



Continuità operativa per i carichi di lavoro di Proxmox VE

NetApp virtualization solutions

NetApp
October 22, 2026

This PDF was generated from <https://docs.netapp.com/it-it/netapp-solutions-virtualization/proxmox/proxmox-business-continuity.html> on October 22, 2026. Always check docs.netapp.com for the latest.

Sommario

Continuità operativa per i carichi di lavoro di Proxmox VE	1
Scopri la continuità operativa di Proxmox VE con SnapMirror sincronizzazione attiva	1
Sfide dei clienti	1
Panoramica della soluzione	2
Come la soluzione reagisce ai guasti	6
Scegli tra SnapMirror active sync e MetroCluster	7
Considerazioni su Corosync per un cluster esteso Proxmox VE	11
Integrazione con Storage Manager per Proxmox	12
Storage condiviso NFS con SnapMirror active sync per NAS	13
Informazioni correlate	17
Configura la continuità operativa di Proxmox VE con storage NAS	17
Passaggio 1: Configura il mediatore	18
Passaggio 2: Proteggi la SVM NFS con SnapMirror active sync	20
Passaggio 3: Configura un VIP LIF con BGP per le reti di livello 3	21
Passaggio 4: Crea il Proxmox VE stretch cluster con un QDevice	22
Passaggio 5: Esegui il provisioning dello storage condiviso NFS protetto	23
Passaggio 6: Configura HA e i backup delle VM	25
Passaggio 7: Verifica del failover pianificato	25
Informazioni correlate	26
Configurare e utilizzare Storage Manager per Proxmox	26
Scopri Storage Manager per Proxmox	27
Installare e configurare Storage Manager per Proxmox	28
Configurare Storage Manager per Proxmox	30
Provisioning dello storage	35
Proteggere le macchine virtuali	46
Ripristinare macchine virtuali o datastore	52
Clonare macchine virtuali	56
Operazioni di monitoraggio	58
Riepilogo	60

Continuità operativa per i carichi di lavoro di Proxmox VE

Scopri la continuità operativa di Proxmox VE con SnapMirror sincronizzazione attiva

Le aziende che eseguono macchine virtuali (VM) business-critical su Proxmox Virtual Environment (VE) e i service provider che ospitano le VM dei clienti su Proxmox VE hanno bisogno che queste VM continuino a funzionare quando un sistema storage o un intero data center va offline. ONTAP SnapMirror active sync replica in modo sincrono lo storage condiviso di un cluster Proxmox VE esteso su due siti ed esegue automaticamente il failover dello storage al sito superstite. Ottieni un recovery point objective (RPO) pari a zero, un ripristino automatizzato senza script o runbook e lo stesso storage condiviso in entrambi i siti, così l'alta disponibilità (HA) di Proxmox VE può riavviare le VM senza alcuna riconfigurazione dello storage. Per lo storage condiviso NFS, la soluzione utilizza SnapMirror active sync per NAS.

Sfide dei clienti

Implementare la resilienza dello storage e del sito per Proxmox VE utilizzando esclusivamente strumenti nativi è difficile:

- **Perdita di dati in seguito a un guasto del sito.** La replica dello storage di Proxmox VE e Proxmox Backup Server sono asincroni. Le modifiche apportate dall'ultima replica o dall'ultimo backup andranno perse in caso di guasto del sito primario.
- **Ripristino manuale e lento.** Il ripristino in un sito secondario di solito implica la promozione delle repliche, il montaggio dello storage con un indirizzo diverso, l'aggiornamento `/etc/pve/storage.cfg` e il riavvio delle macchine virtuali. Ogni passaggio manuale aggiunge tempo di inattività e il rischio di errori durante un'interruzione.
- **Storage esteso che compete con le VM per le risorse host.** Lo storage esteso iperconvergente, come Ceph in modalità stretch, viene eseguito sui nodi Proxmox VE e mantiene due repliche di ogni oggetto in ciascun sito. Il traffico di replica, ripristino e ribilanciamento consuma CPU, memoria e risorse di rete sugli stessi nodi che eseguono le VM.
- **Due decisioni di quorum che devono concordare.** Qualsiasi architettura a due siti richiede un witness in un terzo dominio di errore, sia per il cluster sia per lo storage. Se il cluster e lo storage scelgono siti sopravvissuti diversi dopo un guasto del collegamento tra i siti, le VM si riavviano su nodi che non riescono a raggiungere lo storage attivo.
- **Un indirizzo di storage che deve funzionare in entrambi i siti.** Dopo un failover dello storage, i nodi Proxmox VE devono raggiungere lo storage condiviso allo stesso indirizzo. Tale indirizzo deve essere raggiungibile in entrambi i siti, il che di solito significa una VLAN di livello 2 estesa tra i siti.

