, dass Sie einen starken Benutzernamen und ein starkes Passwort für dieses Konto festlegen.

Wenn Sie den Zugriff des Super-Admins auf das Verwaltungscenter und die OOB-Verwaltung widerrufen möchten, wenden Sie sich an den technischen Support von Synology zur Unterstützung.

## "APM default admin"-Gruppe

Lokale Benutzer in dieser Gruppe haben vollen Zugriff auf das Verwaltungscenter und das Wiederherstellungsportal. Um das Risiko von Datenverlusten durch menschliches Versagen zu verringern, stellen Sie sicher, dass nur vertrauenswürdige Benutzerkonten zu dieser Gruppe hinzugefügt werden.

## "Users"-Gruppe

Die **Users**-Gruppe umfasst alle lokalen Benutzer, daher verwalten Sie deren Berechtigungen bitte sorgfältig. Standardmäßig darf diese Gruppe nur das Wiederherstellungsportal anzeigen und hat keinen Zugriff auf Sicherungsdaten.

### Hinweis:

1. Das Superadmin-Konto kann nicht gelöscht werden.
2. Andere delegierte Administratorkonten können nur auf das Verwaltungscenter und das Wiederherstellungsportal zugreifen.

# Effektive Sicherungsstrategien implementieren

Dieser Artikel bietet Ihnen unsere empfohlenen Strategien, um Ihre wichtigen Daten mit ActiveProtect-Geräten zu schützen.

## Bewerten Sie die Wichtigkeit aller Systeme und Daten

Priorisieren Sie Ihre digitalen Vermögenswerte basierend auf ihrer Wichtigkeit für Ihre Organisation. Um eine effektive Sicherungsstrategie zu etablieren, bewerten Sie jedes System und jede Daten anhand dieser Metriken:

- **Recovery Time Objective (RTO)**: Bestimmt die akzeptable Ausfallzeit für die Datenwiederherstellung nach einer Unterbrechung. Ein kürzeres RTO erfordert schnellere Wiederherstellungsmethoden.
- **Recovery Point Objective (RPO)**: Definiert den maximalen Datenverlust, der ohne signifikante geschäftliche Auswirkungen toleriert werden kann. Ein niedrigeres RPO erfordert häufigere Sicherungen. Im ActiveProtect Manager können Sie die Sicherungshäufigkeit in einem Schutzplan anpassen, um Ihre RPO-Anforderungen zu erfüllen.

## Die 3-2-1-Sicherungsstrategie implementieren

Schützen Sie Ihre Daten mit der 3-2-1-Sicherungsstrategie. Diese Methode gewährleistet Datenredundanz und externe Speicherung, wodurch Ransomware-Risiken gemindert werden. Um Sicherungskopien Ihrer Daten zu aktivieren, lesen Sie diesen Artikel.

## Neue Workloads automatisch schützen

Richten Sie automatisierte Sicherungsregeln ein, um die virtuellen Maschinen und SaaS-Konten Ihrer Organisation zu schützen. Diese Funktion stellt sicher, dass alle neuen Ressourcen, die Ihrer Produktionsumgebung hinzugefügt werden, automatisch gesichert werden, wodurch Sicherheitslücken im Zusammenhang mit digitaler Expansion minimiert werden.

Um automatische Sicherungsregeln für virtuelle Maschinen und Microsoft 365 zu erstellen, lesen Sie die folgenden Artikel:

- Virtuelle Maschinen über eine automatische Sicherungsregel hinzufügen
- Microsoft 365 über eine automatische Sicherungsregel hinzufügen

# Unveränderliche Sicherungen konfigurieren

Unveränderliche Sicherungen schützen Ihre Daten, indem sie nach dem Schreiben unveränderlich und unlöschbar gemacht werden. Dies gewährleistet die Datenintegrität und hilft, regulatorische Anforderungen zu erfüllen. ActiveProtect-Geräte verwenden einen mehrgleisigen Ansatz, um Ihre Sicherungsdaten vor Ransomware zu schützen:

- **Natives Betriebssystem**: Der in jedem ActiveProtect-Gerät eingebettete ActiveProtect Manager (APM) ermöglicht es Ihnen, Daten vor unbefugten oder versehentlichen Änderungen zu schützen.
- **Schutz mit Object Lock und WORM**: Beim Sichern von Daten auf entfernten Speichern (wie Amazon S3) nutzen ActiveProtect-Geräte die Object Lock- oder WORM-Funktionen (write once, read many) des Speichers, um die Datenintegrität zu gewährleisten und Kompromittierungen auf entfernten Speichern zu verhindern.
- **Automatisierte Aufbewahrungssperren**: ActiveProtect-Geräte passen die unveränderlichen oder WORM-Sperrzeiten automatisch gemäß Ihren Datenaufbewahrungsrichtlinien an. Dieser Ansatz optimiert Ihre Speichernutzung und vereinfacht die Konfigurationen.

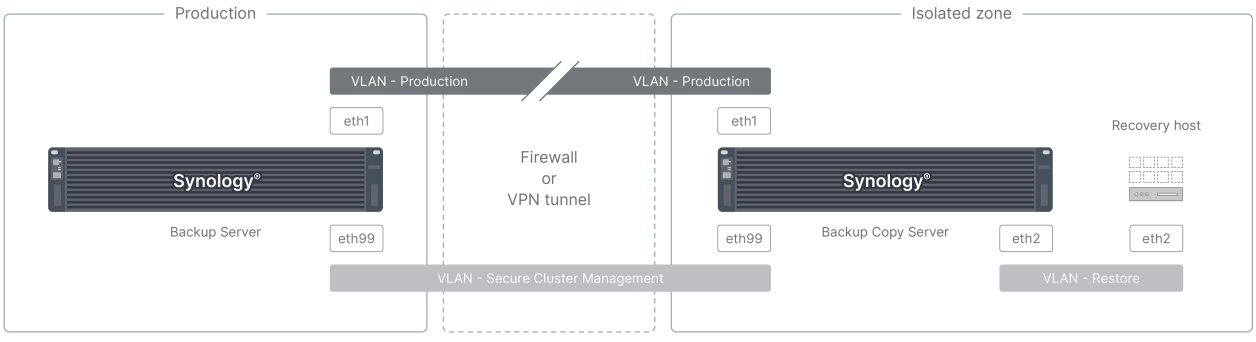
Erstellen Sie einen unveränderlichen Schutzplan, um unveränderliche Sicherungen zu erreichen. Siehe Verwalten Sie Ihre Schutzpläne.

# Ein luftdichtes Umfeld implementieren

Um die Abwehr gegen Ransomware zu stärken, empfehlen wir die Einrichtung eines luftdichten Umfelds für Ihre ActiveProtect-Site. Im Gegensatz zu traditionellen Luftlücken, die auf Bänder für null Konnektivität setzen, ermöglicht Ihnen der ActiveProtect Manager die Planung der Isolation von sekundären Sicherungsservern (d.h. Sicherungskopierservern).[1] Dies beschränkt die Netzwerkverbindung auf wesentliche Datenübertragungszeiten, während sichergestellt wird, dass Ihre Sicherungsdaten von IT-Administratoren leicht zugänglich und verwaltbar sind.

Verwenden Sie die folgenden Methoden, um ein luftdichtes Umfeld einzurichten und gleichzeitig ein effizientes Site-Management aufrechtzuerhalten.

## Eine isolierte Zone einrichten




Stellen Sie Ihren Sicherungskopierserver in einer Zone bereit, die physisch und logisch von der Produktionsumgebung isoliert ist. Diese Zone sollte nur minimale Konnektivität zu anderen Umgebungen haben, mit **nur** den folgenden zwei Ethernet-Verbindungen:

| Verbindung | Beschreibung |
| --- | --- |
| Datenübertragung | • Diese Verbindung überträgt Sicherungsdaten über **Dateninterfaces** zwischen:<br>  ◦ Sicherungsservern in Ihrer Produktionsumgebung<br>  ◦ Dem Sicherungskopierserver in der isolierten Zone<br>• Wenden Sie eine der folgenden Luftlücken-Methoden auf Ihren Sicherungskopierserver in der isolierten Zone an. Die Verbindung der Datenübertragungsleitung ist nur während der Nicht-Isolationszeiten verfügbar:<br>  ◦ Eingehenden Datenverkehr über Firewall-Regeln verweigern<br>  ◦ Ethernet-Interfaces deaktivieren<br>• Der Server in der isolierten Zone steuert die Luftlückenfunktionen.<br>• Für optimale Leistung verwenden Sie Hochgeschwindigkeits-Ethernet zwischen den Servern, um Sicherungskopien zu übertragen, vorzugsweise 10 GbE. |
| Standortverwaltung | • Dieser Link synchronisiert Standortereignisse über **Verwaltungsschnittstellen** zwischen:<br>  ◦ Dem Verwaltungsserver in Ihrer Produktionsumgebung<br>  ◦ Dem Backup-Kopierserver in der isolierten Zone<br>• Um die Sicherheit Ihrer Standortverwaltung zu stärken, stellen Sie sicher, dass dieser Link in ein isoliertes Netzwerksegment bereitgestellt wird. Erfahren Sie mehr |

### Netzwerke über Firewall oder VPN sichern

Um die Verbindungen zur isolierten Zone weiter abzusichern, empfehlen wir, eine Firewall oder einen VPN-Tunnel auf die oben genannten Netzwerkverbindungen anzuwenden. Außerdem sollten Sie nur die erforderlichen Ports und Protokolle für externe Verbindungen zulassen und unnötigen Zugriff blockieren.

### Einen Wiederherstellungs-Host in der isolierten Zone einrichten

Die Bereitstellung eines Wiederherstellungs-Hosts in der isolierten Zone ermöglicht es Ihnen, regelmäßig sofortige Wiederherstellungen durchzuführen, um sicherzustellen, dass Ihre Backup-Daten bei Bedarf korrekt wiederhergestellt werden können.

## Regelmäßige Wiederherstellungsübungen

Planen Sie Wiederherstellungsübungen, um die Effektivität Ihrer Backup- und Wiederherstellungsprozesse zu bewerten. ActiveProtect-Geräte bieten flexible Wiederherstellungsfunktionen, die Ihnen helfen, diese Übungen durchzuführen, und sicherstellen, dass Ihr IT-Team gut vorbereitet ist, um auf kritische Situationen zu reagieren.

## Sicherungen überprüfen

Um die Startfähigkeit gesicherter Workloads zu überprüfen, können Sie die Sicherungsüberprüfung aktivieren, sodass Ihr ActiveProtect-Gerät ein Video während einer Testwiederherstellung für physische Server und virtuelle Maschinen aufzeichnet.

## Daten sofort auf Hypervisoren wiederherstellen

Die sofortige Wiederherstellung ist ideal für die Durchführung von Wiederherstellungsübungen. Sie ermöglicht es Ihnen, Ihre physischen Server und virtuellen Maschinen innerhalb von Minuten mit komprimierten und deduplizierten Sicherungsdateien wiederherzustellen. Im ActiveProtect Manager können Sie Sicherungsabbilder sofort auf den integrierten Hypervisor oder Ihre eigenen wiederherstellen. Weitere Informationen zu den Konfigurationen der sofortigen Wiederherstellung finden Sie in den folgenden Artikeln:

- Physische Server auf virtuelle Maschinen wiederherstellen
- Virtuelle Maschinen wiederherstellen

## SaaS-Daten auf Testkonten wiederherstellen

Führen Sie Wiederherstellungsübungen für Ihre SaaS-Dienste mit Testbenutzerkonten durch. Erstellen Sie beispielsweise mehrere Konten auf Microsoft 365 und stellen Sie sicher, dass sie keine Daten oder Anpassungen enthalten. Stellen Sie dann Ihre Sicherungsversionen auf diesen Testkonten wieder her, um die Datenwiederherstellung zu überprüfen.

### Hinweis:

1. Primäre Backup-Server sollten nicht mit Air Gaps konfiguriert werden, da diese Server eine ständige Kommunikation mit geschützten Maschinen und Diensten erfordern. Ihre Exposition gegenüber der Produktionsumgebung macht sie anfälliger für Cyberangriffe, und Air Gaps können Backup-Aktivitäten behindern.

# Datensicherung & Sicherungskopie

Regelmäßige Datensicherung ist entscheidend, um sich vor unerwarteten Katastrophen und potenziellen Ausfällen zu schützen. Das Vertrauen auf eine einzige Sicherung bietet jedoch möglicherweise nicht ausreichende Sicherheit. Wenn die primäre Sicherung zusammen mit den Produktionsdaten beschädigt oder verloren geht, könnte das Fehlen von Datenwiederherstellungsquellen zu schwerwiegenden Konsequenzen führen.

Um Datensicherheit und Wiederherstellungsbereitschaft zu gewährleisten, folgt ActiveProtect der **3-2-1-1-Strategie der Datensicherung**:

- Schutz von 3 Kopien der Daten: Originaldaten, Sicherungen und Sicherungskopien.
- Speicherung der Daten auf 2 verschiedenen Medien.
- Aufrechterhaltung von 1 externen Kopie, geografisch getrennt für die Notfallwiederherstellung.
- Beibehaltung von 1 unveränderlichen Kopie, die gegen Ransomware-Angriffe unempfindlich ist.

Dieser Abschnitt führt Sie durch die wesentlichen Schritte zur Sicherung verschiedener Arten von Workloads, einschließlich der Installation von Agenten, der Einrichtung von Plänen und der Verwaltung von Workloads für einen reibungslosen und effizienten Sicherungsprozess.

## In diesem Abschnitt

# Schutz-Spickzettel

Dieser Artikel beschreibt alle verfügbaren Schutzparameter für Ihre wertvollen Workloads.

## Sicherungsbereiche & Zeitpläne

<table>
<tr><th colspan="2">Workloads</th><th>Anpassbare Sicherungsbereiche</th><th>Zeitpläne (Sicherungsschemata)</th></tr>
<tr><td rowspan="2">Persönliche Computer</td><td>Windows</td><td rowspan="2"><ul><li>Gesamte Maschinen</li><li>System-Volumes</li><li>Benutzerdefinierte Volumes</li></ul></td><td rowspan="2"><ul><li>Manuelle Sicherung</li><li>Geplante Sicherung</li><li>Ereignisgesteuerte Sicherung</li></ul></td></tr>
<tr><td>macOS</td></tr>
<tr><td rowspan="2">Physische Server</td><td>Windows</td><td rowspan="2"><ul><li>Gesamte Maschinen (inkl. Datenbanken)</li><li>System-Volumes</li><li>Benutzerdefinierte Volumes</li></ul></td><td rowspan="9"><ul><li>Manuelle Sicherung</li><li>Geplante Sicherung</li></ul></td></tr>
<tr><td>Linux</td></tr>
<tr><td rowspan="2">Virtuelle Maschinen</td><td>VMware vSphere</td><td rowspan="2"><ul><li>Gesamte Maschinen (inkl. Datenbanken)</li></ul></td></tr>
<tr><td>Microsoft Hyper-V</td></tr>
<tr><td rowspan="4">Dateiserver</td><td>SMB-Server</td><td rowspan="4"><ul><li>Ausgewählte Ordner</li></ul></td></tr>
<tr><td>NetApp-Server</td></tr>
<tr><td>Nutanix-Server</td></tr>
<tr><td>Synology NAS</td></tr>
<tr><td rowspan="6">Microsoft 365</td><td>Exchange</td><td><ul><li>E-Mails, Kontakte und Kalender</li><li>Archivpostfächer</li></ul></td></tr>
<tr><td>OneDrive</td><td rowspan="5">N/V</td></tr>
<tr><td>Chat</td></tr>
<tr><td>Microsoft 365 Gruppe</td></tr>
<tr><td>SharePoint</td></tr>
<tr><td>Teams</td></tr>
</table>

# Aufbewahrung von Sicherungsversionen

Eine Aufbewahrungsrichtlinie bestimmt, wie lange Daten aufbewahrt werden und welche Daten behalten werden. ActiveProtect bietet die folgenden Optionen zur Verwaltung Ihrer Sicherungsversionen:

- Alle Versionen behalten
- Versionen für eine bestimmte Anzahl von Tagen behalten
- Eine bestimmte Anzahl der neuesten Versionen behalten
- Erweiterte Aufbewahrungsregeln anwenden (z.B. langfristige Aufbewahrungsrichtlinie oder GFS)

# Sicherungskopie

Sicherungskopien fügen eine zusätzliche Schutzschicht hinzu, indem sie Sicherungsversionen an einen sekundären Standort replizieren.

## Kopierzeitplan

- Erstellen Sie eine Sicherungskopie direkt nach jeder Sicherungsversion: Gewährleistet nahtlosen Datenschutz.
- Erstellen Sie Sicherungskopien zu geplanten Zeiten: Optimiert die Ressourcennutzung, indem Kopieraufträge außerhalb der Hauptgeschäftszeiten ausgeführt werden.

## Kopieraufbewahrung

- Alle Sicherungskopien behalten
- Sicherungskopien für eine bestimmte Anzahl von Tagen behalten
- Eine bestimmte Anzahl der neuesten Sicherungskopien behalten
- Erweiterte Aufbewahrungsregeln anwenden (z.B. langfristige Aufbewahrungsrichtlinie oder GFS)
- Keine Sicherungskopien behalten: Nur verfügbar, wenn die Sicherungskopie deaktiviert ist, sodass Sie alle vorhandenen Kopien löschen können.

## Einrichtungsrichtlinien

Für detaillierte Anweisungen lesen Sie die folgenden Artikel:

- Wie man eine Sicherungskopie einrichtet
- Wie man den Sicherungskopieserver bereitstellt

# Pläne zum Schutz verwalten

Ein Plan zum Schutz ist eine umfassende Datensicherungsrichtlinie, die der 3-2-1-1-Strategie der Datensicherung folgt. Diese Pläne sind auf Ihre spezifischen Anforderungen an den Datenschutz zugeschnitten und bieten einen klaren Rahmen, der Folgendes umreißt:

- Datensicherungspläne, die mit Ihren betrieblichen Arbeitsabläufen abgestimmt sind
- Umfang der zu sichernden Daten, wobei kritische Vermögenswerte priorisiert werden
- Aufbewahrungsfristen zur Erfüllung von Compliance- und Wiederherstellungsanforderungen

Durch die Einbeziehung von primären Sicherungen und Sicherungskopien vereinfacht ein Plan zum Schutz Ihr gesamtes Datensicherungsmanagement, sichert Ihre kritischen Daten gegen mehrere Bedrohungen und gewährleistet die Geschäftskontinuität.

## In diesem Abschnitt

# Schutzpläne für physische und virtuelle Maschinen

Sichern Sie Ihre PCs, Macs, physischen Server, virtuellen Maschinen, Datenbanken und Dateiserver einfach, indem Sie Schutzpläne erstellen. Dieser Artikel behandelt wichtige Aspekte wie das Verwalten von Sicherungsplänen, das Anpassen von Sicherungsbereichen und das Festlegen von Aufbewahrungsregeln, um den umfassenden und ununterbrochenen Schutz Ihrer Daten zu gewährleisten.

## Pläne einrichten

1. Gehen Sie zu **Pläne** > **Schutzpläne** im linken Bereich.
2. Klicken Sie auf **Plan erstellen** > **Physische & virtuelle Maschinen**.
3. Wählen Sie einen Plantyp aus. Unveränderliche Schutzpläne verhindern Änderungen oder Löschungen Ihrer Daten innerhalb des festgelegten Aufbewahrungszeitraums und gewährleisten die Datenintegrität.
4. Geben Sie einen Plannamen und eine Beschreibung ein. Wählen Sie eine Zeitzone für die Ausführung von Sicherungen und Sicherungskopien.
5. Konfigurieren Sie die folgenden Einstellungen:
    - Legen Sie die Aufbewahrungsregel fest:
        - Für unveränderliche Schutzpläne: Geben Sie einen Zeitraum an, um Sicherungsversionen zu behalten. Beachten Sie, dass die Verkürzung des Aufbewahrungszeitraums nur Versionen betrifft, die nach der Änderung gesichert wurden.
        - Für Schutzpläne: Wählen Sie, ob alle Sicherungsversionen gespeichert werden sollen, Versionen innerhalb eines bestimmten Zeitraums behalten, die Anzahl der gespeicherten Versionen begrenzen oder bestimmte Versionen gemäß den erweiterten Aufbewahrungsregeln behalten.
    - Konfigurieren Sie Sicherungspläne[1] und Bereiche:
        - Legen Sie einen Standardsicherungsplan für alle eingeschlossenen Maschinen fest und definieren Sie die erlaubte Sicherungszeit.
        - Geben Sie die Sicherungspläne und Bereiche für jeden Maschinentyp an. Benutzerdefinierte Einstellungen überschreiben Standardeinstellungen, wenn Konflikte auftreten.
6. Konfigurieren Sie anwendungsbewusste Sicherung für physische Server und virtuelle Maschinen. Dies stellt sicher, dass die Sicherungsdaten mit der Quelle übereinstimmen und ist unerlässlich für die Sicherung von SQL- und Oracle-Datenbanken.
7. Passen Sie erweiterte Einstellungen an, um die Sicherungsverifizierung zu aktivieren oder die Energieeinstellungen für gesicherte Maschinen anzupassen.
8. Aktivieren Sie Sicherungskopien, um jede Sicherungsversion automatisch an einem anderen Ort zu duplizieren.
9. Bestätigen Sie die Planübersicht.

# Sicherungspläne und Bereiche anpassen

Jeder Maschinentyp hat eine vordefinierte Kombination aus Zeitplan und Bereich. Sie können diese nach Bedarf hinzufügen oder bearbeiten.[2]

## Für PCs/Macs

### Sicherungsbereiche

- **Gesamte Maschine**: Sichern Sie vollständige PCs oder Macs, einschließlich Einstellungen, Anwendungen und Dateien.
- **System-Volume**:
  - Windows: Sichern Sie Partitionen mit Systemdaten, wie Boot-Partition, Systempartition, Wiederherstellungspartition, WinRE Tools (GPT) und für das System reservierte (MBR) Partition.
  - macOS: Sichern Sie System-Volumes, Macintosh HD und Macintosh HD - Data.
- **Benutzerdefiniertes Volume**: Geben Sie Volumennamen ein und trennen Sie diese mit einem Komma und Leerzeichen (z.B., Volume_1, Volume_2).[3] [4]

### Sicherungspläne

- **Dem Standardzeitplan folgen**
- **Manuelle Sicherung**: Sicherungen manuell initiieren.
- **Geplante Sicherung**: Legen Sie fest, dass Sicherungen stündlich, täglich oder wöchentlich ausgeführt werden.
- **Ereignisgesteuerte Sicherung**: Verwenden Sie bestimmte Ereignisse wie Abmeldung, Bildschirmsperre oder Systemstart, um Sicherungen auszulösen. Sie können ein Mindestintervall zwischen den Sicherungen festlegen.

## Für physische Server

### Sicherungsscope

- **Gesamte Maschine**: Sichern Sie vollständige Server, einschließlich Einstellungen, Anwendungen und Dateien.
- **System-Volume**:
  - Windows: Sichern Sie Partitionen mit Systemdaten, wie Boot-Partition, Systempartition, Wiederherstellungspartition, WinRE Tools (GPT) und für das System reservierte (MBR) Partition.
  - Linux: Sichern Sie Partitionen mit Systemdaten, wie "/my/mount/point" oder Swap-Partitionen.
- **Benutzerdefiniertes Volume**: Geben Sie Volumennamen ein und trennen Sie diese mit einem Komma und einem Leerzeichen (z.B. Volume_1, Volume_2).[3]

### Sicherungszeitpläne

- **Dem Standardzeitplan folgen**
- **Manuelle Sicherung**: Starten Sie Sicherungen manuell.

- **Automatische Sicherung**: Planen Sie Sicherungen, die stündlich, täglich oder wöchentlich ausgeführt werden.

## Für Dateiserver und virtuelle Maschinen

### Sicherungszeitpläne

- Dem Standardzeitplan folgen
- **Manuelle Sicherung**: Starten Sie Sicherungen manuell.
- **Automatische Sicherung**: Planen Sie Sicherungen, die stündlich, täglich oder wöchentlich ausgeführt werden.

### Hinweis:

1. Wenn eine manuelle oder geplante Sicherung während eines nicht erlaubten Sicherungszeitraums startet:
    - PCs, Macs und Windows-Server: Die Sicherung wird pausiert und zum nächsten erlaubten Sicherungszeitpunkt fortgesetzt.
    - Linux-Server, virtuelle Maschinen und Dateiserver: Die Sicherung wird abgebrochen.
2. Nur PCs, Macs und physische Server unterstützen mehrere Zeitpläne mit unterschiedlichen Sicherungsscope. Alle in demselben Plan für einen bestimmten Maschinentyp festgelegten Sicherungsscope gelten für die enthaltenen Workloads dieses Typs.
3. Wenn die angegebenen Volumes auf einem Workload nicht vorhanden sind, kann die Sicherung nicht durchgeführt werden, und der Status kann als **Fehlgeschlagen** angezeigt werden.
4. Für das Mac-System-Volume geben Sie $System_Volume ein, um es in Ihre Sicherung einzuschließen.
5. Bevor Sie einen Schutzplan löschen, der bereits auf Workloads, automatische Sicherungsregeln oder Verbindungsschlüssel (PCs/Physische Server) angewendet wurde, müssen Sie einen Ersatzplan für diese betroffenen Elemente auswählen.

# Schutzpläne für Microsoft 365

Sichern Sie Ihre Microsoft 365-Daten, einschließlich Exchange, OneDrive, Chat, Microsoft 365-Gruppe, SharePoint und Teams, ganz einfach, indem Sie Schutzpläne erstellen. Dieser Artikel behandelt wichtige Aspekte wie die Verwaltung von Sicherungsplänen, die Anpassung von Sicherungsumfängen und das Festlegen von Aufbewahrungsregeln, um den umfassenden und ununterbrochenen Schutz Ihrer Daten zu gewährleisten.

## Richten Sie Ihre Pläne ein

1. Gehen Sie zu **Pläne** > **Schutzpläne** im linken Bereich.
2. Klicken Sie auf **Plan erstellen** > **Microsoft 365**.
3. Wählen Sie einen Plantyp aus. Unveränderliche Schutzpläne verhindern Änderungen oder Löschungen Ihrer Daten innerhalb des festgelegten Aufbewahrungszeitraums und gewährleisten die Datenintegrität.
4. Geben Sie einen Plannamen und eine Beschreibung ein. Wählen Sie eine Zeitzone für die Durchführung von Sicherungen und Sicherungskopien.
5. Geben Sie den Sicherungsumfang für Exchange-Benutzer an. Für andere Microsoft 365-Dienste werden die zugehörigen Daten automatisch gesichert, wenn Sie deren Objekte (wie OneDrive-Konten oder SharePoint-Sites) zu Ihrer ActiveProtect-Site hinzufügen. Diese Dienste können nicht individuell konfiguriert werden.
6. Konfigurieren Sie die folgenden Einstellungen:
   - Festlegen der Aufbewahrungsregel:
     - Für unveränderliche Schutzpläne: Geben Sie einen Zeitraum an, um Sicherungsversionen zu behalten. Beachten Sie, dass die Verkürzung des Aufbewahrungszeitraums nur Versionen betrifft, die nach der Änderung gesichert wurden.
     - Für Schutzpläne: Wählen Sie, ob alle Sicherungsversionen gespeichert werden sollen, Versionen innerhalb eines bestimmten Zeitraums behalten werden sollen, die Anzahl der gespeicherten Versionen begrenzt werden soll oder bestimmte Versionen gemäß den erweiterten Aufbewahrungsregeln behalten werden sollen.
   - Bestimmen Sie den Sicherungszeitplan:
     - **Manuelle Sicherung**: Sicherungen manuell initiieren.
     - **Geplante Sicherung**: Sicherungen stündlich, täglich oder wöchentlich ausführen lassen.
7. Sicherungskopien aktivieren, um jede Sicherungsversion automatisch an einem anderen Ort zu duplizieren.
8. Bestätigen Sie die Planübersicht.

**Hinweis:**

- Bevor Sie einen Schutzplan löschen, der bereits auf Workloads oder automatische Sicherungsregeln angewendet wurde, müssen Sie einen Ersatzplan für diese betroffenen Elemente auswählen.

# Sicherungskopie

Sicherungskopien bieten eine zusätzliche Schutzebene, indem sie Ihre Sicherungsversionen automatisch an einem anderen Ort duplizieren. Dies schützt Ihre Daten, falls die ursprünglichen oder primären Sicherungen verloren gehen oder beschädigt werden.

## Wie Sicherungskopie funktioniert

ActiveProtect stellt sicher, dass Ihre Sicherungsversionen erfolgreich an den vorgesehenen Ort kopiert werden, indem:

- **Automatisches Wiederholen**: Bei Problemen wie Internetunterbrechungen oder Stromausfällen wird das System alle 24 Stunden automatisch versuchen, die Kopie erneut durchzuführen.
- **Anpassung an Änderungen**:
  - **Aktivierung der Sicherungskopie**: Wenn Sie die Sicherungskopie zum ersten Mal aktivieren, kopiert das System frühere Versionen basierend auf Ihren Aufbewahrungsregeln. Zum Beispiel, wenn Ihre Aufbewahrungsfrist auf 365 Tage eingestellt ist, kopiert das System Versionen der letzten 365 Tage.
  - **Änderung der Schutzpläne**: Beim Wechsel der Schutzpläne überprüft das System, welche früheren Versionen gemäß den Aufbewahrungsregeln des neuen Plans kopiert werden müssen. Zum Beispiel, wenn Plan A Versionen für 30 Tage und Plan B für 60 Tage aufbewahrt, kopiert das System beim Wechsel von Plan A zu Plan B die Versionen der zusätzlichen 30 Tage, die Plan B abdeckt. Versionen, die bereits von Plan A abgedeckt sind, werden nicht erneut kopiert.

Diese Ansätze gewährleisten eine gründliche Sicherungskopie und minimieren Ausfälle. Wenn ein Kopierfehler auftritt, liegt dies typischerweise an einer verlorenen Verbindung zwischen dem Sicherungsserver und dem Kopierziel.

## Zugriff auf Sicherungskopie-Einstellungen

Die Einstellungen für Sicherungskopien befinden sich in jedem Schutzplan:

1. Gehen Sie zu **Pläne** > **Schutzpläne** im linken Bereich.
2. Klicken Sie auf den Zielplan und navigieren Sie zur Registerkarte **Sicherungskopie**.

## Aufbewahrungsregel konfigurieren

Legen Sie Regeln für das Behalten oder Löschen von Sicherungskopien fest.[1] Für ein besseres Verständnis, wie Aufbewahrungsregeln bestimmen, welche Versionen behalten werden, lesen Sie den Abschnitt Aufbewahrung.

### Für Schutzpläne

- Alle Sicherungskopien speichern

- Sicherungskopien für einen bestimmten Zeitraum behalten
- Die Anzahl der gespeicherten Sicherungskopien begrenzen
- Bestimmte Sicherungskopien basierend auf den erweiterten Aufbewahrungsregeln behalten
- Keine Versionen behalten: Nur verfügbar, wenn die Sicherungskopie deaktiviert ist, was das Löschen aller vorhandenen Sicherungskopien ermöglicht.

### Für unveränderliche Schutzpläne

- Sicherungskopien für einen bestimmten Zeitraum behalten: Während der anfänglichen Aufbewahrungsfrist können Daten nicht verändert oder gelöscht werden. Wenn Sie die Aufbewahrungsfrist verkürzen, betrifft dies nur Versionen, die nach der Anpassung erstellt wurden.

## Kopierziel und Zeitplan festlegen

Wählen Sie **Sicherungskopie aktivieren** und geben Sie die folgenden Einstellungen an:

- **Ziel**: Wählen Sie einen entfernten Speicher oder ein ActiveProtect-Gerät, das sich vom Sicherungsziel unterscheidet.[2] [3]
- **Zeitplan**:
  - **Erstellen Sie eine Sicherungskopie direkt nach jeder Sicherungsversion**: Gewährleistet nahtloses Kopieren der Sicherung.
  - **Erstellen Sie Sicherungskopien zu einem geplanten Zeitpunkt (täglich)**: Ermöglicht eine effiziente Ressourcennutzung, indem der Kopierauftrag außerhalb der Stoßzeiten geplant wird.

**Hinweis:**

1. Bestehende Sicherungskopien werden weiterhin der angegebenen Aufbewahrungsregel folgen, selbst nachdem der Sicherungskopierauftrag deaktiviert wurde.
2. Wenn Sie das Ziel der Sicherungskopie ändern, werden ausstehende Versionen an das neue Ziel kopiert, während bestehende Versionen am ursprünglichen Ort verbleiben.
3. Workloads, die auf Synology NAS gesichert sind, unterstützen keine Sicherungskopien auf entfernten Speicher.

# Erweiterte Aufbewahrungsregeln

ActiveProtect verwendet die langfristige Aufbewahrungsrichtlinie (GFS) für Backups und Backup-Kopien. Dieser Ansatz ermöglicht eine hybride Aufbewahrungsstrategie, die die Dauer des Datenschutzes verlängert und gleichzeitig den Speicherverbrauch minimiert.

1. Gehen Sie zu **Pläne** > **Schutzpläne** im linken Bereich.
2. Klicken Sie auf den Zielschutzplan und gehen Sie zur Registerkarte **Backup-Einstellungen** oder **Backup-Kopie**.
3. Unter **Aufbewahrung** wählen Sie **Erweiterte Aufbewahrungsregeln festlegen** und klicken Sie auf **Regeln festlegen**, um die folgenden GFS-Einstellungen zu konfigurieren:

| Option | Beschreibung |
| --- | --- |
| Alle Versionen behalten für (Tage) | Alle Versionen für eine bestimmte Anzahl von Tagen behalten. |
| Die letzte Version des Tages behalten für (Tage) | Wenn Sie mehrere Versionen an einem Tag haben, wird nur die neueste behalten. Geben Sie an, wie lange Sie diese neueste tägliche Version behalten möchten. |
| Die letzte Version der Woche behalten für (Wochen) | Wenn Sie mehrere Versionen in einer Woche haben, wird nur die neueste behalten. Geben Sie an, wie lange Sie diese neueste wöchentliche Version behalten möchten. |
| Die letzte Version des Monats behalten für (Monate) | Wenn Sie mehrere Versionen in einem Monat haben, wird nur die neueste behalten. Geben Sie an, wie lange Sie diese neueste monatliche Version behalten möchten. |
| Die letzte Version des Jahres behalten für (Jahre) | Wenn Sie mehrere Versionen in einem Jahr haben, wird nur die neueste behalten. Geben Sie an, wie lange Sie diese neueste jährliche Version behalten möchten. |
| Anzahl der zu behaltenden letzten Versionen | Legen Sie die Mindestanzahl der zu behaltenden letzten Versionen fest. Die Aufbewahrungsregeln gelten nur, wenn es mehr Sicherungsversionen als die angegebene Anzahl gibt. |

## Beispiel

Betrachten Sie die folgenden zusammen angewendeten Aufbewahrungsregeln:

- Alle Versionen für 7 Tage behalten
- Die letzte Version jedes Tages für 14 Tage behalten
- Die letzte Version jeder Woche für 3 Wochen behalten

So funktionieren diese Regeln in Kombination:

- In den ersten 7 Tagen werden alle Versionen behalten.

- Dann wird nur die letzte Version jedes Tages für die nächsten 7 Tage behalten, was zu insgesamt 14 Tagen für tägliche Versionen führt.
- Danach wird nur die letzte Version jeder Woche behalten, was eine Gesamtaufbewahrungsdauer von 3 Wochen für wöchentliche Versionen sicherstellt.

Für ein besseres Verständnis, wie Aufbewahrungsregeln bestimmen, welche Versionen behalten werden, siehe den Abschnitt Aufbewahrung.

# Anwendungskonsistente Sicherung

Anwendungskonsistente Sicherung erstellt konsistente Schnappschüsse von Anwendungsdaten auf physischen Servern und virtuellen Maschinen während des Sicherungsprozesses. Dies gewährleistet die Datenkonsistenz und erhöht die Zuverlässigkeit bei der Wiederherstellung von Anwendungen in ihren vorherigen Zustand im Falle einer Katastrophe.

## Bevor Sie beginnen

Stellen Sie sicher, dass Ihre Maschinen die folgenden Anforderungen erfüllen:

- **Für Windows**: Volume Shadow Copy Service (VSS) ist auf der Zielmaschine aktiviert.
- **Für VMware**: Die neueste Version von VMware Tools ist auf der Zielmaschine installiert.

## Anwendungskonsistente Sicherung aktivieren

1. Gehen Sie zu **Pläne** > **Schutzpläne**.
2. Klicken Sie auf den Zielplan und navigieren Sie zur Registerkarte **Anwendungen**.
3. Wählen Sie **Anwendungskonsistente Sicherung aktivieren**.

## Datenbankverarbeitung anpassen

Nach der Aktivierung der anwendungskonsistenten Sicherung können Sie Einstellungen für die Verarbeitung von SQL- oder Oracle-Datenbanken anpassen:

### Verarbeitungsmodus auswählen

Wählen Sie, wie die Sicherung fortgesetzt werden soll, wenn alle Datenbanken oder Datenbankinstanzen nicht verarbeitet werden können oder wenn VSS-Schreiberfehler auftreten:

- **Sicherungen bei Datenbankverarbeitungsfehlern fortsetzen**: Der Sicherungsprozess wird fortgesetzt, um den Abschluss des Sicherungsauftrags sicherzustellen.
- **Sicherungen bei Datenbankverarbeitungsfehlern stoppen**: Der Sicherungsprozess wird beendet, wobei verbleibende Arbeitslastdaten übersprungen werden.

### Protokolleinstellungen konfigurieren

Geben Sie an, wie SQL-Transaktionsprotokolle und Oracle-Archivprotokolle verwaltet werden sollen. Optionen umfassen das Kürzen oder Löschen von Protokollen vom Quell-Datenbankserver.[1]

# Standardanmeldeinformationen festlegen

Um Datenbanksicherungen zu authentifizieren, konfigurieren Sie Standardanmeldeinformationen für das Gastbetriebssystem und die Datenbank, die für alle virtuellen Maschinen oder physischen Server im Schutzplan gelten:

1. Wählen Sie **Standardanmeldeinformationen festlegen**.
2. Klicken Sie auf **Anmeldeeinstellungen** und geben Sie die folgenden Anmeldeinformationen ein.
    - **Gastbetriebssystem-Anmeldeinformationen**: Werden verwendet, um sich bei virtuellen Maschinen für die Datenbankverarbeitung anzumelden. Wenn keine Datenbankanmeldeinformationen bereitgestellt werden, verwendet ActiveProtect auch die Anmeldeinformationen des Gastbetriebssystems zur Verarbeitung von Datenbanken.
    - **Datenbankanmeldeinformationen**: Speziell für die Authentifizierung und Verarbeitung von Datenbanken verwendet.

### Hinweis:

1. Wenn eine Datenbank oder Datenbankinstanz nicht gesichert werden kann, werden die Transaktionsprotokolle nicht gekürzt und die Archivprotokolle nicht gelöscht.

# Erweiterte Maschinen-Einstellungen

Verbessern Sie die Effizienz und Sicherheit der Sicherung mit erweiterten Einstellungen für sowohl physische als auch virtuelle Maschinen. Diese Einstellungen umfassen Sicherungsüberprüfung und Energiemanagement, um die Datenintegrität und eine reibungslose Wiederherstellung in unerwarteten Situationen zu gewährleisten.

Um auf die erweiterten Einstellungen zuzugreifen, gehen Sie zu **Pläne** > **Schutzpläne**. Klicken Sie auf den Zielplan und navigieren Sie zur Registerkarte **Erweiterte Einstellungen**. Die verfügbaren Optionen variieren je nach Maschinentyp:

## Für virtuelle Maschinen

- **Sicherungsüberprüfung aktivieren**: Überprüft die Integrität der gesicherten Daten durch eine Testwiederherstellung auf einer virtuellen Maschine, um eine erfolgreiche Datenwiederherstellung im Katastrophenfall zu gewährleisten.
  - **Videodauer**: Nimmt ein Video während der Testwiederherstellung auf, um die Zuverlässigkeit der Sicherung zu überprüfen. Sie können die Dauer festlegen, und die Wiedergabe erfolgt mit dreifacher Geschwindigkeit.
- **Datastore-Nutzungsüberwachung aktivieren**: Beendet Sicherungen, wenn der Speicherplatz des Host-Datastores unter einen bestimmten Prozentsatz fällt, um das Anhalten virtueller Maschinen und Datenverlust aufgrund unzureichenden Speicherplatzes zu verhindern.

## Für physische Server

- **Sicherungsüberprüfung aktivieren**: Überprüft die Integrität der gesicherten Daten durch eine Testwiederherstellung auf einer virtuellen Maschine, um eine erfolgreiche Datenwiederherstellung im Katastrophenfall zu gewährleisten.
  - **Videodauer**: Nimmt ein Video während der Testwiederherstellung auf, um die Zuverlässigkeit der Sicherung zu überprüfen. Sie können die Dauer festlegen, und die Wiedergabe erfolgt mit dreifacher Geschwindigkeit.
- **Windows-Server nach Abschluss der geplanten Sicherung herunterfahren**: Der Server wird nicht heruntergefahren, wenn eine geplante Sicherung abgebrochen wird.
- **Verhindern, dass Windows-Server während der Sicherung in den Energiesparmodus wechseln**: Diese Option funktioniert nicht, wenn Sie Ihren Server manuell über das **Start**-Menü oder durch Drücken der Ein/Aus-Taste in den Energiesparmodus versetzen.
- **Windows-Server für geplante Sicherungen aus dem Energiesparmodus aktivieren**: Bringt Server automatisch aus dem Energiesparmodus, um geplante Sicherungen durchzuführen, und stellt sicher, dass kritische Daten immer gesichert werden.

## Für Windows-PCs

- **Windows-PCs nach Abschluss der geplanten Sicherung herunterfahren**: Der PC wird nicht heruntergefahren, wenn eine geplante Sicherung abgebrochen wird.
- **Verhindern, dass Windows-PCs während der Sicherung in den Energiesparmodus wechseln**: Diese Option funktioniert nicht, wenn Sie Ihren PC manuell über das **Start**-Menü oder durch Drücken der Ein/Aus-Taste in den Energiesparmodus versetzen.
- **Windows-PCs für geplante Sicherungen aus dem Energiesparmodus aktivieren**: Bringt PCs automatisch aus dem Energiesparmodus, um geplante Sicherungen durchzuführen, und stellt sicher, dass kritische Daten immer gesichert werden.

# Überlegungen und Einschränkungen

Dieser Artikel skizziert die Überlegungen und bekannten Einschränkungen von ActiveProtect in Bezug auf Schutzpläne.

## Aufbewahrung

Bei der Einrichtung von Aufbewahrungsregeln ist es wichtig zu überlegen, wie lange Sie Ihre Daten behalten möchten und welche Versionen aufbewahrt werden sollen. Hier sind einige wichtige Punkte zu beachten:

- **Versionen für bestimmte Tage behalten**: Das System löscht Daten automatisch, sobald der festgelegte Aufbewahrungszeitraum abgelaufen ist.
- **Bestimmte Versionen behalten**: Das System behält eine festgelegte Anzahl erfolgreicher oder teilweise erfolgreicher Versionen. Es behält auch fehlgeschlagene oder abgebrochene Versionen, die nach der letzten (teilweise) erfolgreichen Sicherung erstellt wurden, um Ihnen zu helfen, den neuesten Sicherungsstatus zu verfolgen.
- **Erweiterte Aufbewahrungsregeln**: Ähnlich wie bei der Beibehaltung bestimmter Versionen ermöglicht diese Option komplexere Konfigurationen. Es behält erfolgreiche oder teilweise erfolgreiche Versionen basierend auf Ihren Einstellungen und behält auch fehlgeschlagene oder abgebrochene Versionen, die nach der letzten (teilweise) erfolgreichen Sicherung erstellt wurden, und bietet so einen umfassenden Überblick über Ihren Sicherungsstatus.

## Zeitzone

Beim Ausführen von Sicherungen basierend auf der Zeitzone jedes Sicherungsservers oder Workloads sollten Sie beachten, dass nicht alle Zeitzonen eine einstündige Abweichung von UTC haben.

Für Zeitzonen mit 15-, 30- oder 45-minütigen Abweichungen werden Sicherungen zur nächsten vollen Stunde nach der geplanten Zeit durchgeführt. Wenn Sie beispielsweise Sicherungen für 16:30 planen, werden sie um 17:00 durchgeführt.

# Persönliche Computer sichern

Um Windows-PCs und Mac-Computer zu sichern, müssen Sie auf jedem Endpunkt einen speziellen Agenten installieren, um den Sicherungsprozess zu erleichtern. ActiveProtect ermöglicht es Ihnen, gleichzeitig mehrere Endpunkte bereitzustellen, um die Anforderungen an großflächige Implementierungen zu erfüllen.

## Wie die Sicherung funktioniert

ActiveProtect verwendet eine imagebasierte Sicherung, die die Flexibilität bietet, ein gesamtes System oder bestimmte Volumes zu sichern.

### Windows-PC-Sicherung

ActiveProtect verwendet den Windows Volume Shadow Copy Service (VSS), um sicherzustellen, dass Sicherungen konsistent und genau sind, indem Schnappschüsse der Daten vor der Sicherung erstellt werden. Die Verwendung von Schnappschuss- und Bitmap-Vergleichen ermöglicht inkrementelle Sicherungen.

Der ActiveProtect-Agent führt die folgenden Schritte aus, um Sicherungen aus Schnappschüssen zu erstellen:

1. Sobald ein Schutzplan startet, sendet der ActiveProtect-Agent eine Anfrage an das Windows-Betriebssystem, um einen integrierten Schnappschuss in Form eines neuen LUN mit dem Standard-VSS-Anbieter zu erstellen.
   Wenn der VSS-Anbieter den Schnappschuss nicht erstellen kann, wird der ActiveProtect-Agent auf die Erstellung des Schnappschusses mit dem Standard-VSS-Anbieter des Systems zurückgreifen. Erfahren Sie mehr über den Volume Shadow Copy Service (VSS) und seine Einschränkungen
2. Das erstellte Schnappschuss-LUN verbindet sich mit dem Computer, auf dem der ActiveProtect-Agent installiert ist, um den VSS-Prozess abzuschließen und Speichermetadaten aufzuzeichnen.
3. Der ActiveProtect-Agent liest das Schnappschuss-LUN und überträgt Daten vom Computer auf das ActiveProtect-Gerät.
4. Der ActiveProtect-Agent schließt den Sicherungsprozess ab und löscht Schnappschuss-Metadaten vom Gerät.

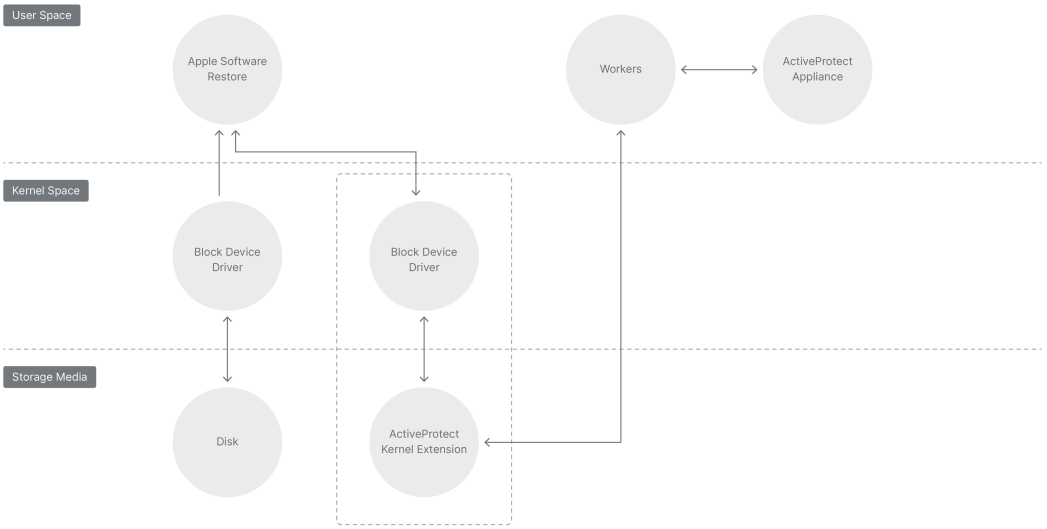
### Mac-Sicherung

ActiveProtect nutzt die Schnappschuss- und Replikationstechnologie des Apple File System (APFS), um zeitpunktgenaue konsistente Sicherungen und inkrementelle Sicherungen auf Blockebene bereitzustellen.

#### Einschränkungen auf einem Mac

Wenn ActiveProtect eine Sicherung durchführt, werden Apple Software Restore (ASR)-Daten zuerst durch einen Blocktreiber verarbeitet, bevor sie durch die Kernel-Erweiterung des ActiveProtect-Agenten gehen. Um optimale Geschwindigkeit und Leistung zu erreichen, sollten Lese-/Schreiboperationen zwischen diesen

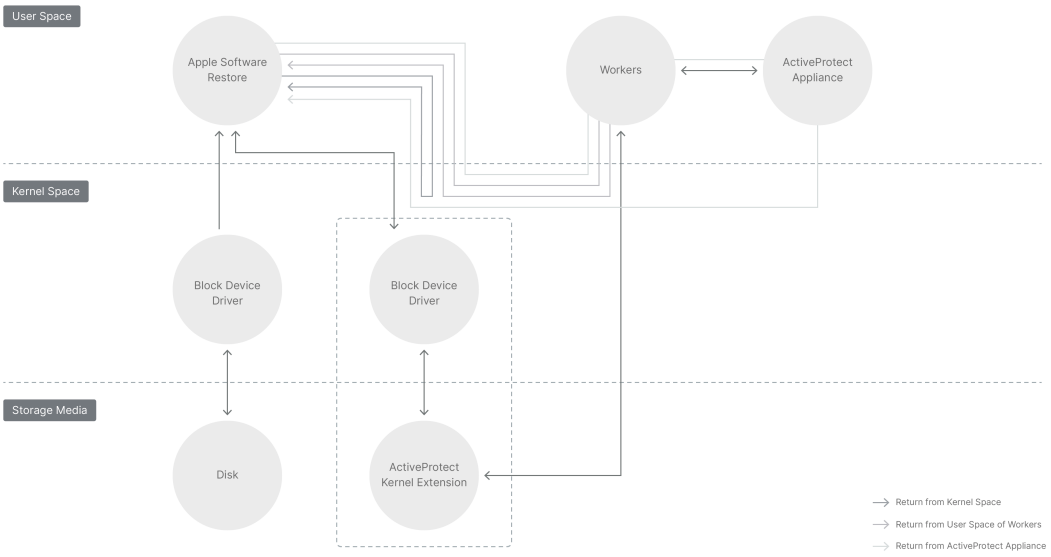
Bereichen idealerweise ununterbrochen ablaufen.




