

ActiveProtect Handbuch zur Bereitstellung des Netzwerks

Synology

Inhaltsverzeichnis

Einführung	3
Trennung von Management-Datenverkehr und Sicherungs-/Wiederherstellungsdatenverkehr	3
Trennung von Sicherungs- und DR-Replikationsdatenverkehr	4
Trennung von Sicherungs- und Wiederherstellungsdatenverkehr vom Produktionsdatenverkehr	5
Netzwerktopologien	6
Kleine und mittelständische Unternehmen	6
Unternehmensumgebungen	7
Personal Computer und physische Server	11
Verbindungsübersicht	11
Netzwerkports zulassen	12
Dediziertes Netzwerk angeben	12
Backup-Bandbreite steuern	15
VMware vSphere	16
Verbindungsübersicht	16
Netzwerkports zulassen	16
Dediziertes Netzwerk festlegen	17
Backup-Bandbreite steuern	19
Microsoft Hyper-V	20
Verbindungsübersicht	20
Netzwerkports zulassen	20
Dediziertes Netzwerk festlegen	21
Sicherungsbandbreite steuern	21
Proxmox VE	22
Verbindungsübersicht	22
Netzwerkports zulassen	23
Dediziertes Netzwerk festlegen	23
Backup-Bandbreite steuern	25
Nutanix AHV	26
Verbindungsübersicht	26
Netzwerkports zulassen	26
Dediziertes Netzwerk angeben	26
Backup-Bandbreite steuern	27
Cloud-VMs	28
Datenverkehr über das Internet leiten	28

Datenverkehr über ein privates Netzwerk leiten	29
Netzwerkports und Domains zulassen	29
Dateiserver	31
Verbindungsübersicht	31
Netzwerk-Ports zulassen	31
Ein dediziertes Netzwerk angeben	31
Sicherungsbandbreite steuern	32
Microsoft 365	33
Verbindungsübersicht	33
Netzwerkports und Domains zulassen	33
Ein dediziertes Netzwerk festlegen	33
Sicherungsbandbreite steuern	34
Google Workspace	35
Verbindungsübersicht	35
Netzwerkports und Domains zulassen	35
Ein dediziertes Netzwerk festlegen	35
Sicherungsbandbreite steuern	36
Sicherungskopie	37
Verbindungsübersicht	37
Dediziertes Netzwerk festlegen	37
Sicherungsbandbreite steuern	37
Air-Gap-Umgebung	38
Backup-Kopierserver in einer isolierten Zone bereitstellen	38

Einführung

Dieser Leitfaden beschreibt die Netzwerkarchitektur von ActiveProtect für Standortverwaltung, Datensicherungen und Sicherungskopien und stellt Strategien zur Netzwerksegmentierung vor, um Datenverkehr zu isolieren, die Sicherheit zu erhöhen und die Systemleistung zu verbessern.

Ein ActiveProtect-System umfasst die folgenden Arten von Netzwerkverkehr:

- Management- und Steuerungsdatenverkehr
- Sicherungs- und Wiederherstellungsdatenverkehr
- Sicherungskopien- und Disaster Recovery (DR)-Replikationsdatenverkehr

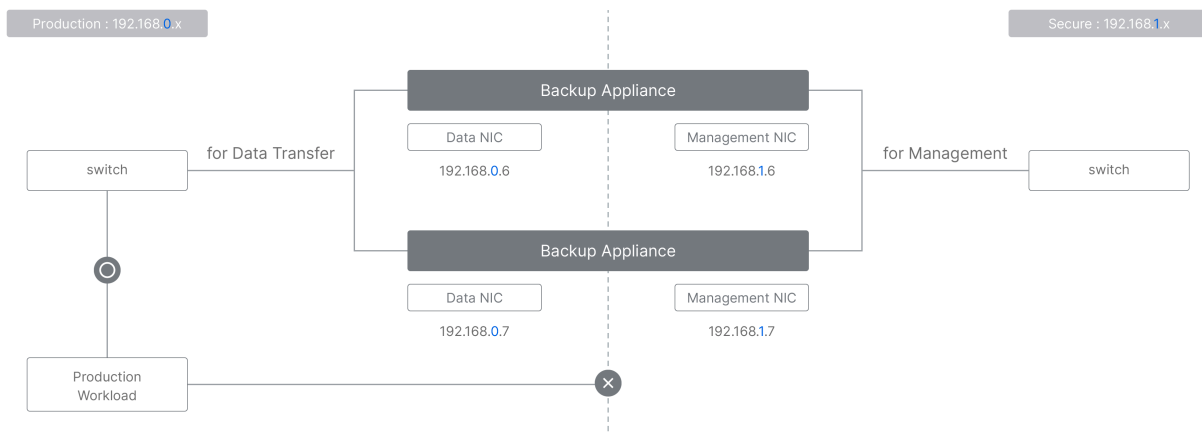
Trennung von Management-Datenverkehr und Sicherungs-/Wiederherstellungsdatenverkehr

ActiveProtect-Geräte bieten zwei Arten von Netzwerkschnittstellen: eine Management-Schnittstelle für die Systemverwaltung und eine oder mehrere Datenschnittstellen für die Übertragung von Sicherungsdaten. Informationen zu Modellen, die mehrere Datenschnittstellen unterstützen, finden Sie in den [Produktspezifikationen](#).

Netzwerkschnittstelle	Funktionen
Management-Schnittstelle	• Dient standardmäßig zur Verwaltung eines ActiveProtect-Systems. • Zugriff auf Verwaltungszentrum und Gerätekonsole. • Stellt bei der Hinzufügung von Sicherungsservern zu Systemen initiale Authentifizierungsverbindungen zu Systemen her und synchronisiert Ereignisse zwischen Verwaltungsserver und Sicherungsservern. • Bietet Out-of-Band (OOB)-Management.
Daten-Schnittstelle	• Dient der Datenübertragung während Sicherungen, Sicherungskopien und Wiederherstellungen. • Zugriff auf das Wiederherstellungsportal.

Um diese Schnittstellen optimal zu nutzen und eine sichere Verwaltungsumgebung zu gewährleisten, empfehlen wir, sie verschiedenen Netzwerksegmenten zuzuweisen. Setzen Sie die Management-Schnittstelle in einem isolierten Netzwerk ein, um administrative und

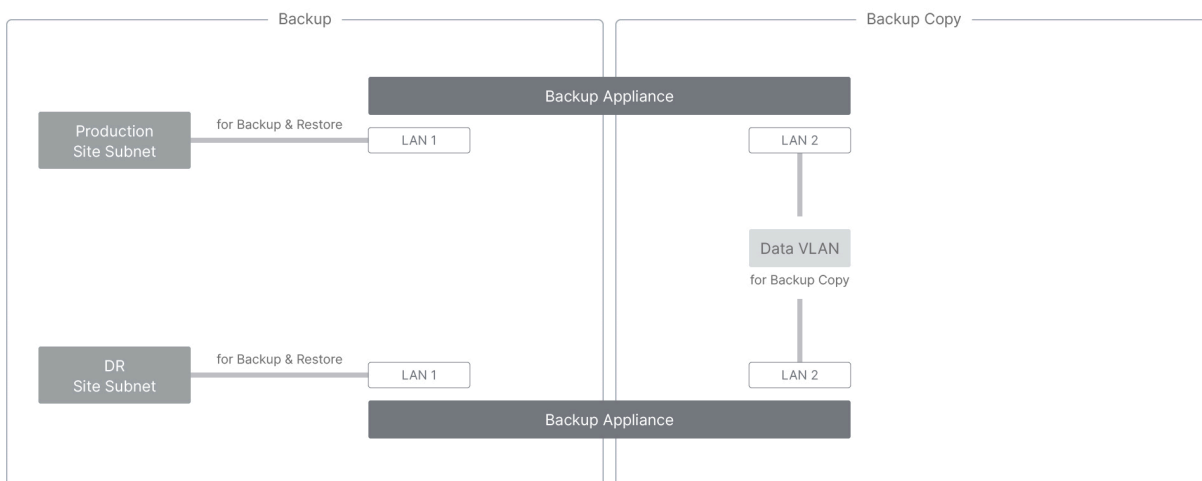
Steuerungsaufgaben zu schützen, und verbinden Sie die Daten-Schnittstelle mit der Arbeitsumgebung, damit Sicherungs- und Wiederherstellungsvorgänge korrekt ausgeführt werden.



Trennung von Sicherungs- und DR-Replikationsdatenverkehr

Bei Modellen, die mehrere Datenschnittstellen unterstützen, können Sie den Datenverkehr nach Typ auf verschiedene Netzwerksegmente aufteilen. So lässt sich Sicherungsdatenverkehr von externen Aktivitäten wie Sicherungskopien und DR-Replikation isolieren, wodurch eine stabile Übertragungsleistung gewährleistet wird.

Sicherungskopien- und DR-Replikationsdatenverkehr umfasst in der Regel Langstreckenübertragungen mit hoher Latenz und kann Sicherheitsgrenzen überschreiten. Solcher Datenverkehr ist häufiger von Firewalls, NAT-Geräten, ISP-Überlastungen oder Leerlauf-Timeouts betroffen. Die Nutzung eines separaten Pfads für die Replikation ermöglicht es zudem, Bandbreitenlimits für Sicherungskopien festzulegen, ohne lokale Sicherungen oder die Produktionsumgebung zu beeinträchtigen.



Nachdem der Datenverkehr getrennt wurde, können Sie Bandbreitenlimits speziell für Sicherungskopien-Übertragungen konfigurieren. Ausführliche Anweisungen finden Sie unter [Sicherungskopie](#).

Trennung von Sicherungs- und Wiederherstellungsdatenverkehr vom Produktionsdatenverkehr

Die Trennung von Sicherungs- und Wiederherstellungsdatenverkehr vom Produktionsnetzwerk trägt dazu bei, die Performance der Produktion aufrechtzuerhalten und die RTO-Anforderungen zu erfüllen. Ein dediziertes Sicherungs- und Wiederherstellungsnetzwerk verhindert außerdem, dass Wiederherstellungsvorgänge die Produktionssysteme beeinträchtigen, und ermöglicht es, für Sicherungs- und Wiederherstellungsdatenverkehr 10GbE-Verbindungen für höhere Durchsatzraten zu nutzen.

Im folgenden Kapitel stellen wir empfohlene Netzwerktopologien für verschiedene Bereitstellungsgrößen vor und erklären, wie Sie diese Bereitstellungsstrategien in der Praxis anwenden.