Sfide per i fornitori di servizi

I fornitori di servizi che sviluppano servizi cloud su Proxmox VE si trovano ad affrontare le stesse sfide, con in più gli accordi sul livello di servizio (SLA) dei tenant:

- **Il sistema storage rappresenta un punto di guasto condiviso.** Proxmox VE HA protegge le VM dei

tenant da un guasto dell'host, ma non da un guasto del sistema storage che ospita i loro dischi. Un'interruzione del sistema storage influisce su tutti i tenant presenti su tale sistema.

- **Impossibile vendere una maggiore disponibilità.** Senza replica sincrona e il failover automatico dello storage, un provider non può offrire un livello di disponibilità premium con zero perdita di dati e maggiori garanzie di uptime.
- **Isolamento dei tenant durante il ripristino.** I test di ripristino, manutenzione e disaster recovery devono interessare solo i tenant coinvolti, non l'intera piattaforma.

Sfide aziendali

Le aziende che migrano carichi di lavoro mission-critical da altri hypervisor a Proxmox VE si aspettano la stessa resilienza del sito di prima, come ad esempio l'assenza di perdita di dati per database e applicazioni aziendali e il ripristino senza un runbook manuale. Soddisfare tale aspettativa utilizzando esclusivamente gli strumenti nativi di Proxmox VE richiede un notevole impegno in termini di progettazione, scripting e gestione operativa.

Panoramica della soluzione

La soluzione combina un cluster stretch Proxmox VE con la sincronizzazione attiva di SnapMirror sui sistemi NetApp AFF in due siti:

