Geschäftskontinuität für Proxmox VE Workloads

NetApp virtualization solutions

NetApp
October 29, 2026

This PDF was generated from https://docs.netapp.com/de-de/netapp-solutions-virtualization/proxmox/proxmox-business-continuity.html on October 29, 2026. Always check docs.netapp.com for the latest.

Inhalt

Geschäftskontinuität für Proxmox VE Workloads . . . 1
Informationen zur Geschäftskontinuität von Proxmox VE mit SnapMirror active sync . . . 1
Kundenherausforderungen . . . 1
Lösungsübersicht . . . 2
Wie die Lösung auf Ausfälle reagiert . . . 6
Die Wahl zwischen SnapMirror active sync und MetroCluster . . . 8
Corosync-Überlegungen für einen Proxmox VE Stretch-Cluster . . . 12
Integration mit Storage Manager für Proxmox . . . 13
Gemeinsam genutzter NFS-Storage mit SnapMirror active sync für NAS . . . 14
Verwandte Informationen . . . 18
Konfiguration der Geschäftskontinuität von Proxmox VE mit NAS Storage . . . 18
Schritt 1: Konfiguration des Mediators . . . 19
Schritt 2: Schutz der NFS SVM mit SnapMirror active sync . . . 21
Schritt 3: Konfiguration einer VIP LIF mit BGP für Layer-3-Netzwerke . . . 22
Schritt 4: Erstellen des Proxmox VE Stretch-Clusters mit einem QDevice . . . 24
Schritt 5: Geschützten gemeinsam genutzten NFS Storage provisionieren . . . 25
Schritt 6: Konfiguration von HA und VM-Backups . . . 26
Schritt 7: Geplantes Failover testen . . . 27
Verwandte Informationen . . . 28
Konfigurieren und Verwenden von Storage Manager für Proxmox . . . 28
Erfahren Sie mehr über Storage Manager für Proxmox . . . 28
Installieren und Einrichten von Storage Manager für Proxmox . . . 30
Storage Manager für Proxmox konfigurieren . . . 32
Storage bereitstellen . . . 37
Virtuelle Maschinen schützen . . . 48
Virtuelle Maschinen oder Datenspeicher wiederherstellen . . . 54
Virtuelle Maschinen klonen . . . 58
Überwachungsvorgänge . . . 60
Zusammenfassung . . . 62

Geschäftskontinuität für Proxmox VE Workloads

Informationen zur Geschäftskontinuität von Proxmox VE mit SnapMirror active sync

Unternehmen, die geschäftskritische virtuelle Maschinen (VMs) in Proxmox Virtual Environment (VE) betreiben, und Serviceprovider, die Kunden-VMs in Proxmox VE hosten, benötigen diese VMs auch dann weiterhin im Betrieb, wenn ein Storage-System oder ein gesamtes Datacenter offline geht. ONTAP SnapMirror active sync repliziert den gemeinsam genutzten Storage eines Proxmox VE Clusters, der sich über zwei Standorte erstreckt, synchron und führt automatisch ein Failover des Storage auf den verbleibenden Standort durch. Sie erhalten ein Recovery Point Objective (RPO) von null, eine automatisierte Wiederherstellung ohne Skripte oder Runbooks und denselben gemeinsam genutzten Storage an beiden Standorten, sodass Proxmox VE High Availability (HA) VMs ohne jegliche Neukonfiguration des Storage neu starten kann. Für gemeinsam genutzten NFS Storage verwendet die Lösung SnapMirror active sync für NAS.

Kundenherausforderungen

Der Aufbau von Storage- und Standortausfallsicherheit für Proxmox VE allein mit nativen Tools ist schwierig:

- **Datenverlust nach einem Standortausfall.** Proxmox VE Storage Replizierung und Proxmox Backup Server sind asynchron. Änderungen, die seit der letzten Replikation oder Sicherung vorgenommen wurden, gehen bei einem Ausfall des primären Standorts verloren.
- **Manuelle, langsame Wiederherstellung.** Die Wiederherstellung an einem sekundären Standort erfordert in der Regel das Hochstufen von Replikaten, das Einbinden von Storage unter einer anderen Adresse, das Aktualisieren `/etc/pve/storage.cfg`, und den Neustart von VMs. Jeder manuelle Schritt verlängert die Ausfallzeit und erhöht das Fehlerrisiko während eines Ausfalls.
- **Gestreckter Storage, der mit VMs um Hostressourcen konkurriert.** Hyperkonvergenter gestreckter Storage, wie beispielsweise Ceph im Stretch-Modus, läuft auf den Proxmox VE-Knoten und speichert zwei Replikate jedes Objekts an jedem Standort. Replikations-, Wiederherstellungs- und Rebalancing-Datenverkehr beanspruchen CPU-, Arbeitsspeicher- und Netzwerkressourcen auf denselben Knoten, auf denen auch die VMs laufen.
- **Zwei Quorumsentscheidungen müssen übereinstimmen.** Jedes Zwei-Standort-Design benötigt einen Zeugen in einer dritten Ausfalldomäne, sowohl für den Proxmox VE-Cluster als auch für den Storage. Wenn der Cluster und der Storage nach einem Ausfall der Verbindung zwischen den Standorten unterschiedliche überlebende Standorte auswählen, werden VMs auf Knoten neu gestartet, die den aktiven Storage nicht erreichen können.
- **Eine Storage-Adresse, die an beiden Standorten funktionieren muss.** Nach einem Storage Failover müssen Proxmox VE Knoten den gemeinsam genutzten Storage unter derselben Adresse erreichen können. Diese Adresse muss an beiden Standorten erreichbar sein, was üblicherweise ein Layer 2 VLAN zwischen den Standorten erfordert.

Herausforderungen für Dienstleister

Service Provider, die Cloud Services auf Proxmox VE aufbauen, stehen vor denselben Herausforderungen, zusätzlich zu den Service-Level-Agreements (SLAs) der Mandanten:

- **Das Storage-System stellt einen gemeinsamen Ausfallpunkt dar.** Proxmox VE HA schützt Mandanten-VMs vor einem Host-Ausfall, jedoch nicht vor einem Ausfall des Storage-Systems, auf dem sich ihre Festplatten befinden. Ein Storage-Ausfall betrifft alle Mandanten auf diesem System.
- **Keine Möglichkeit, höhere Verfügbarkeit zu verkaufen.** Ohne synchrone Replizierung und automatisches Storage Failover kann ein Anbieter kein Premium-Verfügbarkeits-Level mit null Datenverlust und stärkeren Verfügbarkeitszusagen anbieten.
- **Tenant-Isolation während der Wiederherstellung.** Wiederherstellungs-, Wartungs- und Notfallwiederherstellungstests dürfen sich nur auf die betroffenen Tenants auswirken, nicht auf die gesamte Plattform.

Herausforderungen für Unternehmen

Unternehmen, die geschäftskritische Workloads von anderen Hypervisoren auf Proxmox VE migrieren, erwarten dieselbe Standortausfallsicherheit wie zuvor, beispielsweise null Datenverlust für Datenbanken und Geschäftsapplikationen sowie eine Wiederherstellung ohne manuelles Runbook. Diesen Erwartungen allein mit den nativen Tools von Proxmox VE zu entsprechen, erfordert erheblichen Aufwand bei Design, Skripterstellung und Betrieb.

Lösungsübersicht

Die Lösung kombiniert einen Proxmox VE Stretch-Cluster mit SnapMirror active sync auf NetApp AFF-Systemen an zwei Standorten:

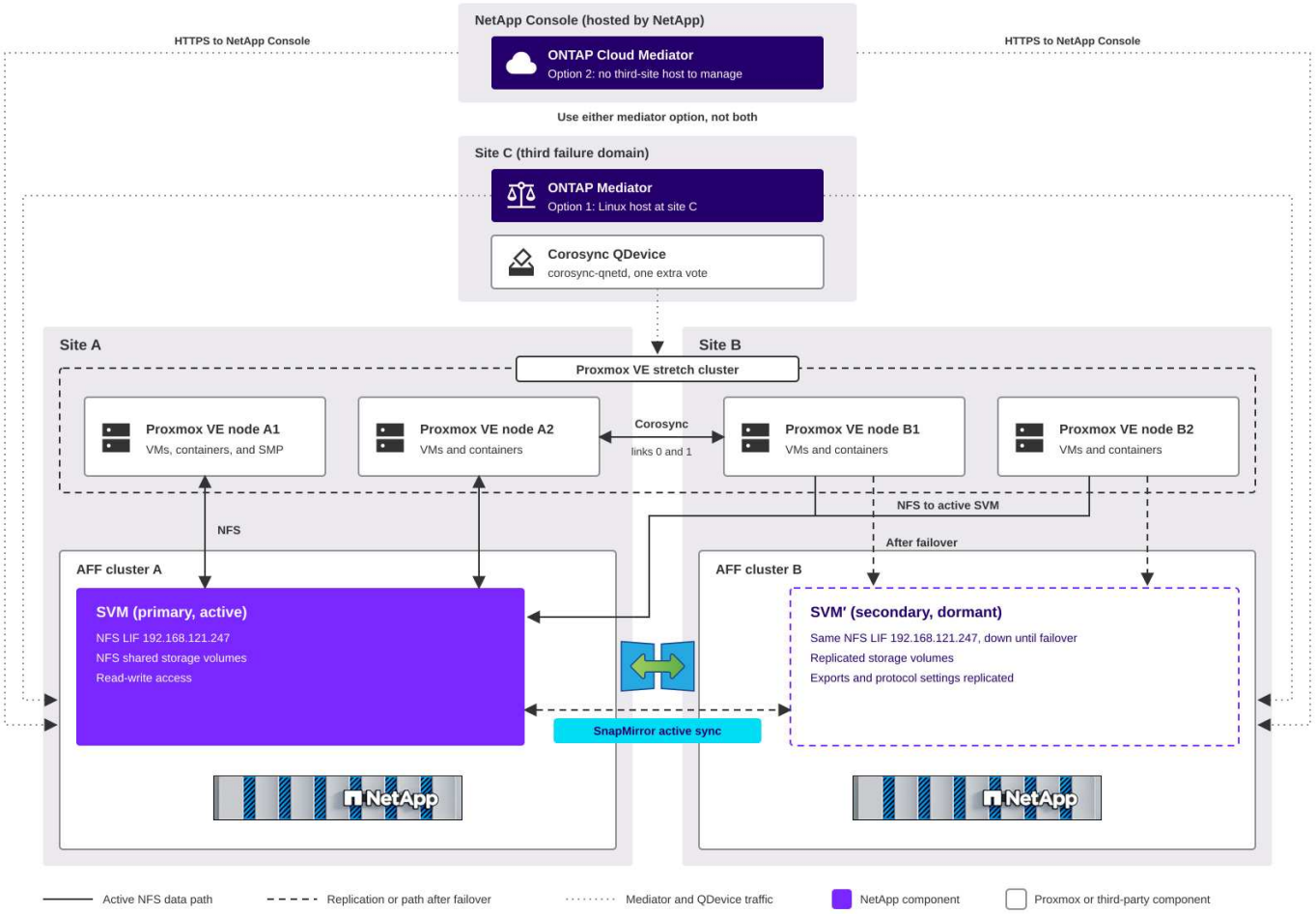
- **Null RPO.** ONTAP repliziert jeden Schreibvorgang synchron vom primären Cluster an Standort A zum sekundären Cluster an Standort B auf den gemeinsam genutzten Storage.
- **Gleicher gemeinsam genutzter Storage an beiden Standorten.** Nach einem Failover präsentiert der sekundäre Cluster Proxmox VE denselben Storage, sodass die Storage-Definitionen in `/etc/pve/storage.cfg` gültig bleiben.
- **Automatisches Failover.** Ein Mediator fungiert als Zeuge außerhalb der beiden Standorte. Sie können ONTAP Mediator an einem dritten Standort installieren oder ONTAP Cloud Mediator verwenden, einen in der NetApp Console gehosteten Service. Wenn das primäre Storage oder der Standort ausfällt, führt ONTAP ohne manuelles Eingreifen ein Failover auf Standort B durch.
- **Feingranulare Kontrolle.** Sie wählen aus, welche Workloads geschützt werden sollen, und Sie können für einzelne Workloads ein Failover durchführen, beispielsweise um einen Mandanten oder eine Applikation für Wartungsarbeiten am Standort zu verschieben.
- **Verwendung der sekundären Kopie.** Sie können die sekundäre Kopie für Entwicklungs-, Test- oder Notfallwiederherstellungstests klonen, ohne die Replikation zu beeinträchtigen.

Wie die Lösung die Herausforderungen bewältigt

Herausforderung	So unterstützt die Lösung	Wofür Sie noch planen
Datenverlust und manuelle Wiederherstellung	Die synchrone Replizierung führt zu einem RPO von null. ONTAP führt automatisch ein Failover durch, und die sekundäre SVM stellt dieselbe NFS-Adresse bereit, sodass `/etc/pve/storage.cfg` gültig bleibt.	Proxmox VE HA startet VMs eines ausgefallenen Standorts weiterhin neu.

Herausforderung	So unterstützt die Lösung	Wofür Sie noch planen
Gestreckter Storage auf den Hosts	Die Replikation läuft auf den AFF Controllern, nicht auf den Proxmox VE Knoten, sodass CPU, Arbeitsspeicher und Netzwerk des Hosts für VMs verfügbar bleiben. ONTAP speichert an jedem Standort eine Kopie, und die Storage-Effizienz gilt für beide Kopien.	Wie bei jeder synchronen Replizierung benötigt die Lösung eine vollständige zweite Kopie an Standort B, und die Replizierung erhöht die Last auf beiden AFF Clustern. Die Dimensionierung beider Cluster muss auf die Replizierungs-Workload ausgelegt sein.
Zwei Quorum-Entscheidungen	ONTAP Mediator oder ONTAP Cloud Mediator als Service in der NetApp Console ist ein ressourcenschonender Zeuge außerhalb des Datenpfads. Diese Lösung zeigt, wie das corosync QDevice auf den primären Cluster abgestimmt wird, sodass beide denselben Standort auswählen.	Für das QDevice wird weiterhin ein dritter Standort benötigt. Dieser ist auch für ONTAP Mediator erforderlich, jedoch nicht für ONTAP Cloud Mediator. Weitere Informationen finden Sie unter Mediator-Optionen.
Eine Storage-Adresse an beiden Standorten	Die sekundäre SVM übernimmt dieselbe NFS LIF-Adresse, sodass kein erneutes Mounten oder keine Neukonfiguration des Storage erforderlich ist.	Das NFS-Subnetz muss an beiden Standorten erreichbar sein, typischerweise über ein gestrecktes Layer-2-VLAN. Der Qualifizierungsstatus von VIP LIFs ist in Layer 3 Netzwerke mit VIP LIFs und BGP beschrieben.

Das folgende Diagramm zeigt die Lösungsarchitektur mit gemeinsam genutztem NFS Storage.



Standort A und Standort B

Jeder Standort verfügt über einen AFF Zwei-Node-Cluster und die Hälfte der Proxmox VE-Knoten. Der primäre Cluster an Standort A stellt den gemeinsam genutzten Storage für alle Proxmox VE-Knoten bereit. Die Knoten an Standort B erreichen den primären Cluster über das standortübergreifende Netzwerk. Bei Verwendung von NFS Storage bleibt die sekundäre SVM an Standort B inaktiv, bis ein Failover auftritt.

Standort C

Eine dritte Ausfalldomäne beherbergt den corosync QDevice Daemon (`corosync-qnetd`) und, wenn Sie Option 1 wählen, ONTAP Mediator. Das QDevice stellt eine zusätzliche Stimme bereit, sodass der Proxmox VE Cluster bei Ausfall eines Standorts das Quorum aufrechterhält.

NetApp Console

Wenn Sie Option 2 wählen, wird ONTAP Cloud Mediator als Service in der NetApp Console ausgeführt, die NetApp hostet und managt. Beide AFF Cluster stellen über HTTPS eine Verbindung dazu her, sodass die Installation und Wartung eines Mediator-Hosts entfällt.

Mediator

ONTAP Mediator oder ONTAP Cloud Mediator unterstützt ONTAP bei der Entscheidung, welcher Cluster Daten bereitstellt. Es kommt nur einer von beiden zum Einsatz, nicht beide. Einen Vergleich finden Sie unter Mediator-Optionen.

Proxmox VE Stretch-Cluster

Alle Proxmox VE Knoten gehören zu einem Cluster und verwenden dieselben Storage-Definitionen. Proxmox VE HA startet VMs von einem ausgefallenen Standort auf den verbleibenden Knoten neu. Storage

Manager for Proxmox (SMP) läuft als HA-VM im Cluster, um gemeinsam genutzten Storage zu provisionieren sowie VMs zu sichern, wiederherzustellen und zu klonen.

Mediator-Optionen

SnapMirror active sync verwendet einen Mediator als passiven Zeugen. Bei einer Netzwerkpartitionierung oder dem Ausfall eines Clusters verwendet ONTAP den Mediator, um zu entscheiden, welche Kopie weiterhin E/A verarbeitet. Der Mediator befindet sich nicht im Datenpfad und initiiert kein Failover selbst. Eine der folgenden Optionen kann verwendet werden, jedoch nicht beide gleichzeitig.

Überlegung	Option 1: ONTAP Mediator	Option 2: ONTAP Cloud Mediator
Wo es ausgeführt wird	Ein Linux-Host, den Sie in einer dritten Ausfalldomäne, z. B. Standort C, mit unabhängiger Stromversorgung und Netzwerkinfrastruktur installieren und managen.	Ein Cloud-Service in der NetApp Console. NetApp hostet und managt ihn, sodass kein Mediator-Host an einem dritten Standort erforderlich ist.
ONTAP Version	ONTAP 9.19.1 oder höher für SnapMirror active sync für NAS.	ONTAP Cloud Mediator ist ab ONTAP 9.17.1 verfügbar. SnapMirror active sync für NAS erfordert ONTAP 9.19.1 oder höher.
Cluster-Konnektivität	Beide Cluster sind mit dem Mediator-Host verbunden. Der Standard-Service-Port ist 31784.	Beide Cluster stellen ausgehende Verbindungen über HTTPS zur NetApp Console her, direkt oder über einen HTTP-Proxy. Die empfohlene Ping-Latenz zur NetApp Console liegt unter 200 ms.
Einrichtung	Das Paket auf dem Linux-Host installieren und es anschließend mit der Hostadresse und einem Mediator-Benutzer zu den Clustern hinzufügen.	Erforderlich sind die Erstellung eines NetApp Console Service-Kontos mit der **ONTAP Mediator Setup Role** sowie das anschließende Hinzufügen des Mediators zu den Clustern mit der Unternehmens-ID, der Client-ID und dem Client-Secret.
Betrieb	Sie spielen Patches ein, aktualisieren den Host und halten ihn verfügbar.	Es gibt keinen Host, der gepatcht oder aktualisiert werden muss. Sie sind auf den Internetzugang an beiden Standorten und auf die Verfügbarkeit des NetApp Console Service angewiesen.
Bestmögliche Übereinstimmung	Umgebungen, die über einen dritten Standort verfügen oder in denen die Storage-Cluster das Internet nicht erreichen können.	Umgebungen ohne einen dritten Standort für einen Mediator oder Umgebungen, die den Betrieb eines solchen vermeiden möchten.

Bei der Auswahl ist Folgendes zu beachten:

- **Das QDevice benötigt weiterhin einen dritten Standort.** ONTAP Cloud Mediator entfernt den Mediator-Host, nicht den corosync QDevice-Host. Das QDevice benötigt einen kleinen Linux-Host, den alle Proxmox VE-Knoten über TCP-Port 5403 erreichen können, und es hat nicht die Anforderung an niedrige Latenz von corosync.

- **Beide Cluster benötigen Zugriff auf die NetApp Console.** Wenn die Cluster einen Proxy verwenden, ist das Root-CA-Zertifikat des Proxy auf beiden Clustern zu installieren. NetApp empfiehlt für jeden Cluster einen anderen Proxyserver.
- **Bei beiden Optionen ist mit demselben Ausfallverhalten zu rechnen.** Wenn der Mediator nicht verfügbar ist, wird die Replikation ohne Datenverlust fortgesetzt, automatische und geplante Failover sind jedoch erst wieder möglich, wenn der Mediator wieder verfügbar ist. Bei ONTAP Cloud Mediator umfasst dies auch einen Verbindungsverlust von den Clustern zur NetApp Console.

> Die Mediatoroptionen in diesem Abschnitt gelten für SnapMirror active sync. Für MetroCluster verwendet diese Lösung ONTAP Mediator oder MetroCluster Tiebreaker. Vor dem Einsatz ist zu überprüfen, ob Ihre ONTAP Version, die Mediatoroption und die Proxmox VE-Version zusammen in der "NetApp Interoperabilitätsmatrix Tool (IMT)" aufgeführt sind.

Vorteile für Dienstleister

- **VM-Verfügbarkeit über die Host-HA hinaus.** Tenant-VMs laufen weiter, wenn das Storage-System, auf dem ihre Festplatten gehostet werden, ausfällt. ONTAP führt ein Failover auf den zweiten AFF Cluster durch, und die VMs setzen die E/A auf demselben gemeinsam genutzten Storage ohne Neustart fort.
- **Eine Premium-Verfügbarkeitsstufe.** Sie können einen VM-Dienst mit Zero-RPO und Speicherausfallsicherheit als Zusatzoption anbieten, parallel zu Standardstufen auf ungeschütztem Storage in denselben Clustern.
- **Mandantenspezifischer Schutz und Failover.** Mit separatem geschütztem Storage für jeden Mandanten oder jede Serviceebene können Sie jeden Mandanten unabhängig schützen, ein Failover durchführen und die Notfallwiederherstellung testen, ohne andere Mandanten zu beeinträchtigen.
- **Bessere Nutzung beider Standorte.** Sie können einige Workloads primär an Standort A und andere primär an Standort B ausführen, sodass beide Rechenzentren aktive Workloads bedienen.

Vorteile für Unternehmen

- **Kein Datenverlust für geschäftskritische VMs** bei einem Storage- oder Standortausfall.
- **Automatisierte Wiederherstellung** ohne Skripte, erneutes Mounten von Storage oder Änderungen an `/etc/pve/storage.cfg`.
- **In ONTAP integriert**, ohne zusätzliche Softwareschicht auf den Proxmox VE Knoten.
- **Tägliche Bedienung über eine einzige Schnittstelle.** Storage Manager für Proxmox stellt den geschützten gemeinsam genutzten Storage bereit und sichert, stellt VMs wieder her und klont sie mit ONTAP Snapshots und FlexClone Technologie.

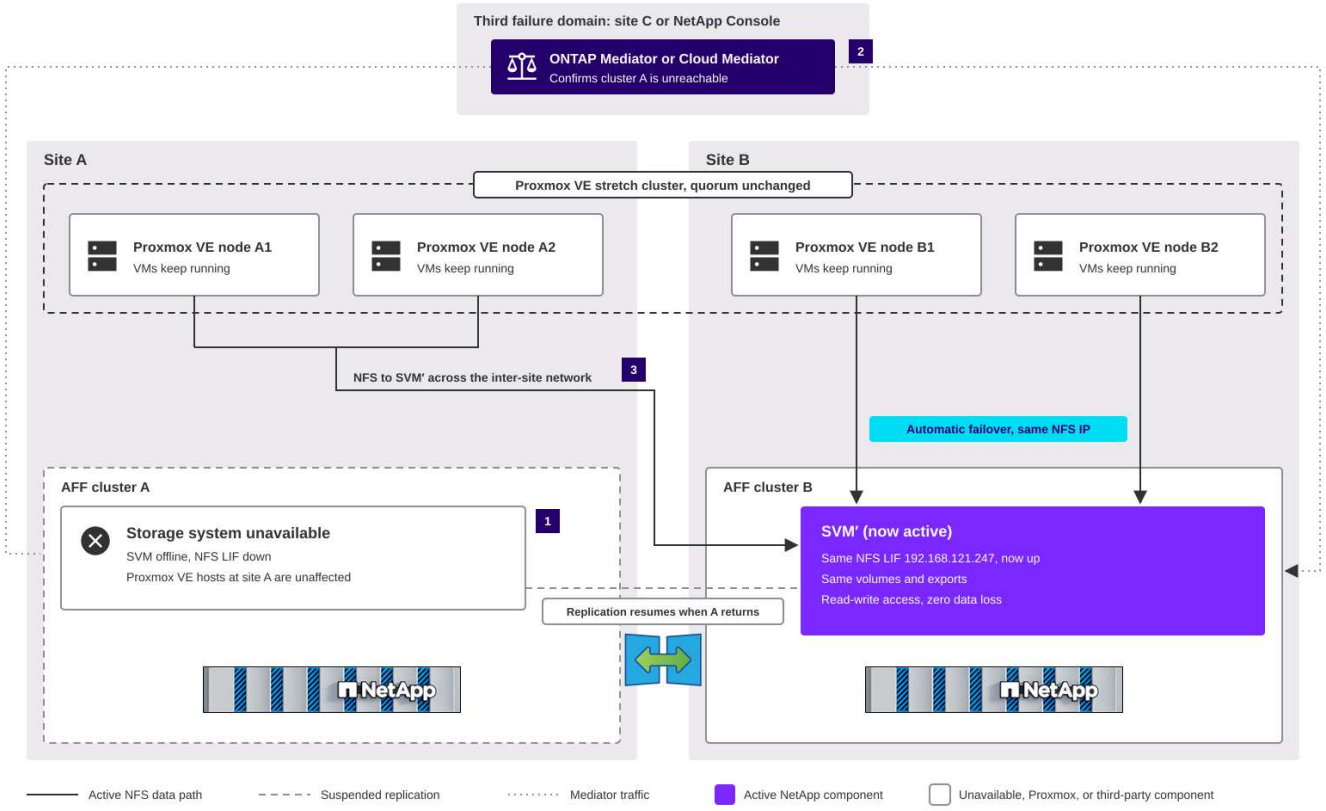
Wie die Lösung auf Ausfälle reagiert

ONTAP und Proxmox VE treffen unabhängige Quorumentscheidungen. Die Architektur sorgt dafür, dass beide denselben verbleibenden Standort auswählen.

Ereignis	ONTAP Verhalten	Verhalten von Proxmox VE
Standort A fällt aus	Der Mediator bestätigt den Ausfall, und ONTAP schaltet das gemeinsam genutzte Storage automatisch auf Cluster B um.	Die Knoten an Standort B und das QDevice halten das Quorum aufrecht. HA isoliert die Knoten an Standort A und startet deren VMs auf den Knoten an Standort B neu. Die bereits an Standort B befindlichen VMs nehmen den I/O nach dem Storage Failover wieder auf.
AFF Cluster A fällt aus, Proxmox VE Knoten an Standort A laufen weiter	Der Mediator bestätigt, dass Cluster A nicht erreichbar ist, und ONTAP schaltet den gemeinsam genutzten Storage automatisch auf Cluster B um.	Es gibt keine Quorumänderung und keinen VM-Neustart. Die VMs auf allen Knoten setzen den I/O nach dem Storage Failover auf demselben gemeinsam genutzten Storage fort, wobei die Knoten von Standort A Cluster B über das standortübergreifende Netzwerk erreichen.
Ein AFF Controller am Standort A fällt aus	Der Partner-Controller übernimmt im Rahmen einer lokalen HA-Übernahme. Es erfolgt kein SnapMirror active sync Failover.	Keine Auswirkungen. Die VMs unterbrechen die E/A-Vorgänge während der Übernahme kurzzeitig.
Standort B fällt aus	Cluster A stellt weiterhin Daten bereit. Die Replikation wird wieder aufgenommen, sobald Standort B wieder verfügbar ist.	Die Knoten von Standort A und das QDevice halten das Quorum aufrecht. HA startet die VMs von Standort B auf den Knoten von Standort A neu.
Verbindung zwischen Standorten fällt aus	Cluster A stellt weiterhin Daten bereit. Es findet kein Failover statt.	Das QDevice gibt seine Stimme der Partition von Standort A, wenn der Trennschalter auf das primäre Cluster ausgerichtet ist. Die Knoten von Standort B verlieren das Quorum und schalten sich selbst ab, und HA startet ihre VMs auf Standort A neu.
Standort C fällt aus, oder die Cluster verlieren den Zugriff auf die NetApp Console	Die Replikation wird ohne Datenverlust fortgesetzt, automatische und geplante Failover sind jedoch erst möglich, wenn der Mediator verfügbar ist. Mit ONTAP Cloud Mediator betrifft ein Standortausfall von Standort C nur das QDevice.	Der Cluster erhält das Quorum durch die Stimmen der vier Knoten aufrecht. Es sind keine VMs betroffen.
Ein Proxmox VE Knoten fällt aus	Keine Auswirkungen.	HA startet die VMs dieses Knotens auf anderen Knoten neu und bevorzugt dabei Knoten am selben Standort.

Storage-Systemausfall

Ein Storage-Systemausfall ist ein Fall, den HA auf Host-Ebene allein nicht bewältigen kann, und der Fall, in dem SnapMirror active sync den größten Mehrwert für Dienstanbieter bietet. Das folgende Diagramm zeigt den Zustand nach dem Ausfall von AFF Cluster A, während alle Proxmox VE-Knoten bei Verwendung von gemeinsam genutztem NFS-Storage weiterhin online bleiben.



1. AFF Cluster A ist nicht mehr verfügbar. Die Proxmox VE-Knoten an Standort A bleiben jedoch in Betrieb, sodass der Cluster sein Quorum nicht verliert und HA keinen Knoten isoliert.
2. Der Mediator, ONTAP Mediator an Standort C oder ONTAP Cloud Mediator in der NetApp Console, bestätigt, dass Cluster A nicht erreichbar ist, und ONTAP aktiviert die sekundäre SVM auf Cluster B mit derselben NFS LIF Adresse, denselben Volumes und denselben Exportrichtlinien.
3. Alle Proxmox VE Knoten setzen die E/A-Operationen auf demselben gemeinsam genutzten Storage fort. Knoten an Standort B erreichen Cluster B lokal, und Knoten an Standort A erreichen es über das standortübergreifende Netzwerk. VMs pausieren die E/A-Operationen während des Failovers und laufen ohne Neustart weiter.

Wenn Cluster A zurückkehrt, wird die Replikation fortgesetzt. Das Failback zu Cluster A sollte während eines Wartungsfensters geplant werden, damit die VMs von Standort A wieder auf lokalen Storage zugreifen.

Standortausfall

Bei einem Standortausfall gehen sowohl das Storage-System als auch die Proxmox VE Knoten an diesem Standort offline. ONTAP führt ein Failover des gemeinsam genutzten Storage auf den verbleibenden Cluster durch, und Proxmox VE HA startet die VMs vom ausgefallenen Standort auf den verbleibenden Knoten neu, wie in der Tabelle beschrieben.

Die Wahl zwischen SnapMirror active sync und MetroCluster

NetApp MetroCluster Konfigurationen bieten außerdem einen RPO von null und eine automatische Wiederherstellung für einen Proxmox VE Stretch-Cluster. Die beiden Lösungen unterscheiden sich darin, was sie schützen:

- **MetroCluster schützt alle Workloads.** MetroCluster kombiniert array-basiertes Clustering mit synchroner Replizierung. Es spiegelt die Daten in jedem gespiegelten Aggregat, den nichtflüchtigen Speicher

(NVRAM) und die Konfiguration jeder SVM auf den Partnerstandort, sodass der gesamte gemeinsam genutzte Storage im Cluster ohne Einrichtung pro Workload geschützt ist.