Nach dem Design von Apple müssen in ASR Lesevorgänge auf einer bestimmten Datenmenge durchgeführt werden, bevor die Sicherungsdaten geschrieben werden können. Daher sind Lesevorgänge stark in den Sicherungsprozess eingebunden und Antworten können in folgender Reihenfolge von einem der drei folgenden Orte erhalten werden:

1. Rückkehr aus dem Kernel-Space (Antwortzeit: 10 µs)
2. Rückkehr aus dem User-Space (Antwortzeit: 100 ms)
3. Rückkehr vom ActiveProtect-Gerät (Antwortzeit: 10 s)

Das bedeutet, dass, wenn ein Lesevorgang weder im Kernel- noch im User-Space Treffer erzielt, die Anfrage direkt an das ActiveProtect-Gerät geht, was zu einer längeren Gesamtantwortzeit und einer Verzögerung des Sicherungsprozesses führt.




### Optimierung von ActiveProtect für macOS

Um Leseanforderungen so schnell wie möglich zu verarbeiten, haben wir die Read-Before-Write-Technologie implementiert, um den Wert eines Datenblocks vor seiner Änderung zu überprüfen. Dazu haben wir Bitmap-Indexierung für den Kernel-Space verwendet. Ein Bitmap-Index ist ein Array von Binärdaten, das verwendet wird, um aufzuzeichnen, ob ein Bereich bereits beschrieben wurde oder nicht.

Der Bitmap-Index hilft dem System, leicht herauszufinden, welche Blöcke bereits Daten enthalten und welche nicht. Das System kann dann schnell mit den "leeren" Datenblöcken antworten, was den Sicherungsprozess reibungsloser macht und die Zeit bis zum Abschluss verkürzt.

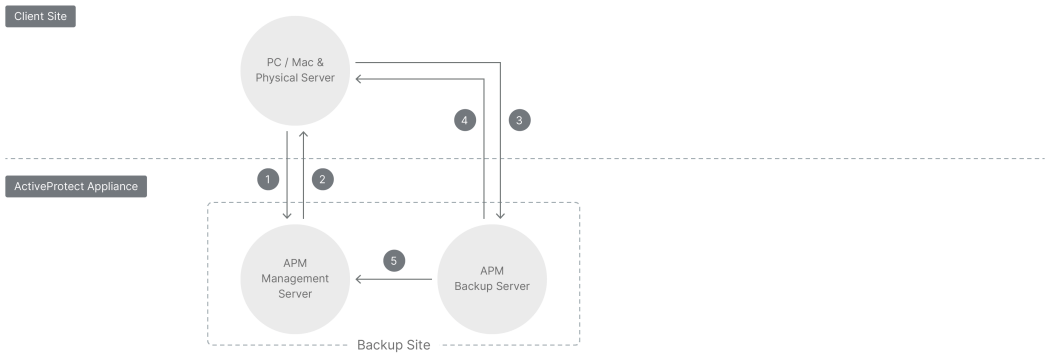
Abschließend konnten wir durch rigoroses Ausprobieren während der Entwicklung die Grenzen von Apple überwinden, was es uns ermöglicht hat, eine Sicherungslösung für macOS zu schaffen, die die Erwartungen übertrifft und konkurrierende Programme, einschließlich der eigenen integrierten Dienste von Mac, übertrifft.

## Authentifizierung

Im **ActiveProtect Manager (APM)** können Sie Verbindungsschlüssel konfigurieren, die als Vorlagen verwendet werden, um automatisch Verbindungen zwischen Agenten und Sicherungsservern an ihrem gewählten Standort herzustellen. Diese Verbindungsschlüssel automatisieren auch die Anwendung des jeweiligen Schutzplans und gewährleisten einen reibungslosen Sicherungsprozess.

Beim Hinzufügen eines physischen Geräts zu APM muss es die folgenden Schritte durchlaufen:

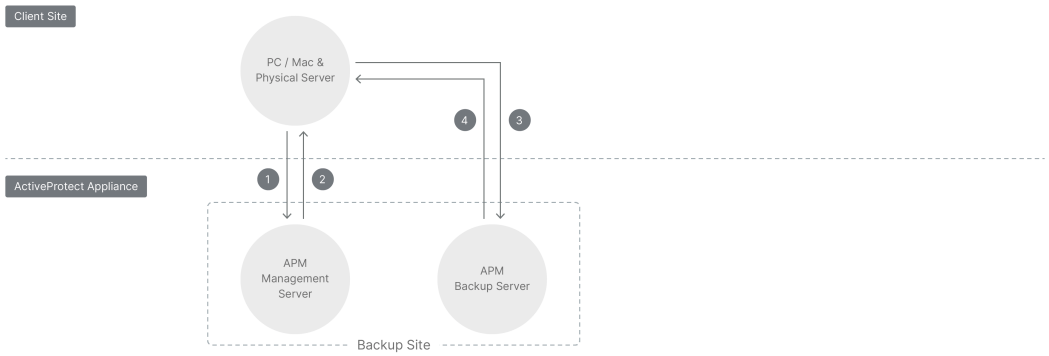
1. Der Client verbindet sich mit dem Verwaltungsserver über den Verbindungsschlüssel und die Serverinformationen über Port 443.
2. Nach der Überprüfung erhält der Client Verbindungs- und Authentifizierungsdetails des Sicherungsziels vom Verwaltungsserver.
3. Der Client verwendet diese Informationen, um sich zu authentifizieren und mit dem Sicherungsziel zu verbinden.
4. Der Client erhält Informationen zum Sicherungsziel und zum Schutzplan.
5. Workload-Informationen werden mit dem Verwaltungsserver synchronisiert.




## Zertifikat

Der Agent initiiert die Verbindung mit dem Verwaltungsserver, um die Verbindungsdetails des Sicherungsservers zu erhalten. Der folgende Validierungsprozess für sowohl den Client als auch das Sicherungsgerät beinhaltet die Verwendung eines Zertifikats:

1. Der Agent verbindet sich über Port 443 mit dem Verwaltungsserver.
2. Nach der Authentifizierung erhält der Agent die IP oder die externe Zugriffsliste des Sicherungsziels und das von APM generierte Zertifikat.
3. Der Agent verbindet sich über Port 8443 mit dem Sicherungsziel unter Verwendung der IP-Liste und des APM-Zertifikats.
4. Der Agent erhält Informationen zum Sicherungsziel und zum Schutzplan.




## Daten-Deduplizierung

ActiveProtect verwendet globale Quell-Deduplizierung, um den Datentransfer zu optimieren und die Sicherungsdauer zu verkürzen. Sie müssen die dedizierten APM-Agenten auf jedem Endpunkt installieren, um Sicherungen durchzuführen.

### Changed Block Tracking (CBT)

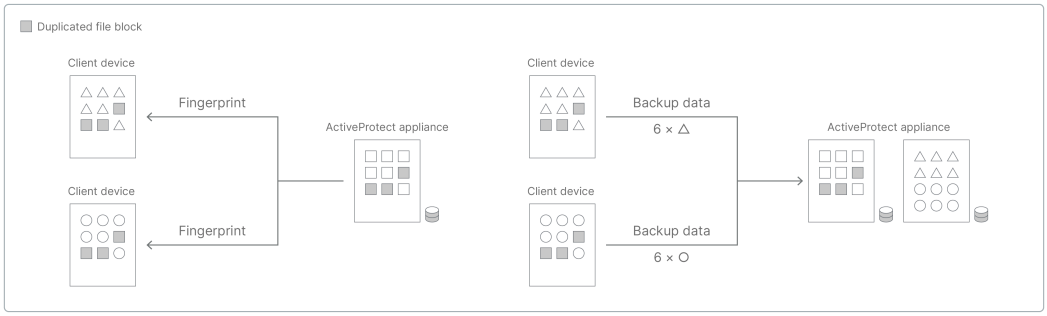
Changed Block Tracking (CBT) ist eine inkrementelle Sicherungstechnologie, die in verschiedenen Sicherungslösungen weit verbreitet ist. Inkrementelle Sicherung sichert speziell Daten, die seit der letzten Sicherung geändert oder erstellt wurden. CBT verbessert inkrementelle Sicherungen, indem es nur die geänderten Datenblöcke erfasst, anstatt das gesamte Dataset zu sichern, was sowohl Zeit als auch Ressourcen spart. Folglich ist die Größe des Sicherungsdatentransfers, also die Menge der durch die Sicherungsanwendung übertragenen Daten, erheblich kleiner als die ursprüngliche Datengröße auf der Sicherungsquelle.

ActiveProtect hat dieses Feature in seine Architektur für die Sicherung von PCs/Macs, physischen Servern und virtuellen Maschinen integriert. Es verwendet eine immer-inkrementelle Sicherung für jede Sicherungsaufgabe, um eine maximale Anzahl verfügbarer Sicherungsversionen zu gewährleisten und gleichzeitig den Speicherverbrauch für die Sicherungsaufbewahrung zu minimieren. Dies wird erreicht, indem nach einer vollständigen Sicherung nur die geänderten Daten selektiv gesichert werden.


### Deduplizierungsprozesse

Während einer Sicherung erfasst ActiveProtect einen Snapshot des zu sichernden Geräts. Anschließend vergleicht es die aktuellen Gerätedaten mit den auf dem Sicherungsgerät gespeicherten Daten. Der Agent

identifiziert und schließt doppelte Dateien aus und lädt nur diejenigen hoch, die zuvor nicht gesichert wurden.




## In diesem Abschnitt

- Systemvoraussetzungen
- Persönliche Computer hinzufügen
- Agenten auf Windows installieren
- Agenten auf Mac installieren
- Verbindungsschlüssel verwalten

# Systemanforderungen

## Windows

### Anforderungen

- Unterstützte Windows Editionen:
  - Windows 11 (alle Editionen)
  - Windows 10 Creators Update (alle Editionen)
  - Windows 10 (alle Editionen)
  - Windows 8.1 (alle Editionen)
  - Windows 7 SP1 (alle Editionen)
- Unterstützte Dateisysteme:
  - NTFS
- Erforderliche Netzwerkports:
  - 8443/443
- Arbeitsverzeichnispfad:
  - C:\ProgramData\ActiveProtect

### Einschränkungen

- Für externe Geräte unterstützt APM nur die Sicherung von NTFS-formatierten externen Festplatten und SSDs. Diskettenlaufwerke, USB-Sticks, Flash-Kartenleser und andere externe Geräte werden nicht unterstützt.
- Personal Computer mit 4Kn-Festplatten werden nicht unterstützt.
- Virtuelle Festplatten (VHD) auf Windows werden nicht unterstützt. Um VHDs zu sichern, sichern Sie das gesamte Gerät oder das Volume, auf dem sich die VHD-Dateien befinden.

## Mac

### Anforderungen

- Unterstützte macOS-Editionen:
  - macOS Catalina 10.15.7
  - macOS Big Sur 11
  - macOS Monterey 12
  - macOS Ventura 13
  - macOS Sonoma 14
  - macOS Sequoia 15

- Unterstützte Dateisysteme:
  - APFS
- Erforderliche Netzwerkports:
  - 8443/443
- Systemvorbereitungen:
  - Für Intel Core
    - Gehen Sie zu System **Einstellungen > Datenschutz & Sicherheit > Festplattenvollzugriff** und wählen Sie den ActiveProtect-Agenten aus der Liste der Anwendungen aus.
    - Ändern Sie das System-Sicherheitsniveau zu **Benutzerverwaltung von Kernel-Erweiterungen von identifizierten Entwicklern zulassen**.
  - Für Apple Silicon
    - Gehen Sie zu System **Einstellungen > Datenschutz & Sicherheit > Festplattenvollzugriff** und wählen Sie den ActiveProtect-Agenten aus der Liste der Anwendungen aus.
    - Ändern Sie das System-Sicherheitsniveau zu **Benutzerverwaltung von Kernel-Erweiterungen von identifizierten Entwicklern zulassen**.
    - Richten Sie ein Secure Token ein.

## Einschränkungen

- Für externe Geräte unterstützt APM nur die Sicherung von APFS-formatierten externen Festplatten und SSDs. Diskettenlaufwerke, USB-Sticks, Flash-Kartenleser und andere externe Geräte werden nicht unterstützt. Um externe Festplatten und SSDs zu sichern, muss der Festplattenvollzugriff aktiviert sein.
- Der ActiveProtect-Agent kann nicht auf Geräten installiert werden, die externe oder Netzwerkvolumes für den Start verwenden. Stellen Sie sicher, dass die geschützten Geräte ein lokales Volume für den Start verwenden.
- Der ActiveProtect-Agent kann keine verschlüsselten Volumes oder APFS-Volumes mit Blockgrößen größer als 4K sichern.

# Persönliche Computer hinzufügen

## Bevor Sie beginnen

### Richten Sie eine externe Adresse für Ihren Verwaltungsserver ein

Der Agent muss sich während der anfänglichen Authentifizierung mit dem Verwaltungsserver verbinden. Wir empfehlen dringend, die externe Adresse Ihres Verwaltungsservers als vollständig qualifizierten Domainnamen (FQDN) zu konfigurieren, damit alle Agenten eine Verbindung herstellen können.

1. Gehen Sie auf Ihrem Verwaltungsserver zu **Infrastruktur** > **Standortverwaltung**.
2. Klicken Sie unter **Externe Adresse und Port** auf **Einrichten**:
   - **Externe Adresse**: Standardmäßig ist dies die IP-Adresse der Out-of-band (OOB)-Schnittstelle. Wenn Sie es als FQDN festlegen, stellen Sie sicher, dass der FQDN auf die OOB-Schnittstellenadresse auf Ihrem DNS-Server verweist.
   - **Port**: Der Standard ist 443. Wenn der verwaltete Server und der Verwaltungsserver in verschiedenen Netzwerken sind, stellen Sie sicher, dass der externe Port auf Port 443 an Ihrem Gateway oder Router umgeleitet wird.

### Zertifikate importieren

Standardmäßig verwendet das System ein selbst signiertes Zertifikat, um Verbindungen für die Standortverwaltung zu sichern. Sie können auch Zertifikate manuell importieren, damit andere Server dem Verwaltungsserver vertrauen. Erfahren Sie, wie Sie Zertifikate für die Standortverwaltung importieren

### Schutzpläne auf Ihre Computer anwenden

Gehen Sie zu **Plan**, um zu überprüfen und zu entscheiden, welchen Schutzplan Sie auf Ihren Computer anwenden möchten.

Folgen Sie diesen Schritten, um persönliche Computer als Workloads hinzuzufügen:

1. Gehen Sie zu **Maschinen** > **PCs/Macs** und klicken Sie auf **Hinzufügen**.
2. Klicken Sie auf **Verbindungsschlüssel erhalten**. Sie können entweder einen neuen Verbindungsschlüssel erstellen oder einen aus der Liste auswählen.
3. Weisen Sie einen Schutzplan und einen Sicherungsserver für den Verbindungsschlüssel zu.
4. Laden Sie den **ActiveProtect-Agent** auf Ihren Computer herunter und installieren Sie ihn:
   - Installieren Sie den APM-Agent auf Windows
   - Installieren Sie den APM-Agent auf Mac
5. Geben Sie die Adresse des Verwaltungsservers ein und fügen Sie den Verbindungsschlüssel in den auf Ihrem Computer installierten Agenten ein.[1]
6. Sobald die Verbindung hergestellt ist, startet der Computer automatisch die Sicherung gemäß den Einstellungen des Schutzplans.

Erfahren Sie, wie Sie persönliche Computer hinzufügen, wenn Ihr Sicherungsserver ein Synology NAS ist.

**Hinweis:**

1. Wir empfehlen dringend, eine Domain-Adresse zu verwenden, um sich mit dem Verwaltungsserver zu verbinden. Dies stellt sicher, dass der Agent und der Server verbunden bleiben, wenn sich die IP-Adresse des Verwaltungsservers ändert. Für eine robustere Einrichtung empfehlen wir, dem Sicherungsserver eine externe Adresse zuzuweisen.

# Agenten auf Windows installieren

Sie können ActiveProtect-Agenten auf Ihren Windows-Computern mit einer der in diesem Artikel bereitgestellten Methoden installieren.

## Agenten über den Agenten-Installer installieren

1. Laden Sie den **ActiveProtect-Agenten** vom **ActiveProtect Manager** oder dem Download Center herunter.
2. Führen Sie den Installer aus und folgen Sie dem Assistenten, um den Vorgang abzuschließen.

## Agenten mit Befehlen installieren

Verwenden Sie die folgenden Befehle, um über SSH eine Verbindung zum Gerät herzustellen und den Agenten bereitzustellen:

1. Laden Sie den **ActiveProtect-Agenten** vom **ActiveProtect Manager** oder dem Download Center herunter.
2. Öffnen Sie die **Eingabeaufforderung** (cmd).
3. Geben Sie den folgenden Befehl ein. Ersetzen Sie "**installer_name**" durch den Dateinamen Ihres Installers, "**copied_connect_key**" durch den Verbindungsschlüssel, den Sie vom ActiveProtect Manager kopiert haben, und "**IP_address**" durch die Adresse des Verwaltungsservers. Geben Sie das Proxy-Passwort für "**proxy_password**" nur ein, wenn Sie über einen Proxy-Server auf den Server zugreifen.

```
msiexec /i "installer_name" APM_ADDRESS="IP_address" PREFER_IPS="addresses"
PROXY_ADDRESS="proxy_address" PROXY_PORT=3128 PROXY_USERNAME="username"
PROXY_PASSWORD="proxy_password" CONNECT_KEY="copied_connect_key"
/qn
```

## Den Agenten massenhaft bereitstellen

Der ActiveProtect-Agent kann auf mehreren Windows-Computern mithilfe eines Gruppenrichtlinienobjekts (GPO) installiert werden. Erfahren Sie, wie Sie den ActiveProtect-Agenten massenhaft bereitstellen

# Agenten auf dem Mac installieren

Sie können ActiveProtect-Agenten auf Ihren Mac-Computern mit einer der in diesem Artikel bereitgestellten Methoden installieren.

## Agenten über das Installationsprogramm installieren

### Bevor Sie beginnen

- Überprüfen Sie die Systemanforderungen und stellen Sie sicher, dass Ihr macOS mit dem **ActiveProtect-Agenten** kompatibel ist.
- Klicken Sie auf das **Apple**-Menü > **Über diesen Mac** > **Übersicht**, um zu überprüfen, ob Ihr Mac-Computer Apple Silicon oder Intel-Prozessoren verwendet. Zusätzliche Schritte sind erforderlich für Apple Silicon-Computer.

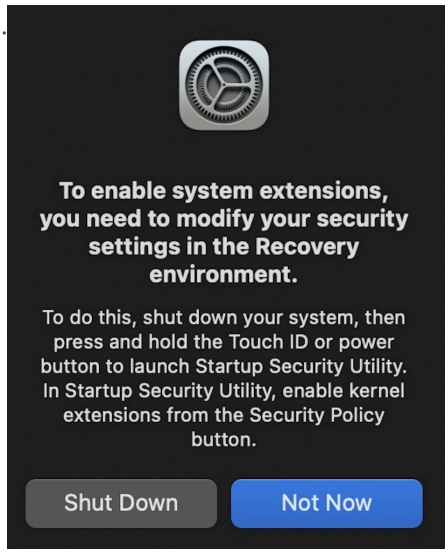
### Den Agenten installieren

1. Laden Sie den **ActiveProtect-Agenten** aus dem **ActiveProtect Manager** oder dem Download-Zentrum herunter.
2. Führen Sie das Installationsprogramm aus. Wenn Sie macOS 13 Ventura oder eine spätere Version verwenden, müssen Sie den **Festplattenvollzugriff** aktivieren, um sicherzustellen, dass ActiveProtect ordnungsgemäß funktioniert. Gehen Sie zu **Systemeinstellungen** > **Datenschutz & Sicherheit** > **Festplattenvollzugriff** und wählen Sie den ActiveProtect-Agenten aus der Liste der Anwendungen aus.
3. Gehen Sie zu **Datenschutz & Sicherheit** und klicken Sie auf **Systemerweiterungen aktivieren**. Wenn das Schloss unten links gesperrt ist, klicken Sie darauf, um das Einstellungsfenster zu entsperren.
4. Klicken Sie auf **Zulassen** unter **Systemsoftware von "Synology Inc." wurde am Laden gehindert**. Um mehrere Systemerweiterungen zu aktivieren, folgen Sie diesen Schritten:
    1. Gehen Sie zu **Datenschutz & Sicherheit** > **Einige Systemsoftware erfordert Ihre Aufmerksamkeit, bevor sie verwendet werden kann** und klicken Sie auf **Details**.
    2. Wählen Sie **Synology Inc. Entwickler** und klicken Sie auf **OK**.
    3. Gehen Sie zurück zu **Datenschutz & Sicherheit** und klicken Sie auf **Zulassen** unter **Systemsoftware von "Synology Inc." wurde am Laden gehindert**.
5. Die Installation wird in Kürze abgeschlossen sein.

### Zusätzliche Schritte für Mac-Computer mit Apple Silicon

Wenn Sie einen Mac mit Apple Silicon verwenden und nach der Installation die folgende Popup-Nachricht sehen, müssen Sie die System-Sicherheitsstufe ändern. Dies ermöglicht es dem Agenten, ordnungsgemäß zu

funktionieren und Ihr Mac wird gesichert.




1. Klicken Sie auf das **Apple**-Menü > **Herunterfahren**. Halten Sie die Einschalttaste gedrückt, bis Sie "Startoptionen werden geladen" sehen.
2. Klicken Sie auf **Optionen** > **Fortfahren**.
3. Klicken Sie in der Menüleiste auf **Dienstprogramme** > **Start-Sicherheitsdienstprogramm**.
4. Wählen Sie die Startdiskette aus, die "Macintosh HD" heißen sollte, wenn Sie ihren Namen nicht geändert haben.


5. Klicken Sie auf **Sicherheitspolitik**.
6. Wählen Sie **Reduzierte Sicherheit**. Wählen Sie **Benutzerverwaltung von Kernel-Erweiterungen von identifizierten Entwicklern zulassen**.
7. Klicken Sie auf **OK**. Starten Sie Ihren Mac neu, damit die Änderungen wirksam werden.

## Agenten mit Befehlen installieren

Verwenden Sie die folgenden Befehle, um sich über SSH mit dem Gerät zu verbinden und den Agenten bereitzustellen:

1. Laden Sie den **ActiveProtect-Agenten** aus dem **ActiveProtect Manager** oder dem Download-Zentrum herunter.

2. Öffnen Sie im **Finder** den Ordner "/Programme/Dienstprogramme" und doppelklicken Sie auf **Terminal**.
3. Erstellen Sie eine neue Konfigurationsdatei für die Installation mit vim:

   ```
   vi ActiveProtectAgentInstallConfig
   ```

4. Geben Sie Ihren Verbindungsschlüssel ein. Ersetzen Sie "**copied_connect_key**" durch den Verbindungsschlüssel, den Sie aus dem ActiveProtect Manager kopiert haben, und "**IP_address**" durch die Adresse des Verwaltungsservers. Wenn Sie über einen Proxy-Server auf den Server zugreifen, ersetzen Sie "**proxy_address**", "**proxy_port**", "**proxy_username**" und "**proxy_password**" durch Ihre Proxy-Informationen.

   ```
   CONNECT_KEY="copied_connect_key"
   APM_ADDRESS="IP_address".
   PROXY_ADDR="proxy_address"
   PROXY_PORT="proxy_port"
   PROXY_USERNAME="proxy_username"
   PROXY_PASSWORD="proxy_password"
   ```

5. Drücken Sie **Esc**, um vim zu verlassen.
6. Geben Sie :wq ein und drücken Sie **Return**, um die Datei zu speichern und zu verlassen.
7. Um den Agenten zu installieren, geben Sie den folgenden Befehl ein. Ersetzen Sie "**installer_name**" durch den Dateinamen Ihres Installationsprogramms.

   ```
   sudo installer -pkg installer_name -target /
   ```

8. Löschen Sie die Konfigurationsdatei, da sie private Informationen enthält.

   ```
   rm ActiveProtectAgentInstallConfig
   ```

# Verbindungsschlüssel verwalten

Sie können Verbindungsschlüssel im ActiveProtect Manager erstellen und verwalten. Verbindungsschlüssel werden verwendet, um Verbindungen zu authentifizieren zwischen Agenten und dem Verwaltungsserver.

## Verbindungsschlüssel erstellen

1. Gehen Sie zu **Maschinen** > **PCs/Macs**.
2. Klicken Sie auf **Mehr** > **Verbindungsschlüssel verwalten** > **Erstellen**.
3. Wählen Sie einen Backup-Server und einen Schutzplan.[1]

## Verbindungsschlüssel verwalten

1. Gehen Sie zu **Maschinen** > **PCs/Macs**.
2. Klicken Sie auf **Mehr** > **Verbindungsschlüssel verwalten**.
3. **Kopieren**[2], **Löschen** oder **Regenerieren**[3] Sie Ihre Verbindungsschlüssel.

**Hinweis:**

1. Sie können nur 1 Verbindungsschlüssel für jede Kombination aus Backup-Server und Schutzplan erstellen.
2. Änderungen am Verbindungsschlüssel wirken sich nicht auf bereits mit dem Server verknüpfte Workloads aus. Der aktualisierte Verbindungsschlüssel gilt nur für neue Workloads.
3. Das Löschen oder Regenerieren von Verbindungsschlüsseln unterbricht nicht die Backups von bereits mit dem Server verknüpften Workloads.

# Physische Server sichern

Um Windows- oder Linux-Server zu sichern, müssen Sie einen dedizierten Agenten installieren, um den Sicherungsprozess zu erleichtern. ActiveProtect ermöglicht es Ihnen, gleichzeitig mehrere Server bereitzustellen, um den Anforderungen großer Implementierungen gerecht zu werden.

## Wie die Sicherung funktioniert

ActiveProtect verwendet eine imagebasierte Sicherung, die die Flexibilität bietet, ein gesamtes System oder bestimmte Volumes zu sichern.

### Windows-Server-Sicherung

ActiveProtect verwendet den Windows Volume Shadow Copy Service (VSS), um sicherzustellen, dass Sicherungen konsistent und genau sind, indem Schnappschüsse der Daten vor der Sicherung erstellt werden. Die Verwendung von Snapshot- und Bitmap-Vergleichen ermöglicht inkrementelle Sicherungen.

Der ActiveProtect-Agent führt die folgenden Schritte aus, um Sicherungen aus Schnappschüssen zu erstellen:

1. Sobald ein Schutzplan startet, sendet der ActiveProtect-Agent eine Anfrage an das Windows-Betriebssystem, um einen integrierten Schnappschuss in Form eines neuen LUN mit dem Standard-VSS-Anbieter zu erstellen.
   Wenn der VSS-Anbieter den Schnappschuss nicht erstellen kann, wird der ActiveProtect-Agent den Schnappschuss mit dem Standard-VSS-Anbieter des Systems erstellen. Erfahren Sie mehr über den Volume Shadow Copy Service (VSS) und seine Einschränkungen
2. Das erstellte Snapshot-LUN verbindet sich mit dem Server, auf dem der ActiveProtect-Agent installiert ist, um den VSS-Prozess abzuschließen und Speichermetadaten aufzuzeichnen.
3. Der ActiveProtect-Agent liest das Snapshot-LUN und überträgt Daten vom Server zum ActiveProtect-Gerät.
4. Der ActiveProtect-Agent schließt den Sicherungsprozess ab und löscht die Snapshot-Metadaten vom Server.

### Linux-Sicherung

ActiveProtect nutzt den auf Snapshot-Treibern basierenden Changed Block Tracking-Mechanismus, um inkrementelle Sicherungen für Linux-Server durchzuführen. Der Snapshot-Treiber verfolgt effizient die Änderungen auf Blockebene und zeichnet die Unterschiede zwischen der aktuellen und der vorherigen Sicherung auf. Während inkrementeller Sicherungen werden nur die geänderten Blöcke an den Sicherungsserver übertragen.

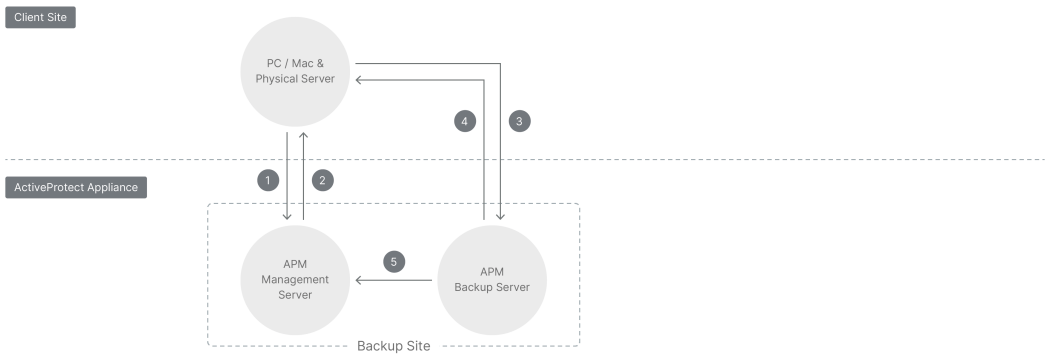
### Authentifizierung

Im **ActiveProtect Manager (APM)** können Sie Verbindungsschlüssel konfigurieren, die als Vorlagen verwendet werden, um automatisch Verbindungen zwischen Agenten und Sicherungsservern an ihrem

gewählten Standort herzustellen. Diese Verbindungsschlüssel automatisieren auch die Anwendung des jeweiligen Schutzplans und gewährleisten einen reibungslosen Sicherungsprozess.

Beim Hinzufügen eines physischen Servers zu APM muss er die folgenden Schritte durchlaufen:

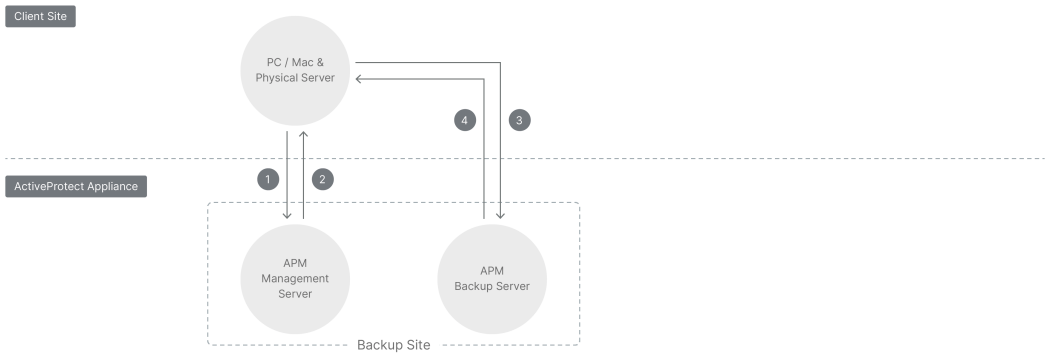
1. Der physische Server verbindet sich mit dem Verwaltungsserver über den Verbindungsschlüssel und die Serverinformationen über Port 443.
2. Nach der Überprüfung erhält der physische Server Verbindungs- und Authentifizierungsdetails für das Sicherungsziel vom Verwaltungsserver.
3. Der physische Server verwendet diese Informationen, um sich zu authentifizieren und mit dem Sicherungsziel zu verbinden.
4. Der physische Server erhält Informationen zum Sicherungsziel und zum Schutzplan.
5. Workload-Informationen werden mit dem Verwaltungsserver synchronisiert.




## Zertifikat

Der Agent initiiert die Verbindung mit dem Verwaltungsserver, um die Verbindungsdetails des Sicherungsservers zu erhalten. Der folgende Validierungsprozess für sowohl den physischen Server als auch das Sicherungsgerät beinhaltet die Verwendung eines Zertifikats:

1. Der Agent verbindet sich über Port 443 mit dem Verwaltungsserver.
2. Nach der Authentifizierung erhält der Agent die IP oder die externe Zugriffsliste des Sicherungsziels und das von APM generierte Zertifikat.
3. Der Agent verbindet sich über Port 8443 mit dem Sicherungsziel unter Verwendung der IP-Liste und des APM-Zertifikats.
4. Der Agent erhält Informationen zum Sicherungsziel und zum Schutzplan.



## Daten-Deduplizierung

ActiveProtect verwendet globale Quell-Deduplizierung, um den Datentransfer zu optimieren und die Sicherungsdauer zu verkürzen. Sie müssen die dedizierten Agenten von APM auf jedem Server installieren, um Sicherungen durchzuführen.

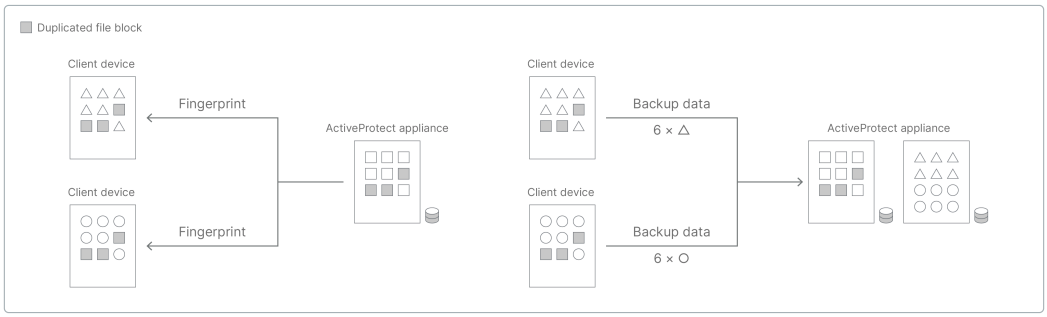
### Changed Block Tracking (CBT)

Changed Block Tracking (CBT) ist eine inkrementelle Sicherungstechnologie, die in verschiedenen Sicherungslösungen weit verbreitet ist. Inkrementelle Sicherung sichert speziell Daten, die seit der letzten Sicherung geändert oder erstellt wurden. CBT verbessert inkrementelle Sicherungen, indem es nur die geänderten Datenblöcke erfasst, anstatt den gesamten Datensatz zu sichern, was sowohl Zeit als auch Ressourcen spart. Folglich ist die Größe der übertragenen Sicherungsdaten, also die Menge der durch die Sicherungsanwendung übertragenen Daten, erheblich kleiner als die ursprüngliche Datengröße auf der Sicherungsquelle.

ActiveProtect hat diese Funktion in seine Architektur für die Sicherung von PCs/Macs, physischen Servern und virtuellen Maschinen integriert. Es verwendet eine fortlaufend inkrementelle Sicherung für jede Sicherungsaufgabe, um eine maximale Anzahl verfügbarer Sicherungsversionen zu gewährleisten und gleichzeitig den Speicherverbrauch für die Sicherungsaufbewahrung zu minimieren. Dies wird erreicht, indem nur die geänderten Daten nach einer vollständigen Sicherung selektiv gesichert werden.


### Deduplizierungsprozesse

Während einer Sicherung erfasst ActiveProtect einen Snapshot des zu sichernden Geräts. Anschließend vergleicht es die aktuellen Gerätedaten mit den auf dem Sicherungsgerät gespeicherten Daten. Der Agent identifiziert und schließt doppelte Dateien aus und lädt nur diejenigen hoch, die zuvor nicht gesichert wurden.




# In diesem Abschnitt

- Systemvoraussetzungen
- Physische Server hinzufügen
- Agenten auf Windows installieren
- Agenten auf Linux installieren

- Verbindungsschlüssel verwalten

# Systemanforderungen

## Windows

### Anforderungen

- Unterstützte Windows Editionen:
  - Windows Server 2022
  - Windows Server 2019
  - Windows Server 2016
- Unterstützte Dateisysteme:
  - NTFS
- Erforderliche Netzwerkports:
  - 8443/443

### Einschränkungen

- Für externe Geräte unterstützt ActiveProtect nur die Sicherung von NTFS-formatierten externen Festplatten und SSDs. Diskettenlaufwerke, USB-Sticks, Flash-Kartenleser und andere externe Geräte werden nicht unterstützt.
- Virtuelle Festplatten (VHD) auf Windows werden nicht unterstützt. Um VHDs zu sichern, sichern Sie das gesamte Gerät oder das Volume, auf dem sich die VHD-Dateien befinden.

## Linux

### Anforderungen

- Unterstützte Kernel-Versionen:
  - Zwischen 2.6 und 6.8
- DEB:
  - Ubuntu: 16.04, 18.04, 20.04, 22.04, 24.04
  - Debian: 10, 11, 12
- RPM:
  - CentOS: 7.8, 7.9, 8.1, 8.5
  - Red Hat Enterprise Linux (RHEL): 6.10, 7.8, 7.9, 8.1, 8.4, 8.5, 8.6, 8.7, 8.8, 8.9, 8.10, 9.0, 9.1, 9.2, 9.3, 9.4
  - Fedora: 38, 39, 40
- Unterstützte Dateisysteme:
  - ext2
  - ext3

    - ext4
    - XFS
- Unterstützte Gerätetypen:
    - /dev/sdx
    - /dev/hdx
    - /dev/vdx
    - /dev/nvmex
    - /dev/mdx
    - /dev/xvdx
- Erforderliche Komponenten auf dem Zielgerät:
    - make Version 4.1 oder höher
    - dkms Version 2.2.0.3 oder höher
    - gcc Version 4.8.2 oder höher
    - bc (für RPM-basierte Systeme, wie Fedora, CentOS und RHEL)
- Erforderlicher Netzwerkport
    - 8443/443

## Einschränkungen

- Externe Geräte können nicht gesichert werden.
- ZFS und Btrfs werden nicht unterstützt.

# Physische Server hinzufügen

## Bevor Sie beginnen

### Richten Sie eine externe Adresse für Ihren Verwaltungsserver ein

Der Agent muss sich während der anfänglichen Authentifizierung mit dem Verwaltungsserver verbinden. Wir empfehlen dringend, die externe Adresse Ihres Verwaltungsservers als vollständig qualifizierten Domainnamen (FQDN) zu konfigurieren, damit alle Agenten eine Verbindung herstellen können.

1. Gehen Sie auf Ihrem Verwaltungsserver zu **Infrastruktur** > **Standortverwaltung**.
2. Klicken Sie unter **Externe Adresse und Port** auf **Einrichten**:
   - **Externe Adresse**: Standardmäßig ist dies die IP-Adresse der Out-of-band (OOB)-Schnittstelle. Wenn Sie sie als FQDN festlegen, stellen Sie sicher, dass der FQDN auf die OOB-Schnittstellenadresse auf Ihrem DNS-Server verweist.
   - **Port**: Der Standardwert ist 443. Wenn der verwaltete Server und der Verwaltungsserver in verschiedenen Netzwerken sind, stellen Sie sicher, dass der externe Port auf Port 443 an Ihrem Gateway oder Router umgeleitet wird.

### Zertifikate importieren

Standardmäßig verwendet das System ein selbstsigniertes Zertifikat, um Verbindungen für die Standortverwaltung zu sichern. Sie können auch Zertifikate manuell importieren, damit andere Server dem Verwaltungsserver vertrauen. Erfahren Sie, wie Sie Zertifikate für die Standortverwaltung importieren

### Schutzpläne auf Ihre physischen Server anwenden

Gehen Sie zu **Plan**, um zu überprüfen und zu entscheiden, welchen Schutzplan Sie auf Ihren physischen Server anwenden möchten.

Befolgen Sie diese Schritte, um physische Server als Workloads hinzuzufügen:

1. Gehen Sie zu **Maschinen** > **Physische Server** und klicken Sie auf **Hinzufügen**.
2. Klicken Sie auf **Verbindungsschlüssel abrufen**. Sie können entweder einen neuen Verbindungsschlüssel erstellen oder einen aus der Liste auswählen.
3. Weisen Sie einen Schutzplan und einen Sicherungsserver für den Verbindungsschlüssel zu.
4. Laden Sie den **ActiveProtect-Agent** auf Ihrem Gerät herunter und installieren Sie ihn:
   - Installieren Sie den APM-Agent auf Windows
   - Installieren Sie den APM-Agent auf Linux
5. Geben Sie die Adresse des Verwaltungsservers ein und fügen Sie den Verbindungsschlüssel in den auf Ihrem Gerät installierten Agenten ein.[1]
6. Sobald die Verbindung hergestellt ist, beginnt das Gerät automatisch mit der Sicherung gemäß den Einstellungen des Schutzplans.

Erfahren Sie wie Sie physische Server hinzufügen, wenn Ihr Sicherungsserver ein Synology NAS ist.

**Hinweis:**

1. Wir empfehlen dringend, eine Domain-Adresse zu verwenden, um eine Verbindung zum Verwaltungsserver herzustellen. Dies stellt sicher, dass der Agent und der Server verbunden bleiben, wenn sich die IP-Adresse des Verwaltungsservers ändert. Für eine robustere Einrichtung empfehlen wir, dem Sicherungsserver eine externe Adresse zuzuweisen.

# Ein Skriptprofil erstellen

Passen Sie ein Skriptprofil für konsistente Sicherungen physischer Server an. Pre-Freeze-Skripte bereiten Maschinen vor der Sicherung vor, um die Datenintegrität zu gewährleisten. Post-Thaw-Skripte stellen Maschinen nach der Sicherung in ihren ursprünglichen Zustand zurück, um das Risiko von Datenverlusten zu minimieren.

1. Gehen Sie zu **Maschinen** > **Physische Server** > **Mehr** und klicken Sie auf **Skripteinstellungen**.
2. Klicken Sie auf **Erstellen**.
3. Geben Sie einen Profilnamen ein und wählen Sie einen Verarbeitungsmodus:
   - **Fehler bei der Skriptausführung ignorieren und Sicherungen fortsetzen**: Sicherungen werden fortgesetzt, auch wenn das Skript nicht ausgeführt werden kann.
   - **Erfolgreiche Skriptausführung erforderlich, um Sicherungen fortzusetzen**: Sicherungen werden gestoppt, wenn das Skript nicht ausgeführt werden kann.
   1. Klicken Sie auf das **Ordner**-Symbol, um Ihre Pre-Freeze- und Post-Thaw-Skripte hochzuladen.
   2. Wählen Sie die Ziel-Physikserver für die Skriptausführung aus.
   3. Bestätigen Sie die Zusammenfassung der Einstellungen.

## Anmeldeinformationen festlegen

Sie können jeder Arbeitslast spezifische Anmeldeinformationen zuweisen, um den Datenbankzugriff zu authentifizieren. Diese Anmeldeinformationen überschreiben die in den Schutzplänen festgelegten Standardwerte.
Um individuelle Anmeldeinformationen festzulegen, folgen Sie diesen Schritten:

1. Wählen Sie die Ziel-Physikalischen Server aus.
2. Klicken Sie auf **Mehr** und wählen Sie dann **Anmeldeinformationen angeben**.
3. Geben Sie die Datenbank-Anmeldeinformationen ein.

# Agenten auf Windows installieren

Sie können ActiveProtect-Agenten auf Ihren Windows-Computern mit einer der in diesem Artikel bereitgestellten Methoden installieren.

## Agenten über das Installationsprogramm installieren

1. Laden Sie den **ActiveProtect-Agenten** vom **ActiveProtect Manager** oder dem Download Center herunter.
2. Führen Sie das Installationsprogramm aus und folgen Sie dem Assistenten, um den Vorgang abzuschließen.

## Agenten mit Befehlen installieren

Verwenden Sie die folgenden Befehle, um sich über SSH remote mit dem Server zu verbinden und den Agenten bereitzustellen:

1. Laden Sie den **ActiveProtect-Agenten** vom **ActiveProtect Manager** oder dem Download Center herunter.
2. Öffnen Sie die **Eingabeaufforderung** (cmd).
3. Geben Sie den folgenden Befehl ein. Ersetzen Sie "**installer_name**" durch den Dateinamen Ihres Installationsprogramms, "**copied_connect_key**" durch den Verbindungsschlüssel, den Sie vom ActiveProtect Manager kopiert haben, und "**IP_address**" durch die Adresse des Verwaltungsservers. Geben Sie das Proxy-Passwort für "**proxy_password**" nur ein, wenn Sie über einen Proxy-Server auf den Server zugreifen.

```
msiexec /i "installer_name" APM_ADDRESS="IP_address" PREFER_IPS="addresses"
PROXY_ADDRESS="proxy_address" PROXY_PORT=3128 PROXY_USERNAME="username"
PROXY_PASSWORD="proxy_password" CONNECT_KEY="copied_connect_key" /qn
```

## Den Agenten massenhaft bereitstellen

Der ActiveProtect-Agent kann auf mehreren Windows-Computern mithilfe eines Gruppenrichtlinienobjekts (GPO) installiert werden. Erfahren Sie, wie Sie den ActiveProtect-Agenten massenhaft bereitstellen

# Agenten auf Linux installieren

Sie können ActiveProtect-Agenten auf Ihren Linux-Servern über die Befehlszeile installieren.

## Installation über das Agenten-Installationsprogramm

1. Laden Sie den **ActiveProtect-Agenten** vom **ActiveProtect Manager** oder dem Download-Zentrum herunter.
2. Um sich mit dem Verbindungsschlüssel bei der Backup-Appliance anzumelden, geben Sie den folgenden Befehl ein.

   ```
   sudo activeprotect-agent-cli -m
   ```

3. Geben Sie die Anmeldedaten ein.
4. Um die Zusammenfassung zu bestätigen und Ihr Linux mit der Backup-Appliance zu verbinden, drücken Sie **y**.

# Verbindungsschlüssel verwalten

Sie können Verbindungsschlüssel im ActiveProtect Manager erstellen und verwalten. Verbindungsschlüssel werden verwendet, um Verbindungen zu authentifizieren zwischen Agenten und dem Verwaltungsserver.

## Verbindungsschlüssel erstellen

1. Gehen Sie zu **Maschinen** > **Physische Server**.
2. Klicken Sie auf **Mehr** > **Verbindungsschlüssel verwalten** > **Erstellen**.
3. Wählen Sie einen Backup-Server und einen Schutzplan.[1]

## Verbindungsschlüssel verwalten

1. Gehen Sie zu **Maschinen** > **Physische Server**.
2. Klicken Sie auf **Mehr** > **Verbindungsschlüssel verwalten**.
3. **Kopieren**[2], **Löschen** oder **Regenerieren**[3] Sie Ihre Verbindungsschlüssel.

**Hinweis:**

1. Sie können nur einen Verbindungsschlüssel für jede Kombination aus Backup-Server und Schutzplan erstellen.
2. Änderungen am Verbindungsschlüssel wirken sich nicht auf bereits mit dem Server verknüpfte Workloads aus. Der aktualisierte Verbindungsschlüssel gilt nur für neue Workloads.
3. Das Löschen oder Regenerieren von Verbindungsschlüsseln unterbricht nicht die Backups von bereits mit dem Server verknüpften Workloads.

# Virtuelle Maschinen sichern

ActiveProtect verwendet einen bildbasierten Ansatz, um virtuelle Maschinen direkt auf der Virtualisierungsebene zu sichern. Es bietet auch die Flexibilität, automatische Sicherungsregeln für eine einfache und nahtlose Datensicherung anzupassen.

## Wie die Sicherung funktioniert

Die Sicherung virtueller Maschinen funktioniert ohne Agenten und nutzt den nativen Snapshot-Dienst, um Daten aus dem Gastbetriebssystem zu extrahieren. Während des Sicherungsprozesses veranlasst das System VMware vSphere und Microsoft Hyper-V, einen Snapshot der virtuellen Maschine mithilfe der nativen API zu erstellen, und sichert dann die Daten, indem es auf diesen Bild-Snapshot verweist.

## Automatisierte Sicherungsstrategie

Automatische Sicherungsregeln sind entscheidend für die Sicherung virtueller Maschinen. Legen Sie Regeln fest, um bestehende und neu hinzugefügte virtuelle Maschinen innerhalb bestimmter Ordner oder Cluster automatisch zu schützen. Dies macht Sicherungen mühelos und hält die Synchronisation mit der VM-Infrastruktur der Organisation aufrecht.

## In diesem Abschnitt

# Systemanforderungen

## Microsoft Hyper-V

- Unterstützte Hyper-V Hypervisoren:
  - Windows Server Hyper-V 2022
  - Windows Server Hyper-V 2019
  - Windows Server Hyper-V 2016
- Unterstütztes System Center Virtual Machine Manager (SCVMM):
  - System Center Virtual Machine Manager 2019
  - System Center Virtual Machine Manager 2016
- Unterstützte Hyper-V Failover-Cluster:
  - Windows Server Hyper-V 2022
  - Windows Server Hyper-V 2019
  - Windows Server Hyper-V 2016
- Unterstützt Hyper-V Generation 1 und 2 virtuelle Maschinen, einschließlich 64 TB VHDX-Festplatten und virtueller Hardwareversionen 5.0 bis 9.0.
- Diensteinstellungen:
  - Erlauben Sie SMB-Verbindungen durch die Firewall auf dem Hyper-V-Host.
  - Aktivieren Sie WinRM auf dem Hyper-V-Host. Für Mitglieder der Administratorengruppe (außer dem Administratorkonto) muss User Account Control (UAC) deaktiviert werden, wenn der Hyper-V-Host nicht Teil einer Domäne ist.
- Speicheranforderung: Das Systemvolume des Hosts muss mindestens 512 MB freien Speicherplatz haben, um einen Datenmover für Sicherungen zu installieren.