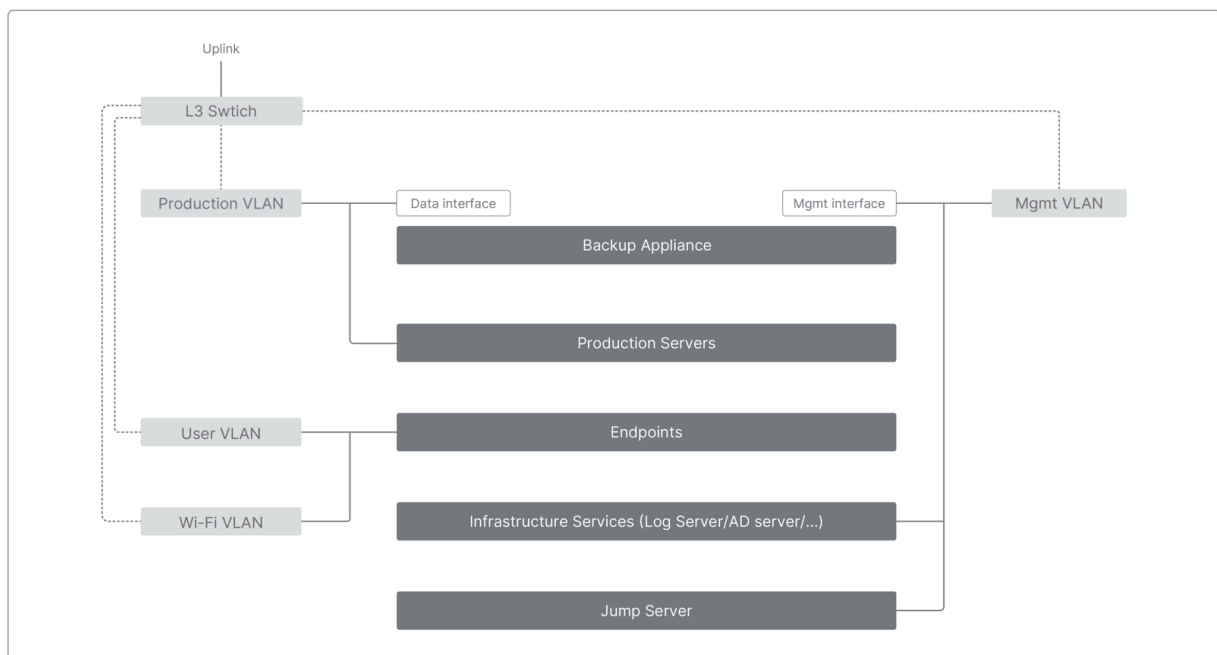
Netzwerktopologien

Die Netzwerkarchitektur sollte die Größe und Komplexität Ihrer Organisation widerspiegeln. Kleine Implementierungen konzentrieren sich in der Regel auf eine einfache Verwaltung, während Unternehmensumgebungen strengere Sicherheitskontrollen und eine Segmentierung der Infrastruktur erfordern, einschließlich der Einhaltung von Rahmenwerken wie NIS2.

Kleine und mittelständische Unternehmen

In SMB-Umgebungen besteht das Hauptziel darin, Verwaltungsdatenverkehr von Nutzdatenverkehr zu trennen und gleichzeitig sowohl lokale Sicherungen als auch Cloud-Sicherungskopien zu unterstützen. Eine einfache Möglichkeit, dies zu erreichen, ist der Einsatz eines Layer-3-(L3)-Switches mit separaten VLANs.

Die folgende Abbildung zeigt unsere empfohlene Netzwerktopologie:



Appliance-Schnittstellenverbindungen

- **Daten-Schnittstelle:** Verbindet sich mit dem Produktions-VLAN. Diese Schnittstelle empfängt Sicherungsdatenverkehr von Produktionsservern und Endgeräten und leitet Sicherungskopien über den L3-Switch an Cloud-Objektspeicher weiter.
- **Management-Schnittstelle:** Verbindet sich mit dem Management-VLAN und überträgt ausschließlich administrativen Datenverkehr. Das VLAN beherbergt Infrastrukturdienste wie Protokollserver, Verzeichnisdienste und Jump-Server.

Firewall- und Zugriffskontrollregeln

Um lokale und Cloud-Umgebungen abzusichern, konfigurieren Sie die folgenden Regeln auf Ihrem L3-Switch und Ihrer Edge-Firewall wie folgt:

- **Produktions-VLAN:** Beschränken Sie den Zugriff nach dem **Least-Privilege**-Prinzip. Erlauben Sie Endgeräten im User-VLAN und User-Wi-Fi-VLAN den Zugriff auf die Daten-Schnittstelle ausschließlich über TCP 8443 und blockieren Sie allen anderen eingehenden Datenverkehr.
- **Management-VLAN:** Wenden Sie einen **Zero-Trust**-Ansatz an, indem Sie sämtlichen Datenverkehr aus dem User- und Produktions-VLAN blockieren. Administrativer Zugriff sollte nur über einen Jump-Server auf bestimmten Ports wie 443 (HTTPS) und 22 (SSH) erlaubt werden.

Die integrierte Firewall von ActiveProtect beschränkt den Datenverkehr bereits auf die für Sicherungen benötigten Ports, sodass für Verbindungen innerhalb desselben VLANs keine zusätzlichen Blockierungsregeln auf dem Switch erforderlich sind.

Bandbreitenkontrolle

Internet- und interne WLAN-Bandbreite sind in SMB-Umgebungen wichtige gemeinsam genutzte Ressourcen. Wir empfehlen, Bandbreitenbeschränkungen für die folgenden Szenarien zu konfigurieren:

- **Cloud-Sicherungskopien:** Der Sicherungskopien-Datenverkehr nutzt die Unternehmens-Internetverbindung. Um eine übermäßige Nutzung der ausgehenden Bandbreite zu verhindern, [konfigurieren Sie Bandbreitenbeschränkungen](#) für den zum Internet gesendeten Datenverkehr.
- **Endgeräte-Sicherungen:** Umfangreiche Sicherungen von Mitarbeiter-Laptops über WLAN können die drahtlose Leistung beeinträchtigen. Legen Sie eingehende Datenverkehrsbeschränkungen für das User-Wi-Fi-VLAN fest oder wenden Sie Geschwindigkeitsbegrenzungen in den ActiveProtect-Agent-Einstellungen an. [Mehr erfahren](#)

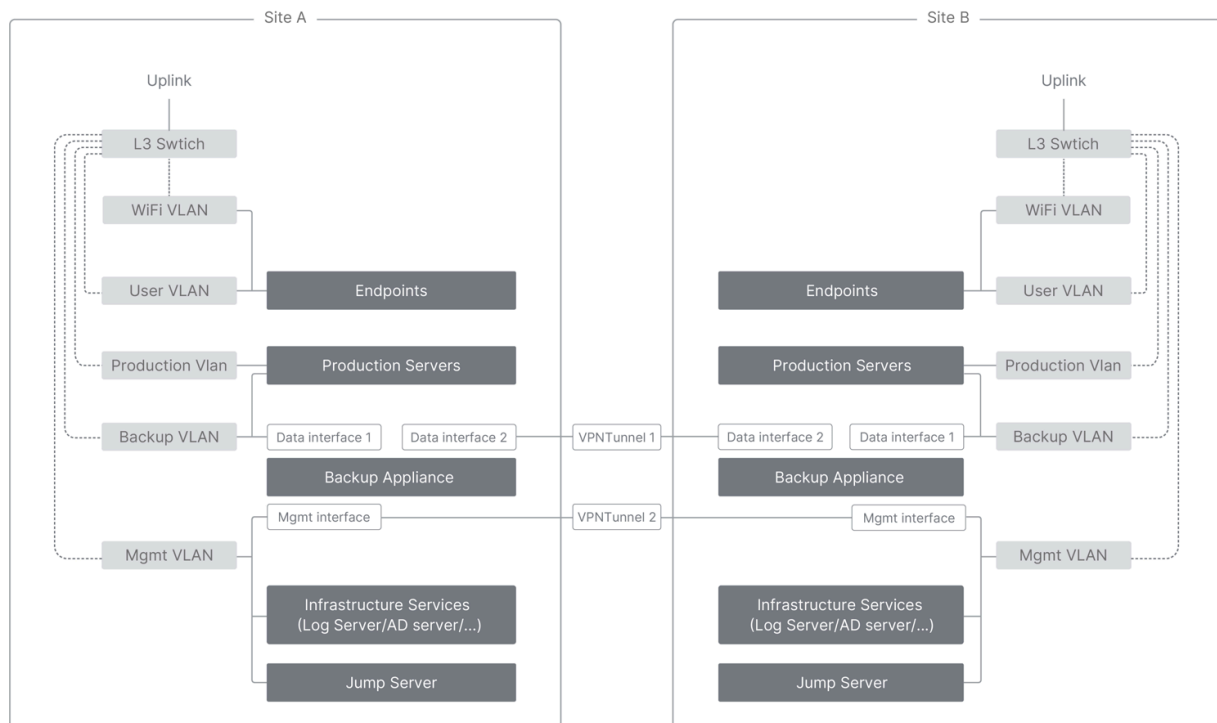
Hinweise:

- Wenn Produktions- und Sicherungsdatenverkehr unterschiedliche Netzwerkschnittstellen verwenden müssen, lesen Sie die arbeitslastspezifischen Anleitungen in den nächsten Kapiteln.

Unternehmensumgebungen

Unternehmen mit strengen Compliance-Anforderungen (wie NIS2) müssen das Least-Privilege-Prinzip durchsetzen und eine physische/logische Netzwerktrennung implementieren. VLAN-übergreifender Datenverkehr sollte durch einen L3-Switch oder eine Firewall gesteuert werden, um Management-, Sicherungs- und Sicherungskopien-Datenverkehr zu trennen.

Die folgende Abbildung zeigt unsere empfohlene Netzwerktopologie:



Appliance-Schnittstellenverbindungen

- **Daten-Schnittstelle 1 (Sicherung):** Verbindet sich mit einem dedizierten Backup-VLAN und verarbeitet Sicherungs- und Wiederherstellungsdatenverkehr für lokale Produktionsserver und Endgeräte.
- **Daten-Schnittstelle 2 (Standortübergreifende Sicherungskopien):** Verbindet sich mit einem dedizierten Replikations-VLAN, das ausschließlich für Sicherungskopien-Datenverkehr zwischen Standorten verwendet wird. Um zu verhindern, dass Sicherungskopien-Aufgaben mit dem täglichen Sicherungsdatenverkehr konkurrieren, halten Sie diese Schnittstelle vom Backup-VLAN getrennt. Erfahren Sie mehr darüber, wie Sie [einen festen Pfad für Sicherungskopien-Datenverkehr festlegen](#).
- **Management-Schnittstelle:** Verbindet sich mit dem Management-VLAN und überträgt ausschließlich administrativen Datenverkehr. Das VLAN beherbergt Infrastrukturdienste wie Protokollserver, Verzeichnisdienste und Jump-Server.

Hinweise:

- In einer typischen Bereitstellung ist das Replikations-VLAN mit dem L3-Switch verbunden, der den Datenverkehr an ein VPN-Gateway zur Verschlüsselung und Übertragung an den entfernten Standort weiterleitet.

Firewall- und Zugriffskontrollregeln

Wenn alle VLANs physisch mit demselben L3-Switch verbunden sind, empfehlen wir, strenge Datenverkehrskontrollen zwischen den Netzwerksegmenten durch Firewall-Regeln und ACLs durchzusetzen.

- **Backup-VLAN:** Richten Sie Firewall- oder Layer-3-ACL-Regeln zwischen dem Backup-VLAN und anderen Netzwerksegmenten ein. Verweigern Sie standardmäßig allen Datenverkehr und erlauben Sie nur die für Sicherungsoperationen erforderlichen Verbindungen.
 - **Produktionsserver:** Da Produktionsserver direkt mit dem Backup-VLAN verbunden sind, können Sie das Routing vom Produktions-VLAN blockieren, ohne den Sicherungsdatenverkehr zu beeinträchtigen.
 - **Mitarbeiter-Endgeräte:** Erlauben Sie den Zugriff auf die Daten-Schnittstelle 1 ausschließlich über TCP 8443 und blockieren Sie allen anderen eingehenden Datenverkehr.
- **Management-VLAN:** Wenden Sie ein **Zero-Trust**-Modell an, indem Sie jeglichen Datenverkehr aus dem User- und Production-VLAN blockieren. Administrativer Zugriff sollte nur über einen Jump-Server auf bestimmten Ports, wie 443 (HTTPS) und 22 (SSH), erlaubt sein.
- **VPN-Tunnel:** Verwenden Sie separate VPN-Tunnel für Backup-Kopien und Management-Datenverkehr, um die Trennung zwischen Daten- und Administrationsverbindungen zu gewährleisten.
 - **Tunnel 1 (Backup-Kopien-Übertragung):** Erlauben Sie Verbindungen ausschließlich zwischen Data Interface 2 an jedem Standort. Blockieren Sie alle anderen VLANs für diesen Tunnel, um die Bandbreite für Backup-Kopien zu reservieren.
 - **Tunnel 2 (Management):** Nutzen Sie diesen Tunnel für zentrales Management und Protokollübertragung. Um standortübergreifendes Management zu unterstützen, erlauben Sie bidirektionalen TCP-8443-Verkehr zwischen den Management-Interfaces beider Appliances. Für andere Management-Dienste, wie Log-Server, erlauben Sie nur die notwendigen Ports und wenden Sie Einweg-Regeln an, um das Risiko lateraler Bewegungen zu minimieren.