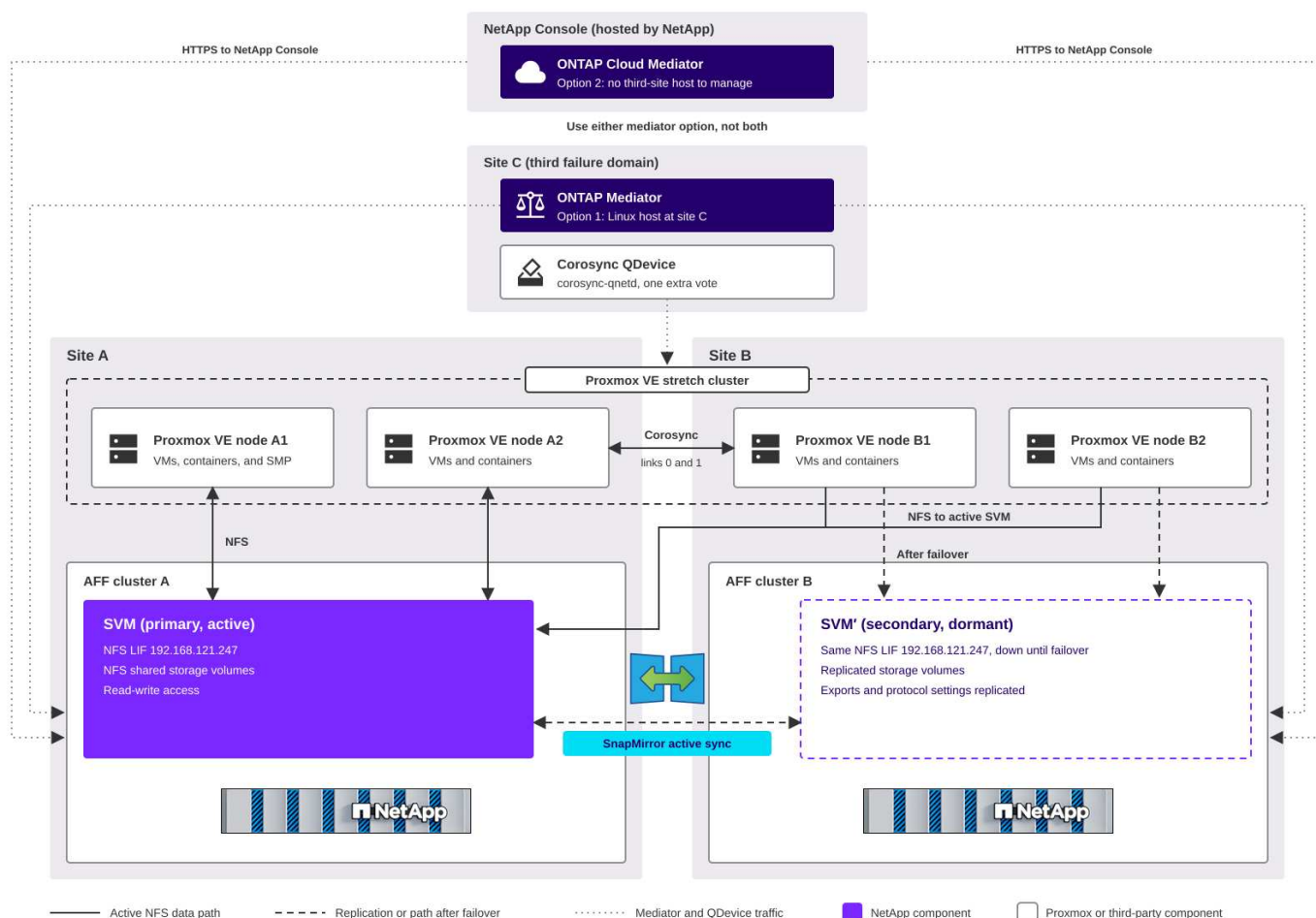
- **RPO zero.** ONTAP replica ogni scrittura sullo storage condiviso in modo sincrono dal cluster primario nel sito A al cluster secondario nel sito B.
- **Stesso storage condiviso in entrambi i siti.** Dopo un failover, il cluster secondario presenta lo stesso storage a Proxmox VE, quindi le definizioni di storage in `/etc/pve/storage.cfg` restano valide.
- **Failover automatico.** Un mediatore funge da testimone esterno ai due siti. Puoi installare ONTAP Mediator in un terzo sito oppure utilizzare ONTAP Cloud Mediator, un servizio ospitato in NetApp Console. Quando lo storage primario o il sito si guasta, ONTAP esegue il failover al sito B senza intervento manuale.
- **Controllo granulare.** Puoi scegliere quali carichi di lavoro proteggere e puoi eseguire il failover dei carichi di lavoro singolarmente, ad esempio per spostare un tenant o un'applicazione per la manutenzione del sito.
- **Utilizzo della copia secondaria.** Puoi clonare la copia secondaria per lo sviluppo, i test o i test di disaster recovery senza compromettere la replica.

Come la soluzione affronta le sfide

Sfida	Come ti aiuta la soluzione	Cosa hai ancora in programma
Perdita di dati e recupero manuale	La replica sincrona offre un RPO pari a zero. ONTAP esegue il failover automaticamente e l'SVM secondario presenta lo stesso indirizzo NFS, quindi <code>/etc/pve/storage.cfg</code> resta valido.	Proxmox VE HA continua a riavviare le VM da un sito guasto.
Storage esteso sugli host	La replica viene eseguita sui controller AFF, non sui nodi Proxmox VE, quindi CPU host, memoria e rete rimangono disponibili per le VM. ONTAP mantiene una copia in ogni sito e l'efficienza dello storage si applica a entrambe le copie.	Come qualsiasi replica sincrona, la soluzione richiede una seconda copia completa nel sito B e la replica aggiunge carico a entrambi i cluster AFF. Dimensiona entrambi i cluster in base al carico di lavoro della replica.