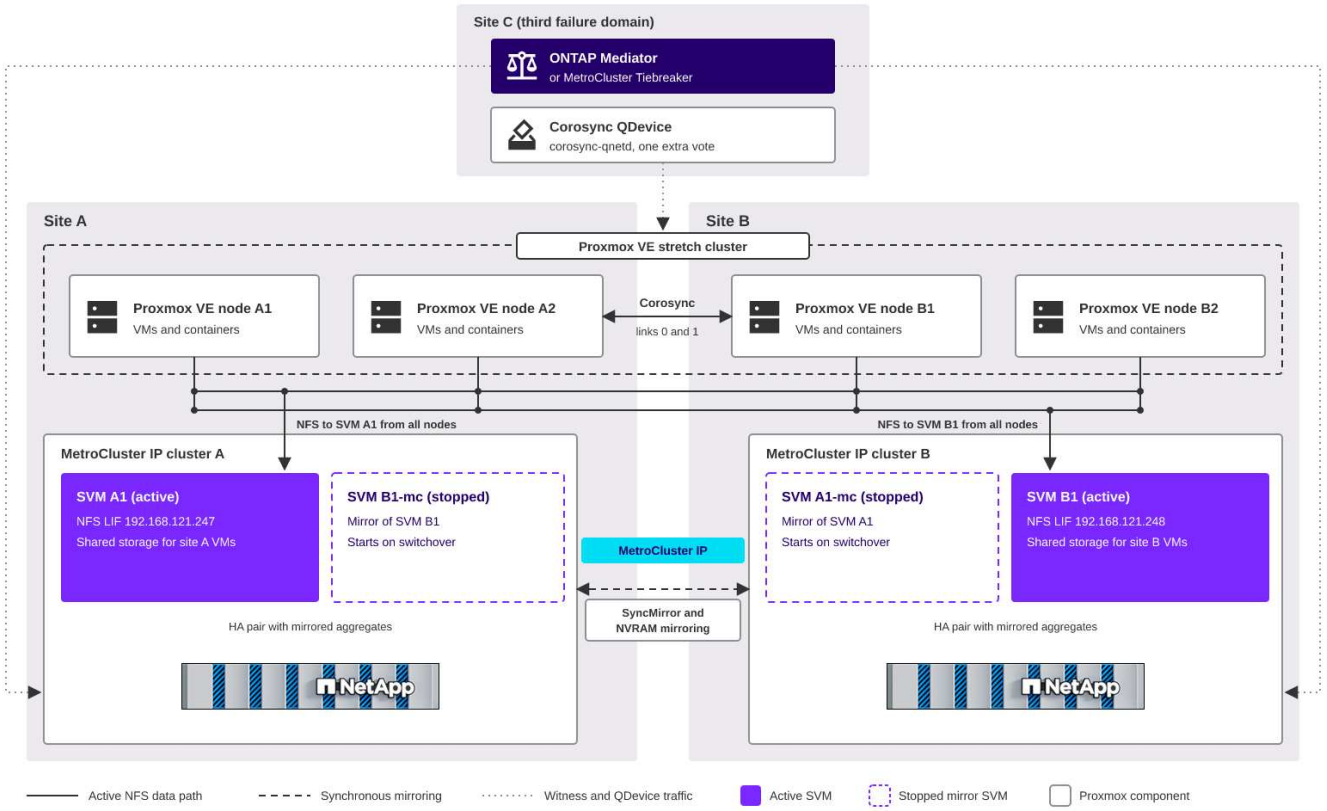
- **SnapMirror active sync schützt eine Teilmenge der Workloads.** Sie wählen aus, welche SVMs oder Volumes geschützt werden sollen, und Sie können für jedes davon unabhängig ein Failover durchführen. Ungeschützte Workloads können dieselben Cluster gemeinsam nutzen.

Beide Lösungen speichern an jedem Standort eine vollständige Kopie der geschützten Daten, benötigen einen Zeugen in einer dritten Ausfalldomäne und erhöhen die Replikationslast auf den Storage-Controllern. Sie unterscheiden sich hinsichtlich Schutzumfang, Failover-Granularität und Clusterdesign.

Vor dem Einsatz einer der beiden Lösungen sollten Sie prüfen, ob Ihre ONTAP Version, MetroCluster oder SnapMirror Active Sync Konfiguration und Ihre Proxmox VE Version gemeinsam in der "NetApp Interoperabilitätsmatrix Tool (IMT)" aufgeführt sind.

MetroCluster Architektur mit Proxmox VE

Das folgende Diagramm zeigt einen Proxmox VE Stretch-Cluster mit einer Vier-Knoten-MetroCluster IP-Konfiguration und gemeinsam genutztem NFS-Storage.



MetroCluster IP Cluster

Jeder Standort verfügt über ein HA-Paar mit gespiegelten Aggregaten. Das MetroCluster IP Back-End-Netzwerk spiegelt Daten (SyncMirror) und NVRAM synchron zum Partnerstandort.

SVMs an beiden Standorten

Jeder Standort kann seine eigenen SVMs bedienen. Für jede SVM unterhält MetroCluster am Partnerstandort eine gestoppte Spiegel-SVM mit dem `-mc` Suffix sowie derselben Konfiguration und denselben LIF-Adressen.

NFS-Zugriff von allen Knoten

Jeder Proxmox VE Knoten bindet den gemeinsamen Storage beider aktiver SVMs, SVM A1 und SVM B1, ein, sodass HA jede VM auf jedem Knoten neu starten kann. Knoten an Standort B erreichen SVM A1, und Knoten an Standort A erreichen SVM B1 über das standortübergreifende Netzwerk. Dies entspricht demselben Zugriffsmodell wie SnapMirror active sync.

Umschaltung

Wenn ein Standort ausfällt, ermöglicht ONTAP Mediator oder MetroCluster Tiebreaker an Standort C eine automatische Umschaltung. Die gespiegelten SVMs am verbleibenden Standort starten und stellen den gesamten gemeinsam genutzten Storage mit denselben NFS-Adressen bereit, und Proxmox VE HA startet die VMs des ausgefallenen Standorts neu. Der Ausfall eines einzelnen Controllers wird durch ein lokales HA-Takeover ohne Umschaltung verarbeitet. Nach der Reparatur des ausgefallenen Standorts werden die Aggregate geheilt und es wird zurückgeschaltet.

Wie MetroCluster auf Fehler reagiert

Die folgende Tabelle zeigt, wie eine MetroCluster IP Konfiguration und der Proxmox VE Stretch-Cluster auf dieselben Fehler wie in Wie die Lösung auf Ausfälle reagiert reagieren. In diesem Beispiel ist SVM A1 an Standort A aktiv und SVM B1 an Standort B aktiv.

Ereignis	ONTAP Verhalten	Verhalten von Proxmox VE
Standort A fällt aus	ONTAP Mediator oder MetroCluster Tiebreaker bestätigt den Ausfall, und ONTAP führt für Standort A ein Failover durch. SVM A1-mc startet an Standort B mit derselben NFS-LIF-Adresse. SVM B1 stellt weiterhin Daten bereit.	Die Knoten an Standort B und das QDevice halten das Quorum aufrecht. HA isoliert die Knoten an Standort A und startet deren VMs auf den Knoten an Standort B neu. VMs, die bereits auf den Knoten an Standort B liefen, bleiben aktiv, und die VMs auf SVM A1 nehmen nach dem Switchover die E/A-Operationen wieder auf.
MetroCluster IP Cluster A fällt aus, Proxmox VE Knoten an Standort A laufen weiter	ONTAP Mediator oder MetroCluster Tiebreaker bestätigt, dass Cluster A nicht erreichbar ist, und ONTAP führt ein Switchover von Standort A durch. SVM A1-mc startet an Standort B mit derselben NFS-LIF-Adresse.	Keine Quorumänderung und kein Neustart der VM. Die VMs auf SVM A1 nehmen nach dem Switchover die E/A wieder auf, wobei die Knoten von Standort A Standort B über das standortübergreifende Netzwerk erreichen.
Ein Controller an Standort A fällt aus	Der HA-Partner an Standort A übernimmt bei einer lokalen HA-Übernahme. Es findet kein Switchover statt.	Keine Auswirkungen. Die VMs unterbrechen die E/A-Vorgänge während der Übernahme kurzzeitig.
Standort B fällt aus	ONTAP schaltet auf Standort B um. SVM B1-mc startet an Standort A mit derselben NFS LIF-Adresse. SVM A1 stellt weiterhin Daten bereit.	Die Knoten von Standort A und das QDevice halten das Quorum aufrecht. HA startet die VMs von Standort B auf den Knoten von Standort A neu, wo sie auf SVM B1 an Standort A zugreifen.

Ereignis	ONTAP Verhalten	Verhalten von Proxmox VE
Verbindung zwischen Standorten fällt aus	Es findet kein Switchover statt, da beide Cluster weiterhin laufen. Jeder Standort bedient weiterhin seine eigenen SVMs, und die Spiegelung zum Partnerstandort wird ausgesetzt, bis die Verbindung wiederhergestellt ist.	Das QDevice gibt seine Stimme der Partition von Standort A, wenn der Trennschalter mit Standort A übereinstimmt. Knoten von Standort B verlieren das Quorum und isolieren sich selbst. HA startet VMs auf SVM A1 auf Knoten von Standort A neu. VMs auf SVM B1 können erst neu gestartet werden, wenn die Verbindung wiederhergestellt ist, da Knoten von Standort A SVM B1 nicht erreichen können.
Standort C fällt aus	Die Spiegelung wird ohne Datenverlust fortgesetzt, ein automatisches Umschalten ist jedoch erst möglich, wenn der Witness verfügbar ist. Sie können weiterhin manuell umschalten.	Der Cluster erhält das Quorum durch die Stimmen der vier Knoten aufrecht. Es sind keine VMs betroffen.
Ein Proxmox VE Knoten fällt aus	Keine Auswirkungen.	HA startet die VMs dieses Knotens auf anderen Knoten neu und bevorzugt dabei Knoten am selben Standort.

Der Ausfall der standortübergreifenden Verbindung ist der Hauptunterschied zu einem Design mit einem primären Standort. Wenn beide Standorte aktive SVMs hosten, mit MetroCluster oder mit zwei SnapMirror active sync SVMs in entgegengesetzte Richtungen, kann der corosync Trennschalter nur einen Standort bevorzugen. VMs, deren aktive SVM sich am anderen Standort befindet, bleiben ausgefallen, bis die Verbindung wiederhergestellt ist. Zur Begrenzung der Auswirkungen empfiehlt sich der Einsatz redundanter standortübergreifender Verbindungen auf separaten physischen Pfaden sowie die Platzierung der kritischsten VMs auf der SVM an dem Standort, den der Trennschalter bevorzugt.

Funktionsvergleich

Überlegung	SnapMirror Active Sync für NAS	MetroCluster IP
Schutzumfang	Ausgewählte SVMs und Volumes	Alle gespiegelten Aggregate und alle SVMs in der Konfiguration
Failover-Granularität	Jede SVM unabhängig	Der gesamte Standort, durch Umschaltung
Ungeschützte Workloads	Ausführung auf ungeschützten SVMs in denselben Clustern	Es können ungespiegelte Aggregate verwendet werden, die nach einer Umschaltung offline gehen, bis Sie sie online schalten
Clusterdesign	Zwei unabhängige Cluster, die über ein IP-Netzwerk verbunden sind	Eine Konfiguration mit zwei Partnerclustern und einem dedizierten MetroCluster IP Back-End-Netzwerk
Witness an Standort C	ONTAP Mediator oder ONTAP Cloud Mediator	ONTAP Mediator oder MetroCluster Tiebreaker
Kopien geschützter Daten	Jeweils einer an jedem Standort	Jeweils eines an jedem Standort, in gespiegelten Aggregaten

Überlegung	SnapMirror Active Sync für NAS	MetroCluster IP
Replikationspfad	SnapMirror synchron über Intercluster-LIFs	SyncMirror und NVRAM-Spiegelung über das MetroCluster IP-Back-End-Netzwerk
NFS-Adresse an beiden Standorten	Erweitertes Layer-2-VLAN. VIP LIFs mit ausstehender BGP-Qualifizierung	Gestrecktes Layer-2-VLAN oder VIP-LIFs mit BGP
Wiederherstellung nach einem Standortausfall	Failback jeder SVM	Die Aggregate reparieren und anschließend den Standort zurückschalten

Auswahlhilfe

- MetroCluster ist die richtige Wahl, wenn alle oder nahezu alle Workloads auf dem Storage einen RPO von null benötigen, beispielsweise wenn ein Unternehmen ausschließlich geschäftskritische VMs im Cluster betreibt oder ein Serviceprovider allen Mandanten dieselbe Verfügbarkeitsstufe anbietet. Sie erhalten eine Schutzdomäne ohne Konfiguration pro Workload.
- SnapMirror active sync ist die richtige Wahl, wenn nur ein Teil der Workloads ein RPO von null benötigt, beispielsweise eine Premium-Stufe für einige Mandanten, oder wenn für jeweils nur einen Mandanten oder eine Applikation ein Failover oder ein Disaster-Recovery-Test erforderlich ist.
- SnapMirror active sync für NAS wird in einer MetroCluster Konfiguration nicht unterstützt. Für jedes Clusterpaar kommt eine eigene Lösung zum Einsatz.
- Die in dieser Lösung enthaltenen Hinweise zu Corosync, QDevice und HA gelten für beide Fälle. Mit MetroCluster richten Sie den QDevice Trennschalter an dem Standort aus, der die Datenversorgung aufrechterhält, wenn die Verbindung zwischen den Standorten ausfällt, und verwenden HA-Knotenaffinitätsregeln, um VMs am selben Standort wie ihre aktive SVM zu halten.
- MetroCluster IP unterstützt außerdem VIP LIFs mit BGP für Layer-3-Netzwerke zwischen Standorten.

Corosync-Überlegungen für einen Proxmox VE Stretch-Cluster

Proxmox VE verwendet corosync für die Clusterzugehörigkeit und das Quorum. Corosync reagiert empfindlicher auf das Netzwerk zwischen den Standorten als SnapMirror active sync, daher empfiehlt es sich, das Clusternetzwerk zuerst zu planen.

Latenz- und Netzwerkdesign

- SnapMirror active sync erfordert eine Intercluster-Round-Trip-Time (RTT) von unter 10 ms. Proxmox empfiehlt eine Corosync-Latenz von unter 5 ms zwischen allen Knoten, daher legt die Corosync-Anforderung die Entfernungsgrenze für die Lösung fest.
- Corosync benötigt eine niedrige, konstante Latenz anstelle einer hohen Bandbreite. Für Corosync empfiehlt sich ein dediziertes Netzwerk, getrennt von Storage- und Live-Migrationsverkehr, damit Storage-Spitzen keine Corosync-Zeitüberschreitungen verursachen.
- Es sollten mindestens zwei Corosync Links, zum Beispiel Link 0 und Link 1, auf separaten physischen Pfaden zwischen den Standorten konfiguriert sein. Corosync verwendet Kronosnet, um die Links bei Ausfall eines Pfads automatisch umzuschalten.

Quorum mit einem QDevice an einem dritten Standort

Die Proxmox VE-Knoten werden gleichmäßig auf Standort A und Standort B verteilt, und an Standort C wird ein QDevice hinzugefügt. Mit vier Knoten und einem QDevice verfügt der Cluster über fünf Stimmen und

benötigt drei für das Quorum, sodass jeder Standort ausfallen kann, ohne dass das Quorum verloren geht. Das QDevice verbindet sich über TCP-Port 5403 mit dem Cluster und unterliegt nicht der Anforderung von corosync an niedrige Latenz, sodass es sich Standort C mit ONTAP Mediator teilen kann. Bei Verwendung von ONTAP Cloud Mediator wird weiterhin ein dritter Standort für das QDevice benötigt, dieser kann jedoch ein kleiner Linux-Host sein, auf dem nicht zusätzlich ein Mediator gehostet wird.

Abstimmung des Trennschalters mit dem primären Cluster

Wenn die Verbindung zwischen den Standorten ausfällt, beide Standorte aber weiterhin Standort C erreichen können, hält ONTAP den primären Cluster an Standort A für die Datenbereitstellung aufrecht. Das QDevice muss seine Stimme demselben Standort geben. Standardmäßig wählt das QDevice die Partition mit der niedrigsten Knoten-ID.

EMPFEHLUNG: Der Proxmox VE-Cluster sollte auf einem Knoten an Standort A erstellt werden, und die anderen Knoten an Standort A sollten hinzugefügt werden, bevor Knoten an Standort B hinzugefügt werden, sodass Standort A die niedrigsten Knoten-IDs erhält. Wenn der primäre Storage für längere Zeit an Standort B verschoben wird, sollte die QDevice `tie_breaker` Einstellung auf eine Knoten-ID von Standort B aktualisiert werden.

Wenn das QDevice stattdessen Standort B bevorzugen würde, würden sich die Knoten von Standort A selbst isolieren, und HA würde VMs auf Knoten von Standort B neu starten, die den aktiven Storage an Standort A nicht erreichen können.

HA-Verhalten und VM-Platzierung

- Proxmox VE HA erkennt typischerweise einen ausgefallenen Knoten und stellt dessen VMs in etwa zwei Minuten wieder her, einschließlich einer 60-sekündigen Watchdog-Fencing-Zeitüberschreitung. Bei einem Standortausfall laufen das SnapMirror active sync Failover und die Proxmox VE HA-Wiederherstellung parallel.
- HA-Knotenaffinitätsregeln mit Knotenprioritäten dienen dazu, VMs auf den Knoten am selben Standort wie ihr primärer Storage zu platzieren und ein Failover zum anderen Standort zu ermöglichen.
- Nach einem Standort Failover ist die HA `failback` Eigenschaft für betroffene VMs bis zum Failback des Storage auf `0` zu setzen. Andernfalls migriert HA die VMs zurück zu den Knoten an Standort A, sobald diese wieder verfügbar sind, während sich der aktive Storage noch an Standort B befindet.
- Die Zeitüberschreitungen für Festplattenzugriffe des Gastbetriebssystems müssen länger sein als die erwartete Failover-Zeit, damit Gäste während eines Storage Failover keine I/O-Fehler melden.

Integration mit Storage Manager für Proxmox

Storage Manager für Proxmox (SMP) bietet Proxmox VE-Administratoren eine zentrale Schnittstelle, um gemeinsam genutzten ONTAP Storage zu provisionieren und VMs mithilfe von ONTAP Snapshots und FlexClone Technologie zu sichern, wiederherzustellen und zu klonen. SMP stellt über die APIs eine Verbindung zum Proxmox VE-Cluster und zu ONTAP her, sodass keine Agenten auf den Proxmox VE-Knoten erforderlich sind.

SMP und SnapMirror active sync schützen vor unterschiedlichen Arten von Ausfällen. SnapMirror active sync hält VMs bei einem Storage- oder Standortausfall in Betrieb, repliziert jedoch jeden Schreibvorgang synchron, einschließlich einer versehentlichen Löschung, eines fehlgeschlagenen Gast-Updates oder von durch Ransomware verschlüsselten Daten. SMP Snapshots liefern zeitpunktgenaue Kopien für die Wiederherstellung nach solchen logischen Ausfällen. Zusammen bieten sie kontinuierliche Verfügbarkeit und eine schnelle operative Wiederherstellung aus demselben ONTAP Storage.

Schutzschicht	Schützt vor	Wiederherstellungspunkt	Verwaltet mit
SnapMirror aktive Synchronisierung	Storage-Systemausfall und Standortausfall	Kein Datenverlust	ONTAP
SMP Backups (ONTAP snapshots)	Versehentliches Löschen, Datenbeschädigung, fehlgeschlagene Updates und Ransomware	Letzte geplante oder bedarfsgesteuerte Datensicherung	SMP
SnapMirror asynchrones Fan-out oder Proxmox Backup Server	Verlust beider Standorte und langfristige Aufbewahrung	Letzte Replikation oder Sicherung	ONTAP oder Proxmox Backup Server

Datensicherung und Wiederherstellung

SMP erstellt absturzkonsistente oder dateikonsistente Backups als ONTAP Snapshots der Storage Volumes, entweder bedarfsgesteuert oder gemäß Richtlinien, und stellt einzelne VMs, Storage oder Ressourcengruppen wieder her:

- Mit Ressourcengruppen und Sicherungsrichtlinien lassen sich derselbe Zeitplan und dieselbe Aufbewahrungsdauer auf die VMs eines Mandanten oder einer Applikation anwenden.
- Für VMs, auf denen der QEMU Guest Agent ausgeführt wird, sollten dateikonsistente Backups verwendet werden, damit die Gastdateisysteme angehalten werden, bevor ONTAP den Snapshot erstellt.
- SMP verwaltet den aktiven Storage. Nach einem SnapMirror active sync Failover ist in SMP eine Erkennung erforderlich, damit der Storage Cluster B zugeordnet wird, bevor Sicherungs- oder Wiederherstellungsvorgänge ausgeführt werden.
- Für eine dritte Kopie außerhalb der beiden Standorte oder für eine längere Aufbewahrung eignet sich eine asynchrone Fan-out-Beziehung mit SnapMirror von den geschützten Volumes aus, alternativ kann Proxmox Backup Server verwendet werden.
- Manipulationssichere Snapshots werden mit SnapMirror active sync nicht unterstützt, daher darf die Snapshot-Sperre in SMP für geschützte Volumes nicht aktiviert werden.

VM-Klonen

SMP nutzt ONTAP FlexClone Technologie, um platzsparende VM-Klone für Entwicklung, Tests und schnelle Provisionierung zu erstellen. Klone, die Sie in geschütztem Storage erstellen, verbrauchen Replikationsbandbreite und Kapazität an beiden Standorten. Klone und Test-Storage, die keine Geschäftskontinuität benötigen, sollten vom Schutz durch SnapMirror active sync ausgeschlossen werden.

SMP Platzierung

- Die SMP-VM läuft als HA-Ressource auf einem durch SnapMirror active sync geschützten gemeinsam genutzten Storage, sodass SMP auch nach einem Storage- oder Standortausfall verfügbar bleibt.
- Die Registrierung des Proxmox VE Cluster und beider ONTAP Cluster in SMP stellt sicher, dass SMP den aktiven Storage an beiden Standorten erreichen kann.

Gemeinsam genutzter NFS-Storage mit SnapMirror active sync für NAS

Ab ONTAP 9.19.1 schützt SnapMirror active sync NAS-Workloads. Die folgenden Hinweise gelten nur für

gemeinsam genutzten NFS-Storage. Für den Einsatz der Lösung mit NFS-Storage ist die "NAS Konfigurationsworkflow" zu verwenden.

Schutz auf SVM-Ebene und Netzwerkidentität

- SnapMirror active sync für NAS schützt eine gesamte Storage VM (SVM). Sie können alle Volumes in der SVM schützen oder einzelne Volumes ausschließen. Nur FlexVol Volumes werden unterstützt, und die SVM darf keine LUNs enthalten.
- Die sekundäre SVM bleibt im Ruhezustand, wobei ihre LIFs bis zu einem Failover inaktiv sind. ONTAP repliziert die SVM-Konfiguration, einschließlich LIF-IP-Adressen, Exportrichtlinien und NFS-Einstellungen, sodass die sekundäre SVM nach einem Failover denselben NFS-Endpunkt bereitstellt.
- Failover ist bei NFSv3 und höher unterbrechungsfrei.
- SnapMirror active sync für NAS ist Aktiv/Passiv, sodass VMs auf Knoten an Standort B über das standortübergreifende Netzwerk Lese- und Schreibzugriffe auf die primäre SVM ausführen. Für aktive Workloads an beiden Standorten kommen zwei SVMs mit entgegengesetzten Replikationsrichtungen zum Einsatz, mit jeweils einer primären SVM an jedem Standort, und die Knotenaffinitätsregel jeder VM ist auf den Standort ihrer primären SVM abzustimmen.
- SnapMirror active sync für NAS wird auf AFF A-Series- und C-Series-Zwei-Knoten-Clustern unterstützt.

Einstellungen des NFS-Clients

Beim NFS Storage sollten NFSv3 oder NFSv4.1 zum Einsatz kommen. Das standardmäßige Hard-Mount-Verhalten sollte beibehalten werden, und die `soft`Mount-Option sollte nicht hinzugefügt werden, damit NFS-E/A-Vorgänge während eines Failover wiederholt werden, anstatt fehlzuschlagen.

Mehrere TCP-Verbindungen zum Storage sorgen für bessere Performance und Fehlertoleranz. Zum Einsatz kommt entweder nConnect oder Session Trunking, nicht beides:

- **nConnect.** Öffnet mehrere TCP-Verbindungen zu einer einzelnen NFS-LIF-Adresse, beispielsweise `nconnect=4`. nConnect funktioniert mit NFSv3 und NFSv4.1 sowie mit einer einzelnen VIP-LIF-Adresse und ist daher die empfohlene Option für SnapMirror active sync für NAS, einschließlich Layer-3-Netzwerken.
- **Session-Trunking.** Fasst beispielsweise mehrere Daten-LIFs in einer NFSv4.1-Session zusammen `vers=4.1,trunkdiscovery,max_connect=16`. Session-Trunking erfordert NFSv4.1 oder höher. Verwenden Sie es nur, wenn die geschützte SVM über mehrere Daten-LIFs verfügt, die Clients an beiden Standorten erreichen können, z. B. in einem Stretched-Layer-2-Netzwerk. Weitere Informationen finden Sie unter "NFS Trunking".

Die Befehle für die Mount-Optionen und die Verifizierungsschritte sind unter "Konfigurieren Sie NFS-Speicher für Proxmox VE" beschrieben.

NFS Storage Provisionierung mit SMP

SMP provisioniert ein ONTAP Volume, erstellt oder wählt eine Exportrichtlinie aus und bindet das Volume als gemeinsam genutzten NFS Storage auf den ausgewählten Proxmox VE Knoten ein. Für Storage in einer geschützten SVM:

- Das Volume ist in der primären SVM zu provisionieren, und als bevorzugte LIF ist die NFS LIF oder in einem Layer 3 Netzwerk die VIP LIF auszuwählen. Die sekundäre SVM verwendet nach einem Failover dieselbe Adresse, sodass die Storage-Definition gültig bleibt.
- Das Storage muss auf allen Proxmox VE-Knoten an beiden Standorten eingebunden sein, damit HA VMs auf jedem Knoten neu starten kann.

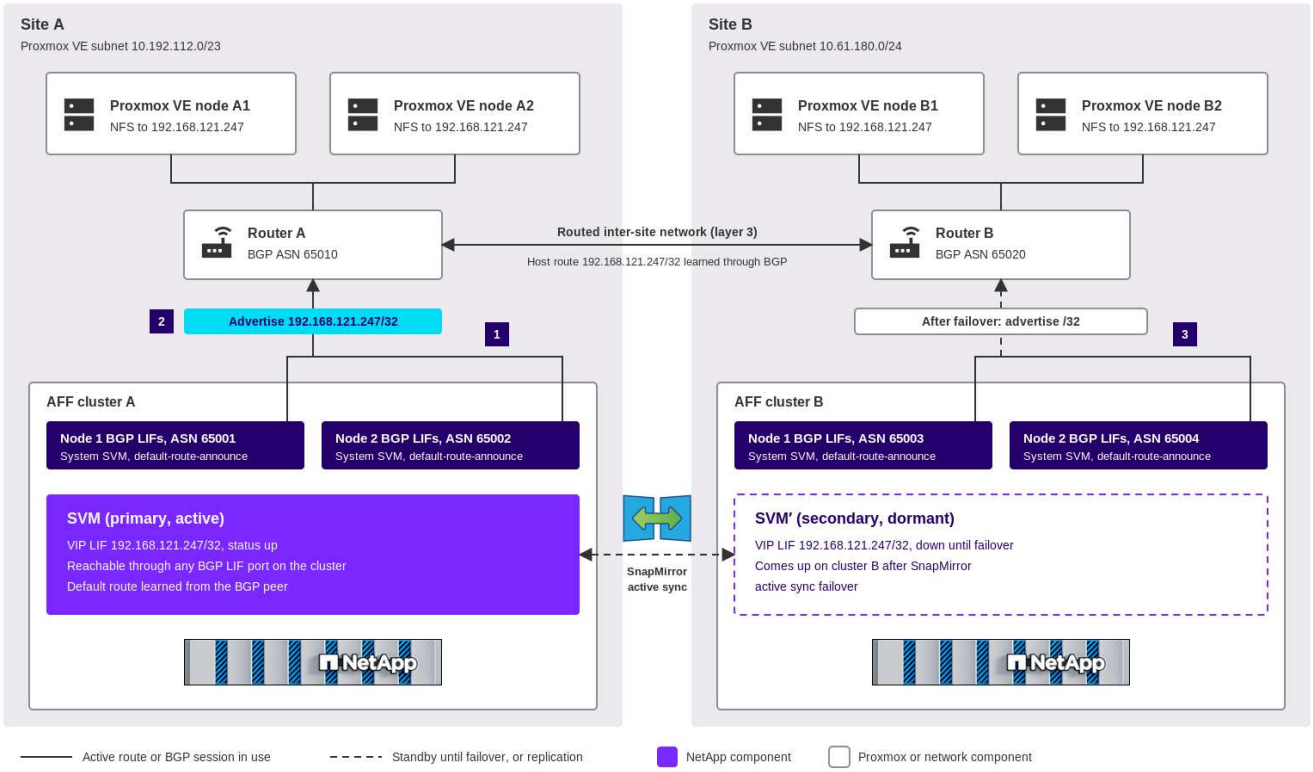
- Es ist sicherzustellen, dass die Exportrichtlinie die Proxmox VE Knoten an beiden Standorten zulässt. ONTAP repliziert die Exportrichtlinie auf die sekundäre SVM.
- Nach der Provisionierung ist zu prüfen, ob das Volume in den SnapMirror Active Sync-Schutz einbezogen ist.

Layer 3 Netzwerke mit VIP LIFs und BGP

SnapMirror active sync für NAS erfordert dieselbe IP-Adresse auf den primären und sekundären SVMs. Wenn das NFS VLAN zwischen Standorten erweitert wird, wandert die LIF IP-Adresse mit der SVM. Wenn die Standorte über ein geroutetes Layer-3-Netzwerk verbunden sind, existiert das Subnetz einer LIF von Standort A an Standort B nicht.

> Zum Zeitpunkt der Veröffentlichung hat NetApp VIP-LIFs mit BGP für SnapMirror active sync für NAS noch nicht als qualifizierte Konfiguration dokumentiert. Vor der Planung eines Layer-3-Designs ist die aktuelle Unterstützung bei NetApp zu bestätigen. Andernfalls ist das NFS-VLAN zwischen den Standorten zu erweitern. MetroCluster IP-Konfigurationen unterstützen VIP-LIFs mit BGP.

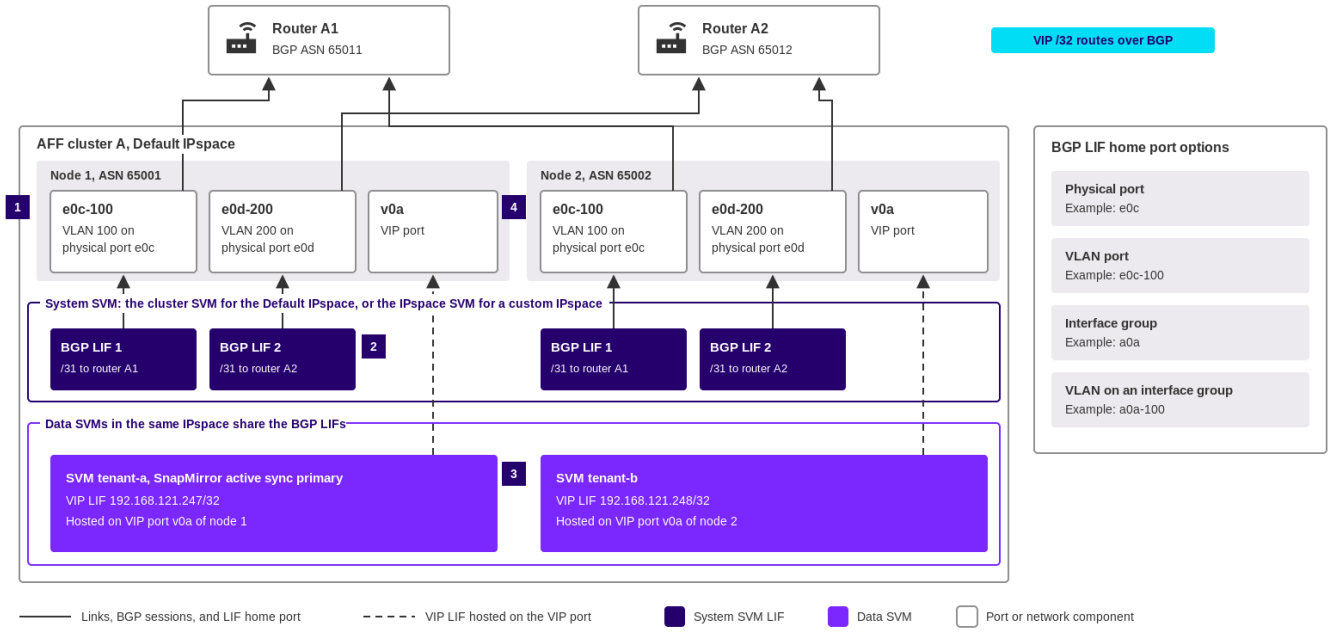
ONTAP virtual IP (VIP) LIFs lösen dieses Problem. Ein VIP LIF gehört zu keinem Subnetz. ONTAP kündigt die VIP-Adresse gegenüber den Peer-Routern mithilfe des Border Gateway Protocol (BGP) als /32-Hostroute an, sodass die Adresse ohne VLAN-Erweiterung zwischen Standorten verschoben werden kann.