## VMware vSphere

- Unterstützte VMware vSphere Versionen: 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7.0, 8.0
- Unterstützte VMware Editionen:
  - VMware kostenlose ESXi
  - VMware vSphere Essentials, VMware vSphere Essentials Plus
  - VMware vSphere Standard, VMware vSphere Advanced
  - VMware vSphere Enterprise, VMware vSphere Enterprise Plus
- Unterstützt alle Typen und Versionen von VMware virtueller Hardware, einschließlich 62 TB VMDK
- Diensteinstellungen:
  - Um anwendungsbewusste Sicherungen durchzuführen oder Pre-Freeze/Post-Thaw-Skripte auszuführen, stellen Sie sicher, dass **VMware Tools** auf der virtuellen Maschine installiert ist. (Nicht verfügbar für die kostenlose ESXi-Version)

- Für die kostenlose Version von VMware ESXi aktivieren Sie die folgenden Dienste:
  - **Secure Shell (SSH)** und **ESXi Shell** für Sicherungen
  - Changed Block Tracking für inkrementelle Sicherungen

## Netzwerk

Um die Sicherungsfunktionalität sicherzustellen, ergreifen Sie während der Hypervisor-Einrichtung die folgenden Maßnahmen:

- Wenn der Hypervisor hinter einem NAT steht, konfigurieren Sie Portweiterleitungsregeln darauf.
- Wenn der Hypervisor hinter einer Firewall steht, erlauben Sie Sicherungsdienste durch die Firewall-Regeln.
- Stellen Sie sicher, dass die folgenden TCP-Ports geöffnet sind, um die Kommunikation zwischen Ihren Sicherungsservern und virtuellen Maschinen zu ermöglichen:

| Typ | | TCP-Port | Details |
|---|---|---|---|
| Microsoft Hyper-V | • Hyper-V-Hosts | 445 (SMB-Port) | Dieser Port wird für den Empfang und die Übertragung von Daten zwischen Ihrem Sicherungsserver und Hyper-V verwendet. |
| | • SCVMM<br>• Failover-Cluster<br>• Hyper-V-Hosts | 5985 | Dieser Port wird für die Übertragung und Verschiebung von Daten verwendet. |
| | • SCVMM<br>• Failover-Cluster<br>• Hyper-V-Hosts | 5986 | Dieser Port wird für die Verschlüsselung während der Übertragung und Bewegung von Daten verwendet. |
| VMware vSphere | • vCenter-Server<br>• ESXi-Hosts | 443 | Dieser Port wird für die Verbindung zur VMware-Infrastruktur verwendet. |
| | • ESXi-Hosts | 902 | Dieser Port wird für die Übertragung und Bewegung von Daten verwendet. |

# Einschränkungen

## Microsoft Hyper-V

- Virtuelle Maschinen
  - Virtuelle Maschinen mit Konfigurationsversionen 5.0 oder früher werden nicht unterstützt. Weitere Informationen finden Sie unter Upgrade der virtuellen Maschinenversion.
  - Backup-, Sofortwiederherstellungs- und Vollwiederherstellungsoperationen können nicht auf virtuellen Maschinen durchgeführt werden, wenn ihre Namen, Ordnerstandorte oder Festplattennamen Sonderzeichen wie [ ] ‘ , enthalten.
  - Die Verbindung zu Backup-Servern über einen anderen Port als den Out-of-Band (OOB)-Port kann zu Betriebsfehlern führen, einschließlich Backup-Fehlern, Sofortwiederherstellungsproblemen, vollständigen Maschinenwiederherstellungsfehlern und erfolglosen Migrationen vom integrierten Hypervisor zu Hyper-V.
- Virtuelle Hardware
  - Durchgeschleifte virtuelle Festplatten und Gastfestplatten, die über In-Guest-FC oder iSCSI verbunden sind, werden nicht unterstützt und werden während der Backups automatisch übersprungen.
  - Durchgeschleifte virtuelle Festplatten werden auf virtuellen Maschinen, die Hyper-V-Versionen 2016 bis 2019 ausführen, nicht unterstützt.

## VMware vSphere

- Verschlüsselte virtuelle Maschinen, eine in VMware vSphere 6.5 eingeführte Funktion, werden derzeit nicht unterstützt.
- Fehlertolerante Maschinen, eine in VMware vSphere 6.0 eingeführte Funktion, werden derzeit nicht unterstützt.
- VMware unterstützt keine Snapshots für die folgenden Festplattentypen, die während der Verarbeitung übersprungen werden: Raw Device Mapping (RDM)-Festplatten im physischen Modus, unabhängige Festplatten, Festplatten, die über einen In-Guest-iSCSI-Initiator verbunden sind, und Festplatten, die am SCSI-Bus-Sharing beteiligt sind.
- Die Verbindung zu Backup-Servern über einen anderen Port als den Out-of-Band (OOB)-Port kann zu Sofortwiederherstellungsfehlern führen.

# Virtuelle Maschinen hinzufügen

Dieser Artikel bietet eine Schritt-für-Schritt-Anleitung zum Hinzufügen virtueller Maschinen für den Backup-Schutz und beschreibt die notwendigen Schritte im Prozess.

## Bevor Sie beginnen

- Stellen Sie sicher, dass Sie Ihre Hypervisoren hinzufügen, indem Sie zu **Infrastruktur** > **Hypervisoren** gehen. Dies ermöglicht es ActiveProtect, Ihre virtuellen Maschinen zu identifizieren.
- Stellen Sie sicher, dass Ihre virtuellen Maschinen die Systemanforderungen erfüllen.

## Automatische Sicherungsregel festlegen

Legen Sie eine automatisierte Regel fest, um anzugeben, welche Ordner oder Cluster gesichert werden sollen, zusammen mit den entsprechenden Schutzplänen und Sicherungsservern. ActiveProtect sichert automatisch virtuelle Maschinen innerhalb der ausgewählten Einheiten.

1. Gehen Sie zu **Maschinen** > **Virtuelle Maschinen**.
2. Klicken Sie in der oberen Leiste auf **Hinzufügen**.
3. Wählen Sie **Automatische Sicherung: Nach Cluster oder Ordner**.
4. Wählen Sie einen Server für die Durchführung von Sicherungen und die Speicherung von Sicherungsdaten.
5. Wählen Sie die Ordner oder Cluster aus, die Sie sichern möchten. Für VMware vSphere können Sie die Ressourcenansicht über die obere Leiste wechseln.
6. Wählen Sie einen anzuwendenden Schutzplan aus.
7. Bestätigen Sie die Zusammenfassung der Regel.

## Automatische Sicherungsregeln bearbeiten

Sie können die automatischen Sicherungsregeln anpassen, indem Sie in der oberen Leiste auf **Automatische Sicherungseinstellungen** klicken.

Die folgenden Aktionen sind verfügbar:

- **Schutzpläne ändern**: Ändern Sie den Schutzplan, der mit einer automatischen Sicherungsregel verbunden ist. Bestehende Workloads werden weiterhin durch die Pläne gesichert, die ihnen zugewiesen wurden, als sie durch die automatische Sicherungsregel hinzugefügt wurden. Bei Bedarf können Sie die Schutzpläne für diese Workloads ändern, indem Sie auf **Mehr** > **Plan ändern** klicken.
- **Automatische Sicherungsregeln hinzufügen oder anpassen**: Erstellen Sie neue Regeln oder ändern Sie den Umfang bestehender. Wenn mehrere Regeln vorhanden sind, basiert die Priorität auf ihrer Reihenfolge, wobei die Regeln oben eine höhere Priorität haben. Sie können die Priorität anpassen, indem Sie Regeln nach oben oder unten ziehen.

Zum Beispiel, wenn ein Hypervisor-Ordner in zwei verschiedenen Regeln enthalten ist, wird eine neue virtuelle Maschine, die diesem Ordner hinzugefügt wird, der obersten Regel folgen. Die Einstellungen der anderen Regel werden nicht angewendet, um doppelte Sicherungen zu verhindern.

## Einzelne virtuelle Maschinen hinzufügen

Wenn Sie lieber bestimmte virtuelle Maschinen anstelle ganzer Ordner oder Cluster sichern möchten, können Sie diese manuell als Workloads hinzufügen.[1]

1. Gehen Sie zu **Maschinen** > **Virtuelle Maschinen**.
2. Klicken Sie in der oberen Leiste auf **Hinzufügen**.
3. Wählen Sie **Einzelsicherung: Nach spezifischer VM**.
4. Wählen Sie einen Server für die Durchführung von Sicherungen und die Speicherung von Sicherungsdaten.
5. Wählen Sie die virtuellen Maschinen aus, die Sie sichern möchten. Das System führt eine Vorbedingungsprüfung durch, um zu bestätigen, dass die ausgewählten Maschinen ordnungsgemäß gesichert werden können.
6. Wählen Sie einen anzuwendenden Schutzplan aus.
7. Bestätigen Sie die Zusammenfassung der Sicherung.

## Ein Skriptprofil erstellen

Passen Sie ein Skriptprofil an, um konsistente Sicherungen virtueller Maschinen sicherzustellen. Pre-Freeze-Skripte bereiten Maschinen vor der Sicherung vor und gewährleisten die Datenintegrität, während Post-Thaw-Skripte Maschinen nach der Sicherung in ihren ursprünglichen Zustand zurückversetzen und das Risiko von Datenverlusten minimieren.

1. Gehen Sie zu **Maschinen** > **Virtuelle Maschinen** > **Mehr** und klicken Sie auf **Skripteinstellungen**.
2. Klicken Sie auf **Erstellen**.
3. Geben Sie einen Profilnamen ein und wählen Sie einen der folgenden Verarbeitungsmodi:
   - **Fehler bei der Skriptausführung ignorieren und Sicherungen fortsetzen**: Sicherungen werden fortgesetzt, selbst wenn das Skript nicht ausgeführt werden kann.
   - **Erfolgreiche Skriptausführung erforderlich, um Sicherungen fortzusetzen**: Sicherungen werden gestoppt, wenn das Skript nicht ausgeführt werden kann.
4. Klicken Sie auf das **Ordner**-Symbol, um Ihre Pre-Freeze- und Post-Thaw-Skripte hochzuladen.
5. Wählen Sie die Ziel-VMs für die Skriptausführung aus.[2]
6. Bestätigen Sie die Zusammenfassung der Einstellungen.

## Anmeldeinformationen festlegen

Sie können spezifische Anmeldeinformationen für jede Arbeitslast zuweisen. Diese individuellen Anmeldeinformationen überschreiben die in den Schutzplänen festgelegten Standardwerte.

Um individuelle Anmeldeinformationen festzulegen, folgen Sie diesen Schritten:

1. Wählen Sie die Ziel-VMs aus.
2. Klicken Sie auf **Mehr** und wählen Sie dann **Anmeldeinformationen festlegen**.
3. Geben Sie die folgenden Anmeldeinformationen auf den jeweiligen Registerkarten ein:
    - **Gast-OS-Anmeldeinformationen**: Werden verwendet, um Pre-Freeze/Post-Thaw-Skripte auszuführen und sich bei virtuellen Maschinen zur Datenbankverarbeitung anzumelden. Wenn keine Datenbank-Anmeldeinformationen bereitgestellt werden, verwendet ActiveProtect auch die Gast-OS-Anmeldeinformationen zur Verarbeitung von Datenbanken.
    - **Datenbank-Anmeldeinformationen**: Speziell für die Authentifizierung und Verarbeitung von Datenbanken verwendet.

### Hinweis:

1. Beim Hinzufügen einer Hyper-V-VM kann das Betriebssystem aus folgenden Gründen als unbekannt aufgeführt sein:
    - Die virtuelle Maschine ist derzeit heruntergefahren.
    - Gast-Tools sind auf der Linux-VM nicht installiert.
2. Das Ausführen von Skripten auf Hyper-V-VMs erfordert sowohl die Gast-OS-Anmeldeinformationen als auch die IP-Adresse der virtuellen Maschine. Wenn die IP-Adresse fehlt, wird eine Fehlermeldung angezeigt. Wenn ein Integrationsdienst installiert ist, wird die IP-Adresse während der Skriptausführung automatisch erkannt und angewendet.

# Datenbanken sichern

ActiveProtect erleichtert die Sicherung Ihrer kritischen Datenbanken, unabhängig davon, ob sie auf physischen Servern oder virtuellen Maschinen gehostet werden. Dieser Abschnitt erklärt, wie ActiveProtect Ihre Daten schützt und führt Sie durch den Prozess der Einrichtung des Datenbankschutzes.

## Mühelose Sicherungen

ActiveProtect vereinfacht den Sicherungsprozess und stellt sicher, dass Ihre Datenbanken mit minimalem Aufwand geschützt sind:

- **Automatische Erkennung**: Erkennt automatisch physische Server oder virtuelle Maschinen, die Datenbanken und deren spezifische Versionen hosten.
- **Transaktionale Konsistenz**: Stellt sicher, dass Datenbanken in einem konsistenten Zustand gesichert werden, selbst während aktiver Transaktionen, um die Datenintegrität für eine zuverlässige Wiederherstellung zu gewährleisten.
- **Effiziente Protokollverarbeitung**: Verarbeitet Datenbankprotokolle direkt auf der Quellmaschine, wodurch manueller Aufwand und Speicherplatznutzung reduziert werden.

## Wie die Sicherung funktioniert

ActiveProtect erstellt blockbasierte Image-Sicherungen, die ganze Volumes, Maschinen und Server, einschließlich Ihrer Datenbanken, schützen. Um die Datenkonsistenz während des Prozesses sicherzustellen, verwendet ActiveProtect anwendungsbewusste Sicherungen. Diese Methode integriert sich nahtlos mit Microsoft SQL Server und Oracle Database, wie unten beschrieben.

### Microsoft SQL Server

ActiveProtect nutzt den Volume Shadow Copy Service (VSS), um unvollständige Datenbanktransaktionen zu verhindern. Hier ist eine Aufschlüsselung, wie die anwendungsbewusste Sicherung auf Windows-basierten virtuellen Maschinen mit Microsoft SQL Server funktioniert:

1. **Komponentenbereitstellung**: ActiveProtect stellt eine nicht-persistente Laufzeitkomponente auf dem Gast-OS bereit.
2. **Schnappschussinitiierung**: Die bereitgestellte Komponente fungiert als VSS-Anforderer und löst einen Schnappschuss des Gast-OS aus.
3. **Datenbankberuhigung**: Der VSS-Schreiber interagiert mit dem SQL Server und beruhigt vorübergehend die I/O-Aktivitäten, um die Datenkonsistenz sicherzustellen.
4. **Schnappschusserfassung**: ActiveProtect erstellt einen Schnappschuss der virtuellen Maschine über den Hypervisor.
5. **Aktivitätsfortsetzung**: Der VSS-Schreiber setzt die pausierten I/O-Aktivitäten auf dem SQL Server fort.
6. **Sicherungserstellung**: Der erfasste Schnappschuss wird zur Erstellung der Datenbanksicherung verwendet.

7. **Protokollkürzung (Optional)**: Wenn konfiguriert, kürzt ActiveProtect die Transaktionsprotokolle nach einer erfolgreichen Sicherung.

### Oracle Database

ActiveProtect stellt die Datenkonsistenz während der Sicherungen durch spezielle Befehle sicher.

- Für den **NOARCHIVELOG**-Modus: ActiveProtect fährt die Datenbank vorübergehend herunter, führt die Sicherung durch und startet sie neu.
- Für den **ARCHIVELOG**-Modus: So funktioniert der Sicherungsprozess auf einer virtuellen Maschine:
  1. **Komponentenbereitstellung**: ActiveProtect stellt eine nicht-persistente Laufzeitkomponente auf dem Gast-OS bereit.
  2. **Eingang in den Sicherungsmodus**: Die Datenbank wird mit dem Befehl "Alter Database Begin Backup" in den Sicherungsmodus versetzt, um die Datenkonsistenz während des Schnappschusses sicherzustellen.
  3. **Schnappschussinitiierung**: Die bereitgestellte Komponente fungiert als VSS-Anforderer und löst einen Schnappschuss des Gast-OS aus.
  4. **Schnappschusserfassung**: ActiveProtect erstellt einen Schnappschuss der virtuellen Maschine über den Hypervisor.
  5. **Austritt aus dem Sicherungsmodus**: Die Datenbank verlässt den Sicherungsmodus mit dem Befehl "Alter Database End Backup".
  6. **Sicherungserstellung**: Der erfasste Schnappschuss wird zur Erstellung der Datenbanksicherung verwendet.
  7. **Protokolllöschung (Optional)**: Wenn konfiguriert, löscht ActiveProtect die Archivprotokolle nach einer erfolgreichen Sicherung.

## In diesem Abschnitt



**Hinweis:**

- Workloads, die auf Synology NAS gesichert werden, unterstützen keine Datenbanksicherungen.

# Systemanforderungen

## Microsoft SQL Server

- Unterstützte Versionen:
  - Microsoft SQL Server 2022
  - Microsoft SQL Server 2019
  - Microsoft SQL Server 2017
- Unterstützte Betriebssysteme:
  - Windows Server 2022 Core
  - Windows Server 2019 Core
  - Windows Server 2016 Core

## Oracle Database

### Anforderungen

- Unterstützte Versionen (inkl. Oracle Database Express Edition):
  - Oracle Database 21c
  - Oracle Database 19c
  - Oracle Database 18c
- Unterstützte Betriebssysteme:
  - Windows Server 2022 Core
  - Windows Server 2019 Core
  - Windows Server 2016 Core
  - Red Hat Enterprise Linux 9.4
  - Red Hat Enterprise Linux 8.8

### Einschränkungen

- **Automatic Storage Management (ASM)** wird nicht unterstützt.
- **Oracle Real Application Clusters (RAC)** werden nicht unterstützt.
- Oracle-Server, die **Data Guard** verwenden, werden nicht unterstützt.
- Für Windows-basierte virtuelle Maschinen und physische Server werden unterschiedliche Oracle Database-Versionen auf demselben Server nicht unterstützt.
- Bei der Durchführung von Backups im **NOARCHIVELOG**-Modus wird ActiveProtect Datenbanken herunterfahren und das Schreiben von Daten vorübergehend aussetzen.

# Microsoft SQL Server hinzufügen

Dieser Artikel führt Sie durch den Prozess des Hinzufügens von Microsoft SQL Server zu ActiveProtect, um Ihre Datenbankdaten zu schützen.

## Bevor Sie beginnen

### Systemanforderungen

Stellen Sie sicher, dass sowohl Ihr Betriebssystem als auch Ihre Datenbankversionen die erforderlichen Systemanforderungen erfüllen.

### Volume Shadow Copy Service (VSS) aktivieren

ActiveProtect nutzt VSS, um vor der Sicherung Schnappschüsse Ihrer Daten zu erstellen und so Konsistenz und Genauigkeit zu gewährleisten. Befolgen Sie diese Schritte, um VSS auf dem physischen Server oder der virtuellen Maschine, auf der Ihre Datenbank läuft, zu aktivieren:

1. Drücken Sie die **Windows-Taste + R**, um das **Ausführen**-Dialogfeld zu öffnen.
2. Geben Sie "services.msc" ein und drücken Sie **Enter**, um **Dienste** zu öffnen.
3. Suchen Sie den **Volume Shadow Copy Service**.
4. Überprüfen Sie die **Status**-Spalte, um zu sehen, ob der Dienst läuft oder nicht. Wenn "Gestartet" angezeigt wird, läuft VSS. Wenn "Gestoppt" angezeigt wird, läuft es nicht.
5. (Optional) Rechtsklicken Sie und wählen Sie **Eigenschaften** für eine detaillierte Konfiguration.

## Microsoft SQL Server sichern

### Microsoft SQL Server hinzufügen

Fügen Sie den physischen Server oder die virtuelle Maschine, die den Microsoft SQL Server hostet, zu Ihrer ActiveProtect-Site hinzu:

- Anweisungen zum Hinzufügen physischer Server
- Anweisungen zum Hinzufügen virtueller Maschinen

### Datenbankverarbeitung anpassen

ActiveProtect gewährleistet die Konsistenz der Datenbankdaten, indem VSS verwendet wird, um während der Sicherungen Schnappschüsse zu erfassen. Dieser Ansatz vereinfacht die Wiederherstellung Ihrer SQL Server-Daten bei Bedarf. Um dies einzurichten, aktivieren Sie die anwendungskonsistente Sicherung und passen Sie die Datenbankverarbeitung im zugewiesenen Schutzplan Ihrer Workload an.

## Anmeldeinformationen angeben

Um sich während der Sicherungen zu authentifizieren, geben Sie Datenbank- und Gast-OS-Anmeldeinformationen von einem Konto mit ausreichenden Berechtigungen an:

- Standardanmeldeinformationen: Legen Sie diese im Schutzplan fest, um sie auf alle zugehörigen virtuellen Maschinen oder physischen Server anzuwenden.
- Workload-spezifische Anmeldeinformationen:
  1. Navigieren Sie zu **Maschinen** > **Physische Server** oder **Virtuelle Maschinen**.
  2. Wählen Sie den Ziel-Server oder die virtuelle Maschine aus.
  3. Klicken Sie auf **Mehr** > **Anmeldeinformationen angeben**. Diese Anmeldeinformationen überschreiben die Standardanmeldeinformationen.

# Oracle Database hinzufügen

Dieser Artikel führt Sie durch den Prozess des Hinzufügens von Oracle Database zu ActiveProtect, um Ihre Datenbankdaten zu schützen.

## Bevor Sie beginnen

Stellen Sie sicher, dass sowohl Ihr Betriebssystem als auch Ihre Datenbankversionen die erforderlichen Systemanforderungen erfüllen.

## Oracle Database sichern

### Oracle Database hinzufügen

Fügen Sie den physischen Server oder die virtuelle Maschine, die die Oracle Database hostet, zu Ihrer ActiveProtect-Site hinzu:

- Anweisungen zum Hinzufügen physischer Server
- Anweisungen zum Hinzufügen virtueller Maschinen

### Datenbankverarbeitung anpassen

ActiveProtect stellt die Konsistenz der Datenbankdaten sicher, indem spezielle Mechanismen verwendet werden, um während der Sicherungen Schnappschüsse zu erfassen. Dieser Ansatz vereinfacht die Wiederherstellung Ihrer Oracle Database-Daten bei Bedarf. Um dies einzurichten, aktivieren Sie die anwendungskonsistente Sicherung und passen Sie die Datenbankverarbeitung im zugewiesenen Schutzplan Ihrer Workload an.

### Anmeldeinformationen festlegen

Um sich während der Sicherungen zu authentifizieren, geben Sie Datenbank- und Gast-OS-Anmeldeinformationen von einem Konto mit ausreichenden Berechtigungen an:

- Standardanmeldeinformationen: Legen Sie diese im Schutzplan fest, um sie auf alle zugehörigen virtuellen Maschinen oder physischen Server anzuwenden.
- Workload-spezifische Anmeldeinformationen:
  1. Navigieren Sie zu **Maschinen** > **Physische Server** oder **Virtuelle Maschinen**.
  2. Wählen Sie den Ziel-Server oder die virtuelle Maschine aus.
  3. Klicken Sie auf **Mehr** > **Anmeldeinformationen festlegen**. Diese Anmeldeinformationen überschreiben die Standardanmeldeinformationen.

# Ein Konto mit ausreichenden Berechtigungen vorbereiten

ActiveProtect verwendet hauptsächlich die Datenbankauthentifizierung, um Datenbanken zu verarbeiten. Wenn dies fehlschlägt, wechselt es zur Betriebssystemauthentifizierung mit:

- **Virtuelle Maschinen**: Gast-Betriebssystemkonto[1]
- **Physische Server**: Administratorkonto
  - Windows: system
  - Linux: root

Dieser Artikel beschreibt die erforderlichen Berechtigungen für sowohl die Datenbank- als auch die Betriebssystemauthentifizierung.

## Datenbankauthentifizierung

### Microsoft SQL Server

- Verwenden Sie ein **Systemadministrator**-Konto mit der **sysadmin**-Rolle.

### Oracle Database

- Verwenden Sie ein Konto mit **SYSDBA**-Berechtigungen.

## Betriebssystemauthentifizierung

### Microsoft SQL Server

- **Gast-Betriebssystemkonto**: Muss Mitglied der Gruppe **Lokale Administratoren** sein.
- **Administratorkonto und Gast-Betriebssystemkonto**: Müssen die **sysadmin**-Rolle haben.

### Oracle Database

- Gast-Betriebssystemkonto:
  - **Windows**: Muss Mitglied der Gruppe **Lokale Administratoren** sein.
  - **Linux**: Muss Mitglied der Gruppe **oinstall** sein oder als **sudoer** konfiguriert sein.
- Administratorkonto oder Gast-Betriebssystemkonto:
  - Betriebssystemauthentifizierung ist aktiviert.
  - Das Konto ist Mitglied der Gruppe **oinstall**.

**Um die Betriebssystemauthentifizierung zu aktivieren:**

1. Verwenden Sie die Eingabeaufforderung, um die Datei zu finden:

   ```
   $ORACLE_HOME/network/admin/sqlnet.ora
   ```

2. Überprüfen Sie, ob die Zeile "SQLNET.AUTHENTICATION_SERVICES= (NONE)" vorhanden ist. Wenn ja, ist die Betriebssystemauthentifizierung deaktiviert.
3. Um die Betriebssystemauthentifizierung zu aktivieren, entfernen Sie die gesamte Zeile "SQLNET.AUTHENTICATION_SERVICES= (NONE)" aus der Datei.

**Hinweis:**

1. Gast-Betriebssystemanmeldeinformationen sind erforderlich, um sich bei der virtuellen Maschine anzumelden, während Datenbankanmeldeinformationen für den Zugriff auf die Datenbank und deren Verarbeitung unerlässlich sind. Um Datenbanken auf virtuellen Maschinen zu verarbeiten, stellen Sie sicher, dass beide Anmeldeinformationen die erforderlichen Berechtigungen haben.

# Dateiserver sichern

ActiveProtect nutzt den SMB-Dienst und VSS, um zuverlässige Backups Ihrer Dateiserver-Daten zu erstellen:

- **Server Message Block (SMB)**: Ein Netzwerkkommunikationsprotokoll, das den Zugriff auf Dateien, Verzeichnisse und andere Netzwerkressourcen ermöglicht. Es erlaubt ActiveProtect, mit Ihren Dateiservern zu kommunizieren.
- **Volume Shadow Copy Service (VSS)**: Eine Microsoft-Technologie, die Schattenkopien von Datenträgern als zeitpunktbezogene Backups erstellt. Sie erfasst den Zustand Ihrer Dateien zu einem bestimmten Zeitpunkt, um die Datenintegrität während des Backup-Prozesses zu gewährleisten.

## In diesem Abschnitt

# Systemanforderungen

ActiveProtect unterstützt mehrere Arten von Dateiservern, die jeweils spezifische Anforderungen für die Durchführung von Backups und Wiederherstellungen haben. Nachfolgend sind die Details für jeden unterstützten Servertyp aufgeführt:

## SMB (Windows) Server

- Verbindungsberechtigungen des Kontos:
  - Für Backups benötigt das Konto mindestens Leseberechtigungen.
  - Für Backups und Wiederherstellungen sind Lese-/Schreibberechtigungen erforderlich.
- VSS für SMB: Um den Volume Shadow Copy Service (VSS) für SMB-Backups zu verwenden, wird ein Domänenkonto mit Administrator- oder Backup-Operator-Berechtigungen benötigt.

## NetApp Server

- Unterstützte Version: NetApp ONTAP 9.11
- SMB-Dienst: Für Konfigurationsdetails siehe SMB-Freigabe von NetApp erstellen.
- Verbindungsberechtigungen des Kontos:
  - Für Backups benötigt das Konto mindestens Leseberechtigungen.
  - Für Backups und Wiederherstellungen sind Lese-/Schreibberechtigungen erforderlich.

## Nutanix Server

- Unterstützte Version: Nutanix Files 3.6.5
- SMB-Dienst: Für Konfigurationsdetails siehe Freigabe (SMB) von Nutanix erstellen.
- Verbindungsberechtigungen des Kontos:
  - Für Backups benötigt das Konto mindestens Leseberechtigungen.
  - Für Backups und Wiederherstellungen sind Lese-/Schreibberechtigungen erforderlich.

## Synology NAS

- SMB-Dienst: Gehen Sie zu **Systemsteuerung** > **Dateidienste** > **SMB/AFP/NFS**, um den SMB-Dienst auf dem Synology NAS zu aktivieren.
- Verbindungsberechtigungen des Kontos:
  - Für Backups benötigt das Konto mindestens Leseberechtigungen.
  - Für Backups und Wiederherstellungen sind Lese-/Schreibberechtigungen erforderlich.

# Dateiserver hinzufügen

Dieser Artikel bietet Anweisungen zum Hinzufügen von Dateiservern für den Datenschutz.

## Bevor Sie beginnen

Stellen Sie sicher, dass Ihr Dateiserver die Systemanforderungen erfüllt und dass Sie über ein Konto mit ausreichenden Berechtigungen verfügen, um Sicherungen und Wiederherstellungen durchzuführen.

## Dateiserver hinzufügen

1. Gehen Sie zu **Maschinen** > **Dateiserver** und klicken Sie auf **Hinzufügen**.
2. Wählen Sie einen Server für die Durchführung von Sicherungen und die Speicherung von Sicherungsdaten.
3. Geben Sie die Details des Dateiservers ein und stellen Sie die Anmeldedaten eines Kontos mit mindestens Leseberechtigungen zur Verbindung mit dem Dateiserver bereit. Legen Sie das Verbindungstimeout in Sekunden fest.
4. Wählen Sie die Ordner aus, die Sie sichern möchten. Für SMB-Server wählen Sie, ob Sie den Volume Shadow Copy Service (VSS) für SMB-Dateifreigaben aktivieren möchten oder nicht.
5. Wählen Sie einen Schutzplan aus, den Sie anwenden möchten.
6. Bestätigen Sie die Zusammenfassung der Sicherung.

### VSS für SMB-Dateifreigaben

VSS für SMB-Dateifreigaben wird von Windows Server 2012 und höher unterstützt. Dieses Framework ermöglicht Volumensicherungen, selbst wenn Anwendungen aktiv Daten auf diese Volumes schreiben. Um Konflikte und Dateninkonsistenzen beim Sichern häufig zugegriffener Daten zu vermeiden, empfehlen wir dringend die Verwendung von VSS.

## Serververbindungen bearbeiten

Wenn sich der Standort oder die Anmeldedaten eines Dateiservers ändern, aktualisieren Sie die Verbindungseinstellungen, um Unterbrechungen bei der Sicherung zu vermeiden.

Um Verbindungen zu bearbeiten, wählen Sie den Dateiserver aus und klicken Sie auf **Mehr** > **Verbindungen bearbeiten**.

# Microsoft 365 sichern

Mit ActiveProtect können Sie die Microsoft 365-Daten Ihrer Organisation proaktiv schützen und sicherstellen, dass immer eine Sicherung zur Wiederherstellung verfügbar ist, wenn dies erforderlich ist.

## Wie die Sicherung funktioniert

ActiveProtect nutzt Microsoft Entra ID-Anwendungen, um während Sicherungs- und Wiederherstellungssitzungen Daten mit Ihrer Microsoft 365-Organisation auszutauschen. Wenn Sie einen Microsoft 365-Mandanten zu Ihrer ActiveProtect-Site hinzufügen, registriert das System automatisch eine neue Entra ID-Anwendung, um auf die Daten Ihrer Organisation zuzugreifen.

## Automatisierte Sicherungsstrategie

Automatische Sicherungsregeln sind entscheidend für Microsoft 365-Sicherungen. Legen Sie Regeln fest, um bestehende und neu hinzugefügte Objekte, die Ihren Kriterien entsprechen, automatisch zu schützen. Ebenso werden geschützte Konten, Websites oder Teams, die aus Ihrem Microsoft 365 entfernt werden, nicht mehr gesichert. Ihre zuvor gesicherten Daten werden gemäß dem festgelegten Archivierungsplan zur Aufbewahrung auf den zugewiesenen Sicherungsservern archiviert.

Dieser Ansatz macht Sicherungen mühelos und hält die Synchronisation mit dem ursprünglichen Microsoft 365-Mandanten aufrecht.

## In diesem Abschnitt

# Fähigkeiten und Einschränkungen

Dieser Artikel listet die Fähigkeiten und Einschränkungen von ActiveProtect für die Sicherung von Microsoft 365-Daten auf.

## Was gesichert werden kann

- Unterstützte Microsoft-Pläne: Microsoft 365 Business, Enterprise, Education und Exchange Online
- Unterstützte Objekte:

| Dienste | Objekte |
| --- | --- |
| Microsoft Exchange | • E-Mails, Anhänge und Ordnerstrukturen in den folgenden Postfächern:<br>  ◦ Benutzerpostfächer<br>  ◦ Freigegebene Postfächer<br>  ◦ Archivpostfächer<br>  ◦ Ressourcenpostfächer<br>• Kontakte<br>• Kalendereereignisse zusammen mit ihren Anhängen |
| Microsoft OneDrive | • Ordner, Unterordner und Dateien<br>• OneNote |
| Microsoft Chat | • 1-zu-1-Nachrichten |
| Microsoft 365 Gruppe | • Gruppen-E-Mails und Kalender |
| Microsoft SharePoint | • Dokumentbibliotheken und Listen auf den folgenden Websites:<br>  ◦ Zusammenarbeitswebsites<br>  ◦ Kommunikationswebsites<br>  ◦ Persönliche Websites |
| Microsoft Teams | • Beiträge in Teamkanälen |

## Was nicht gesichert werden kann

### Microsoft Exchange (E-Mail)

- Websitepostfächer, öffentliche Ordnerpostfächer und lokale Postfächer
- Zieldateien von Freigabelinks: Links zu Ordnern oder Dateien auf OneDrive for Business oder anderen unterstützten Speicherorten werden gesichert, jedoch nicht die verlinkten Dateien

- E-Mails im Ordner „**Gelöscht**“, wenn sich Kontakte oder Kalender im Ordner befinden
- Notizen

## Microsoft Exchange (Kontakte)

- Alle Kontakte außer **Ihre Kontakte** (z. B. in **Favoriten**, **Ihre Kontaktlisten**, **Gelöscht**, **Gruppen** und **Verzeichnis**)
- Daten in **Dateien**, **Nachrichten** und **LinkedIn** in den Kontaktinformationen

## Microsoft Exchange (Kalender)

- Kalenderereignisse vor **01.01.1970** oder nach **01.01.2070**
- Kalender über **Kalender hinzufügen** > **Persönliche Kalender hinzufügen** oder **Aus Verzeichnis hinzufügen**
- Kalender in **Gruppen**
- Entfernte Kalender

## Microsoft OneDrive

- Dateien und Ordner in **Für mich freigegeben**
- Ordnerverknüpfungen

## Microsoft Chat

- Chat mit sich selbst
- Inhalt im Chatraum:
  - Anhänge
  - App-Nachrichten, wie Genehmigungen, Umfragen und Lob
  - Audionachrichten
  - Loop-Nachrichten
  - Angeheftete Nachrichten
  - Besprechungsinhalte
  - Registerkarten

## Microsoft SharePoint

- Listenberechtigungen
- Nicht durchsuchbare Websites (Wie Sie eine Website durchsuchbar machen können)
- Zwei Arten von Spalten: **Nachschlagen** und **Person oder Gruppe**
- Umfrageoptionen
- Elemente der Benutzeroberfläche in einer nicht standardmäßigen Sprache, darunter Titel und Beschreibungen von Seiten, Listen und Spalten
- Einstellungen von Listen und Dokumentbibliotheken
- Website-Gruppenberechtigungen

- SharePoint-Websites auf Microsoft Loop (nicht unterstützt von der Microsoft 365 API)

## Microsoft Teams

- ID
- OdataContext
- Links, die zu einem bestimmten Team in Microsoft Teams-Clients führen
- InternelD
- Team-Bilder
- Apps
- Gäste
- Mitglieder von Standardkanälen
- Die folgenden Einstellungen in **Team verwalten**:
  - **Für mich anzeigen** und **Für Mitglieder anzeigen** in **Kanäle**
  - **Mitgliedern erlauben, benutzerdefinierte Apps hochzuladen** in **Einstellungen** > **Mitgliederberechtigungen**
  - **Tags** in **Einstellungen**

# Schützen Sie die Daten Ihrer Organisation auf Microsoft 365

Schützen Sie Ihre Exchange-Daten (E-Mails, Kontakte, Kalender), OneDrive-Dateien, 1-zu-1-Chat, SharePoint-Websites und Teams-Kanäle mit ActiveProtect. Dieser Artikel führt Sie durch die Schritte zur Einrichtung von Backups für Ihren Microsoft 365-Mandanten.

## Fügen Sie Ihre Mandanten hinzu

1. Gehen Sie zur Seite **Cloud-Anwendungen** und klicken Sie auf **Hinzufügen**.
2. Geben Sie die Microsoft 365-Region an.
3. Melden Sie sich als globaler Admin an, um Zugriffsberechtigungen zu autorisieren.
4. Bestätigen Sie die Mandanteninformationen.
5. Wählen Sie, ob Sie die Selbstbedienungswiederherstellung aktivieren möchten oder nicht. Nicht-Admin-Benutzer können auf das Wiederherstellungsportal zugreifen und ihre Exchange- oder OneDrive-Daten wiederherstellen, indem sie sich mit Benutzernamen anmelden, die ihren Microsoft 365-Konten entsprechen.[1]
6. Wählen Sie einen Archivierungsplan für Objekte, die aus dem Quell-Microsoft 365 gelöscht wurden. Dieser Plan bestimmt die Datenaufbewahrungsfrist vor der automatischen Entfernung.
7. Bestätigen Sie die Einstellungen.

## Legen Sie Ihre automatischen Sicherungsregeln fest

Richten Sie Regeln ein, die festlegen, welche Microsoft 365-Objekte gesichert werden müssen. ActiveProtect wird dann automatisch bestehende und neu hinzugefügte Objekte basierend auf diesen Kriterien identifizieren und schützen, um eine nahtlose Datensicherung zu gewährleisten.

Um Ihre automatischen Sicherungsregeln zu konfigurieren, geben Sie den Zielmandanten ein und klicken Sie auf **Aktionen** > **Einstellungen für automatische Sicherung**:

### Um Regeln für Kollaborationsdienste festzulegen:

1. Wählen Sie die Dienste aus, die Sie sichern möchten:
   - **Microsoft 365-Gruppen**: Sichert Gruppenmails und Kalender.
   - **SharePoint-Websites**: Sichert Dokumentbibliotheken und Listen auf Team- und Kommunikationswebsites.
   - **SharePoint-Persönliche Websites**: Sichert Dokumentbibliotheken und Listen auf persönlichen Websites.
   - **Teams**: Sichert Teamkanäle und Beiträge.
2. Weisen Sie jedem aktivierten Typ einen Schutzplan und einen Sicherungsserver zu.

**Um Regeln für Benutzerdienste festzulegen:**

1. Klicken Sie auf **Hinzufügen**.
2. Wählen Sie einen Server für die Durchführung von Backups und die Speicherung von Sicherungsdaten.
3. Wählen Sie die Microsoft 365-Gruppen, deren Mitglieder individuell **Exchange**, **OneDrive** oder **Chat** gesichert werden sollen.[2]
4. Wählen Sie einen anzuwendenden Schutzplan aus.
5. Speichern Sie die Regel.

Bestehende und zukünftige Microsoft 365-Konten mit Lizenzen in den ausgewählten Gruppen werden automatisch gesichert. Sie können wählen, ob Sie unlizensierte Konten in die Sicherung einbeziehen möchten, indem Sie auf **Geschützter Kontotyp** klicken.

## Automatische Sicherungsregeln bearbeiten

Wenn Sie die Einstellungen für die automatische Sicherung ändern müssen, beachten Sie, dass Änderungen an Schutzplänen und Sicherungsservern nur neu hinzugefügte Workloads betreffen. Bestehende Workloads werden weiterhin durch die Pläne und Server gesichert, die ihnen bei der Hinzufügung über die automatische Sicherungsregel zugewiesen wurden.

Bei Bedarf können Sie die Schutzpläne für diese Workloads anpassen, indem Sie auf **Mehr** > **Plan ändern** klicken.

## Individuelle Workloads hinzufügen

Wenn Sie bestimmte Objekte sichern möchten, können Sie diese manuell mit den folgenden Schritten hinzufügen:

1. Geben Sie den Ziel-Mandanten ein.
2. Klicken Sie auf **Aktionen** > **Individuelle Workloads hinzufügen**.
3. Wählen Sie einen Server für die Durchführung von Backups und die Speicherung von Sicherungsdaten.
4. Wählen Sie die Objekte aus, die gesichert werden sollen. Wenn Sie gerade ein Objekt in Microsoft 365 hinzugefügt haben, klicken Sie unten rechts auf das **Aktualisieren**-Symbol, um die Liste zu aktualisieren.
5. Wählen Sie einen Schutzplan aus, der angewendet werden soll.
6. Bestätigen Sie die Sicherungszusammenfassung.

## Mandanteneinstellungen bearbeiten

Geben Sie den Ziel-Mandanten ein und klicken Sie auf **Aktionen** > **Mandanten bearbeiten**. Sie können hier Folgendes tun:

- Benennen Sie den Mandanten auf ActiveProtect um.
- Starten Sie die erneute Authentifizierung, wenn die für Backups verwendete Microsoft Entra ID-Anwendung widerrufen oder geändert wurde.

- Aktivieren oder deaktivieren Sie die Selbstbedienungs-Wiederherstellung.
- Ändern Sie den Archivierungsplan für Objekte, die aus der Quelle Microsoft 365 gelöscht wurden.

**Hinweis:**

1. Wenn Sie eine große Anzahl von Benutzern haben, die eine Selbstbedienungs-Wiederherstellung benötigen, sollten Sie in Betracht ziehen, Ihr ActiveProtect-Gerät mit Microsoft Entra Domain Services zu verbinden. Dies ermöglicht es Mandantenbenutzern, das Wiederherstellungsportal mit ihren Microsoft 365-Anmeldeinformationen zu nutzen.
2. Wenn ein Benutzer mehreren Gruppen angehört, wird ActiveProtect ihn der ersten Gruppe hinzufügen, die es erkennt, basierend auf der alphabetischen Reihenfolge. Zum Beispiel, wenn ein Benutzer sowohl zu Gruppe A als auch zu Gruppe B gehört, wird seine Sicherung den Regeln von Gruppe A folgen. Wenn dies nicht Ihrer gewünschten Konfiguration entspricht, können Sie den Plan später anpassen oder die Arbeitslast mit Ihren bevorzugten Einstellungen erneut hinzufügen.
3. Beim Hinzufügen einer neuen Arbeitslast wird das System zunächst initialisiert, was einige Zeit in Anspruch nehmen kann. Diese Verzögerung tritt nur während der anfänglichen Einrichtung auf und hat keinen Einfluss auf zukünftige Sicherungsoperationen oder die Systemleistung.

# Microsoft 365-Drosselung

Drosselung ist ein Prozess, der hilft, die Servergesundheit und Reaktionsfähigkeit zu erhalten, indem er den übermäßigen Ressourcenverbrauch aktiv kontrolliert. Er begrenzt die Anzahl gleichzeitiger Anfragen an einen Dienst, verhindert die Übernutzung von Ressourcen und gewährleistet eine zuverlässige Leistung.

## Wie die Drosselung funktioniert

### Exchange Online

Die Drosselung in Exchange Online hilft, die Zuverlässigkeit und Verfügbarkeit des Servers zu gewährleisten, indem sie die Menge an Serverressourcen begrenzt, die ein einzelner Benutzer oder eine Anwendung verbrauchen kann. Exchange Online-Ressourcen, wie Postfächer und andere verwandte Objekte, werden ständig überwacht, und die Exchange Web Services (EWS)-Budgets, die jedem Mandanten oder jeder Organisation zugewiesen sind, ändern sich entsprechend.

Wenn hohe Lastfaktoren erkannt werden, werden EWS-Verbindungen proportional eingeschränkt, und die Serverleistung verschlechtert sich infolgedessen. Selbst wenn ein Benutzer innerhalb seines Drosselungslimits liegt, kann es zu Verlangsamungen kommen, bis die Gesundheit der Ressource wieder auf betriebliche Niveaus zurückkehrt.

### SharePoint, OneDrive for Business und Teams

Wie bei Exchange Online wird die Drosselung auch bei SharePoint, OneDrive for Business und Teams eingesetzt, um die optimale Leistung und Zuverlässigkeit ihrer jeweiligen Dienste zu gewährleisten. Bei diesen drei Diensten verwendet die Drosselung Microsoft Graph APIs, um die Anzahl der Benutzeraktionen und gleichzeitigen Anrufe zu begrenzen und die Übernutzung gemeinsamer Ressourcen zu verhindern. Dies garantiert eine stabilere und vorhersehbarere Leistung, wenn mehrere Mandanten diese Dienste gleichzeitig nutzen.

## Wie man die Drosselung lindert

Die Drosselung kann die Sicherungs- und Wiederherstellungsprozesse von Microsoft 365 in ActiveProtect verlangsamen, indem sie die Anzahl gleichzeitiger Anfragen begrenzt. Jeder Microsoft 365-Dienst kann auf Drosselungsprobleme stoßen. Da die Sicherungs- und Wiederherstellungsgeschwindigkeiten manchmal von der aktiven Microsoft 365-Drosselungsrichtlinie beeinflusst werden, kann die Anpassung der Konfigurationen in unserer Sicherungssoftware das Problem möglicherweise nicht vollständig lösen.

Wenn Sie beim Sichern oder Wiederherstellen großer Datenmengen auf Drosselung stoßen, können Sie die EWS-Drosselung vorübergehend deaktivieren in Exchange Online.

# Geschützte Workloads verwalten

Dieser Artikel führt Sie durch verschiedene Vorgänge zur Verwaltung geschützter Workloads.

## Sicherungen manuell auslösen oder abbrechen

### Manuelle Sicherungen initiieren

Wenn wesentliche Änderungen in Ihren Quelldaten auftreten, initiieren Sie manuell Sicherungen, um die aktualisierten Informationen sofort zu sichern.

Wählen Sie die Ziel-Workloads aus und klicken Sie auf **Sicherung**.

### Sicherungen abbrechen

Um eine laufende Sicherung zu stoppen, wählen Sie die Ziel-Workloads aus und klicken Sie auf (**Mehr**) > **Sicherung abbrechen** in den folgenden Situationen:

- Um Bandbreite und Ressourcen für andere kritische Aufgaben freizugeben.
- Um Sicherungen zu stoppen, die unbeabsichtigt gestartet wurden.

### Sicherungsüberprüfung abbrechen

Um eine laufende Sicherungsüberprüfung zu stoppen, navigieren Sie zu **Sicherungsaktivitäten** > **Laufende Aktivitäten** und wählen Sie die Ziel-Workloads aus, die Sie abbrechen möchten.

## Sicherungseinstellungen anpassen

Ändern Sie den Schutzplan oder den Sicherungsserver, der einem Workload zugewiesen ist, wenn die anfänglichen Einstellungen nicht mehr Ihren sich entwickelnden Anforderungen oder Szenarien entsprechen.

### Schutzpläne ändern

Um einen neuen Plan zuzuweisen, wählen Sie die Ziel-Workloads aus und klicken Sie auf **Mehr** > **Plan ändern**.

Für Workloads, die derzeit gesichert werden, tritt der neue Plan nach Abschluss der Sicherung in Kraft. Änderungen an Sicherungszeiträumen, in denen Sicherungen erlaubt oder eingeschränkt sind, gelten jedoch sofort.

### Sicherungsserver ändern

Um Workloads einem neuen Server zuzuweisen:

1. Wählen Sie den Ziel-Workload aus und klicken Sie auf **Mehr** > **Archivieren**, um die vorherigen Sicherungsdaten zu bewahren.
2. Fügen Sie denselben Workload erneut hinzu und weisen Sie ihn dem neuen Sicherungsserver zu.

# Agent-Updates konfigurieren (PCs, Macs und physische Server)

Legen Sie Präferenzen für die Aktualisierung von Sicherungsagenten auf Ihren PCs, Macs und physischen Servern fest, um sicherzustellen, dass sie die neuesten Softwareversionen ausführen.

1. Wählen Sie die Ziel-Workloads aus und klicken Sie auf **Mehr** > **Agent-Updates konfigurieren**.
2. Wählen Sie im Popup-Fenster eine der folgenden Optionen:
   - **Automatisch das neueste Update installieren**: Das System wird alle Agenten aktualisieren, wenn eine neue Version veröffentlicht wird.[1]
   - **Mich benachrichtigen und mir die Entscheidung überlassen, ob das Update installiert werden soll**: Sie erhalten eine E-Mail-Benachrichtigung, wenn eine neue Version verfügbar ist, sodass Sie entscheiden können, ob Sie das Update für alle Agenten herunterladen möchten.

# Individuelle Workloads verwalten

Um einen bestimmten Workload zu verwalten, klicken Sie darauf und führen Sie die folgenden Aktionen auf den entsprechenden Registerkarten aus:

## Workload-Details anzeigen

Auf der Registerkarte **Allgemein** können Sie Arbeitslastinformationen, Planeinstellungen und Datengröße überprüfen.

## Sicherungsversionen verwalten

Auf der Registerkarte **Versionen** können Sie alle verfügbaren Sicherungsversionen anzeigen und:

- Protokolle für bestimmte Versionen aufrufen, um Probleme zu verfolgen und zu beheben.
- Versionen sperren, um eine Löschung durch Aufbewahrungsrichtlinien zu verhindern.
- Auf das Wiederherstellungsportal zugreifen, um gesicherte Daten zu durchsuchen oder wiederherzustellen.

## Selbstbedienungs-Wiederherstellungsberechtigungen zuweisen (nur Maschinen)

Auf der Registerkarte **Selbstbedienungsberechtigung** können Sie Domain/LDAP- oder lokale Benutzer hinzufügen, die mit einer Arbeitslast verknüpft werden sollen. Diese Benutzer können dann die gesicherten Daten der Arbeitslast über das Wiederherstellungsportal wiederherstellen.

**Hinweis:**

1. Um automatische Updates durchzuführen, stellen Sie sicher, dass die folgenden Anforderungen erfüllt sind:
   - Der Verwaltungsserver muss eine Internetverbindung haben.

- Backup-Server müssen mit dem Verwaltungsserver verbunden sein, und Agenten müssen mit ihren jeweiligen Backup-Servern verbunden sein.

# Schutz von Workloads beenden

Dieser Abschnitt bietet eine umfassende Anleitung zum Beenden der Sicherung bestimmter Workloads, einschließlich der zu befolgenden Schritte und wichtiger zu berücksichtigender Faktoren.

## In diesem Abschnitt

- Sicherungsschutz einstellen
- Archiveinstellungen verwalten

# Datensicherungsschutz beenden

Dieser Artikel führt Sie durch die Beendigung des Datensicherungsschutzes für bestimmte Workloads, einschließlich der notwendigen Schritte für verschiedene Workload-Typen.

## Workloads archivieren oder löschen

Workloads, die keinen Datensicherungsschutz mehr benötigen, können entweder archiviert oder gelöscht werden, je nachdem, ob Sie deren Sicherungsdaten behalten möchten oder nicht.

### Workloads archivieren

Wählen Sie die Ziel-Workloads aus und klicken Sie auf **Mehr** > **Archivieren**. Archivierte Workloads werden nicht mehr gesichert, aber ihre vorherigen Sicherungsdaten werden aufbewahrt und später gemäß dem zugewiesenen Archivierungsplan gelöscht.

### Workloads löschen

Wählen Sie die Ziel-Workloads aus und klicken Sie auf **Mehr** > **Löschen**. Diese Aktion entfernt dauerhaft alle zugehörigen Sicherungsdaten und Sicherungskopien.

Workloads mit gesperrten oder unveränderlichen Versionen können nicht gelöscht werden. Wenn diese Versionen nicht mehr benötigt werden, können Sie:

- Für gesperrte Versionen: Entsperren Sie die Versionen manuell, bevor Sie mit der Löschung fortfahren.
- Für unveränderliche Versionen: Archivieren Sie die Workloads und setzen Sie ein Löschdatum, das mit dem Ende der unveränderlichen Periode übereinstimmt. Die Workloads werden automatisch gelöscht, wenn die Periode abläuft.