Bandbreitenkontrolle

- **Standortübergreifende Backup-Kopien:** Backup-Kopien übertragen Daten über WAN-Verbindungen zwischen Standorten. Nachdem Sie diesen Datenverkehr auf Data Interface 2 isoliert haben, setzen Sie eingehende Bandbreitenlimits auf der Zielseite für die entsprechenden Netzwerksegmente. So bleibt die WAN-Leistung auch dann stabil, wenn mehrere Appliances gleichzeitig Backup-Kopieraufgaben ausführen. [Mehr erfahren](#)
- **Endpoint-Backups:** Umfangreiche Backups von Mitarbeiter-Laptops über WLAN können die drahtlose Leistung beeinträchtigen. Setzen Sie eingehende Datenverkehrslimits für das User-Wi-Fi-VLAN oder legen Sie Geschwindigkeitsbegrenzungen in den ActiveProtect-Agent-Einstellungen fest. [Mehr erfahren](#)

Hinweise:

- Wenn Produktions- und Backup-Datenverkehr unterschiedliche Netzwerkschnittstellen verwenden müssen, lesen Sie die workloadspezifischen Anleitungen in den nächsten Kapiteln.

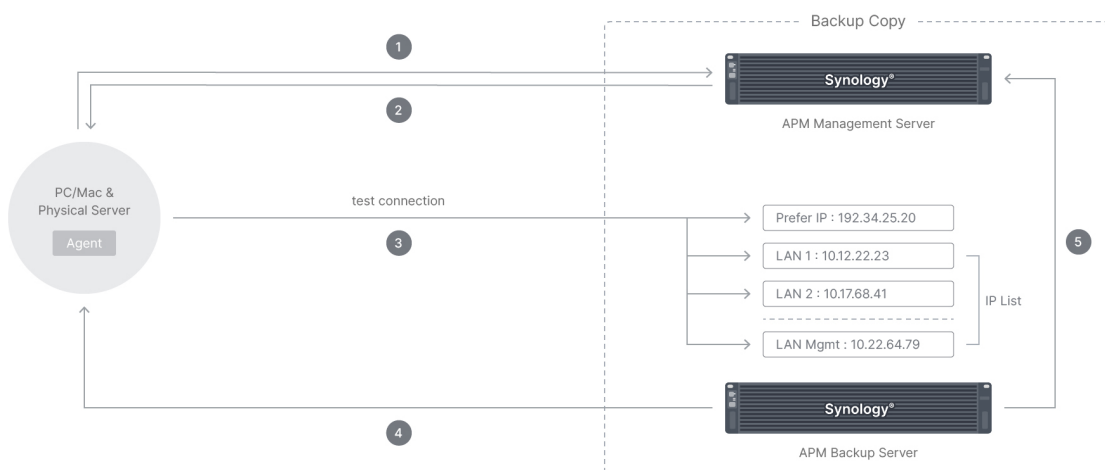
Personal Computer und physische Server

Verbindungsübersicht

Der auf Ihren Personal Computern und physischen Servern installierte Agent stellt die Verbindung zum ActiveProtect Manager (APM) her, um Sicherungen durchzuführen.

Der Verbindungsprozess funktioniert wie folgt:

1. Der Agent verwendet die bereitgestellte Management-Server-Adresse und den Verbindungsschlüssel, um sich über Port 443 beim APM zu authentifizieren.
2. Nach erfolgreicher Authentifizierung sendet der APM dem Agenten eine Liste von IP-Adressen und externen Zugriffsmöglichkeiten für das Sicherungsziel.
3. Der Agent testet anschließend diese IPs, indem er über Port 8443 eine Verbindung zum Sicherungsserver herstellt, um zu ermitteln, welche Routen erreichbar sind. Wenn mehrere Pfade verfügbar sind, wählt der Agent die Schnittstelle in folgender Prioritätsreihenfolge aus:
 - Bevorzugte Adresse (falls [während der Installation konfiguriert](#))
 - LAN 1 (10GbE)
 - LAN 2 (10GbE)
 - OOB (Out-of-Band)
 - Externe Adresse und benutzerdefinierter Port (siehe [Details zum Sicherungsgerät anzeigen](#))
4. Der Agent erhält sein zugewiesenes Sicherungsziel und den Schutzplan und meldet die Informationen zur Workload zurück an den APM.



Für optimale Leistung und Sicherheit sollte der Sicherungsdatenverkehr die Datenschnittstellen (LAN 1, LAN 2) und nicht die Management-Schnittstelle (OOB) nutzen. Dies erfordert eine korrekte

Netzwerktrennung zwischen Daten- und Managementnetzwerken. Bei richtiger Segmentierung priorisiert der Agent automatisch die Datenschnittstellen für den Sicherungsdatenverkehr. Sind die Netzwerke nicht segmentiert, kann der Agent den Sicherungsdatenverkehr über die Management-Schnittstelle leiten, was die Leistung und Sicherheit beeinträchtigt.

Weitere Informationen zum Ablauf der Sicherung finden Sie unter [Personal Computer sichern](#) und [Physische Server sichern](#).

Netzwerkports zulassen

Weitere Informationen zu den von ActiveProtect Manager benötigten Ports finden Sie unter [Netzwerkzugriff absichern](#). Um die Sicherheit zu erhöhen, empfehlen wir, Ihre Firewall so zu konfigurieren, dass nur die für Sicherungs- und Wiederherstellungsvorgänge erforderlichen Ports und Domains zugelassen werden.

Dediziertes Netzwerk angeben

Dedizierte Netzwerkverbindung während der Erstinstallation konfigurieren

Wenn Sie möchten, dass Agenten über eine bestimmte Netzwerkschnittstelle eine Verbindung zum Sicherungsserver herstellen, konfigurieren Sie eine bevorzugte Adresse für diese Schnittstelle. Für externe Verbindungen konfigurieren Sie stattdessen eine externe Adresse und einen benutzerdefinierten Port.

Wie im Verbindungsmechanismus beschrieben, versucht ein Agent, der per Befehlszeile installiert wurde, beim Verbindungsaufbau zum Sicherungsserver zunächst die bevorzugte Adresse zu verwenden. Schlägt diese Verbindung fehl, wird nacheinander jede Schnittstellenadresse aus der vom Management-Server bereitgestellten Liste ausprobiert.

Ausführliche Anweisungen finden Sie im Installationshandbuch für Ihr Betriebssystem:

- [Agent auf Windows-PCs installieren](#)
- [Agent auf Mac installieren](#)
- [Agent auf Windows-Servern installieren](#)
- [Agent auf Linux installieren](#)

Wenn der Agent Verbindungsprobleme hat, authentifizieren Sie sich erneut und bearbeiten Sie die Verbindungseinstellungen, um die Management-Server-Adresse und den Verbindungsschlüssel erneut einzugeben.

Dedizierte Netzwerkverbindung bearbeiten

Wenn sich die Adresse des Sicherungsservers ändert und die bestehende bevorzugte Adresse ungültig wird, können sich die Agenten möglicherweise nicht mehr verbinden. Erstellen Sie in diesem Fall eine neue Konfigurationsdatei mit der aktualisierten bevorzugten Adresse, um die Verbindung wiederherzustellen. Dadurch wird sichergestellt, dass der Agent sich mit demselben Sicherungsserver verbindet, denselben Schutzplan anwendet und die inkrementellen Sicherungen fortsetzt.

Erstellen Sie eine Konfigurationsdatei mit dem Namen `ActiveProtectAgentInstallConfig` und geben Sie die Parameter entsprechend Ihrem Betriebssystem ein.

Windows

1. Verwenden Sie den **Registrierungs-Editor**, um die Einträge unter folgendem Pfad zu erstellen: `HKEY_LOCAL_MACHINE\SOFTWARE\Synology\ActiveProtectAgentCustom\ConnectionInfo`. Jeder Wert muss den Registrierungstyp `REG_SZ` verwenden.

Parameter	Beispiel	Erforderlich
PREFER_IPS	10.17.20.0:8522	Ja
PROXY_ADDRESS	proxy.example.com	Optional
PROXY_PORT	8080	Optional
PROXY_USERNAME	proxyuser	Optional
PROXY_PASSWORD	proxypassword123	Optional

2. Führen Sie den folgenden Befehl aus, um den Dienst neu zu starten.

```
net stop "ActiveProtect Agent Service"
net start "ActiveProtect Agent Service"
```

3. Der Agent stellt automatisch die Verbindung zum Backup-Server mit den aktualisierten Einstellungen her.

Mac

1. Speichern Sie die Datei unter `/usr/local/etc/ActiveProtectAgentConfig`.

Parameter	Beispiel	Erforderlich
prefer_ips	10.17.20.0:8522	Ja
proxy_addr	proxy.example.com	Optional

Parameter	Beispiel	Erforderlich
proxy_port	8080	Optional
proxy_username	proxyuser	Optional
proxy_password	proxypassword123	Optional

2. Führen Sie den folgenden Befehl aus, um den Dienst neu zu starten.

```
sudo launchctl unload "/Library/LaunchDaemons/com.synology.activeprotect.plist"
sudo launchctl load "/Library/LaunchDaemons/com.synology.activeprotect.plist"
```

3. Der Agent stellt automatisch die Verbindung zum Backup-Server mit den aktualisierten Einstellungen her.

Linux

1. Speichern Sie die Datei unter /usr/local/etc/ActiveProtectAgentConfig.

Parameter	Beispiel	Erforderlich
prefer_ips	10.17.20.0:8522, 10.17.21.0:8522	Ja
proxy_addr	proxy.example.com	Optional
proxy_port	8080	Optional
proxy_username	proxyuser	Optional
proxy_password	proxypassword123	Optional

2. Führen Sie den folgenden Befehl aus, um den Dienst neu zu starten.

```
systemctl restart "activeprotect-agent-service"
```

3. Der Agent stellt automatisch die Verbindung zum Backup-Server mit den aktualisierten Einstellungen her.

Hinweise:

- Wenn PREFER_IPS oder prefer_ips fehlt, falsch ist oder nicht mit dem ursprünglichen Backup-Server übereinstimmt, schlägt der Verbindungstest oder die Authentifizierung fehl und der Agent verwendet weiterhin seine bestehenden Verbindungseinstellungen.
- Proxy-Parameter sind nur erforderlich, wenn der Agent über einen Proxy-Server eine Verbindung zum Backup-Server herstellt.
- Da die Konfigurationsdatei sensible Informationen enthält, löschen Sie sie, nachdem die Verbindung erfolgreich hergestellt wurde.

Backup-Bandbreite steuern

Sie können die Bandbreitennutzung sowohl auf Server- als auch auf Agent-Seite steuern:

- Auf dem Backup-Server: [Bandbreitenkontrolle konfigurieren](#), um zu verhindern, dass Backups zu viel Netzwerkbandbreite verbrauchen. Sie können beispielsweise Begrenzungen für Wi-Fi- oder VPN-Netzwerke festlegen. Dies hilft, den Datenverkehr gleichmäßig zu verteilen, wenn Mitarbeitende ihre Geräte sichern, und verhindert eine Überlastung des Firmennetzwerks.
- Auf dem Agent: [Geschwindigkeitsbegrenzung aktivieren](#), um eine maximale Upload-Geschwindigkeit von einem einzelnen Gerät zum entsprechenden Backup-Server festzulegen.