Sfida	Come ti aiuta la soluzione	Cosa hai ancora in programma
Due decisioni del quorum	ONTAP Mediator, o ONTAP Cloud Mediator come servizio nella NetApp Console, è un witness leggero esterno al percorso dei dati. Questa soluzione mostra come allineare il QDevice corosync con il cluster primario in modo che entrambi scelgano lo stesso sito.	Per il QDevice è ancora necessaria una terza posizione. È necessaria anche per ONTAP Mediator, ma non per ONTAP Cloud Mediator. Vedi Opzioni del mediatore .
Un indirizzo di storage in entrambe le sedi	L'SVM secondario assume lo stesso indirizzo NFS LIF, quindi non è necessario alcun rimontaggio o riconfigurazione dello storage.	La sottorete NFS deve essere raggiungibile in entrambi i siti, in genere tramite una VLAN di livello 2 estesa. Consulta Reti di livello 3 con VIP LIFs e BGP per lo stato di qualificazione delle VIP LIF.

Il diagramma seguente mostra l'Architettura della soluzione con storage condiviso NFS.



Sito A e sito B

Ogni sito dispone di un cluster a due nodi AFF e di metà dei nodi Proxmox VE. Il cluster primario nel sito A fornisce lo storage condiviso a tutti i nodi Proxmox VE. I nodi nel sito B raggiungono il cluster primario attraverso la rete tra i siti. Con lo storage NFS, l'SVM secondario nel sito B rimane inattivo fino a quando non si verifica un failover.

Sito C

Un terzo dominio di errore ospita il demone corosync QDevice (`corosync-qnetd`) e, se scegli l'opzione 1, ONTAP Mediator. QDevice fornisce un voto aggiuntivo in modo che il cluster Proxmox VE mantenga il quorum quando un sito si guasta.

NetApp Console

Se scegli l'opzione 2, ONTAP Cloud Mediator viene eseguito come servizio nella NetApp Console, che NetApp ospita e gestisce. Entrambi i cluster AFF si connettono a questo servizio tramite HTTPS, quindi non devi installare né gestire un host mediatore.

Mediator

ONTAP Mediator o ONTAP Cloud Mediator aiuta ONTAP a decidere quale cluster fornisce i dati. Utilizzane uno solo, non entrambi. Per un confronto, vedi [Opzioni del mediatore](#).

cluster stretch Proxmox VE

Tutti i nodi Proxmox VE appartengono a un unico cluster e condividono le stesse definizioni di storage. Proxmox VE HA riavvia le VM da un sito guasto sui nodi rimanenti. Storage Manager for Proxmox (SMP) viene eseguito come VM HA sul cluster per effettuare il provisioning dello storage condiviso e per eseguire il backup, il ripristino e la clonazione delle VM.

Opzioni del mediatore

SnapMirror active sync utilizza un mediatore come testimone passivo. Durante una partizione di rete o il guasto di un cluster, ONTAP utilizza il mediatore per decidere quale copia continua a gestire le operazioni di I/O. Il mediatore non si trova nel percorso dei dati e non avvia autonomamente i failover. Puoi utilizzare una delle seguenti opzioni, ma non entrambe contemporaneamente.

Considerazione	Opzione 1: ONTAP Mediator	Opzione 2: ONTAP Cloud Mediator
Dove viene eseguito	Un host Linux che installi e gestisci in un terzo dominio di errore, come il sito C, con alimentazione e infrastruttura di rete indipendenti.	Un servizio cloud in NetApp Console. NetApp lo ospita e lo gestisce, quindi non ti serve un host mediatore in un terzo sito.
Versione ONTAP	ONTAP 9.19.1 o versione successiva per la sincronizzazione attiva di SnapMirror per NAS.	ONTAP Cloud Mediator è disponibile a partire da ONTAP 9.17.1. SnapMirror active sync per NAS richiede ONTAP 9.19.1 o versioni successive.
Connettività del cluster	Entrambi i cluster si connettono all'host mediatore. La porta di servizio predefinita è la 31784.	Entrambi i cluster si connettono outbound a NetApp Console tramite HTTPS, direttamente o tramite un proxy HTTP. La latenza ping consigliata verso NetApp Console è inferiore a 200 ms.
Configurazione	Installa il pacchetto sull'host Linux, quindi aggiungilo ai cluster specificando l'indirizzo dell'host e un utente mediatore.	Crea un account di servizio NetApp Console con il ruolo ONTAP Mediator Setup Role , quindi aggiungi il mediatore ai cluster con l'ID dell'organizzazione, l'ID client e il segreto client.