1. Jeder Knoten an beiden Standorten verfügt über BGP-LIFs im System-SVM, die mit den Routern an seinem Standort verbunden sind. BGP-LIFs sind knotenspezifisch und werden nicht repliziert, daher müssen sie auf beiden Clustern konfiguriert werden.
2. Die primäre SVM hostet die NFS VIP LIF. Cluster A kündigt die /32-Hostroute an, und die Proxmox VE-Knoten an beiden Standorten erreichen den Storage über das geroutete Netzwerk.
3. Nach einem SnapMirror active sync Failover wird die VIP LIF auf der sekundären SVM aktiviert, Cluster B

kündigt die Host-Route an, und die Router konvergieren auf Standort B.

Bei der erstmaligen Planung von BGP in ONTAP ist es hilfreich zu wissen, welcher SVM jede LIF gehört. BGP LIFs gehören zur System-SVM des IPspace, nicht zu den Daten-SVMs. Ein Satz von BGP LIFs auf jedem Cluster bedient die VIP LIFs aller Daten-SVMs in diesem IPspace, sodass Sie nicht für jeden Mandanten BGP LIFs erstellen. Das folgende Diagramm zeigt das LIF- und Port-Layout auf einem Cluster, mit BGP LIFs auf VLAN Ports.



1. Jeder Knoten verfügt über zwei Ports für BGP, in diesem Beispiel die VLAN-Ports `e0c-100` und `e0d-200`. Jeder Port ist direkt mit einem anderen Router verbunden.
2. Jeder Knoten verfügt über zwei BGP-LIFs in der system SVM, jeweils eine pro Port, mit einem /31-Subnetz und einer BGP-Peer-Gruppe zu einem Router. Für den Default IPspace ist die system SVM die cluster SVM. Für einen benutzerdefinierten IPspace ist es die SVM mit demselben Namen wie der IPspace.
3. Data SVMs im selben IPspace hosten VIP LIFs und benötigen keine eigenen BGP LIFs. Die BGP Peer-Gruppen kündigen die VIP-Routen für alle SVMs im IPspace an.
4. ONTAP erstellt beim Erstellen der ersten BGP-Peer-Gruppe auf jedem Knoten einen VIP-Port, zum Beispiel `v0a`. VIP-LIFs werden auf dem VIP-Port gehostet und sind über jeden Port auf dem Knoten erreichbar, der eine BGP-LIF im IPspace hostet.

Der Home-Port eines BGP LIF kann ein physischer Port, ein VLAN-Port, eine Schnittstellengruppe oder ein VLAN auf einer Schnittstellengruppe sein. Eine Schnittstellengruppe ist nicht erforderlich. NetApp Technical Report TR-4949 empfiehlt für jeden IPspace zwei BGP LIFs auf zwei separaten Ports, die jeweils direkt mit einem anderen First-Hop-Router verbunden sind.

Beachten Sie die folgenden Richtlinien:

- BGP-LIFs führen kein Failover durch. Die Redundanz ergibt sich aus zwei BGP-LIFs pro Knoten, die jeweils mit einem anderen Router per BGP-Peering verbunden sind. Wenn ein Knoten alle seine BGP-Sitzungen für eine SVM verliert, verschiebt ONTAP die VIP-LIF auf einen anderen Knoten, der für diese SVM über eine aktive BGP-Sitzung verfügt.
- Zum Einsatz kommt externes BGP (eBGP) mit einer eindeutigen privaten autonomen Systemnummer (ASN) für jeden ONTAP Knoten und jeden Router.

- Für jeden BGP LIF und den zugehörigen Router wird ein /31-Subnetz (Netzmaske 255.255.255.254) verwendet. Dem BGP LIF wird die Adresse mit ungerader Nummer und dem Router die Adresse mit gerader Nummer zugewiesen.
- ONTAP verarbeitet keine Routen von den Routern. Die Router müssen so konfiguriert sein, dass sie /32-Hostrouten von ONTAP akzeptieren und keine Routenaktualisierungen an den Cluster senden.
- Proxmox VE Knoten dürfen sich nicht im selben Subnetz wie die VIP-Adresse befinden. Ein redundanter Layer-3-Router, beispielsweise mit VRRP oder HSRP, muss sich im Pfad zwischen den Knoten und dem Storage befinden.
- Die BGP-Peer-Gruppen werden `-use-peer-as-next-hop true` so konfiguriert, dass jeder Cluster seine Standardroute von seinen lokalen Routern bezieht. Routen, die auf ein Gateway an Standort A verweisen, sind an Standort B nach einem Failover nicht gültig.
- Multipath-Routing muss aktiviert sein, damit ausgehender VIP-Datenverkehr alle verfügbaren BGP-LIF-Ports nutzt.
- Die BGP-Haltezeit ist gegenüber dem Standardwert von 180 Sekunden zu verringern. TR-4949 empfiehlt eine Haltezeit von 3 Sekunden. Ein Router zieht die Route aus einem ausgefallenen Cluster erst zurück, wenn der Haltetimer abgelaufen ist, und bei einem Storage-Systemausfall bleibt der Router an Standort A online.

Verwandte Informationen

- "ONTAP SnapMirror Active Sync-Architektur"
- "Voraussetzungen für ONTAP SnapMirror active sync"
- "Vorbereitung der Konfiguration des ONTAP Cloud Mediators"
- "Der ONTAP Cloud Mediator für SnapMirror Aktiv-Sync wird konfiguriert"
- "ONTAP MetroCluster Überlegungen zu virtueller IP und BGP"
- "MetroCluster Datenschutz und Notfallwiederherstellung"
- "Konfigurieren und Verwenden von Storage Manager für Proxmox"
- "TR-4949: BGP/VIP mit ONTAP im Rechenzentrum"
- "Proxmox VE Cluster-Manager"
- "Proxmox VE Hochverfügbarkeit"

Konfiguration der Geschäftskontinuität von Proxmox VE mit NAS Storage

Zum Schutz von Proxmox Virtual Environment (VE) VMs vor einem Standortausfall wird ONTAP SnapMirror active sync für NAS mit einem Proxmox VE Stretch-Cluster kombiniert. Es wird ein Mediator konfiguriert, entweder ONTAP Mediator oder ONTAP Cloud Mediator in der NetApp Console, die NFS Storage VM (SVM) geschützt, ihre NFS-Adresse optional mit einer virtuellen IP (VIP) LIF und Border Gateway Protocol (BGP) über ein geroutetes Netzwerk portabel gemacht, der Stretch-Cluster mit einem QDevice erstellt und anschließend der gemeinsam genutzte Storage provisioniert sowie Hochverfügbarkeit (HA) und VM-Backups mit Storage Manager for Proxmox konfiguriert. Das Ergebnis sind kein Datenverlust und die automatische Wiederherstellung der VMs am verbleibenden Standort.

Über diesen Arbeitsablauf

Vor dem Start empfiehlt sich die Prüfung von "Lösungsarchitektur, Ausfallverhalten und Überlegungen zum Corosync-Design". Die Werte in spitzen Klammern, z. B. `<primary_svm>`, werden durch die Werte Ihrer Umgebung ersetzt.

Bevor Sie beginnen

- Zwei AFF A-Series oder C-Series Zwei-Knoten-Cluster müssen mit ONTAP 9.19.1 oder höher ausgeführt werden, einer an Standort A und einer an Standort B.
- Die in ONTAP One enthaltenen Lizenzen für SnapMirror und SnapMirror synchron müssen auf beiden Clustern installiert sein.
- Die Cluster müssen im default IPspace mit einer Cluster Peer-Beziehung verbunden sein, wobei die Round-Trip-Time (RTT) zwischen den Clustern unter 10 ms liegen muss.
- Sie müssen eine Mediatoroption auswählen. Einen Vergleich finden Sie unter "Mediator-Optionen".
  - Für ONTAP Mediator muss ein Linux-Host an Standort C oder in einer anderen dritten Ausfalldomäne installiert sein und von den Cluster- und Knotenmanagement-LIFs beider Cluster aus erreichbar sein.
  - Für ONTAP Cloud Mediator müssen beide Cluster ausgehenden HTTPS-Zugriff auf die NetApp Console haben, entweder direkt oder über einen Proxyserver, mit einer Ping-Latenz von unter 200 ms. Außerdem benötigen Sie ein NetApp Console Unternehmen und die Berechtigung zum Erstellen eines Dienstkontos.
- Eine SVM an Standort A muss NFS für die Proxmox VE-Knoten bereitstellen. Die SVM muss ausschließlich FlexVol Volumes für NAS ohne LUNs enthalten, und ihre Exportrichtlinie muss alle Proxmox VE-Knoten zulassen.
- Es muss eine gerade Anzahl von Knoten mit Proxmox VE 9.0 oder höher installiert sein, gleichmäßig auf Standort A und Standort B verteilt, wobei die corosync-Latenz zwischen allen Knoten unter 5 ms liegen muss.
- Für den corosync QDevice daemon muss an Standort C oder an einem anderen dritten Standort ein Linux-Host verfügbar sein, der von allen Proxmox VE Knoten über TCP-Port 5403 erreichbar ist. Dieser Host wird für beide Mediator-Optionen benötigt.
- Das NFS-VLAN muss zwischen Standort A und Standort B erweitert werden. Für ein geroutetes Layer-3-Netzwerk muss an jedem Standort ein BGP-fähiger Router verfügbar sein, und Sie müssen mit NetApp bestätigen, dass VIP-LIFs mit BGP mit SnapMirror active sync für NAS unterstützt werden.
- Ihre ONTAP und Proxmox VE Versionen müssen zusammen in der "NetApp Interoperabilitätsmatrix Tool (IMT)" aufgeführt sein.
- Für die Provisionierung von gemeinsam genutztem Storage und die Sicherung von VMs muss Storage Manager for Proxmox mit Netzwerkzugriff auf die Proxmox VE-Knoten und auf beide ONTAP Cluster installiert sein.

Schritt 1: Konfiguration des Mediators

Vor der Initialisierung der SnapMirror active sync Beziehung muss der Cluster Peer-Beziehung ein Mediator hinzugefügt werden. ONTAP benötigt den Mediator für geplante und automatische Failover. Der Mediator kann von einem der beiden Cluster aus hinzugefügt werden, und ONTAP fügt ihn automatisch dem anderen Cluster hinzu. Es sollte nur eine Mediator-Option verwendet werden, nicht beide.

Eine der folgenden Optionen steht zur Auswahl.

ONTAP Mediator

Diese Option ist zu verwenden, wenn der Mediator auf einem Linux-Host an Standort C installiert wird. Informationen zur Installation finden Sie unter "ONTAP Mediator installieren oder aktualisieren".

Schritte

1. Der Mediator kann auf einem der beiden Cluster hinzugefügt werden:

```
snapmirror mediator add -peer-cluster <peer_cluster> -type on-prem
-mediator-address <mediator_ip> -username <mediator_user>
```

   Bei entsprechender Aufforderung erfolgt die Eingabe des Mediatorpassworts.

2. Zu prüfen ist, ob der Mediator verbunden ist und ob der Quorumstatus `true` lautet:

```
snapmirror mediator show
```

ONTAP Cloud Mediator

Diese Option ermöglicht das Hosting des Mediators als Dienst in der NetApp Console, sodass kein Mediator-Host an einem dritten Standort erforderlich ist.

Bevor Sie beginnen

- Die Firewalls an beiden Standorten müssen HTTPS-Datenverkehr von beiden Clustern zum NetApp Console API-Endpunkt zulassen. Der aktuelle Hostname des Endpunkts ist unter "Vorbereitung der Konfiguration des ONTAP Cloud Mediators" angegeben.
- Wenn die Cluster Proxyserver verwenden, sollten die IP-Adresse, der Port und die Zugangsdaten des Proxyservers verfügbar sein. Für jeden Cluster sollte ein anderer Proxyserver verwendet werden. Das Root-CA-Zertifikat des Proxyservers muss in ONTAP installiert sein.
- ONTAP enthält gängige Root-CA-Zertifikate, sodass die Installation des NetApp Console Zertifikats in der Regel nicht erforderlich ist. Die Überprüfung erfolgt mit `security certificate show -common-name Sectigo*|USERTrust*|AAA*`.

Schritte

1. In der NetApp Console können Sie Ihre Unternehmens-ID kopieren.
2. Erstellung eines Mitgliedsdienstkontos in der NetApp Console:
   a. Als Unternehmen ist dasjenige festzulegen, in dem Sie ONTAP Cloud Mediator verwenden.
   b. Die Einstellung für die Kategorie lautet **Application**.
   c. Die Rolle sollte auf **ONTAP Mediator Setup Role** gesetzt sein.
   d. Beim Erstellen des Kontos sollten Sie die Client ID und das Client Secret speichern.
3. Der Mediator kann auf einem der beiden Cluster hinzugefügt werden:

```
snapmirror mediator add -peer-cluster <peer_cluster> -type cloud
-org-id <console_org_id> -service-account-client-id <client_id> -use
-http-proxy-local <true|false> -use-http-proxy-remote <true|false>
```

Bei Aufforderung ist das Client-Geheimnis einzugeben.

System Manager kann ebenfalls verwendet werden. Die Auswahl erfolgt über **Schutz** > **Übersicht** > **Mediator** > **Hinzufügen**; als Mediatortyp ist **Cloud** auszuwählen, und die Unternehmen-ID, die Client-ID und das Clientgeheimnis sind einzugeben.

4. Zu überprüfen ist, ob der Mediator-Typ `cloud`, der Verbindungsstatus `connected` und der Quorum-Status `true` sind:

```
snapmirror mediator show
```

Schritt 2: Schutz der NFS SVM mit SnapMirror active sync

Eine ruhende Ziel-SVM wird auf dem Cluster an Standort B erstellt, und die SVM von Standort A wird dorthin repliziert. ONTAP repliziert die Daten synchron und repliziert die SVM-Konfiguration, einschließlich der NFS LIF-Adressen und Exportrichtlinien. Dieser Schritt lässt sich auch in System Manager abschließen, indem für die SVM **Protect** ausgewählt und die `AutomatedFailOver` Richtlinie gewählt wird.

Schritte

1. Auf dem Cluster am Standort B wird die Ziel-SVM erstellt:

```
vserver create -vserver <secondary_svm> -sub-type dp-destination
```

2. Erstellung einer SVM Peer-Beziehung mit der primären SVM auf dem Cluster an Standort B:

```
vserver peer create -vserver <secondary_svm> -peer-vserver <primary_svm>
-peer-cluster <site_a_cluster> -applications snapmirror
```

3. Auf dem Cluster an Standort A erfolgt die Annahme der SVM-Peer-Anfrage:

```
vserver peer accept -vserver <primary_svm> -peer-vserver <secondary_svm>
```

4. Erstellung der SnapMirror Active Sync-Beziehung auf dem Cluster an Standort B:

```
snapmirror create -source-path <primary_svm>: -destination-path
<secondary_svm>: -policy AutomatedFailOver
```

5. Initialisierung der Beziehung:

```
snapmirror initialize -destination-path <secondary_svm>:
```

6. Prüfen, ob die Beziehung synchron ist:

```
snapmirror show -destination-path <secondary_svm>:
```

Das `Mirror State` ist `Snapmirrored`, und das `Relationship Status` ist `InSync`.

7. Optional lassen sich Volumes ausschließen, die keinen Schutz benötigen, z. B. Scratch- oder Test-Volumes:

```
volume modify -vserver <primary_svm> -volume <volume_name> -smas
-protection unprotected
```

Schritt 3: Konfiguration einer VIP LIF mit BGP für Layer-3-Netzwerke



Zum Zeitpunkt der Veröffentlichung hat NetApp VIP-LIFs mit BGP noch nicht als qualifizierte Konfiguration für SnapMirror active sync für NAS dokumentiert. Vor Abschluss dieses Schritts sollte die aktuelle Unterstützung mit NetApp bestätigt werden. Andernfalls kann das NFS-VLAN zwischen den Standorten erweitert und dieser Schritt übersprungen werden.

Wenn das NFS VLAN zwischen Standort A und Standort B erweitert ist, kann dieser Schritt übersprungen werden. Sind die Standorte über ein geroutetes Netzwerk verbunden, werden auf jedem Knoten beider Cluster BGP LIFs erstellt, und die NFS-Adresse wird anschließend auf einer VIP LIF in der primären SVM gehostet. Die VIP-Adresse darf nicht zum Subnetz der Proxmox VE Knoten gehören.

Bevor Sie beginnen

- Jeder Router muss so konfiguriert sein, dass er eine BGP-Sitzung von den BGP LIFs an seinem Standort akzeptiert, /32-Hostrouten akzeptiert und keine Routenaktualisierungen an ONTAP sendet.
- Jeder ONTAP Knoten und jeder Router muss über eine eindeutige private ASN verfügen, und jedes BGP LIF- und Routerpaar muss ein /31-Subnetz haben.

Schritte

1. Wechsel auf jedem Cluster zum erweiterten Berechtigungsstufe Level:

```
set -privilege advanced
```

2. Auf jedem Knoten beider Cluster ist eine BGP-Konfiguration mit einer eindeutigen ONTAP ASN für den Knoten, einer Haltezeit von 3 Sekunden und der Management-IP-Adresse des Knotens als Router-ID zu erstellen:

```
network bgp config create -node <node_name> -asn <node_asn> -holdtime 3
-routerid <node_mgmt_ip>
```

3. Optional lässt sich auf jedem Knoten beider Cluster auf jedem der beiden Ports, die mit den Routern verbunden sind, ein VLAN-Port erstellen:

```
network port vlan create -node <node_name> -vlan-name <port_name>-
```

```
<vlan_id>
```

Sie können auch physische Ports, Schnittstellengruppen oder VLANs auf Schnittstellengruppen als BGP LIF Home-Ports verwenden. Die Ports müssen zu einer Broadcast-Domäne im IPspace gehören.

4. Auf jedem Knoten beider Cluster werden im System SVM zwei BGP LIFs konfiguriert, jeweils eine pro Port, mit einem /31-Subnetz zum Router an diesem Port:

```
network interface create -vserver <system_svm> -lif <bgp_lif_name>
-service-policy default-route-announce -home-node <node_name> -home-port
<vlan_or_port> -address <bgp_lif_ip> -netmask-length 31
```

Für den Default IPspace `<system_svm>` ist dies der Clustername. Für einen benutzerdefinierten IPspace ist es der IPspace-Name. Die BGP LIFs werden für jeden Node nur einmal erstellt und bedienen die VIP LIFs aller Daten-SVMs im IPspace.

5. Für jede BGP LIF erfolgt die Erstellung einer BGP Peer-Gruppe mit dem jeweiligen Router sowie das Erlernen der Standardroute von diesem Router:

```
network bgp peer-group create -peer-group <peer_group_name> -ipspace
<ipspace> -bgp-lif <bgp_lif_name> -peer-address <router_ip> -peer-asn
<router_asn> -use-peer-as-next-hop true
```

6. Es ist zu überprüfen, ob jede Peer-Gruppe aktiv ist:

```
network bgp peer-group show -ipspace <ipspace>
```

7. Multipath-Routing wird auf jedem Cluster aktiviert:

```
network options multipath-routing modify -is-enabled true
```

8. Auf dem Cluster an Standort A erfolgt die Erstellung der NFS VIP LIF in der primären SVM:

```
network interface create -vserver <primary_svm> -lif <vip_lif_name>
-role data -data-protocol nfs -home-node <node_name> -address
<vip_address> -is-vip true -failover-policy broadcast-domain-wide
```

9. Im Cluster an Standort A ist zu prüfen, ob der BGP-Status `up` für die primäre SVM auf jedem Knoten vorliegt:

```
network bgp vserver-status show
```

10. Auf beiden Routern ist zu überprüfen, ob die /32-Route für die VIP-Adresse von Cluster A erlernt wurde.

Schritt 4: Erstellen des Proxmox VE Stretch-Clusters mit einem QDevice

Der Cluster wird von einem Knoten an Standort A aus erstellt, damit die Knoten an Standort A die niedrigsten Knoten-IDs erhalten, und an Standort C wird ein QDevice hinzugefügt. Das QDevice weist Standort A das Stimmrecht zu, wenn die standortübergreifende Verbindung ausfällt, was der SVM entspricht, die ONTAP aktiv hält.

Schritte

1. Auf dem ersten Knoten von Standort A wird der Cluster mit zwei corosync Links in separaten Netzwerken erstellt:

```
pvecm create <cluster_name> --link0 <node_link0_ip> --link1
<node_link1_ip>
```

2. Der Beitritt zum Cluster erfolgt auf jedem verbleibenden Knoten von Standort A und anschließend auf jedem Knoten von Standort B:

```
pvecm add <first_node_ip> --link0 <node_link0_ip> --link1
<node_link1_ip>
```

3. Sicherzustellen ist, dass die Knoten an Standort A die niedrigsten Knoten-IDs aufweisen:

```
pvecm nodes
```

4. Die Installation des QDevice Daemon erfolgt auf dem QDevice-Host an Standort C oder an einem anderen dritten Standort:

```
apt install corosync-qnetd
```

5. Auf jedem Proxmox VE-Knoten erfolgt die Installation des QDevice client:

```
apt install corosync-qdevice
```

6. Hinzufügen des QDevice zum Cluster auf einem Proxmox VE-Knoten:

```
pvecm qdevice setup <qdevice_ip>
```

7. Überprüfung, ob der Cluster mit der QDevice-Abstimmung beschlussfähig ist:

```
pvecm status
```

Für einen Cluster mit vier Knoten gilt: `Expected votes` ist `5`, `Quorum` ist `3`, und die `Flags` umfassen `Quorate Qdevice`.

Schritt 5: Geschützten gemeinsam genutzten NFS Storage provisionieren

Zum Provisionieren des NFS Storage in der primären SVM und zum Einbinden auf allen Proxmox VE Knoten an beiden Standorten wird die NFS LIF oder VIP-Adresse verwendet, die beide SVMs gemeinsam nutzen. Storage Manager for Proxmox (SMP) erstellt in einem einzigen Workflow das ONTAP Volume, die Exportrichtlinie und die Proxmox VE Storage-Definition. Wenn SMP nicht verwendet wird, erfolgt die Erstellung des Volumes in ONTAP und das Hinzufügen als NFS Storage mit der Proxmox VE CLI.

Für die Provisionierung des Storage kann eine der folgenden Methoden verwendet werden.

Storage Manager for Proxmox

SMP dient zum Provisionieren des Storage. SMP muss installiert sein, und der Proxmox VE Cluster sowie beide ONTAP Cluster müssen als Pläne hinzugefügt werden. Einzelheiten sind unter "Konfigurieren und Verwenden von Storage Manager für Proxmox" zu finden.

1. In SMP erfolgt die Auswahl von **Provision** > **Add Volume** und anschließend von **NFS**.
2. In **ONTAP Details** erfolgt die Auswahl der primären SVM sowie die Eingabe von Volume-Name und -Größe; außerdem wird die NFS LIF oder VIP LIF als bevorzugte LIF ausgewählt.
3. Erforderlich ist eine Exportrichtlinie, die die Proxmox VE Knoten an beiden Standorten zulässt; alternativ kann eine solche erstellt werden.
4. In **Proxmox Details** erfolgt die Auswahl des Clusters und aller Knoten an beiden Standorten sowie von NFS v3 oder NFS v4.1 und den Inhaltstypen.
5. Es ist sicherzustellen, dass **Mount the datastore** ausgewählt ist; anschließend ist **Provision** auszuwählen.
6. Auf dem Cluster A ist zu prüfen, ob das Volume in den Schutz von SnapMirror active sync einbezogen ist:

```
volume show -vserver <primary_svm> -volume <volume_name> -fields
smas-protection
```

CLI

In der Proxmox VE CLI kann ein bereits in der primären SVM vorhandenes Volume als NFS Storage hinzugefügt werden.

1. Auf einem Proxmox VE-Knoten erfolgt das Hinzufügen des NFS Storage:

```
pvesm add nfs <storage_id> --server <nfs_lif_or_vip_address>
--export <export_path> --content images,rootdir --options
vers=<nfs_version>,nconnect=4
```

Verwendet werden `3` oder `4.1` für `<nfs_version>`. Die `soft` Mount-Option sollte nicht hinzugefügt werden.

2. Zu überprüfen ist, ob der Storage auf jedem Knoten aktiv ist:

```
pvesm status --storage <storage_id>
```

Festlegen der NFS-Mount-Optionen

Mit nConnect lassen sich mehrere TCP-Verbindungen zur NFS LIF oder VIP-Adresse öffnen, um die Performance und Fehlertoleranz zu verbessern. Wenn die geschützte SVM über mehrere Daten-LIFs verfügt, die Clients an beiden Standorten erreichen können, kann stattdessen NFSv4.1 Session Trunking verwendet werden. Verwenden Sie entweder nConnect oder Session Trunking, nicht beides. Einzelheiten finden Sie unter "Konfigurieren Sie NFS-Speicher für Proxmox VE".

Schritte

1. Wenn Sie den Storage mit SMP oder ohne nConnect provisioniert haben, werden die Mount-Optionen auf einem Proxmox VE-Knoten festgelegt:

```
pvesm set <storage_id> --options vers=<nfs_version>,nconnect=4
```

Für die Verwendung von Session Trunking ist stattdessen folgende Einstellung erforderlich:

```
pvesm set <storage_id> --options vers=4.1,trunkdiscovery,max_connect=16
```

Proxmox VE wendet neue Mount-Optionen beim nächsten Einhängen des Storage an. Das erneute Einhängen des Storage auf jedem Knoten erfolgt während eines Wartungsfensters, nachdem die VMs von diesem Knoten migriert wurden.

2. Überprüfung der Optionen in `/etc/pve/storage.cfg`.
3. Auf jedem Proxmox VE Knoten muss sichergestellt sein, dass mehrere Verbindungen zur NFS-Serveradresse bestehen:

```
ss -an | grep :2049
```

Schritt 6: Konfiguration von HA und VM-Backups

Die VMs werden mit Knotenaffinitätsregeln zur Hochverfügbarkeit hinzugefügt, die Standort A bevorzugen, wo die primäre SVM Daten bereitstellt. Anschließend werden die VMs mit SMP Backup-Richtlinien vor logischen Fehlern wie versehentlichem Löschen oder Ransomware geschützt. SnapMirror active sync repliziert diese Fehler synchron und ersetzt daher keine zeitpunktgenauen Backups.

Schritte

1. Hinzufügen jeder geschützten VM zu HA:

```
ha-manager add vm:<vm_id> --state started
```

2. Erstellung einer Knotenaffinitätsregel, die Knoten an Standort A bevorzugt und ein Failover auf Knoten an Standort B ermöglicht:

```
ha-manager rules add node-affinity <rule_name> --resources
vm:<vm_id>,vm:<vm_id> --nodes
"<site_a_node1>:2,<site_a_node2>:2,<site_b_node1>:1,<site_b_node2>:1"
```

3. Optional kann die Zeitüberschreitung für Datenträger in jedem Gastbetriebssystem so erhöht werden, dass sie länger ist als die erwartete Dauer des Storage Failover.
4. In SMP wird **Protect** > **Backup** > **Resource Group** ausgewählt, und es wird eine Ressourcengruppe für die VMs oder das Storage jedes Mandanten oder jeder Applikation erstellt.
5. Unter **Protect** > **Backup** > **Policies** > **Add** lässt sich eine Richtlinie mit der Sicherungshäufigkeit und Aufbewahrungsdauer für die Ressourcengruppe erstellen.

   Für VMs, auf denen der QEMU guest agent ausgeführt wird, wird in **Advanced Options** die Option **VM Consistency** ausgewählt.

6. Zur Überprüfung der Richtlinie wird eine bedarfsgesteuerte Datensicherung ausgeführt und anschließend eine Test-VM daraus wiederhergestellt.

Schritt 7: Geplantes Failover testen

Vor dem Platzieren von Produktions-VMs auf dem gemeinsam genutzten Storage empfiehlt sich eine Validierung des Designs. Ein geplanter Failover verschiebt die aktive SVM ohne Datenverlust zu Standort B, sodass dies während eines Wartungsfensters getestet und anschließend ein Failback durchgeführt werden kann.

Schritte

1. Live-Migration der Test-VMs zu den Knoten von Standort B.
2. Vor dem Failover ist sicherzustellen, dass HA die VMs nicht auf die Knoten von Standort A zurückverschiebt:

```
ha-manager set vm:<vm_id> --failback 0
```

3. Auf dem Cluster von Standort B wird ein geplantes Failover gestartet:

```
snapmirror failover start -destination-path <secondary_svm>:
```

4. Überwachung des Failovers bis zum Abschluss:

```
snapmirror failover show
```

5. Es ist sicherzustellen, dass VM I/O weiterläuft und der Storage auf allen Proxmox VE-Knoten aktiv bleibt.
6. Wenn Sie eine VIP LIF verwenden, sollten Sie sicherstellen, dass beide Router die /32-Route von Cluster B lernen.
7. In SMP wird eine Erkennung für die ONTAP Pläne ausgeführt und anschließend ein On-Demand-Backup, um zu überprüfen, ob SMP die VMs der SVM an Standort B schützt.
8. Nach Abschluss des Tests erfolgt das Failback zu Standort A, und anschließend wird `failback` für die Test-VMs wieder auf `1` gesetzt.

Ergebnis

Die Proxmox VE VMs laufen weiterhin auf demselben gemeinsam genutzten NFS-Storage, während sich die aktive SVM zwischen Standorten bewegt, und der Cluster erholt sich automatisch von einem ungeplanten Standortausfall.

Verwandte Informationen

- "Mit ONTAP SnapMirror Active Sync für NAS schützen"
- "ONTAP VIP LIFs konfigurieren"
- "Vorbereitung der Installation des ONTAP Mediators"
- "Vorbereitung der Konfiguration des ONTAP Cloud Mediators"
- "Der ONTAP Cloud Mediator für SnapMirror Aktiv-Sync wird konfiguriert"
- "snapmirror mediator add"
- "Konfigurieren Sie NFS-Speicher für Proxmox VE"
- "Proxmox VE corosync Unterstützung für externe Abstimmung"

Konfigurieren und Verwenden von Storage Manager für Proxmox

Storage Manager für Proxmox (SMP) bietet umfassende Speicherbereitstellung und Lebenszyklusverwaltung für virtuelle Maschinen in Proxmox-Umgebungen mit NetApp ONTAP-Speichersystemen. SMP ermöglicht Administratoren, Speicher direkt zu verwalten und vereinfacht den Betrieb durch automatisierte Bereitstellungs-, Backup-, Restore- und Klonfunktionen.

Erfahren Sie mehr über Storage Manager für Proxmox

Storage Manager für Proxmox (SMP) bietet umfassendes Speichermanagement für virtuelle Maschinen in Proxmox-Umgebungen, die NetApp Speichersysteme nutzen. Indem Administratoren den Speicher direkt verwalten können, vereinfacht SMP sowohl Speicher- als auch Datenmanagementaufgaben in Proxmox-Umgebungen.

Hauptmerkmale

- **End-to-End-Speicherverwaltung**: SMP bietet eine vollständige Lebenszyklusverwaltung für virtuelle Maschinen, von der Speicherbereitstellung bis zu Backup und Recovery.
- **Direkte Speicherverwaltung**: Proxmox-Administratoren können den Speicher direkt verwalten, wodurch die Abläufe optimiert und die Komplexität reduziert wird.

- **Eigenständiges Installationsprogramm**: SMP wird als eigenständiges Installationsprogramm bereitgestellt, das sich nahtlos über APIs mit Proxmox-Knoten verbindet.