Beachten Sie, dass beim Versuch, große Mengen von Workloads (etwa 150.000) zu löschen, der Löschvorgang verlangsamt oder abgebrochen werden kann, insbesondere bei hoher Systemlast oder Netzwerkinstabilität.

## Agenten deinstallieren

Nach dem Archivieren oder Löschen der Workloads deinstallieren Sie die Sicherungsagenten von den jeweiligen PCs, Macs oder physischen Servern.

### Auf Windows

#### Um Agenten zu deinstallieren:

1. Gehen Sie auf Ihrem Windows-Gerät zu **Systemsteuerung** > **Programme** > **Programme und Funktionen**.
2. Wählen Sie **Synology ActiveProtect Agent** oder **Synology Active Backup for Business Agent**.
3. Klicken Sie auf **Deinstallieren**.

**Um den Agenten vollständig zu entfernen:**

1. Melden Sie sich mit einem Administratorkonto an Ihrem Computer an.
2. Navigieren Sie zu folgendem Pfad:

   ```
   %ProgramData%\ActiveProtect
   ```

3. Entfernen Sie den Ordner **ActiveProtectAgent**.

### Auf Mac

**Um Agenten zu deinstallieren:**

1. Gehen Sie zu **Finder** > **Anwendungen**.
2. Wählen Sie **Synology ActiveProtect Agent**.
3. Verschieben Sie die App in den **Papierkorb** mit einer der folgenden Methoden:
   - Ziehen Sie die App in den **Papierkorb**.
   - Wählen Sie **Datei** > **In den Papierkorb verschieben** aus der Menüleiste.
   - Drücken Sie **Befehl-Löschen** auf Ihrer Tastatur.

**Um den Agenten vollständig zu entfernen:**

1. Geben Sie den folgenden Befehl ein, um Datenbankdateien zu entfernen:

   ```
   sudo rm -r /Library/Synology/ActiveProtect\ Agent
   ```

2. Öffnen Sie **Festplattendienstprogramm** und wählen Sie das **synodata**-Volume aus der Seitenleiste aus.
3. Klicken Sie auf die (−) Minus-Schaltfläche in der Symbolleiste, um das Volume zu löschen.

## Microsoft 365-Mandanten entfernen

Wenn Sie keinen Backup-Schutz mehr für einen gesamten Microsoft 365-Mandanten benötigen, können Sie den Mandanten und alle zugehörigen Backup-Daten gleichzeitig von der ActiveProtect-Website löschen.

1. Navigieren Sie zu **Cloud-Anwendungen** im linken Bereich.
2. Wählen Sie den Mandanten aus, den Sie entfernen möchten, und klicken Sie auf **Löschen**.
3. Folgen Sie den Anweisungen auf dem Bildschirm, um den Löschvorgang abzuschließen.

# Archivierungspläne verwalten

Erstellen Sie einen Archivierungsplan, um den Datenaufbewahrungszeitraum für Workloads festzulegen, die keinen Backup-Schutz mehr benötigen. Dies bewahrt Daten für potenzielle Wiederherstellungsanforderungen und verbessert die Speichereffizienz.

## Einen Archivierungsplan einrichten

1. Gehen Sie zu **Pläne** > **Archivierungspläne**.
2. Verwenden Sie den integrierten Plan, der zur Bearbeitung verfügbar ist, oder klicken Sie in der oberen rechten Ecke auf **Plan erstellen**, um einen neuen zu erstellen.
3. Geben Sie die folgenden Planeinstellungen an:
    - Geben Sie einen Plannamen und eine Beschreibung ein.
    - Geben Sie an, wann die Daten der archivierten Workloads gelöscht werden sollen. Sie haben die Möglichkeit, die neueste Version zu behalten.
4. Bestätigen Sie die Planübersicht.

## Einen Archivierungsplan anwenden

Sie können einen Archivierungsplan in den folgenden Szenarien anwenden:

- Beim Archivieren eines Workloads müssen Sie einen Archivierungsplan zuweisen, um die vorherigen Sicherungsdaten zu behalten und zu löschen.
- Wenn Sie einen Microsoft 365-Mandanten zu Ihrer ActiveProtect-Site hinzufügen, müssen Sie einen Archivierungsplan für Workloads zuweisen, die aus der Quellorganisation gelöscht wurden.

# Nicht verwaltete Workloads steuern

Nicht verwaltete Workloads stellen ein Risiko für den Datenschutz dar, da sie nicht mehr gesichert werden und keine Aufbewahrungsregeln angewendet werden. Dieser Artikel erklärt, wie Workloads unbeabsichtigt nicht verwaltet werden können und wie man sie handhabt, um die Einhaltung der Aufbewahrungsanforderungen sicherzustellen.

## Ursachen für nicht verwaltete Workloads

Ein Workload wird in zwei Situationen nicht verwaltet: wenn ein ActiveProtect-Gerät vom Standort entfernt wird oder wenn es sich im Reset-Modus 2 befindet. In diesen Fällen umgehen bestehende Kopier-Workloads und Sicherungsdaten die Verwaltung, da kein Schutzplan vorhanden ist.

## Nicht verwaltete Workloads handhaben

### Nicht verwaltete Workloads identifizieren

Wählen Sie in der Workload-Liste **Nicht verwaltet** aus dem oberen Dropdown-Menü. Wenn alle Workloads geschützt oder archiviert sind, wird diese Option nicht angezeigt.

### Wählen Sie eine Aktion

Nachdem Sie die nicht verwalteten Workloads ausgewählt haben, wählen Sie eine der folgenden Optionen aus der oberen Leiste:

- **Wiederherstellungsportal öffnen**: Stellen Sie die gesicherten Daten über das Portal wieder her oder laden Sie sie herunter.
- **Archivieren**: Wenden Sie einen Archivierungsplan auf die gesicherten Daten an. Die Daten werden automatisch gelöscht, wenn die angegebene Aufbewahrungsfrist abläuft.
- **Löschen**: Entfernen Sie die Workloads und ihre zugehörigen Daten vom ActiveProtect-Standort.

### Empfohlener Ansatz

Wenn Sie keine spezifischen Anforderungen für nicht verwaltete Workloads haben, wird dringend empfohlen, sie zu archivieren. Die Archivierung hält die Daten bei Bedarf zugänglich und gibt Speicherplatz frei, nachdem die Aufbewahrungsfrist endet. Dieser Ansatz verwaltet Daten effizient, während er sie für eine potenzielle zukünftige Nutzung bewahrt.

# Agent-Einstellungen konfigurieren

Sie können den Bandbreitenverbrauch verwalten, Sicherungsstatus überprüfen und Protokolldetails vom **ActiveProtect-Agenten** einsehen.

## Bandbreitenverbrauch begrenzen

Um sicherzustellen, dass genügend Verkehr für andere Dienste verfügbar ist, begrenzen Sie die für Sicherungen verwendete Bandbreite:

1. Klicken Sie auf das Symbol des **ActiveProtect-Agenten** in der Taskleiste.
2. Klicken Sie auf das Kontosymbol > **Einstellungen** > **Upload-Geschwindigkeitsbegrenzung**.

## Sicherungsstatus überprüfen

1. Klicken Sie auf das Symbol des **ActiveProtect-Agenten** in der Taskleiste.
2. Der neueste Sicherungsstatus wird im Popup-Menü angezeigt.

| Symbol | Status | Details |
|---|---|---|
|  | Bereit | Bereit, das Gerät zu sichern. |
|  | Vorbereitung auf die Sicherung | Vorbereitung auf die Sicherung. |
| | Sicherung läuft | Ihr Gerät wird gesichert. |
|  | Erfolgreich | Die letzte Sicherung ist abgeschlossen. |
|  | Abgebrochen | Die letzte Sicherung wurde abgebrochen. Sie können Sicherungen über den ActiveProtect Manager abbrechen. Wenn ein Gerät länger als 72 Stunden getrennt bleibt, wird die Sicherung automatisch abgebrochen. |
| | Teilweise erfolgreich | Die letzte Sicherung wurde abgeschlossen, aber einige Daten wurden nicht gesichert. Dies könnte daran liegen, dass bestimmte Festplatten nicht gesichert wurden oder der Schutzplan nicht anwendbar ist. |
|  | Fehlgeschlagen | Die letzte Sicherung konnte nicht abgeschlossen werden. Überprüfen Sie das Protokoll für weitere Informationen. |

## Protokoll anzeigen

1. Klicken Sie auf das Symbol des **ActiveProtect-Agenten** in der Taskleiste.

2. Klicken Sie auf das Kontosymbol > **Aktivitäten**, um Protokolle vergangener Ereignisse anzuzeigen.

# Datenwiederherstellung

Im Falle von Datenverlust oder -beschädigung bietet ActiveProtect verschiedene Wiederherstellungsoptionen, die für jeden Workload-Typ geeignet sind. Dieser Abschnitt bietet umfassende Anleitungen, um Ihnen zu helfen, Ihre gesicherten Daten nahtlos wiederherzustellen und die Geschäftskontinuität zu gewährleisten.

## In diesem Abschnitt

# Wiederherstellungs-Spickzettel

Die folgende Tabelle fasst die verfügbaren Wiederherstellungsoptionen für jeden Workload-Typ zusammen:

| Was wiederherzustellen ist | | Wiederherstellungsmethoden |
|---|---|---|
| Persönliche Computer | • Windows<br>• macOS | • Gesamte Maschinenwiederherstellung<br>  ◦ Windows: Wiederherstellungsmedien<br>  ◦ macOS: Wiederherstellungstool<br>• Datei- und Ordnerebene-Download |
| Physische Server | • Windows<br>• Linux | • Gesamte Maschinenwiederherstellung mit Wiederherstellungsmedien<br>• Datei- und Ordnerebene-Download<br>• Sofortige oder vollständige Wiederherstellung zu VMware vSphere, Microsoft Hyper-V und integriertem Hypervisor |
| Virtuelle Maschinen | • VMware vSphere<br>• Microsoft Hyper-V | • Datei- und Ordnerebene-Download<br>• Sofortige oder vollständige Wiederherstellung zu VMware vSphere, Microsoft Hyper-V und integriertem Hypervisor |
| Datenbanken | • Microsoft SQL Server<br>• Oracle Database | • Dateiebene-Download<br>• Datenbank- und Instanzebene-Download |
| Dateiserver | • SMB-Server<br>• NetApp-Server<br>• Nutanix-Server<br>• Synology NAS | • Dateiebene-Download |

| | | |
|---|---|---|
| Microsoft 365 | Exchange (Mail)<br>• Mail<br>• Archivierte Mail | • Datei- und Ordnerebene-Wiederherstellung<br>• Datei- und Ordnerebene-Download im PST- oder EML-Format |
| | Exchange (Kontakte) | • Dateiebene-Wiederherstellung<br>• Dateiebene-Download im CSV-Format |
| | Exchange (Kalender) | • Dateiebene-Wiederherstellung<br>• Dateiebene-Download im ICS-Format |
| | OneDrive | • Datei- und Ordnerebene-Wiederherstellung<br>• Datei- und Ordnerebene-Download |
| | Microsoft 365 Gruppe<br>• Mail<br>• Kalender | • Datei- und Ordnerebene-Wiederherstellung und -Download für Mail<br>• Dateiebene-Wiederherstellung und -Download für Kalender |
| | SharePoint<br>• Dokumentbibliotheken<br>• Listen | • Datei- und Ordnerwiederherstellung<br>• Datei- und Ordnerdownload |
| | Teams (1-zu-1-Chat & Gruppenchat) | • Datei- und Ordnerdownload im HTML-Format |
| | Teams (Kanalbeiträge) | • Datei- und Ordnerwiederherstellung<br>• Datei- und Ordnerdownload im HTML-Format |

# Navigieren Sie im Wiederherstellungsportal

Das Wiederherstellungsportal bietet eine benutzerfreundliche Oberfläche zum Durchsuchen und Wiederherstellen gesicherter Daten. Sie können bestimmten Benutzern die Berechtigung erteilen, Daten auf bestimmten Sicherungsservern wiederherzustellen, oder die Selbstbedienungswiederherstellung aktivieren, sodass Endbenutzer ihre eigenen Daten unabhängig wiederherstellen können.

## Starten Sie das Wiederherstellungsportal

### Für Administratoren

Um das Wiederherstellungsportal für jede Workload zu betreten, folgen Sie diesen Schritten:

1. Melden Sie sich bei Ihrem ActiveProtect-Gerät an.
2. Navigieren Sie im linken Fenster zum entsprechenden Bereich unter **Workloads**. Der Zugriff hängt von Ihren Berechtigungen ab:[1]
   - Administratoren können auf alle Workloads zugreifen.
   - Benutzer mit Wiederherstellungsberechtigung können auf Workloads auf bestimmten Sicherungsservern zugreifen.
3. Fahren Sie mit der Maus über die Ziel-Workload oder eine bestimmte Version und klicken Sie auf das ⋮-Symbol > **Wiederherstellungsportal öffnen**.

### Für Selbstbedienungsbenutzer

Mit den vom Administrator erteilten Selbstbedienungsberechtigungen können Sie Ihre gesicherten Daten wiederherstellen, indem Sie das Wiederherstellungsportal über eine der folgenden URLs aufrufen:

- https://die externe Adresse Ihres Servers/portal
- https://die IP-Adresse Ihres Servers/portal

Sobald Sie im Wiederherstellungsportal sind, finden Sie alle Workloads, für die Sie Selbstbedienungsberechtigungen haben. Verwenden Sie das linke Fenster, um zwischen verschiedenen Workload-Typen zu navigieren. Wenn keine Workloads angezeigt werden, wenden Sie sich an Ihren Systemadministrator, um Datenzugriffsberechtigungen zu erhalten.

## Zugriff auf Workload-Daten

### Workload-Details

Jede Workload verfügt über die folgenden Registerkarten, die ihre Wiederherstellungshistorie anzeigen:

- **Versionen**: Sie finden alle verfügbaren Wiederherstellungspunkte. Klicken Sie auf die gewünschte Version, um auf die Daten zuzugreifen.
- **Aktuelle Aufgaben**: Sie finden laufende Aufgaben sowie Aufgaben, die in den letzten 72 Stunden abgeschlossen[2] oder abgebrochen wurden. Bei Bedarf können Sie eine laufende Wiederherstellung oder einen Download abbrechen, indem Sie auf die Schaltfläche **Abbrechen** klicken oder mit der Maus darüber fahren und auf das X-Symbol klicken.

## Gesicherte Daten

Auf der rechten Seite finden Sie alle verfügbaren Wiederherstellungspunkte über die Versionslinie. Klicken Sie auf die gewünschte Version, um die Dateien oder Ordner auszuwählen, die Sie wiederherstellen möchten.

### Hinweis:

1. Wenn Sie das Wiederherstellungsportal direkt über die URL aufrufen, finden Sie nur Workloads, für die Sie Selbstbedienungsberechtigungen haben.
2. Der Status „Erfolgreich“ für eine sofortige Wiederherstellung zeigt nur an, dass der Wiederherstellungsprozess abgeschlossen ist. Es garantiert nicht, dass die virtuelle Maschine über die Hypervisor-Konsole verbunden werden kann.

# Physische Geräte wiederherstellen

Die ActiveProtect-Lösung bietet die folgenden Methoden zur Wiederherstellung Ihrer physischen Maschinen-Backups:

- **Gesamtes Gerät wiederherstellen:** Erstellen Sie ein bootfähiges ISO-Image oder ein USB-Laufwerk und starten Sie Ihre Maschine über das **ActiveProtect Wiederherstellungstool**. Sie können später Ihre gesamte Maschine (Bare-Metal-Wiederherstellung) oder ein bestimmtes Volume über Ihren Backup-Server wiederherstellen.
- **Granulare (Datei- oder Ordnerebene) Wiederherstellung:** Wählen Sie einzelne Dateien oder Ordner im **Wiederherstellungsportal** über den Verwaltungsserver aus. Sie können die Daten entweder an ihrem ursprünglichen Ort wiederherstellen oder auf eine andere Maschine oder einen anderen Ort herunterladen.

Backups physischer Maschinen können auch auf eine virtuelle Maschine über VMware vSphere, Microsoft Hyper-V oder Synology VMM mit den folgenden Methoden wiederhergestellt werden:

- Sofortige Wiederherstellung zu VMware und Hyper-V
- Vollständige Wiederherstellung zu VMware und Hyper-V
- Sofortige Wiederherstellung zum integrierten Hypervisor

## In diesem Abschnitt

# Gesamte Windows- oder Linux-Maschinen wiederherstellen

Sie können eine vollständige Maschine oder ein Volume mit Wiederherstellungsmedien in einen früheren Zustand versetzen. Der **ActiveProtect Recovery Media Creator** hilft Ihnen, Wiederherstellungsmedien für Bare-Metal- oder Volume-Level-Wiederherstellungen auf sowohl Windows- als auch Linux-Maschinen zu erstellen.

Sie können dieses Tool vom Wiederherstellungsportal oder dem Download-Zentrum (unter **Desktop-Dienstprogramme**) herunterladen.

Um Daten von Ihrem Synology NAS wiederherzustellen, lesen Sie Wiederherstellungen nach dem Beitritt zu einer ActiveProtect-Site für Details.

## Anforderungen und Einschränkungen

- Um Windows-Maschinen wiederherzustellen, müssen Sie den ActiveProtect Recovery Media Creator installieren. Die folgenden Betriebssysteme werden unterstützt:
  - Windows 11 (alle Editionen)
  - Windows 10 (alle Editionen)
  - Windows Server 2022
  - Windows Server 2019
  - Windows Server 2016
- Eine Netzwerkverbindung ist während der Wiederherstellung erforderlich.
- Wir empfehlen, alle erforderlichen Treiber zu installieren bevor Sie mit der Wiederherstellung beginnen.
- Nur einfache Volumes werden für die Wiederherstellung dynamischer Festplatten unterstützt.
- Unterstützte Medientypen:
  - USB-Laufwerke:
    - Erforderliche Kapazität: 1 GB
    - Erforderliche lokale Systemvolumenspeicherkapazität für temporäre Dateien: 2,5 GB
    - Unterstütztes Wiederherstellungsmodell: UEFI 64-Bit
  - ISO-Images:
    - Erforderliche Kapazität: 1 GB
    - Erforderliche lokale Systemvolumenspeicherkapazität für temporäre Dateien: 2,5 GB
    - Unterstütztes Wiederherstellungsmodell: Legacy/UEFI 64-Bit

**Hinweis:**

- Es gibt keine Systemanforderungen für Linux, da der ActiveProtect Recovery Media Creator als ISO-Datei verfügbar ist.

# ActiveProtect Recovery Media Creator installieren

1. Melden Sie sich bei Ihrem ActiveProtect-Gerät an.
2. Gehen Sie zu **Maschinen** > **PCs/Macs** oder **Physische Server**, um Ihre Maschine auszuwählen.
3. Klicken Sie auf **Mehr** > **Wiederherstellungsportal öffnen**.
4. Klicken Sie auf **Wiederherstellen** > **Gesamte Maschine wiederherstellen** und laden Sie den **ActiveProtect Recovery Media Creator** herunter.

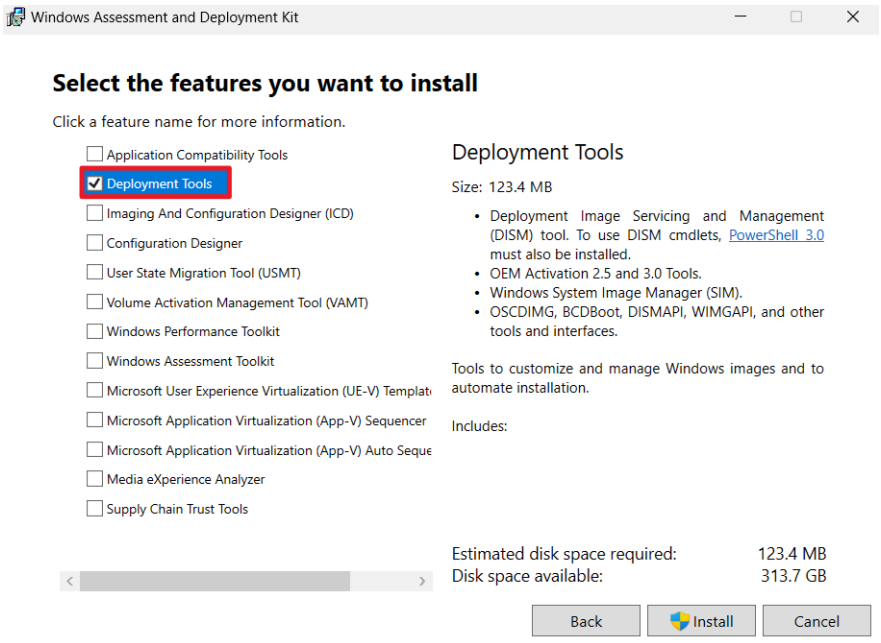
Sie können den ActiveProtect Recovery Media Creator auch aus dem Download-Zentrum (unter **Desktop-Dienstprogramme**) herunterladen. Für Linux ist es als ISO-Image mit dem Namen "**Synology-Recovery-Media.iso**" verfügbar.

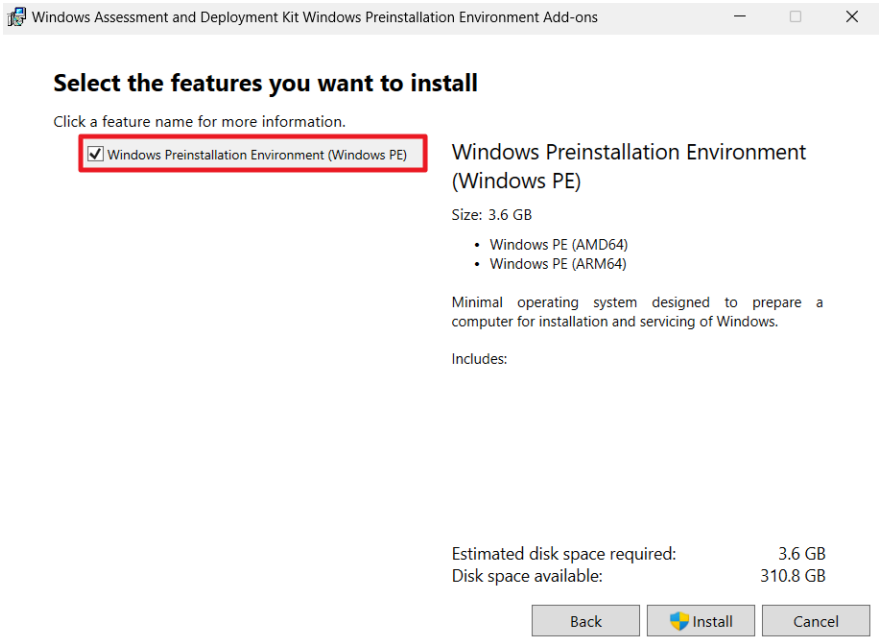
# Wiederherstellungsmedien erstellen

Mit dem ActiveProtect Recovery Media Creator können Sie ein bootfähiges USB-Laufwerk oder ein ISO-Image für die CD-Erstellung erstellen. Starten Sie von diesen Medien, um auf das eingebettete Wiederherstellungstool zuzugreifen und Ihre Maschine von Ihrem Backup-Server wiederherzustellen.

## Wiederherstellungsmedien für Windows erstellen

1. Starten Sie den **ActiveProtect Recovery Media Creator** und wählen Sie **USB-Medien** oder **ISO-Medien**:
   - Für USB-Medien stecken Sie ein USB-Laufwerk mit der erforderlichen Kapazität ein.
   - Für ISO-Medien geben Sie den Speicherort an, an dem die Wiederherstellungsmedien gespeichert werden sollen.
2. Klicken Sie auf **Erstellen**.
3. Wenn das Windows Assessment and Deployment Kit (ADK) oder die Windows Preinstallation Environment (Windows PE) nicht installiert sind, führt Sie der Medienersteller durch den Installationsprozess. Stellen Sie sicher, dass **Bereitstellungstools** und **Windows Preinstallation Environment** ausgewählt sind, um Wiederherstellungsmedien zu erstellen.






4. Wählen Sie für USB-Medien Ihr Ziel-USB-Laufwerk aus und klicken Sie auf **Erstellen**. Sobald der Prozess beginnt, kann er nicht rückgängig gemacht werden.
5. Die Wiederherstellungsmedien erkennen automatisch Ihre Zeitzonen- und Spracheinstellungen und wenden diese auf die Wiederherstellungsumgebung an. Wenn sie nicht erkannt werden können, werden Pacific Standard Time (PST) und Englisch als Standard verwendet. Dies kann beeinflussen, wie Sicherungszeiten im ActiveProtect Wiederherstellungstool angezeigt werden.
6. Nachdem die Wiederherstellungsmedien erstellt wurden, erscheint eine Nachricht in der Fortschrittsleiste.
7. Klicken Sie auf **Fertig stellen**, um das Verzeichnis zum Speichern des ISO-Images zu öffnen. Sie können das Image entweder auf die für die Wiederherstellung vorgesehene virtuelle Maschine mounten oder das Image mit einem Drittanbieter-Tool auf eine Disk brennen und die Disk in die Maschine einlegen, die Sie wiederherstellen möchten.

### Hinweis:

- Wenn Sie Windows ADK und Windows PE im Voraus herunterladen möchten, empfehlen wir, die Version **10.1.25398.1** herunterzuladen (Windows ADK/Windows PE).
- Um andere Versionen von Windows ADK und PE zu installieren, siehe Download und Installation des Windows ADK und Bootfähige Windows PE-Medien erstellen von Microsoft.
- Wenn Sie Wiederherstellungsmedien manuell erstellen, indem Sie WinPE durch WinRE ersetzen, müssen Sie eine WinRE-kompatible Version des Windows ADK herunterladen.
- Sie müssen mit dem Internet verbunden sein, wenn Sie Windows ADK herunterladen und installieren. Falls Sie den Online-ADK-Installer nicht verwenden können, siehe Windows ADK offline installieren von Microsoft.
- Wenn das Gerät, das Sie zur Erstellung von Wiederherstellungsmedien verwenden, eine 32-Bit-Version von Windows ausführt, andere Sprach- oder Regionseinstellungen hat oder andere Windows-Versionen und Treiber verwendet als das Gerät, das Sie wiederherstellen möchten, müssen Sie die Wiederherstellungsmedien manuell erstellen.

## Wiederherstellungsmedien für Linux erstellen

ActiveProtect-Wiederherstellungsmedien für Linux werden über ISO-Images bereitgestellt, die auch auf einen USB gebrannt werden können.

Bevor Sie beginnen, stellen Sie sicher, dass Sie die ISO-Datei "**Synology-Recovery-Media.iso**" heruntergeladen haben. Siehe Installation des ActiveProtect Recovery Media Creator für Anweisungen.

### Erstellen Sie ein bootfähiges USB-Laufwerk mit ISO-Brennsoftware

1. Verwenden Sie eine ISO-Brennsoftware von Drittanbietern, um "Synology-Recovery-Media.iso" auf ein USB-Laufwerk oder eine DVD zu kopieren.
2. Sie können dieses USB-Laufwerk oder die DVD verwenden, um das Gerät zu starten, das Sie wiederherstellen möchten.

### Erstellen Sie ein bootfähiges USB-Laufwerk für Legacy BIOS

1. Öffnen Sie ein Linux-Terminal und geben Sie den folgenden Befehl ein, um die Pakete und Abhängigkeiten zu installieren. Ubuntu wird als Beispiel verwendet.

   ```
   apt-get install syslinux syslinux-utils
   ```

2. Stecken Sie ein USB-Laufwerk ein.
3. Listen Sie alle Partitionen auf, um das eingesteckte USB-Laufwerk zu lokalisieren. Die Partitionen werden mit den Namen ihrer Geräte angezeigt. Zum Beispiel: "/dev/sda", "/dev/sdb" oder "/dev/sdc". Hier verwenden wir "/dev/sdc" als Beispiel.

   ```
   fdisk -l
   ```

4. Geben Sie den folgenden Befehl ein, um das USB-Laufwerk auf FAT32 zu formatieren. Ersetzen Sie "/dev/sdc" durch den tatsächlichen Namen des USB-Laufwerks.

   ```
   mkdosfs -I /dev/sdc -F 32
   ```

5. Geben Sie den folgenden Befehl ein, um "Synology-Recovery-Media.iso" auf das USB-Laufwerk zu kopieren.

   ```
   dd if=Synology-Recovery-Media.iso of=/dev/sdc bs=1M
   ```

6. Sie können dieses USB-Laufwerk verwenden, um das Gerät zu starten, das Sie wiederherstellen möchten.

### Erstellen Sie ein bootfähiges USB-Laufwerk für UEFI

1. Öffnen Sie ein Linux-Terminal und geben Sie den folgenden Befehl ein, um die heruntergeladenen Wiederherstellungsmedien zu mounten. Ubuntu wird als Beispiel verwendet.

   ```
   mkdir -p /mnt/apm
   mount -o loop Synology-Recovery-Media.iso /mnt/apm
   ```

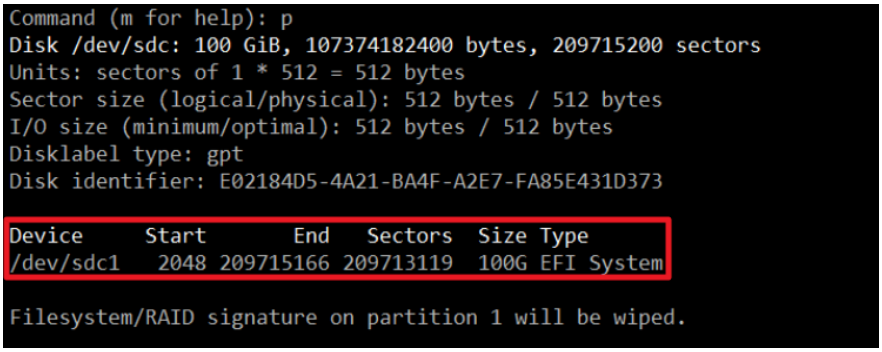
2. Stecken Sie ein USB-Laufwerk ein.
3. Listen Sie alle Partitionen auf, um das eingesteckte USB-Laufwerk zu lokalisieren. Die Partitionen werden mit den Namen ihrer Geräte angezeigt. Hier verwenden wir "/dev/sdc" als Beispiel.

```
fdisk -l
```

4. Geben Sie die folgenden Befehle ein, um das USB-Laufwerk als GPT-formatierten Datenträger einzurichten und eine EFI-Systempartition zu erstellen.

```
fdisk /dev/sdc
```

   - g: Erstellen Sie eine neue leere GPT-Partitionstabelle
   - n und 1: Erstellen Sie eine Partition mit Standardwerten
   - t und 1: Ändern Sie den Partitions-Typ in EFI-Systempartition
   - w: Änderungen speichern




5. Geben Sie den folgenden Befehl ein, um das neu erstellte Volume zu formatieren.

```
mkfs.vfat -I /dev/sdc1
```

6. Geben Sie den folgenden Befehl ein, um das Volume zu mounten.

```
mkdir -p /mnt/usb
mount /dev/sdc1 /mnt/usb
```

7. Geben Sie den folgenden Befehl ein, um "Synology-Recovery-Media.iso" auf das USB-Laufwerk zu kopieren.

```
cp -r /mnt/apm/* /mnt/usb/
```

8. Geben Sie den folgenden Befehl ein, um das USB-Laufwerk und die Wiederherstellungsmedien zu unmounten.

```
umount /mnt/usb
umount /mnt/apm
```

9. Sie können dieses USB-Laufwerk verwenden, um das Gerät zu starten, das Sie wiederherstellen möchten.

## Wiederherstellungsmedien booten

Sobald Sie erfolgreich Wiederherstellungsmedien für das wiederherzustellende Gerät erstellt haben, können Sie Ihr Wiederherstellungslaufwerk verwenden, um das Gerät davon zu booten.

1. Mounten Sie das ISO-Image oder stecken Sie ein USB-Laufwerk in das wiederherzustellende Gerät.

2. Drücken Sie **F2**, um in den BIOS-Modus zu gelangen. Beachten Sie, dass diese Taste je nach Hersteller variieren kann.
3. Gehen Sie zu **Boot** und priorisieren Sie **CD-ROM-Laufwerk** oder **Wechselmedien** je nach Standort der Wiederherstellungsmedien.
4. Verlassen Sie den Setup-Prozess und Sie werden zum **ActiveProtect Wiederherstellungstool** geleitet, um die Wiederherstellung zu starten.

# Stellen Sie Ihre Maschine wieder her

## Treiber und Netzwerkadapter laden (optional)

Im ActiveProtect Wiederherstellungstool:

1. Klicken Sie auf das ⋯ Mehr-Symbol > **Liste der Hardwaretreiber**.
2. Überprüfen Sie, ob Treiber und Netzwerkadapter installiert werden müssen.
3. Falls erforderlich, klicken Sie auf **Treiber laden**.

### Hinweis:

1. Die Wiederherstellung kann fehlschlagen, wenn der erforderliche Treiber nicht installiert ist.
2. Dies gilt nicht für Treiber, die einen Systemneustart erfordern. Weitere Informationen finden Sie unter Geräteinstallationen und Systemneustarts von Microsoft.

## Von Backup-Server wiederherstellen

Im ActiveProtect Wiederherstellungstool:

1. Geben Sie die Anmeldedaten Ihres Verwaltungsservers ein.[1]
2. Wählen Sie die Workload aus, die Sie wiederherstellen möchten. Workloads mit Selbstbedienungswiederherstellung oder delegierten Wiederherstellungsberechtigungen werden hier angezeigt.
3. Geben Sie den Wiederherstellungsmodus an.
4. Wählen Sie die Sicherungsversion[2] aus, die Sie wiederherstellen möchten.
   - Wenn die ausgewählte Version mehr Treiber erfordert, erhalten Sie eine Benachrichtigung. Um dieses Problem zu beheben, laden Sie die erforderlichen Treiber und versuchen Sie es erneut.
   - Wenn die ausgewählte Version zusätzlichen Speicherplatz erfordert, erhalten Sie eine Benachrichtigung mit einer Liste aller Laufwerke, die mehr Kapazität benötigen. Um dieses Problem zu beheben, ziehen Sie in Betracht, die installierten Laufwerke zu ersetzen.[3]
5. Bestätigen Sie die Zusammenfassung und klicken Sie auf **Weiter**.

Sobald die Wiederherstellung begonnen hat[4], ist es nicht möglich, sie zu stoppen oder auf den Zustand vor der Wiederherstellung zurückzusetzen. Eine Unterbrechung während des Prozesses kann verhindern, dass die Maschine erfolgreich startet.

**Hinweis:**

1. Wenn Single Sign-On (SSO) auf dem ActiveProtect-Gerät aktiviert ist und ein zeitbasiertes Einmalpasswort (TOTP) für die Authentifizierung erforderlich ist, kann der Wiederherstellungsprozess fehlschlagen, wenn das TOTP abläuft. In diesem Fall authentifizieren Sie sich erneut mit dem ActiveProtect-Gerät, indem Sie Ihre Anmeldedaten erneut eingeben und ein gültiges TOTP bereitstellen.
2. Die Sicherungsversion ist nur verfügbar, wenn sie mit dem ausgewählten Wiederherstellungsmodus kompatibel ist. Wenn Sie beispielsweise **System-Volume-Wiederherstellung** wählen, können Sie nur die Versionen wiederherstellen, die das Systemvolume enthalten.
3. Stellen Sie sicher, dass jedes Laufwerk in Ihrem Gerät über genügend Kapazität verfügt, um die Sicherungsgröße für die ausgewählte Version zu speichern.
4. Wenn die Internetverbindung während des Wiederherstellungsprozesses unterbrochen wird, versucht das ActiveProtect Wiederherstellungstool kontinuierlich, die Verbindung zum Server wiederherzustellen und die Wiederherstellung fortzusetzen.

# Probleme bei der Windows-Wiederherstellung beheben

## Erstellung von Wiederherstellungsmedien schlägt fehl

Wenn der Erstellungsprozess an irgendeinem Punkt fehlschlägt, wird der ActiveProtect Recovery Media Creator den aktuellen Schritt automatisch abschließen und dann **boot.wim** aushängen und löschen. Wiederherstellungsmedien, die im USB-Format erstellt wurden, können nicht zurückgesetzt werden, sobald der Erstellungsprozess begonnen hat.

Wenn die Erstellung von Wiederherstellungsmedien während des Erstellungsprozesses fehlschlägt, öffnen Sie den extrahierten Ordner mit dem Namen **Synology Restore Media Creator** und holen Sie das Protokoll mit dem Titel **restore-media.log**. Senden Sie das Protokoll dann an den technischen Support von Synology für weitere Unterstützung.

## Wiederherstellung schlägt fehl

Wenn eine Bare-Metal- oder Volume-Level-Wiederherstellung fehlgeschlagen ist, können Sie Wiederherstellungsprotokolle abrufen und sie an den technischen Support von Synology senden, um weitere Unterstützung zu erhalten.

Beachten Sie, dass "recovery.log" nur über das **ActiveProtect Wiederherstellungstool** abrufbar ist, bevor Sie Ihre Maschine neu starten oder herunterfahren.

1. Klicken Sie auf das Zahnradsymbol > **Befehlszeilenschnittstelle**.
2. Geben Sie "notepad" ein und drücken Sie **Enter**, um den Editor zu starten. Wählen Sie **Öffnen** im Editor, um den Laufwerksbuchstaben des eingesteckten USB-Laufwerks zu überprüfen.
3. Geben Sie den folgenden Befehl ein, um die Datei auf das USB-Laufwerk zu kopieren. Nach Ausführung des Befehls wird eine Bestätigungsmeldung angezeigt. Wenn der Laufwerksbuchstabe des USB-Laufwerks beispielsweise "S" ist, sollte der Befehl so aussehen:

```
copy X:\ActiveProtectRecovery\recovery.log* S:
xcopy /E /I X:\ActiveProtectRecovery\resource\command S:
```

4. Gehen Sie zu dem USB-Laufwerk, auf das Sie die Protokolldateien kopiert haben, und senden Sie sie an den technischen Support von Synology zur weiteren Fehlerbehebung.

## Wiederherstellungstool stürzt ab

Wenn das ActiveProtect-Wiederherstellungstool abstürzt, während Sie versuchen, eine Bare-Metal- oder Volume-Level-Wiederherstellung durchzuführen, finden Sie die Dump-Datei und senden Sie sie an den technischen Support von Synology für weitere Unterstützung.

1. Geben Sie "notepad" ein und drücken Sie **Enter**, um den Editor zu starten. Wählen Sie **Öffnen** im Editor, um den Laufwerksbuchstaben des eingesteckten USB-Laufwerks zu überprüfen.
2. Geben Sie den folgenden Befehl ein, um die Dump-Datei, Protokolldatei und andere Dateien auf das USB-Laufwerk zu kopieren. Nach Ausführung des Befehls wird eine Bestätigungsmeldung angezeigt. Wenn der Laufwerksbuchstabe des USB-Laufwerks beispielsweise "S" ist, sollte der Befehl so aussehen:

   ```
   copy X:\ActiveProtectRecovery\recovery.log* S:
   copy X:\recovery.dmp S:
   xcopy /E /I X:\ActiveProtectRecovery\resource\command S:
   ```

3. Gehen Sie zu dem USB-Laufwerk, auf das Sie die Dateien kopiert haben, und senden Sie sie an den technischen Support von Synology zur weiteren Fehlerbehebung.

# Gesamte Mac-Computer wiederherstellen

Um vollständige Maschinen oder Volumes in einen vorherigen Zustand zurückzusetzen, müssen Sie den **Apple Migrationsassistenten** und das **ActiveProtect Wiederherstellungstool** verwenden.

Sie können das **ActiveProtect Wiederherstellungstool** vom Wiederherstellungsportal oder dem Download-Zentrum (unter **Desktop-Dienstprogramme**) herunterladen.

Um Daten von Ihrem Synology NAS wiederherzustellen, lesen Sie Wiederherstellungen nach dem Beitritt zu einer ActiveProtect-Site für Details.

## Anforderungen und Einschränkungen

### ActiveProtect Wiederherstellungstool

- Unterstützte macOS-Versionen:
  - macOS Catalina 10.15.7
  - macOS Big Sur 11
  - macOS Monterey 12
  - macOS Ventura 13
  - macOS Sonoma 14
  - macOS Sequoia 15
- Eine Netzwerkverbindung ist während der Wiederherstellung erforderlich.

## Bevor Sie beginnen

### Festplattenvollzugriff aktivieren

Wenn Sie macOS 13 Ventura oder eine spätere Version verwenden, müssen Sie den **Festplattenvollzugriff** aktivieren, um sicherzustellen, dass das Wiederherstellungstool auf alle Daten Ihres Geräts zugreifen kann, um Wiederherstellungsoperationen durchzuführen.

1. Öffnen Sie die **Systemeinstellungen**.
2. Gehen Sie zu **Datenschutz & Sicherheit** > **Festplattenvollzugriff** und wählen Sie das **ActiveProtect Wiederherstellungstool** aus der Liste der Anwendungen. Wenn das Schloss in der unteren linken Ecke gesperrt ist, klicken Sie darauf, um das **Datenschutz**-Fenster zu entsperren.

### Kernel-Erweiterungen aktivieren

Um Ihren Mac wiederherzustellen, benötigt das Wiederherstellungstool Zugriff auf Kernel-Erweiterungen.

1. Öffnen Sie die **Systemeinstellungen**.
2. Gehen Sie zu **Datenschutz & Sicherheit** und klicken Sie auf **Systemerweiterungen aktivieren**. Wenn das Schloss unten links gesperrt ist, klicken Sie darauf, um das Einstellungsfenster zu entsperren.

3. Klicken Sie auf **Zulassen** unter **Systemsoftware von "Synology Inc." wurde am Laden gehindert**. Um mehrere Systemerweiterungen zu aktivieren, folgen Sie diesen Schritten:
    a. Gehen Sie zu **Datenschutz & Sicherheit** > **Einige Systemsoftware erfordert Ihre Aufmerksamkeit, bevor sie verwendet werden kann** und klicken Sie auf **Details**.
    b. Wählen Sie **Synology Inc. Entwickler** und klicken Sie auf **OK**.
    c. Gehen Sie zurück zu **Datenschutz & Sicherheit** und klicken Sie auf **Zulassen** unter **Systemsoftware von "Synology Inc." wurde am Laden gehindert**.
4. Starten Sie Ihren Mac neu.

### Für Macs mit Apple Silicon

Wenn Sie einen Mac mit Apple Silicon verwenden und nach der Installation die folgende Popup-Nachricht sehen, müssen Sie das System-Sicherheitsniveau ändern, um Erweiterungen zuzulassen. Sie müssen Ihren Mac während dieses Vorgangs herunterfahren, daher empfehlen wir, diesen Artikel auf Ihrem mobilen Gerät zu öffnen.

1. Klicken Sie auf das Apple-Menü > **Herunterfahren**. Halten Sie die Einschalttaste gedrückt, bis "Startoptionen werden geladen" angezeigt wird.
2. Klicken Sie auf **Optionen** > **Fortfahren**.
3. Klicken Sie in der Menüleiste auf **Dienstprogramme** > **Start-Sicherheitsdienstprogramm**.
4. Wählen Sie die Startdiskette aus, die "Macintosh HD" heißen sollte, wenn Sie ihren Namen nicht zuvor geändert haben.


5. Klicken Sie auf **Sicherheitspolitik**.
6. Wählen Sie **Reduzierte Sicherheit** und dann **Benutzerverwaltung von Kernel-Erweiterungen von identifizierten Entwicklern zulassen**.
7. Klicken Sie auf **OK** und starten Sie Ihren Mac neu.

### Hinweis:

- Bevor Sie die Wiederherstellung durchführen, aktualisieren Sie die OS-Version des Backup-Zielgeräts auf die neueste Version, damit sie mit der des Backup-Quellgeräts kompatibel ist.

- Sie müssen Apple Software Restore (ASR) verwenden, um Ihren Mac wiederherzustellen. Stellen Sie sicher, dass Sie mindestens doppelt so viel freien Speicherplatz auf Ihrem Mac haben wie die Datenmenge, die Sie wiederherstellen. Wenn Sie zusätzlichen Speicherplatz benötigen, können Sie eine APFS-formatierte externe Festplatte an Ihr Gerät anschließen. Das ActiveProtect Wiederherstellungstool wählt automatisch das Volume mit dem meisten verfügbaren Speicherplatz aus, um Ihr Backup wiederherzustellen.
- Die auf Ihrer externen Festplatte gespeicherten Daten werden nach Abschluss der Wiederherstellung nicht gelöscht.
- Wenn Sie nach der Wiederherstellung Ihres Geräts auf beschädigte Anwendungen stoßen, versuchen Sie, die Anwendungen neu zu installieren oder zu aktualisieren.

## Stellen Sie Ihren Mac über das Wiederherstellungstool wieder her

1. Öffnen Sie das Wiederherstellungstool.
2. Geben Sie die Anmeldedaten Ihres Verwaltungsservers ein.[1]
3. Wählen Sie die Arbeitslast aus, die Sie wiederherstellen möchten.
4. Wählen Sie eine Sicherungsversion aus.
5. Wählen Sie die Volumes aus, die Sie wiederherstellen möchten. Das Wiederherstellungstool ordnet automatisch Volumes vom Sicherungsquelle den verfügbaren Containern auf Ihrem Mac zu.
6. Überprüfen Sie die Wiederherstellungseinstellungen und beginnen Sie mit der Wiederherstellung.
7. Wenn Sie sich entschieden haben, das System-Volume wiederherzustellen, klicken Sie auf **Jetzt wiederherstellen**, um den Apple Migrationsassistenten zu starten. Alle Apps werden während dieses Vorgangs geschlossen, daher empfehlen wir, diesen Artikel auf Ihrem mobilen Gerät zu öffnen.

**Hinweis:**

1. Wenn Single Sign-On (SSO) auf dem ActiveProtect-Gerät aktiviert ist und ein zeitbasiertes Einmalpasswort (TOTP) für die Authentifizierung erforderlich ist, kann der Wiederherstellungsprozess fehlschlagen, wenn das TOTP abläuft. In diesem Fall authentifizieren Sie sich erneut mit dem ActiveProtect-Gerät, indem Sie Ihre Anmeldedaten erneut eingeben und ein gültiges TOTP bereitstellen.

## Stellen Sie Ihr System-Volume mit dem Apple Migrationsassistenten wieder her

1. Der Apple Migrationsassistent wird automatisch gestartet. Klicken Sie auf **Fortfahren**.
2. Wählen Sie **Von einem Mac, Time Machine-Backup oder Startvolume** und klicken Sie auf **Fortfahren**.
3. Wählen Sie das System-Volume (z.B. Macintosh HD) und klicken Sie auf **Fortfahren**.
4. Nachdem der Apple Migrationsassistent die Dateien vom Volume gescannt hat, wählen Sie die Informationen aus, die Sie wiederherstellen möchten, und klicken Sie auf **Fortfahren**.
5. Folgen Sie dem Assistenten, um die Wiederherstellungseinrichtung abzuschließen.

6. Nach Abschluss der Einrichtung beginnt der Apple Migrationsassistent mit der Wiederherstellung des System-Volumes.

# Einzelne Dateien wiederherstellen

Sie können einzelne Dateien oder Ordner von Ihrem ActiveProtect-Gerät über das Wiederherstellungsportal wiederherstellen:

1. Gehen Sie zu **Workloads** > **Maschinen** und wählen Sie die Workload aus, die Sie wiederherstellen möchten.
2. Klicken Sie auf **Wiederherstellungsportal öffnen**.
3. Finden Sie die Datei, die Sie wiederherstellen möchten.
4. Klicken Sie auf **Herunterladen**. Wählen Sie den Quellserver aus, wenn es mehr als einen gibt.
5. Sehen Sie den Fortschritt in **Letzte Aufgaben**.

**Hinweis:**

- Das Herunterladen von Dateien von einem entfernten Standort kann länger dauern.
- Die folgenden Daten können nicht über das Wiederherstellungsportal heruntergeladen oder wiederhergestellt werden:
  - Daten, die mit dem Windows Encrypting File System (EFS) verschlüsselt sind
  - Daten auf Windows Server 2019-Volumes mit aktivierter Deduplizierung

# Physische Server in virtuelle Maschinen wiederherstellen

Physische Server können als virtuelle Maschinen zu VMware vSphere, Microsoft Hyper-V und dem integrierten Hypervisor mit den folgenden Methoden wiederhergestellt werden:

- **Sofortige Wiederherstellung zu VMware und Hyper-V**: Konvertiert die Sicherungsabbilder eines physischen Servers in eine virtuelle Maschine und startet die Maschine schnell mit einer komprimierten und deduplizierten Sicherungsdatei, wodurch die Ausfallzeit der Maschine minimiert wird. Die wiederhergestellten virtuellen Maschinen haben jedoch eine eingeschränkte I/O-Leistung und erfordern eine Migration für volle Leistung und Datensynchronisation.
- **Sofortige Wiederherstellung zum integrierten Hypervisor**: Bindet das gesicherte Abbild Ihres physischen Servers auf dem integrierten Hypervisor für die Notfallwiederherstellung oder Softwaretests ein. Diese Option steht nur Administratoren oder Benutzern mit Wiederherstellungsberechtigungen zur Verfügung.
- **Vollständige Wiederherstellung zu VMware und Hyper-V**: Konvertiert die Sicherungsabbilder eines physischen Servers in eine virtuelle Maschine und stellt die gesamte Maschine aus einer Sicherungsdatei wieder her. Diese Methode erfordert zwar mehr Zeit und Ressourcen, bietet jedoch volle I/O-Leistung.

## Den Wiederherstellungsassistenten starten

**Einen einzelnen Server wiederherstellen:**

1. Gehen Sie zu **Maschinen** > **Physische Server** und wählen Sie den physischen Server aus, den Sie wiederherstellen möchten.
2. Klicken Sie im oberen Menü auf **Mehr** und wählen Sie **Wiederherstellungsportal öffnen**.
3. Wählen Sie im Wiederherstellungsportal die Zielversion aus und klicken Sie auf **Wiederherstellen** > **In virtuelle Maschine wiederherstellen**.

**Mehrere Server wiederherstellen:**

1. Gehen Sie zu **Maschinen** > **Physische Server** und wählen Sie die physischen Server aus, die Sie wiederherstellen möchten.
2. Klicken Sie im oberen Menü auf **Mehr** und wählen Sie **In virtuelle Maschine wiederherstellen**.
3. Wählen Sie die Version zur Wiederherstellung. Wählen Sie die neueste Sicherung oder grenzen Sie die Versionen nach Zeit ein.