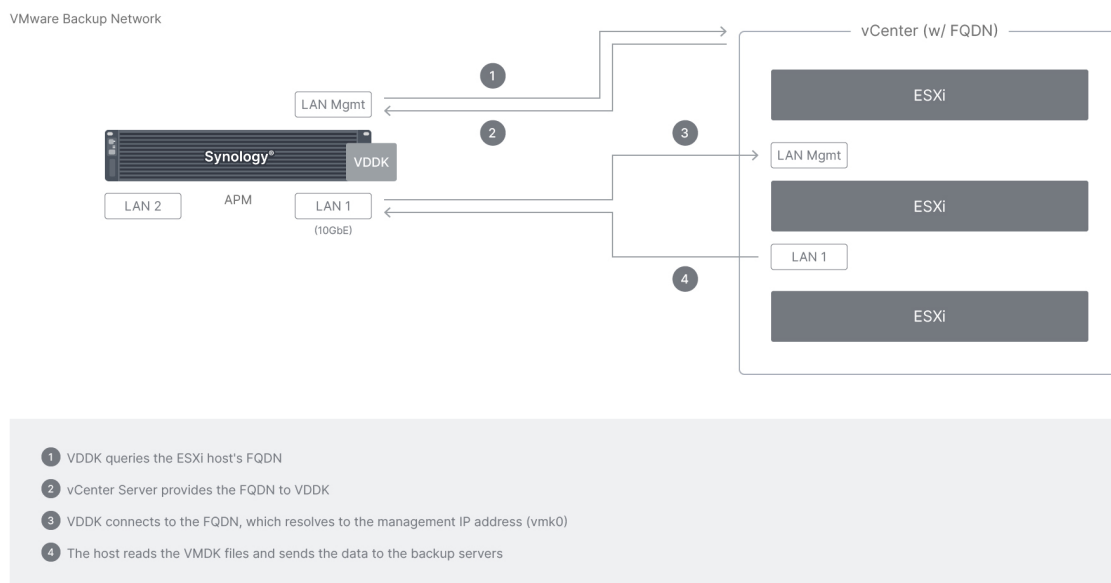
VMware vSphere

Verbindungsübersicht

ActiveProtect Manager (APM) verbindet sich mit VMware-Umgebungen über das **VMware Virtual Disk Development Kit (VDDK)** im **Network Block Device (NBD)**-Modus, der gängige Speichertypen wie VMFS, NFS und vSAN unterstützt.

Der Verbindungsprozess beginnt damit, dass VDDK den vCenter Server abfragt, um den FQDN des ESXi-Hosts zu erhalten. Anschließend verbindet sich VDDK über den TCP-Port 902 mit dem NFC-Dienst (Network File Copy) des Hosts. Standardmäßig wird der FQDN des ESXi-Hosts auf seine **IP-Adresse des Management-Netzwerks (vmk0)** aufgelöst. Die Datenschnittstelle von APM verwendet diese IP, um VDDK-Daten zu übertragen, wobei der hostd-Prozess auf dem ESXi-Host den NFC-Datenverkehr für Backup und Wiederherstellung verwaltet.

Da diese Verbindung davon abhängt, wie der ESXi-Host über DNS aufgelöst wird, wird der Datenübertragungsweg nicht direkt von APM bestimmt.



Weitere Informationen zum Ablauf von Backups finden Sie unter [Virtuelle Maschinen sichern](#).

Netzwerkports zulassen

Weitere Informationen zu den von APM benötigten Ports finden Sie unter [Sicherer Netzwerkzugriff](#). Um die Sicherheit zu erhöhen, empfehlen wir, Ihre Firewall so zu konfigurieren, dass nur die für Backup- und Wiederherstellungsvorgänge erforderlichen Ports und Domains zugelassen werden.

Dediziertes Netzwerk festlegen

Um zu verhindern, dass der Backup-Datenverkehr das VMware-Management-Netzwerk überlastet, empfehlen wir, auf jedem ESXi-Host ein dediziertes 10GbE-Netzwerksegment für Backups zu erstellen oder zuzuweisen.

Sie können den Backup-Datenverkehr auf dieses Netzwerksegment auf eine der folgenden Arten leiten:

- **vSphereBackupNFC-Tags und statische Routen konfigurieren (empfohlen):** Die bevorzugte Methode zur Trennung des Backup-Datenverkehrs. Erfordert vSphere 7.0 oder höher.
- **DNS-Einträge für ESXi-Hosts bearbeiten:** Verwenden Sie diese Methode, wenn Ihr ESXi-Host einen FQDN hat.
- **ESXi-Hosts per IP-Adresse hinzufügen:** Verwenden Sie diese Option nur, wenn die anderen Methoden nicht angewendet werden können.

Hinweis:

- Standardmäßig verbindet sich APM über das Standard-Gateway mit Hypervisoren, in der Regel über die 10GbE-LAN-1-Schnittstelle. Um eine andere Netzwerkschnittstelle zu verwenden, erstellen Sie eine statische Route in der [Gerätekonsole](#) > **Systemsteuerung** > **Netzwerk** > **Statische Route**.

Tags und statische Routen konfigurieren

Standardmäßig ist vmk0 die einzige VMkernel-Schnittstelle auf einem ESXi-Host und mit dem Management-Netzwerk verbunden. Während NBD-Übertragungen (wie Backups) kommuniziert VDDK über vmk0, wodurch Backup- und Management-Datenverkehr möglicherweise denselben Netzwerkpfad nutzen.

vSphereBackupNFC-Tags

Um Netzwerküberlastungen zu vermeiden, weisen Sie das **vSphereBackupNFC**-Tag einer dedizierten Schnittstelle für Backups zu:

1. Melden Sie sich beim vSphere Web Client an und wählen Sie den gewünschten ESXi-Host aus.
2. [Neue VMkernel-Schnittstelle erstellen](#) (z. B. vmk2) oder [eine bestehende bearbeiten](#), die vom Management-Netzwerk getrennt ist.
3. Verbinden Sie diese Schnittstelle mit einem dedizierten 10GbE-VLAN für Backups.
4. Führen Sie den folgenden Befehl aus, um sie für den Backup-Datenverkehr zu taggen:

```
esxcli network ip interface tag add -i vmk2 -t vSphereBackupNFC
```

5. Überprüfen Sie das Tag mit folgendem Befehl:

```
esxcli network ip interface tag get -i vmk2
```

6. Nach der Konfiguration wird der gesamte NBD- und NFC-Datenverkehr, einschließlich Backups, Wiederherstellungen und vSphere Replication, automatisch über diese getaggte Schnittstelle geleitet.

Statische Routen

Wenn sich Ihr ActiveProtect-Gerät und die getaggte VMkernel-Schnittstelle in unterschiedlichen Subnetzen befinden, führen Sie die folgenden Schritte aus, um auf dem ESXi-Host eine [statische Route](#) hinzuzufügen. Das vSphereBackupNFC-Tag erstellt nicht automatisch Routen über Subnetzgrenzen hinweg.

Beispiel:

- Schnittstelle des ESXi-Hosts: 10.10.20.11/24 (vmk2)
- ActiveProtect-Gerät: 10.10.30.100/24
- VLAN-Gateway für Backups: 10.10.20.1

Führen Sie den folgenden Befehl auf dem ESXi-Host aus, um eine statische Route zu erstellen:

```
esxcli network ip route ipv4 add -n 10.10.30.0/24 -g 10.10.20.1
```

Diese statische Route stellt sicher, dass der Datenverkehr zum Subnetz 10.10.30.0/24 (dem ActiveProtect-Gerät) die Backup-Schnittstelle vmk2 anstelle des Management-Netzwerks verwendet.

DNS-Einträge für ESXi-Hosts bearbeiten

Für vSphere-Versionen vor 7.0, die das vSphereBackupNFC-Tag nicht unterstützen, können Sie den Backup-Datenverkehr steuern, indem Sie festlegen, wie der FQDN des ESXi-Hosts aufgelöst wird. Diese Methode setzt voraus, dass die ESXi-Hosts mit FQDNs konfiguriert sind.

Es gibt zwei Möglichkeiten, den FQDN des ESXi-Hosts seinem Backup-Netzwerk zuzuordnen:

- **Auf dem DNS-Server:** Erstellen Sie einen Eintrag, der den FQDN des ESXi-Hosts auf sein dediziertes 10GbE-Backup-Netzwerk verweist.
- **Auf dem ActiveProtect-Gerät:** Wenn Sie die DNS-Einträge nicht ändern können, bearbeiten Sie die Datei [/etc/hosts](#) auf dem Gerät. Gehen Sie zur [Gerätekonsole](#) > **Systemsteuerung** > **Netzwerk** > **Allgemein** und fügen Sie einen Eintrag hinzu, der den FQDN des ESXi-Hosts mit seinem 10GbE-Backup-Netzwerk verknüpft.

Nach der Konfiguration löst APM den FQDN des ESXi-Hosts bei VDDK-Verbindungen auf die IPs des Backup-Netzwerks auf und leitet so den gesamten Backup-Datenverkehr über die richtige Schnittstelle.

ESXi-Hosts per IP-Adresse hinzufügen

Wenn Sie weder vSphereBackupNFC-Tags noch DNS-Einträge verwenden können, fügen Sie jeden ESXi-Host mit der IP-Adresse seines Backup-Netzwerks zu APM hinzu. Dadurch wird sichergestellt, dass VDDK für alle Datenübertragungen die 10GbE-Backup-Schnittstelle verwendet.

1. Gehen Sie zu **ActiveProtect Manager** > **Infrastruktur** > [Hypervisoren](#) und fügen Sie Ihren ESXi-Host hinzu.
2. Geben Sie die IP-Adresse aus dem Backup-Netzwerk des Hosts ein.
3. Nach dem Hinzufügen verwendet APM diese IP-Adresse für alle NBD/NFC-Verbindungen.

Hinweis:

- Jeder ESXi-Host sollte bei dieser Methode einzeln hinzugefügt werden.
- Wenn sich APM und der ESXi-Host in unterschiedlichen Subnetzen befinden, müssen Sie eine [statische Route](#) konfigurieren.

Backup-Bandbreite steuern

Nachdem Sie ein dediziertes Netzwerk für VMware-Backups zugewiesen haben, können Sie den Datenverkehr in diesem Netzwerk steuern, um zu verhindern, dass Backup-Vorgänge zu viel Bandbreite beanspruchen.

Ausführliche Anweisungen finden Sie in [diesem Artikel](#).

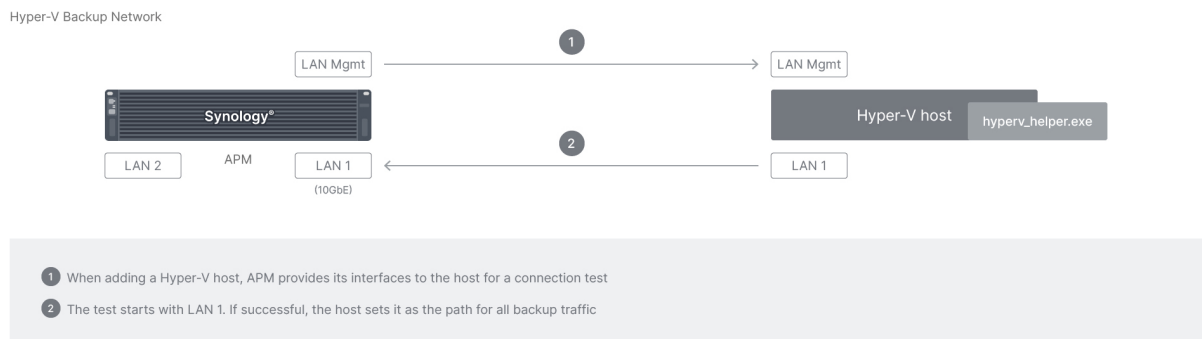
Microsoft Hyper-V

Verbindungsübersicht

Wenn der ActiveProtect Manager (APM) eine Sicherung durchführt, überträgt der Hyper-V-Host die Arbeitslastdaten über IP-Adressen seiner systemdefinierten Schnittstelle an APM. Da APM die Netzwerkeinstellungen des Hosts nicht ändern kann, empfehlen wir, den Hyper-V-Server und eine der 10GbE-Schnittstellen von APM im selben Backup-Subnetz zu platzieren. Dadurch bleibt der Sicherungsverkehr vom Produktionsverkehr getrennt, was optimale Leistung und Sicherheit gewährleistet.