Considerazione	Opzione 1: ONTAP Mediator	Opzione 2: ONTAP Cloud Mediator
Operazioni	Applichi patch e aggiornamenti al sistema host e lo mantieni disponibile.	Nessun host da sottoporre a patch o aggiornare. Dipendi dall'accesso a internet da entrambi i siti e dalla disponibilità del servizio NetApp Console.
Migliore corrispondenza	Ambienti che dispongono di un terzo sito o che non consentono ai cluster di storage di raggiungere internet.	Ambienti senza un terzo sito per un mediatore o che vogliono evitare di gestirne uno.

Tieni presente quanto segue al momento della scelta:

- **Il QDevice necessita comunque di una terza posizione.** ONTAP Cloud Mediator rimuove l'host del mediatore, non l'host del QDevice di corosync. Il QDevice necessita di un piccolo host Linux raggiungibile da tutti i nodi Proxmox VE sulla porta TCP 5403 e non richiede la bassa latenza di corosync.
- **Entrambi i cluster devono avere accesso a NetApp Console.** Se i cluster utilizzano un proxy, installa il certificato della CA radice del proxy su entrambi i cluster. NetApp consiglia un proxy server diverso per ciascun cluster.
- **Con entrambe le opzioni, pianifica lo stesso comportamento in caso di errore.** Quando il mediatore non è disponibile, la replica continua senza perdita di dati, ma i failover automatici e pianificati non sono possibili finché il mediatore non torna di nuovo disponibile. Con ONTAP Cloud Mediator, questo include una perdita di connettività dai cluster alla NetApp Console.



Le opzioni del mediatore in questa sezione si applicano alla sincronizzazione attiva di SnapMirror. Per MetroCluster, questa soluzione utilizza ONTAP Mediator o MetroCluster Tiebreaker. Prima di eseguire il deployment, verifica che la tua versione di ONTAP, l'opzione del mediatore e la versione di Proxmox VE siano elencate insieme in "[NetApp Interoperability Matrix Tool \(IMT\)](#)".

Vantaggi per i fornitori di servizi

- **Disponibilità delle VM oltre l'HA dell'host.** Le VM del tenant continuano a funzionare quando il sistema storage che ospita i loro dischi si guasta. ONTAP esegue il failover al secondo AFF cluster e le VM riprendono le operazioni di I/O sullo stesso storage condiviso senza bisogno di riavvio.
- **Un livello di disponibilità premium.** Puoi offrire un servizio VM a RPO zero e resiliente allo storage come componente aggiuntivo, insieme ai livelli standard su storage non protetto negli stessi cluster.
- **Protezione e failover per singolo tenant.** Con uno storage protetto separato per ogni tenant o livello di servizio, puoi proteggere, eseguire il failover e testare il disaster recovery per ogni tenant in modo indipendente, senza influire sugli altri tenant.
- **Uso ottimale di entrambi i siti.** Puoi impostare alcuni carichi di lavoro come primari nel sito A e altri come primari nel sito B, in modo che entrambi i data center gestiscano carichi di lavoro attivi.

Vantaggi per le imprese

- **Zero perdita di dati per le VM business-critical** durante un guasto del sistema storage o del sito.
- **Ripristino automatico** senza script, rimontaggi di storage o modifiche a `/etc/pve/storage.cfg`.
- **Integrato in ONTAP**, senza alcun livello software aggiuntivo sui nodi Proxmox VE.
- **Operazioni quotidiane da un'unica interfaccia.** Storage Manager per Proxmox esegue il provisioning

dello storage condiviso protetto ed effettua il backup, il ripristino e la clonazione delle VM con snapshot ONTAP e la tecnologia FlexClone.