## Sofortige Wiederherstellung zu VMware und Hyper-V

1. Wählen Sie im Wiederherstellungsassistenten **Sofortige Wiederherstellung**.
2. Wenn die Version an mehreren Orten gespeichert ist, können Sie den Ort auswählen, von dem die Daten wiederhergestellt werden sollen. Beachten Sie, dass Daten aus dem Remote-Speicher nicht sofort wiederhergestellt werden können.

3. Wählen Sie zwischen VMware[1] und Hyper-V. Klicken Sie dann auf **Weiter**, um mit den folgenden Zieleinstellungen fortzufahren:
   - Für plattformübergreifende Wiederherstellung (z.B. von VMware zu Hyper-V), konfigurieren Sie die Einstellungen der virtuellen Maschine in den nachfolgenden Schritten.
   - Für plattformgleiche Wiederherstellung (z.B. von VMware zu VMware), wählen Sie eine der folgenden Optionen:
     - **Am ursprünglichen Speicherort wiederherstellen**: Stellt die ausgewählte virtuelle Maschine am ursprünglichen Speicherort wieder her, wobei der ursprüngliche Name und die Einstellungen beibehalten werden, was die Wahrscheinlichkeit von Eingabefehlern minimiert.
     - **An einem neuen Speicherort oder mit unterschiedlichen Einstellungen wiederherstellen**: Ermöglicht es Ihnen, Ziel und Einstellungen für die wiederhergestellte virtuelle Maschine anzupassen.
4. Überprüfen Sie die Zusammenfassung der Operation. Entscheiden Sie, ob die virtuelle Maschine nach der Wiederherstellung eingeschaltet werden soll. Klicken Sie auf **Fertig**, um die Wiederherstellung zu starten.
5. Sobald die Wiederherstellung abgeschlossen ist, können Sie die wiederhergestellte virtuelle Maschine migrieren zur Produktionsumgebung für volle I/O-Leistung und Datensynchronisation.

### Einstellungen der virtuellen Maschine konfigurieren

Passen Sie die Einstellungen für die wiederhergestellte virtuelle Maschine an, einschließlich ihres Standorts und Netzwerks.

1. Geben Sie den Hypervisor an.[2] Wählen Sie aus vorhandenen Hypervisors, die zur ActiveProtect-Site hinzugefügt wurden, oder verwenden Sie einen anderen.[3]
2. Befolgen Sie die Anweisungen auf dem Bildschirm, um den Namen der virtuellen Maschine, das Betriebssystem, den Zielordner, den Host, den Ressourcenpool und den Netzwerkadapter anzugeben.

## Sofortige Wiederherstellung zum integrierten Hypervisor

1. Wählen Sie im Wiederherstellungsassistenten **Sofortige Wiederherstellung**.
2. Wenn die Version an mehreren Standorten gespeichert ist, können Sie den Standort auswählen, von dem die Daten wiederhergestellt werden sollen. Beachten Sie, dass Daten aus dem entfernten Speicher nicht sofort wiederhergestellt werden können.
3. Wählen Sie **Wiederherstellung zum integrierten Hypervisor**.
4. Folgen Sie den Anweisungen auf dem Bildschirm, um die Einstellungen der virtuellen Maschine zu konfigurieren.[4] [5] [6]
5. Klicken Sie auf **Fertig**, um die Wiederherstellung zu starten.
6. Sobald die Wiederherstellung abgeschlossen ist, wird die virtuelle Maschine automatisch eingeschaltet. Sie können dann [7] verbinden oder die wiederhergestellte virtuelle Maschine migrieren zur Produktionsumgebung für volle I/O-Leistung und Datensynchronisation.

# Vollständige Wiederherstellung zu VMware und Hyper-V

1. Wählen Sie im Wiederherstellungsassistenten **Vollständige Wiederherstellung**.
2. Wenn die Version an mehreren Standorten gespeichert ist, können Sie den Standort auswählen, von dem die Daten wiederhergestellt werden sollen.
3. Wählen Sie zwischen VMware und Hyper-V. Klicken Sie dann auf **Weiter**, um mit den folgenden Zieleinstellungen fortzufahren:
   - Für plattformübergreifende Wiederherstellung (z.B. von VMware zu Hyper-V), konfigurieren Sie die Einstellungen der virtuellen Maschine in den folgenden Schritten.
   - Für plattformgleiche Wiederherstellung (z.B. von VMware zu VMware), wählen Sie eine der folgenden Optionen:
     - **Am ursprünglichen Speicherort wiederherstellen**: Stellt die ausgewählte virtuelle Maschine am ursprünglichen Speicherort wieder her, wobei ihr ursprünglicher Name und ihre Einstellungen beibehalten werden, was die Wahrscheinlichkeit von Eingabefehlern minimiert.
     - **An einem neuen Speicherort oder mit unterschiedlichen Einstellungen wiederherstellen**: Ermöglicht es Ihnen, Ziel und Einstellungen für die wiederhergestellte virtuelle Maschine anzupassen.
4. Überprüfen Sie die Zusammenfassung der Operation. Entscheiden Sie, ob die virtuelle Maschine nach der Wiederherstellung eingeschaltet werden soll. Klicken Sie auf **Fertig**, um die Wiederherstellung zu starten.

## Einstellungen der virtuellen Maschine konfigurieren

Passen Sie die Einstellungen der wiederhergestellten virtuellen Maschine an, einschließlich ihres Standorts und Netzwerks.

1. Geben Sie den Hypervisor an. Wählen Sie aus den vorhandenen Hypervisors, die zur ActiveProtect-Site hinzugefügt wurden, oder verwenden Sie einen anderen.[3]
2. Folgen Sie den Anweisungen auf dem Bildschirm, um den Namen der virtuellen Maschine, das Betriebssystem, den Zielordner, den Host, den Ressourcenpool, das Datastore und den Netzwerkadapter anzugeben.

### Hinweis:

1. Der NFS-Dienst wird während der sofortigen Wiederherstellung zu VMware automatisch aktiviert.
2. Stellen Sie sicher, dass der Hypervisor berechtigt ist, auf das iSCSI-Target auf Ihrem Backup-Server zuzugreifen und es zu mounten. Während einer sofortigen Wiederherstellung zu Hyper-V wird ein Sicherungs-Image auf ein temporäres iSCSI-Target auf dem Backup-Server geklont. Der Hypervisor mountet dann das iSCSI-Target.
3. Nur Administratoren oder Benutzer mit Wiederherstellungsberechtigung können auf bestehende Hypervisors in der ActiveProtect-Site wiederherstellen.
4. Der integrierte Hypervisor unterstützt die VirtIO-, e1000- und rtl8139-Netzwerkschnittstellen für sofort wiederhergestellte virtuelle Maschinen. Einige Betriebssysteme virtueller Maschinen unterstützen das VirtIO-Modell nicht, was möglicherweise zu einem Fehler bei der Netzwerkerkennung führt. Um dies zu beheben, bearbeiten Sie den Netzwerkadapter der virtuellen Maschine über das Wiederherstellungsportal.

5. Der integrierte Hypervisor unterstützt die Grafikkarten cirrus, vga und vmvga für sofort wiederhergestellte virtuelle Maschinen. Wenn Sie beim Verbinden einen schwarzen Bildschirm sehen, versuchen Sie, die Wiederherstellung abzubrechen und sie erneut mit einem anderen Grafikkartentyp zu starten.
6. Der integrierte Hypervisor unterstützt keine gemounteten USB-Geräte mit ext4-Dateisystem. Wenn verbunden, werden Sie möglicherweise aufgefordert, das Gerät zu formatieren. Seien Sie vorsichtig und fahren Sie nicht mit der Formatierung fort, es sei denn, Sie beabsichtigen, die Daten zu löschen.
7. Das Verbinden mit sofort wiederhergestellten virtuellen Maschinen öffnet einen neuen Tab, der möglicherweise blockiert wird, wenn Ihr Browser Pop-ups verhindert.

# Virtuelle Maschinen wiederherstellen

ActiveProtect bietet verschiedene Methoden zur Wiederherstellung virtueller Maschinen, die jeweils für spezifische Szenarien geeignet sind:

- **Sofortige Wiederherstellung zu VMware und Hyper-V**: Stellt Sicherungsabbilder schnell auf dem Hypervisor wieder her und startet die virtuelle Maschine mit einer komprimierten und deduplizierten Sicherungsdatei. Es minimiert die Ausfallzeit, indem Ihre virtuelle Maschine innerhalb von Minuten wieder aufgenommen wird. Diese schnelle Methode kann jedoch zu einer begrenzten I/O-Leistung führen.
- **Sofortige Wiederherstellung auf den integrierten Hypervisor**: Bindet die Sicherungsabbilder Ihrer virtuellen Maschine auf dem integrierten Hypervisor für eine schnelle Notfallwiederherstellung oder Softwaretests ein. Diese Option steht nur Administratoren oder Benutzern mit Wiederherstellungsberechtigungen zur Verfügung.
- **Vollständige Wiederherstellung zu VMware und Hyper-V**: Stellt eine gesamte virtuelle Maschine vollständig aus einer Sicherungsdatei auf dem Hypervisor wieder her. Dieser Prozess erfordert zwar mehr Zeit und Ressourcen, bietet jedoch volle I/O-Leistung.

## In diesem Abschnitt

# Virtuelle Maschinen sofort zu VMware und Hyper-V wiederherstellen

Starten Sie schnell eine virtuelle Maschine mit einer komprimierten und deduplizierten Sicherungsdatei. Während sofort wiederhergestellte Maschinen die Ausfallzeit reduzieren können, haben sie möglicherweise eine begrenzte I/O-Leistung. Für optimale Leistung und vollständige Datensynchronisation migrieren Sie diese Maschinen nach der Wiederherstellung zurück in die Produktionsumgebung.

## Anwendungsszenario

Die sofortige Wiederherstellung ist ideal, wenn Sie Ihre virtuellen Maschinen innerhalb von Minuten zurückbringen müssen, um Dienstunterbrechungen zu minimieren und Leistungsschwankungen tolerieren können. Die Geschwindigkeit der sofortigen Wiederherstellung hängt von den Hardware-I/O-Fähigkeiten des zugrunde liegenden Sicherungsservers ab.

## Den Wiederherstellungsassistenten starten

**Eine einzelne Maschine wiederherstellen:**

1. Gehen Sie zu **Maschinen** > **Virtuelle Maschinen** und wählen Sie die virtuelle Maschine aus, die Sie wiederherstellen möchten.
2. Klicken Sie im oberen Menü auf **Mehr** und wählen Sie **Wiederherstellungsportal öffnen**.
3. Wählen Sie im Wiederherstellungsportal die Zielversion aus und klicken Sie auf **In virtuelle Maschine wiederherstellen**.

**Mehrere Maschinen wiederherstellen:**

1. Gehen Sie zu **Maschinen** > **Virtuelle Maschinen** und wählen Sie die virtuellen Maschinen aus, die Sie wiederherstellen möchten.
2. Klicken Sie im oberen Menü auf **Mehr** und wählen Sie **In virtuelle Maschine wiederherstellen**.
3. Wählen Sie die Version zur Wiederherstellung. Wählen Sie die neueste Sicherung oder grenzen Sie die Versionen nach Zeit ein.

## Wiederherstellungseinstellungen konfigurieren

Befolgen Sie diese Schritte im Wiederherstellungsassistenten, um die Einstellungen zu konfigurieren:

1. Wählen Sie **Sofortige Wiederherstellung**.
2. Wenn die Version an mehreren Standorten gespeichert ist, können Sie den Standort auswählen, von dem die Daten wiederhergestellt werden sollen. Beachten Sie, dass Daten aus dem entfernten Speicher nicht sofort wiederhergestellt werden können.

3. Wählen Sie zwischen VMware[1] und Hyper-V[2]. Klicken Sie dann auf **Weiter**, um mit den folgenden Zieleinstellungen fortzufahren:
   - Für plattformübergreifende Wiederherstellung (z.B. von VMware zu Hyper-V), konfigurieren Sie die Einstellungen der virtuellen Maschine in den folgenden Schritten.
   - Für gleichartige Plattformwiederherstellung (z.B. von VMware zu VMware), wählen Sie eine der folgenden Optionen:
     - **Am ursprünglichen Speicherort wiederherstellen**: Stellt die ausgewählte virtuelle Maschine am ursprünglichen Speicherort wieder her, wobei der ursprüngliche Name und die Einstellungen beibehalten werden, was die Wahrscheinlichkeit von Eingabefehlern minimiert. Diese Option hebt die Registrierung der ursprünglichen virtuellen Maschine am Produktionsstandort automatisch auf und ersetzt diese.
     - **An einem neuen Speicherort oder mit unterschiedlichen Einstellungen wiederherstellen**: Ermöglicht es Ihnen, Ziel und Einstellungen für die wiederhergestellte virtuelle Maschine anzupassen.
4. Überprüfen Sie die Zusammenfassung der Operation. Entscheiden Sie, ob die virtuelle Maschine nach der Wiederherstellung eingeschaltet werden soll. Klicken Sie auf **Fertig**, um die Wiederherstellung zu starten.
5. Sobald die Wiederherstellung abgeschlossen ist, können Sie die wiederhergestellte virtuelle Maschine migrieren in die Produktionsumgebung für volle I/O-Leistung und Datensynchronisation.

## Einstellungen der virtuellen Maschine konfigurieren

Passen Sie die Einstellungen für die wiederhergestellte virtuelle Maschine an, einschließlich ihres Standorts und Netzwerks.

1. Geben Sie den Hypervisor an.[3] Wählen Sie aus den vorhandenen Hypervisoren, die zur ActiveProtect-Site hinzugefügt wurden, oder verwenden Sie einen anderen.[4]
2. Befolgen Sie die Anweisungen auf dem Bildschirm, um den Namen der virtuellen Maschine, das Betriebssystem, den Zielordner, den Host, den Ressourcenpool und den Netzwerkadapter anzugeben.

**Hinweis:**

1. Der NFS-Dienst wird während der sofortigen Wiederherstellung zu VMware automatisch aktiviert.
2. Das System wird automatisch CPU- und Speicherkonfigurationen zuweisen, um die Wiederherstellung abzuschließen, angesichts der begrenzten Ressourcen. Sie können diese Einstellungen anschließend manuell anpassen.
3. Stellen Sie sicher, dass der Hypervisor berechtigt ist, auf das iSCSI-Target auf Ihrem Backup-Server zuzugreifen und es bereitzustellen. Während einer sofortigen Wiederherstellung zu Hyper-V wird ein Sicherungs-Image auf ein temporäres iSCSI-Target auf dem Backup-Server geklont. Der Hypervisor stellt dann das iSCSI-Target bereit.
4. Nur Administratoren oder Benutzer mit Wiederherstellungsberechtigung können auf bestehende Hypervisoren im ActiveProtect-Standort wiederherstellen.

# Virtuelle Maschinen sofort auf den integrierten Hypervisor wiederherstellen

Starten Sie schnell virtuelle Maschinen auf dem integrierten Hypervisor. Dies schafft eine sichere und isolierte Umgebung für die Validierung der Notfallwiederherstellung, das Durchsuchen von Daten und das Testen von Upgrades. Nur Administratoren oder Benutzer mit Wiederherstellungsberechtigungen können auf diese Option zugreifen.

## Anwendungsszenario

Diese Methode ist ideal, wenn eine Sandbox-Umgebung für Wiederherstellungstests oder Upgrade-Versuche benötigt wird.

## Den Wiederherstellungsassistenten starten

1. Gehen Sie zu **Maschinen** > **Virtuelle Maschinen** und wählen Sie die virtuelle Maschine aus, die Sie wiederherstellen möchten.
2. Klicken Sie auf das **Mehr**-Menü in der oberen Leiste und wählen Sie **Wiederherstellungsportal öffnen.**[1]
3. Wählen Sie im Wiederherstellungsportal die Zielversion aus und klicken Sie auf **In virtuelle Maschine wiederherstellen**.

## Wiederherstellungseinstellungen konfigurieren

Befolgen Sie diese Schritte im Wiederherstellungsassistenten, um die Einstellungen zu konfigurieren:

1. Wählen Sie **Sofortige Wiederherstellung**.
2. Wenn die Version an mehreren Orten gespeichert ist, können Sie den Ort auswählen, von dem die Daten wiederhergestellt werden sollen. Beachten Sie, dass Daten aus dem entfernten Speicher nicht sofort wiederhergestellt werden können.
3. Wählen Sie **Wiederherstellung auf den integrierten Hypervisor**.
4. Befolgen Sie die Anweisungen auf dem Bildschirm, um die Einstellungen der virtuellen Maschine zu konfigurieren.[2] [3] [4]
5. Klicken Sie auf **Fertig**, um die Wiederherstellung zu starten.
6. Sobald die Wiederherstellung abgeschlossen ist, wird die virtuelle Maschine automatisch eingeschaltet. Sie können dann [5] verbinden oder die wiederhergestellte virtuelle Maschine migrieren zur Produktionsumgebung für volle I/O-Leistung und Datensynchronisation.

**Hinweis:**

1. Die Wiederherstellung auf den integrierten Hypervisor ist nicht verfügbar, wenn Sie **In virtuelle Maschine wiederherstellen** aus dem Menü auswählen. Diese Option ist nur über das Wiederherstellungsportal

zugänglich.

2. Der integrierte Hypervisor unterstützt die virtuellen Netzwerkschnittstellen VirtIO, e1000 und rtl8139 für sofort wiederhergestellte virtuelle Maschinen. Einige Betriebssysteme virtueller Maschinen unterstützen das VirtIO-Modell nicht, was möglicherweise zu einem Fehler bei der Netzwerkerkennung führt. Um dies zu beheben, bearbeiten Sie den Netzwerkadapter der virtuellen Maschine über das Wiederherstellungsportal.
3. Der integrierte Hypervisor unterstützt die Grafikkarten cirrus, vga und vmvga für sofort wiederhergestellte virtuelle Maschinen. Wenn Sie beim Verbinden einen schwarzen Bildschirm sehen, versuchen Sie, die Wiederherstellung abzubrechen und mit einem anderen Grafikkartentyp neu zu starten.
4. Der integrierte Hypervisor unterstützt keine eingebundenen USB-Geräte mit ext4-Dateisystem. Wenn Sie verbunden sind, werden Sie möglicherweise aufgefordert, das Gerät zu formatieren. Seien Sie vorsichtig und fahren Sie nicht mit der Formatierung fort, es sei denn, Sie beabsichtigen, die Daten zu löschen.
5. Das Verbinden mit sofort wiederhergestellten virtuellen Maschinen öffnet einen neuen Tab, der möglicherweise blockiert wird, wenn Ihr Browser Pop-ups verhindert.

# Virtuelle Maschinen migrieren

Nach Abschluss einer sofortigen Wiederherstellung können Sie die wiederhergestellte virtuelle Maschine in die Produktionsumgebung migrieren. Dies gewährleistet optimale I/O-Leistung und vollständige Datensynchronisation.

## Migrationsanforderungen

Die folgende Tabelle zeigt Szenarien, die die Migration virtueller Maschinen unterstützen:

| | Migration zu VMware | Migration zu Hyper-V |
|---|---|---|
| Sofortige Wiederherstellung zu VMware | Automatische Migration[1] | Kann nicht migrieren |
| Sofortige Wiederherstellung zu Hyper-V | Kann nicht migrieren | Manuelle Migration |
| Sofortige Wiederherstellung zum integrierten Hypervisor | Automatische Migration | Automatische Migration |

## Automatische Migration durchführen

1. Starten Sie das Wiederherstellungsportal.
2. Navigieren Sie zum Abschnitt **Letzte Aufgaben**.
3. Wenn eine sofortige Wiederherstellungsaufgabe vollständig abgeschlossen ist, wird ihr Status als **Bereit zur Migration** angezeigt. Um fortzufahren, wählen Sie die Aufgabe aus und klicken Sie auf **Migrieren**.

**Hinweis:**

1. Die Migration von virtuellen Maschinen basiert auf nativen VMware vCenter-Migrationstools wie vMotion und Storage vMotion. Wenn Ihre VMware vSphere-Lizenz diese Funktionen nicht unterstützt oder Sie VMs zwischen eigenständigen ESXi-Hosts migrieren, stehen die VMware vCenter-Migrationsmethoden nicht zur Verfügung. In diesen Fällen wird die Migrationsoption deaktiviert, und Sie müssen die ESXi-virtuellen Maschinen manuell migrieren.

# Virtuelle Maschinen vollständig auf VMware und Hyper-V wiederherstellen

Im Falle eines Ausfalls der primären virtuellen Maschine stellen Sie eine vollständige virtuelle Maschine aus einer Sicherungsdatei in ihrem aktuellsten Zustand oder zu einem früheren Zeitpunkt wieder her. Diese Methode bietet volle I/O-Leistung in den wiederhergestellten virtuellen Maschinen, erfordert jedoch mehr Ressourcen und Zeit im Vergleich zu einer sofortigen Wiederherstellung.

## Anwendungsszenario

Eine vollständige Wiederherstellung wird empfohlen, wenn optimale I/O-Leistung erforderlich ist und etwas Ausfallzeit akzeptabel ist.

## Den Wiederherstellungsassistenten starten

**Um eine einzelne Maschine wiederherzustellen:**

1. Gehen Sie zu **Maschinen** > **Virtuelle Maschinen** und wählen Sie die virtuelle Maschine aus, die Sie wiederherstellen möchten.
2. Klicken Sie im oberen Menü auf **Mehr** und wählen Sie **Wiederherstellungsportal öffnen**.
3. Wählen Sie im Wiederherstellungsportal die Zielversion aus und klicken Sie auf **In virtuelle Maschine wiederherstellen**.

**Um mehrere Maschinen wiederherzustellen:**

1. Gehen Sie zu **Maschinen** > **Virtuelle Maschinen** und wählen Sie die virtuellen Maschinen aus, die Sie wiederherstellen möchten.
2. Klicken Sie im oberen Menü auf **Mehr** und wählen Sie **In virtuelle Maschine wiederherstellen**.
3. Wählen Sie die Version zur Wiederherstellung. Wählen Sie die aktuellste Sicherung oder grenzen Sie die Versionen nach Zeit ein.

## Wiederherstellungseinstellungen konfigurieren

Befolgen Sie diese Schritte im Wiederherstellungsassistenten, um die Einstellungen zu konfigurieren:

1. Wählen Sie **Vollständige Wiederherstellung**.
2. Wenn die Version an mehreren Orten gespeichert ist, können Sie den Ort auswählen, von dem die Daten wiederhergestellt werden sollen.
3. Wählen Sie zwischen VMware und Hyper-V[1]. Klicken Sie dann auf **Weiter**, um mit den folgenden Zieleinstellungen fortzufahren:

- Für plattformübergreifende Wiederherstellung (z.B. von VMware zu Hyper-V), konfigurieren Sie die Einstellungen der virtuellen Maschine in den folgenden Schritten.
- Für gleichartige Plattformwiederherstellung (z.B. von VMware zu VMware), wählen Sie eine der folgenden Optionen:
  - **Wiederherstellung am ursprünglichen Ort**: Stellt die ausgewählte virtuelle Maschine an ihrem ursprünglichen Ort wieder her, wobei ihr ursprünglicher Name und ihre Einstellungen beibehalten werden, was die Wahrscheinlichkeit von Eingabefehlern minimiert. Diese Option meldet die ursprüngliche virtuelle Maschine automatisch ab und ersetzt sie am Produktionsstandort.
  - **Wiederherstellung an einem neuen Ort oder mit unterschiedlichen Einstellungen**: Ermöglicht es Ihnen, das Ziel und die Einstellungen für die wiederhergestellte virtuelle Maschine anzupassen.

4. Überprüfen Sie die Zusammenfassung der Operation. Entscheiden Sie, ob die virtuelle Maschine nach der Wiederherstellung eingeschaltet werden soll. Klicken Sie auf **Fertig**, um die Wiederherstellung zu starten.

## Einstellungen der virtuellen Maschine konfigurieren

Passen Sie die Einstellungen für die wiederhergestellte virtuelle Maschine an, einschließlich ihres Standorts und Netzwerks.

1. Geben Sie den Hypervisor an. Wählen Sie aus den vorhandenen Hypervisoren, die zur ActiveProtect-Site hinzugefügt wurden, oder verwenden Sie einen anderen.[2]
2. Befolgen Sie die Anweisungen auf dem Bildschirm, um den Namen der virtuellen Maschine, das Betriebssystem, den Zielordner, den Host, den Ressourcenpool, das Datastore und den Netzwerkadapter anzugeben.

**Hinweis:**

1. Das System wird automatisch CPU- und Speicherkonfigurationen zuweisen, um die Wiederherstellung abzuschließen, angesichts der begrenzten Ressourcen. Sie können diese Einstellungen anschließend manuell anpassen.
2. Nur Administratoren oder Benutzer mit Wiederherstellungsberechtigung können auf bestehende Hypervisoren in der ActiveProtect-Site wiederherstellen.

# Datenbanken wiederherstellen

ActiveProtect bietet effiziente und flexible Methoden zur Wiederherstellung von Datenbanken in verschiedenen Szenarien:

- **Datenbanken wiederherstellen**: Stellt Datenspeicher wieder her, ohne andere Dienste auf der Maschine zu unterbrechen. Sie können eine Datenbank problemlos auf einen bestimmten Zeitpunkt zurücksetzen.
- **Wiederherstellung auf virtuelle Maschine**: Stellt eine Datenbank, einschließlich ihrer Daten und Konfigurationseinstellungen, auf einer virtuellen Maschine wieder her. Sobald die virtuelle Maschine läuft, können Sie schnell spezifische Daten oder Tabellen lokalisieren und exportieren.

## In diesem Abschnitt

# Microsoft SQL Server wiederherstellen

Dieser Artikel führt Sie durch die Wiederherstellung von Sicherungen Ihres Microsoft SQL Servers. Wählen Sie die Wiederherstellungsmethode, die am besten zu Ihren Bedürfnissen passt.

## Eine gesamte Datenbank wiederherstellen

Sie können eine gesamte Microsoft SQL-Datenbank einfach zu jedem Wiederherstellungspunkt mit .mdf- und .ldf-Dateien wiederherstellen. Diese Methode ermöglicht es Ihnen, die Datenbank auf einem anderen Server wiederherzustellen, was nützlich ist für die Entwicklung von SQL Server-Anwendungen oder die Analyse von Datenbanken mit Drittanbieter-Tools.

1. Navigieren Sie zu **Maschinen** > **Virtuelle Maschinen** oder **Physische Server** und wählen Sie die Maschine aus, die Sie wiederherstellen möchten.
2. Klicken Sie im oberen Menü auf **Mehr** und wählen Sie **Wiederherstellungsportal öffnen**.
3. Im Wiederherstellungsportal klicken Sie auf die Zielversion, um auf die Daten zuzugreifen.
4. Wählen Sie auf der Registerkarte **Datenbanken** im Dropdown-Menü in der oberen linken Ecke **Microsoft SQL Server** aus.
5. Wählen Sie die Datenbank, die Sie wiederherstellen möchten, aus dem linken Bereich aus. Klicken Sie auf **Alle herunterladen**, um die .mdf- und .ldf-Dateien zu erhalten.[1]
6. Verschieben Sie die heruntergeladenen Dateien zur Wiederherstellung auf die Zielmaschine.
7. Führen Sie im **Eingabeaufforderung** den folgenden Befehl als Administrator für die .mdf- und .ldf-Dateien aus. Ersetzen Sie File_Path durch Ihre tatsächlichen Dateipfade:

   ```
   icacls File_Path /grant MSSQLSERVER:(F)
   ```

8. Geben Sie den folgenden Befehl ein, um die SQL-Abfrageeingabeschnittstelle zu öffnen und eine Verbindung zum SQL Server herzustellen:

   ```
   sqlcmd -S localhost
   ```

9. Um die Microsoft SQL-Datenbank wiederherzustellen, geben Sie den folgenden Befehl ein. Ersetzen Sie [Database_Name] durch den Namen Ihrer Datenbank und Disk:\Path\File_Name.mdf und Disk:\Path\File_Name.ldf durch Ihre tatsächlichen Dateipfade:

   ```
   USE [master]
   GO
   CREATE DATABASE [Database_Name] ON
   ( FILENAME = N'Disk:\Path\File_Name.mdf' ),
   ( FILENAME = N'Disk:\Path\File_Name.ldf' )
   FOR ATTACH
   GO
   ```

# Wiederherstellung auf virtuelle Maschine

Wenn Sie schnell bestimmte Tabellen oder kritische Daten aus Ihren Microsoft SQL Server-Sicherungen wiederherstellen müssen, ist die sofortige Wiederherstellung auf VMware/Hyper-V oder den integrierten Hypervisor eine ideale Lösung. Diese Funktion führt ein Sicherungsabbild als virtuelle Maschine aus, sodass Sie einfach auf die benötigten Daten oder Tabellen zugreifen und diese exportieren können.

### Hinweis:

1. Beim Wiederherstellen von Datenbanken auf einem physischen Server können Sie auf mehrere ZIP-Dateien stoßen, wenn sich die Datenbankdateien auf verschiedenen Volumes befinden. Um erfolgreiche Downloads sicherzustellen, erlauben Sie Pop-up-Fenster in Ihrem Browser.

# Oracle Database wiederherstellen

Dieser Artikel führt Sie durch die Wiederherstellung Ihrer Oracle Database-Sicherungen. Wählen Sie die Wiederherstellungsmethode, die am besten zu Ihren Bedürfnissen passt.

## Eine gesamte Datenbank wiederherstellen

Sie können eine gesamte Oracle Database zu einem bestimmten Zeitpunkt auf dem ursprünglichen Server mithilfe gesicherter Dateien wiederherstellen.

1. Navigieren Sie zu **Maschinen** > **Virtuelle Maschinen** oder **Physische Server** und wählen Sie die Maschine aus, die Sie wiederherstellen möchten.
2. Klicken Sie im oberen Menü auf **Mehr** und wählen Sie **Wiederherstellungsportal öffnen**.
3. Klicken Sie im Wiederherstellungsportal auf die Zielversion, um auf die Daten zuzugreifen.
4. Wählen Sie auf der Registerkarte **Datenbanken** im Menü in der oberen linken Ecke **Oracle Database** aus.
5. Wählen Sie die Instanz, die Sie wiederherstellen möchten, aus dem linken Bereich aus. Klicken Sie auf **Alle herunterladen**, um die Datenbankdateien zu erhalten.
6. Starten Sie SQL*Plus und verbinden Sie sich mit der Datenbank mit SYSDBA-Berechtigung. Geben Sie den folgenden Befehl ein, wobei Sie {db_identifier} durch den **System Identifier** der Datenbank ersetzen:

   ```
   set ORACLE_SID={db_identifier}
   SQLPLUS / AS SYSDBA
   ```

7. Fahren Sie die Datenbank herunter:

   ```
   SHUTDOWN IMMEDIATE;
   ```

8. Öffnen Sie die Datenbank im NOMOUNT-Modus:

   ```
   startup nomount;
   ```

9. Verwenden Sie einen Texteditor und suchen Sie die Datei **SPFILE{db_name}.ora** im Ordner **$ORACLE_HOME/database** des Backups (z.B. SPFILERDBINSTANCE.ORA). Diese Datei enthält Informationen zum Pfad der Steuerdatei. Kopieren Sie diese Dateien vom Backup auf Ihren Rechner.
10. Verschieben Sie die Steuerdateien an den entsprechenden Ort:
    - Überprüfen Sie den aktuellen Speicherort mit diesem Befehl:

      ```
      SELECT value FROM v$parameter WHERE name = 'control_files';
      ```

    - Um das Überschreiben der Originaldaten zu vermeiden, ändern Sie den Dateispeicherort mit diesem Befehl:

      ```
      ALTER SYSTEM SET CONTROL_FILES='{first_path}', -
      '{second_path}', -
      ...
      '{nth_path}', -
      ```

```
...
'{last_path}' SCOPE=SPFILE;
```

Beispiel:

```
ALTER SYSTEM SET CONTROL_FILES=
'G:\HAMMER2\CONTROLFILE\O1_MF_L0OSN515_.CTL', -
'G:\FAST_RECOVERY_AREA\HAMMER2\CONTROLFILE\O1_MF_L0OSN51O_.CTL'
SCOPE=SPFILE;
```

11. Datenbank mounten:

```
ALTER DATABASE MOUNT;
```

12. Überprüfen Sie, welche Daten- und Logdateien wiederhergestellt werden müssen:

```
SELECT Name FROM v$datafile;
SELECT Member FROM v$logfile;
```

Beispiel:

```
NAME
--------------------------------------------------------------------------------
G:\HAMMER2\DATAFILE\O1_MF_SYSTEM_L0OSFKM0_.DBF
G:\HAMMER2\DATAFILE\O1_MF_SYSAUX_L0OSGBVW_.DBF
G:\HAMMER2\DATAFILE\O1_MF_UNDOTBS1_L0OSGT4Z_.DBF
G:\BIGFILE
G:\HAMMER2\DATAFILE\O1_MF_USERS_L0OSGVDF_.DBF
MEMBER
--------------------------------------------------------------------------------
G:\HAMMER2\ONLINELOG\O1_MF_3_L0OSNBC0_.LOG
G:\FAST_RECOVERY_AREA\HAMMER2\ONLINELOG\O1_MF_3_L0OSNFRO_.LOG
G:\HAMMER2\ONLINELOG\O1_MF_2_L0OSNB9K_.LOG
G:\FAST_RECOVERY_AREA\HAMMER2\ONLINELOG\O1_MF_2_L0OSNF6M_.LOG
G:\HAMMER2\ONLINELOG\O1_MF_1_L0OSNB9K_.LOG
G:\FAST_RECOVERY_AREA\HAMMER2\ONLINELOG\O1_MF_1_L0OSNF45_.LOG
```

13. Platzieren Sie die gesicherten Daten- und Logdateien an den entsprechenden Orten. Falls erforderlich, ändern Sie ihre Dateipfade in der Datenbank:

```
ALTER DATABASE RENAME FILE ''
TO '';
```

Beispiel:

```
ALTER DATABASE RENAME FILE 'G:\HAMMER2\DATAFILE\O1_MF_SYSTEM_L0OSFKM0_.DBF'
TO 'C:\User\Desktop\Oracle\O1_MF_SYSTEM_L0OSFKM0_.DBF';
```

14. Ändern Sie die Dateiberechtigungen, falls sie falsch sind. Geben Sie den folgenden Befehl ein und ersetzen Sie "ORA_OraDB19Home1_SVCACCTS:(F)" durch Ihren Oracle-Gruppennamen:

```
icacls "{new_path_file}" /grant ORA_OraDB19Home1_SVCACCTS:(F)
```

15. Stellen Sie die Datenbank aus dem Sicherungsmodus wieder her:

```
RECOVER DATABASE;
```

16. Schließlich schalten Sie die Datenbank in den offenen Modus:

```
ALTER DATABASE OPEN;
```

# Wiederherstellung auf virtuelle Maschine

Wenn Sie schnell bestimmte Tabellen oder kritische Daten aus Ihren Oracle Database-Sicherungen wiederherstellen müssen, ist die sofortige Wiederherstellung zu VMware/Hyper-V oder dem integrierten Hypervisor eine ideale Lösung. Diese Funktion führt ein Sicherungsabbild als virtuelle Maschine aus und ermöglicht Ihnen einfachen Zugriff, um die erforderlichen Daten oder Tabellen zu finden und zu exportieren.

## Betrieb nach der Wiederherstellung fortsetzen

Nach einem der folgenden Wiederherstellungsprozesse bleibt die Datenbank im Sicherungsmodus und steht nicht für den regulären Gebrauch zur Verfügung:

- Sofortige Wiederherstellung auf virtuelle Maschinen
- Vollständige Wiederherstellung auf virtuelle Maschinen
- Bare-Metal-Wiederherstellung von physischen Servern

Um die Datenbank nach der Wiederherstellung in den offenen Modus zu schalten, befolgen Sie diese Schritte:

1. Verbinden Sie sich mit dem Oracle Database-Server über SQL*Plus als Benutzer mit SYSDBA-Berechtigung.

   ```
   set ORACLE_SID={db_identifier}
   SQLPLUS / AS SYSDBA
   ```

2. Führen Sie die folgenden Befehle aus:

   ```
   RECOVER DATABASE;
   ALTER DATABASE OPEN;
   ```

3. Geben Sie den folgenden Befehl ein, um zu überprüfen, ob die Datenbank im Sicherungsmodus ist:

   ```
   SELECT * FROM v$backup;
   ```

   Hier ist ein Ausgabe-Beispiel eines Geräts während einer Sofortwiederherstellung. **ACTIVE** zeigt an, dass die Datei im Sicherungsmodus ist, **NOT ACTIVE** zeigt an, dass die Datei in einem normalen Zustand ist.

   ```
   FILE# STATUS CHANGE# TIME CON_ID
   ---------- ------------------ ---------- --------- ----------
   1 ACTIVE 4229743 05-MAY-23 0
   3 ACTIVE 4229751 05-MAY-23 0
   4 ACTIVE 4229759 05-MAY-23 0
   ```

```
5 ACTIVE 4229775 05-MAY-23 0
7 ACTIVE 4229767 05-MAY-23 0
```

# Dateiserver wiederherstellen

Sie können einzelne Dateien für Dateiserver über das Wiederherstellungsportal wiederherstellen:

1. Gehen Sie zu **Workloads** > **Maschinen** > **Dateiserver** und wählen Sie die wiederherzustellende Workload aus.
2. Klicken Sie auf **Wiederherstellungsportal öffnen**.
3. Finden Sie die Datei, die Sie wiederherstellen möchten.
4. Klicken Sie auf **Herunterladen**. Wählen Sie den Quellserver aus, wenn es mehr als einen gibt.
5. Sehen Sie den Fortschritt in **Aktuelle Aufgaben**.

**Hinweis:**

- Das Herunterladen von Dateien von einem entfernten Standort kann länger dauern.

# Microsoft 365 wiederherstellen

ActiveProtect bietet ein nahtloses Wiederherstellungserlebnis für Microsoft 365-Daten mit anpassbaren Einstellungen, die auf Ihre Bedürfnisse zugeschnitten sind. Dazu gehören Optionen zur Übernahme von Quellberechtigungen und Replikationsrichtlinien. Sie können sogar Daten auf ein anderes Konto innerhalb desselben Mandanten wiederherstellen, vorausgesetzt, es gehört zum selben Workload-Typ. Dieser integrierte Ansatz erhöht Ihre Kontrolle und Effizienz bei der Verwaltung der Datenwiederherstellung.

Sie können die folgenden gesicherten Microsoft 365-Daten über das ActiveProtect Wiederherstellungsportal wiederherstellen oder herunterladen:

- **Exchange**:
  - E-Mail
  - Archivpostfächer
  - Kontakte
  - Kalendereereignisse
- **OneDrive**: Ordner und Dateien
- **Chat**: 1-zu-1-Nachrichten
- **Microsoft 365-Gruppen**:
  - E-Mail
  - Kalendereereignisse
- **SharePoint**: Dokumentbibliotheken und Listen
- **Teams**: Kanalbeiträge

## In diesem Abschnitt

# Exchange-Mail wiederherstellen

Dieser Artikel erklärt, wie Sie Exchange-Mail mit dem ActiveProtect Wiederherstellungsportal wiederherstellen oder herunterladen können. Es umfasst persönliche E-Mails, Archivpostfächer und Gruppenpostfächer.

## Zugriff auf E-Mails

1. Starten Sie das Wiederherstellungsportal.
2. Wählen Sie in der oberen linken Ecke **Exchange** aus dem Dropdown-Menü.
3. Klicken Sie auf der Registerkarte **Versionen** auf die Zielversion.
4. Verwenden Sie das Dropdown-Menü in der oberen linken Ecke, um zwischen **Mail** und **Archivpostfächern** zu wechseln.

## E-Mail-Inhalt in der Vorschau anzeigen

1. Doppelklicken Sie auf eine E-Mail, um sie zu öffnen.
2. Im **Vorschaufenster** können Sie die detaillierten Nachrichteninformationen und den Inhalt anzeigen.
3. Anhänge werden am unteren Rand des Fensters aufgelistet. Sie können einen bestimmten Anhang herunterladen, indem Sie auf den Pfeil nach unten daneben klicken, oder alle Anhänge herunterladen, indem Sie auf **Alle herunterladen** klicken.

## E-Mails herunterladen

E-Mails können im EML- oder PST-Format auf Ihr lokales Gerät exportiert werden. Wenn mehrere E-Mails ausgewählt sind, werden sie in eine ZIP-Datei komprimiert. Die benötigte Zeit hängt von der Größe der E-Mails ab.[1]

- **Einzelne E-Mail**: Bewegen Sie den Mauszeiger über die Zielnachricht und klicken Sie auf das ⋮-Symbol > **Herunterladen**.
- **Mehrere E-Mails**: Wählen Sie die Zielnachrichten aus und wählen Sie im **Herunterladen**-Menü in der oberen Leiste, die ausgewählten herunterzuladen.
- **E-Mail-Ordner oder gesamte Postfächer**: Wählen Sie die entsprechende Aktion direkt aus dem **Herunterladen**-Menü in der oberen Leiste.
- **Suchergebnisse**: Verwenden Sie die Suchleiste, um Nachrichten zu filtern, und wählen Sie dann im **Herunterladen**-Menü in der oberen Leiste, alle oder ausgewählte Ergebnisse herunterzuladen.

## E-Mails wiederherstellen

1. Starten Sie das Wiederherstellungsfenster mit einer der folgenden Methoden:

- **Einzelne E-Mail**: Bewegen Sie den Mauszeiger über die Zielnachricht und klicken Sie auf das ⋮-Symbol > **Wiederherstellen**.
- **Mehrere E-Mails**: Wählen Sie die Zielnachrichten aus und wählen Sie im **Wiederherstellen**-Menü in der oberen Leiste, die ausgewählten wiederherzustellen.
- **E-Mail-Ordner oder gesamte Postfächer**: Wählen Sie die entsprechende Aktion direkt aus dem **Wiederherstellen**-Menü in der oberen Leiste.
- **Suchergebnisse**: Verwenden Sie die Suchleiste, um Nachrichten zu filtern, und wählen Sie dann im **Wiederherstellen**-Menü in der oberen Leiste, alle oder ausgewählte Ergebnisse wiederherzustellen.

2. Geben Sie im Popup-Wiederherstellungsfenster die folgenden Einstellungen an:
   - **Zielkonto**: Klicken Sie auf **Ändern**, um ein anderes Konto als die Quelle auszuwählen.
   - **Zielordner**:
     - **Ziel**:
       - Wenn das Ziel-Microsoft 365-Konto von der Quelle abweicht, wird ein neuer Ordner erstellt, um die wiederhergestellten Daten zu speichern.
       - Wenn das Ziel-Microsoft 365-Konto mit der Quelle identisch ist, können Sie die Daten in den ursprünglichen Ordner oder einen neuen Ordner wiederherstellen. Gruppenpostfächer können nur in die ursprünglichen Ordner wiederhergestellt werden.
     - **Replikationsrichtlinie**: Wenn Sie in den ursprünglichen Ordner wiederherstellen, müssen Sie wählen, ob Nachrichten mit identischen Namen am Ziel überschrieben oder übersprungen werden sollen.
   - **Wiederherstellen von**: Wenn das Backup an mehreren Orten gespeichert ist, können Sie den Ort auswählen, von dem die Daten wiederhergestellt werden sollen.
3. Klicken Sie auf **Wiederherstellen**, um den Wiederherstellungsprozess zu starten.

### Hinweis:

1. In den folgenden Situationen wird die Download-Aufgabe im Hintergrund ausgeführt, und Sie können die Datei später unter **Letzte Aufgaben** > **Download** abrufen:
   - Auswahl von mehr als 1.000 E-Mails
   - Herunterladen aller E-Mails in Ordnern oder Suchergebnissen

# Exchange-Kontakte wiederherstellen

Dieser Artikel führt Sie durch die Wiederherstellung oder den Download von Exchange-Kontakten mithilfe des ActiveProtect-Wiederherstellungsportals.

## Kontakte aufrufen

1. Starten Sie das Wiederherstellungsportal.
2. Wählen Sie in der oberen linken Ecke **Exchange** aus dem Dropdown-Menü.
3. Klicken Sie auf der Registerkarte **Versionen** auf die Zielversion.
4. Wählen Sie in der oberen linken Ecke **Kontakte** aus dem Dropdown-Menü, um auf die gesicherten Kontakte zuzugreifen.

## Kontakte anzeigen

Doppelklicken Sie auf einen Kontakt, um das **Vorschaufenster** zu öffnen, in dem Sie alle Kontaktinformationen wie Name, E-Mail-Adresse, Telefonnummer usw. anzeigen können.

## Kontakte herunterladen

Sie können Kontakte im CSV-Format auf Ihr lokales Gerät exportieren:

- **Einzelner Kontakt**: Fahren Sie mit der Maus über den Zielkontakt und klicken Sie auf das ⋮-Symbol > **Herunterladen**.
- **Mehrere Kontakte**: Wählen Sie die Zielkontakte aus und klicken Sie in der oberen Leiste auf **Herunterladen**. Die ausgewählten Kontakte werden in eine ZIP-Datei komprimiert, was je nach Größe einige Zeit in Anspruch nehmen kann.

## Kontakte wiederherstellen

1. Starten Sie das Wiederherstellungsfenster mit einer der folgenden Methoden:
   - **Einzelner Kontakt**: Fahren Sie mit der Maus über den Zielkontakt und klicken Sie auf das ⋮-Symbol > **Wiederherstellen**.
   - **Mehrere Kontakte**: Wählen Sie die Zielkontakte aus und klicken Sie in der oberen Leiste auf **Wiederherstellen**.
2. Geben Sie im Popup-Fenster die folgenden Einstellungen an:
   - **Zielkonto**: Klicken Sie auf **Ändern**, um ein anderes Konto als die Quelle auszuwählen.
   - **Zielordner**: Die ausgewählten Kontakte werden in einem neuen Ordner unter dem Zielkonto wiederhergestellt. Der Ordnername wird hier angezeigt.

- **Wiederherstellen von**: Wenn das Backup an mehreren Orten gespeichert ist, können Sie den Ort auswählen, von dem die Daten wiederhergestellt werden sollen.

3. Klicken Sie auf **Wiederherstellen**, um den Wiederherstellungsprozess zu starten.

# Exchange-Kalendererereignisse wiederherstellen

Dieser Artikel führt Sie durch die Wiederherstellung oder den Download von Exchange-Kalendererereignissen mithilfe des ActiveProtect Wiederherstellungsportals. Es umfasst sowohl persönliche als auch Gruppenkalender.

## Kalendererereignisse aufrufen

1. Starten Sie das Wiederherstellungsportal.
2. Wählen Sie in der oberen linken Ecke **Exchange** aus dem Dropdown-Menü.
3. Klicken Sie auf der Registerkarte **Versionen** auf die Zielversion.
4. Wählen Sie in der oberen linken Ecke **Kalender** aus dem Dropdown-Menü, um auf die gesicherten Ereignisse zuzugreifen.

## Kalendererereignisse herunterladen

Sie können Kalendererereignisse im ICS-Format auf Ihr lokales Gerät exportieren:

- **Einzelnes Ereignis**: Fahren Sie mit der Maus über das Zielereignis und klicken Sie auf das **Herunterladen**-Symbol.
- **Mehrere Ereignisse**: Wählen Sie die Zielereignisse aus und klicken Sie in der oberen Leiste auf **Herunterladen**. Die ausgewählten Ereignisse werden in eine ZIP-Datei komprimiert, was je nach Größe einige Zeit in Anspruch nehmen kann.

## Persönliche Kalendererereignisse wiederherstellen

1. Starten Sie das Wiederherstellungsfenster mit einer der folgenden Methoden:
   - **Einzelnes Ereignis**: Fahren Sie mit der Maus über das Zielereignis und klicken Sie auf das **Wiederherstellen**-Symbol.
   - **Mehrere Ereignisse**: Wählen Sie die Zielereignisse aus und klicken Sie in der oberen Leiste auf **Wiederherstellen**.
2. Geben Sie im Popup-Fenster die folgenden Einstellungen an:
   - **Zielkonto**: Klicken Sie auf **Ändern**, um ein anderes Konto als die Quelle auszuwählen.
   - **Zielordner**: Die ausgewählten Ereignisse werden in einem neuen Ordner unter dem Zielkonto wiederhergestellt. Der Ordnername wird hier angezeigt.
   - **Wiederherstellen von**: Wenn das Backup an mehreren Orten gespeichert ist, können Sie den Ort auswählen, von dem die Daten wiederhergestellt werden sollen.
3. Klicken Sie auf **Wiederherstellen**, um den Wiederherstellungsprozess zu starten.

# Gruppenkalenderereignisse wiederherstellen

1. Starten Sie das Wiederherstellungsfenster mit einer der folgenden Methoden:
   - **Einzelnes Ereignis**: Fahren Sie mit der Maus über das Zielereignis und klicken Sie auf das **Wiederherstellen**-Symbol.
   - **Mehrere Ereignisse**: Wählen Sie die Zielereignisse aus und klicken Sie in der oberen Leiste auf **Wiederherstellen**.
2. Geben Sie im Popup-Fenster die folgenden Einstellungen an:
   - **Zielkonto**: Klicken Sie auf **Ändern**, um ein anderes Konto als die Quelle auszuwählen.
   - **Zielordner**:
     - Wenn das Ziel-Microsoft 365-Konto von der Quelle abweicht, wird ein neuer Ordner erstellt, um die wiederhergestellten Daten zu speichern.
     - Wenn das Ziel-Microsoft 365-Konto mit der Quelle identisch ist, werden die ausgewählten Ereignisse in den ursprünglichen Ordner wiederhergestellt. Legen Sie die Replikationsrichtlinie fest, um zu bestimmen, ob Ereignisse mit identischen Namen am Ziel überschrieben oder übersprungen werden sollen.
   - **Wiederherstellen von**: Wenn das Backup an mehreren Orten gespeichert ist, können Sie den Ort auswählen, von dem die Daten wiederhergestellt werden sollen.
3. Klicken Sie auf **Wiederherstellen**, um den Wiederherstellungsprozess zu starten.

# OneDrive-Dateien wiederherstellen

Dieser Artikel führt Sie durch die Wiederherstellung oder das Herunterladen von OneDrive-Dateien und -Ordnern mit dem ActiveProtect-Wiederherstellungsportal.

## Dateien zugreifen

1. Starten Sie das Wiederherstellungsportal.
2. Wählen Sie in der oberen linken Ecke **OneDrive** aus dem Dropdown-Menü aus.
3. Klicken Sie auf der Registerkarte **Versionen** auf die Zielversion, um auf die gesicherten Dateien zuzugreifen.