Wenn Sie einen Hyper-V-Host hinzufügen, stellt APM dem Host seine Schnittstelleninformationen für einen Verbindungstest zur Verfügung, beginnend mit der standardmäßigen 10GbE-Schnittstelle (LAN 1). Besteht der Test, wird LAN 1 als bevorzugter Pfad für den gesamten Sicherungsverkehr festgelegt. Andernfalls testet der Host die anderen Schnittstellen, bis eine funktionierende Verbindung gefunden wird.

Dies stellt sicher, dass in Umgebungen mit mehreren Schnittstellen Hyper-V-Hosts APM-Schnittstellen mit hoher Bandbreite für Datenübertragungen priorisieren.



Weitere Informationen zum Ablauf der Sicherung finden Sie unter [Virtuelle Maschinen sichern](#).

Netzwerkports zulassen

Einzelheiten zu den von APM benötigten Ports finden Sie unter [Sicherer Netzwerkzugriff](#). Um die Sicherheit zu erhöhen, empfehlen wir, Ihre Firewall so zu konfigurieren, dass nur die für Sicherungs- und Wiederherstellungsvorgänge erforderlichen Ports und Domains zugelassen werden.

Dediziertes Netzwerk festlegen

Um den Hyper-V-Host zu zwingen, sich für Sicherungen mit einem bestimmten APM-Netzwerksegment zu verbinden, legen Sie einen manuellen Verbindungspfad fest:

1. Gehen Sie zu **ActiveProtect Manager > Infrastruktur > Hypervisoren** und wählen Sie Ihren Hyper-V-Host aus.
2. Geben Sie im Tab **Benutzerdefinierte Verbindung** die IP-Adresse und den Port der Schnittstelle Ihres Backup-Servers für Sicherungsübertragungen ein.

Wenn Ihr Backup-Server beispielsweise über eine 10GbE-LAN1-Schnittstelle mit der IP 10.10.10.11 für Hyper-V-Sicherungen verfügt, geben Sie 10.10.10.11 und die Portnummer in die Felder ein. Dadurch wird diese Schnittstelle bei Verbindungstests priorisiert.

Diese Einstellung ist auch nützlich, wenn der Hypervisor den Backup-Server nicht direkt erreichen kann, zum Beispiel wenn sich der Backup-Server hinter einem NAT-Router befindet.

Hinweis:

- Standardmäßig verbindet sich APM über sein Standard-Gateway mit Hypervisoren, in der Regel über die 10GbE-LAN 1-Schnittstelle. Um eine andere Netzwerkschnittstelle zu verwenden, erstellen Sie eine statische Route in der [Gerätekonsole](#) > **Systemsteuerung** > **Netzwerk** > **Statische Route**.

Sicherungsbandbreite steuern

Nachdem Sie ein dediziertes Netzwerk für Hyper-V-Sicherungen zugewiesen haben, können Sie den Datenverkehr in diesem Netzwerk steuern, um zu verhindern, dass Sicherungsvorgänge zu viel Bandbreite beanspruchen.

Ausführliche Anweisungen finden Sie in [diesem Artikel](#).

Proxmox VE

Verbindungsübersicht

Beim Sichern von Proxmox VE-VMs verwendet APM die Proxmox VE API oder das QEMU Machine Protocol (QMP) über SSH für Verwaltung und Steuerung und liest VM-Festplattendaten über eine Network Block Device (NBD)-Verbindung.

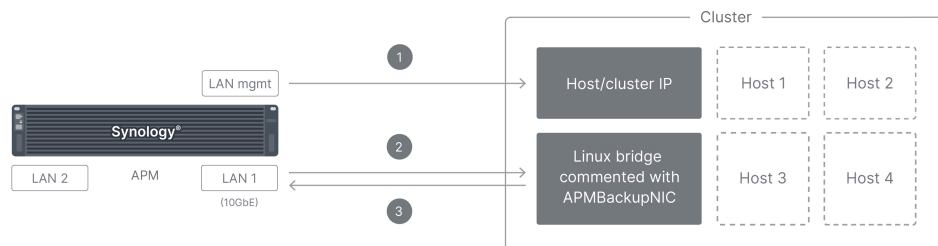
Die Host- oder Cluster-IP-Adresse, die Sie beim Hinzufügen eines Proxmox VE-Hypervisors eingeben, dient als Verwaltungsendpunkt. APM nutzt diese für Authentifizierung, das Abrufen von VM-Informationen, das Erstellen von Snapshots und andere Steuerungsoperationen.

Wenn ein Sicherungsauftrag mit der Übertragung von Festplattendaten beginnt, startet QEMU auf dem Proxmox VE-Host einen temporären NBD-Server und stellt die VM-Festplatten für APM bereit. APM liest Bitmap- oder Rohdaten der Festplatte über diese NBD-Verbindung und überträgt die Daten an den Backup-Server.

An diesem Punkt wählt APM eine Linux Bridge für den Backup-Datenverkehr anhand folgender Regeln¹:

- APM sucht nach einer Linux Bridge mit APMBackupNIC im Kommentarfeld und verwendet diese Bridge für den Backup-Datenverkehr.²
- Wenn keine Bridge mit APMBackupNIC gekennzeichnet ist, versucht APM andere Linux Bridges auf dem Node, bis eine erreichbar ist. In diesem Fall können Verwaltungs- und Backup-Datenverkehr dasselbe Netzwerksegment nutzen.

Das folgende Diagramm zeigt, wie APM während eines Backups mit Proxmox VE verbunden wird:



1. APM verbindet sich zur Authentifizierung und Steuerung mit der Host- oder Cluster-IP-Adresse.
2. APM erstellt Festplattensnapshots über die Proxmox VE API, startet den QEMU NBD-Dienst und stellt eine NBD-Verbindung her.
3. APM überträgt die VM-Festplattendaten über die NBD-Verbindung.

Weitere Informationen zum Ablauf der Sicherung finden Sie unter [Virtuelle Maschinen sichern](#).

Hinweise:

1. Diese Regeln gelten auch, wenn APM die Netzwerkschnittstelle für SSH-Verbindungen zu einzelnen Proxmox VE-Hosts auswählt. Da SSH direkt zu jedem Host verbindet, reicht die Cluster-IP allein nicht aus.
2. Sie können APMBackupNIC zu einem Kommentarfeld hinzufügen, das bereits anderen Text enthält.

Netzwerkports zulassen

Weitere Informationen zu den von APM benötigten Ports finden Sie unter [Netzwerkzugriff absichern](#). Um die Sicherheit zu erhöhen, empfehlen wir, Ihre Firewall so zu konfigurieren, dass nur die für Backup- und Wiederherstellungsvorgänge erforderlichen Ports und Domains zugelassen werden.

Dediziertes Netzwerk festlegen

Um zu verhindern, dass der Backup-Datenverkehr Ihr Proxmox VE-Managementnetzwerk überlastet, empfehlen wir, auf jedem Proxmox VE-Host ein dediziertes 10GbE-Netzwerksegment für Backups einzurichten.

Linux Bridge verbindet VMs mit einem physischen Netzwerk und fungiert als virtueller Switch auf dem Host. Sie können Netzwerkeinstellungen über die Proxmox VE-GUI oder durch direktes Bearbeiten von `/etc/network/interfaces` verwalten. Weitere Informationen finden Sie im [Proxmox VE Administrationshandbuch](#).

Um Verwaltungs- und Backup-Datenverkehr zu trennen, richten Sie auf jedem Proxmox VE-Host mindestens zwei Linux Bridges ein: eine für die Verwaltung und eine für das Backup. Die Verwaltungsnetzwerkschnittstelle von APM sollte mit dem Proxmox VE-Managementsegment verbunden sein, und die Datennetzwerkschnittstelle von APM sollte sich im selben Segment wie die Proxmox VE-Backup-Linux Bridge befinden.

Beachten Sie das folgende Beispiel:

APM-Netzwerkconfiguration:

Schnittstelle	IP-Adresse
Verwaltung	192.168.10.100/24
Daten	10.10.50.100/24

Proxmox VE Linux Bridge-Konfiguration:

	Verwaltungsnetzwerk	Backup-Netzwerk
Name	vmbr0	vmbr1
IPv4/CIDR	192.168.10.11/24	10.10.50.11/24
Kommentar	Verwaltungsnetzwerk	APMBackupNIC

Geben Sie beim Hinzufügen des Hypervisors die Proxmox VE-Managementnetzwerk-IP (z. B. 192.168.10.11) ein. APM verwendet diese Adresse, um sich mit Proxmox VE zu verbinden. Wenn ein Backup-Auftrag mit der Übertragung von Festplattendaten beginnt, sucht APM nach einer Linux Bridge mit dem Tag APMBackupNIC und verwendet deren IP-Adresse, um die NBD-Verbindung herzustellen.

Wenn auf einem Node nur eine Linux Bridge verfügbar ist, verwendet APM diese dennoch für die Übertragung der Backup-Daten. In diesem Fall teilen sich Verwaltungs- und Backup-Datenverkehr dasselbe Netzwerk, und eine Trennung des Datenverkehrs ist nicht möglich.

Mit dieser Konfiguration werden Proxmox VE-Verwaltungsdatenverkehr und NBD-Backup-Datenverkehr auf getrennte Schnittstellen und Netzwerksegmente verteilt, wodurch die Auswirkungen von Backup-Übertragungen auf das Verwaltungsnetzwerk reduziert werden. Für eine konsistente Trennung des Datenverkehrs versehen Sie auf jedem Proxmox VE-Node eine dedizierte Backup-Linux Bridge mit dem Tag APMBackupNIC.

Hinweise:

- Standardmäßig verbindet sich APM über das Standard-Gateway mit dem Hypervisor, in der Regel die 10GbE-LAN-1-Schnittstelle. Um eine andere Netzwerkschnittstelle zu verwenden, erstellen Sie eine statische Route in der **Gerätekonsole > Systemsteuerung > Netzwerk**.
- Die Backup-Linux-Bridge muss über eine IP-Adresse verfügen, die von der Datennetzwerkschnittstelle von APM erreichbar ist. Wenn auf der Bridge keine IP-Adresse konfiguriert ist oder APM diese nicht erreichen kann, können Sicherungen während der Übertragung der Festplattendaten fehlschlagen.
- Wir empfehlen, das Standard-Gateway von Proxmox VE im Management-Netzwerk zu setzen. Die Backup-Linux-Bridge sollte sich im selben Segment wie die Datennetzwerkschnittstelle von APM befinden und vom Management-Netzwerk getrennt sein.
- Bei einer Cluster-Bereitstellung wenden Sie auf jedem Proxmox VE-Knoten die gleiche Netzwerkkonfiguration an und stellen Sie sicher, dass sich die Backup-Linux-Bridge auf jedem Knoten im Backup-Netzwerk befindet und dass die Datennetzwerkschnittstelle von APM die Backup-IP auf jedem Knoten erreichen kann.
- Die Proxmox VE-Cluster-Kommunikation wird von Corosync übernommen. Wenn Sie die Netzwerkkonfiguration auf einem Knoten ändern, überprüfen Sie, dass die Cluster-Kommunikation und das Quorum nicht beeinträchtigt werden. Weitere Informationen finden Sie in der [Cluster Manager-Dokumentation](#) von Proxmox.