Fähigkeiten

Jede Komponente von SMP ist darauf ausgelegt, die Effizienz des Speichermanagements zu verbessern:

- **Speicherbereitstellung**: Speicherressourcen für Proxmox-Hosts und zugehörige virtuelle Maschinen einfach zuweisen und verwalten.
  - **NFS-Speicherbereitstellung**: Richten Sie ONTAP NFS-Speicher ein und konfigurieren Sie ihn für die Verwendung mit Ihrer Proxmox-Umgebung.
  - **iSCSI-Speicherbereitstellung**: Implementieren Sie Thick LVM mit Multipath für ein robustes und effizientes iSCSI-Speichermanagement.
- **Backup und Recovery**: Führen Sie zuverlässige Backups und schnelle Recoveries durch, um die Integrität und Verfügbarkeit der Daten zu gewährleisten.
  - **Absturzkonsistente und dateikonsistente Backups**: Gewährleisten Sie die Datenintegrität durch die Einrichtung von absturzkonsistenten und dateikonsistenten Backup-Mechanismen.
  - **VM-Wiederherstellungsvorgänge**: Führen Sie Wiederherstellungsprozesse für virtuelle Maschinen aus, um Daten wiederherzustellen und die Systemverfügbarkeit aufrechtzuerhalten.
- **Speichereffizienz**: ONTAP bietet eine umfassende Suite von Speichereffizienztechnologien, die den für Daten benötigten Speicherplatz minimieren. Diese Technologien reduzieren nicht nur den Speicherverbrauch, sondern verbessern auch die Systemleistung und bieten:
  - **Schnelle VM-Bereitstellung**: Optimieren Sie die Bereitstellung virtueller Maschinen für eine schnellere Bereitstellung.
  - **Schnellere Datensatzkopien**: Beschleunigen Sie die Duplizierung von Datensätzen für ein effizientes Datenmanagement.

Voraussetzungen

Bitte stellen Sie sicher, dass Sie Folgendes erledigt haben, bevor Sie fortfahren:

- Funktionierender Proxmox Virtual Environment (PVE) 9.x oder neuer Cluster.
- ONTAP All Flash FAS (AFF) Storage mit aktiviertem NFS- und iSCSI-Protokoll auf SVM-Ebene. Anweisungen finden Sie unter "Konfigurieren von NFS-Datenspeichern mit ONTAP" und "Konfigurieren Sie Proxmox VE 9.x für iSCSI mit ONTAP-Speicher".



Für die iSCSI-LUN-Konfiguration sollte Folgendes aktiviert sein:

Multipath und iSCSI auf allen Proxmox-Hosts installieren:

```
apt update
apt install open-iscsi multipath-tools -y
systemctl enable --now iscsid multipathd
```

iSCSI-Initiator konfigurieren und über iSCSI verbinden (auf Proxmox-Hosts):

Erstellen oder aktualisieren `/etc/multipath.conf`:

```
touch /etc/multipath.conf
```

Oder verwenden Sie:

```
cat << 'EOF' > /etc/multipath.conf
defaults {
    user_friendly_names yes
    find_multipaths yes
}
blacklist {
    devnode "^sd[a]$"
}
EOF
```

- Proxmox-Hosts und ONTAP-Speicher sind vom SMP-Host aus über das Netzwerk erreichbar.

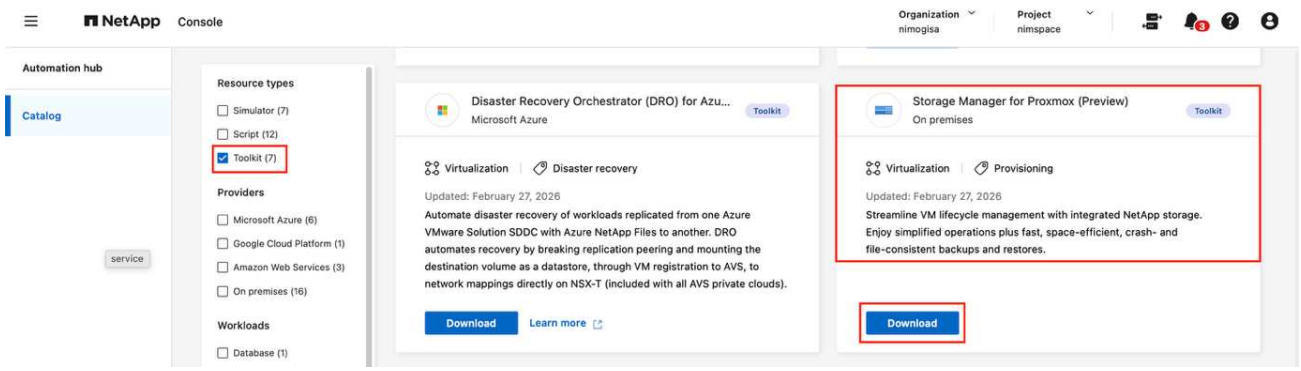
Installieren und Einrichten von Storage Manager für Proxmox

Um mit SMP zu beginnen, verwenden Sie ein Windows-Betriebssystem auf einer dafür vorgesehenen virtuellen Maschine. SMP kann unter Windows Server 2019, 2022 und 2025 ausgeführt werden.

Schritte

1. Laden Sie das SMP-Paket (~17MB) von der "NetApp Console Automation-Hub" herunter.

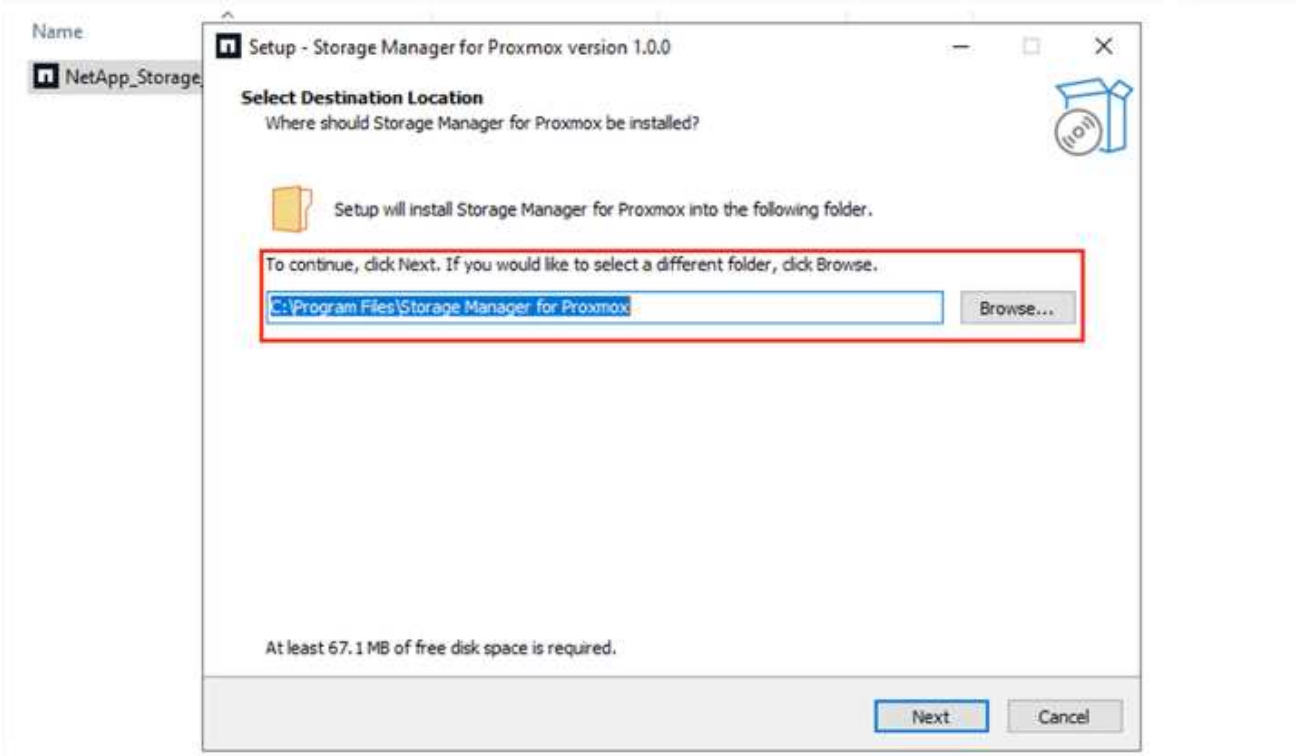
▼ **SMP-Downloadseite anzeigen**



2. Entpacken Sie das Paket.
3. Führen Sie die ausführbare Datei aus, um den Dienst zu installieren und zu starten.

> Es sind keine zusätzlichen Paketabhängigkeiten erforderlich, da SMP die verfügbaren APIs nutzt, um sowohl Bereitstellungs- als auch Datensicherungs-Workflows zu orchestrieren.

▼ **SMP-Installationsassistent anzeigen**



Alternative Installation mit dem Shift-Toolkit

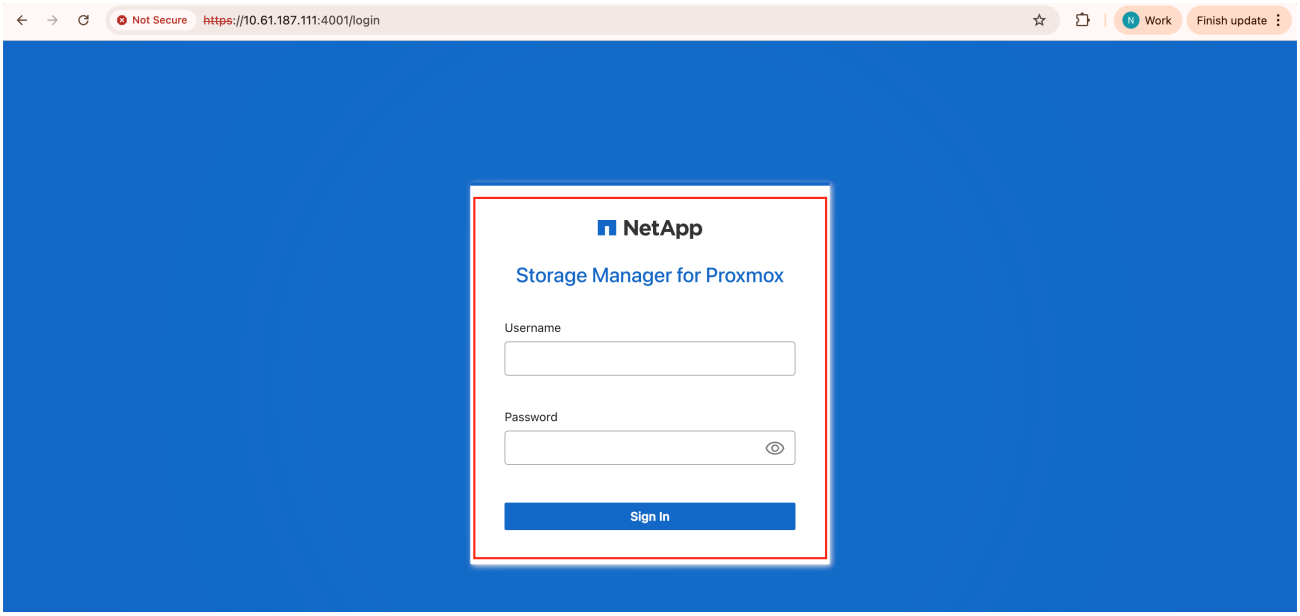
Alternativ zum eigenständigen Installationsprogramm können Sie Proxmox VE Storage Manager mithilfe des Shift toolkit installieren:

- Open Shift Toolkit.
- Navigieren Sie zu **Einstellungen** > **Erweitert** > **Speicherverwaltung**.
- Aktivieren Sie Proxmox VE über den Kippschalter.
- Warten Sie, bis das System die notwendigen Komponenten automatisch installiert hat.
- Nach Abschluss der Installation können Sie auf den Storage Manager zugreifen, indem Sie auf **Ansicht** klicken oder einen Webbrowser zu `https://<Shift_server_IP>:4001` öffnen.

  Zum Beispiel: `https://10.61.187.117:4001`

4. Öffnen Sie einen Webbrowser und greifen Sie auf die SMP-Benutzeroberfläche zu, indem Sie `https://<IP address specified during installation>:4001` eingeben

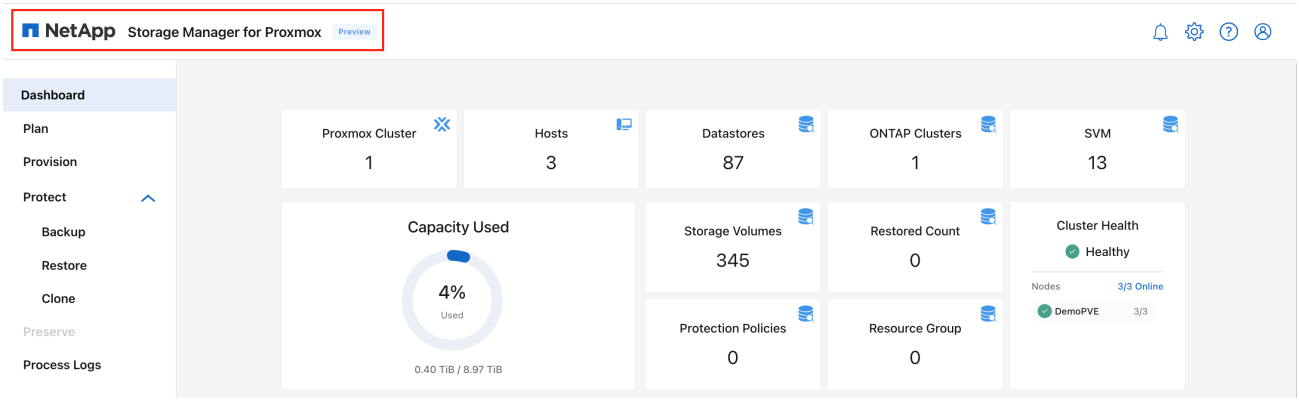
▼ SMP-Anmeldebildschirm anzeigen



5. Die Anmeldung bei SMP erfolgt mit dem Standardbenutzernamen `admin` und dem Passwort `admin`.

   Bei entsprechender Aufforderung erfolgt die Änderung des Standardpassworts. Dieselben Standardanmeldeinformationen gelten auch bei der Installation von SMP mit Shift toolkit.

▼ SMP-Startseite anzeigen



Storage Manager für Proxmox konfigurieren

Sobald Speicher und Konnektivität sowohl zum Speicher als auch zu den Proxmox-Knoten ordnungsgemäß konfiguriert sind, konfigurieren Sie SMP, um die Bereitstellung und den Schutz virtueller Maschinen mithilfe von ONTAP Snapshot und FlexClone-Funktionen zu automatisieren.

Im ersten Schritt müssen der ONTAP-Speicherendpunkt und anschließend die Ziel-Proxmox-Knoten zu SMP hinzugefügt werden.

Bevor Sie beginnen

Stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- SMP ist installiert
- Die SMP-Instanz verfügt über Konnektivität zu den Proxmox-Knoten und Speichersystemen
- ONTAP Cluster zur Bereitstellung von NFS- oder iSCSI-Speicherpools

- Die DNS-Auflösung erfolgt bei Verwendung von DNS-Namen. Andernfalls verwenden Sie IP-Adressen für die Erkennung.
- Die Umgebung unterstützt Versionen von Proxmox Virtual Environment-Servern

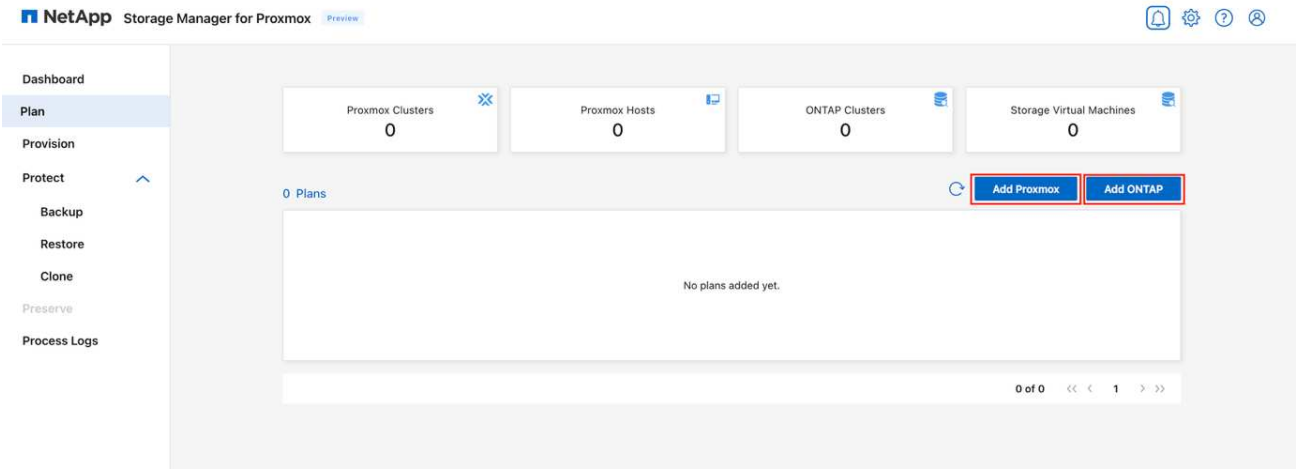
Über diese Aufgabe

Sobald die Verbindung zwischen Hypervisor und Storage hergestellt ist, ist die Konfiguration mit wenigen Klicks und in etwa 2 Minuten erledigt.

Schritte

1. Melden Sie sich bei SMP an.
2. Wählen Sie in der linken Navigationsleiste von SMP die Option **Plan**.
3. Klicken Sie auf **Plan hinzufügen**.

▼ Plan hinzufügen anzeigen

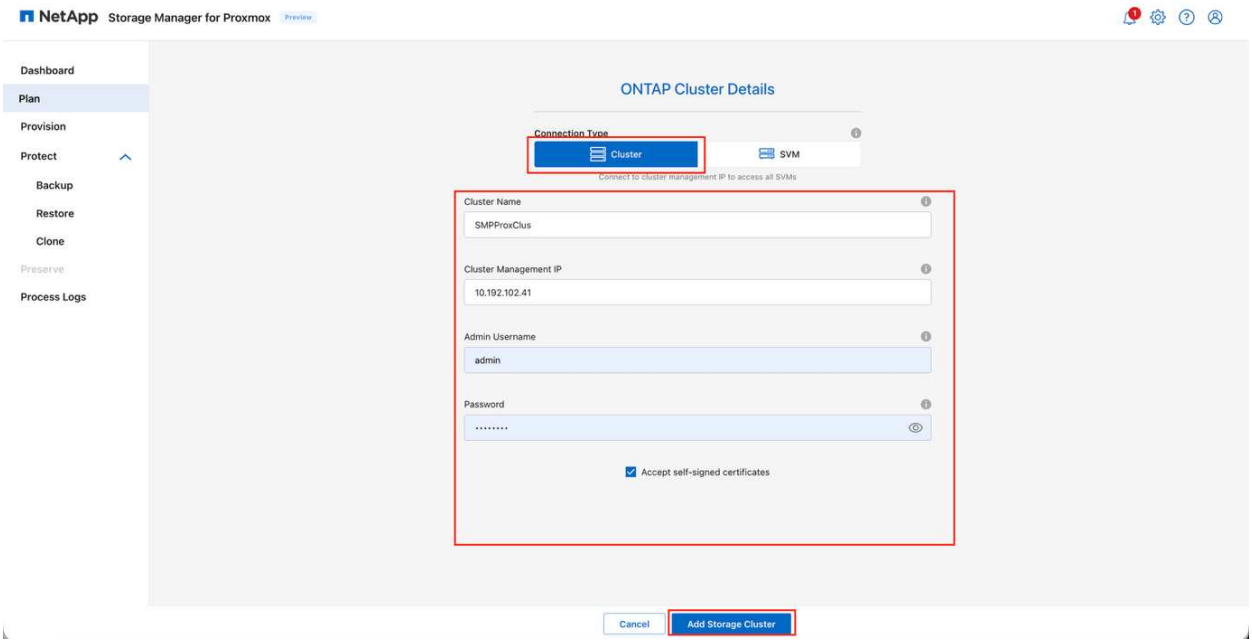


4. Klicken Sie auf **Add ONTAP**, um die Anmeldeinformationen eines ONTAP-Speichersystems hinzuzufügen.

   Sie können ONTAP entweder über den Cluster-Endpunkt oder die SVM-Management-LIF hinzufügen.

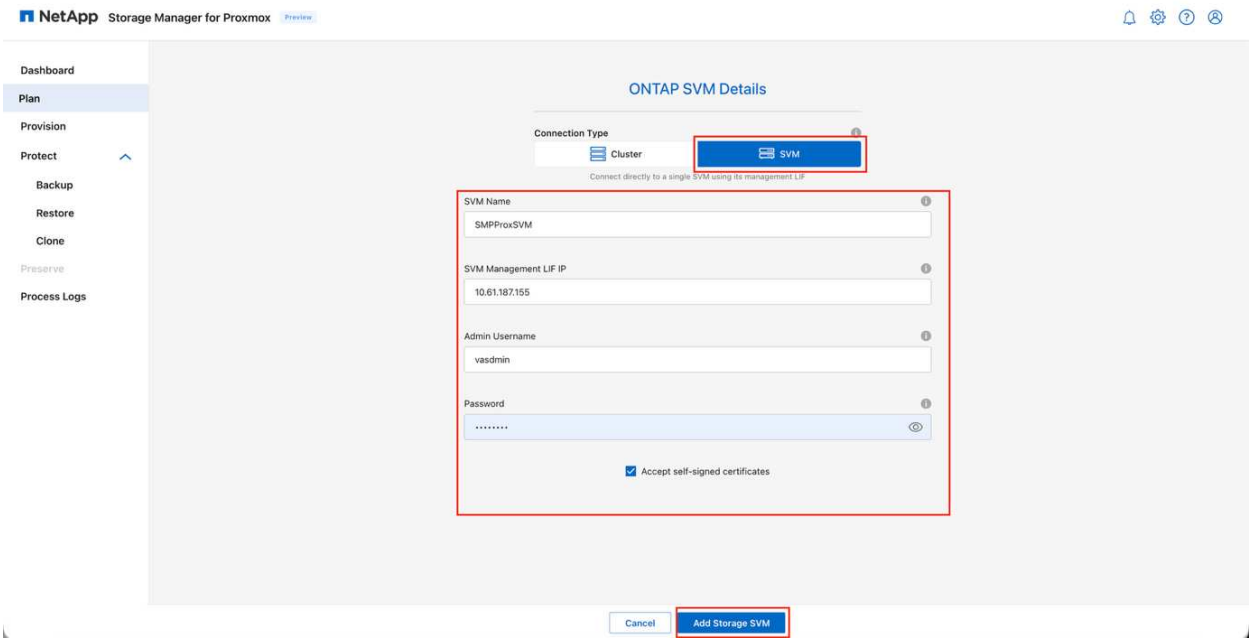
5. Um den Cluster-Endpunkt hinzuzufügen, geben Sie die folgenden Details an:
   a. Cluster-IP-Adresse oder FQDN
   b. Benutzername für den Zugriff auf den ONTAP Cluster
   c. Passwort für den Zugriff auf den ONTAP Cluster
   d. Wählen Sie **Selbstsigniertes Zertifikat akzeptieren** und klicken Sie auf **Speichercluster hinzufügen**

▼ Add ONTAP: Cluster-Endpunkt anzeigen



6. Um die SVM-Verwaltungs-LIF hinzuzufügen, geben Sie die folgenden Details an:
   a. SVM-Management LIF oder FQDN
   b. Benutzername für den Zugriff auf die SVM
   c. Passwort für den Zugriff auf die SVM
   d. Wählen Sie **Selbstsigniertes Zertifikat akzeptieren** und klicken Sie auf **Speichercluster hinzufügen**

▼ Ansicht hinzufügen ONTAP: SVM-Management LIF



7. Klicken Sie auf **Proxmox hinzufügen**, um die Anmeldeinformationen eines Proxmox-Knotens hinzuzufügen, der bei SMP registriert werden soll.

   Um Proxmox-Knoten hinzuzufügen, geben Sie die IP-Adresse eines der vorhandenen Proxmox-Knoten an. Der Erkennungsauftrag fragt den Cluster automatisch ab, um alle wichtigen Konfigurationsdetails zu erfassen.

8. Bitte geben Sie folgende Details an:

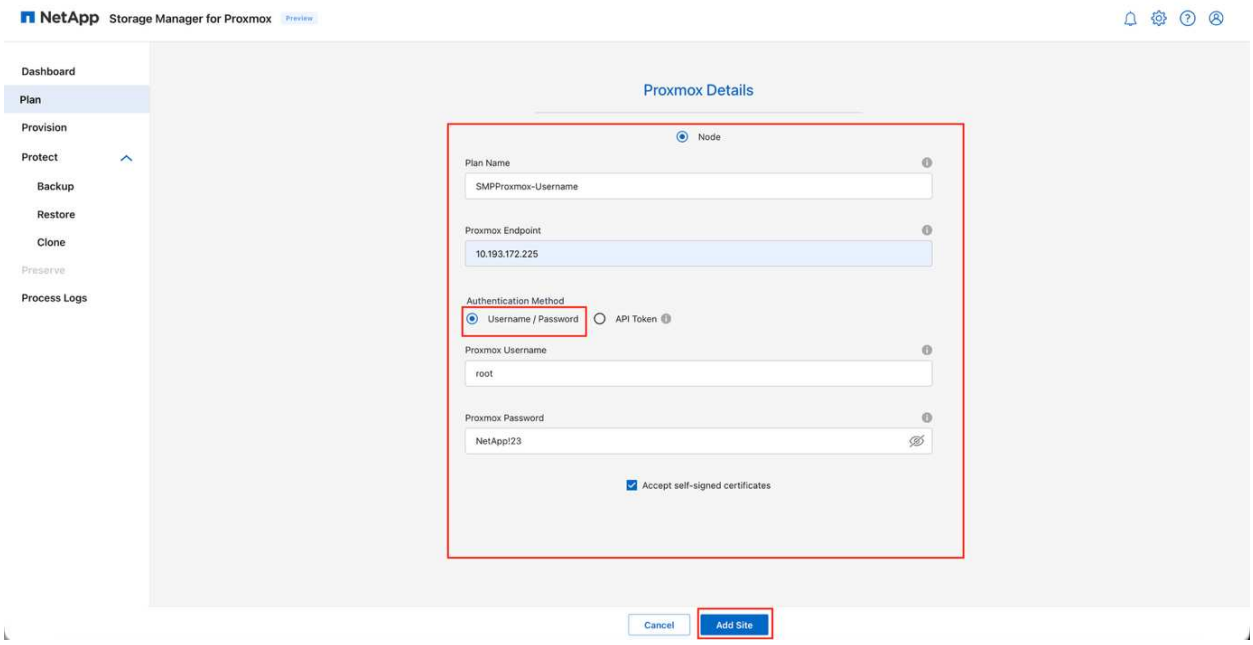
   a. Proxmox eigenständige IP-Adresse oder FQDN

   b. Benutzername für den Zugriff auf Proxmox

   c. Passwort für den Zugriff auf den Proxmox-Host zur Durchführung einer Ressourceninventur

   d. Wählen Sie **Selbstsigniertes Zertifikat akzeptieren** und klicken Sie auf **Weiter**

▼ Proxmox hinzufügen: Knotenanmeldeinformationen anzeigen

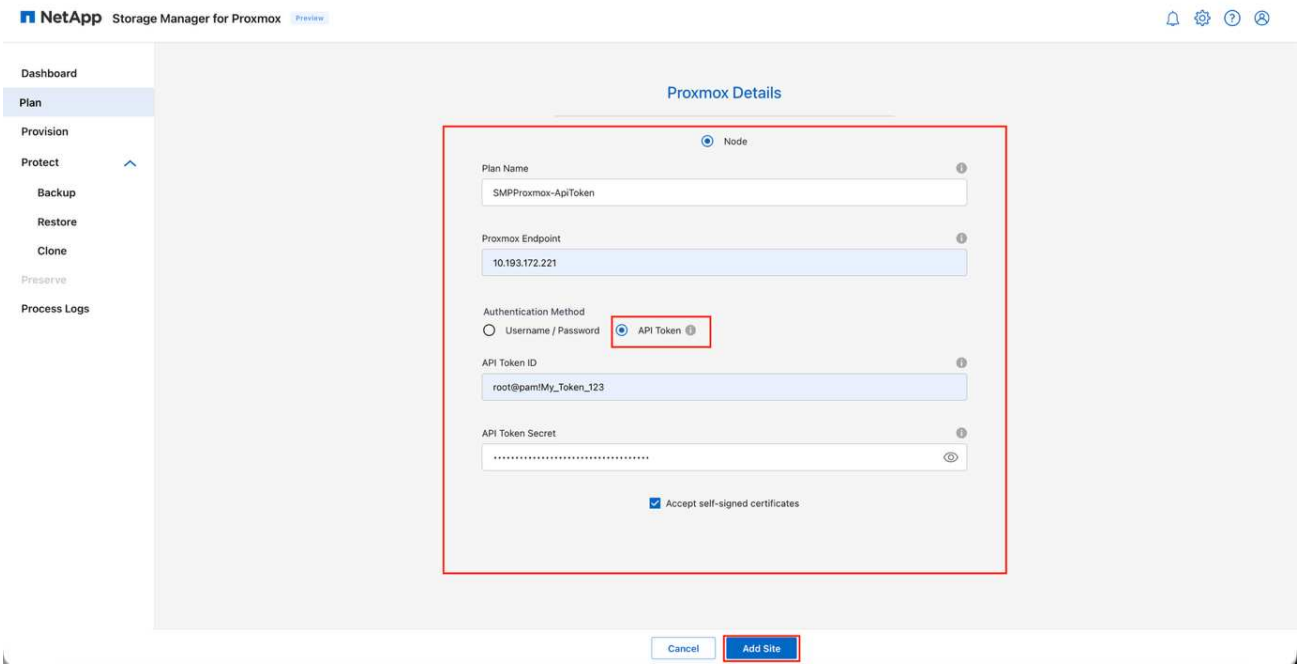


Alternativ können Sie ein API-Token verwenden, um auf die APIs zuzugreifen, indem Sie Folgendes angeben:

- API-Token-ID
- API-Token-Geheimnis

> In dieser Version ist die Verwendung eines API-Tokens nur für NFS-Operationen zulässig.

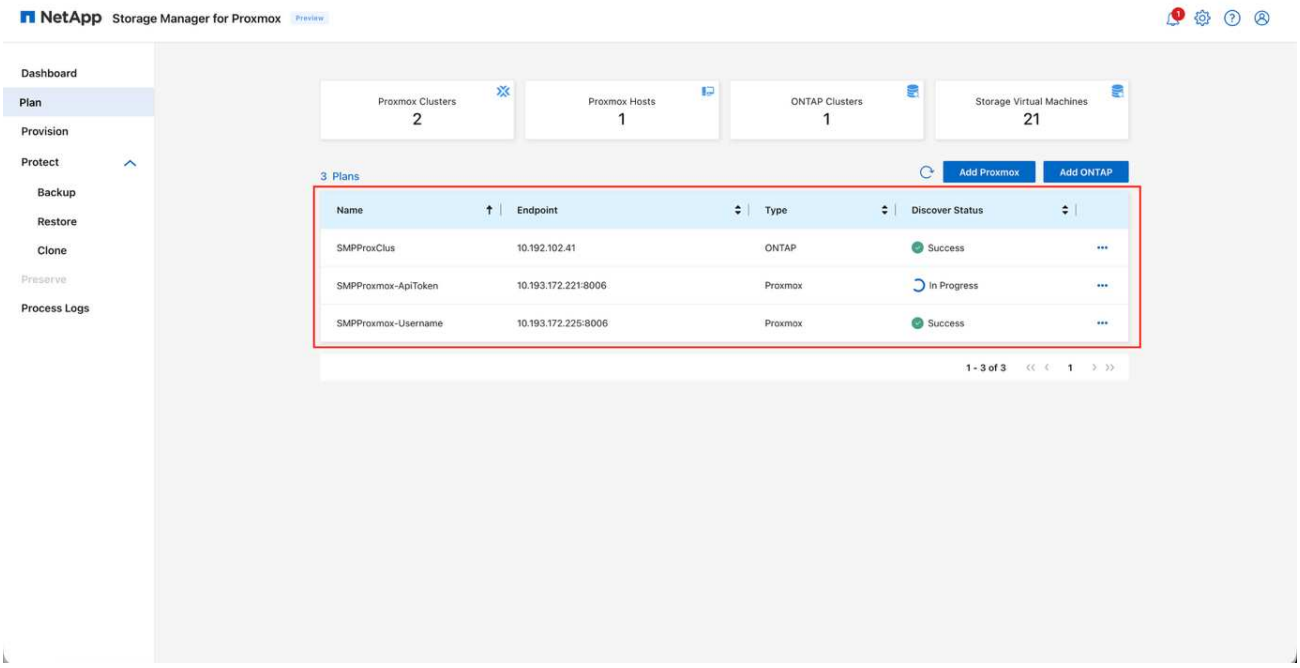
▼ Add Proxmox anzeigen: API-Token



9. Überprüfen Sie, ob die Erkennungsaufträge erfolgreich sind und der Status für jeden Plan als **Success** markiert ist.