## Dateien oder Ordner herunterladen

- **Einzelnes Element**: Fahren Sie mit der Maus über das Zielobjekt und klicken Sie auf das **Herunterladen**-Symbol.
- **Mehrere Elemente**: Wählen Sie die Zielobjekte aus und klicken Sie in der oberen Leiste auf **Herunterladen**. Die ausgewählten Elemente werden in eine ZIP-Datei komprimiert, was je nach Größe einige Zeit in Anspruch nehmen kann.

## Dateien oder Ordner wiederherstellen

1. Starten Sie das Wiederherstellungsfenster mit einer der folgenden Methoden:
    - **Einzelnes Element**: Fahren Sie mit der Maus über das Zielobjekt und klicken Sie auf das **Wiederherstellen**-Symbol.
    - **Mehrere Elemente**: Wählen Sie die Zielobjekte aus und klicken Sie in der oberen Leiste auf **Wiederherstellen**.
2. Geben Sie im Popup-Fenster die folgenden Einstellungen an:
    - **Elemente wiederherstellen**: Wählen Sie, ob die Freigabeberechtigungen der Quellobjekte übernommen werden sollen.
    - **Zielkonto**: Klicken Sie auf **Ändern**, um ein anderes Konto als die Quelle auszuwählen.
    - Zielordner:
        - Ziel:
            - Wenn das Ziel-Microsoft 365-Konto von der Quelle abweicht, wird ein neuer Ordner erstellt, um die wiederhergestellten Daten zu speichern.
            - Wenn das Ziel-Microsoft 365-Konto mit der Quelle identisch ist, können Sie die Daten in den ursprünglichen Ordner oder einen neuen Ordner wiederherstellen.
        - **Replikationsrichtlinie**: Wenn Sie in den ursprünglichen Ordner wiederherstellen, müssen Sie wählen, ob Sie Elemente mit identischen Namen am Ziel überschreiben oder überspringen

möchten.

- **Wiederherstellen von**: Wenn das Backup an mehreren Orten gespeichert ist, können Sie den Ort auswählen, von dem die Daten wiederhergestellt werden sollen.

3. Klicken Sie auf **Wiederherstellen**, um den Wiederherstellungsprozess zu starten.

# 1-zu-1-Chat wiederherstellen

Dieser Artikel führt Sie durch den Prozess des Herunterladens von Chat-Nachrichten mit dem ActiveProtect Wiederherstellungsportal. Wenn Sie Kanalbeiträge wiederherstellen möchten, lesen Sie Kanalbeiträge in Teams wiederherstellen.

## Nachrichten abrufen

1. Starten Sie das Wiederherstellungsportal.
2. Wählen Sie in der oberen linken Ecke **Chat** aus dem Dropdown-Menü.
3. Klicken Sie auf der Registerkarte **Versionen** auf die gewünschte Version, um auf die gesicherten Nachrichten zuzugreifen.

## Nachrichteninhalt in der Vorschau anzeigen

Doppelklicken Sie auf eine Nachricht, um das **Vorschaufenster** zu öffnen, in dem Sie den vollständigen Inhalt anzeigen können.

## Nachrichten herunterladen

Nachrichten können im HTML-Format auf Ihr lokales Gerät exportiert werden. Wenn mehrere Nachrichten ausgewählt sind, werden sie in eine ZIP-Datei komprimiert. Die benötigte Zeit hängt von der Größe der Nachrichten ab.[1]

- **Einzelne Nachricht**: Fahren Sie mit der Maus über die Zielnachricht und klicken Sie auf das ⋮-Symbol > **Herunterladen**.
- **Alle Nachrichten im ausgewählten Chat**: Navigieren Sie zum Zielchat im linken Bereich. Wählen Sie dann die entsprechende Aktion aus dem **Herunterladen**-Menü in der oberen Leiste.
- **Suchergebnisse**: Verwenden Sie die Suchleiste, um Nachrichten zu filtern, und wählen Sie dann aus dem **Herunterladen**-Menü in der oberen Leiste, ob Sie alle oder ausgewählte Ergebnisse herunterladen möchten.

**Hinweis:**

1. In den folgenden Situationen wird die Download-Aufgabe im Hintergrund ausgeführt, und Sie können die Datei später unter **Letzte Aufgaben** > **Herunterladen** abrufen:
    - Auswahl von mehr als 5.000 Nachrichten
    - Herunterladen aller Nachrichten in Chats oder Suchergebnissen

# SharePoint-Elemente wiederherstellen

Dieser Artikel führt Sie durch die Wiederherstellung oder das Herunterladen von SharePoint-Dokumentbibliotheken und -Listen mit dem ActiveProtect-Wiederherstellungsportal. Um zu beginnen, starten Sie das Wiederherstellungsportal, um auf die gesicherten Elemente zuzugreifen.

## Dokumentbibliothekselemente herunterladen

- **Einzelnes Element**: Fahren Sie mit der Maus über das Zielobjekt und klicken Sie auf das **Herunterladen**-Symbol.
- **Mehrere Elemente**: Wählen Sie die Zielobjekte aus und klicken Sie in der oberen Leiste auf **Herunterladen**. Die ausgewählten Elemente werden in eine ZIP-Datei komprimiert, was je nach Größe einige Zeit in Anspruch nehmen kann.

## Listen und Dokumentbibliotheken wiederherstellen

1. Starten Sie das Wiederherstellungsfenster mit einer der folgenden Methoden:
   - **Einzelnes Element**: Fahren Sie mit der Maus über das Zielobjekt und klicken Sie auf das **Wiederherstellen**-Symbol.
   - **Mehrere Elemente**: Wählen Sie die Zielobjekte aus und klicken Sie in der oberen Leiste auf **Wiederherstellen**.
2. Geben Sie im Popup-Fenster die folgenden Einstellungen an:
   - **Elemente wiederherstellen**: Wählen Sie, ob die Freigabeberechtigungen der Quellobjekte übernommen werden sollen.
   - **Zielwebsite**: Klicken Sie auf **Ändern**, um eine andere Website als die Quelle auszuwählen.
   - **Zielpfad**: Die ausgewählten Elemente werden in einem neuen Ordner auf der Zielwebsite wiederhergestellt. Der Speicherort jedes wiederhergestellten Elements wird hier aufgelistet.
   - **Wiederherstellen von**: Wenn das Backup an mehreren Orten gespeichert ist, können Sie den Ort auswählen, von dem die Daten wiederhergestellt werden sollen.
3. Klicken Sie auf **Wiederherstellen**, um den Wiederherstellungsprozess zu starten.

# Kanalbeiträge in Teams wiederherstellen

Dieser Artikel führt Sie durch die Wiederherstellung oder das Herunterladen von Kanalbeiträgen in Microsoft Teams mithilfe des ActiveProtect Wiederherstellungsportals. Um zu beginnen, starten Sie das Wiederherstellungsportal, um auf die gesicherten Beiträge zuzugreifen.

## Beitragsinhalt in der Vorschau anzeigen

Doppelklicken Sie auf einen Beitrag, um das **Vorschaufenster** zu öffnen, in dem Sie den vollständigen Inhalt anzeigen können.

## Beiträge herunterladen

Beiträge können im HTML-Format auf Ihr lokales Gerät exportiert werden. Wenn mehrere Beiträge ausgewählt sind, werden sie in eine ZIP-Datei komprimiert. Die benötigte Zeit hängt von der Größe der Beiträge ab.[1]

- **Einzelner Beitrag**: Fahren Sie mit der Maus über den Zielbeitrag und klicken Sie auf das ⋮-Symbol > **Herunterladen**.
- **Alle Beiträge im ausgewählten Kanal**: Navigieren Sie zum Zielkanal im linken Bereich. Wählen Sie dann die entsprechende Aktion aus dem **Download**-Menü in der oberen Leiste.
- **Suchergebnisse**: Verwenden Sie die Suchleiste, um Beiträge zu filtern, und wählen Sie dann aus, ob Sie alle oder ein ausgewähltes Ergebnis aus dem **Download**-Menü in der oberen Leiste herunterladen möchten.

## Beiträge wiederherstellen

1. Öffnen Sie das Wiederherstellungsfenster mit einer der folgenden Methoden:
   - **Einzelner Beitrag**: Fahren Sie mit der Maus über den Zielbeitrag und klicken Sie auf das ⋮-Symbol > **Wiederherstellen**.
   - **Alle Beiträge im ausgewählten Kanal**: Navigieren Sie zum Zielkanal im linken Bereich. Wählen Sie dann die entsprechende Aktion aus dem **Wiederherstellen**-Menü in der oberen Leiste.
   - **Suchergebnisse**: Verwenden Sie die Suchleiste, um Beiträge zu filtern, und wählen Sie dann aus, ob Sie alle oder ein ausgewähltes Ergebnis aus dem **Wiederherstellen**-Menü in der oberen Leiste wiederherstellen möchten.
2. Geben Sie im Popup-Wiederherstellungsfenster die folgenden Einstellungen an:
   - **Wiederherstellungsobjekte**: Wählen Sie, ob die Mitglieder und Berechtigungen des Quellkanals übernommen werden sollen.
   - **Zielteam**:
     - **Ursprüngliches(r) Team und Kanal**: Die Daten am ursprünglichen Speicherort wiederherstellen.

        - **Neues Team und neuer Kanal**: Ein neues Team und einen neuen Kanal für die wiederhergestellten Daten erstellen.
    - **Wiederherstellen von**: Wenn das Backup an mehreren Orten gespeichert ist, können Sie den Ort auswählen, von dem die Daten wiederhergestellt werden sollen.
3. Klicken Sie auf **Wiederherstellen**, um den Wiederherstellungsprozess zu starten.

### Hinweis:

1. In den folgenden Situationen wird die Download-Aufgabe im Hintergrund ausgeführt, und Sie können die Datei später unter **Letzte Aufgaben** > **Herunterladen** abrufen:
    - Auswahl von mehr als 5.000 Beiträgen
    - Herunterladen aller Beiträge in Kanälen oder Suchergebnissen

# Selbstbedienungswiederherstellung aktivieren

Aktivieren Sie die Selbstbedienungswiederherstellung, um nicht-administrativen Benutzern Zugriff auf das Wiederherstellungsportal zu gewähren, damit sie Daten durchsuchen und wiederherstellen können, um die Effizienz zu steigern.

Die Methode zur Aktivierung der Selbstbedienungswiederherstellung hängt vom Workload-Typ ab:

## Für Maschinen

### Maschinen einem bestimmten Benutzer zuordnen

1. Unter **Benutzerverwaltung** gehen Sie zur Seite **Lokale Benutzer** oder **Domain/LDAP-Benutzer**.
2. Klicken Sie auf den gewünschten Benutzer.
3. Fügen Sie auf der Registerkarte **Selbstbedienungswiederherstellung** Maschinen hinzu, um sie mit dem ausgewählten Benutzer zu verknüpfen. Der Benutzer kann dann die gesicherten Daten der zugeordneten Maschinen im Wiederherstellungsportal wiederherstellen.

### Benutzer einer bestimmten Maschine zuordnen

1. Unter **Maschinen** gehen Sie zur Seite des gewünschten Workload-Typs.
2. Klicken Sie auf die gewünschte Maschine.
3. Fügen Sie auf der Registerkarte **Selbstbedienungsberechtigung** Domain/LDAP- oder lokale Benutzer hinzu, um sie mit der ausgewählten Maschine zu verknüpfen. Diese zugeordneten Benutzer können dann die gesicherten Daten der Maschine im Wiederherstellungsportal wiederherstellen.

## Für Microsoft 365

Sie können die Selbstbedienungswiederherstellung für jeden Microsoft 365-Mandanten aktivieren, wodurch alle Benutzer in der Organisation Zugriff auf das Wiederherstellungsportal erhalten.

1. Verbinden Sie Ihr ActiveProtect-Gerät mit Microsoft Entra Domain Services, wodurch Benutzer sich mit ihren Microsoft 365-Anmeldedaten im Wiederherstellungsportal anmelden können.
2. Gehen Sie zur Seite **Cloud-Anwendungen** und geben Sie den gewünschten Mandanten ein.
3. Klicken Sie auf **Aktionen** > **Mandant bearbeiten** > **Selbstbedienungsberechtigung**.
4. Aktivieren Sie die Selbstbedienungswiederherstellung, damit Mandantenbenutzer ihre Exchange- oder OneDrive-Daten wiederherstellen können.

# Benutzerverwaltung

ActiveProtect ermöglicht es Ihnen, Benutzer hinzuzufügen und ihnen administrative Berechtigungen zu erteilen, wie z.B. Backup, Wiederherstellung und Systemüberwachung. Mit robuster Zugriffssteuerung können Sie mit Ihrem Team zusammenarbeiten, um Workloads zu schützen und gleichzeitig die Sicherheit zu gewährleisten.

## In diesem Abschnitt

# Verwalten von Verzeichnisbenutzern und -gruppen

Schließen Sie Ihre Synology ActiveProtect-Geräte an einen Verzeichnisdienst an, wie z.B. Microsoft Active Directory oder C2 Identity. Sie können die Berechtigungen von Verzeichnisbenutzern für Sicherung, Wiederherstellung und Systemüberwachung verwalten.

Wenn Sie eine ActiveProtect-Site mit mehreren Servern einrichten, schließen Sie Ihren Verwaltungsserver an einen Verzeichnisdienst an und konfigurieren Sie einen Failover-Server. Dies stellt sicher, dass derselbe Satz von Benutzern auf Ihre Site zugreifen kann, da Verzeichnisbenutzer und deren Berechtigungen mit dem Failover-Server synchronisiert werden.

## In diesem Abschnitt

# Domain beitreten

Um Benutzer und Gruppen aus einem Domain-Dienst hinzuzufügen, verwenden Sie die folgenden Schritte, um Ihr Synology ActiveProtect-Gerät als Domain-Client zu konfigurieren.

**Wichtig:**

- Der Beitritt zu einem Verzeichnisdienst führt dazu, dass ActiveProtect-Geräte bestimmte Dienste neu starten und die folgenden Aufgaben abbrechen:
  - Sicherung von virtuellen Maschinen und physischen Servern
  - Wiederherstellung und Migration von virtuellen Maschinen
  - Wiederherstellung und Migration von physischen Servern als virtuelle Maschinen

## Fügen Sie Ihr Gerät einer Domain hinzu

1. Gehen Sie zu **Benutzerverwaltung** > **Domain/LDAP-Benutzer** und klicken Sie auf **Gerätekonsole öffnen**.
2. In der **Gerätekonsole** gehen Sie zu **Systemsteuerung** > **Domain/LDAP** > **Domain/LDAP**.
3. Klicken Sie auf **Beitreten** und geben Sie die folgenden Informationen ein:

| Option | Beschreibung |
|---|---|
| Servertyp | Wählen Sie **Domain** oder **Automatisch erkennen**. |
| Serveradresse | Geben Sie den FQDN oder die IP-Adresse eines Domain-Controllers ein. |
| DNS-Server | Geben Sie die IP-Adresse eines DNS-Servers ein, der die IP-Adressen von Domain-Controllern auflösen kann. |

4. Konfigurieren Sie die folgenden Einstellungen:

| Option | Beschreibung |
|---|---|
| Verwaltungsmodus | ◦ **Vertrauenswürdige Domains**: Verwalten Sie Benutzer in allen vertrauenswürdigen Domains. Dieser Modus ermöglicht es Ihnen, Benutzer und Gruppen nach Domain zu filtern.[1]<br>◦ **Einzeldomain mit OUs**: Verwalten Sie nur Benutzer in der Domain, der Ihr ActiveProtect-Gerät beitritt. Dieser Modus ermöglicht es Ihnen, Benutzer und Gruppen nach OU zu filtern. |
| Domain-Konto | Das Administratorkonto Ihrer Domain. |
| Domain-Kennwort | Das Kennwort des angegebenen Domain-Kontos. |
| DNS-Schnittstelle registrieren | Wählen Sie die NICs aus, die Sie beim DNS-Server registrieren möchten.[2] |

| | |
|---|---|
| Maschinenkonto in spezifischer OU registrieren | Wählen Sie, um Ihr Sicherungsgerät in der angegebenen OU zu registrieren. |

5. Klicken Sie auf **Weiter**, um eine Vorbedingungsprüfung durchzuführen (drei Arten von Ergebnissen wie folgt). Ihr ActiveProtect-Gerät wird der Domain beitreten, nachdem die Prüfung bestanden wurde:

| Status | Details |
|---|---|
|  | Das Testelement war erfolgreich. |
|  | Einige kleinere Probleme können die Domaindienste beeinträchtigen. |
|  | Einige kritische Probleme werden dazu führen, dass der Domainbeitritt fehlschlägt. |

**Anmerkung:**

1. Wenn Sie Benutzer und Gruppen vertrauenswürdiger Domains verwalten möchten, sollten diese Domains eine gegenseitige Vertrauensstellung mit der Domain haben, der Ihr ActiveProtect-Gerät beitritt.
2. Wenn der Hostname Ihres ActiveProtect-Geräts einen Unterstrich (_) enthält, schlägt die Registrierung fehl, da Unterstriche bei DNS nicht verwendet werden können.

# In ein LDAP-Verzeichnis einbinden

Um Benutzer und Gruppen aus einem LDAP-Dienst hinzuzufügen, verwenden Sie die folgenden Schritte, um Ihr Synology ActiveProtect-Gerät als LDAP-Client zu konfigurieren.

**Wichtig:**

- Der Beitritt zu einem Verzeichnisdienst führt dazu, dass ActiveProtect-Geräte bestimmte Dienste neu starten und die folgenden Aufgaben abbrechen:
  - Sicherung von virtuellen Maschinen und physischen Servern
  - Wiederherstellung und Migration von virtuellen Maschinen
  - Wiederherstellung und Migration von physischen Servern als virtuelle Maschinen

## Fügen Sie Ihr Gerät einem LDAP-Verzeichnis hinzu

1. Gehen Sie zu **Benutzerverwaltung** > **Domain/LDAP-Benutzer** und klicken Sie auf **Gerätekonsole öffnen**.
2. Gehen Sie in der **Gerätekonsole** zu **Systemsteuerung** > **Domain/LDAP** > **Domain/LDAP**.
3. Klicken Sie auf **Beitreten** und geben Sie die folgenden Informationen ein:

| Option | Beschreibung |
|---|---|
| Servertyp | Wählen Sie **LDAP** oder **Automatisch erkennen**. |
| Serveradresse | Geben Sie den FQDN oder die IP-Adresse des LDAP-Servers ein. |
| DNS-Server | Geben Sie die IP-Adresse eines DNS-Servers ein, der die IP-Adresse von LDAP-Servern auflösen kann. |

4. Geben Sie Ihre LDAP-Informationen ein, einschließlich Bind DN, Base DN und Verschlüsselungstyp.
5. (Optional) Konfigurieren Sie die Einstellungen der Profile, UID/GID-Verschiebung oder Client-Zertifikate.
6. Klicken Sie auf **Weiter**, um eine Vorbedingungsprüfung durchzuführen (drei Arten von Ergebnissen wie folgt). Ihr ActiveProtect-Gerät wird dem LDAP-Verzeichnis beitreten, nachdem die Prüfung bestanden wurde:

| Status | Details |
|---|---|
| ✅ | Das Testelement war erfolgreich. |
| ⚠️ | Einige kleinere Probleme können die LDAP-Dienste beeinträchtigen. |
| ❗ | Einige kritische Probleme werden dazu führen, dass der LDAP-Beitritt fehlschlägt. |

### Über LDAP-Profile

LDAP-Attribute variieren zwischen LDAP-Servern. Die Option **Profil** ermöglicht es Ihnen, festzulegen, wie Benutzer- und Gruppeninformationen den Attributen Ihres LDAP-Servers zugeordnet werden.

- **Standard**: Für Synology LDAP-Server oder Mac Open Directory.
- **IBM Lotus Domino**: Für IBM Lotus Domino 8.5.
- **Benutzerdefiniert**: Für benutzerdefinierte Zuordnungen, geben Sie die folgenden Attribute an.

| Typ | Attribut | Beschreibung |
|---|---|---|
| filter | passwd | Eine erforderliche objectClass für Benutzer |
| | group | Eine erforderliche objectClass für Gruppen |
| group | cn | Gruppennamen |
| | gidNumber | GID-Nummern der Gruppen |
| | memberUid | Gruppenmitglieder |
| passwd | uidNumber | UID-Nummern der Benutzer |
| | uid | Benutzernamen |
| | userPassword | Passwörter der Benutzer |
| | gidNumber | Primäre GID-Nummern der Benutzer |

## Über UID/GID-Verschiebung

Vermeiden Sie Konflikte zwischen LDAP- und lokalen Benutzern/Gruppen, indem Sie die UID/GID von LDAP-Benutzern/Gruppen um 1.000.000 verschieben. Diese Option ist für nicht-Synology LDAP-Server mit einem eindeutigen numerischen ID-Attribut für jeden Benutzer und jede Gruppe verfügbar.

## Über Client-Zertifikate

Synology ActiveProtect-Geräte unterstützen Client-Zertifikate, die einige LDAP-Server zur Authentifizierung von Clients verwenden. Wählen Sie **Client-Zertifikat aktivieren**, um ein Client-Zertifikat hochzuladen.

# Verzeichnisbenutzer und -gruppen anzeigen und bearbeiten

Unter **Benutzerverwaltung** > **Domain/LDAP-Benutzer** können Sie Domain/LDAP-Benutzer und -Gruppen auf Ihrem Synology ActiveProtect-Gerät verwalten.

## Domain / LDAP-Benutzer

- **Allgemein**: Anzeigen des Benutzernamens und der Beschreibung.
- **Gruppen**: Anzeigen der Gruppen, zu denen ein Benutzerkonto gehört.
- Delegation: Berechtigungen an Ihre Teammitglieder vergeben, damit sie administrative Aufgaben wie Sicherung, Wiederherstellung und Systemüberwachung durchführen können.
- Self-Service: Aktivieren Sie die Selbstbedienungswiederherstellung, um nicht-administrativen Benutzern Zugriff auf das Wiederherstellungsportal zu gewähren, damit sie Daten selbst durchsuchen und wiederherstellen können.

## Domain / LDAP-Gruppen

- **Allgemein**: Anzeigen des Gruppennamens und der Beschreibung.
- Delegation: Gruppenmitgliedern erlauben, administrative Aufgaben wie Sicherung, Wiederherstellung und Systemüberwachung durchzuführen.

# Domäneneinstellungen konfigurieren

Sobald Ihr Synology ActiveProtect-Gerät einem Domain-Dienst beigetreten ist, können Sie Domain-Informationen unter **Benutzerverwaltung** > **Domain/LDAP-Benutzer** > **Verzeichnisinformationen** einsehen.

Wenn Sie die Domain-Client-Einstellungen ändern müssen, gehen Sie zur Gerätekonsole > **Systemsteuerung** > **Domain/LDAP** > **Domain/LDAP**. Klicken Sie auf **Einstellungen**, um die erweiterten Einstellungen zu überprüfen:

## Allgemeine Informationen bearbeiten

| Option | Beschreibung |
|---|---|
| DNS-Server | Geben Sie den Server an, der die IP-Adressen der Domain-Controller (DC) auflöst. |
| DC IP/FQDN | Geben Sie die IP-Adressen oder FQDNs der Domain-Controller ein.[1] |
| Benutzer-/Gruppenliste aktualisieren | Legen Sie fest, wie oft Ihr ActiveProtect-Gerät die Benutzer-/Gruppenlisten aktualisiert.[2] Für manuelle Updates klicken Sie auf **Domain-Daten aktualisieren** unter **Benutzerverwaltung** > **Domain-Benutzer**. |
| IWA | Integrierte Windows-Authentifizierung (IWA) bietet eine einfachere Möglichkeit, auf Ihr ActiveProtect-Gerät zuzugreifen. Wenn ein Domain-Benutzer an einem Computer angemeldet ist, kann er auf das ActiveProtect-Gerät zugreifen, ohne seine Anmeldedaten erneut eingeben zu müssen. Erfahren Sie, wie Sie IWA einrichten. |

## Verwaltungsmodus ändern

| Option | Beschreibung |
|---|---|
| Vertrauenswürdige Domains | Verwalten Sie Benutzer über alle vertrauenswürdigen Domains hinweg. Sie können auch auf **DC IP einstellen** klicken, um festzulegen, wie Ihr ActiveProtect-Gerät mit Domain-Controllern kommuniziert. Dieser Modus ermöglicht es Ihnen, Benutzer und Gruppen nach Domain zu filtern.[3] |
| Einzeldomain mit OUs | Verwalten Sie Benutzer nur innerhalb der Domain, der Ihr ActiveProtect-Gerät beitritt. Dieser Modus ermöglicht es Ihnen, Benutzer und Gruppen nach OU zu filtern. |

## Erweiterte Einstellungen verwalten

| Option | Beschreibung |
|---|---|

| | |
|---|---|
| Daten vertrauenswürdiger Domänen direkt von entsprechenden Domänen abrufen | Fordern Sie Domain-Daten direkt von vertrauenswürdigen Domains an. Aktivieren Sie diese Option, wenn Sie einigen Benutzern oder Gruppen keine Berechtigungen zuweisen können. |
| LDAP-Verschlüsselung | Wählen Sie einen Verschlüsselungstyp für die Verbindung Ihres ActiveProtect-Geräts mit Domain-Controllern. |
| Verschachtelte Gruppenebenen | Geben Sie die Anzahl der Ebenen für die Erweiterung verschachtelter Gruppen an. Zum Beispiel gelten bei einer Ebene von 2 die Berechtigungen einer Gruppe für ihre Benutzer, unmittelbare untergeordnete Gruppen (Ebene 1) und untergeordnete Gruppen dieser untergeordneten Gruppen (Ebene 2).[4] |

## Domain erneut beitreten

Der erneute Beitritt zur Domain ist nur erforderlich, wenn Anomalien auftreten, wie das Ablaufen des Computerkontos Ihres ActiveProtect-Geräts.

1. Gehen Sie zur **Gerätekonsole** > **Systemsteuerung** > **Domain/LDAP** > **Domain/LDAP** > **Einstellungen**.
2. Wählen Sie die Registerkarte **Allgemein** und klicken Sie auf **Domain erneut beitreten**.
3. Geben Sie Ihr Domain-Konto und Ihr Passwort ein. Klicken Sie auf **OK**, um den erneuten Beitrittsprozess zu starten.

**Anmerkung:**

1. Sie können die folgenden Sonderzeichen im Feld **DC IP/FQDN** eingeben:
   - **Komma (,)**: Trennen Sie mehrere Domain-Controller mit Kommas.
   - **Sternchen (*)**: Fügen Sie ein Sternchen nach der letzten Adresse hinzu. Ihr ActiveProtect-Gerät versucht, mit anderen DCs zu verbinden, wenn die Verbindung mit den angegebenen fehlschlägt. Stellen Sie sicher, dass Sie ein Komma verwenden, um das Sternchen von der letzten Adresse zu trennen.
2. Automatische Aktualisierungen der Benutzer-/Gruppenlisten können den Ruhezustand des Systems beeinflussen.
3. Um Benutzer und Gruppen vertrauenswürdiger Domains zu verwalten, müssen diese Domains eine gegenseitige Vertrauensstellung mit der Domain haben, der Ihr ActiveProtect-Gerät beitritt.
4. Die Erweiterung verschachtelter Gruppen kann unter bestimmten Umständen zeitaufwändig sein, z. B. wenn der Server keine Attributindizierung hat oder Gruppen stark verschachtelt sind.

# LDAP-Einstellungen konfigurieren

Sobald Ihr Synology ActiveProtect-Gerät einem LDAP-Dienst beitritt, können Sie LDAP-Informationen unter **Benutzerverwaltung** > **Domain/LDAP-Benutzer** > **Verzeichnisinformationen** einsehen.

Wenn Sie die LDAP-Clienteinstellungen ändern müssen, gehen Sie zur Gerätekonsole > **Systemsteuerung** > **Domain/LDAP** > **Domain/LDAP**. Klicken Sie auf **Einstellungen**, um die erweiterten Einstellungen zu überprüfen:

## Allgemeine Informationen bearbeiten

| Option | Beschreibung |
|---|---|
| Verschlüsselung | Wählen Sie einen Verschlüsselungstyp aus, um Ihr ActiveProtect-Gerät mit den LDAP-Servern zu verbinden. |
| Base DN | Geben Sie den Ausgangspunkt ein, von dem aus der Edge-Server nach Benutzerdaten sucht. Wenn der FQDN Ihres LDAP-Servers beispielsweise "ldap.synology.com" lautet, ist sein Base DN "dc=ldap,dc=synology,dc=com". |
| Profil | Wählen Sie ein Profil aus, das bestimmt, wie Benutzer- und Gruppeninformationen LDAP-Attributen zugeordnet werden. Weitere Informationen finden Sie unter Über LDAP-Profile. |

## Erweiterte Einstellungen verwalten

| Option | Beschreibung |
|---|---|
| Benutzer-/Gruppenliste aktualisieren | Legen Sie fest, wie oft Ihr ActiveProtect-Gerät die Benutzer-/Gruppenlisten aktualisiert.[1] Für manuelle Updates klicken Sie auf **LDAP-Daten aktualisieren** unter **Benutzerverwaltung** > **LDAP-Benutzer**. |
| Gruppenmitglied-Attribut | • **memberOf**: Ein Benutzerattribut, das sich auf Gruppen bezieht, zu denen Benutzer gehören. Wenn Sie diese Option auswählen, beziehen sich Gruppenobjekte auf ihre Benutzer mit dem Attribut member.<br>• **memberUID**: Ein Gruppenattribut, das sich auf seine Mitglieder bezieht. Wenn Sie diese Option auswählen, enthalten Benutzerobjekte keine Informationen über ihre Gruppen. |
| UID/GID-Verschiebung aktivieren | Vermeiden Sie Konflikte zwischen LDAP- und lokalen Benutzern/Gruppen, indem Sie die UID/GID von LDAP-Benutzern/Gruppen um 1.000.000 verschieben. Diese Option ist für nicht-Synology LDAP-Server verfügbar, die ein eindeutiges numerisches ID-Attribut für jeden Benutzer und jede Gruppe haben. |

| | |
|---|---|
| Verschachtelte Gruppen erweitern | Geben Sie die Anzahl der Ebenen an, um verschachtelte Gruppen zu erweitern. Beispielsweise gelten bei einer Ebene von 2 die Berechtigungen einer Gruppe für ihre Benutzer, unmittelbare untergeordnete Gruppen (Ebene 1) und untergeordnete Gruppen dieser untergeordneten Gruppen (Ebene 2).[2] |
| Client-Zertifikat aktivieren | Laden Sie ein Client-Zertifikat für die LDAP-Authentifizierung hoch. Bestimmte LDAP-Dienste erfordern ein Zertifikat zur Authentifizierung von LDAP-Clients. |

## Einem LDAP-Verzeichnis erneut beitreten

Ein erneuter Beitritt zu einem LDAP-Verzeichnis ist nur erforderlich, wenn Anomalien auftreten, wie z. B. ungültige Authentifizierungsdaten.

1. Gehen Sie zur **Gerätekonsole** > **Systemsteuerung** > **Domain/LDAP** > **Domain/LDAP** > **Einstellungen**.
2. Unter der Registerkarte **Allgemein** klicken Sie auf **LDAP erneut beitreten**.
3. Geben Sie Ihr Bind DN (oder das Administratorkonto Ihres LDAP-Servers) und das Passwort ein. Klicken Sie auf **OK**, um den Wiederbeitrittsprozess zu starten.

**Hinweis:**

1. Automatische Aktualisierungen von Benutzer-/Gruppenlisten können den Systemruhezustand beeinflussen.
2. Die Erweiterung verschachtelter Gruppen kann unter bestimmten Umständen zeitaufwändig sein, z. B. wenn der Server keine Attributindizierung hat oder Gruppen stark verschachtelt sind.

# Lokale Benutzer verwalten

Erstellen Sie lokale Benutzer und erlauben Sie ihnen, administrative Aufgaben auszuführen oder ihre eigenen Daten wiederherzustellen.

**Empfehlungen:**

- Wir empfehlen, Ihr ActiveProtect-Gerät einem Domain/LDAP-Verzeichnis beizutreten, um eine zentrale Verwaltung von Benutzerkonten und Zugriffskontrolle zu ermöglichen.

## In diesem Abschnitt

# Benutzer erstellen

Administratoren können lokale Benutzer auf dem ActiveProtect-Gerät unter **Verwaltung** > **Benutzerverwaltung** > **Lokale Benutzer** > **Benutzer** erstellen.

## Einen neuen Benutzer erstellen

1. Klicken Sie auf **Hinzufügen**.
2. Geben Sie die Informationen des Benutzers ein. Der Benutzername und das Kennwort sind erforderlich.
3. Fügen Sie den Benutzer einer Gruppe hinzu. Der Benutzer erbt die APM-Verwaltungsberechtigungen der Gruppe.
4. Bestätigen Sie, dass die Einstellungen des Benutzers korrekt sind, und klicken Sie auf **Hinzufügen**.

## Benutzernamenbeschränkung

- Bei dem Benutzernamen wird die Groß-/Kleinschreibung nicht berücksichtigt, und er kann aus 1 bis 64 Unicode-Zeichen bestehen, darf jedoch nicht die folgenden Symbole enthalten: ! " # $ % & ' ( ) * + , / : ; < = > ? @ [ ] \ ^ ` { } | ~
- Das erste Zeichen darf kein Minus- oder Leerzeichen sein und das letzte Zeichen darf kein Leerzeichen sein.
- Bestimmte Benutzernamen sind für die Systemnutzung reserviert, wie etwa mailer-daemon und postmaster.
- Die Benutzerbeschreibung darf bis zu 64 anzeigbare Unicode-Zeichen enthalten.

## Kennwortbeschränkung

- Beim Kennwort wird die Groß-/Kleinschreibung berücksichtigt und es ist auf maximal 127 anzeigbare Zeichen beschränkt, einschließlich Buchstaben, Zahlen, Zeichen und Leerzeichen.

# Benutzerinformationen anzeigen und bearbeiten

Administratoren können Benutzer auf dem ActiveProtect-Gerät unter **Benutzerverwaltung** > **Lokale Benutzer** > **Benutzer** anzeigen und verwalten.

## Benutzerstatus überprüfen

Benutzer haben drei mögliche Status:

- **Normal**: Dieses Benutzerkonto kann sich anmelden und alle Funktionen nutzen, für die es Berechtigungen hat.
- **Deaktiviert**: APM behält die Informationen des Benutzers, entzieht ihm jedoch den Zugriff auf APM und dessen Funktionen.
- **Kennwort abgelaufen**: Das Kennwort des Benutzerkontos ist abgelaufen; der Benutzer kann sich nicht anmelden, bis ein neues Kennwort konfiguriert ist.

## Benutzerinformationen bearbeiten

- **Allgemein**: Bearbeiten Sie den Benutzernamen, die E-Mail und die Beschreibung des Benutzers.
- **Sicherheit**: Ändern Sie das Kennwort eines Benutzers und seinen Aktivierungsstatus.
- **Gruppen**: Anzeigen und Verwalten der Gruppen, denen ein Benutzerkonto angehört.
- **Delegation**: Berechtigungen zuweisen an Ihre Teammitglieder, damit sie administrative Aufgaben wie Sicherung, Wiederherstellung und Systemüberwachung durchführen können.
- **Selbstbedienungswiederherstellung**: Selbstbedienungswiederherstellung aktivieren, um nicht-administrativen Benutzern Zugriff auf das Wiederherstellungsportal zu gewähren, damit sie eigenständig Daten durchsuchen und wiederherstellen können, um die Effizienz zu steigern.

# Kontosicherheit gewährleisten

Um die Kontosicherheit zu gewährleisten, ist es wichtig, starke Kennwörter für alle Konten zu verwenden und Benutzer zu deaktivieren, wenn sie nicht mehr benötigt werden.

Einstellungen in Bezug auf Kennwortsicherheit und Ablauf können unter **Benutzerverwaltung** > **Lokale Benutzer** > **Kennwortsicherheit** konfiguriert werden.

## Kennwort zurücksetzen

Sie können Benutzern erlauben, vergessene Kennwörter per E-Mail zurückzusetzen. Wenn ein Benutzer sein Kennwort vergisst, kann er auf der Anmeldeseite auf „Kennwort vergessen?“ klicken. Nach Eingabe des Benutzernamens sendet das System eine E-Mail mit einem Link zum Zurücksetzen des Kennworts.

### Hinweis:

- Bevor Sie diese Option aktivieren, stellen Sie sicher, dass E-Mail-Benachrichtigungen korrekt unter **Systemeinstellungen** > **Benachrichtigungen** > **E-Mail-Einstellungen** konfiguriert sind.
- Um Systemnachrichten zu erhalten, muss in den Benutzereinstellungen eine E-Mail-Adresse angegeben werden.
- Benutzer in der Gruppe **APM default admin** können diese Methode nicht verwenden, um ihre Kennwörter zurückzusetzen.

## Kennwortstärke

Um Benutzeranmeldedaten vor Brute-Force-Angriffen zu schützen, wird empfohlen, eine Mindestkennwortlänge von 8 Zeichen zu haben und mindestens drei der fünf Kennwortstärkeregeln zu erfüllen.

Sie können zusätzliche Einstellungen in Bezug auf Kennwortsicherheit und Stärkeregeln festlegen.

### Hinweis:

- Nach der Konfiguration von Kennwortstärkebeschränkungen werden die neuen Beschränkungen nur angewendet, wenn neue Benutzer erstellt werden oder bestehende Benutzer ihre Kennwörter ändern. Sie gelten nicht für bestehende Kennwörter aktueller Benutzer.

## Kennwortablauf

Benutzerkonten mit permanenten Kennwörtern können anfällig für Cyberangriffe sein. Um den Kontoschutz zu stärken, empfehlen wir, dass Benutzer ihre Kennwörter regelmäßig ändern.

## Benutzer deaktivieren

Um sicherzustellen, dass Benutzer nur bei Bedarf auf das Backup-Gerät zugreifen können, können Sie das Konto so einstellen, dass es nach einer bestimmten Zeit deaktiviert wird.

Weitere Informationen finden Sie unter Benutzerinformationen anzeigen und bearbeiten.

# Benutzer löschen

Um die Datensicherheit zu gewährleisten, können Sie Benutzerkonten löschen, wenn deren Besitzer die Organisation verlassen.

Um einen Benutzer zu löschen, gehen Sie zu **Benutzer Verwaltung** > **Lokale Benutzer** > **Benutzer**. Wählen Sie einen Benutzer aus und klicken Sie auf **Löschen**.

**Hinweis:**

- Sobald ein Benutzer gelöscht wird, löscht APM alle seine Informationen. Diese Aktion ist nicht rückgängig zu machen.
- Sobald ein Benutzer gelöscht wird, kann er sich nicht mehr bei APM anmelden.
- Der Super-Admin kann nicht gelöscht werden.

# Lokale Gruppen verwalten

Verwalten Sie effizient mehrere Benutzer gleichzeitig, indem Sie eine Gruppe erstellen. Gruppen organisieren Benutzer, was es einfacher macht, Zugriffsrechte auf Funktionen und andere Ressourcen in großen Mengen zuzuweisen. Benutzer in der Gruppe erben die Berechtigungen der Gruppe in APM.

Um Gruppen zu verwalten, gehen Sie zu **Benutzerverwaltung** > **Lokale Benutzer** > **Gruppen**.

## Gruppen erstellen

1. Klicken Sie auf **Hinzufügen** und geben Sie die Gruppeninformationen an. Der **Gruppenname** ist erforderlich.
2. Fügen Sie Benutzer zur Gruppe hinzu und delegieren Sie deren APM-Berechtigungen.
3. Überprüfen Sie die Zusammenfassungsseite und klicken Sie auf **Fertig**.

**Hinweis:**

- Die Gruppe **users** enthält standardmäßig alle lokalen APM-Benutzer. Die Mitgliederliste für diese Gruppe kann nicht geändert werden.
- Die Gruppe **APM Standard-Admin** enthält den Benutzer super admin. Dieser Benutzer kann nicht aus dieser Gruppe entfernt werden.

## Gruppen bearbeiten

Doppelklicken Sie auf die Gruppe, die Sie anzeigen oder bearbeiten möchten. Sie können den Namen, die E-Mail und die Beschreibung der Gruppe bearbeiten sowie die Mitglieder der Gruppe anzeigen und verwalten und den Kontostatus jedes Mitglieds einsehen.

Für die Delegation von Gruppenberechtigungen siehe Berechtigungen delegieren für weitere Informationen.

## Gruppen löschen

Wählen Sie eine Gruppe aus und klicken Sie auf **Löschen**. Dieser Vorgang ist nicht rückgängig zu machen.

**Hinweis:**

- Wenn eine Gruppe gelöscht wird, entfernt APM alle zugehörigen Informationen, einschließlich Berechtigungen. Mitglieder, die Teil dieser Gruppe waren, erben deren Berechtigungen nicht mehr.
- Die Gruppe **users** kann nicht gelöscht werden.
- Die Gruppe **APM Standard-Admin** kann nicht gelöscht werden.

# Administrative Berechtigungen delegieren

Um die Effizienz des ActiveProtect-Sitemanagements zu steigern, weisen Sie Ihren Teammitgliedern Berechtigungen zu, damit sie administrative Aufgaben wie Sicherung, Wiederherstellung und Systemüberwachung durchführen können.

Dieser Artikel führt Sie durch die Delegation von Berechtigungen an Benutzer und Gruppen. Für ein effizientes Berechtigungsmanagement empfehlen wir, den Benutzerzugriff nach **Gruppen** zu gewähren. Alle Gruppenmitglieder erben dieselben Berechtigungen.

1. Unter **Benutzerverwaltung** gehen Sie zur Seite **Lokale Benutzer** oder **Domain/LDAP Benutzer**.
2. Doppelklicken Sie auf den Zielbenutzer oder die Zielgruppe.
3. Auf der Registerkarte **Delegation** können Sie die folgenden Einstellungen bearbeiten, nachdem Sie auf **Berechtigungen delegieren** > **Berechtigungsdelegation aktivieren** geklickt haben:
   - **Voller Zugriff**: Dieser Benutzer oder diese Gruppe hat vollständige Berechtigungen für das Verwaltungscenter und das Wiederherstellungsportal. Beachten Sie, dass der Zugriff auf die Gerätekonsole und den Out-of-Band-Management (OOB)-Dienst nicht enthalten ist.[1]
   - **Teilweiser Zugriff**: Dieser Benutzer oder diese Gruppe kann die folgenden Berechtigungen erhalten:

| Berechtigungen | Erlaubte Aktionen |
|---|---|
| Sicherung | ▪ Kann manuelle Sicherungen durchführen und abbrechen.<br>▪ Kann Details zu geschützten Workloads anzeigen.<br>▪ Kann Sicherungsaktivitäten und Protokolle anzeigen. |
| Wiederherstellung | ▪ Kann Bare-Metal-Wiederherstellungen durchführen.<br>▪ Kann sofortige/vollständige Wiederherstellungen zu Hypervisoren im Standort und eingebauten Hypervisor durchführen.<br>▪ Kann Dateien und Ordner wiederherstellen.<br>▪ Kann Sicherungsversionen herunterladen.<br>▪ Kann Details zu geschützten, archivierten und nicht verwalteten Workloads anzeigen.<br>▪ Kann Wiederherstellungsaktivitäten und Protokolle anzeigen. |
| Überwachung | ▪ Kann alle Details im Verwaltungscenter anzeigen (außer dem Wiederherstellungsportal, der Gerätekonsole und OOB) |

**Hinweis:**

1. Nur der **Superadministrator** hat Zugriff auf die Gerätekonsole und den OOB-Dienst. Dieses Konto wird während der Erstinstallation Ihres ActiveProtect-Geräts erstellt.
2. Benutzer können Berechtigungen von ihren Gruppen erben. Wenn die Berechtigungen eines Benutzers Konflikte aufweisen, überschreibt "Erlauben" "Kein Zugriff".

# Erteilen Sie Benutzern Selbstbedienungsberechtigungen

Steigern Sie die betriebliche Effizienz und Produktivität, indem Sie nicht-administrativen Benutzern Zugriff auf das Wiederherstellungsportal gewähren. Dies ermöglicht es ihnen, unabhängig Daten zu durchsuchen und wiederherzustellen, was eine schnelle Wiederherstellung versehentlich gelöschter Dateien oder früherer Dokumentversionen ohne IT-Unterstützung ermöglicht.

Für Schritt-für-Schritt-Anleitungen zur Einrichtung der Selbstbedienungsdatenwiederherstellung, siehe Selbstbedienungswiederherstellung aktivieren.

# SSO aktivieren

ActiveProtect Manager unterstützt vier **Single Sign-On (SSO)**-Protokolle: OIDC, SAML 2.0, CAS und Synology SSO. Nachdem Sie Ihr ActiveProtect-Gerät als SSO-Client konfiguriert haben, können Benutzer, die sich auf der SSO-Seite angemeldet haben, auf das Gerät zugreifen, ohne sich erneut anmelden zu müssen.

In diesem Artikel werden ein SSO-Server und Ihr ActiveProtect-Gerät wie folgt bezeichnet:

- **SSO-Server**: Ihr Identitätsanbieter (IdP)
- **SSO-Client**: Ihr ActiveProtect-Gerät

## OIDC SSO

OpenID Connect (OIDC) ist ein offenes Authentifizierungsprotokoll, das gemeinsam mit OAuth 2.0 funktioniert. Es ermöglicht Ihrem ActiveProtect-Gerät, Benutzeridentitäten zu verifizieren und Profilinformationen im JSON-Format von einem IdP abzurufen. Befolgen Sie die unten stehenden Anweisungen, um Ihr Gerät mit OIDC SSO-Diensten oder Entra ID zu integrieren.

### Richten Sie Ihr Gerät als OIDC SSO-Client ein

1. Gehen Sie zu Gerätekonsole > **Systemsteuerung** > **Domain/LDAP** > **SSO-Client**.
2. Wählen Sie das Kontrollkästchen **OpenID Connect SSO-Dienst aktivieren** und klicken Sie auf **OpenID Connect SSO-Einstellungen**.
3. Wählen Sie **OIDC** im Dropdown-Menü **Profil** aus.
4. Geben Sie die Informationen in die Felder des eingeblendeten Fensters ein:

| Option | Beschreibung |
|---|---|
| Kontotyp | Gewähren Sie SSO-Berechtigungen für drei Benutzertypen: Domain- (oder AD-) Benutzer, LDAP-Benutzer und lokale Benutzer. |
| Name | Ein benutzerdefinierter Profilname. Dieser wird auf der SSO-Anmeldeoberfläche angezeigt. |
| Well-known URL | Diese URL bietet alle erforderlichen IdP-Informationen für Ihr ActiveProtect-Gerät. |
| Anwendungs-ID | Die eindeutige Kennung Ihres ActiveProtect-Geräts. Diese wird häufig als **Client-ID** bezeichnet. |
| Anwendungsgeheimnis | Der private Schlüssel, der nur Ihrem ActiveProtect-Gerät und IdP bekannt ist. Er ermöglicht Ihrem ActiveProtect-Gerät, sich beim IdP zu authentifizieren. |
| Umleitungs-URI | Die URL Ihres ActiveProtect-Geräts, wohin Benutzer weitergeleitet werden, nachdem Ihr IdP Authentifizierungsanfragen bestätigt hat. |

| | |
|---|---|
| Autorisierungsbereich | Dieser enthält einen oder mehrere mit Zugriffstokens verknüpfte Bereiche. Er bestimmt, welche Dienste verfügbar sind, wenn Zugriffstokens für den Zugriff auf durch OAuth 2.0 geschützte Endpunkte verwendet werden. |
| Benutzeranspruch | Eine Gruppe von Benutzerattributen, die von jedem Autorisierungsbereich zurückgegeben werden. Das System verwendet diese zur Identifizierung von Benutzern. |

5. Klicken Sie auf **Speichern** und schließen Sie das eingeblendete Fenster.
6. Klicken Sie auf **Übernehmen**, um Ihre Einstellungen zu speichern.

## Richten Sie Ihr Gerät als Entra ID SSO-Client ein

1. Stellen Sie sicher, dass Ihr ActiveProtect-Gerät einer Entra-Domain (ehemals „Azure AD“) über VPN oder einer mit einer Entra-Domain synchronisierten Domain beigetreten ist.
2. Gehen Sie zu Gerätekonsole > **Systemsteuerung** > **Domain/LDAP** > **SSO-Client**.
3. Markieren Sie das Kontrollkästchen **OpenID Connect SSO-Dienst aktivieren** und klicken Sie auf **OpenID Connect SSO-Einstellungen**.
4. Wählen Sie **Azure** im Dropdown-Menü **Profil** aus.
5. Geben Sie die **Anwendungs-ID**, **Schlüssel**, **Verzeichnis-ID** und **Umleitungs-URI** in die entsprechenden Felder ein. Im Microsoft Entra Admin Center finden Sie die **Anwendungs-ID** als Application (client) ID, die Schlüssel als **Clientgeheimnisse** und die Verzeichnis-ID als **Directory (tenant) ID**. Um die Informationen zu erhalten, lesen Sie die Anweisungen im nächsten Abschnitt.
6. Klicken Sie auf **Speichern** und schließen Sie das eingeblendete Fenster.
7. Klicken Sie auf **Übernehmen**, um Ihre Einstellungen zu speichern.

### So erhalten Sie die Anwendungs-ID, Schlüssel und Verzeichnis-ID für Entra ID SSO:

1. Melden Sie sich mit einem Administratorkonto beim Microsoft Entra Admin Center an.
2. Gehen Sie zu **Identität** > **Anwendungen** > **App-Registrierungen**. Klicken Sie auf **Neue Registrierung**.
3. Geben Sie den **Namen** Ihrer Anwendung ein.
4. Wählen Sie **Nur Konten in diesem Organisationsverzeichnis**.
5. Geben Sie die **Umleitungs-URI** ein, die Sie in der Gerätekonsole angegeben haben.
6. Klicken Sie auf **Registrieren**, um die Registrierung abzuschließen. Sobald die Anwendung erfolgreich registriert ist, wird sie auf der Seite **App-Registrierungen** angezeigt.
7. Klicken Sie auf den angezeigten Namen der Anwendung, um die **Anwendungsclient-ID** und **Directory Mandanten-ID** anzuzeigen.
8. Wechseln Sie zur Seite **Zertifikate und Geheimnisse**. Überprüfen Sie die geheimen Clientschlüssel Ihrer Anwendung oder klicken Sie auf die Schaltfläche **Neuer geheimer Clientschlüssel**, um einen neuen einzurichten.