Backup-Bandbreite steuern

Nachdem Sie ein dediziertes Netzwerk für Proxmox VE-Backups zugewiesen haben, können Sie den Datenverkehr in diesem Netzwerk verwalten, um zu verhindern, dass Sicherungsvorgänge zu viel Bandbreite beanspruchen.

Weitere Informationen finden Sie unter [Bandbreitensteuerung konfigurieren](#).

Nutanix AHV

Verbindungsübersicht

Bevor Sie Backups konfigurieren, stellen Sie sicher, dass eine [Data Services IP \(DSIP\)](#) für Ihren Cluster in Nutanix Prism Element eingerichtet ist. Der ActiveProtect Manager (APM) sichert virtuelle Maschinen, indem er über iSCSI eine Verbindung zur DSIP des Clusters herstellt.

Die DSIP ist eine virtuelle IP, die von den **Controller-VMs (CVMs)** des Nutanix-Clusters bereitgestellt wird und als Einstiegspunkt für Speicherdienste wie iSCSI dient. Da sie nicht an eine physische Schnittstelle oder einen Host gebunden ist, können Sie keine Netzwerkschnittstelle für den Backup-Verkehr angeben.

Wie APM eine Verbindung zu Nutanix AHV herstellt

Wenn Sie einen Nutanix AHV-Cluster als Backup-Quelle hinzufügen, bestimmt APM den Verbindungsweg wie folgt:

1. Es werden Schnittstellen mit höherer Bandbreite (z. B. 10GbE LAN1) als primärer Datenpfad priorisiert.
2. Es verbindet sich mit **Prism Element** für Verwaltungsaufgaben und mit der **DSIP** für die Datenübertragung.
3. Wenn der bevorzugte Netzwerkpfad nicht verfügbar ist, wechselt APM automatisch zu einer anderen Schnittstelle.

Weitere Informationen darüber, wie Backups funktionieren, finden Sie unter [Virtuelle Maschinen sichern](#).

Netzwerkports zulassen

Weitere Informationen zu den von APM benötigten Ports finden Sie unter [Sicheren Netzwerkzugriff](#). Um die Sicherheit zu erhöhen, empfehlen wir, Ihre Firewall so zu konfigurieren, dass nur die für Backup- und Wiederherstellungsvorgänge erforderlichen Ports zugelassen werden.

Dediziertes Netzwerk angeben

Standardmäßig wird der DSIP-Verkehr über die CVM-Managementschnittstelle (eth0) geleitet, was dazu führen kann, dass Backup-Verkehr mit Verwaltungsaufgaben konkurriert. Um Netzwerküberlastungen zu vermeiden, empfehlen wir folgende Bereitstellungen:

- Erstellen Sie ein dediziertes iSCSI-Netzwerksegment für den DSIP-Verkehr. [Mehr erfahren](#)

- Platzieren Sie die segmentierte DSIP und die APM-10GbE-Schnittstelle im selben Subnetz mit Layer-2-Konnektivität.

Konfigurationsschritte

1. Gehen Sie in Prism Element zu **Netzwerkconfiguration > Interne Schnittstellen** und [erstellen Sie ein iSCSI-Netzwerksegment](#) für Nutanix Volumes.
 - Setzen Sie die VLAN-ID auf **0**, um die Konnektivität mit APM sicherzustellen.¹
 - Weisen Sie diesem Netzwerksegment einen IP-Pool zu (in der Regel **Anzahl der Nodes + 1 Adresse**). Stellen Sie sicher, dass dieser Bereich sich nicht mit dem Managementnetzwerk überschneidet.
 - Wählen Sie **Volumes** als Funktionstyp aus.
2. Konfigurieren Sie in APM die 10GbE-[Schnittstelle](#) Ihres ActiveProtect-Geräts mit einer IP-Adresse im selben Subnetz, während Sie den Management-Verkehr in einem separaten Subnetz belassen.

Wenn sich beide Schnittstellen in derselben Layer-2-Broadcast-Domäne befinden, leitet APM den iSCSI-Verkehr automatisch über die 10GbE-Schnittstelle, ohne dass statische Routen oder Gateways erforderlich sind.² Dadurch wird sichergestellt, dass der Backup-Verkehr vom Management-Verkehr getrennt ist und stets das Hochgeschwindigkeitsnetzwerk verwendet wird.

Backup-Bandbreite steuern

Nachdem Sie ein dediziertes Netzwerk für Nutanix AHV-Backups zugewiesen haben, können Sie die Ein- und Ausgangsbandbreite steuern, um zu verhindern, dass Backup- oder Datenübertragungsaktivitäten zu viel Bandbreite verbrauchen.

Ausführliche Anweisungen finden Sie in [diesem Artikel](#).

Hinweise:

1. Wenn VLAN auf der APM-10GbE-Schnittstelle in der [Gerätekonsole > Systemsteuerung > Netzwerk > Netzwerkschnittstelle](#) aktiviert ist, verwenden Sie dieselbe VLAN-ID, wenn Sie das iSCSI-Netzwerksegment in Prism Element konfigurieren.
2. Wenn sich Ihre APM 10GbE-Schnittstelle und die DSIP in unterschiedlichen Subnetzen befinden müssen, richten Sie eine statische Route ein:
 - a. Gehen Sie zur [Gerätekonsole > Systemsteuerung > Netzwerk > Statische Route](#).
 - b. Fügen Sie eine Route zum DSIP-Subnetz hinzu und geben Sie die 10GbE-Schnittstelle an.

Cloud-VMs

Datenverkehr über das Internet leiten

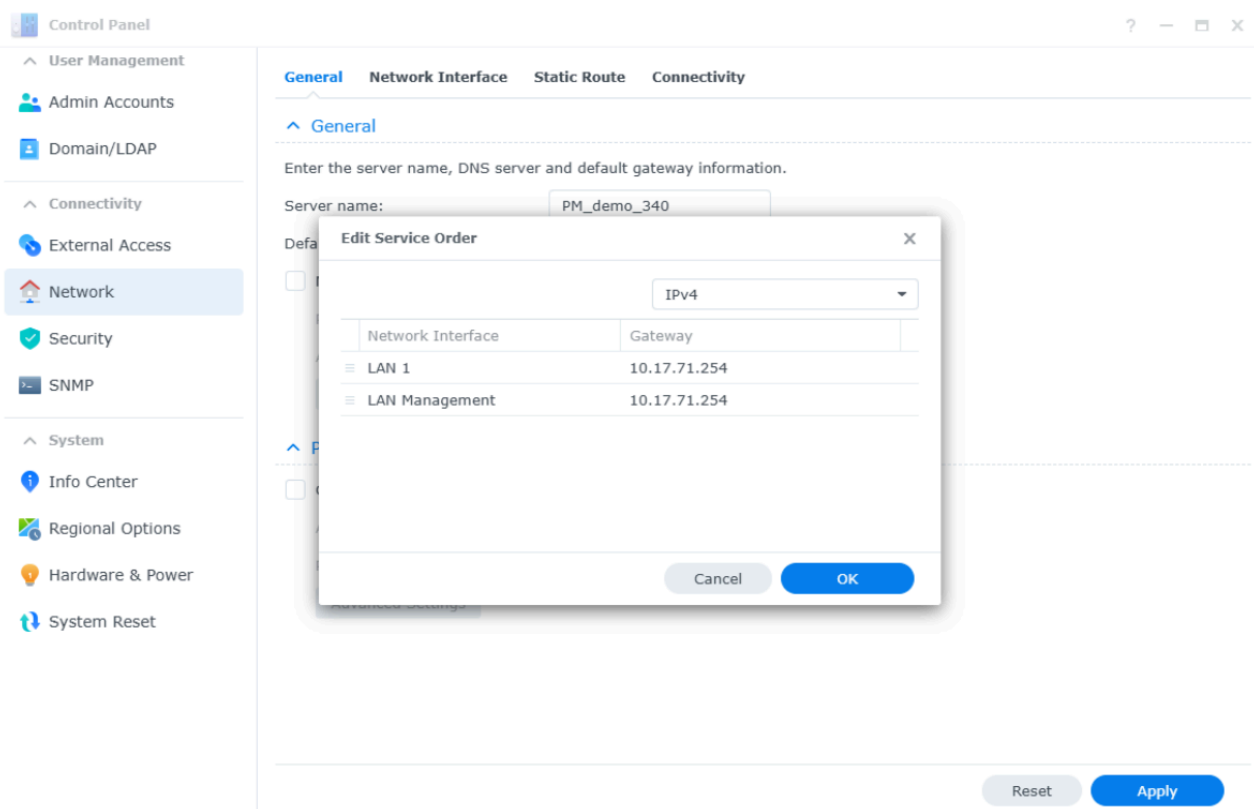
Um virtuelle Maschinen zu sichern, die in Cloud-Umgebungen gehostet werden (z. B. Amazon Web Services oder Microsoft Azure), startet ActiveProtect Manager (APM) temporäre **Worker-Instanzen** in derselben Region und verbindet sich über einen SSH-Reverse-Tunnel mit ihnen. Standardmäßig wird diese Verbindung über das Standard-Gateway von APM geleitet, in der Regel die Schnittstelle 10GbE LAN 1, und mit der öffentlichen IP-Adresse der Worker-Instanz verbunden.

Weitere Informationen zur Funktionsweise der Datensicherung finden Sie unter [Virtuelle Maschinen sichern](#).

Ein dediziertes Netzwerk angeben

Um den SSH-Reverse-Tunnel über eine bestimmte Netzwerkschnittstelle zu leiten, muss diese Schnittstelle als Standard-Gateway festgelegt werden:

1. Gehen Sie zu [Gerätekonsole](#) > **Systemsteuerung** > **Netzwerk** > **Allgemein**.
2. Legen Sie diese Netzwerkschnittstelle als Standard-Gateway fest.



Sicherungsbandbreite steuern

Nachdem Sie ein dediziertes Netzwerk für die Sicherung von Cloud-VMs zugewiesen haben, können Sie den Datenverkehr über die öffentliche IP-Adresse verwalten, damit Sicherungsvorgänge nicht übermäßig viel Bandbreite verbrauchen.

Detaillierte Anweisungen finden Sie in [diesem Artikel](#).

Datenverkehr über ein privates Netzwerk leiten

Wenn Ihr lokales Rechenzentrum über ein Site-to-Site-VPN oder eine dedizierte Verbindung (z. B. AWS Direct Connect oder Azure ExpressRoute) mit der Cloud verbunden ist, können Sie den Sicherungsdatenverkehr statt über das Internet über das private Netzwerk leiten. In dieser Konfiguration stellt APM den SSH-Reverse-Tunnel über die private IP-Adresse der Worker-Instanz her.

Ein dediziertes Netzwerk angeben

1. Gehen Sie zur Seite **Hypervisoren** > *Ihr Cloud-Hypervisor* > **Worker**.
2. Aktivieren Sie im Abschnitt **Sicherungsverbindung** die Option **Private IP für Sicherungen verwenden**.^{1 2} Diese Option stellt sicher, dass die Worker-Instanz Daten vollständig innerhalb Ihres privaten Netzwerks an APM überträgt.