   Nach dem Hinzufügen führt SMP automatisch einen Erkennungsscan durch und zeigt die VMs zusammen mit ihren zugehörigen Metadaten an. Vorhandene Speichervolumes oder zugeordnete LUNs werden ebenfalls erkannt.

   ▼ Ergebnisse der Planfindung anzeigen



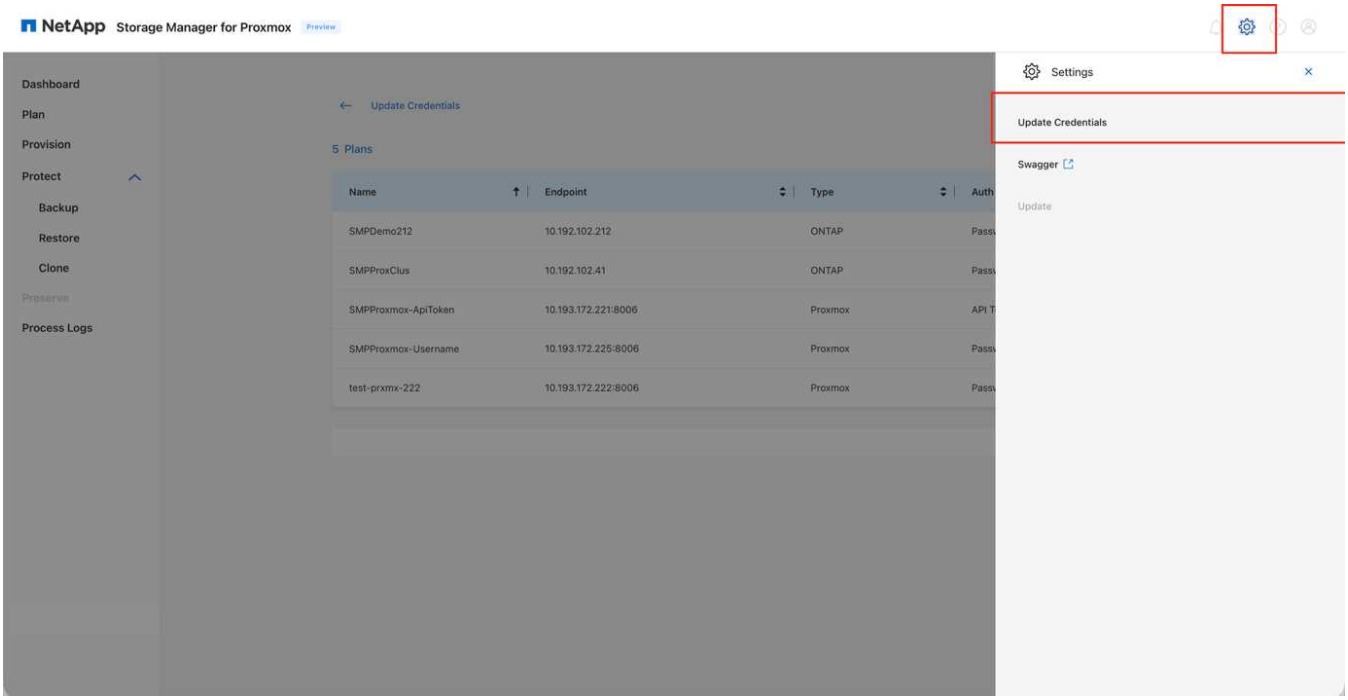
Nachdem Sie fertig sind

- Wenn Änderungen an den Proxmox-Knoten oder dem Speicher vorgenommen werden, führen Sie die Erkennung durch, um die neuesten Informationen abzurufen. Klicken Sie auf die drei Punkte neben dem Plannamen und klicken Sie auf **Discover**.
- Stellen Sie sicher, dass das ONTAP-Speichersystem zuerst hinzugefügt wird, damit der Erkennungsauftrag

die vorhandenen Ressourcen entsprechend zuordnen kann. Wenn Proxmox zuerst hinzugefügt wird, führen Sie einen Erkennungsauftrag für ONTAP aus.

- Falls die Anmeldeinformationen oder das API-Token später aktualisiert werden müssen, navigieren Sie zu **Einstellungen** und wählen Sie die Option **Anmeldeinformationen aktualisieren**.

▼ Anmeldeinformationen anzeigen/aktualisieren



Storage bereitstellen

Durch die Bereitstellung eines Volumes als Speicherpool, üblicherweise als Datenspeicher bezeichnet, wird ein logischer Container für virtuelle Maschinen und deren virtuelle Festplatten (QCOW2 oder RAW) erstellt. SMP ermöglicht die Bereitstellung eines Datenspeichers und dessen anschließende Anbindung entweder an einen einzelnen Host oder an alle Hosts innerhalb eines Clusters.

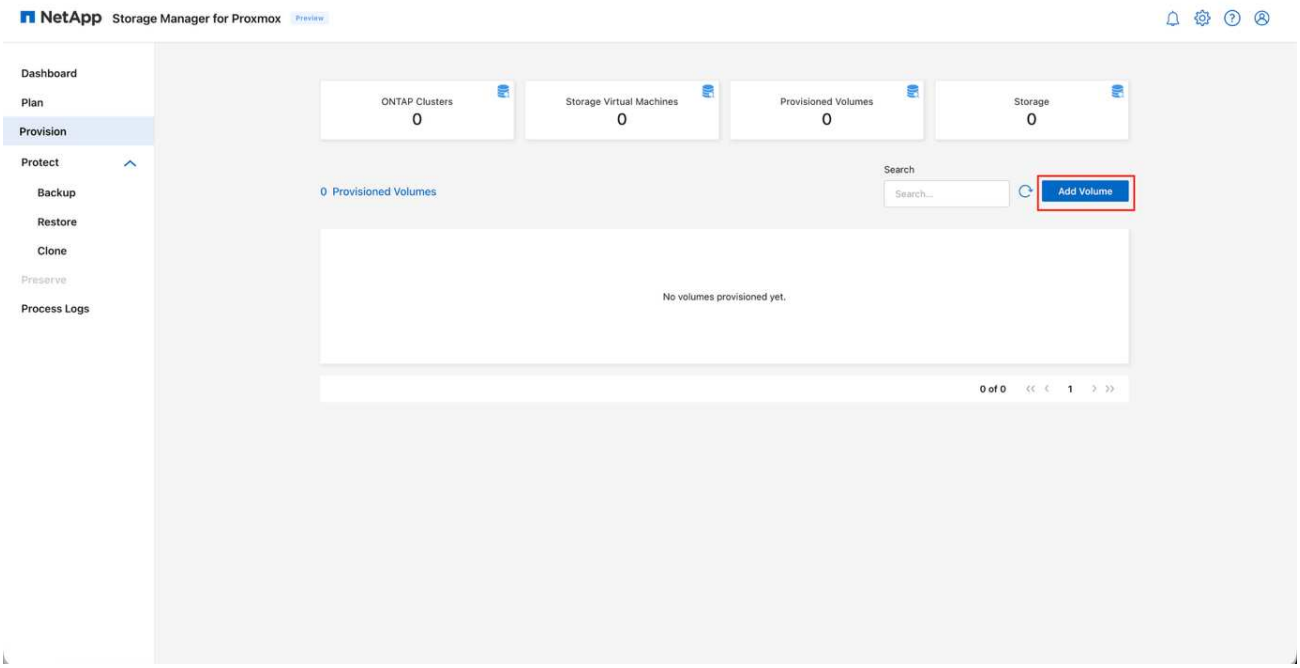
NFS-Speicher bereitstellen

Verwenden Sie SMP, um ein ONTAP Volume als NFS-Datenspeicher bereitzustellen und einzubinden.

Schritte

1. Wechseln Sie in der SMP-Benutzeroberfläche zur Registerkarte **Provision**.
2. Navigieren Sie zu **Add Volume**.

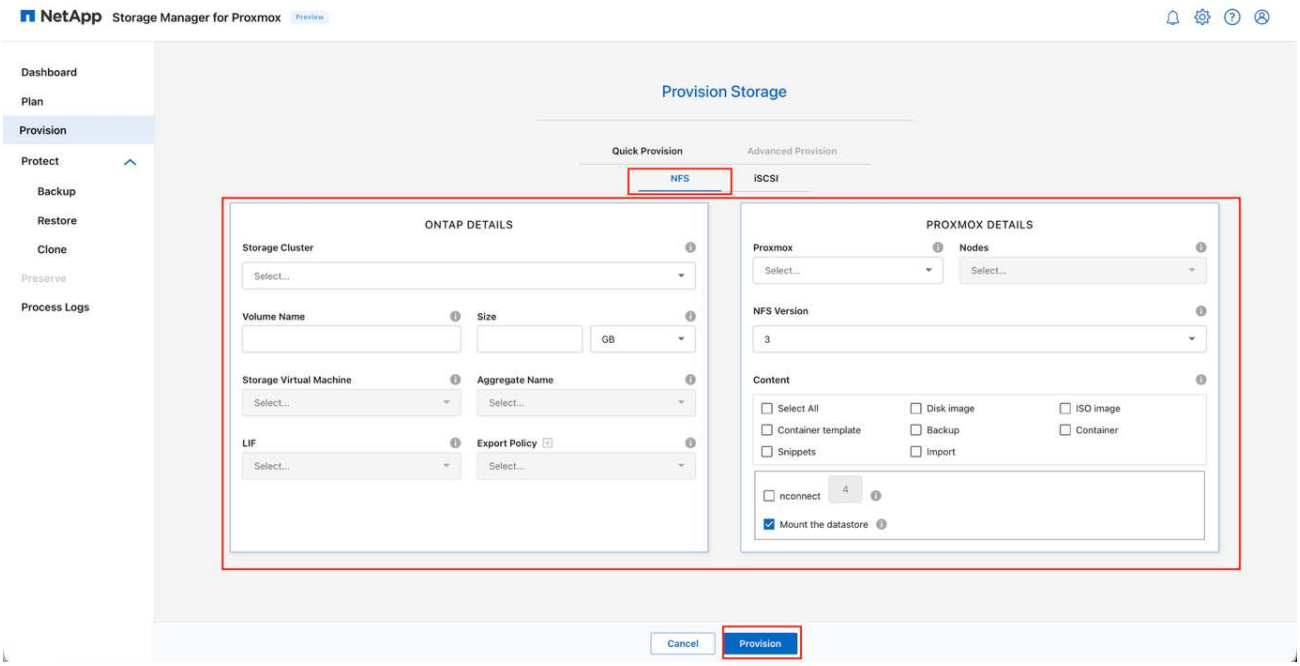
▼ Registerkarte „Bereitstellung anzeigen“: Volume hinzufügen



3. Im Assistenten für neue Volumes wählen Sie im Schritt „Schnellbereitstellung“ **NFS** aus.

> NFS ist standardmäßig ausgewählt. Die Schnellbereitstellung ermöglicht eine schnellere Einrichtung mit Standardeinstellungen für Standardbereitstellungen. Die erweiterte Bereitstellung bietet erweiterte Optionen für HA- und BCDR-Funktionen, die in zukünftigen Versionen eingeführt werden.

▼ Assistent für neues Volume anzeigen: NFS



4. Geben Sie im Abschnitt **ONTAP-Details** folgende Informationen an:
   a. Wählen Sie den ONTAP-Cluster oder die entsprechende Storage Virtual Machine (SVM) aus dem Dropdown-Menü **Speichercluster** aus
   b. Geben Sie im Feld **Volume Name** einen eindeutigen Wert an

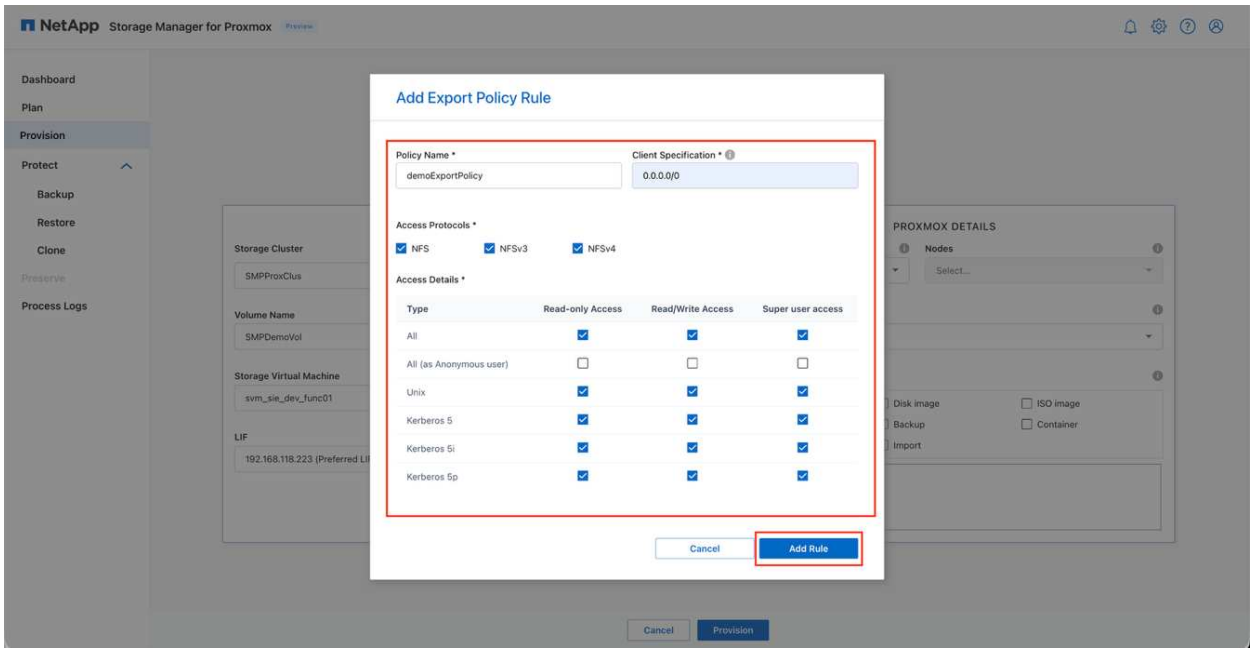
c. Geben Sie im Feld **Größe** die erforderliche Kapazität für das Datenspeichervolume ein

d. Wählen Sie ONTAP-Speicherressourcen aus, indem Sie die entsprechenden Optionen für Folgendes auswählen:

   - Aggregatname
   - Storage Virtual Machine (SVM)
   - Bevorzugte LIF für den Datenspeicherzugriff

e. Wählen Sie eine vorhandene **Exportrichtlinie** aus oder erstellen Sie eine benutzerdefinierte Richtlinie, indem Sie bei Bedarf auf das (+) klicken

▼ ONTAP Details anzeigen: NFS



5. Geben Sie im Abschnitt **Proxmox-Details** die folgenden Informationen an:

   a. Wählen Sie im Feld **Proxmox** den Zielcluster aus und anschließend alle Knoten, die Zugriff auf den Datenspeicher benötigen

   b. Wählen Sie im Feld **NFS Version** das bevorzugte NFS-Protokoll (NFS v3 oder NFS v4.1)

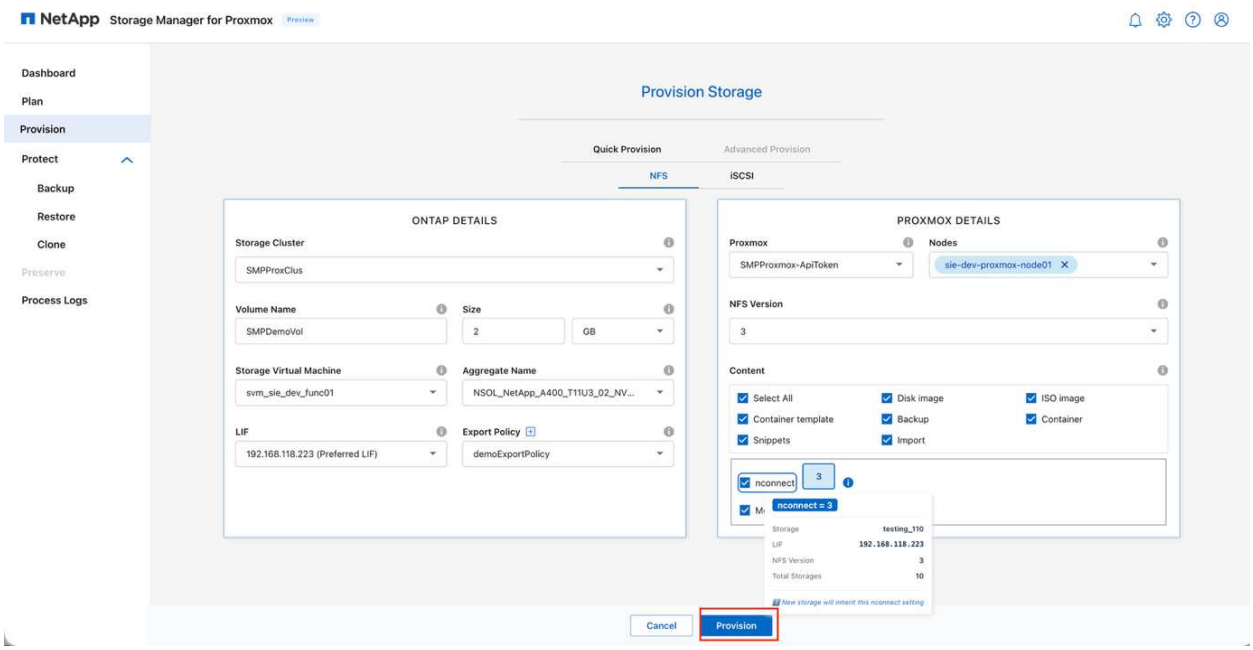
   c. Wählen Sie im Abschnitt **Inhalt** die Inhaltstypen aus, die für diesen Datenspeicher aktiviert werden sollen:

      - Datenträgerabbild
      - ISO-Bild
      - Containervorlage
      - Backup
      - Ausschnitte
      - Importieren
      - Oder wählen Sie **Alle** Inhaltstypen

   d. (Optional) Aktivieren Sie die Option **nconnect**, wenn mehrere TCP-Verbindungen gewünscht sind.

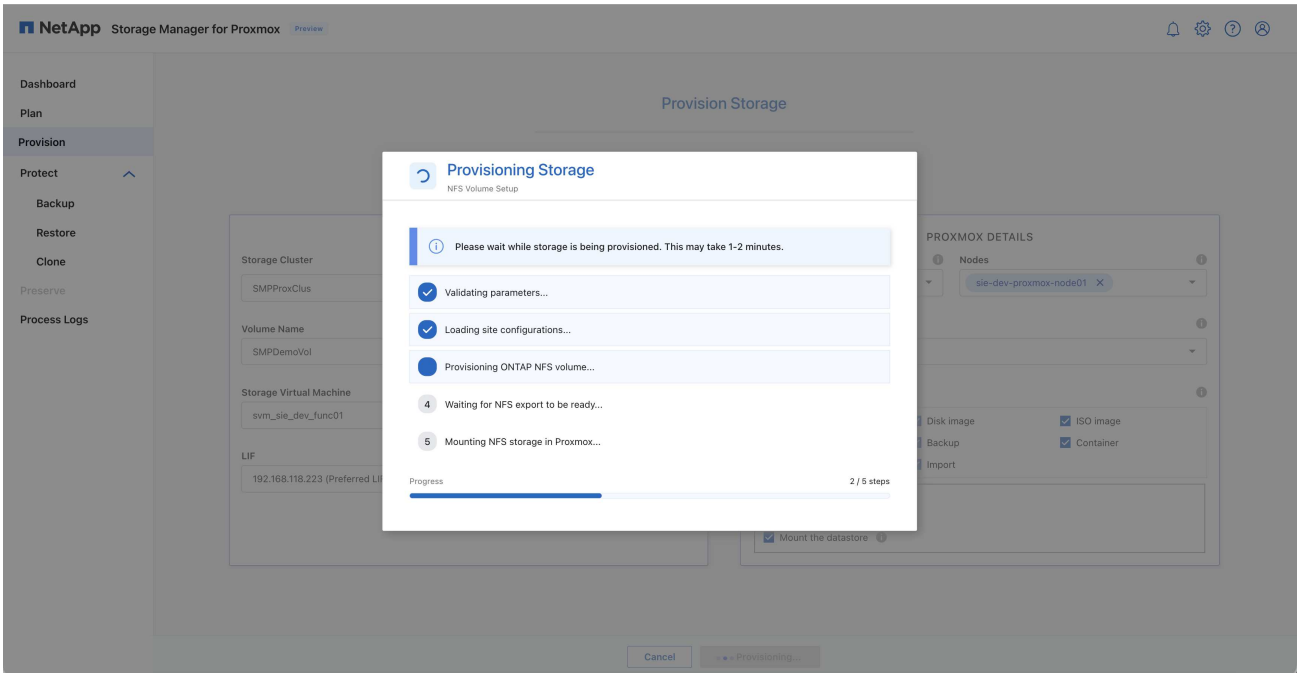
   e. Stellen Sie sicher, dass **Datenspeicher einbinden** aktiviert ist, damit der Datenspeicher auf den ausgewählten Proxmox-Knoten eingebunden wird.

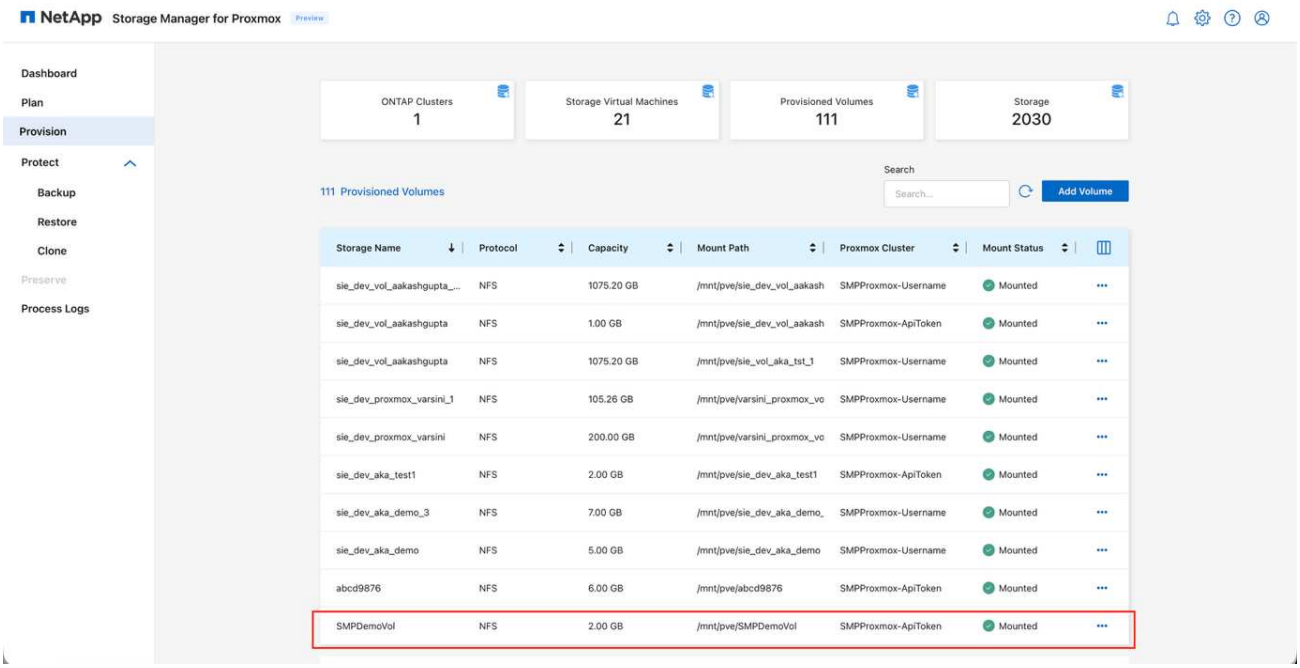
▼ **Proxmox-Details anzeigen: NFS**



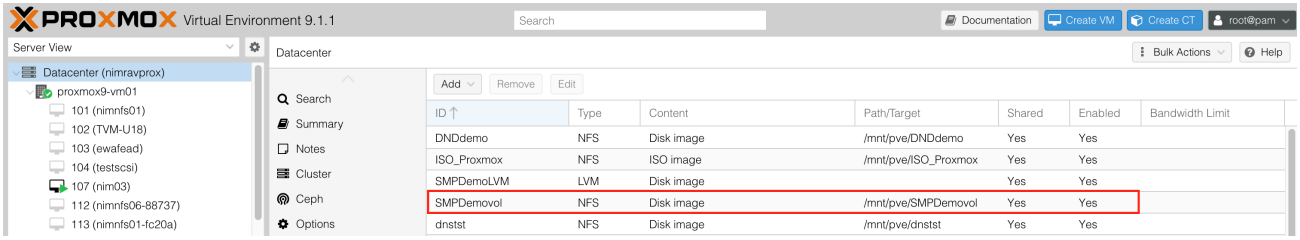
6. Klicken Sie auf **Provision**, um das ONTAP-Volume zu erstellen und den Datenspeicher (Speicherpool) innerhalb des ausgewählten Proxmox-Clusters zu registrieren.

▼ **NFS-Bereitstellungsergebnis anzeigen**





▼ **NFS-Datenspeicher in Proxmox anzeigen**



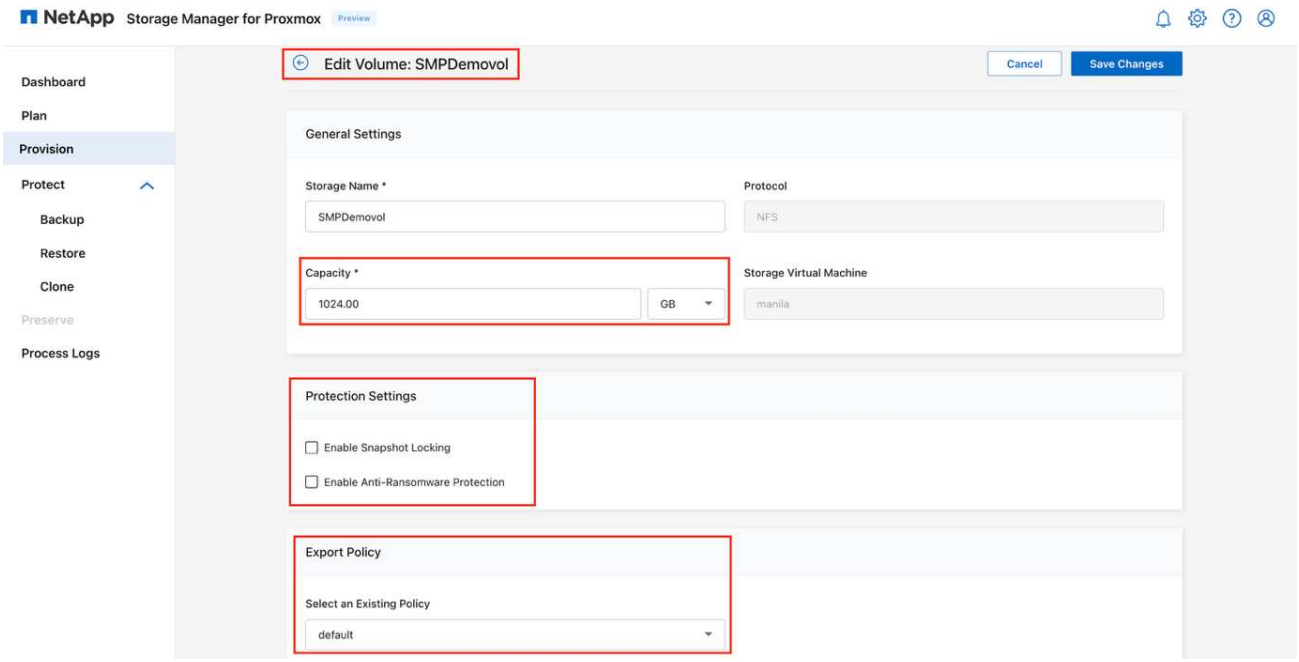
Bearbeiten eines bereitgestellten Volumes

Verwenden Sie SMP, um die Volume-Einstellungen nach der Bereitstellung zu ändern.

Schritte

1. Suchen Sie in der SMP-Benutzeroberfläche das Volume auf der Registerkarte **Provision**.
2. Klicken Sie auf die drei vertikalen Punkte (⋮) neben dem Volume.
3. Wählen Sie im Kontextmenü **Bearbeiten**, um die Lautstärkeeinstellungen zu öffnen.

▼ **Dialogfeld „Volume bearbeiten“ anzeigen**



4. Passen Sie die Volume-Einstellungen nach Bedarf an:
   - **Volume anpassen**: Passen Sie die Speicherkapazität des Volumes an

     Die Größenänderung ist nur für NFS-Volumes anwendbar.

   - **Snapshot Locking**: Aktivieren Sie diese Option, um zu verhindern, dass Snapshots gelöscht oder verändert werden.

     Hierfür muss die SnapLock-Lizenz auf dem Cluster installiert und die Compliance-Uhr des Clusters initialisiert werden.

   - **Schutz vor Ransomware**: Aktivieren Sie diese Funktion, um ungewöhnliche Aktivitäten, die auf einen Ransomware-Angriff hindeuten könnten, proaktiv zu erkennen und Warnungen auszugeben.
   - **Exportrichtlinie**: Aktualisieren oder ändern Sie die Exportrichtlinie
5. Klicken Sie auf **Speichern**, um die Änderungen zu übernehmen.

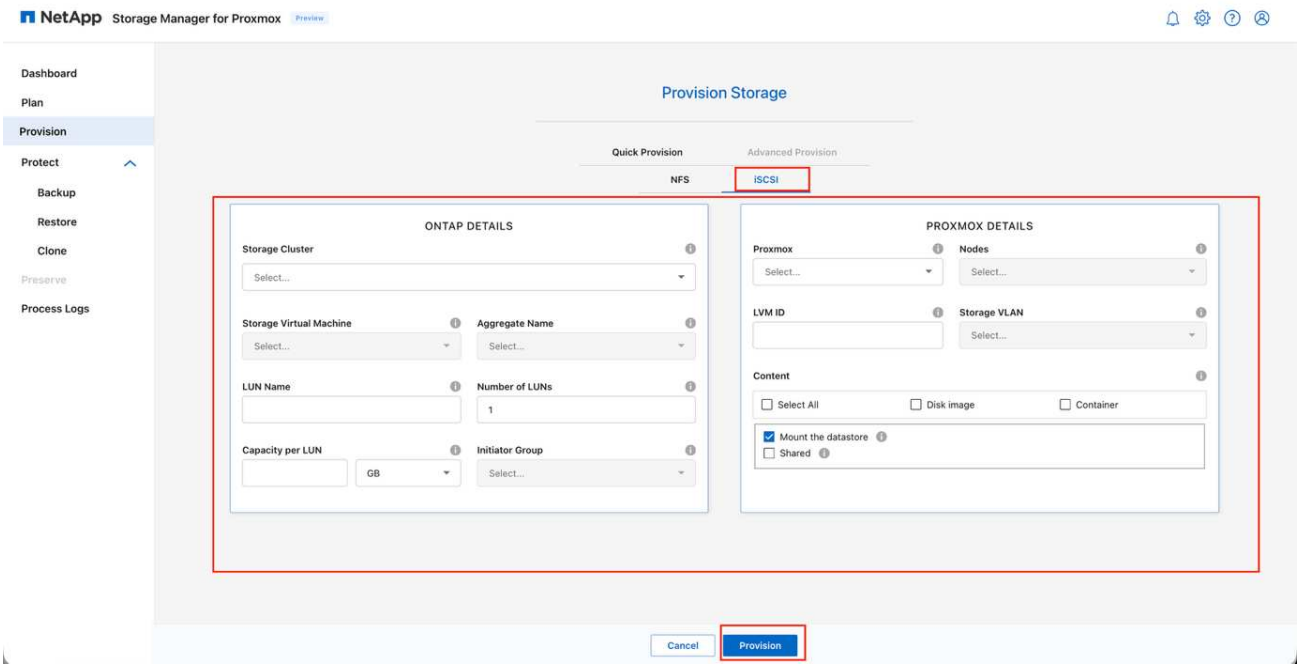
iSCSI-Speicher bereitstellen

Verwenden Sie SMP, um ein iSCSI-Backend für virtuelle Maschinen einzurichten.