### Wichtig:

- Die Benutzeroberfläche von Microsoft Entra ID kann ohne Vorankündigung geändert werden. Weitere Informationen zum Entra ID-Mechanismus finden Sie auf den folgenden Webseiten:
  - Microsoft Entra ID Dokumentation

- Microsoft Entra Domain Services Dokumentation

## SAML SSO

SAML (Security Assertion Markup Language) ist ein offener Standard für die Benutzerauthentifizierung. Unter diesem System können Client-Anwendungen Informationen von Benutzern abrufen und verifizieren, indem sie XML-basierte Assertionen mit einem IdP austauschen.

Folgen Sie diesen Schritten, um Ihr ActiveProtect-Gerät als SAML SSO-Client einzurichten:

1. Gehen Sie zu Gerätekonsole > **Systemsteuerung** > **Domain/LDAP** > **SSO-Client**.
2. Markieren Sie das Kontrollkästchen **SAML SSO-Dienst aktivieren** und klicken Sie auf **SAML SSO-Einstellungen**.
3. Klicken Sie im eingeblendeten Fenster auf **Metadaten importieren** und laden Sie eine von Ihrem IdP abgerufene SAML-Metadaten-Datei hoch. Sie können auch Informationen in den Feldern eingeben:

| Option | Beschreibung |
|---|---|
| Name | Ein benutzerdefinierter Profilname. Dieser wird auf der Benutzeroberfläche für die SSO-Anmeldung angezeigt. |
| Kontotyp | Erteilen Sie SSO-Berechtigungen für drei Benutzertypen: Domain (oder AD)-Benutzer, LDAP-Benutzer und lokale Benutzer. |
| SP-Entitäts-ID | Die URL dieses ActiveProtect-Geräts, wo Benutzer weitergeleitet werden, nachdem Ihr IdP SAML-Assertionen bestätigt. Diese Adresse muss mit HTTPS beginnen und kann keine QuickConnect-Adresse sein. Wird häufig als **Umleitungs-URI**, **Anwendungs-ID** oder **Assertionsverbraucherdienst-URL (ACS URL)** bezeichnet. |
| IdP-Entitäts-ID | Das einzigartige Attribut, das zur Erkennung Ihres IdP verwendet wird. Wird häufig als **IdP-Aussteller**, **Aussteller** oder **Kennung** bezeichnet. |
| IdP-Single-Sign-on-URL | Der IdP-Endpunkt, von dem SAML-Antworten gesendet werden. Wird häufig als **Anmelde-URL**, **SSO-URL** oder **SAML-Endpunkt** bezeichnet. |
| Zertifikat | Das öffentliche Schlüsselzertifikat Ihres IdP. Dieses wird zur Verifizierung der SAML-Assertionen und Antworten Ihres IdPs verwendet. |

4. Klicken Sie auf **Speichern** und schließen Sie das eingeblendete Fenster.
5. Klicken Sie auf **Übernehmen**, um Ihre Einstellungen zu speichern.
6. Wenn Ihr IdP die folgenden Optionen bietet, stellen Sie sicher, dass Sie diese auf der IdP-Website wie folgt konfigurieren:

| Option | Auswahl |
|---|---|
| Typ der SAML-Bindung | Die Option der HTTP-Umleitung |
| Format der Namens-ID | Nicht angegeben |

| | |
|---|---|
| Wert/Attribut der Namens-ID | Benutzername, Konto oder E-Mail-Option je nach Anforderungen |
| SAML-Assertion/Antwort-Signierung | ○ SAML-Antwort: Signieren<br>○ SAML-Assertion: Signieren oder nicht signieren |

## CAS SSO

CAS (Central Authentication Service) ist ein ticketbasiertes Protokoll für die Benutzerauthentifizierung. Unter diesem Protokoll verifiziert der IdP die Identitäten von Endbenutzern, indem er Servicetickets sendet und validiert.

Folgen Sie diesen Schritten, um Ihr ActiveProtect-Gerät als CAS SSO-Client einzurichten:

1. Gehen Sie zu Gerätekonsole > **Systemsteuerung** > **Domain/LDAP** > **SSO-Client**.
2. Markieren Sie das Kontrollkästchen **CAS SSO-Dienst aktivieren** und klicken Sie auf **CAS SSO-Einstellungen**.
3. Geben Sie die Informationen in den Feldern im eingeblendeten Fenster an:

| Option | Beschreibung |
|---|---|
| Name | Ein benutzerdefinierter Profilname. Dieser wird auf der SSO-Anmeldeschnittstelle angezeigt. |
| Kontotyp | Gewähren Sie SSO-Berechtigungen für drei Benutzertypen: Domain (oder AD)-Benutzer, LDAP-Benutzer und lokale Benutzer. |
| Service-ID | Die URL Ihres ActiveProtect-Geräts. Ihr IdP wird Benutzer nach erfolgreicher Authentifizierung an diesen Ort weiterleiten. |
| Server-URL | Die URL Ihres IdP. |
| Server-Validierungs-URL | Diese URL wird von Ihrem ActiveProtect-Gerät verwendet, um die Gültigkeit eines Servicetickets mit Ihrem IdP zu bestätigen, der ein XML-Dokument zurücksendet. |

4. Klicken Sie auf **Speichern** und schließen Sie das eingeblendete Fenster.
5. Klicken Sie auf **Übernehmen**, um Ihre Einstellungen zu speichern.

## Synology SSO

Synology SSO ist eine Lösung zur Benutzerauthentifizierung, die auf dem OAuth 2.0-Framework basiert. Sie bietet eine Single-Sign-On-Architektur speziell für Synology-Geräte. Um dieses Protokoll zu verwenden, müssen Sie einen Synology NAS mit installiertem SSO Server haben.

Folgen Sie diesen Schritten, um Ihr ActiveProtect-Gerät als Synology SSO-Client einzurichten:

1. Gehen Sie zu Gerätekonsole > **Systemsteuerung** > **Domain/LDAP** > **SSO-Client**.

2. Markieren Sie das Kontrollkästchen **Synology SSO-Dienst aktivieren** und klicken Sie auf **Synology SSO-Einstellungen**.
3. Geben Sie die Informationen in den Feldern im eingeblendeten Fenster an:

| Option | Beschreibung |
| --- | --- |
| Name | Ein benutzerdefinierter Profilname. Dieser wird auf der SSO-Anmeldeschnittstelle angezeigt. |
| Kontotyp | Gewähren Sie SSO-Berechtigungen für drei Benutzertypen: Domain (oder AD)-Benutzer, LDAP-Benutzer und lokale Benutzer. |
| SSO-Server-URL | Die vollständige URL des **SSO Servers**. Finden Sie sie auf Ihrem Synology NAS > **SSO Server** > **Allgemeine Einstellungen**. |
| Anwendungs-ID | Geben Sie den Namen Ihres ActiveProtect-Geräts ein, das auf Ihrem Synology NAS > **SSO Server** > **Anwendung** konfiguriert ist. |

4. Klicken Sie auf **Speichern** und schließen Sie das eingeblendete Fenster.
5. Klicken Sie auf **Übernehmen**, um Ihre Einstellungen zu speichern.

**Hinweis:**

- Wenn Sie SSO standardmäßig für die Anmeldung bei Ihrem ActiveProtect-Gerät verwenden möchten, wählen Sie **SSO standardmäßig auf der Anmeldeseite auswählen** in der **Gerätekonsole** > **Systemsteuerung** > **Domain/LDAP** > **SSO-Client**.
- Wenn Sie Ihr ActiveProtect-Gerät als Azure- oder WebSphere-SSO-Client einrichten, dürfen sich lokale Benutzer nicht über OIDC SSO anmelden.
- Um lokalen Benutzern die Anmeldung über SSO zu erlauben, gehen Sie zu Ihrem IdP und vergewissern Sie sich, dass er Benutzer mit denselben Benutzernamen wie auf Ihrem ActiveProtect-Gerät enthält.
- Webbrowser können SSO-Anmeldungen blockieren, wenn Ihr IdP HTTPS ohne ein vertrauenswürdiges Zertifikat verwendet. Wenn Ihr IdP HTTP verwendet und Ihr ActiveProtect-Gerät HTTPS, müssen Benutzer ihre Browser so konfigurieren, dass unsichere Verbindungen erlaubt sind.

# Überwachung

ActiveProtect bietet umfassende Überwachungsfunktionen, um Sie über den Sicherungsstatus und die Systemgesundheit Ihrer Organisation auf dem Laufenden zu halten. Sein zentrales Dashboard bietet vollständige Übersicht, sodass Sie die Infrastrukturgesundheit überwachen, Datenübertragungen verfolgen und den Schutzstatus von Workloads überprüfen können.

Um über den Status Ihrer ActiveProtect-Site auf dem Laufenden zu bleiben, können Sie Benachrichtigungsalarme für bestimmte Ereignisse anpassen, Sicherungs- und Wiederherstellungsaktivitäten verwalten und Protokolle zu Prüfzwecken überprüfen. Diese Funktionen vereinfachen die Problemverfolgung und Fehlerbehebung und verbessern die betriebliche Effizienz insgesamt.

## In diesem Abschnitt

# Dashboard navigieren

Die Seite **Dashboard** bietet einen vollständigen Überblick über Ihre ActiveProtect-Site und zeigt den Status des Datenschutzes sowie wichtige Kennzahlen an, um Ihnen zu helfen, Probleme proaktiv zu identifizieren und zu lösen.

Beachten Sie, dass einige Abschnitte möglicherweise nicht sichtbar sind, wenn ihre entsprechenden Einstellungen nicht konfiguriert wurden.

## Geschützte Workloads und Daten

Dieser Abschnitt zeigt die Anzahl der Workloads und die Größe der von ActiveProtect geschützten Daten. Während die Datengröße die Gesamtmenge der von jedem Workload übertragenen Sicherungsdaten darstellt, spiegelt sie nicht den tatsächlich auf Ihrem Sicherungsserver genutzten Speicherplatz wider.

## Deduplizierungsverhältnis

Das Deduplizierungsverhältnis vergleicht die Menge der Originaldaten mit dem tatsächlich genutzten Speicherplatz nach Entfernung doppelter Datenblöcke. Dieser Prozess behält nur einzigartige Datenblöcke bei, wodurch der Bedarf an Sicherungsspeicher reduziert wird, während die Datenintegrität erhalten bleibt.

## Letzter Sicherungsstatus von Maschinen & Cloud-Anwendungen

Dieser Abschnitt zeigt die Anzahl der Workloads für jeden Sicherungsstatus an:

- **Erfolg**: Alle Elemente wurden erfolgreich gesichert.
- **Warnung**: Teilweise Sicherung. Einige Elemente sind fehlgeschlagen, wurden abgebrochen oder nur teilweise erfolgreich.
- **Fehler**: Sicherung fehlgeschlagen. Keine Elemente wurden gesichert.

## Status der Sicherungskopie

Dieser Abschnitt zeigt die Anzahl der Versionen, die kopiert oder in der Warteschlange sind, zusammen mit allen Plänen, die Kopierprobleme haben, damit Sie den Kopierstatus schnell überprüfen und notwendige Anpassungen vornehmen können.

Wenn der Status der Sicherungskopie im Schutzplan **Ziel getrennt** anzeigt, doppelklicken Sie auf den Plan und überprüfen Sie die Registerkarte **Eingeschlossene Workloads**, um betroffene Workloads zu identifizieren. Dieses Problem tritt typischerweise aufgrund einer Netzwerkunterbrechung zwischen dem Sicherungsserver, der die Workloads hostet, und dem Ziel der Sicherungskopie auf.

# Aktuelle Sicherungen

Dieser Abschnitt bietet eine Kalenderansicht, die den täglichen Sicherungsstatus für alle Workloads der letzten 5 Wochen zusammenfasst:

- **Erfolg**: Alle Workloads wurden erfolgreich gesichert.
- **Warnung**: Einige Workloads-Sicherungen sind fehlgeschlagen, wurden abgebrochen oder waren nur teilweise erfolgreich.
- **Fehler**: Keiner der Workloads wurde gesichert.
- **Keine Sicherungen**: An diesem Tag fanden keine Sicherungen statt.
- **Bevorstehend**: Sicherungen sind für die kommende Zukunft geplant.

# Verpasste oder erfolglose Sicherungen

Dieser Abschnitt listet Workloads auf, die innerhalb von 12 Stunden nach ihrer geplanten Zeit nicht gesichert wurden. Es wird nur eine verpasste Version pro Workload angezeigt, und sobald eine Sicherung rechtzeitig abgeschlossen ist, wird der Workload aus der Liste entfernt.

Wenn ein Sicherungsserver getrennt ist, werden die ihm zugewiesenen Workloads hier nicht aktualisiert, bis der Server wieder verbunden ist.

## Beispiel

Workload A ist geplant, jeden Tag um 9:00 Uhr gesichert zu werden. Die letzte erfolgreiche Sicherung wurde am 10.8. um 14:00 Uhr abgeschlossen, und die nächste Sicherung wird am 11.8. um 9:00 Uhr erwartet.

### Was gilt als verpasste oder erfolglose Sicherung?

Folgendes gilt als verpasste oder erfolglose Sicherungen:

- Wenn die Sicherung bis 21:00 Uhr am 11.8. nicht abgeschlossen wurde, wird die Sicherung an diesem Tag als verpasst markiert.
- Wenn die Sicherung vor 21:00 Uhr am 11.8. fehlgeschlagen, abgebrochen oder nur teilweise erfolgreich war, wird die Sicherung an diesem Tag als nicht erfolgreich markiert.

### Wann wird eine verpasste/nicht erfolgreiche Sicherung eines Workloads gelöscht?

Die Sicherung von Workload A begann am 11.8. um 9:00 Uhr und lief über die nächsten zwei Tage, erfolgreich abgeschlossen am 13.8. um 19:00 Uhr. In diesem Fall:

- Zwischen 21:00 Uhr am 11.8. und 19:00 Uhr am 13.8. erscheint Workload A in der Tabelle für verpasste oder nicht erfolgreiche Sicherungen.
- Ab 19:00 Uhr am 13.8. wird Workload A aus der Tabelle entfernt.

# Status des Sicherungsservers

In diesem Abschnitt können Sie den Status der Sicherungsserver in Ihrer ActiveProtect-Site überwachen.

Die Status der Sicherungsserver werden wie folgt kategorisiert:

- **In Ordnung**: Der Server läuft reibungslos ohne Probleme.
- **Warnung**: Der Server hat kleinere Probleme, die keine unmittelbare Bedrohung für die Daten darstellen.
- **Kritisch**: Der Server hat Probleme, die zu Datenbeschädigung führen könnten.
- **Getrennt**: Der Server ist nicht mit dem Verwaltungsserver verbunden oder synchronisiert.

## Status des Remote-Speichers

In diesem Abschnitt wird die Anzahl der Remote-Speicher in der ActiveProtect-Site und alle damit verbundenen Fehler angezeigt. Ein Klick auf die Fehleranzahl leitet Sie zur Seite **Remote-Speicher** für detaillierte Informationen weiter.

## Übersicht über die Sicherungsdauer

In diesem Abschnitt können Sie die Sicherungsleistung überwachen, indem Sie die Dauer verfolgen. Bewegen Sie den Mauszeiger über jede Leiste, um Workload-Anzahlen und Sicherungstypen anzuzeigen. Längere Sicherungszeiten können auf getrennte Quellen, Sicherungsserver oder andere Infrastrukturprobleme hinweisen.

## Zunahme der Sicherungsdaten

In diesem Abschnitt werden sowohl die gesamte Datenzunahme als auch die tatsächliche Datenzunahme nach der Deduplizierung angezeigt. Es wird die Datenreduktionsrate hervorgehoben, die Ihre Speicherersparnisse zeigt.

## Trend der Speichernutzung

In diesem Abschnitt können Sie verfolgen, wie sich die Speichernutzung, einschließlich Sicherungen, Systemdateien und Metadaten, nach der Deduplizierung im Laufe der Zeit ändert, was Ihnen hilft, die zukünftige Skalierbarkeit zu planen, während die Daten Ihrer Organisation wachsen.

# Sicherungs- und Wiederherstellungsaktivitäten überwachen

Die Seite **Aktivitäten** bietet eine zentrale Ansicht der Sicherungs- und Wiederherstellungsaufgaben. Durch den Zugriff auf diese Seite können Sie den Fortschritt der Aktivitäten leicht überwachen, Sicherungen/Wiederherstellungen überwachen und laufende Aufgaben abbrechen, um Ressourcen freizugeben.

## Sicherungsaktivitäten überwachen

Gehen Sie zu **Aktivitäten** > **Sicherungsaktivitäten**. Diese Seite zeigt laufende und kürzlich durchgeführte Sicherungen an und hilft Ihnen, die Ressourcennutzung zu überwachen.

### Laufende Aktivitäten

Diese Registerkarte listet aktuelle Sicherungen auf. Sie können:

- Details einer bestimmten Sicherung durch Doppelklicken anzeigen.
- Eine Sicherung oder Sicherungsüberprüfung abbrechen, um Ressourcen freizugeben oder wenn sie unbeabsichtigt gestartet wurde.

### Verlauf

Diese Registerkarte zeigt abgeschlossene und abgebrochene Sicherungen der letzten 5 Wochen an.[1] Sie können:

- Verwenden Sie die Suchleiste, um Sicherungen zu filtern und Arbeitslasten mit Leistungsproblemen zu identifizieren.
- Aktivitäten für die Überprüfung exportieren. Sie können die Daten durch Anwenden eines Suchfilters verfeinern.

## Wiederherstellungsaktivitäten überwachen

Gehen Sie zu **Aktivitäten** > **Wiederherstellungsaktivitäten**. Diese Seite zeigt Wiederherstellungen an, die sowohl vom Wiederherstellungsportal als auch vom Wiederherstellungsassistenten initiiert wurden. Dateidownloads und Exporte sind hier nicht aufgeführt.

### Laufende Aktivitäten

Diese Registerkarte listet aktuelle Wiederherstellungsaktivitäten auf. Sie können:

- Details einer bestimmten Aktivität durch Doppelklicken anzeigen.

- Eine Wiederherstellung abbrechen, um Ressourcen freizugeben oder wenn sie unbeabsichtigt gestartet wurde.
- Sofort wiederhergestellte virtuelle Maschinen verwalten:
  - Verschieben Sie die wiederhergestellte virtuelle Maschine in die Produktionsumgebung für bessere I/O-Leistung und vollständige Datensynchronisation. Für virtuelle Maschinen, die als **Bereit zur Migration** markiert sind, wählen Sie **Migrieren mit Wiederherstellungsportal**, um den Migrationsprozess zu starten.[2]
  - Migration für virtuelle Maschinen abbrechen, die als **Bereit zur Migration** oder **Manuelle Migration erforderlich** markiert sind. Die sofort wiederhergestellten virtuellen Maschinen werden dann vom Hypervisor gelöscht.

## Verlauf

Diese Registerkarte zeigt alle abgeschlossenen und abgebrochenen Wiederherstellungsaktivitäten an. Sie können:

- Aktivitäten für die Überprüfung exportieren. Sie können die Daten durch Anwenden eines Suchfilters verfeinern.
- Wiederherstellungsaktivitäten löschen, um Speicherplatz freizugeben. Diese Aktion kann nicht rückgängig gemacht werden. Es wird empfohlen, Aktivitäten vor dem Löschen zu exportieren.

**Hinweis:**

1. Für Sicherungsversionen mit Aufbewahrungsfristen von mehr als 5 Wochen werden die Aktivitäten entfernt, sobald die Aufbewahrungsfrist endet.
2. Die VM-Migration basiert auf den nativen Tools von VMware vCenter: vMotion und Storage vMotion. Nur VMware vSphere-Lizenzen, die diese Funktionen unterstützen, können Migrationen durchführen. Wenn Ihre Lizenz vMotion und Storage vMotion nicht umfasst oder Sie VMs zwischen eigenständigen ESX(i)-Hosts migrieren müssen, ist die VMware vCenter-Migration nicht verfügbar und die Option ist deaktiviert.

# Benachrichtigungseinstellungen konfigurieren

Um Ihre Benachrichtigungseinstellungen festzulegen und Benachrichtigungen für bestimmte Ereignisse zu erhalten, navigieren Sie zur Seite **Systemeinstellungen** > **Benachrichtigungen** im linken Bereich. Diese Einstellungen gelten für alle ActiveProtect-Geräte innerhalb Ihrer Site.[1]

## Absender und Empfänger einrichten

Unter **E-Mail-Einstellungen** wählen Sie **E-Mail-Benachrichtigungen aktivieren**, um den Absender und die Empfänger festzulegen:

### Absender

Um einen Absender für die Zustellung von Benachrichtigungen festzulegen, klicken Sie auf **Anmelden** und konfigurieren Sie die SMTP-Servereinstellungen im Popup-Fenster. Zum Beispiel können Sie den Gmail SMTP-Server verwenden, um ActiveProtect E-Mail-Benachrichtigungen zu senden.

### Empfänger

Geben Sie an, wie Sie den Betreff der Benachrichtigung anpassen und wohin die Benachrichtigungen zugestellt werden sollen:

- **Benachrichtigungsbetreff-Präfix**: Geben Sie den Text ein, der in der Betreffzeile der Benachrichtigungs-E-Mails angezeigt werden soll.
- **Empfänger-E-Mails**: Geben Sie die E-Mail-Adresse jedes Empfängers ein.
- **Benachrichtigungssprache**: Wählen Sie die bevorzugte Sprache für die Benachrichtigungs-E-Mails aus.

## Benachrichtigungsregeln aktivieren

Unter **Regeln** wählen Sie die Ereignisse aus, über die Sie benachrichtigt werden möchten. Alle Empfänger, die im Abschnitt **Empfänger** konfiguriert sind, folgen denselben Regeln.

**Hinweis:**

1. Wenn Sie Active Backup for Business auf Ihrer Site ausführen, können Sie die Benachrichtigungseinstellungen auf dem entsprechenden Synology NAS anpassen.

# Protokolle überwachen

ActiveProtect verfügt über ein umfassendes Protokollierungssystem, das Ihnen hilft, Probleme mit Ihrem Gerät zu identifizieren und zu lösen. Diese Protokolle liefern wichtige Informationen zu Sicherungen, Wiederherstellungen, Benutzerverbindungen und Geräteoperationen. Sie erfassen auch potenzielle Probleme mit Speicher, Temperatur oder Batterie sowie andere wichtige Details.

Um Ihre Protokolle zu überprüfen, navigieren Sie zur Seite **Protokolle** im linken Bereich.

## Protokolle filtern

### Server und Protokollkategorie angeben

- **Sicherungsserver**: Protokolle von jedem Sicherungsserver werden separat angezeigt. Wählen Sie einen Server aus, um seine Protokolle anzuzeigen.
- **Protokollkategorie**: Wählen Sie die Art der Protokolle, die Sie überprüfen möchten:
  - **Aktivitätsprotokolle**: Ereignisse, die im Verwaltungscenter und im Wiederherstellungsportal auftreten, einschließlich Sicherungen, Wiederherstellungen, Arbeitslast-/Planaktualisierungen, Infrastrukturänderungen und Benutzerverwaltung. Weitere Informationen zur Interpretation dieser Protokolle finden Sie im Abschnitt Aktivitätsprotokolle.
  - **Laufwerksinformationen**: Details zu in den Sicherungsserver eingesetzten Laufwerken.
  - **Verbindungsprotokolle**: Aufzeichnungen der Benutzeranmeldeaktivitäten, einschließlich Zeitstempel, Benutzeridentitäten und Anmeldeerfolg oder -fehler.
  - **Erweiterte Systemprotokolle**: Protokolle, die von Systemdiensten generiert werden und Einblicke in die interne Funktionalität von ActiveProtect bieten. Diese Protokolle sind entscheidend für die Diagnose von Systemproblemen und Leistungsanomalien.

### Aktivitätsprotokolle

Aktivitätsprotokolle sind unerlässlich für die Überwachung von Sicherungen, Wiederherstellungen und Infrastrukturvorgängen. Jeder Protokolleintrag enthält die folgenden Details:

- Ebene:
  - **Information**: Zeigt an, dass eine Aufgabe erfolgreich abgeschlossen wurde.
  - **Warnung**: Zeigt unvollständige Serversynchronisation oder eine Sicherung/Wiederherstellung an, die nur teilweise erfolgreich oder abgebrochen wurde.
  - **Fehler**: Zeigt einen fehlgeschlagenen Vorgang an, wie z.B. Sicherungs-/Wiederherstellungsfehler, Serversynchronisationsprobleme oder Infrastrukturverwaltungsprobleme.
- Typ:
  - **Datenschutz**: Beinhaltet Ereignisse im Zusammenhang mit dem Schutz von Arbeitslasten, wie Anpassungen der Planeinstellungen und die Ausführung von Sicherungs-/Wiederherstellungsaufträgen.

    - **Systemverwaltung**: Beinhaltet Ereignisse im Zusammenhang mit Infrastrukturänderungen und Benutzerverwaltungsaktivitäten.
- **Datum & Uhrzeit**: Zeigt an, wann das Ereignis aufgetreten ist, und bietet eine klare Zeitachse der Aktionen.
- **Benutzername**: Identifiziert den Benutzer, der das Ereignis initiiert hat. Bei geplanten Sicherungen wird der Benutzername als **System** aufgeführt.
- **Ereignis**: Bietet eine kurze Beschreibung des Ereignisses. Für Sicherungs- und Wiederherstellungsaufträge mit den Status **Erfolgreich**, **Teilweise erfolgreich** und **Fehlgeschlagen** können Sie auf das Ereignis doppelklicken, um weitere Details anzuzeigen.

# Prüfprotokolle

## Protokolle exportieren

Um Protokolle herunterzuladen, klicken Sie auf **Exportieren** in der oberen rechten Ecke. Sie können wählen, ob Sie alle Protokolle oder nur die aus einem bestimmten Zeitraum exportieren möchten.[1]

Für erweiterte Systemprotokolle können Sie auch über Out-of-Band-Management (OOB) exportieren.

## Protokolleinstellungen verwalten

Klicken Sie auf **Einstellungen** in der oberen rechten Ecke, um die folgenden Optionen zu konfigurieren:

- **Protokolllöschung**: Legen Sie einen Zeitraum für das automatische Löschen abgelaufener Aktivitätsprotokolle fest.[2]
- **Protokollweiterleitung**: Konfigurieren Sie einen syslog-Server, um Protokolle zur zentralen Überwachung und Verwaltung weiterzuleiten.

### Hinweis:

1. Die Exportzeit hängt von der Anzahl und Größe der Protokolle ab. Die Verarbeitung kann bei einem großen Volumen an Protokollen länger dauern.
2. Systemerweiterte Protokolle, Verbindungsprotokolle und Laufwerksinformationen werden automatisch gelöscht, wenn sie die Systemgrenzen erreichen. Die Löschregeln sind:
    - **Erweiterte Systemprotokolle und Verbindungsprotokolle**: Wenn die Gesamtzahl 10.000 Einträge erreicht, behalten Sie 2/3 der Protokolle.
    - **Laufwerksinformationen**: Wenn die Gesamtzahl 600.000 Einträge erreicht, behalten Sie 9/10 der Protokolle.

# Gerätewartung

Um die Leistung und Zuverlässigkeit Ihres Synology ActiveProtect-Geräts sicherzustellen, konfigurieren Sie die Wartungseinstellungen in der **Gerätekonsole**. Diese Konsole ermöglicht es Ihnen, Netzwerkverbindungen, Verzeichnisdienste, Systemspeicher und Hardware-Ressourcen zu verwalten und zu überwachen.

## Anmelden bei der Gerätekonsole

Sie können auf die Gerätekonsole mit einer der folgenden Methoden zugreifen:

- Gehen Sie zu **ActiveProtect Manager** > **Infrastruktur** > **Backup-Server**. Wählen Sie Ihren Verwaltungsserver aus und klicken Sie auf **Mehr**> **Gerätekonsole öffnen**.
- Gehen Sie zu "https://*Verwaltungs-IP oder FQDN des Geräts*:**5001**", zum Beispiel "https://backup-1.synology.com:**5001**".

**Hinweis:**

- Standardmäßig kann auf die Gerätekonsole nur über den Verwaltungsport zugegriffen werden. Um den Zugriff auf die Gerätekonsole über den Datenport zu ermöglichen, lesen Sie diesen Artikel.
- Die Standardportnummer der Gerätekonsole ist 5001. Sie können sie unter **Gerätekonsole** > **Systemsteuerung** > **Netzwerk** > **Konnektivität** ändern.

## In diesem Abschnitt

# Netzwerkverbindungen verwalten

Konfigurieren Sie Netzwerkeinstellungen, um Ihr Synology ActiveProtect-Gerät mit dem Internet zu verbinden, und verwalten Sie Datenfluss-Steuerregeln, um den zulässigen ausgehenden Datenverkehr zu regeln, wenn Clients auf Dienste auf Ihrem Gerät zugreifen.

## In diesem Abschnitt

# Allgemeine Netzwerkeinstellungen bearbeiten

Gehen Sie zur **Gerätekonsole** > **Systemsteuerung** > **Netzwerk**, um allgemeine Netzwerkoptionen wie Standard-Gateway, DNS-Server und Proxy-Einstellungen zu bearbeiten. Klicken Sie auf **Übernehmen**, um alle vorgenommenen Änderungen zu speichern.

## Synology ActiveProtect-Gerät umbenennen

Um Ihr Synology ActiveProtect-Gerät umzubenennen, geben Sie den neuen Gerätenamen ein.

Der Gerätename ist nicht case-sensitiv und kann zwischen 1 und 15 Zeichen enthalten, bestehend aus Buchstaben, Zahlen, Unterstrichen und Minuszeichen. Das erste Zeichen des Namens muss ein Buchstabe sein.

## Standard-Gateway festlegen

Klicken Sie auf **Bearbeiten**, und suchen Sie dann die Netzwerkschnittstelle, die Sie als Standard-Gateway festlegen möchten. Ziehen Sie die gewünschte Netzwerkschnittstelle an die Spitze der Liste.

## DNS-Server-IP-Adresse festlegen

Sie können die IP-Adresse Ihres DNS-Servers manuell konfigurieren. Geben Sie hier die IP-Adresse Ihres bevorzugten DNS-Servers ein. Eine alternative DNS-Server-IP-Adresse kann ebenfalls eingegeben werden, um eine Sicherung zu bieten, falls der bevorzugte DNS-Server Probleme hat.

### Erweiterte Einstellungen

- **Antwort auf ARP-Anfrage, wenn die Ziel-IP-Adresse die lokale Adresse ist, die in der Eingangsschnittstelle konfiguriert wurde**: Aktivieren Sie diese Option, um auf ARP-Anfragen zu antworten und sicherzustellen, dass die ARP-Tabelle vollständig ist.
- **Mehrere Gateways aktivieren**: Aktivieren Sie diese Option, um mehr als einen Gateway in der Schnittstelle zu unterstützen.
- **Zuerst IPv4-Adresse verwenden, um Domainnamen aufzulösen**: Aktivieren Sie diese Option, um Domainnamen mit IPv4 für Clients aufzulösen, die IPv6 nicht unterstützen.
- **Erkennen von IP-Konflikten aktivieren**: Aktivieren Sie diese Option, um automatisch zu erkennen, falls die IP-Adresse bereits im Netzwerk vorhanden ist.

**Hinweis:**

- Die Felder **DNS-Server** und **Standard-Gateway** werden automatisch ausgefüllt und können nicht geändert werden, wenn alle Netzwerkschnittstellen automatisch konfiguriert werden.

# Über einen Proxy-Server verbinden

Um dem Backup-Gerät die Verbindung über einen Proxy-Server zu ermöglichen, wählen Sie **Über einen Proxy-Server verbinden** und geben Sie die **Adresse** und den **Port** ein.

**Hinweis:**

- Klicken Sie auf **Erweiterte Einstellungen**, um den HTTP-Proxy, HTTPS-Proxy und die Authentifizierungsinformationen zu konfigurieren.
- Standardmäßig sind die HTTPS-Proxy-Einstellungen identisch mit dem HTTP-Proxy.
- Lokale Adressen umgehen standardmäßig den Proxy-Server.

# HTTP/2 aktivieren

Sie können die HTTPS-Verbindungen beschleunigen, indem Sie HTTP/2 aktivieren.

Gehen Sie zur **Gerätekonsole** > **Systemsteuerung** > **Netzwerk** > **Konnektivität** und wählen Sie **HTTP/2 aktivieren**.

# Zugänglichkeit der Datenschnittstelle zu Verwaltungsdiensten aktivieren

Standardmäßig ist die Datenschnittstelle für die Übertragung von datensicherungsbezogenen Daten (z. B. Sicherung, Sicherungskopie, Wiederherstellung) und die Ermöglichung des Zugriffs von Mitarbeitern auf das Wiederherstellungsportal ausgelegt. Alle Verwaltungsfunktionen für die Standorte und Backup-Geräte sind standardmäßig über die Datenschnittstelle nicht zugänglich, einschließlich der folgenden Funktionen:

- Zugriff auf das Verwaltungscenter
- Zugriff auf die Gerätekonsole
- Zugriff auf die Out-of-Band-Management-Konsole
- Herstellen von anfänglichen Authentifizierungsverbindungen zu Standorten beim Hinzufügen von Backup-Servern zu Standorten sowie Synchronisieren von Ereignissen zwischen dem Verwaltungsserver und den Backup-Servern.

Um den gesamten Zugriff auf Verwaltungsdienste über den Zugriff von der Datenschnittstelle zu ermöglichen, gehen Sie zur **Gerätekonsole** > **Systemsteuerung** > **Netzwerk** > **Konnektivität** und aktivieren Sie die Option **Zugriff auf Gerätekonsole und Verwaltungscenter über Datenport erlauben**.

# Gerätekonsolen-Port anpassen

Der Standard-HTTPS-Port für den Zugriff auf die Gerätekonsole ist 5001. Wenn Sie die Standardportnummern ändern möchten, gehen Sie zur **Gerätekonsole** > **Systemsteuerung** > **Netzwerk** > **Konnektivität** und geben Sie die Portnummer im Feld **Gerätekonsolen-Port (HTTPS)** ein.

# Netzwerkschnittstellen konfigurieren

Gehen Sie zu **Systemsteuerung** > **Netzwerk** > **Netzwerk-Schnittstelle**, um die Netzwerkschnittstellen Ihres ActiveProtect-Geräts anzuzeigen und zu konfigurieren.

## IP-Adresse einer Schnittstelle konfigurieren

Je nach Ihren Netzwerkeinstellungen können Sie entweder DHCP, ein Protokoll zur automatischen IP-Adresszuweisung, konfigurieren oder manuell eine spezifische IP-Adresse verwenden, die von Ihrem Netzwerkdienstanbieter bereitgestellt wird.

Um DHCP eine IP-Adresse dem System zuweisen zu lassen, wählen Sie eine vorhandene Netzwerkschnittstelle, klicken Sie auf **Bearbeiten** und wählen Sie **Netzwerkkonfiguration automatisch erhalten (DHCP)** auf der Registerkarte **IPv4**.

Um dem System manuell eine spezifische IP-Adresse zuzuweisen, wählen Sie eine vorhandene Netzwerkschnittstelle, klicken Sie auf **Bearbeiten** und wählen Sie **Manuelle Konfiguration verwenden** auf der Registerkarte **IPv4**. Wenn kein DNS-Server oder Standard-Gateway verfügbar ist, lassen Sie das Feld leer.

**Hinweis:**

- Die Verwendung einer dynamischen IP-Adresse kann dazu führen, dass sich die IP-Adresse ändert, wenn das Gerät neu gestartet wird, was dazu führen könnte, dass der Agent die Verbindung zum Backup-Gerät verliert. Um dieses Problem zu vermeiden, wird empfohlen, eine statische IP-Adresse zu verwenden.
- Jumbo Frames sind Ethernet-Frames mit mehr als der standardmäßigen maximalen Übertragungseinheit (MTU) von 1500 Bytes, wodurch die Ethernet-Übertragung großer Dateien effizienter wird. Diese Funktion kann nur in einer Gigabit-Netzwerkumgebung aktiviert werden. Damit Jumbo Frames ordnungsgemäß funktionieren, müssen alle Computer und Geräte im Netzwerk, die auf das Gerät zugreifen, Jumbo Frames unterstützen und denselben MTU-Wert verwenden.
- Wenn Ihre Netzwerkumgebung VLAN-Einstellungen erfordert, wählen Sie eine vorhandene Netzwerkschnittstelle, klicken Sie auf **Bearbeiten** und **VLAN (802.1Q) aktivieren** auf der Registerkarte **IPv4**. Geben Sie eine VLAN-ID an. Beachten Sie, dass der LAN-Verwaltungsport diese Funktion nicht unterstützt.
- Wenn Sie nach der Änderung der oben genannten Einstellungen keine Verbindung zu Ihrem Backup-Gerät herstellen können, drücken Sie die RESET-Taste am Gerät, um die Netzwerkeinstellungen wiederherzustellen.

## 802.1X konfigurieren

802.1X ist ein Netzwerk-Authentifizierungsprotokoll, das mit einem RADIUS-Server verwendet wird, um den Netzwerkzugang auf authentifizierte Clients zu beschränken. Sie können Ihr Gerät so konfigurieren, dass es sich mit Netzwerken verbindet, die durch 802.1X-Authentifizierung gesichert sind.

Um die 802.1X-Authentifizierung zu aktivieren, führen Sie die folgenden Schritte aus:

1. Wechseln Sie zu **Systemsteuerung** > **Netzwerk** > **Netzwerk-Schnittstelle**.

2. Wählen Sie eine vorhandene Netzwerkschnittstelle und klicken Sie auf **Bearbeiten**.
3. Gehen Sie zur Registerkarte **802.1X** und **802.1X-Authentifizierung aktivieren**.
4. Wählen Sie eines der folgenden Protokolle aus dem Dropdown-Menü **Authentifizierung** aus. Wenn Sie nicht sicher sind, welches Protokoll am besten geeignet ist, wählen Sie **Automatisch**.

| Authentifizierungstyp | Beschreibung |
|---|---|
| Protected EAP (PEAP) | Verwenden Sie ein CA-Zertifikat (optional), um eine sichere Verbindung herzustellen. Diese sichere Verbindung wird von der inneren Authentifizierung verwendet. |
| Tunneled TLS (TTLS) | Verwenden Sie ein CA-Zertifikat (optional), um eine sichere Verbindung herzustellen. Diese sichere Verbindung wird von der inneren Authentifizierung verwendet. |
| TLS | Verwenden Sie TLS (Transport Layer Security) zur Authentifizierung. |

5. Wenn Sie TTLS oder PEAP auswählen, wählen Sie eines der inneren Authentifizierungsprotokolle aus dem Dropdown-Menü aus.

| Authentifizierungstyp | Beschreibung |
|---|---|
| MS CHAP v2 | Die Authentifizierungsinformationen werden mit Microsoft CHAP v2 verschlüsselt. |
| GTC | Die Authentifizierungsinformationen verwenden GTC (Generic Token Card) für die Verschlüsselung. |

6. Geben Sie den Benutzernamen und das Passwort/den privaten Schlüssel ein.
7. Wenn ein CA-Zertifikat erforderlich ist, klicken Sie auf **Importieren** und dann auf **Durchsuchen**, um ein vom Radius-Server exportiertes Zertifikat (z. B. ca.crt) zu suchen und zu importieren.

# VPN-Verbindung konfigurieren

Sie können Ihr ActiveProtect-Gerät so einrichten, dass es über die Protokolle PPTP, OpenVPN oder L2TP/IPSec mit einem bestehenden VPN (Virtual Private Network)-Server unter **Systemsteuerung** > **Netzwerk** > **Netzwerkschnittstelle** verbunden wird.

## VPN-Profile erstellen

Um VPN-Profile zu erstellen, die zum schnellen Wechseln und Verbinden mit verschiedenen VPN-Servern verwendet werden können, klicken Sie auf **Erstellen** und wählen Sie **VPN-Profil erstellen**. Drei Verbindungstypen stehen zur Verfügung.

| Verbindungstyp | Beschreibung |
|---|---|
| PPTP | PPTP (Point-to-Point Tunneling Protocol) ist eine häufig genutzte VPN-Lösung, die von den meisten Clients (einschließlich Windows, Mac, Linux und Mobilgeräte) unterstützt wird. |
| OpenVPN | Eine Open-Source-Lösung zur Implementierung des VPN-Dienstes. Sie schützt die VPN-Verbindung mit dem Verschlüsselungsmechanismus SSL/TLS. Beachten Sie, dass das Synology ActiveProtect-Gerät nur Verbindungen zu OpenVPN-Servern unterstützt, die tun-style Tunnels auf Layer 3 unterstützen. |
| L2TP/IPSec | L2TP (Layer 2 Tunneling Protocol) über IPSec bietet virtuelle private Netzwerke mit erhöhter Sicherheit und wird von den meisten Clients (wie Windows, Mac, Linux und Mobilgeräte) unterstützt. |

### PPTP- oder L2TP/IPSec-Profil erstellen

1. Gehen Sie zu **Systemsteuerung** > **Netzwerk** > **Netzwerkschnittstelle**. Klicken Sie auf **Erstellen** und wählen Sie **VPN-Profil erstellen**.
2. Wählen Sie **PPTP** oder **L2TP/IPSec**.
3. Geben Sie die folgenden Informationen an. Bitte beachten Sie, dass der Benutzername, das Passwort, die Adresse und der Pre-Shared Key des VPN-Servers vom Administrator des VPN-Servers bereitgestellt werden sollten.
   - Profilname
   - VPN-Serveradresse
   - Benutzername
   - Passwort
   - (Nur für L2TP/IPSec) Pre-Shared Key
4. Wählen Sie ein Authentifizierungsprotokoll aus.

| Authentifizierungstyp | Beschreibung |
|---|---|

| | |
|---|---|
| PAP | Das Passwort wird während der Authentifizierung nicht verschlüsselt. |
| CHAP | Das Passwort wird mit CHAP (Challenge-Handshake Authentication Protocol) verschlüsselt. |
| MS CHAP | Das Passwort wird mit Microsoft CHAP Version 1 verschlüsselt. |
| MS CHAP v2 | Das Passwort wird mit Microsoft CHAP Version 2 verschlüsselt. |

5. Wenn Sie über **PPTP** mit dem **MS CHAP oder MS CHAP v2**-Protokoll eine Verbindung zum VPN-Server herstellen, müssen Sie ein **Verschlüsselungs**protokoll auswählen.

| Verschlüsselungsprotokoll | Beschreibung |
|---|---|
| Kein MPPE | Die VPN-Verbindung wird nicht mit Microsoft Point-to-Point Encryption geschützt. |
| MPPE erforderlich (40/128 Bit) | Die VPN-Verbindung wird mit 40-Bit- oder 128-Bit-Microsoft Point-to-Point Encryption geschützt. |
| Maximales MPPE (128 Bit) | Die VPN-Verbindung wird mit 128-Bit-Microsoft Point-to-Point Encryption geschützt, was das höchste Sicherheitsniveau bietet. |

6. Je nach Bedarf können Sie auch die folgenden Optionen aktivieren:

| Option | Beschreibung |
|---|---|
| Standard-Gateway im Remote-Netzwerk verwenden | Leitet den Netzwerkverkehr Ihres Backup-Geräts zum angegebenen VPN-Server. |
| Anderen Netzwerkgeräten erlauben, über die Internetverbindung dieses Synology-Servers zu verbinden | Erlaubt Netzwerkgeräten, die sich im selben lokalen Netzwerk wie Ihr Backup-Gerät befinden, sich mit demselben VPN-Server zu verbinden. |
| Wieder verbinden, wenn die VPN-Verbindung verloren geht | Wenn die VPN-Verbindung unerwartet verloren geht, versucht das System fünfmal, die Verbindung wiederherzustellen, wobei alle 30 Sekunden ein Versuch unternommen wird. |

## OpenVPN-Profil (via .ovpn) erstellen

1. Gehen Sie zu **Systemsteuerung** > **Netzwerk** > **Netzwerkschnittstelle**. Klicken Sie auf **Erstellen** und wählen Sie **VPN-Profil erstellen**.
2. Wählen Sie die **OpenVPN**-Methode.
3. Geben Sie einen Namen für das Profil an und klicken Sie im Feld **.ovpn-Datei importieren** auf **Durchsuchen**, um eine vom VPN-Server exportierte .ovpn-Datei auszuwählen und zu importieren.
4. Geben Sie die vom Administrator Ihres VPN-Servers bereitgestellten Informationen ein: Ihren **Benutzernamen**, Ihr **Passwort** und importieren Sie die **CA-Zertifikatdatei** (z. B. ca.crt).
5. Wenn der VPN-Server-Anbieter Ihnen auch einen **TLS-auth Schlüssel**, **Client-Schlüssel**, **Client-Zertifikat** oder eine **Zertifikatsentzugsliste** bereitgestellt hat, klicken Sie auf **Erweiterte Optionen** und importieren Sie diese in die entsprechenden Felder.

6. Je nach Bedarf können Sie auch die folgenden Optionen aktivieren:

| Option | Beschreibung |
| --- | --- |
| Standard-Gateway im Remote-Netzwerk verwenden | Leitet den Netzwerkverkehr Ihres Backup-Geräts zum angegebenen VPN-Server. |
| Anderen Netzwerkgeräten erlauben, über die Internetverbindung dieses Synology-Servers zu verbinden | Erlaubt Netzwerkgeräten, die sich im selben lokalen Netzwerk wie Ihr Backup-Gerät befinden, sich mit demselben VPN-Server zu verbinden. |
| Wieder verbinden, wenn die VPN-Verbindung verloren geht | Wenn die VPN-Verbindung unerwartet verloren geht, versucht das System fünfmal, die Verbindung wiederherzustellen, wobei alle 30 Sekunden ein Versuch unternommen wird. |

**Hinweis:**

- Die Einstellungen für Authentifizierung und Verschlüsselung müssen identisch mit den auf dem VPN-Server angegebenen Einstellungen sein. Für weitere Details wenden Sie sich an den Administrator Ihres VPN-Servers.

## Mit einem VPN-Server verbinden oder trennen

1. Wählen Sie ein VPN-Profil aus.
2. Klicken Sie auf **Verbinden** oder **Trennen**.

**Hinweis:**

- Sie können nur ein Profil gleichzeitig verbinden.

# Link Aggregation aktivieren

ActiveProtect-Geräte unterstützen Multi-LAN und die Link Aggregation-Technologie, die die Bandbreite durch das Zusammenfassen mehrerer Netzwerkschnittstellen erhöht und bei Verbindungsverlust ein Traffic-Failover bietet.

Befolgen Sie diese Schritte, um die Link Aggregation zu aktivieren:

1. Gehen Sie zu **Systemsteuerung** > **Netzwerk** > **Netzwerkschnittstelle**. Klicken Sie auf **Erstellen** > **Bond erstellen**.
2. Wählen Sie einen Modus.

| Modus | Beschreibung |
| --- | --- |
| Balance-SLB | Gleicht den Netzwerkverkehr aus, ohne dass Unterstützung für spezielle Netzwerkswitches erforderlich ist, und ermöglicht die Verbindung zwischen zwei Switches. |
| Balance-TCP | Ermöglicht die Verbindung mit Switches, die für die dynamische Link Aggregation (IEEE 802.3ad LACP) konfiguriert sind. Werden mehrere Switches verwendet, müssen sie stapelbar und korrekt konfiguriert sein. |
| Aktiver Modus/Sicherungsmodus | Bietet Ihrem Sicherungsgerät Network Fault Tolerance unter Verwendung zweier Netzwerkschnittstellen. Bei Ausfall der aktiven Netzwerkschnittstelle übernimmt die andere Schnittstelle, um die Netzwerkverbindung aufrechtzuerhalten. Sie können diesen Modus wählen, ohne den Switch zu konfigurieren. |

3. Wählen Sie die Schnittstellen aus, um die Link Aggregation zu erstellen.
4. Geben Sie die IP-Adresse, die Subnetzmaske und das Gateway an. Die folgenden optionalen Einstellungen sind ebenfalls verfügbar: **Als Standard-Gateway festlegen**, **Jumbo Frame aktivieren** oder **VLAN aktivieren**.
5. Nach Abschluss sehen Sie eine neue Schnittstelle namens **Bond #** unter **Systemsteuerung** > **Netzwerk** > **Netzwerkschnittstelle**, die ebenso wie andere Schnittstellen (wie z. B. LAN) konfiguriert werden kann.

**Hinweis:**

- Bei aktivierter Link Aggregation wird der Netzwerkverkehr für jedes angeschlossene Gerät automatisch angepasst und ausgeglichen.
- Sind die Netzwerkschnittstellen mit mehreren Switches verbunden, müssen Sie darauf achten, dass die Switch-Ports sich im selben LAN oder VLAN befinden.
- Das Kombinieren der LAN-Ports mit der LAN-Management-Schnittstelle ist nicht erlaubt.

# Systemspeicher verwalten

Sie können die Speicherkapazität Ihres Synology ActiveProtect-Geräts in der **Gerätekonsole** mit dem **Speicher-Manager** organisieren und überwachen. Je nach Modell und Anzahl der installierten Laufwerke können Sie die folgenden Aufgaben durchführen:

- Überwachen Sie den gesamten Speicherstatus Ihres Synology ActiveProtect-Geräts.
- Kontrollieren Sie den Status der installierten Laufwerke.
- Richten Sie Zeitpläne für die Datenbereinigung ein, um die Speicherleistung zu optimieren.

## In diesem Abschnitt:

# ActiveProtect-Gerät Speicherlayout

Synology ActiveProtect-Geräte werden mit vorkonfigurierten Speicherlayouts geliefert. Sobald alle Festplatten installiert sind, initialisiert das System automatisch und richtet den Speicherpool und den SSD-Cache (falls zutreffend) gemäß der vordefinierten Konfiguration des spezifischen Modells ein. Dies gewährleistet eine effiziente und zuverlässige Speicherinstallation.

## Speicherlayout

Beziehen Sie sich auf die folgenden Standard-Speicherlayouts für jedes Modell:

| Modell | Speicherpool | SSD-Cache |
|---|---|---|
| DP320 | 2 × 8TB HDD (RAID 1) | N/V |
| DP340 | 4 × 8TB HDD (RAID 5) | 2 × 400GB SSD (RAID1) |
| DP7400 | 10 × 20TB HDD (RAID 6 + 1 Hot-Spare) | 2 × 3840GB SSD (RAID1) |

### RAID-Typen

Ein Speicherpool ist eine Sammlung von einem oder mehreren Laufwerken, die durch RAID geschützt werden können. Das Niveau des Datenschutzes variiert je nach RAID-Typ:

| RAID-Typ | Anzahl der Laufwerke | Tolerierbare Laufwerksausfälle | Beschreibung | Speicherkapazität |
|---|---|---|---|---|
| RAID 1 | ≧2 | N – 1 | • Schreibt identische Daten gleichzeitig auf alle Laufwerke.<br>• Bietet Datenredundanz. | Größe des kleinsten Laufwerks |
| RAID 5 | ≧3 | 1 | • Implementiert Striping auf Blockebene mit Parity-Daten, die über alle eingeschlossenen Laufwerke verteilt sind, wodurch die Datenredundanz effizienter ist als bei RAID 1. | (N – 1) x (Größe des kleinsten Laufwerks) |
| RAID 6 | ≧4 | 2 | • Implementiert zwei Datenparitätsschichten, um redundante Daten gleich der Größe von zwei Laufwerken zu speichern, und bietet ein höheres Maß an Datenredundanz als RAID 5. | (N – 2) x (Größe des kleinsten Laufwerks) |

**Hinweis:**

- „N“ steht für die Gesamtzahl der Festplatten.