Come la soluzione reagisce ai guasti

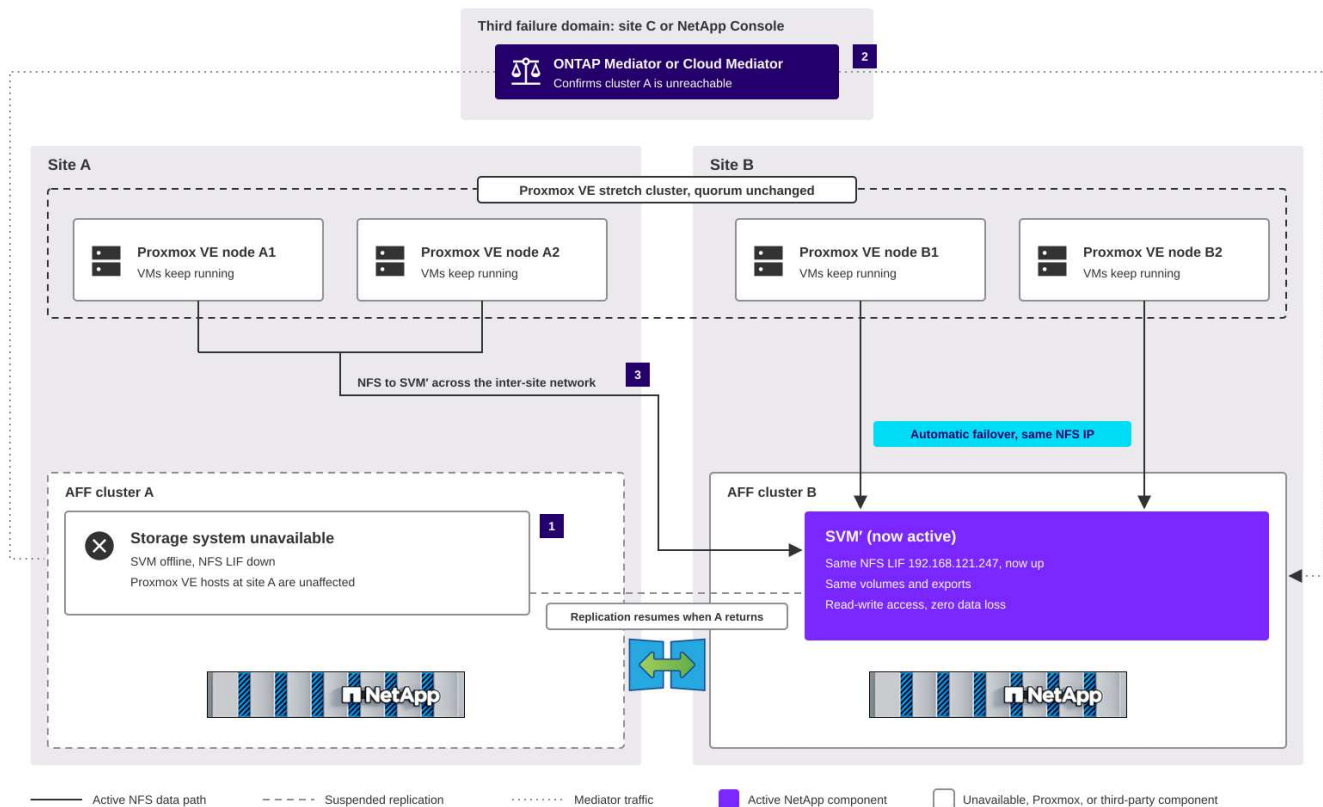
ONTAP e Proxmox VE prendono decisioni indipendenti sul quorum. La progettazione li allinea in modo che entrambi scelgano lo stesso sito di sopravvivenza.