Schritte

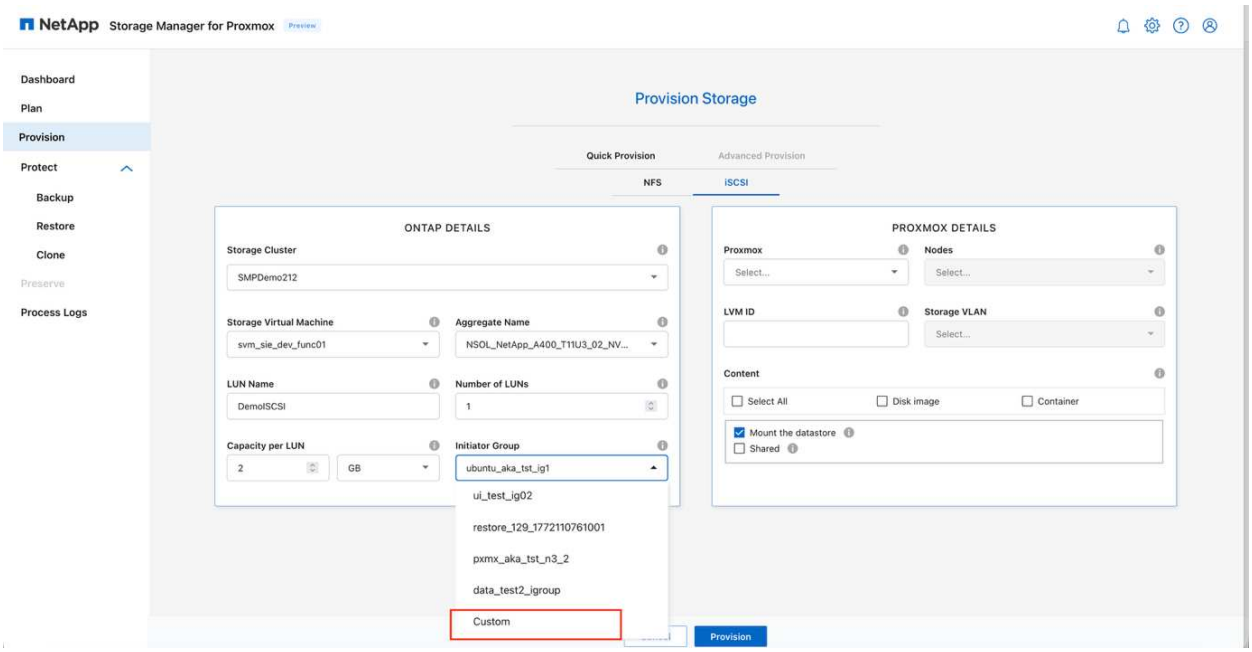
1. Wechseln Sie in der SMP-Benutzeroberfläche zur Registerkarte **Provision**.
2. Navigieren Sie zu **Add Volume**.
3. Im Assistenten für neue Volumes wählen Sie im Schritt „Schnellbereitstellung“ **iSCSI** aus.

▼ Assistent für neues Volume anzeigen: iSCSI

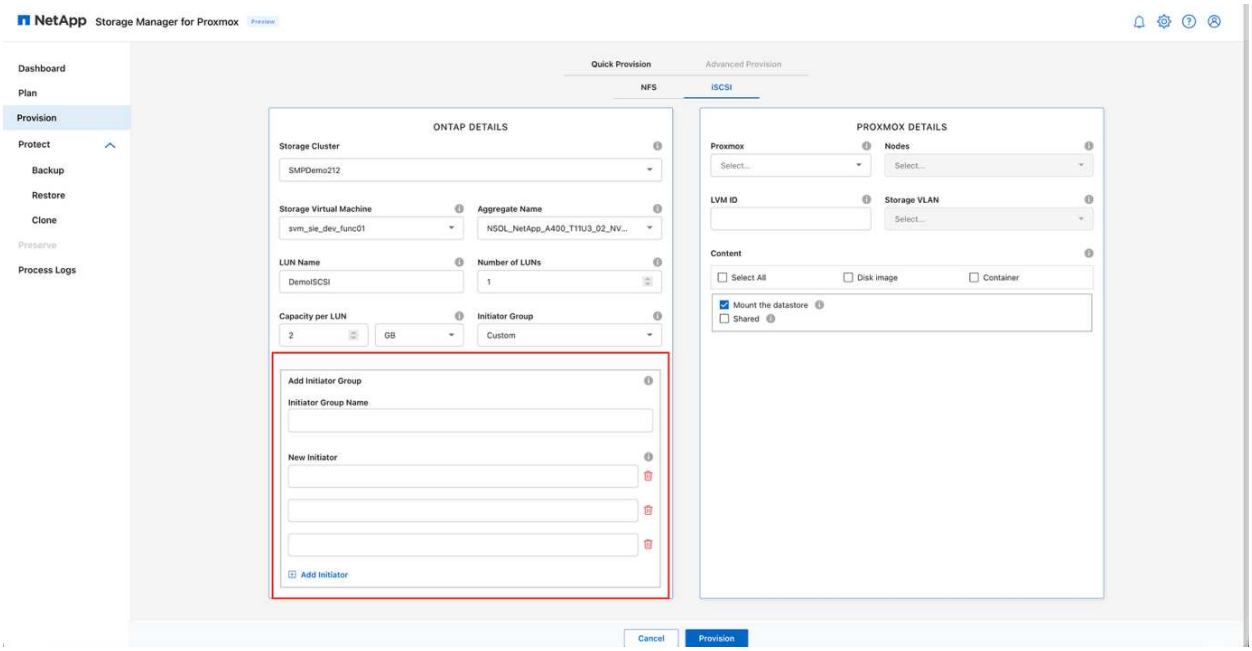


4. Geben Sie unter dem iSCSI-Protokoll im Abschnitt **ONTAP-Details** die folgenden Informationen an:
   a. Wählen Sie den entsprechenden ONTAP-Cluster oder die angegebene Storage Virtual Machine (SVM) aus dem Dropdown-Menü **Speichercluster** aus
   b. Wählen Sie die Optionen für:
      - Aggregatname
      - Storage Virtual Machine (SVM)
   c. Geben Sie im Feld **LUN Name** einen eindeutigen Wert ein
   d. Geben Sie die benötigte Anzahl an LUNs im Feld **Anzahl der LUNs** an (Standardwert ist 1; zusätzliche LUNs gleicher Größe können parallel erstellt werden)
   e. Geben Sie die gewünschte Größe für jede LUN im Feld **Kapazität pro LUN** ein
   f. Wählen Sie eine **Initiatorgruppe** (Initiatorgruppe) für die iSCSI-Zugriffskontrolle. Sie können eine vorhandene Initiatorgruppe auswählen oder eine neue Initiatorgruppe erstellen.

▼ ONTAP Details anzeigen: iSCSI-LUN-Konfiguration



▼ **iSCSI-Initiatorgruppe Auswahl anzeigen**



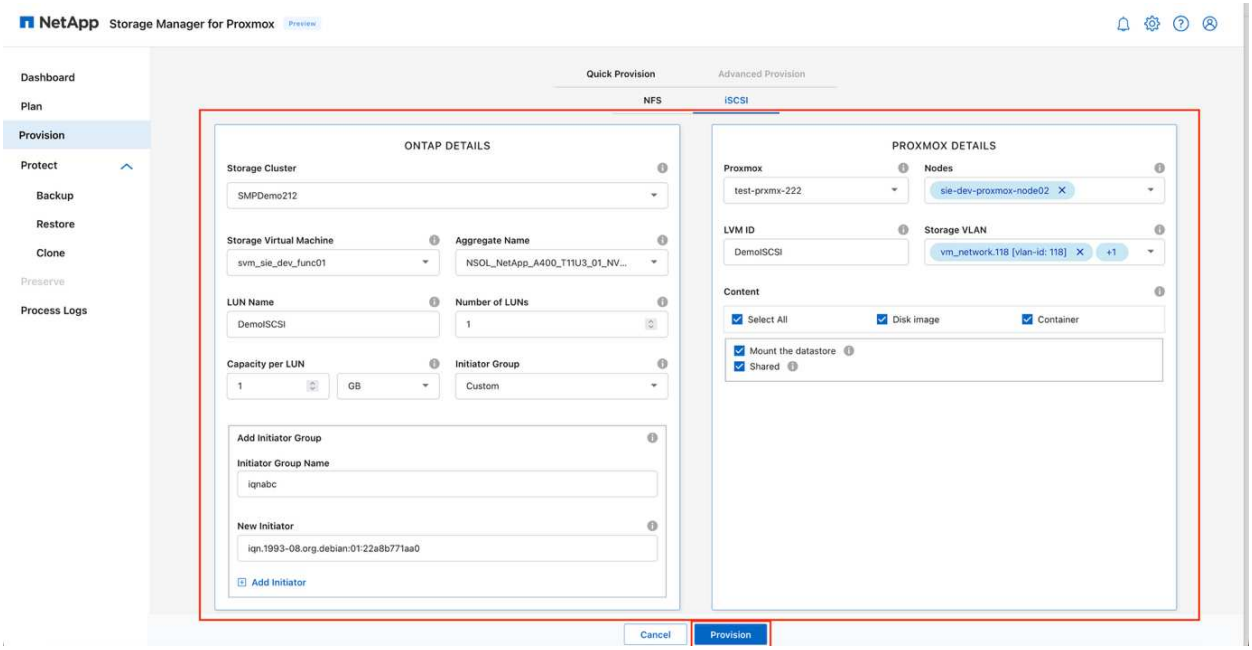
5. Geben Sie im Abschnitt **Proxmox-Details** die folgenden Informationen an:
   a. Wählen Sie im Dropdown-Menü **Proxmox** den Zielcluster und anschließend alle Knoten aus, die Zugriff auf den Speicher benötigen
   b. Wählen Sie die entsprechende **LVM ID** aus, die den iSCSI-basierten Speicherpool innerhalb von Proxmox repräsentiert.
   c. Wählen Sie im Feld **Knoten** alle Knoten aus, die Zugriff auf die präsentierten iSCSI-Ziele benötigen.
   d. (Optional) Falls eine VLAN-Segmentierung erforderlich ist, wählen Sie das gewünschte **Storage VLAN** aus.
   e. Wählen Sie im Abschnitt **Inhalt** die von diesem Datenspeicher unterstützten Inhaltstypen aus:
      - Datenträgerabbild

- Container
- Oder wählen Sie **Alle** Inhaltstypen

f. Stellen Sie sicher, dass **Datenspeicher einbinden** ausgewählt ist, damit der Speicher auf den ausgewählten Proxmox-Knoten verfügbar ist

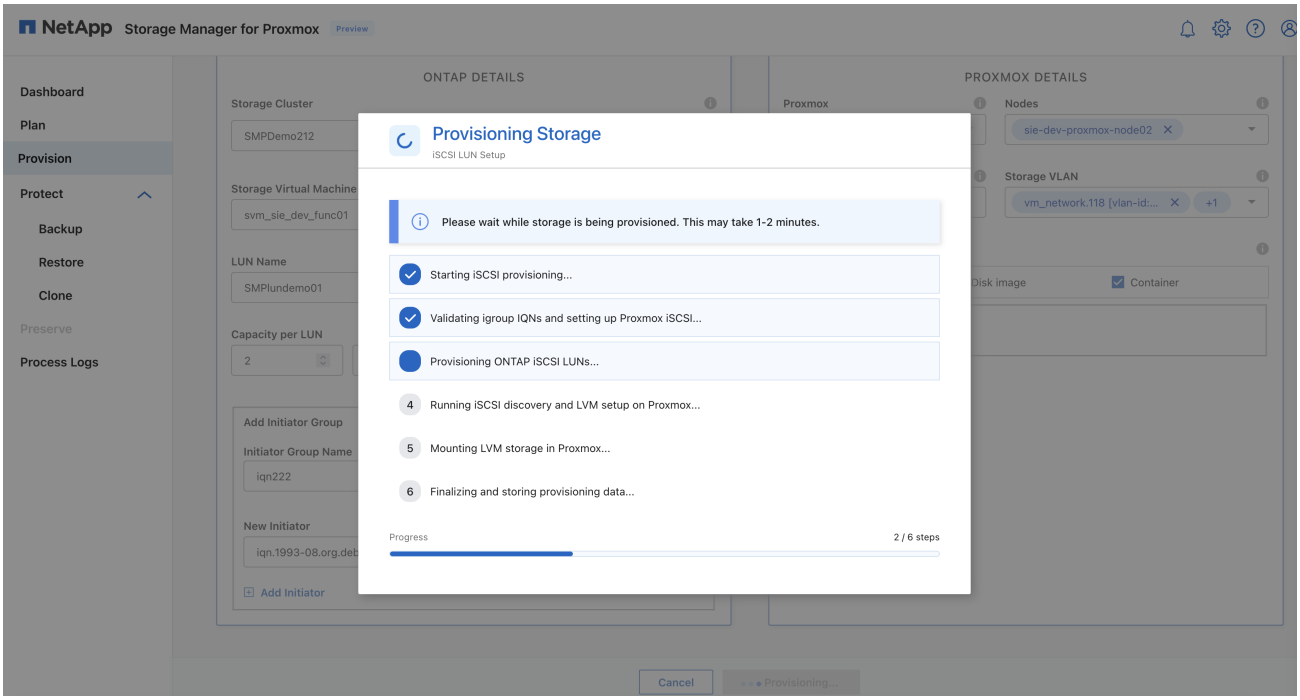
g. (Optional) Aktivieren Sie **Shared**, wenn der Speicherpool gleichzeitig von mehreren Knoten genutzt wird.

▼ **Proxmox-Details anzeigen: iSCSI**

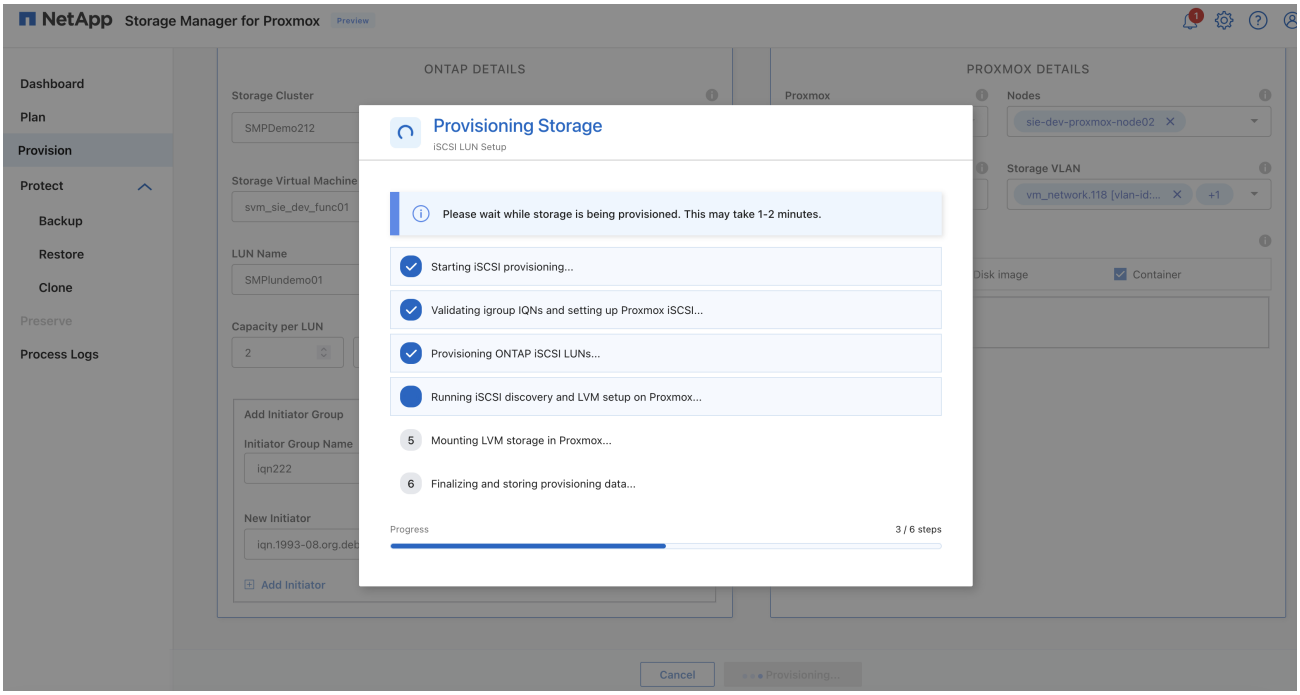


6. Klicken Sie auf **Provision**, um die ONTAP LUN zu erstellen und den Datenspeicher (Speicherpool) innerhalb des ausgewählten Proxmox-Clusters zu registrieren.

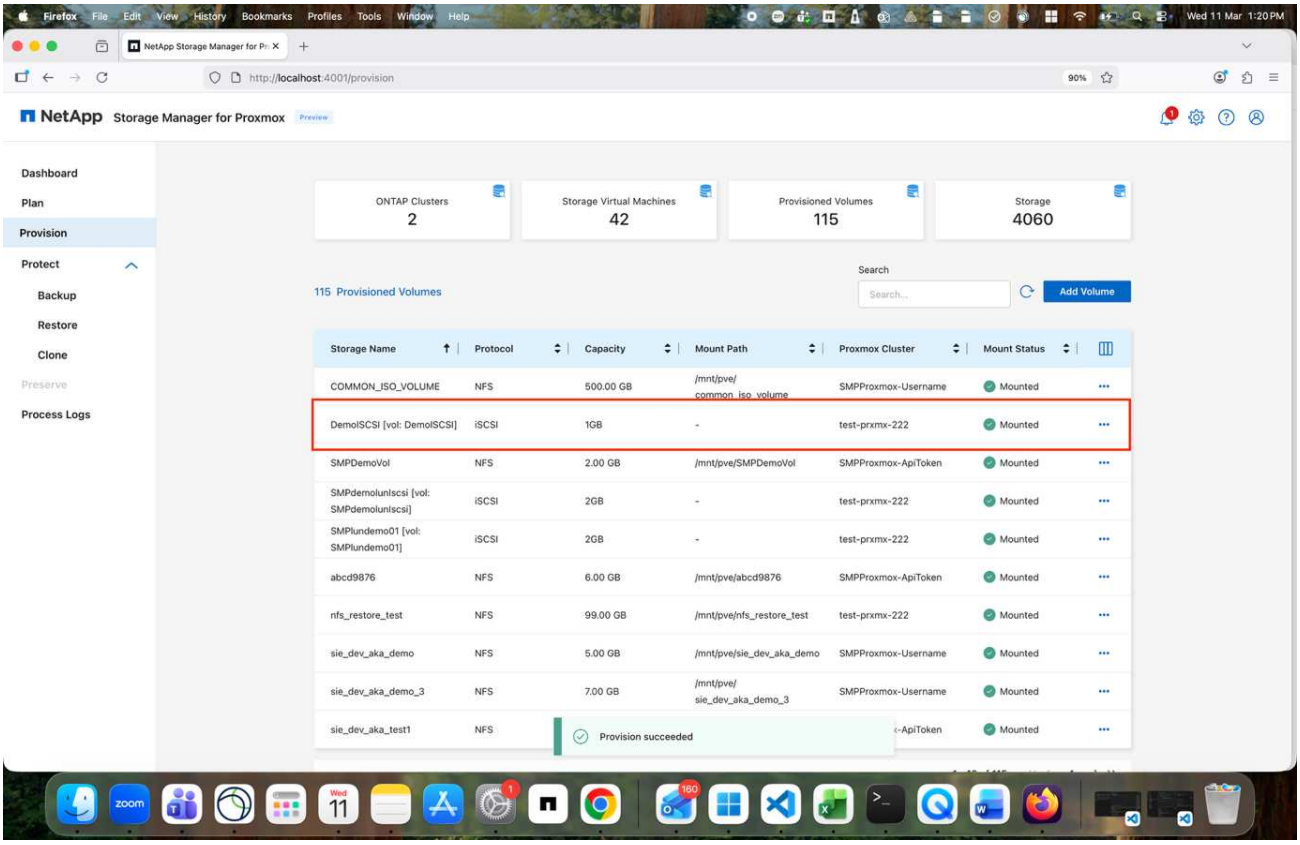
▼ **iSCSI-LUN-Bereitstellung anzeigen**



▼ iSCSI-Bereitstellung abgeschlossen



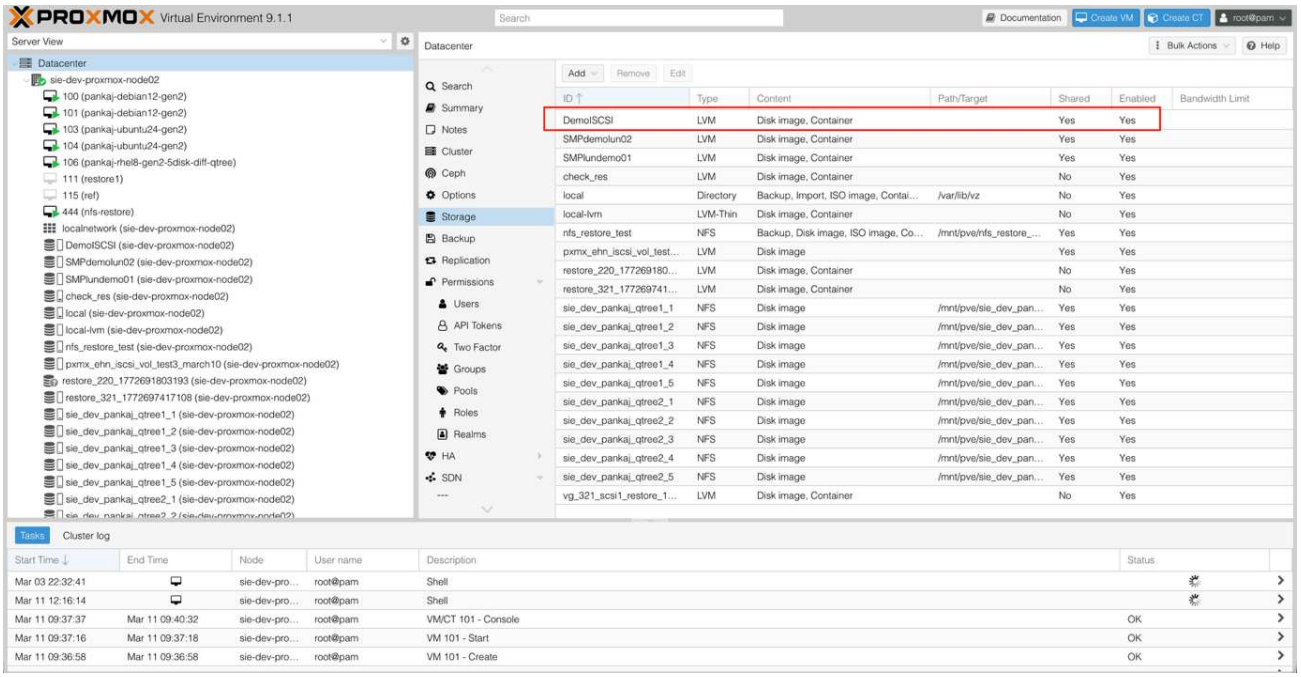
▼ iSCSI-Datenspeicher in Proxmox anzeigen



7. Überprüfen Sie, ob die NFS- und iSCSI-LUNs durch Zugriff auf den Proxmox-Endpunkt verbunden wurden.

   Der angeschlossene Speicher steht nun für die Bereitstellung virtueller Maschinen zur Verfügung.

▼ Proxmox-Speicheransicht anzeigen



Optionen zur Volumenkonfiguration

Wenn SMP neue ONTAP FlexVol Volumes und LUNs bereitstellt, werden automatisch mehrere Standardkonfigurationswerte angewendet:

ONTAP-Einstellung	Standardwert
Snapshot-Reserve (-percent-snapshot-space)	0%
Teilreserve (-fractional-reserve)	0%
Zugriffszeitaktualisierung (-atime-update)	Deaktiviert
Minimale Vorauslese (-min-readahead)	Deaktiviert
Geplante Snapshots	Keine
Speichereffizienz	Aktiviert
Volumengarantie	Keine (thin provisioned)
automatische Größenanpassung	wachsen_schrumpfen
LUN Speicherplatzreservierung	Deaktiviert
LUN-Speicherplatzzuweisung	Aktiviert

NConnect-Verhalten

Bei der Verwendung von NFS-Speicher mit Proxmox VE ist das spezifische Verhalten des Linux-NFS-Client (wie er von Debian, dem Basisbetriebssystem von Proxmox VE, verwendet wird) zu beachten. Der Linux-Kernel kann die Mount-Parameter wiederverwenden, die beim ersten Mounten eines NFS-Exports auf einem Knoten festgelegt wurden. Wird derselbe Export erneut mit anderen Mount-Optionen gemountet, werden diese neuen Optionen möglicherweise nicht angewendet.

Es empfiehlt sich, separate Exporte zu erstellen und einzubinden sowie unterschiedliche NFS-Server-IP-Adressen zu verwenden, beispielsweise für verschiedene Daten-LIFs. SMP erkennt automatisch bestehende Verbindungen und deren zugehörige nconnect-Werte und wendet den entsprechenden nconnect-Wert auf

neue Verbindungen an.

Virtuelle Maschinen schützen

Wenn virtuelle Maschinen auf ONTAP-gestützten NFS-Datenspeichern laufen, ist der effizienteste Schutzansatz, Proxmox die Dateisystemkonsistenz herstellen zu lassen, während ONTAP den tatsächlichen Sicherungspunkt auf der Speicherebene erfasst. ONTAP Snapshots liefern schnelle, platzsparende, zeitpunktgenaue Kopien des Datenspeicher-Volumes und können später zur Wiederherstellung ganzer Datenspeicher, einzelner Dateien oder VM-Inhalte verwendet werden.

SMP bietet einen einfachen Orchestrator für absturzkonsistenten und VM-konsistenten Datenschutz sowie Klonmanagement. Diese Software vereinfacht Backup-, Restore- und Klon-Lebenszyklen durch die Erstellung von Backup-Richtlinien, die auf mehrere Jobs angewendet werden können. Diese Richtlinien können Zeitplan, Aufbewahrungsrichtlinie, Replikation und weitere Funktionen definieren. Optional kann die Auswahl dateikonsistenter Snapshots erfolgen; dieser Ansatz nutzt die Fähigkeit von QEMU, E/A-Vorgänge vor der Erstellung eines ONTAP Snapshots anzuhalten.

SMP ermöglicht den Schutz eines gesamten Datenspeichers, wobei ein ONTAP NFS-Volume mehrere VMs, Gruppen von VMs, die sich über mehrere Datenspeicher erstrecken können, oder einzelne VMs enthalten kann.

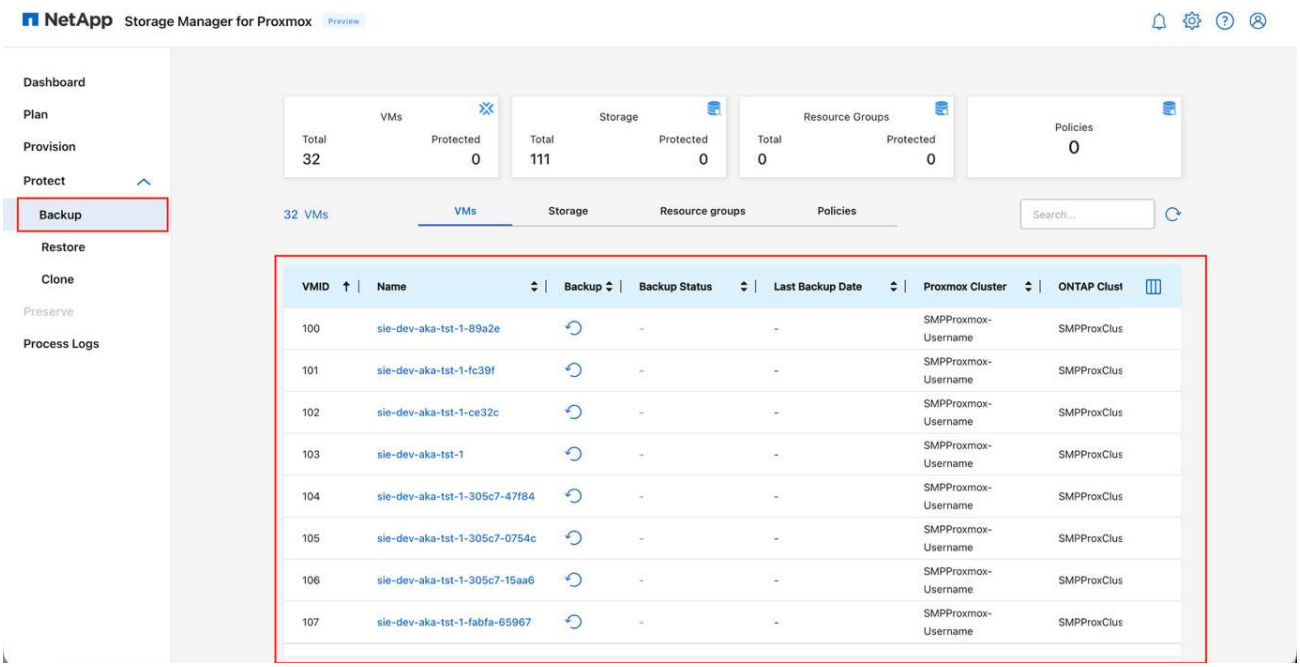
Virtuelle Maschinen sichern

Sobald die ONTAP Volumes bereitgestellt wurden, verwenden Sie die Backup-Option, um alle auf dem Proxmox-Cluster laufenden VMs aufzulisten und eine absturzkonsistente oder dateikonsistente Sicherung der virtuellen Maschinen durchzuführen.

Schritte

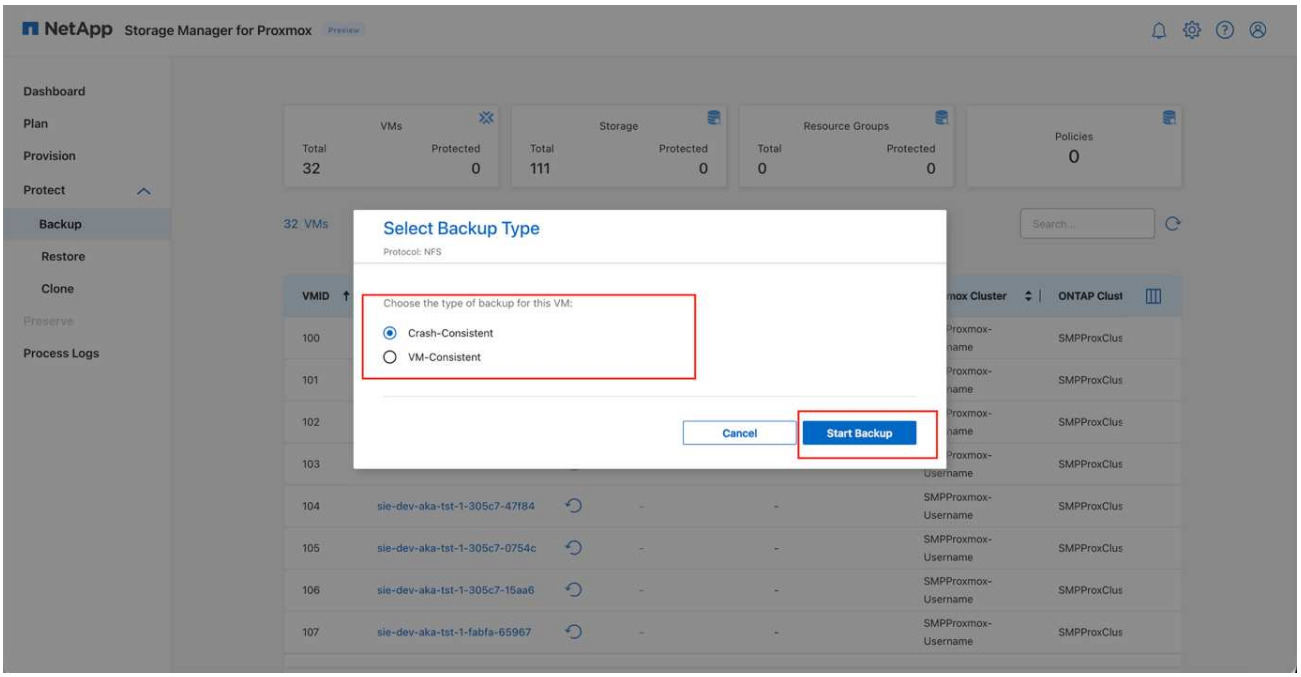
1. Greifen Sie auf **Protect** > **Backup** im linken Navigationsbereich zu.