## SSD-Cache

Der SSD-Cache verbessert die Leistung, indem er I/O-Operationen optimiert, die häufig auf zufällig platzierte Daten zugreifen. Dies ist besonders vorteilhaft für Operationen mit hohen Wiederlesemustern, wie z. B. die Deduplizierungs-Engine in Backup-Prozessen. Durch das Caching von Referenzdatenblöcken verbessert der SSD-Cache die Backup-Effizienz und verkürzt die Zeit, die zum Lesen von Daten aus dem Speicher benötigt wird.

## Hot-Spare

Wenn ein Laufwerk abstürzt und den Speicherpool beeinträchtigt, ist ein Hot-Spare ein Standby-Laufwerk, das das defekte Laufwerk automatisch ersetzen kann. Dies ermöglicht es dem Speicherpool, sich schnell zu reparieren und in einen gesunden Zustand zurückzukehren.

# Speicherstatus überwachen

## Gesamtstatus des Laufwerks überprüfen

Gehen Sie zu **Gerätekonsole** > **Speicher-Manager** > **Laufwerksinformationen**. Die Farbe der Laufwerke zeigt ihren Gesamtstatus an. Um weitere Informationen anzuzeigen, bewegen Sie Ihren Mauszeiger über ein Laufwerk.

| Farbe oder Symbol | Status | Details |
|---|---|---|
| Grün |  | Das Laufwerk ist in gutem Zustand und einem Speicherpool zugewiesen. |
| |  | Das Laufwerk ist in gutem Zustand, aber keinem Speicherpool zugewiesen. |
| Rot |  | Kritische Probleme wurden auf dem Laufwerk festgestellt. Dieses Laufwerk ist einem Speicherpool zugewiesen. |
| |  | Kritische Probleme wurden auf dem Laufwerk festgestellt. Dieses Laufwerk ist keinem Speicherpool zugewiesen. |
| Grau |  | Das Laufwerk wurde deaktiviert. |
| Schwarz |  | Der Laufwerkeinschub ist leer, da kein Laufwerk eingesetzt ist. |
|  | | Das Laufwerk ist als Hot-Spare zugewiesen. |
|  | | Das Laufwerk wird für SSD-Caching verwendet. |

## Laufwerke inspizieren

1. Gehen Sie zu **Gerätekonsole** > **Speicher-Manager** > **Laufwerksinformationen**, klicken Sie auf ein Laufwerk, um die folgenden Details anzuzeigen:
    - Standort
    - Zuordnungsrolle
    - Laufwerkstatus
    - Temperatur
    - Laufwerksaktion
    - Seriennummer
    - Firmware-Version
    - 4k natives Laufwerk

2. Sie können auf **Integritätsstatus** klicken, um die folgenden Details anzuzeigen:
    - Temperatur
    - Einschaltzeit

## Laufwerkstatus

| Laufwerkstatus | Details |
|---|---|
| Gesund | Dieses Laufwerk ist in gutem Zustand, oder Warnungen dafür wurden unterdrückt oder deaktiviert. |
| Kritisch | Auf diesem Laufwerk sind ein oder mehrere der folgenden kritischen Probleme aufgetreten:<br>• Kritische Fehler<br>• Nur-Lese-Modus<br>• Erreichen der Grenze der SSD-Ausdauer<br>Wir empfehlen, das Laufwerk sofort zu ersetzen. |
| Systempartition ausgefallen | Die Systempartition dieses Laufwerks ist nicht mehr zugänglich und muss repariert werden. Um dieses Problem zu beheben, klicken Sie auf **Systempartition reparieren**. |
| Nicht erkannt | Dieses Laufwerk ist mit Ihrem ActiveProtect-Gerät nicht kompatibel. Ersetzen Sie es sofort durch ein kompatibles Laufwerk, um den normalen Betrieb fortzusetzen. |
| Firmware-Aktualisierung erforderlich | Auf diesem Laufwerk sind ein oder mehrere Probleme aufgetreten, die mit einer Firmware-Aktualisierung behoben werden können. Weitere Informationen finden Sie unter Firmware aktualisieren. |
| Deaktiviert | Dieses Laufwerk wurde deaktiviert. |

## Zuweisungsrolle

| Zuweisungsrolle | Details |
|---|---|
| - | Dieses Laufwerk wird nicht verwendet, und es wurde ihm keine Rolle zugeordnet. |
| Speicherpool-ID | Dieses Laufwerk wurde einem Speicherpool zugewiesen. Das ActiveProtect-Gerät ist auf 1 Speicherpool beschränkt. Alle zusätzlichen Speicherpools werden deaktiviert. |
| ID des verfügbaren Pools | Der Speicherpool kann **online zusammengebaut** werden. |
| ID der SSD-Cache-Gruppe | Dieses Laufwerk wurde einer SSD-Cache-Gruppe zugewiesen. |
| Hot Spare | Dieses Laufwerk wurde als Hot-Spare-Laufwerk zugewiesen. |

## Laufwerkswarnungen

Standardmäßig wird das Synology ActiveProtect-Gerät Sie benachrichtigen, wenn fehlerhafte Sektoren auf dem Laufwerk erkannt werden oder wenn die erwartete Lebensdauer einer SSD 3 Monate erreicht.

Fehlerhafte Sektoren sind nur dann ein Problem, wenn ihre Anzahl stark ansteigt, was darauf hindeuten könnte, dass das Laufwerk ausfällt. Wenn Sie eine Warnung über fehlerhafte Sektoren per E-Mail-Benachrichtigung erhalten, wird empfohlen, Datenbereinigung zu planen.

Die erwartete Lebensdauer einer Synology SSD basiert auf ihrem aktuellen E/A-Workload. Je nach Änderungen im E/A-Workload im Laufe der Zeit kann sich die erwartete Lebensdauer einer Synology SSD verlängern oder verkürzen. Bei einer neu installierten Synology SSD kann das System mindestens 24 Stunden benötigen, um die Lebensdauer zu schätzen. Wenn Sie eine Benachrichtigung über die geschätzte Lebensdauer der SSD erhalten, sollten Sie in Erwägung ziehen, die SSD zu ersetzen, um Ausfälle zu vermeiden.

# Datenbereinigung konfigurieren

Die Datenbereinigung ist eine Wartungsfunktion, die fehlerhafte oder unvollständige Daten in Speicherpools korrigiert. Wir empfehlen, regelmäßig eine Datenbereinigung durchzuführen, um die Datenkonsistenz sicherzustellen und Datenverlust bei Laufwerksausfällen zu vermeiden.

## Datenbereinigung planen

1. Gehen Sie zu **Gerätekonsole** > **Speichermanager** > **Aufgabenplan** und klicken Sie auf **Datenbereinigung planen**.
2. Wählen Sie **Datenbereinigungszeitplan aktivieren** und sehen Sie sich die folgenden Einstellungen an oder passen Sie sie an:
    - **Häufigkeit**: Wählen Sie eine der folgenden Optionen:
        - **Monatlich wiederholen**
        - **Alle drei Monate wiederholen**
        - **Alle sechs Monate wiederholen**
        - **Jährlich wiederholen**
    - **Datenbereinigung nur in bestimmten Zeiträumen durchführen**: Klicken Sie auf **Zeitplan festlegen**, um die Datenbereinigung zu einem bestimmten Zeitpunkt zu planen, um die Systemleistung nicht zu beeinträchtigen.
    - **Nächste Ausführungszeit**: Wählen Sie, ob Sie **Später ausführen** möchten.
3. Klicken Sie auf **Speichern**.

# Reparieren Sie Ihren Speicher

Speicherpool- und SSD-Cache-Fehler können aufgrund von Laufwerksausfällen oder anderen Problemen auftreten. Die **Automatische Reparatur**-Funktion des Synology ActiveProtect-Geräts vereinfacht den Speicherreparaturprozess und maximiert die Verfügbarkeit des Dienstes.

Jedes Mal, wenn ein defektes Laufwerk ersetzt wird, reorganisiert das System automatisch das Speicherlayout auf seine vordefinierte Konfiguration, um die Systemleistung und Stabilität zu erhalten.

Wenn Ihr Modell Hot-Spare-Laufwerke unterstützt, wird ein Hot-Spare-Laufwerk automatisch jedes defekte Laufwerk ersetzen, sodass der Speicherpool ohne Unterbrechung funktionsfähig bleibt.

## Automatische Reparatur aktivieren

Wenn **Automatische Reparatur** aktiviert ist, werden alle neu installierten Laufwerke automatisch formatiert. Gehen Sie wie folgt vor:

1. Gehen Sie zu **Gerätekonsole** > **Speichermanager** > **Laufwerksinformationen** und klicken Sie auf ein Laufwerk.
2. Klicken Sie auf **Einstellungen**.
3. Wählen Sie **Automatische Reparatur aktivieren**.
4. Klicken Sie auf **Übernehmen**.

## Speicherpool reparieren

### Für Modelle mit Hot-Spare-Unterstützung

Wenn ein Speicherpool aufgrund eines defekten Laufwerks fehlerhaft wird, verwendet das System automatisch das Hot-Spare-Laufwerk, um ihn zu reparieren.

Sobald die Reparatur abgeschlossen ist, wird das defekte Laufwerk als **Deaktiviert** markiert. Sie können dann das defekte Laufwerk entfernen und durch ein einwandfreies ersetzen. Das System weist das neue Laufwerk automatisch als Hot-Spare zu.

### Für Modelle ohne Hot-Spare-Unterstützung

Wenn ein Speicherpool aufgrund eines defekten Laufwerks fehlerhaft wird oder ein Laufwerk den kritischen Status erreicht, gehen Sie wie folgt vor:

1. Gehen Sie zu **Gerätekonsole** > **Speichermanager** > **Laufwerksinformationen** und klicken Sie auf ein Laufwerk.
2. Wählen Sie das defekte oder kritische Laufwerk aus und klicken Sie auf **Aktion** > **Laufwerk deaktivieren**.[1]
3. Bestätigen Sie die Aktion, indem Sie das Passwort Ihres ActiveProtect Manager-Kontos eingeben.
4. Sobald das Laufwerk deaktiviert ist, entfernen Sie es aus dem Backup-Gerät und ersetzen Sie es durch ein einwandfreies.[2] [3]

5. Sobald das Ersatzlaufwerk installiert ist, repariert das System den fehlerhaften Speicherpool automatisch, wenn **Automatische Reparatur** aktiviert ist. Wenn **Automatische Reparatur** nicht aktiviert ist, müssen Sie das neue Laufwerk auswählen und auf **Aktion** > **Reparieren** klicken, um den Reparaturvorgang zu starten.

## SSD-Cache-Gruppe reparieren

Wenn eine SSD-Cache-Gruppe aufgrund eines defekten Laufwerks fehlerhaft wird oder ein Laufwerk den kritischen Status erreicht, gehen Sie wie folgt vor:

1. Gehen Sie zu **Gerätekonsole** > **Speichermanager** > **Laufwerksinformationen** und klicken Sie auf ein Laufwerk.
2. Wählen Sie das defekte oder kritische Laufwerk aus und klicken Sie auf **Aktion** > **Laufwerk deaktivieren.**[1]
3. Bestätigen Sie die Aktion, indem Sie das Passwort Ihres ActiveProtect Manager-Kontos eingeben.
4. Wenn Sie eine M.2 SSD verwenden, müssen Sie Ihr Backup-Gerät herunterfahren.
5. Entfernen Sie das defekte oder kritische Laufwerk aus Ihrem Backup-Gerät und ersetzen Sie es durch ein einwandfreies.[2] [3]
6. Sobald das Ersatzlaufwerk installiert ist, repariert das System den fehlerhaften Speicherpool automatisch, wenn **Automatische Reparatur** aktiviert ist. Wenn **Automatische Reparatur** nicht aktiviert ist, müssen Sie das neue Laufwerk auswählen und auf **Aktion** > **Reparieren** klicken, um den Reparaturvorgang zu starten.

**Anmerkung:**

1. Um Laufwerke zu reaktivieren, führen Sie eine der folgenden Aktionen aus:
   - Entfernen Sie das Laufwerk aus dem Einschub, warten Sie einige Sekunden, und setzen Sie es dann wieder ein.
   - Starten Sie das System neu.
2. Stellen Sie sicher, dass das Ersatzlaufwerk mit Ihrem ActiveProtect-Gerät kompatibel ist und die gleiche Kapazität wie das vorherige hat.
3. Alle Daten auf dem Ersatzlaufwerk werden gelöscht.

# Führen Sie Laufwerks-Benchmark-Tests durch

Sie können einen Leistungstest durchführen, um den sequentiellen Lese-/Schreibdurchsatz, Random IOPS und die Latenz eines Laufwerks zu bewerten.

Es gibt zwei Arten von Tests:

- **Basistest**: Dieser Test wird auf Laufwerken innerhalb einer RAID-Konfiguration ausgeführt, wie z.B. in einem Speicherpool oder einer SSD-Cache-Gruppe. Die Daten auf dem Laufwerk werden nicht beeinträchtigt.
- **Erweiterter Test**: Dieser Test wird auf Laufwerken ausgeführt, die sich nicht in einer RAID-Konfiguration befinden, wie z.B. nicht zugewiesene Laufwerke oder Hot-Spare-Laufwerke. Er bietet eine höhere Genauigkeit, garantiert jedoch keine Datenintegrität. Stellen Sie sicher, dass keine wichtigen Daten auf dem Laufwerk gespeichert sind, bevor Sie den Test durchführen.

Um einen Benchmark-Test durchzuführen, folgen Sie diesen Schritten:

1. Gehen Sie zu **Gerätekonsole** > **Speichermanager** > **Laufwerksinformationen** und klicken Sie auf das Laufwerk.
2. Klicken Sie auf **Aktion** > **Benchmark**.
3. Klicken Sie auf **Test jetzt ausführen**.
4. Bestätigen Sie, dass Sie den Test durchführen möchten, und klicken Sie auf **Ja**.

**Hinweis:**

1. Die für diesen Test benötigte Zeit kann je nach Systemauslastung variieren.
2. Um die Systemverfügbarkeit sicherzustellen, können Sie den Test nicht auf mehr als 3 Laufwerken gleichzeitig durchführen oder wenn sich nur 1 Laufwerk in Ihrem ActiveProtect-Gerät befindet.
3. Zur Genauigkeit wird das System Sie auffordern, zu bestätigen, bevor der Leistungstest fortgesetzt wird, wenn die Laufwerksauslastung 5 % überschreitet.
4. Um eine Überhitzung durch erzwungene Lese-/Schreibfunktionen von M.2 SSDs zu verhindern, unterstützt der Test keine Messungen des Lese-/Schreibdurchsatzes für M.2 SSDs.

# Ihre Laufwerke identifizieren

Die Funktion **Laufwerk identifizieren** ändert vorübergehend die Farbe der Laufwerksanzeige, sodass Sie das richtige Laufwerk in Ihrem ActiveProtect-Gerät leicht identifizieren und entfernen können.

Um Ihr Laufwerk zu identifizieren, folgen Sie diesen Schritten:

1. Gehen Sie zu **Anwendungskonsole** > **Speichermanager** > **Laufwerksinformationen** und klicken Sie auf das Laufwerk.
2. Klicken Sie auf **Laufwerk identifizieren**.
3. Wählen Sie die Dauer für die Farbänderung der Laufwerksanzeige.
4. Klicken Sie auf **Identifizieren**.

**Hinweis:**

- Der Anzeigestatus gilt nicht für Laufwerke, die über M.2 SSD-Adapterkarten installiert wurden, aufgrund von Designunterschieden.

# Secure Erase auf Ihren Laufwerken ausführen

Sie können **Secure Erase** verwenden, um alle auf einem bestimmten Laufwerk gespeicherten Daten dauerhaft zu entfernen. Stellen Sie sicher, dass das Laufwerk nicht verwendet wird und dass seine Daten gesichert wurden, bevor Sie diese Funktion verwenden.

Um Secure Erase auszuführen, folgen Sie diesen Schritten:

1. Gehen Sie zu **Gerätekonsole** > **Speicher-Manager** > **Laufwerksinformationen** und klicken Sie auf das Laufwerk.
2. Wählen Sie ein Laufwerk aus und klicken Sie auf **Aktion** > **Secure Erase**.
3. Bestätigen Sie, dass Sie die Risiken verstehen, und klicken Sie dann auf **OK**.
4. Geben Sie das Passwort Ihres ActiveProtect Manager-Kontos ein und klicken Sie auf **Senden**.

**Hinweis:**

- Das Laufwerk wird während Secure Erase vorübergehend gesperrt und wird automatisch entsperrt, sobald der Vorgang abgeschlossen ist.
- Wenn Secure Erase unterbrochen wird, können Sie den Vorgang einfach neu starten. Wenn Sie ein Laufwerk entfernen müssen, während es noch gesperrt ist, starten Sie das System neu, um es zu entsperren.

# Firmware der Laufwerke aktualisieren

Um die Synology-Laufwerke in Ihrem ActiveProtect-Gerät mit Ihrem System kompatibel zu halten, stellen Sie sicher, dass die Firmware Ihrer Laufwerke auf dem neuesten Stand ist.

Um die Firmware der Laufwerke zu aktualisieren, gehen Sie wie folgt vor:

1. Gehen Sie zu **Gerätekonsole** > **Speichermanager** > **Laufwerksinformationen** und klicken Sie auf das Laufwerk.
2. Klicken Sie auf **Aktion** > **Firmware-Aktualisierung**.
3. Klicken Sie auf **Aktualisieren**.

**Hinweis:**

- Wenn die Synology-Laufwerke in Gebrauch sind, wird das System automatisch neu gestartet, um alle Dienste sicher herunterzufahren und Anwendungsfehler zu vermeiden.

# Laufwerksdatenbanken aktualisieren

Die Laufwerksdatenbank enthält Informationen wie Laufwerkstemperatur, Kompatibilitätsliste und Firmwareaktualisierungen. Diese Datenbank wird automatisch und regelmäßig aktualisiert, um die Kompatibilitätsinformationen auf dem neuesten Stand zu halten, ohne die Laufwerksleistung zu beeinträchtigen.

Sie können auch wählen, sofort oder manuell mit dem **Synology HDD/SSD-Offline-Update-Paket** zu aktualisieren, das Sie im Download-Zentrum erhalten.

Um die Laufwerksdatenbank zu aktualisieren, folgen Sie diesen Schritten:

1. Gehen Sie zur **Gerätekonsole** > **Speichermanager** > **Laufwerksinformationen** und klicken Sie auf ein Laufwerk.
2. Klicken Sie auf **Einstellungen** > **Jetzt aktualisieren** oder **Manuelle Aktualisierung**.

### Hinweis:

- Die Datenbank wird automatisch aktualisiert, wenn Sie ein neues Laufwerk in Ihr ActiveProtect-Gerät einfügen.
- Wir empfehlen, die Datenbank in den folgenden Situationen manuell zu aktualisieren:
  - Es gibt ein Problem mit dem Mechanismus zur Erkennung der Laufwerkstemperatur.
  - Das System konnte ein in der Synology-Kompatibilitätsliste aufgeführtes Laufwerk nicht erkennen.
  - Das System konnte keine Verbindung zum Synology-Server herstellen.

# Hardware und Energie

In der **Gerätekonsole** > **Systemsteuerung** > **Hardware und Energie** können Sie Funktionen wie Verhalten nach Stromausfall, Wake on LAN, Signalton-Steuerung, Lüftergeschwindigkeit und Arbeitsspeicherkomprimierung konfigurieren. Sie können auch das ActiveProtect-Gerät an eine zusätzliche Sicherheits-Stromversorgung anschließen, falls ein Stromausfall auftritt.

## In diesem Abschnitt:

# USV-Dienste einrichten

USV (Unterbrechungsfreie Stromversorgung) ist ein Reservestromgerät, das es dem ActiveProtect-Gerät ermöglicht, bei einem Stromausfall für kurze Zeit weiter zu arbeiten. Dies gibt dem Backup-Gerät genügend Zeit, Daten zu speichern und Speicher zu trennen, bevor es heruntergefahren wird.

### Standby-Modus

Das ActiveProtect-Gerät wechselt automatisch in den **Standby-Modus**, wenn die Leistung des USV-Geräts niedrig ist. In diesem Modus werden alle Dienste gestoppt und der Speicher wird getrennt, um Datenverlust zu vermeiden und ein sicheres Herunterfahren zu gewährleisten, wenn das USV-Gerät keinen Strom mehr hat.

Sie können die Zeitspanne konfigurieren, bevor das ActiveProtect-Gerät bei einem Stromausfall in den **Standby-Modus** wechselt. Wenn jedoch der Akku des USV-Geräts vor der angegebenen Zeit auf ein niedriges Niveau sinkt, wechselt das System sofort in den **Standby-Modus**.

Um das ActiveProtect-Gerät automatisch zu starten, sobald die Stromversorgung wiederhergestellt ist, gehen Sie zu **Systemsteuerung** > **Hardware & Energie** > **Allgemein** > **Automatisch neu starten, wenn das Stromversorgungsproblem behoben ist**.

In der **Gerätekonsole** > **Systemsteuerung** > **Hardware & Energie** > **USV** können Sie den Standby-Modus, USB-USV, SNMP-USV und Synology-USV-Servereinstellungen konfigurieren.

## USB-USV-Unterstützung

USB-USV ist ein Reservestromgerät, das über einen USB-Anschluss mit Ihrem ActiveProtect-Gerät verbunden wird.

Sobald die Installation abgeschlossen ist und das USB-USV-Gerät an das ActiveProtect-Gerät angeschlossen ist, können Sie die USB-USV-Unterstützung aktivieren.

### USB-USV-Unterstützung aktivieren

1. Gehen Sie zu **Systemsteuerung** > **Hardware & Energie** > **USV** und wählen Sie **USV-Unterstützung aktivieren**.
2. Wählen Sie **USB-USV**.
3. Geben Sie die Zeitspanne an, bevor das ActiveProtect-Gerät in den Standby-Modus wechselt.
4. Wenn Sie **USV herunterfahren, wenn das System in den Standby-Modus wechselt** auswählen, wird das ActiveProtect-Gerät bei Stromausfall sofort heruntergefahren. Wir empfehlen Folgendes zu tun:
   - Gehen Sie zu **Systemsteuerung** > **Hardware & Energie** > **Allgemein** und wählen Sie **Automatisch neu starten, wenn das Stromversorgungsproblem behoben ist**, um sicherzustellen, dass das ActiveProtect-Gerät automatisch neu startet, sobald die Stromversorgung wiederhergestellt ist.
   - Bevor Sie die USV verwenden, führen Sie einen Stromausfall-Simulationstest durch, um festzustellen, ob die USV wie erwartet funktioniert. Um den Test durchzuführen, wählen Sie **USV herunterfahren**,

**wenn das System in den Standby-Modus wechselt** und entfernen Sie manuell das Stromkabel des USV-Geräts.

5. Wählen Sie **Netzwerk-USV-Server aktivieren**, wenn das ActiveProtect-Gerät mit einer USB-USV verbunden ist und als Netzwerk-USV-Server dient. Klicken Sie auf **Zugelassene Synology ActiveProtect-Geräte** und geben Sie die Standard-Gateway-IP-Adressen aller Backup-Geräte ein, die Sie erlauben, sich mit dieser USV zu verbinden.
6. Klicken Sie auf **Geräteinformationen**, um Details zum USB-USV-Gerät zu erhalten.
7. Klicken Sie auf **Übernehmen**.

# SNMP-USV-Unterstützung

SNMP-USV ist ein Reservestromgerät, das über SNMP mit Ihrem ActiveProtect-Gerät verbunden wird.[1]

Sobald die SNMP-USV an das ActiveProtect-Gerät angeschlossen und mit demselben Netzwerk verbunden ist, können Sie die SNMP-USV-Unterstützung aktivieren.

## SNMP-USV-Unterstützung aktivieren

1. Gehen Sie zu **Systemsteuerung** > **Hardware & Energie** > **USV** und wählen Sie **USV-Unterstützung aktivieren**.
2. Wählen Sie **SNMP-USV**.
3. Geben Sie die Zeitspanne an, bevor das ActiveProtect-Gerät in den Standby-Modus wechselt.
4. Geben Sie die Informationen für das SNMP-USV-Gerät ein.
5. Wählen Sie **Netzwerk-USV-Server aktivieren**, wenn das ActiveProtect-Gerät über SNMP verbunden ist und als Netzwerk-USV-Server dient. Klicken Sie auf **Zugelassene Synology ActiveProtect-Geräte** und geben Sie die Standard-Gateway-IP-Adressen aller Backup-Geräte ein, die Sie erlauben, sich mit dieser USV zu verbinden.
6. Klicken Sie auf **Übernehmen**.

# Synology-USV-Server

Wenn mehrere ActiveProtect-Geräte USV-Geräte verwenden, erhält nur das über USB-Anschluss oder Netzwerk verbundene Backup-Gerät USV-Statusinformationen. Dieses Backup-Gerät dient als Netzwerk-USV-Server und leitet Informationen an die Client-Backup-Geräte weiter.

Um sicherzustellen, dass USV-Informationen erfolgreich weitergeleitet werden, stellen Sie sicher:

- Alle ActiveProtect-Geräte befinden sich im selben Netzwerk.
- Netzwerkgeräte wie Switches oder Hubs, die mit jedem ActiveProtect-Gerät verbunden sind, sind mit demselben USV-Gerät verbunden.

## Synology USV-Server aktivieren

1. Melden Sie sich beim ActiveProtect-Gerät an, das über USB oder Netzwerk mit dem USV-Gerät verbunden ist.

2. Gehen Sie zu **Systemsteuerung** > **Hardware und Energie** > **USV** und wählen Sie **Netzwerk-USV-Server aktivieren**, um dem ActiveProtect-Gerät zu ermöglichen, USV-Informationen an die Client-Backup-Geräte weiterzuleiten.
3. Klicken Sie auf **Zulässige Synology ActiveProtect-Geräte** und geben Sie die Standard-Gateway-IP-Adressen der Client-Backup-Geräte ein.
4. Klicken Sie auf **Übernehmen**.

## USV-Unterstützung auf dem Client-ActiveProtect-Gerät aktivieren

1. Melden Sie sich beim Client-ActiveProtect-Gerät an.
2. Gehen Sie zu **Systemsteuerung** > **Hardware und Energie** > **USV** und wählen Sie **USV-Unterstützung aktivieren**.
3. Wählen Sie **Synology USV-Server**.
4. Geben Sie die Zeit an, bevor das ActiveProtect-Gerät in den Standby-Modus wechselt.
5. Geben Sie die IP-Adresse des Netzwerk-USV-Servers ein.
6. Klicken Sie auf **Übernehmen**.

### Hinweis:

1. ActiveProtect-Gerät unterstützt SNMPv1-, SNMPv2c- und SNMPv3-USV-Geräte.

# Zusätzliche Hardwareeinstellungen konfigurieren

In **Gerätekonsole** > **Systemsteuerung** > **Hardware und Energie** > **Allgemein** können Sie Speicherkomprimierung, Verhalten nach Stromausfall, Wake on LAN, Signalton-Steuerung, Lüftermodus und LED-Helligkeitssteuerung konfigurieren.

## Speicherkomprimierung

Wenn mehrere Anwendungen laufen, wird die am wenigsten genutzte Daten komprimiert, um die Speichernutzung zu minimieren. Dies verbessert die Systemreaktionsfähigkeit und reduziert die Notwendigkeit, auf Auslagerungsdateien im Speicher zuzugreifen und diese zu ändern.

## Verhalten nach Stromausfall

Wenn das System wegen eines unerwarteten Stromausfalls heruntergefahren wurde, kann die Funktion Wiederherstellung nach Stromausfall das System automatisch hochfahren, nachdem die Stromversorgung wiederhergestellt wurde.

## Wake on LAN

Wenn Wake on LAN (WOL)[1] aktiviert ist, können Sie Ihr ActiveProtect-Gerät über eine IP-Adresse und MAC-Adresse mit WOL-Anwendungen wie Synology Assistant oder ähnlichen Tools aus der Ferne einschalten.

Wake on LAN wird nur aktiviert, wenn das Backup-Gerät ordnungsgemäß heruntergefahren wurde. Zum Herunterfahren können Sie entweder die physische Ein-/Aus-Taste drücken oder zu **Infrastruktur** > **Backup-Server** > **Mehr** > **Herunterfahren** gehen. Denken Sie daran, das Netzkabel nach dem Herunterfahren an eine funktionsfähige Steckdose angeschlossen zu lassen.

## Signalton-Steuerung

Wenn bestimmte Ereignisse oder Fehler auftreten, gibt das ActiveProtect-Gerät einen Signalton aus, um Sie zu benachrichtigen. Sie können anpassen, welche Ereignisse diese Warnungen auslösen und sie deaktivieren, wenn sie auftreten.

## Lüftermodus

Die folgenden Lüftermodi[2] sind verfügbar:

| Lüftermodus | Details |
| --- | --- |
| Modus Volle Geschwindigkeit | Der Lüfter arbeitet mit voller Geschwindigkeit, was das ActiveProtect-Gerät kühler hält, aber mehr Lärm erzeugt |
| Kühlmodus | Der Lüfter arbeitet mit höherer Geschwindigkeit, was das ActiveProtect-Gerät kühler hält, aber mehr Lärm erzeugt. |
| Stiller Modus | Der Lüfter arbeitet mit geringerer Geschwindigkeit und erzeugt weniger Lärm, aber das ActiveProtect-Gerät könnte wärmer werden. |
| Energiesparmodus | Der Lüfter arbeitet mit geringerer Geschwindigkeit und erzeugt weniger Lärm, aber das ActiveProtect-Gerät könnte wärmer werden. Wenn das ActiveProtect-Gerät kühl ist, wird der Lüfter stoppen, um Energie zu sparen. Der Energiesparmodus ist nur bei bestimmten Modellen verfügbar. |

# LED-Helligkeitssteuerung

Sie können die Helligkeit der LED-Anzeigen wie Ein/Aus und Laufwerkstatus auf Ihrem ActiveProtect-Gerät anpassen.

## LED-Helligkeit nach Zeitplan anpassen

1. Gehen Sie zu **LED-Helligkeitssteuerung** > **Zeitplan festlegen**.
2. Klicken Sie auf eine Helligkeitsoption:
   - **Standardhelligkeit**: LED-Anzeigen sind standardmäßig auf die höchste Helligkeitsstufe eingestellt.
   - **Angepasste Helligkeit**: Die Helligkeitsstufe, die über den Schieberegler festgelegt wird.
   - **Aus**: LED-Anzeigen sind ausgeschaltet.
3. Klicken Sie auf die Zeitfenster in der Tabelle, um die Helligkeitsstufe zu bestimmten Zeiten des Tages anzupassen.

**Hinweis:**

1. WOL wird von 10GbE-LAN-Ports nicht unterstützt.
2. Der Lüftermodus steuert nur die Lüfter in Ihrem ActiveProtect-Gerät. Wenn Ihr Backup-Gerät über ein Netzteil verfügt, werden die Einstellungen der Netzteillüfter separat über das Netzteil gesteuert.

# Regionale Einstellungen

In **Gerätekonsole** > **Systemsteuerung** > **Regionale Optionen** können Sie die Datums-, Zeit- und Spracheinstellungen für Ihr ActiveProtect-Gerät ändern.

## Datums- und Zeiteinstellungen

In **Gerätekonsole** > **Systemsteuerung** > **Regionale Optionen** > **Uhrzeit** können Sie die Datums- und Zeiteinstellungen Ihres Backup-Geräts anzeigen und anpassen und wählen, ob Sie das Datum und die Uhrzeit manuell oder automatisch mit einem NTP (Network Time Protocol) Server einstellen möchten.

### Datums- und Zeiteinstellungen festlegen

Gehen Sie zu **Datum & Uhrzeit** und **Zeitzone**, um die folgenden Einstellungen anzupassen:

- Datumsformat
- Zeitformat
- Zeitzone

### Datum und Uhrzeit manuell einstellen

1. Gehen Sie zu **Zeiteinstellung** und wählen Sie **Manuell**.
2. Stellen Sie das Datum und die Uhrzeit ein.

### Datum und Uhrzeit automatisch über einen NTP-Server synchronisieren

1. Gehen Sie zu **Zeiteinstellung** und wählen Sie **Mit NTP-Server synchronisieren**.
2. Geben Sie die Adresse Ihres NTP-Servers ein oder wählen Sie einen aus der Liste.
3. Klicken Sie auf **Jetzt aktualisieren**, um zu überprüfen, ob Ihr ActiveProtect-Gerät erfolgreich mit dem NTP-Server synchronisieren kann.
4. Klicken Sie auf **Übernehmen**.

## Spracheinstellungen

In **Systemsteuerung** > **Regionale Optionen** > **Sprache** können Sie Ihre bevorzugte Sprache für die ActiveProtect Manager (APM) Oberfläche und die Anwendungs-Codepage auswählen.

### Anzeigesprache

Sie können Ihre bevorzugte Anzeigesprache auswählen oder sie so einstellen, dass sie mit der Standardsprache Ihres Browsers übereinstimmt.

## Codepage

Für Anwendungen, die Nicht-Unicode-Zeichenfolgen in Unicode umwandeln, wie z. B. den FTP-Dienst und die UPnP-Unterstützung, müssen Sie die passende Codepage aus der Liste auswählen.

### Hinweis:

- Um die Spracheinstellungen für E-Mail-Benachrichtigungen zu konfigurieren, klicken Sie auf das Hauptmenüsymbol und gehen Sie zu **Verwaltungscenter** > **Systemeinstellungen** > **Benachrichtigungen** > **Benachrichtigungssprache**.

# Ressourcenmonitor

Gehen Sie zur **Gerätekonsole** > **Ressourcenmonitor**, um die Daten zur Ressourcennutzung anzuzeigen. Detaillierte Angaben zu Datum, Uhrzeit und Informationen im Diagramm werden bei Mouseover angezeigt.

Auf der Registerkarte **Überblick** werden Diagramme für **CPU**, **Arbeitsspeicher**, **Netzwerk**, **Festplatte**, **Volume**, **LUN** und **NFS** angezeigt.

## CPU

Sie können die gesamte CPU-Auslastung unter **Benutzer**, **System** und **I/O Warten** anzeigen. Die CPU-Auslastung könnte hoch sein, wenn der **Ressourcenmonitor** das erste Mal gestartet wird, da das System seine Ressourcendaten sammeln und gleichzeitig die UI-Seite laden muss.

| Typ | Beschreibung |
|---|---|
| Benutzer | Zeigt den Prozentsatz der CPU an, der für die Ausführung von Benutzeranwendungen verwendet wird. |
| System | Zeigt den Prozentsatz der CPU an, der im Kern des Systems, Hardware/Software-IRQs verwendet wird. |
| I/O Warten | Zeigt den Prozentsatz der CPU an, wenn sie im Leerlauf ist und von keinem Programm verwendet wird. |
| Auslastung | Ist die Summe der CPU-Auslastung von **Benutzer** und **System**. |

Die **Durchschnittsleistung** zeigt die Länge der Ausführungswarteschlange (d. h. die Summe der Anzahl der Prozesse, die derzeit ausgeführt werden, plus der Anzahl der wartenden Prozesse) innerhalb von 1, 5 und 15 Minuten an.

## Arbeitsspeicher

Sie können die gesamte Speichernutzung des physischen Speichers und des Auslagerungsspeichers anzeigen. Eine hohe Speicherauslastung ist auf häufiges Zwischenspeichern von Daten zurückzuführen, was eine schnelle Abfrage ohne Zugriff auf die Festplatte ermöglicht. Der Zwischenspeicher wird freigegeben, wenn der Gesamtspeicher nicht ausreicht.

Eine hohe Auslastung des Auslagerungsspeichers weist auf unzureichenden Systemspeicher hin und wirkt sich auch auf die Systemleistung aus. Sie können die Rate von Swap-In und Swap-Out anzeigen, indem Sie den Typ auf **Swap** ändern.

## Netzwerk

Sie können die gesendeten und empfangenen Daten in KB pro Sekunde anzeigen.

## Festplatte

Sie können die gesamte Festplattennutzung, den Durchsatz oder IOPS anzeigen. Durch Klicken auf **Benutzerdefinierte Ansicht** können Sie auswählen, welche Festplatten in das Diagramm aufgenommen werden sollen.

## Volume

Sie können den gesamten Übertragungsstatus von Volumes, die Übertragungsauslastung, den Lese-/Schreibdurchsatz oder IOPS anzeigen. Durch Klicken auf **Benutzerdefinierte Ansicht** können Sie auswählen, welche Volumes in das Diagramm aufgenommen werden sollen.

## LUN

Bei der Durchführung von Sofortwiederherstellungen von virtuellen Maschinen auf den integrierten Hypervisor und auf Hyper-V können Sie den aktuellen Status aller laufenden iSCSI LUNs oder den Status eines bestimmten LUN anzeigen. Drei Diagramme werden standardmäßig angezeigt: **Lese-/Schreibdurchsatz**, **IOPS** und **Latenz**. Für detailliertere Informationen klicken Sie auf die Schaltfläche **Diagramme auswählen**.

## NFS

Bei der Durchführung von Sofortwiederherstellungen von virtuellen Maschinen auf VMware können Sie den Gesamtstatus des NFS-Dienstes anzeigen, einschließlich der **Lese-/Schreib-IOPS** und **Latenz**-Status.

# Info-Center

Gehen Sie zu **Systemsteuerung** > **Info-Center**, um grundlegende Informationen zu verschiedenen Aspekten Ihres ActiveProtect-Gerätsystems anzuzeigen, wie z.B. Hardwarespezifikationen, Netzwerk, Speicher und Dienste.

## Allgemein

Auf der Registerkarte **Allgemein** werden grundlegende Informationen zu Ihrem ActiveProtect-Gerät angezeigt, wie Seriennummer, Modellname, Größe des physischen Speichers, APM-Version, Zeitinformationen und Systemtemperaturstatus.

### Systemtemperaturstatus

Der Systemtemperaturstatus des ActiveProtect-Geräts wird durch grüne oder orange Lichter angezeigt.

- **Grün**: Die Systemtemperatur ist normal.
- **Orange**: Die Temperatur des ActiveProtect-Geräts ist zu hoch. Wenn das Überhitzungsproblem weiterhin besteht, kann Ihr Gerät herunterfahren, um Hardwarefehler zu vermeiden.

## Netzwerk

Die Registerkarte **Netzwerk** zeigt Netzwerkinformationen wie DNS-Server, IP-Adresse und Subnetz-Maske an.

## Speicher

Die Registerkarte **Speicher** zeigt Informationen zum Laufwerkstatus an.

### Status

Es gibt die folgenden möglichen Statusarten eines Laufwerks:

- **Gesund**: Dieses Laufwerk ist in gutem Zustand, oder Warnungen dafür wurden unterdrückt oder deaktiviert.
- **Kritisch**: Auf diesem Laufwerk sind ein oder mehrere der folgenden kritischen Probleme aufgetreten:
  - Kritische Fehler
  - Nur-Lese-Modus
  - Erreichen der Grenze der SSD-Ausdauer
- **Systempartition ausgefallen**: Das System kann nicht auf die Partitionen dieses Laufwerks zugreifen.
- **Erkannt**: Ein Laufwerk mit Speicherpooldaten wurde erkannt. Es wurde jedoch kein Speicherpool zugewiesen.

- **Nicht erkannt**: Das Laufwerk ist nicht mit Ihrem ActiveProtect-Gerät kompatibel.
- **Firmware-Aktualisierung erforderlich**: Auf diesem Laufwerk sind ein oder mehrere Probleme aufgetreten, die mit einer Firmware-Aktualisierung behoben werden können.
- **Deaktiviert**: Dieses Laufwerk ist deaktiviert.

Weitere Informationen zur Fehlerbehebung bei Laufwerksproblemen finden Sie unter Systemspeicher verwalten.

## Dienst

Auf der Registerkarte **Dienst** werden nur Dienste angezeigt, die für das ActiveProtect-Gerät aktiviert sind, um sicherzustellen, dass alle Dienste und Funktionen ordnungsgemäß funktionieren. Wenn das ActiveProtect-Gerät in einem privaten Netzwerk eingesetzt wird, stellen Sie sicher, dass diese Dienstports zugänglich sind und richten Sie die richtige Portweiterleitung für diese Dienste auf Ihrem Router ein.

## Geräteanalyse

Auf der Registerkarte **Geräteanalyse** können Sie Folgendes tun:

- **Aktivieren Sie das Senden von Geräteanalysen**, um Synology zu erlauben, Ihre Daten zu sammeln, um die Benutzererfahrung zu verbessern.
- **Erlauben Sie, dass dieses Synology ActiveProtect-Gerät im Web Assistant angezeigt wird**, um Ihr Synology-Gerät im lokalen Netzwerk zu lokalisieren.

# Support-Center

Wenn Sie Unterstützung benötigen, bietet das Synology Support-Center einen direkten, schnell reagierenden Support-Kanal, der mit erfahrenen technischen Support-Ingenieuren besetzt ist. Sie können ein technisches Support-Ticket einreichen, um Hilfe für Ihr ActiveProtect-Gerät zu erhalten oder den Synology Support-Ingenieuren zu erlauben, eine Ferndiagnose durchzuführen.

## Support kontaktieren

Das Synology Support-Center ist Ihre vertrauenswürdige Ressource zur Behebung von Problemen mit Ihrem Synology ActiveProtect-Gerät während der Garantiezeit des Produkts. Unser Team ist hier, um die Leistung Ihres ActiveProtect-Geräts zu erhalten und zu optimieren. Um Unterstützung zu erhalten, gehen Sie zu **Support-Center** > **Support kontaktieren** und reichen Sie ein Support-Ticket ein.

### Bevor Sie ein neues Support-Ticket erstellen:

- Um Zeit zu sparen, empfehlen wir Ihnen, das Wissenszentrum zu durchsuchen, bevor Sie ein neues Support-Ticket erstellen, da Ihre Frage wahrscheinlich bereits gestellt wurde und es einen bestehenden Artikel gibt, der das Problem behandelt.
- Sie müssen sich bei Ihrem Synology-Konto anmelden, um ein neues Support-Ticket von der Geräte-Konsole aus zu erstellen.
- Alle Pflichtfelder im neuen Support-Ticket müssen ausgefüllt werden.
- Um Missverständnisse zu vermeiden, reichen Sie das Support-Ticket bitte in Englisch oder Chinesisch ein.

### Tipps für das Erstellen eines neuen Support-Tickets:

- Beschreiben Sie das Problem, das Sie melden, und geben Sie alle Schritte an, die Sie unternommen haben, um das Problem selbst zu beheben. Geben Sie Details an, die den Synology Support-Ingenieuren helfen, das Problem zu verstehen. Falls möglich, geben Sie nummerierte Schritte inklusive Screenshots an, um das Problem zu reproduzieren.
- Unser Support-System entfernt Anhänge, die größer als 200 MB sind.
- Gehen Sie zu **Support-Center** > **Support-Dienste** und aktivieren Sie den **Diagnosedienst**, um die Diagnosedaten Ihres Synology ActiveProtect-Geräts automatisch zu übermitteln, wenn Sie ein Support-Ticket einreichen. Dies kann den Fehlerbehebungsprozess erleichtern.

### Was Sie nach dem Senden eines Support-Tickets erwarten können:

- Ein Synology Support-Ingenieur wird sich kurz nach dem Senden des Support-Tickets mit Ihnen in Verbindung setzen.
- Falls Sie nichts von uns hören, ist es sehr wichtig, dass Sie sicherstellen, dass diese E-Mails nicht durch Sicherheitssoftware auf Ihrem Computer oder in Ihrem Netzwerk blockiert werden.

- Jedes Support-Ticket hat eine eindeutige ID, die im Betreff der als Antwort auf das Support-Ticket gesendeten E-Mails zu finden ist.
- Unsere Support-Ingenieure können Sie bitten, Protokolle zu erstellen von Ihrem ActiveProtect-Gerät oder Fernzugriff zu aktivieren, um weitere Diagnosen von einem Synology-Büro aus durchzuführen.

## Protokolle erstellen

Sie können den Synology Support-Ingenieuren Protokolle von Ihrem Synology ActiveProtect-Gerät zur Verfügung stellen.

Gehen Sie zu **Support-Center** > **Support-Dienste** > **Protokollerstellung** und klicken Sie auf **Protokolle erstellen**. Der Download wird in wenigen Minuten abgeschlossen sein.

**Hinweis:**

- Die Protokolle Ihres Synology ActiveProtect-Geräts werden ausschließlich für Systemdiagnosen verwendet. Synology wird auf keine anderen persönlichen Informationen auf Ihrem Synology ActiveProtect-Gerät zugreifen oder diese offenlegen. Weitere Informationen finden Sie in unserer Offenlegung zur Datensammlung in Diensten.

## Fernzugriff aktivieren

Gehen Sie zu **Support-Center** > **Support-Dienste** > **Fernzugriff** und **Fernzugriff aktivieren**, um den Synology Support-Ingenieuren den Fernzugriff auf Ihr Synology ActiveProtect-Gerät zu ermöglichen. Ein zufälliges Konto wird für den Zugriff generiert.

Aktivieren Sie den Fernzugriff nur, wenn Sie von den Synology Support-Ingenieuren dazu aufgefordert werden.

**Hinweis:**

- Der Fernzugriff wird nach 14 Tagen automatisch deaktiviert. Er sollte bis dahin nicht manuell deaktiviert werden, es sei denn, ein Synology Support-Ingenieur fordert Sie dazu auf.
- Entfernen Sie alle Inhalte von Ihrem Synology ActiveProtect-Gerät, die Sie als privat betrachten.
- Obwohl Synology nicht garantieren kann, dass die Bereitstellung des Fernzugriffs Ihr Problem lösen wird, wird Synology angemessene Anstrengungen unternehmen, um die Support-Dienste professionell durchzuführen.

# Out-of-Band-Management

Out-of-Band (OOB) Management ermöglicht es Ihnen, sicher mit Ihrem ActiveProtect-Gerät zu verbinden und wesentliche Hardware-Operationen bei einem Geräteausfall auszuführen. Dies erfolgt über einen dedizierten LAN-Port, bekannt als **LAN-Verwaltung (Out-of-Band)**-Port, und einen SSH/Telnet-Client. Auf dieser Konsole sind die folgenden grundlegenden Hardware-Operationen verfügbar: Gerät ein-/ausschalten oder neu starten, Systemprotokolle in Echtzeit überwachen, frühere Systemprotokolle anzeigen und Gerät zurücksetzen.

## Zugriff auf die Out-of-Band-Management-Konsole

Um auf die Out-of-Band-Management-Konsole zuzugreifen, müssen Sie einen SSH-Client verwenden und eine sichere und authentifizierte SSH-Verbindung zum ActiveProtect-Gerät herstellen. Die folgenden Schritte gelten für die PuTTY-Anwendung. Die Methoden gelten jedoch für jeden SSH-Client, den Sie bevorzugen.

1. Geben Sie die statische IP des LAN-Verwaltungsports und die dedizierte Portnummer 57 ein, um eine Verbindung zur Out-of-Band-Management-Konsole herzustellen.
2. Wählen Sie **SSH (Standard)** als Verbindungstyp und klicken Sie auf **Öffnen**.
3. Geben Sie den Benutzernamen und das Passwort des **Super-Admins** ein und klicken Sie dann auf **Eingabe**.
4. Sobald die Authentifizierung erfolgt ist, geben Sie die entsprechende Nummer ein, um die gewünschte Aktion auszuführen.

**Hinweis:**

- Beachten Sie, dass jeweils nur eine SSH-/Telnet-Client-Verbindung erlaubt ist. Neue Sitzungen beenden die bestehende Sitzung (falls vorhanden).
- Um die Sicherheit Ihres ActiveProtect-Geräts zu gewährleisten, blockiert das System die IP-Adressen nach 10 fehlgeschlagenen Anmeldeversuchen bei der Konsole innerhalb von 5 Minuten. Um die Sperrliste zu löschen, gehen Sie zu **Systemsteuerung** > **Netzwerk** > **Netzwerkschnittstelle** und wählen Sie die LAN-Verwaltungsschnittstelle aus. Klicken Sie auf **Bearbeiten** und öffnen Sie die **Sperrliste** unter dem Tab **Out-of-Band-Management**.

## Verfügbare Konsolenaktionen

| Befehl | Aktion | Beschreibung |
|---|---|---|
| 1 | System zwangsweise neu starten | Simulieren Sie ein erzwungenes Herunterfahren des Geräts und schalten Sie es automatisch wieder ein.<br>Dies wird nicht empfohlen und sollte nur verwendet werden, wenn das System vollständig nicht reagiert. |

| | | |
|---|---|---|
| 2 | System ausschalten (normales Herunterfahren) | Simulieren Sie das Drücken der Ein/Aus-Taste einmal. |
| 3 | System ausschalten (hartes Herunterfahren) | Simulieren Sie das Drücken und Halten der **Ein/Aus**-Taste, bis Sie einen Piepton hören. Die Stromversorgung der Hardware des Geräts wird sofort unterbrochen.<br>Diese Option ist eine gewaltsame Methode, das System herunterzufahren, und wird nicht empfohlen, es sei denn, das System reagiert überhaupt nicht. |
| 4 | System einschalten | Gerät einschalten. |
| 5 | Echtzeit-Systemprotokolle überwachen | Echtzeit-**APM**-Systemprotokolle in der Out-of-Band (OOB)-Management-Konsole ausgeben.<br>Wenn Daten fehlen, können Sie diese jederzeit mit der Funktion (**6**) **Historische Systemprotokolle ausgeben** sammeln. |
| 6 | Historische Systemprotokolle ausgeben | Frühere und aktuelle historische APM-Systemprotokolle in der Out-of-Band (OOB)-Management-Konsole ausgeben. |
| 7 | Erweiterte Optionen | 1. Historische Out-of-Band-Management-Konsolenprotokolle ausgeben: Die Out-of-Band (OOB) Management-Konsole gibt alle historischen OOB-Management-Systemprotokolle aus.<br>2. System zurücksetzen (beeinträchtigt nicht die Daten): Gerät zurücksetzen (Reset-Modus 2) und das System neu installieren.<br>3. Zurück zum Hauptmenü. |
| 8 | Abmelden | Von der Out-of-Band-Management-Konsole abmelden. |