Sicherungsbandbreite steuern

Die Anforderungen an das Bandbreitenmanagement variieren je nach Architektur Ihres lokalen Netzwerks. Informationen zum Konfigurieren von Bandbreitenlimits für eingehenden und ausgehenden Datenfluss oder zum Einschränken des Datenverkehrs aus bestimmten Netzwerkknoten finden Sie in [diesem Artikel](#).

Netzwerkports und Domains zulassen

Einzelheiten zu den von APM benötigten Ports und Domains finden Sie unter [Sicherer Netzwerkzugriff](#). Zur Erhöhung der Sicherheit empfehlen wir, Ihre Firewall so zu konfigurieren, dass nur die für Sicherungs- und Wiederherstellungsvorgänge erforderlichen Ports und Domains zugelassen werden.

Hinweise:

1. Wenn Sie private IP-Adressen für Sicherungen verwenden, erzwingt das System, dass der gesamte Sicherungsdatenverkehr über das private Netzwerk geleitet wird. Wenn die private Verbindung nicht erreichbar ist, schlägt die Sicherungsaufgabe sofort fehl, ohne alternative öffentliche Routen zu versuchen.
2. Diese Routing-Option gilt nur für Sicherungsdatenverkehr.

Dateiserver

Verbindungsübersicht

ActiveProtect Manager (APM) verbindet sich mit Dateiservern über die von Ihnen angegebene Serveradresse und den Port. Standardmäßig wird dieser Datenverkehr über den Standard-Gateway geleitet, bei dem es sich in der Regel um die 10GbE-LAN-1-Schnittstelle handelt.

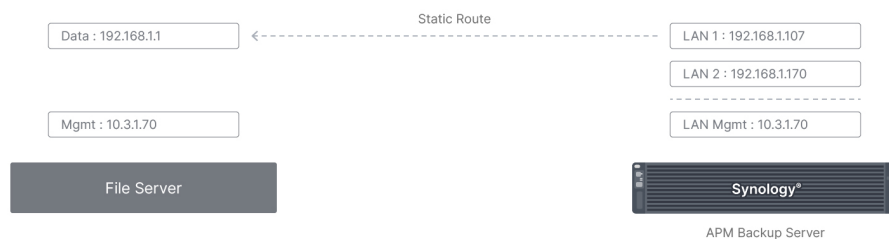
Weitere Informationen zur Funktionsweise der Sicherung finden Sie unter [Dateiserver sichern](#).

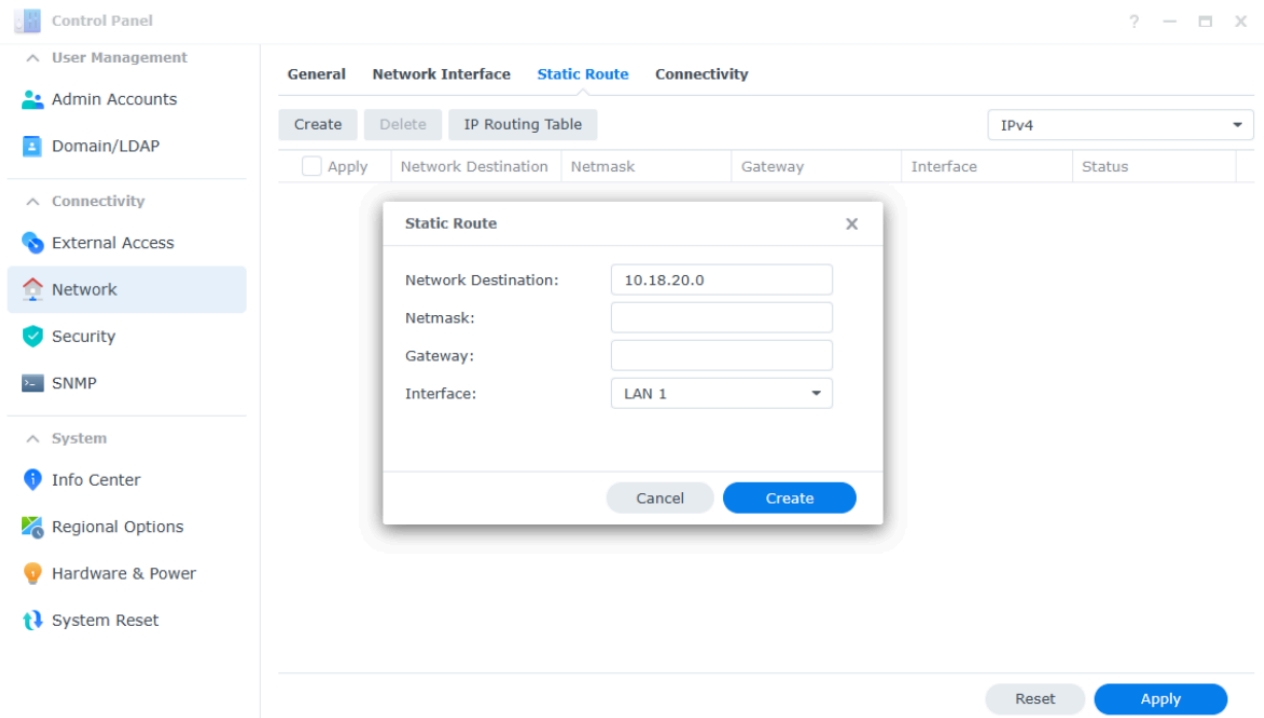
Netzwerk-Ports zulassen

Einzelheiten zu den von APM benötigten Ports finden Sie unter [Sicheren Netzwerkzugang](#). Um die Sicherheit zu erhöhen, empfehlen wir, Ihre Firewall so zu konfigurieren, dass nur die für Sicherungs- und Wiederherstellungsvorgänge erforderlichen Ports zugelassen werden.

Ein dediziertes Netzwerk angeben

Um eine andere Netzwerkschnittstelle für Dateiserver-Sicherungen zu verwenden, erstellen Sie eine statische Route in [Gerätekonsole](#) > **Systemsteuerung** > **Netzwerk** > **Statische Route**. Legen Sie die Adresse des Dateiservers als Netzwerkziel fest und wählen Sie die bevorzugte Netzwerkschnittstelle aus, um den Sicherungsverkehr entsprechend zu leiten.





Da das System das Netzwerksegment des Dateiservers nicht automatisch erkennen kann, stellen Sie bitte Folgendes sicher:

- Die Verwaltungs- und Datenschnittstellen befinden sich in getrennten Netzwerken.
- Die Datenschnittstelle befindet sich im selben Subnetz wie die LAN-1- und LAN-2-Schnittstelle von APM.

Sicherungsbandbreite steuern

Nachdem Sie ein dediziertes Netzwerk für Dateiserver-Sicherungen zugewiesen haben, können Sie den Netzwerkverkehr verwalten, um zu verhindern, dass Sicherungsvorgänge übermäßig viel Bandbreite verbrauchen.

Detaillierte Anweisungen finden Sie in [diesem Artikel](#).

Microsoft 365

Verbindungsübersicht

ActiveProtect Manager (APM) verbindet sich über sein Standard-Gateway, bei dem es sich in der Regel um die Schnittstelle 10GbE LAN 1 handelt, mit Microsoft 365-Diensten.

Weitere Informationen zur Funktionsweise der Sicherung finden Sie unter [Microsoft 365 sichern](#).

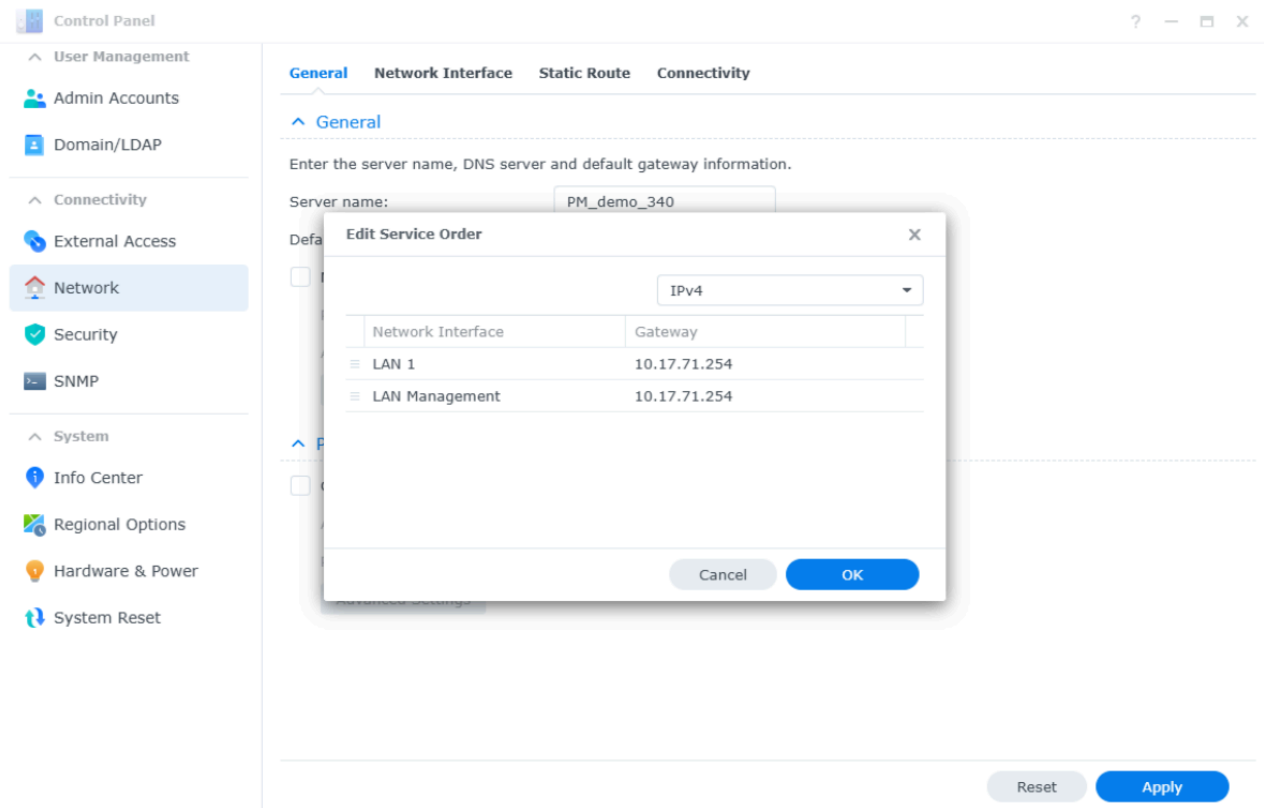
Netzwerkports und Domains zulassen

Ausführliche Informationen zu den von APM benötigten Ports und Domains finden Sie unter [Netzwerkzugriff sichern](#). Zur Erhöhung der Sicherheit empfehlen wir, Ihre Firewall so zu konfigurieren, dass nur die für Sicherungs- und Wiederherstellungsvorgänge erforderlichen Ports und Domains zugelassen werden.

Ein dediziertes Netzwerk festlegen

Microsoft 365 verwendet einen breiten Bereich öffentlicher IP-Adressen, die nicht eindeutig definiert werden können. Daher können Sie keine statische Route zur Weiterleitung des Datenverkehrs verwenden. Stattdessen müssen Sie eine bestimmte Netzwerk-Schnittstelle als Standard-Gateway festlegen.

Gehen Sie dazu zu [Gerätekonsole](#) > **Systemsteuerung** > **Netzwerk** > **Allgemein** und legen Sie diese Netzwerk-Schnittstelle als Standard-Gateway fest.



Sicherungsbandbreite steuern

Nachdem Sie ein dediziertes Netzwerk für Microsoft 365-Sicherungen zugewiesen haben, können Sie den Datenverkehr über die öffentliche IP-Adresse verwalten, um zu verhindern, dass Sicherungsvorgänge übermäßig viel Bandbreite verbrauchen.