▼ **Seite „Protect Backup“ anzeigen**



2. Wählen Sie die zu sichernde virtuelle Maschine aus und klicken Sie auf **Sichern**.

▼ **Dialogfeld „Sicherung anzeigen“: VM-Auswahl**

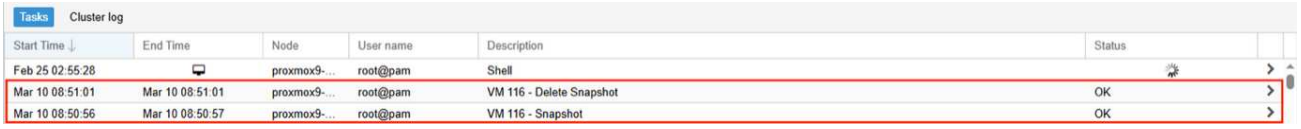


3. Der Backup-Workflow ermöglicht die Auswahl zwischen absturzkonsistentem und dateikonsistentem Schutz.

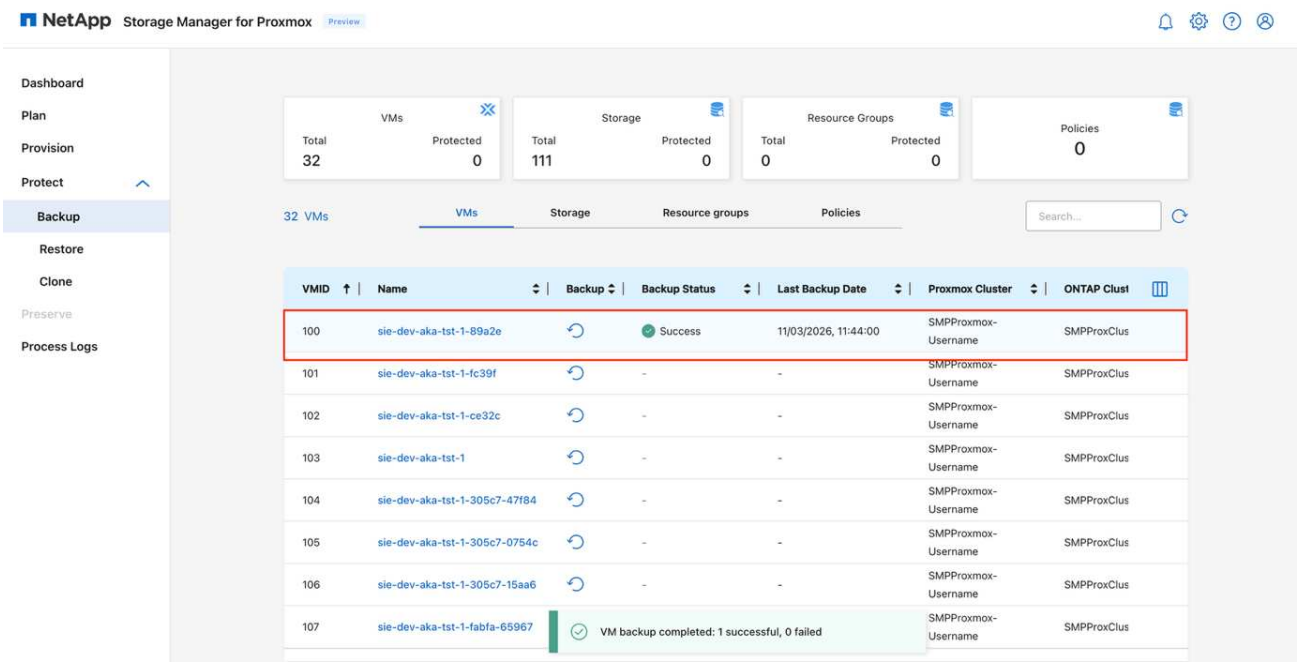
   Der dateikonsistente Modus verwendet optional QEMU fsfreeze, um sicherzustellen, dass das Dateisystem im Gastsystem vor der Erstellung des Snapshots inaktiv ist. Schlägt fsfreeze fehl, greift das System auf einen Proxmox-Snapshot zurück.

   > Dieser Ausweichmechanismus gilt nur für virtuelle Maschinen, die auf NFS-Volumes gespeichert sind.

▼ Dialogfeld „Sicherung anzeigen“: Konsistenzoptionen



▼ Sicherungsfortschritt anzeigen

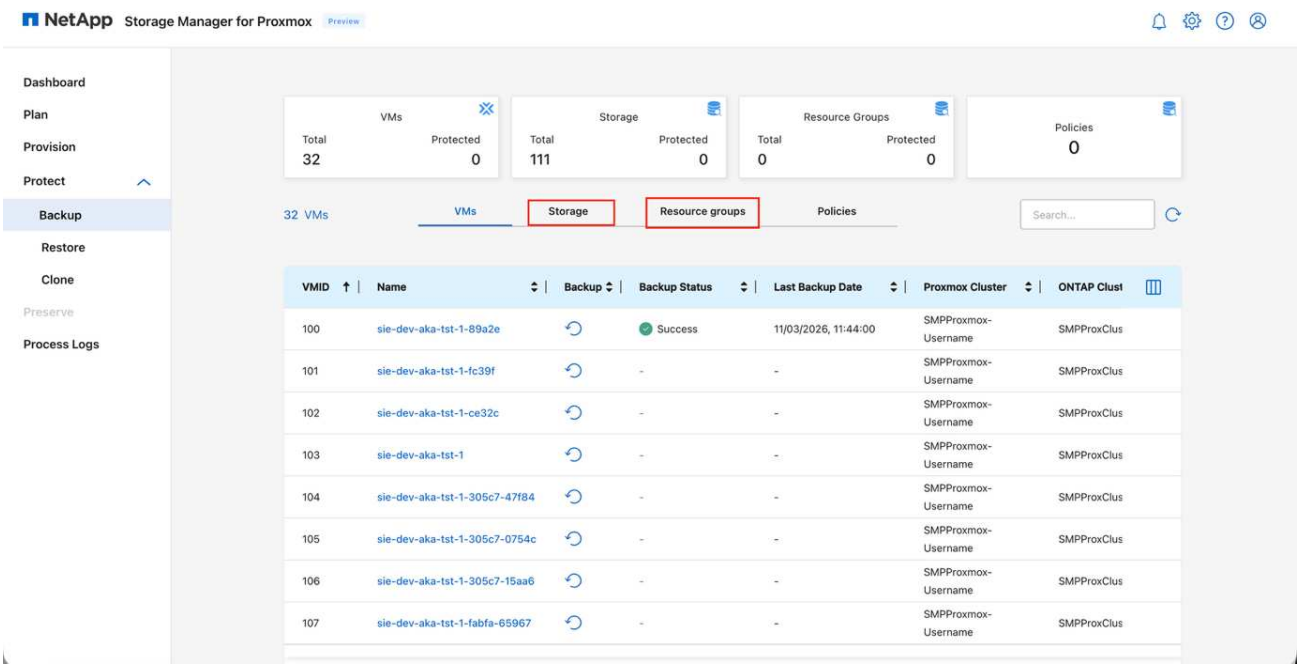


ONTAP-Snapshots werden auf Volume-Ebene erstellt und erfassen alle VM-Festplatten und Konfigurationsdateien im NFS-Datenspeicher in einem einzigen Snapshot. Bei aktiviertem VM-konsistentem Schutz wird fsfreeze nur für die ausgewählten VMs ausgeführt; alle anderen VMs im Volume werden als absturzkonsistent in denselben ONTAP-Snapshot aufgenommen.

Zusätzliche Backup-Optionen

- Um einen einzelnen Datenspeicher zu sichern, wählen Sie die Registerkarte **Storage** und anschließend die Option **Backup**.
- Um mehrere Datenspeicher als eine Einheit zu sichern oder VM-Gruppen zu schützen, die sich über verschiedene Datenspeicher erstrecken, verwenden Sie die Option **Resource Group**. Resource Groups ermöglichen es, Datenspeicher oder VMs in logischen Schutzgruppen zu organisieren.

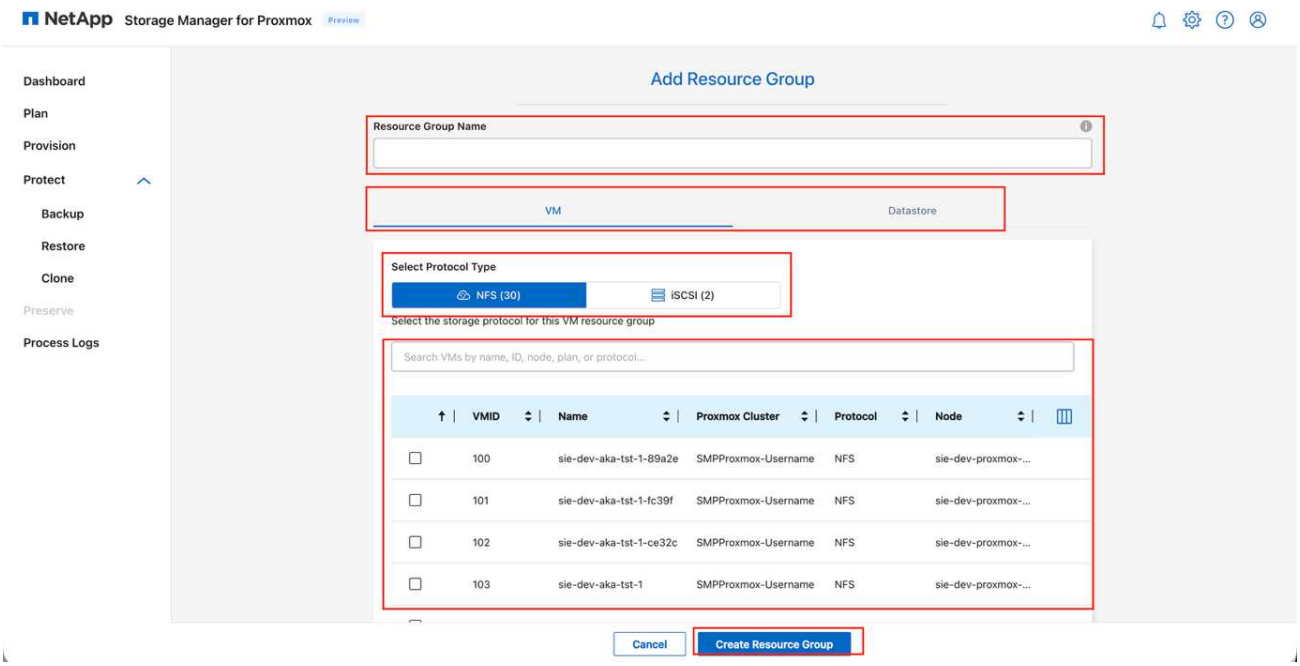
▼ Registerkarte „Ressourcengruppe anzeigen“



Erstellen Sie eine Ressourcengruppe

1. Öffnen Sie die Registerkarte **Ressourcengruppe** und wählen Sie **Hinzufügen**.
2. Geben Sie einen Namen für die neue Ressourcengruppe ein.
3. Wählen Sie den Ressourcentyp: **VM** oder **Datastore**.
4. Wählen Sie das passende **Protokoll** aus.
5. Wählen Sie anhand des ausgewählten Ressourcentyps die spezifischen VMs oder Datenspeicher aus, die einbezogen werden sollen.
6. Klicken Sie auf **Ressourcengruppe erstellen**, um die Einrichtung abzuschließen.

▼ **Dialogfeld „Ressourcengruppe erstellen“ anzeigen**



Backups auf Datenspeicher- (Volume-) Ebene sind immer absturzkonsistent. Eine

> Ressourcengruppe kann nur einen Ressourcentyp enthalten: entweder VMs oder Datenspeicher. Für iSCSI-basierten Speicher sind Backups immer absturzkonsistent.

Details zum Backup-Workflow

Der übergeordnete Backup-Workflow umfasst:

1. **Schutzbereich definieren**: Wählen Sie aus, ob das Schutzziel ein Datenspeicher (ONTAP-Volume), eine Ressourcengruppe (mehrere Volumes oder VMs) oder eine einzelne VM ist.
2. **Bestätigen Sie die Konsistenzmethode**: Wählen Sie aus, wie die Konsistenz vor dem ONTAP Snapshot erstellt wird:
   - QEMU-Gastagenten-Einfrieren/Auftauen für die Quieszierung des Gastdateisystems und die Windows VSS-Integration.
3. **VM-Konfigurationsdateien sichern**.
4. **ONTAP-Snapshot erstellen**: Erfassen Sie einen ONTAP-Snapshot des Datenspeicher-Volumes, während sich die VMs in einem konsistenten Zustand befinden. Dies wird zur aufbewahrten Sicherungskopie.
5. **Temporäre Proxmox-Snapshots entfernen**: Löschen Sie die Proxmox-Snapshots, nachdem der ONTAP-Snapshot abgeschlossen ist, um ein Anwachsen der Delta-Datei zu verhindern.
6. **Aufbewahrungs- und Replikationsrichtlinien anwenden (mithilfe von Richtlinien)**: Wenden Sie die konfigurierte ONTAP Aufbewahrungsrichtlinie an und replizieren Sie den Snapshot-Satz, wenn die Replikation für die Notfallwiederherstellung aktiviert ist.

Dieser Ansatz minimiert Speicherplatz und Netzwerkbandbreite, indem nur geänderte Informationen gespeichert werden. Verwenden Sie Snapshot-Kopien, um schnell Kopien der VM oder des Datenspeichers zu erstellen, ohne die Leistung zu beeinträchtigen, und senden Sie sie dann mithilfe der NetApp SnapMirror-Technologie zur langfristigen, externen Datensicherung an ein Sekundärsystem.

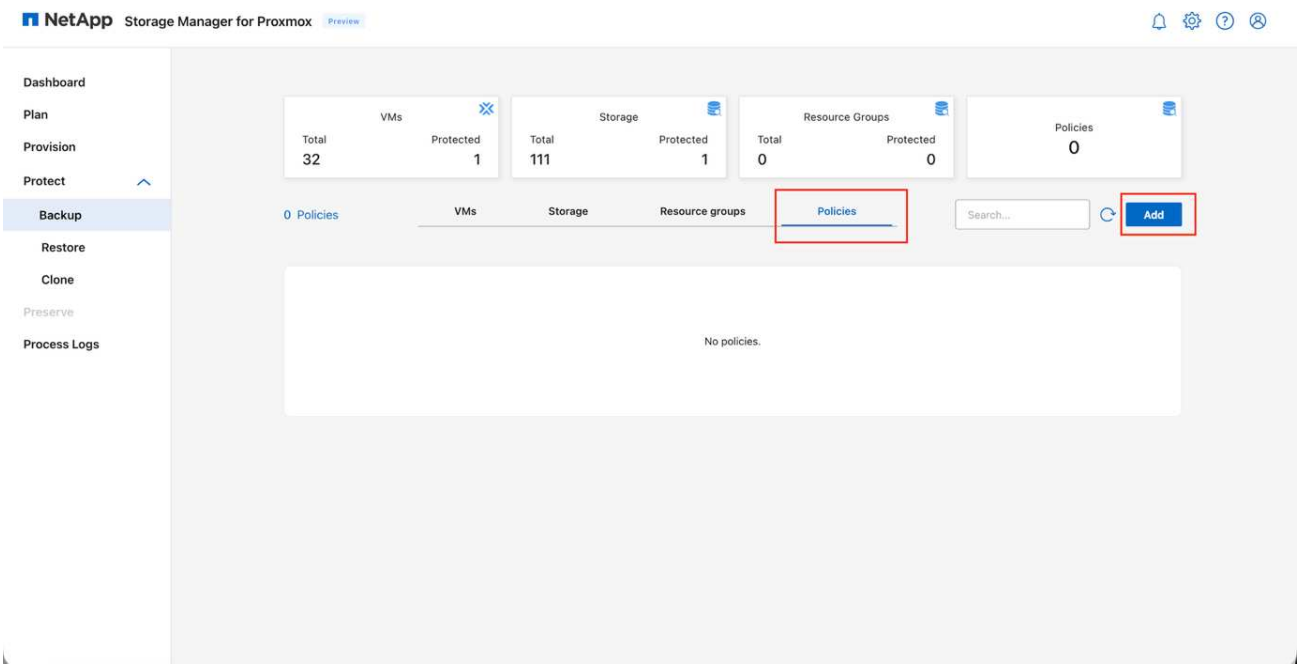
Automatisieren Sie VM-Sicherungsaufgaben

Automatisieren Sie Proxmox-VM-Backups durch die Konfiguration eines Zeitplans. Regelmäßige Backups sind entscheidend für den Datenschutz und die Wiederherstellung nach einem Datenverlust.

Schritte

1. Gehen Sie zu **Schutz** > **Sicherung** > **Richtlinien** und klicken Sie auf **Hinzufügen**, um eine neue Sicherungsrichtlinie und einen Zeitplan hinzuzufügen.

   ▼ Seite „Sicherungsrichtlinien anzeigen“

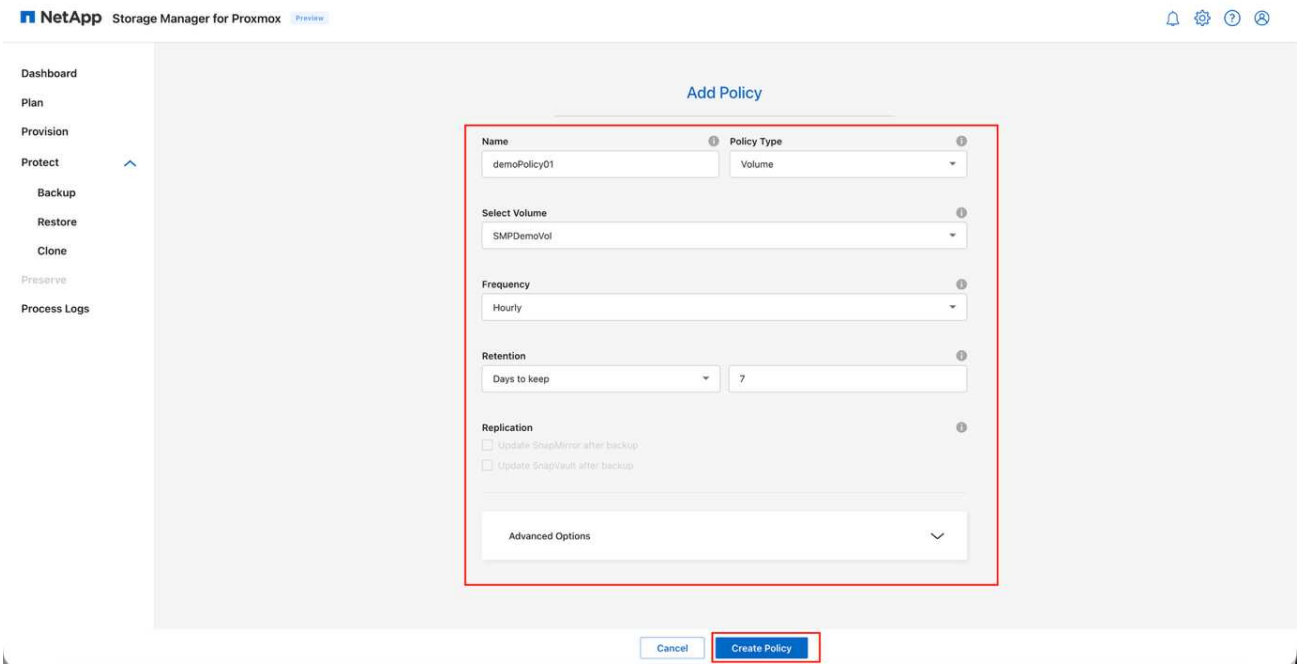


2. Allgemeine Einstellungen konfigurieren:
   a. Geben Sie einen Namen für die Richtlinie ein.
   b. Wählen Sie den **Richtlinientyp** (Volume oder Ressourcengruppe) aus.
   c. Wählen Sie das **Ziel** basierend auf dem ausgewählten Typ aus
   d. Legen Sie die **Sicherungshäufigkeit** fest (stündlich, täglich, wöchentlich oder monatlich)
   e. Konfigurieren Sie **Aufbewahrung**, indem Sie entweder "Tage zum Behalten" oder "Anzahl zum Behalten" angeben (der Standardwert für die Aufbewahrung ist 7)
   f. Wählen Sie den **Replikationsmodus** (in der aktuellen Version deaktiviert):
      - Aktualisieren Sie SnapMirror nach der Datensicherung
      - Aktualisiere SnapVault nach Datensicherung

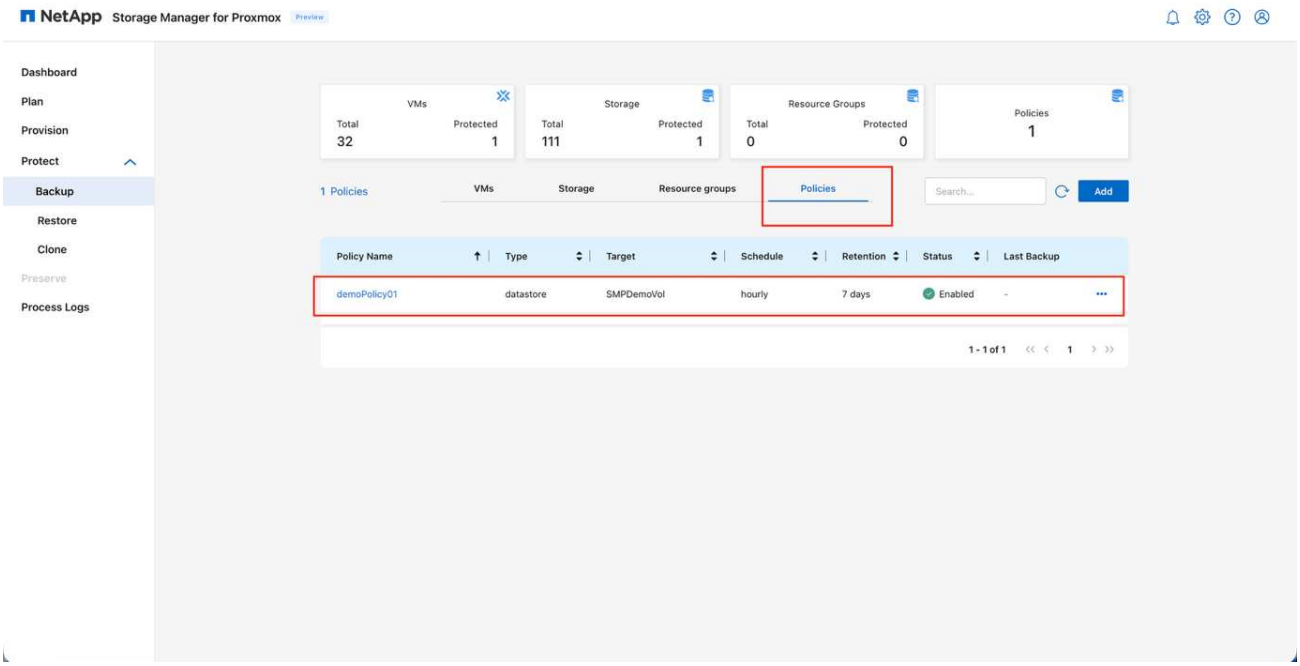
      SnapMirror-Replikation muss in ONTAP über die CLI oder den System Manager konfiguriert werden.

3. Aktivieren Sie unter **Erweiterte Optionen** die **VM-Konsistenz**, wenn Proxmox-Snapshots oder fsfreeze vor dem Auslösen des ONTAP Snapshot verwendet werden sollen.
4. Klicken Sie auf **Richtlinie erstellen**, um die Konfiguration zu speichern.

▼ Sicherungsrichtlinie anzeigen: Zeitplan und Aufbewahrungsrichtlinie



▼ **Sicherungsrichtlinie anzeigen: Replikations- und erweiterte Optionen**



Ein VM-Sicherungsauftrag kann auch sofort durch Klicken auf **Backup** ausgelöst werden, anstatt auf den geplanten Ausführungszeitpunkt einer Ressourcengruppe zu warten.

Virtuelle Maschinen oder Datenspeicher wiederherstellen

Verwenden Sie SMP, um eine Proxmox-VM aus einem Backup wiederherzustellen.

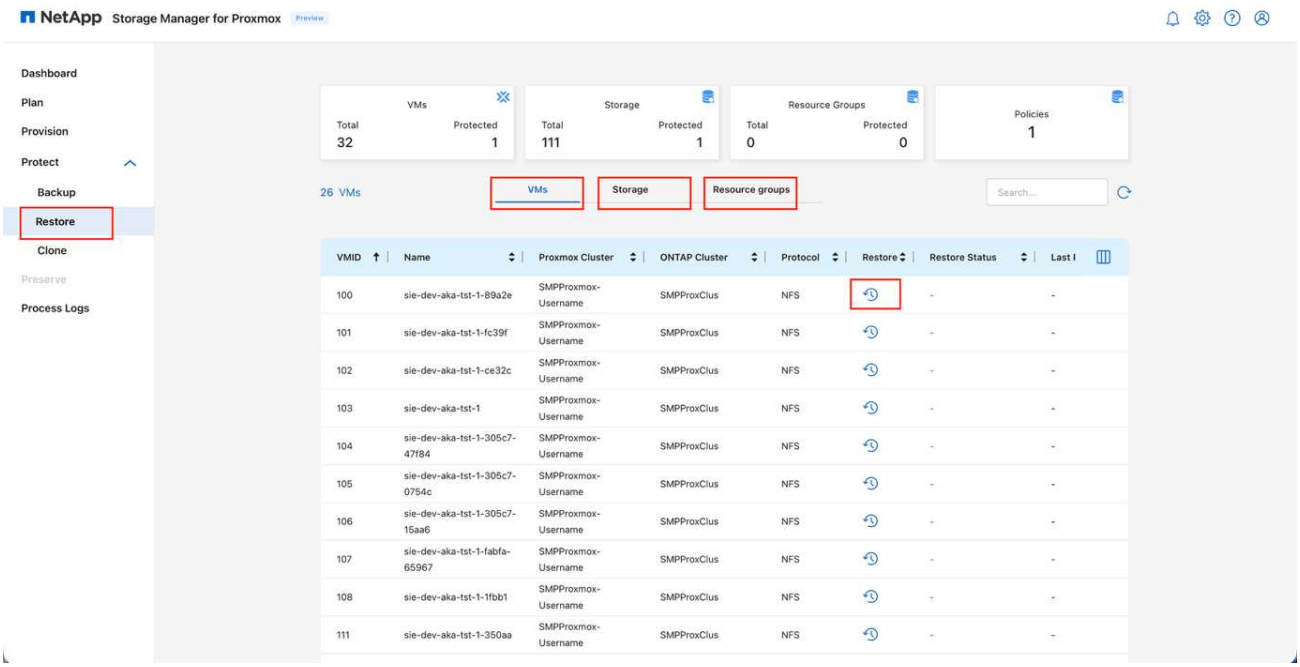
Bevor Sie beginnen

Virtuelle Maschinen müssen vor der Wiederherstellung ausgeschaltet werden.

Schritte

1. Wählen Sie im Navigationsbereich auf der linken Seite der Weboberfläche die Option **Wiederherstellen** aus.
2. Wählen Sie die virtuelle Maschine, den Speicher oder die Ressourcengruppe aus, die wiederhergestellt werden soll.

▼ **Seite „Wiederherstellen“ anzeigen**

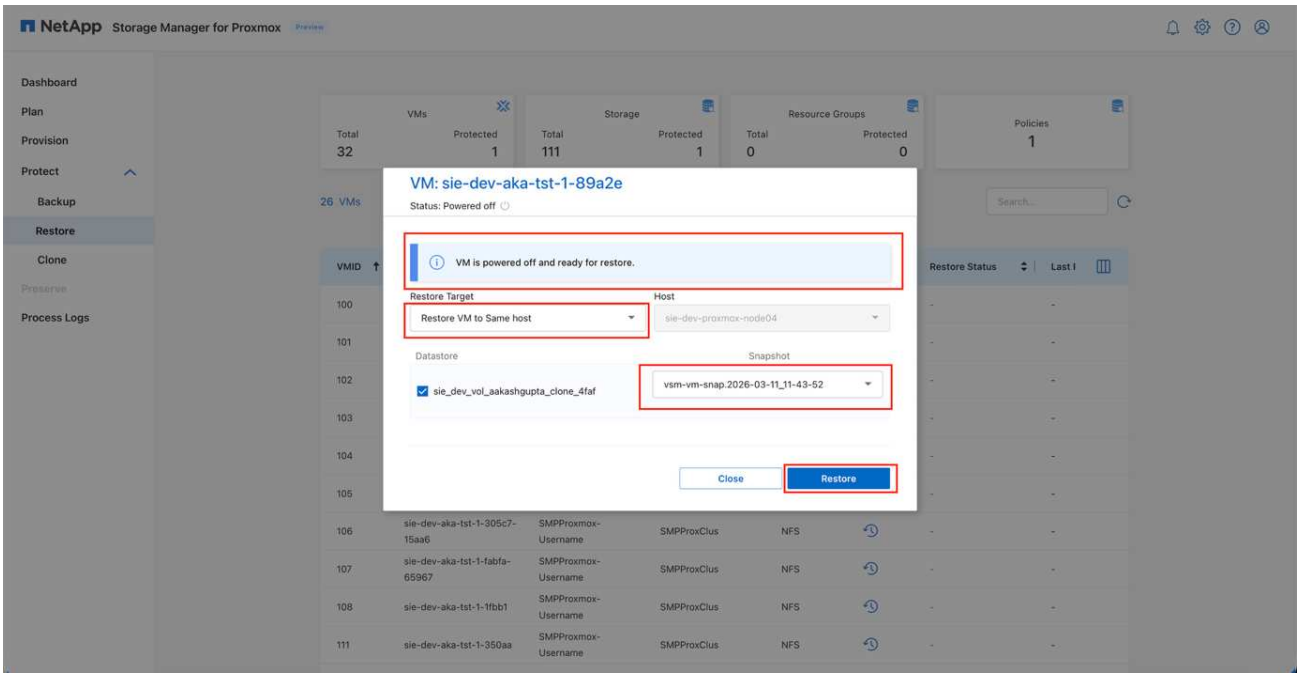


3. Klicken Sie auf das Symbol **Wiederherstellen**.

Je nach Auswahl (VM, Storage oder Ressourcengruppe) öffnet sich das Wiederherstellungs-Popup-Fenster.