Evento	Comportamento di ONTAP	Comportamento di Proxmox VE
Il sito A ha un guasto	Il mediatore conferma il guasto e ONTAP esegue automaticamente il failover dello storage condiviso al cluster B.	I nodi del sito B e il QDevice mantengono il quorum. L'HA isola i nodi del sito A e riavvia le relative VM sui nodi del sito B. Le VM già presenti sul sito B riprendono le operazioni di I/O dopo il failover dello storage.
Il cluster AFF A si blocca, i nodi Proxmox VE del sito A continuano a funzionare	Il mediatore conferma che cluster A non è raggiungibile e ONTAP esegue automaticamente il failover dello storage condiviso al cluster B.	Nessuna modifica del quorum e nessun riavvio delle VM. Le VM su tutti i nodi riprendono le operazioni di I/O sullo stesso storage condiviso dopo il failover dello storage, con i nodi del sito A che raggiungono il cluster B attraverso la rete tra i siti.
Un controller AFF nel sito A si guasta	Il partner controller subentra in un takeover HA locale. Non si verifica alcun failover attivo di SnapMirror.	Nessun impatto. Le macchine virtuali interrompono brevemente le operazioni di I/O durante il takeover.
Il sito B si guasta	Il cluster A continua a fornire dati. La replica riprende quando il sito B torna operativo.	I nodi del sito A e il QDevice mantengono il quorum. L'HA riavvia le VM del sito B sui nodi del sito A.
Il collegamento tra siti non funziona	Il cluster A continua a servire i dati. Non si verifica alcun failover.	Il QDevice assegna il proprio voto alla partizione del sito A quando l'interruttore è allineato con il cluster primario. I nodi del sito B perdono il quorum e si auto-isolano, e HA riavvia le loro VM sul sito A.
Il sito C non funziona o i cluster perdono l'accesso alla NetApp Console	La replica continua senza perdita di dati, ma i failover automatici e pianificati non sono possibili finché il mediatore non è disponibile. Con ONTAP Cloud Mediator, un guasto del sito C influisce solo sul QDevice.	Il cluster mantiene il quorum grazie ai voti dei quattro nodi. Nessuna VM è interessata.
Un nodo Proxmox VE non funziona	Nessun impatto.	HA riavvia le VM da quel nodo su altri nodi, privilegiando i nodi nello stesso sito.

Guasto del sistema storage

Il guasto di un sistema storage è un caso che l'HA a livello host da sola non può gestire, ed è il caso in cui SnapMirror active sync aggiunge il massimo valore per i service provider. Il diagramma seguente mostra lo stato dopo il guasto del cluster AFF A, mentre tutti i nodi Proxmox VE rimangono online utilizzando lo storage

condiviso NFS.



1. Il cluster AFF A diventa non disponibile. I nodi Proxmox VE nel sito A continuano a funzionare, quindi il cluster non perde il quorum e l'HA non isola alcun nodo.
2. Il mediatore, ONTAP Mediator nel sito C o ONTAP Cloud Mediator nella NetApp Console, conferma che il cluster A non è raggiungibile e ONTAP attiva la SVM secondaria sul cluster B con lo stesso indirizzo NFS LIF, gli stessi volumi e le stesse policy di esportazione.
3. Tutti i nodi Proxmox VE riprendono le operazioni di I/O sullo stesso storage condiviso. I nodi del sito B raggiungono cluster B localmente, mentre i nodi del sito A lo raggiungono tramite la rete tra i siti. Le macchine virtuali mettono in pausa le operazioni di I/O durante il failover e continuano a funzionare senza riavviarsi.

Quando cluster A torna operativo, la replica riprende. Pianifica il failback al cluster A durante una finestra di manutenzione in modo che le VM del sito A possano accedere nuovamente allo storage locale.

Guasto del sito

In caso di guasto di un sito, sia il sistema storage che i nodi Proxmox VE di quel sito vanno offline. ONTAP esegue il failover dello storage condiviso sul cluster superstite e Proxmox VE HA riavvia le VM del sito guasto sui nodi superstiti, come descritto nella tabella.

Scegli tra SnapMirror active sync e MetroCluster

NetApp MetroCluster configurations offrono anche RPO pari a zero e ripristino automatico per un cluster stretch Proxmox VE. Le due soluzioni differiscono per ciò che proteggono:

- **MetroCluster protegge tutti i carichi di lavoro.** MetroCluster combina il clustering basato su array con la replica sincrona. Esegue il mirroring dei dati in ogni aggregato mirrorato, della memoria non volatile

(NVRAM) e della configurazione di ogni SVM nel sito partner, in modo che tutto lo storage condiviso sul cluster sia protetto senza una configurazione per singolo carico di lavoro.