Detaillierte Anweisungen finden Sie in [diesem Artikel](#).

Google Workspace

Verbindungsübersicht

ActiveProtect Manager (APM) verbindet sich über sein Standard-Gateway, bei dem es sich in der Regel um die Schnittstelle 10GbE LAN 1 handelt, mit Google Workspace-Diensten.

Weitere Informationen zur Funktionsweise der Sicherung finden Sie unter [Google Workspace sichern](#).

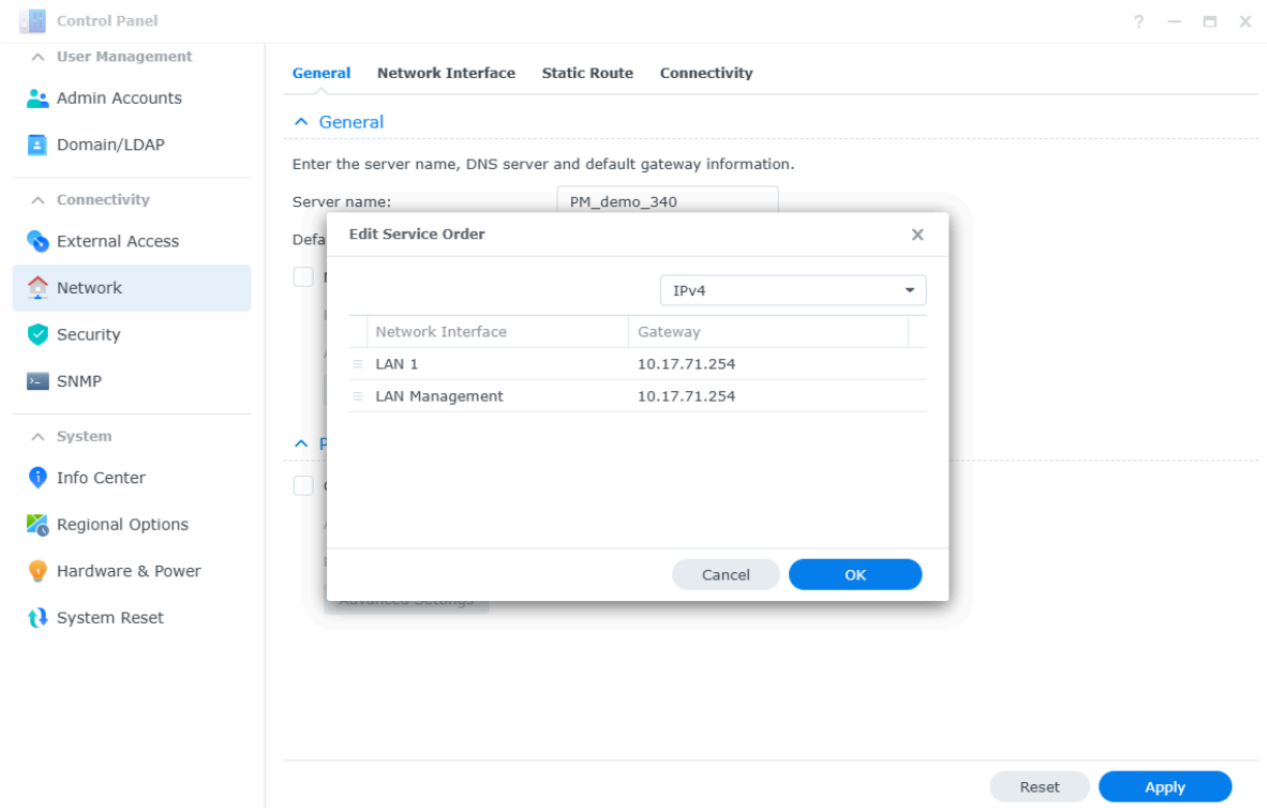
Netzwerkports und Domains zulassen

Ausführliche Informationen zu den von APM benötigten Ports und Domains finden Sie unter [Netzwerkzugriff sichern](#). Um die Sicherheit zu erhöhen, empfehlen wir Ihnen, Ihre Firewall so zu konfigurieren, dass nur die für Sicherungs- und Wiederherstellungsvorgänge erforderlichen Ports und Domains erlaubt sind.

Ein dediziertes Netzwerk festlegen

Google Workspace verwendet eine große Bandbreite öffentlicher IP-Adressen, die nicht eindeutig definiert werden können. Daher können Sie keine statische Route zur Steuerung des Datenverkehrs verwenden. Stattdessen müssen Sie eine bestimmte Netzwerk-Schnittstelle als Standard-Gateway festlegen.

Gehen Sie dazu zu [Gerätekonsole](#) > **Systemsteuerung** > **Netzwerk** > **Allgemein** und legen Sie diese Netzwerk-Schnittstelle als Standard-Gateway fest.



Sicherungsbandbreite steuern

Nachdem Sie ein dediziertes Netzwerk für Google Workspace-Sicherungen zugewiesen haben, können Sie den Datenverkehr über die öffentliche IP-Adresse verwalten, um zu verhindern, dass Sicherungsvorgänge übermäßig viel Bandbreite verbrauchen.

Detaillierte Anweisungen finden Sie in [diesem Artikel](#).

Sicherungskopie

Verbindungsübersicht

Bei Sicherungskopieraufträgen initiiert der Quell-Backup-Server die Verbindung zum Ziel-Backup-Kopierserver über das Standard-Gateway. Der Quellserver testet die Verbindung mithilfe der IP-Liste des Zielservers. Wenn mehrere Pfade verfügbar sind, wird folgende Prioritätsreihenfolge verwendet:

- LAN 2 (10GbE)
- LAN 1 (10GbE)
- OOB (Out-of-Band)



Dediziertes Netzwerk festlegen

Sie können den Netzwerkpfad sowohl für ausgehenden als auch für eingehenden Datenverkehr festlegen:

- Quellserver (ausgehender Datenverkehr): Gehen Sie zu [Gerätekonsole](#) > **Systemsteuerung** > **Netzwerk** > **Statische Route**. Erstellen Sie eine Route, bei der das Netzwerkziel die IP des Zielservers ist, und wählen Sie die Schnittstelle aus, die der Quellserver verwenden soll.
- Zielservers (eingehender Datenverkehr): Gehen Sie zu **Infrastruktur** > **Backup-Server** > **Konnektivität** > [Netzwerkzuweisung](#). Weisen Sie eine bestimmte Netzwerkschnittstelle zu, um den Sicherungskopierverkehr zu empfangen.

Sicherungsbandbreite steuern

Auf dem Zielservers können Sie den eingehenden Datenverkehr begrenzen, um zu verhindern, dass Sicherungskopieraufträge zu viel Bandbreite verbrauchen. Wenn mehrere Quell-Backup-Server gleichzeitig Kopiervorgänge durchführen, wird der Netzwerkverkehr gleichmäßig verteilt.

Ausführliche Anweisungen finden Sie in [diesem Artikel](#).

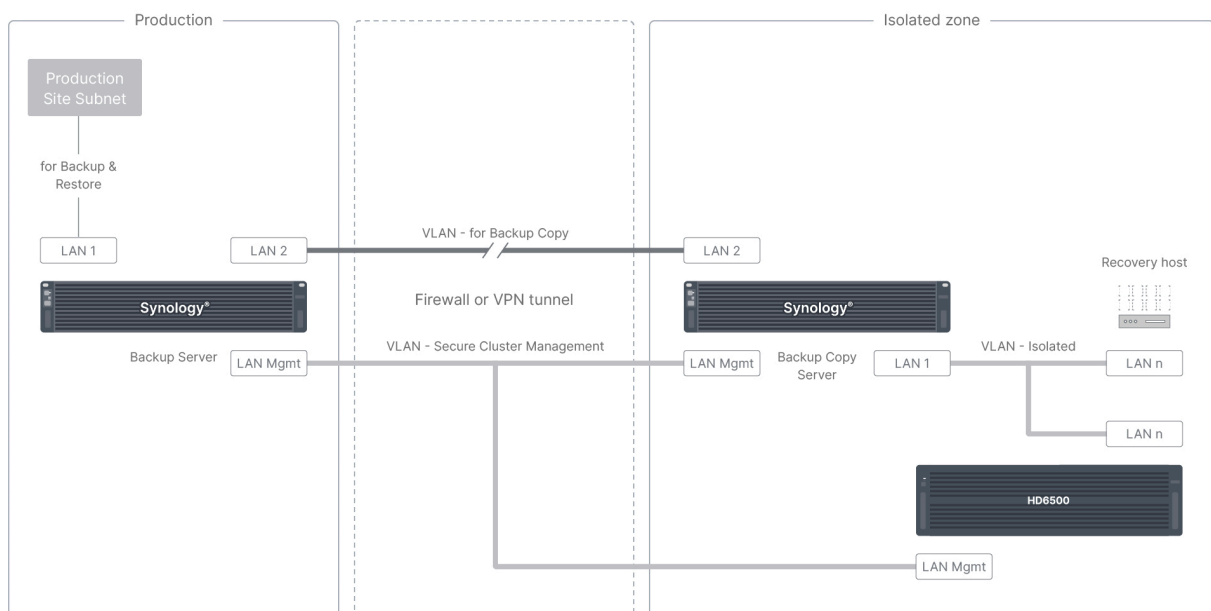
Air-Gap-Umgebung

Um sich vor Ransomware zu schützen, empfehlen wir, eine Air-Gap-Umgebung für Ihre ActiveProtect-Website einzurichten. Im Gegensatz zu herkömmlichen Air-Gap-Lösungen, die für vollständige Trennung auf Bänder setzen, können Sie mit ActiveProtect festlegen, wann und wie sekundäre Sicherungsserver (d. h. Backup-Kopierserver) isoliert werden. Mit diesem Ansatz sind Verbindungen nur dann verfügbar, wenn sie für die Datenübertragung benötigt werden, während IT-Administratoren weiterhin einfach auf Backups zugreifen und diese verwalten können.

Backup-Kopierserver in einer isolierten Zone bereitstellen

Um Ihre Daten zu schützen und gleichzeitig das Site-Management zu vereinfachen, stellen Sie Ihren Backup-Kopierserver in einer Zone bereit, die physisch und logisch vom Produktionsumfeld isoliert ist. Stellen Sie sicher, dass die folgenden Bedingungen erfüllt sind:

- Stellen Sie sicher, dass diese Zone nur über zwei physische Netzwerkschnittstellen mit anderen Umgebungen kommunizieren kann: die Datenschnittstelle und die Managementschnittstelle.
- Aktivieren Sie den [Hardened Mode](#) auf dem Backup-Kopierserver, sodass die Datenschnittstelle offline bleibt, wenn sie nicht verwendet wird, und während festgelegter Sperrzeiten vollständig deaktiviert ist.
- Wenden Sie eine Firewall oder ein VPN auf die Datenschnittstelle und die Managementschnittstelle an, [sodass nur die erforderlichen Ports und Protokolle zugelassen werden](#).



Die Bereitstellung eines Wiederherstellungs-Hosts in der isolierten Zone ermöglicht es Ihnen, regelmäßig Sofortwiederherstellungen durchzuführen und so sicherzustellen, dass Ihre Sicherungsdaten bei Bedarf erfolgreich wiederhergestellt werden können.

Mit dieser Konfiguration sind nur erlaubte Verbindungen in die und aus der isolierten Zone möglich, und der Backup-Kopierserver kommuniziert nur bei Bedarf mit dem Rest der Site.

Hinweise:

- Wir empfehlen, ActiveProtect Vault in der isolierten Zone bereitzustellen, damit gestufte Daten und Sicherungskopien durch die Isolierung geschützt bleiben und über den Sicherungsserver in dieser Zone wiederhergestellt werden können.