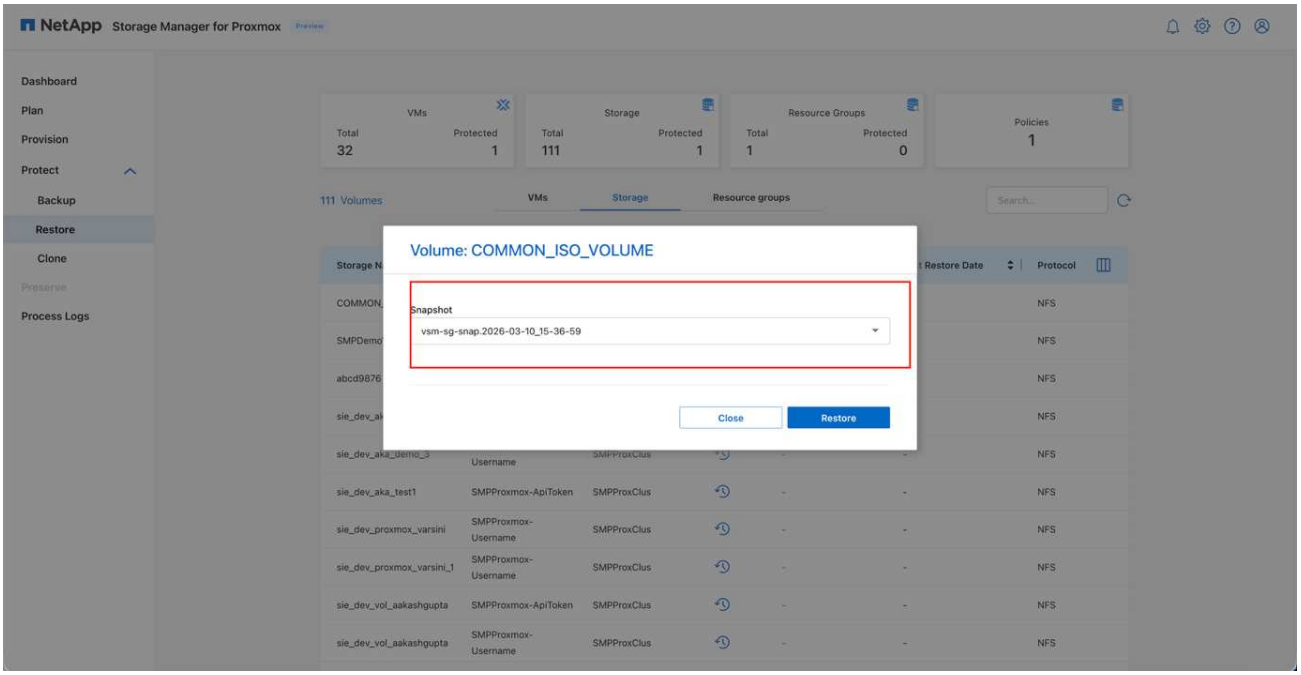
> Je nach ausgewählter Ressource werden die für die jeweiligen Komponenten erstellten Snapshots angezeigt. Beispielsweise werden Snapshots auf Ressourcengruppenebene nur angezeigt, wenn eine Ressourcengruppe ausgewählt ist. Gleiches gilt für Speicher. Bei virtuellen Maschinen hingegen werden alle komponentenübergreifend erstellten Snapshots zur Auswahl angezeigt.

▼ **Dialogfeld „Wiederherstellen“ anzeigen: Snapshot-Auswahl**

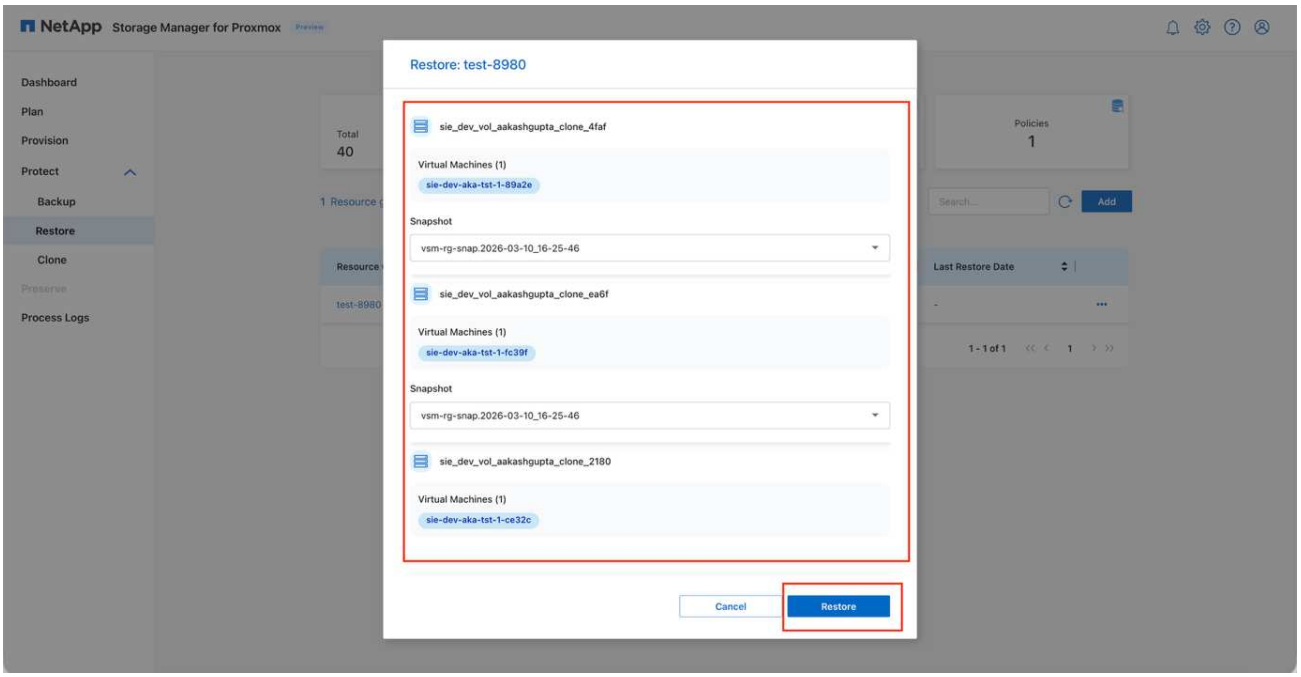


4. Wählen Sie die gewünschten Optionen aus:
   a. **Wiederherstellungsziel**: Option zur Wiederherstellung auf demselben Host oder einem alternativen Host
   b. **Host**: Wenn ein alternativer Host ausgewählt ist, können Sie über das Dropdown-Menü einen beliebigen verfügbaren Host innerhalb des Clusters auswählen
   c. **Momentaufnahme**: Wählen Sie die passende Momentaufnahme für zeitpunktgenauen Restore
5. Klicken Sie auf **Wiederherstellen**.

▼ Wiederherstellung läuft

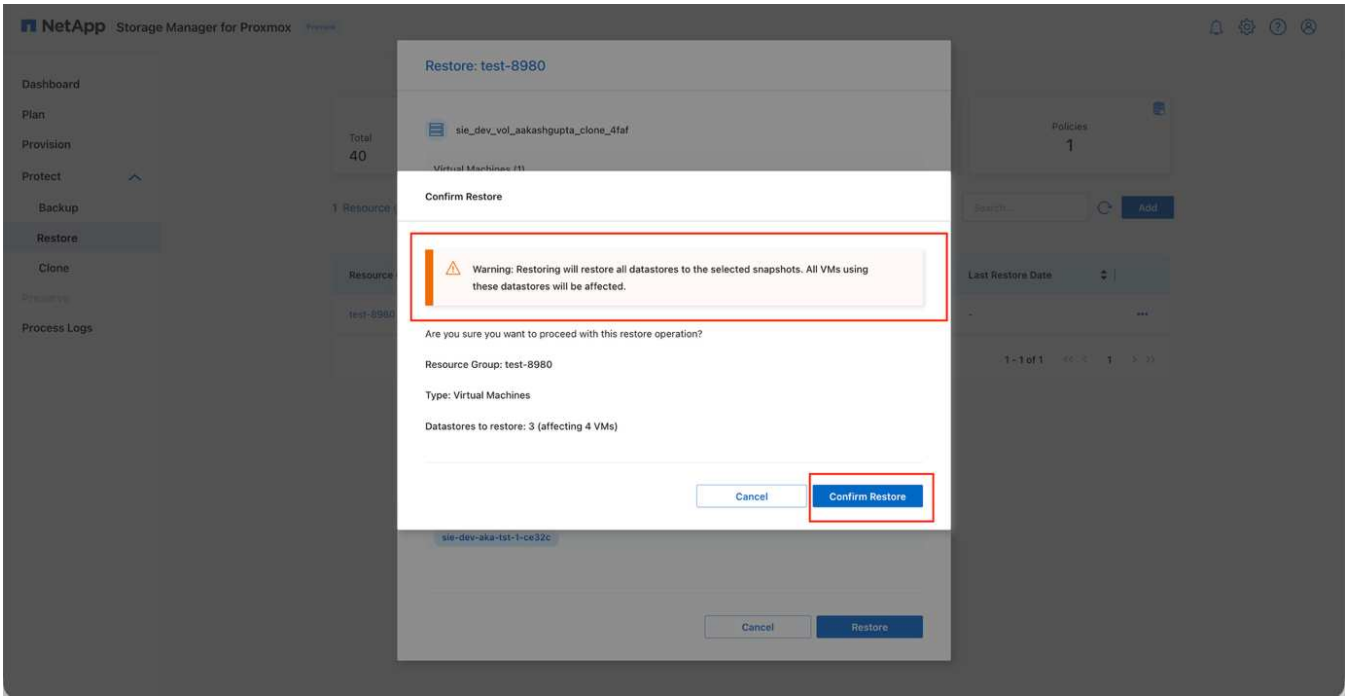


▼ Wiederherstellung abgeschlossen



Wenn eine Wiederherstellung auf Speicherebene eingeleitet wird, werden alle virtuellen Maschinen auf diesem Volume oder LUN ausgeschaltet, und das System stellt die gesamte Speichereinheit als Ganzes wieder her.

▼ **Wiederherstellung auf Speicherebene anzeigen**



Details zum Wiederherstellungs-Workflow

Der Wiederherstellungsablauf variiert je nach zugrunde liegendem Speichertyp und umfasst die folgenden Hauptschritte:

1. **Wiederherstellungsbereich definieren**: Wählen Sie aus, ob das Schutzziel ein Datenspeicher (ONTAP-Volume), eine Ressourcengruppe (mehrere Volumes oder VMs) oder eine einzelne VM ist.

2. **Wiederherstellungsvorgang ausführen**: Der VM-Wiederherstellungsprozess unterscheidet sich je nach Speicherprotokoll:
   - **NFS-basierte Wiederherstellungen**: Bei der Wiederherstellung eines Volumes oder Datenspeichers auf NFS initiiert SMP eine Volume-Snap-Restore-Operation auf dem Ziel-Volume. Für VMs, die auf NFS-Volumes gehostet werden, validiert SMP die Wiederherstellungsparameter einschließlich VM-ID, Snapshot-Name, Standort-IDs und Speichertyp. Wenn die VM läuft, stoppt SMP sie durch Abfrage ihres Status und Ausführung eines Stoppbefehls. Das System stellt dann die VM-Festplatten mithilfe einer Dateiwiederherstellung aus dem Snapshot wieder her.
   - **iSCSI-basierte Wiederherstellungen**: Bei iSCSI-Datenspeichern oder LUNs stellt SMP die LUN aus dem Snapshot wieder her, verifiziert das wiederhergestellte Gerät, führt einen iSCSI-Rescan auf allen Proxmox-Knoten durch und stellt die Geräteverfügbarkeit sicher. Für VMs auf iSCSI-Speicher klont SMP die Snapshot-LUNs, ordnet die geklonten LUNs dem Proxmox-Host zu und importiert sie per iSCSI-Erkennung. Anschließend wird der wiederhergestellte Speicher hinzugefügt und die VM-Konfigurationen aktualisiert. Die VM-Festplatten werden zurück auf ihren ursprünglichen Speicher verschoben, wobei der Fortschritt pro VM protokolliert wird. Der Prozess schließt mit Bereinigungsaktivitäten ab, einschließlich der Entfernung temporärer Speicher und der Löschung geklonter LUNs.

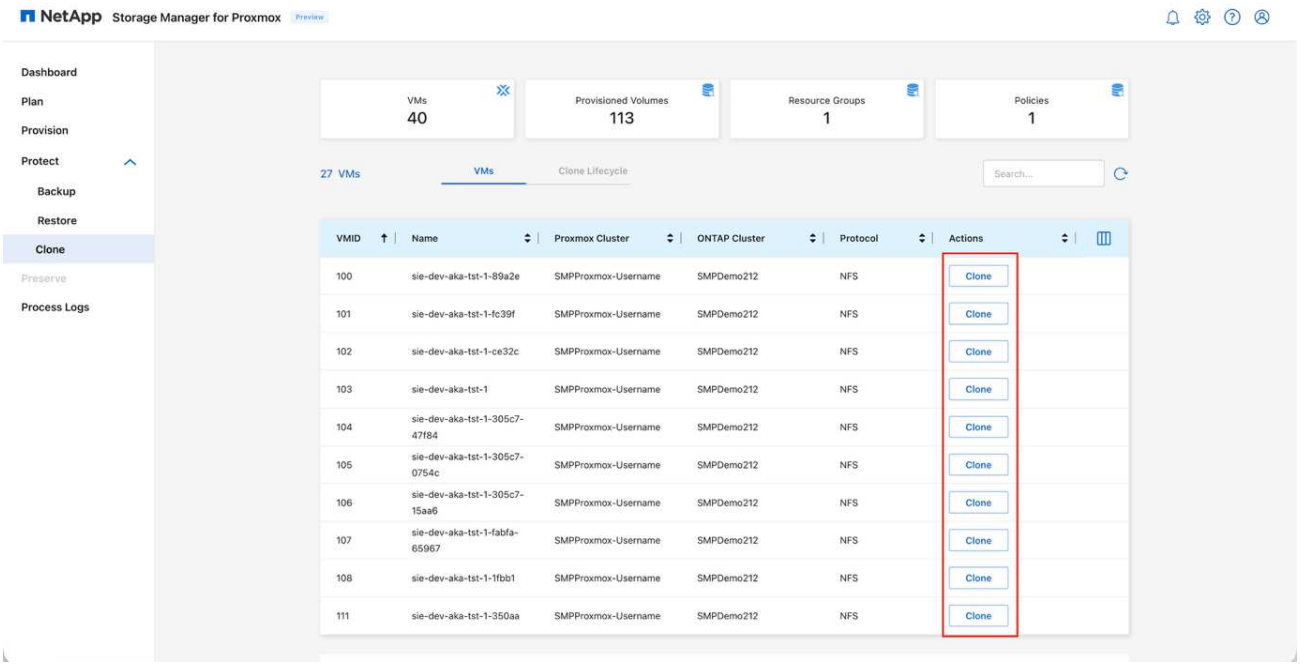
Virtuelle Maschinen klonen

Verwenden Sie SMP, um Klone virtueller Maschinen für Entwicklung, Tests oder schnelle Bereitstellung zu erstellen.

Schritte

1. Öffnen Sie den Bereich **Schützen** und wählen Sie im linken Navigationsmenü **Klonen** aus.
2. Suchen Sie in der VM-Liste die gewünschte VM und klicken Sie in der Spalte **Aktionen** auf **Klonen**.
3. Im Fenster „VM klonen“ wählen Sie den **Zielknoten** aus, auf dem der Klon erstellt werden soll.

▼ **Dialogfeld „VM klonen“ anzeigen**



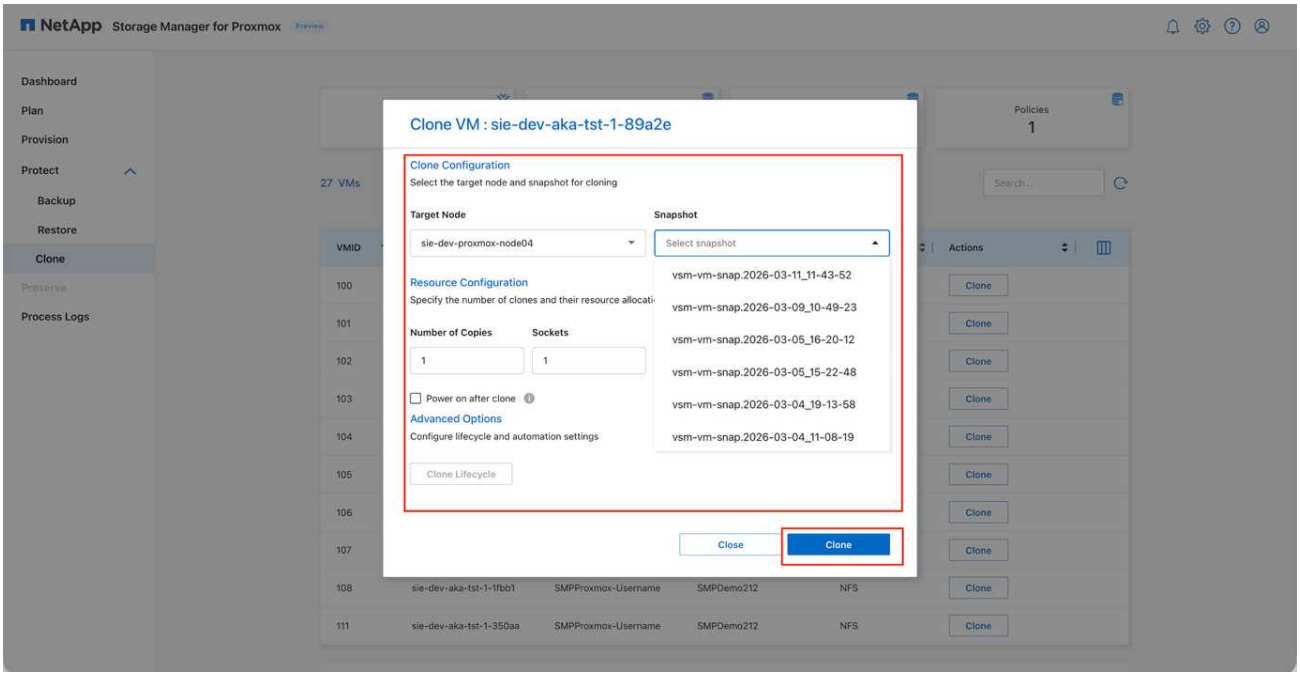
4. Wählen Sie den **Snapshot** aus, der als Quelle für den Klon verwendet werden soll.

In der aktuellen Version wird das Klonen auf dem aktiven Dateisystem durchgeführt. In einer zukünftigen Version wird der Klon-Workflow die Auswahl eines Snapshots ermöglichen, in welchem Fall Dateiklonen mithilfe eines neuen Volumes erstellt werden, das aus dem ausgewählten Snapshot erstellt wurde.

5. Geben Sie die **Anzahl der Kopien**, **CPU-Kerne**, **Sockel** und **Speicher** für die geklonte VM an.
6. (Optional) Aktivieren Sie **Einschalten nach Klonen**, wenn die geklonte VM nach der Erstellung automatisch starten soll.
7. (Optional) Wählen Sie **Neuen Datenspeicher erstellen**, wenn der Klon auf einem neu erstellten Datenspeicher abgelegt werden soll.
8. Unter **Erweiterte Optionen** aktivieren Sie die **Netzwerkkonfiguration**, wenn Netzwerkeinstellungen automatisch auf den Klon angewendet werden sollen.
9. Klicken Sie auf **Klonen**, um den Klonprozess zu starten.

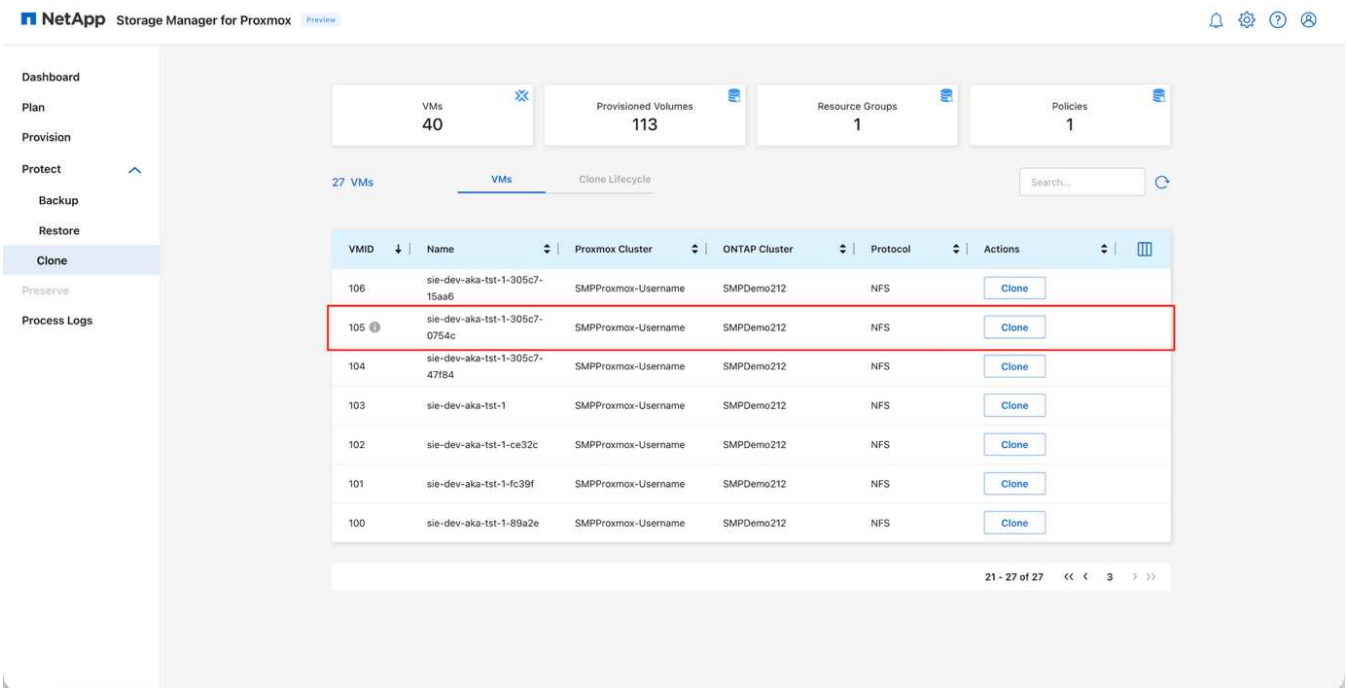
   Der Klon-Workflow stellt die neue VM mithilfe der Rapid-Cloning-APIs von ONTAP bereit und weist der geklonten Instanz eine eindeutige fünfstellige GUID zu.

▼ Klonvorgang anzeigen



Die geklonte VM wird sowohl in der Sicherungs- als auch in der Klonliste angezeigt und kann mithilfe bestehender Sicherungsrichtlinien geschützt werden. Um die geklonten VMs in diesen Listen sichtbar zu machen, führen Sie eine Erkennung für die Proxmox- und ONTAP-Pläne durch.

▼ Geklonte VMs in Listen anzeigen



Details zum Klon-Workflow

SMP automatisiert das schnelle Klonen von virtuellen Maschinen, indem es die rechenintensiven Aufgaben an ONTAP auslagert, um speicherseitige Klone anstelle von hostseitigen Dateikopien durchzuführen. Im Hintergrund nutzt SMP ONTAP FlexClone-Semantik (snapshot-basierte, beschreibbare, platzsparende Klone), sodass Klone schnell erstellt werden und anfänglich wenig Kapazität belegen; Datenzugriffe über den Proxmox-Host werden nach Möglichkeit vermieden.

Dieser Ansatz beschleunigt die VM-Bereitstellung, indem er die Klonarbeit in ONTAP verschiebt und so schnelle, schlanke und speichereffiziente Klone liefert, die sich für Entwicklung/Test, Labore und schnelle Aktualisierungszyklen eignen.

Standardmäßig wird das aktive Dateisystem geklont. Der Klon-Workflow ermöglicht auch die Auswahl eines Snapshots. In diesem Fall werden Dateiklone mithilfe eines neuen Volumes durchgeführt, das aus dem ausgewählten Snapshot erstellt wird.

Überwachungsvorgänge

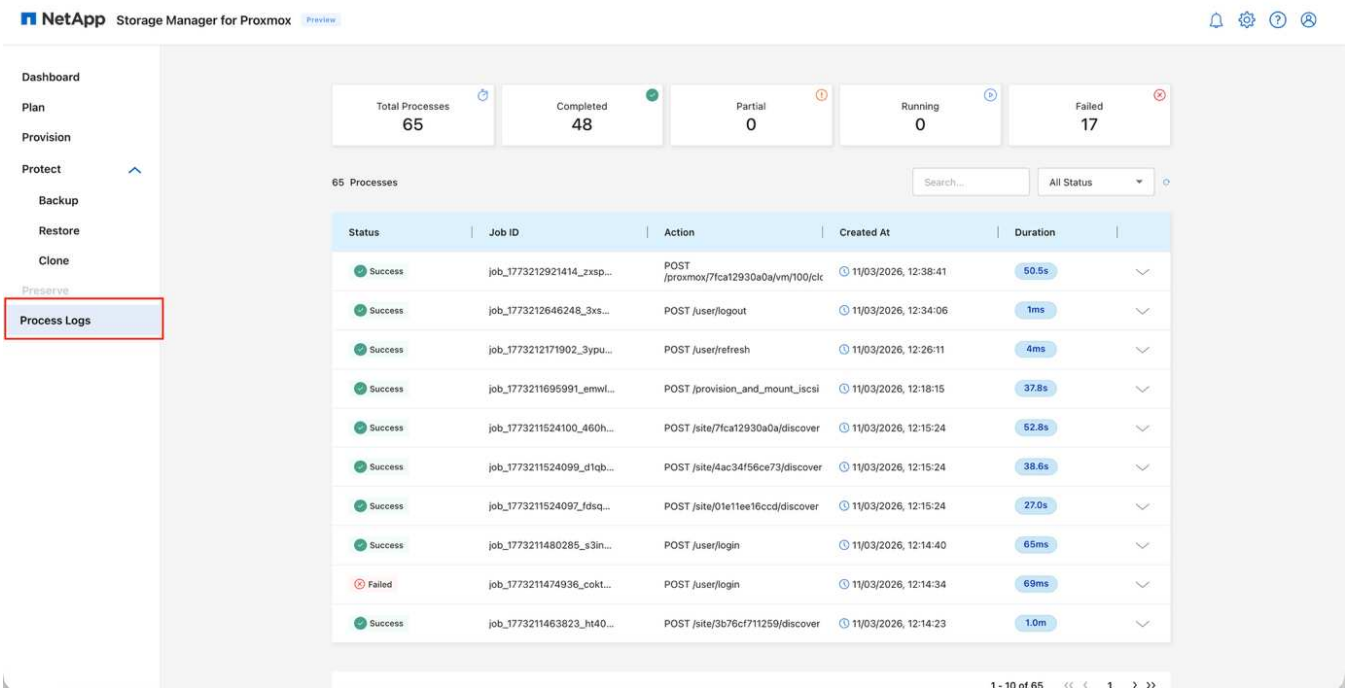
Nutzen Sie die Prozessprotokolle und Dashboard-Ansichten, um SMP-Vorgänge zu überwachen und zu verfolgen.

Prozessprotokolle

Die Ansicht „Prozessprotokolle“ bietet eine konsolidierte Aufzeichnung aller über Storage Manager für Proxmox durchgeführten Operationen. Jeder Eintrag zeigt den Auftragsstatus, die Auftrags-ID, die durchgeführte Aktion, die Startzeit und die Dauer an. So lassen sich abgeschlossene Aufgaben leicht nachverfolgen, fehlgeschlagene oder unvollständige Operationen identifizieren und die Abfolge der in der Umgebung ausgeführten Aktionen überprüfen.

Filter und Suchoptionen sind verfügbar, um schnell bestimmte Jobs zu finden oder die Liste nach Status einzugrenzen.

▼ Prozessprotokolle anzeigen

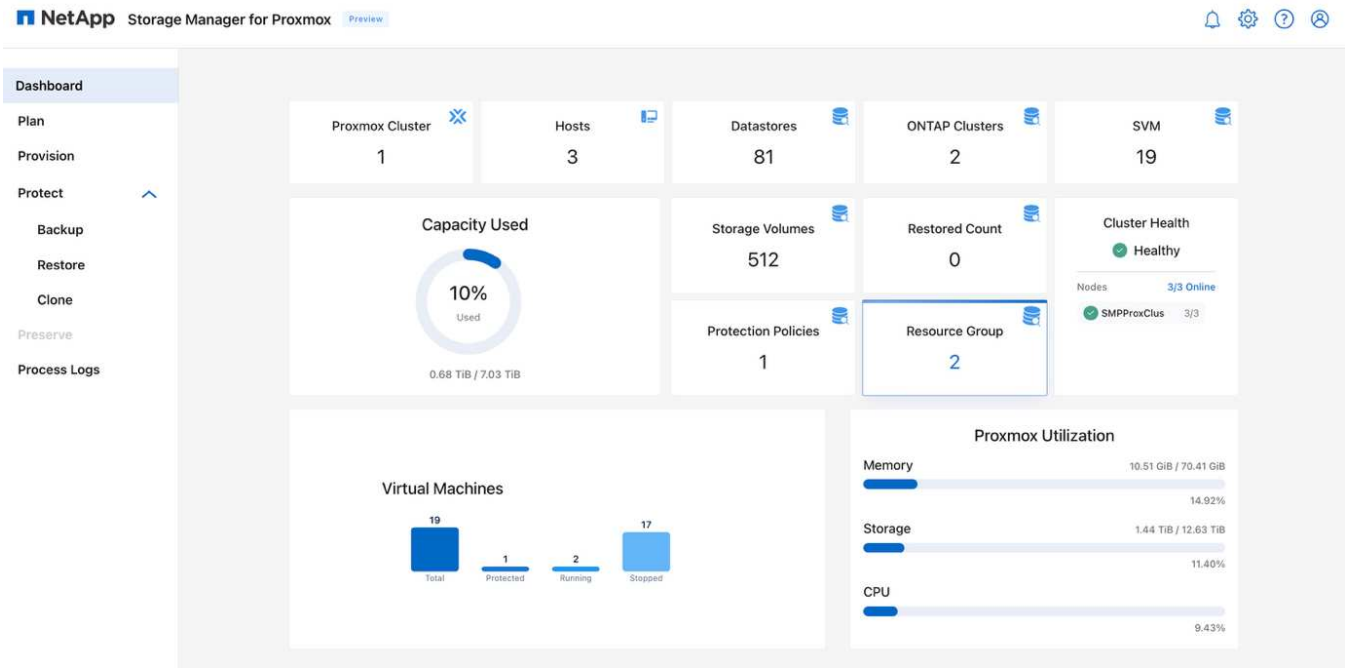


Dashboard

Das Dashboard bietet einen schnellen Überblick über die gesamte Storage Manager for Proxmox-Umgebung. Es fasst wichtige Bestandsdaten wie die Anzahl der Proxmox-Cluster, Hosts, Datastores, ONTAP Cluster und geschützten virtuellen Maschinen zusammen. Auch die Kapazitätsauslastung, das gesamte Speichervolumen, die Schutzrichtlinien und die Ressourcengruppen werden angezeigt, um einen klaren Überblick über die Systemnutzung zu geben.

Der Clusterzustand wird prominent angezeigt und gibt den Status aller verbundenen Knoten an. Im unteren Bereich des Dashboards wird die VM-Verteilung (gesamt, laufend und gestoppt) hervorgehoben und die Proxmox-Ressourcenauslastung für Arbeitsspeicher, Speicher und CPU in Echtzeit dargestellt. Diese Ansicht ermöglicht eine schnelle Beurteilung des Systemzustands, die Identifizierung von Ressourcenengpässen und die Überwachung des allgemeinen Betriebszustands.

▼ Dashboard anzeigen



Zusammenfassung

Storage Manager für Proxmox bietet eine optimierte und einheitliche Möglichkeit, Schutz-, Klon- und Wiederherstellungsvorgänge in Proxmox-Umgebungen zu verwalten. Durch die direkte Integration mit ONTAP bringt die Lösung die Effizienz, Zuverlässigkeit und Leistung von Enterprise-Klasse-Speicher in die täglichen VM-Workflows. ONTAPs platzsparende Snapshots, schnelle Klonfunktionen und integrierte Replikation bieten einen konsistenten und vorhersehbaren Datenschutz, während SMP diese Funktionen in einer intuitiven, aufgabenorientierten Benutzeroberfläche vereinfacht.

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.