- **SnapMirror active sync protegge un sottoinsieme di carichi di lavoro.** Scegli quali SVM o volumi proteggere e puoi eseguire il failover di ciascuno in modo indipendente. I carichi di lavoro non protetti possono condividere gli stessi cluster.

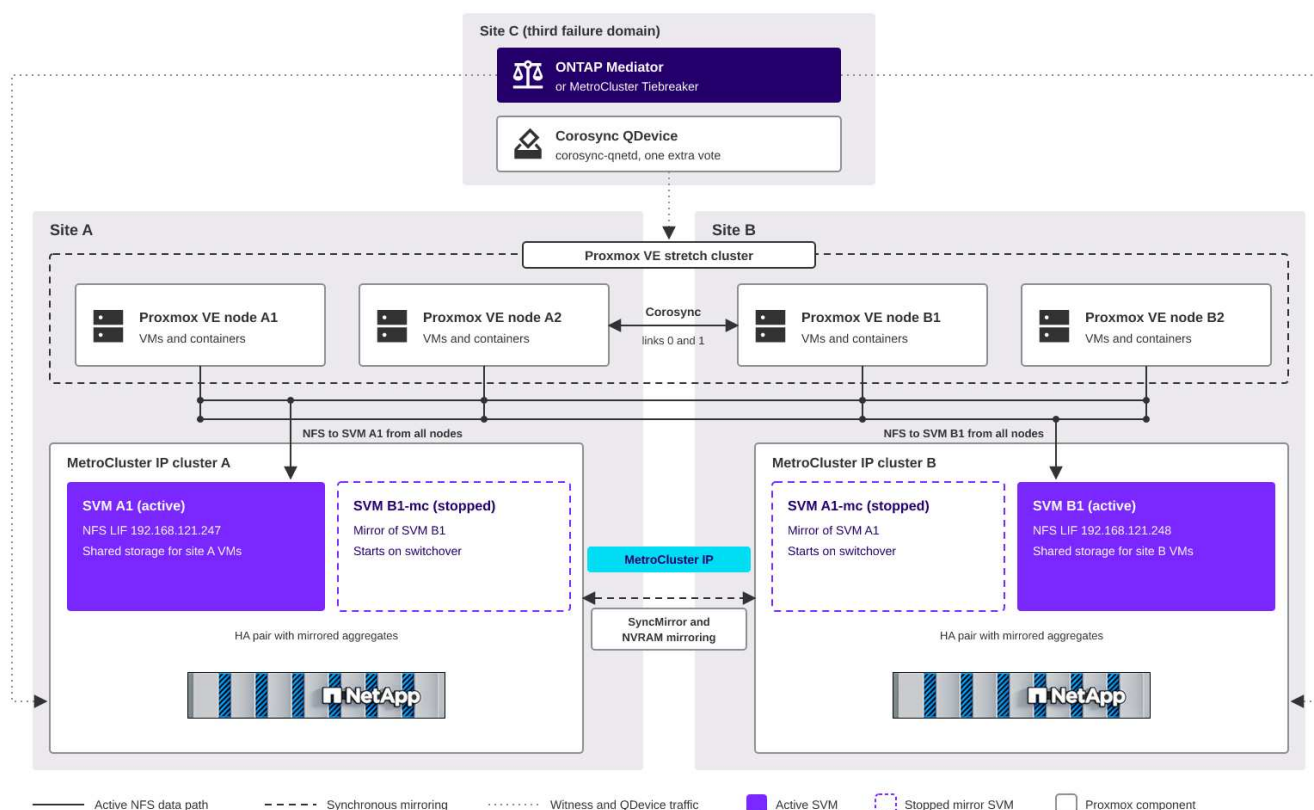
Entrambe le soluzioni mantengono una copia completa dei dati protetti in ogni sito, necessitano di un testimone in un terzo dominio di errore e aggiungono carico di replica ai controller di storage. Differiscono per ambito di protezione, granularità del failover e progettazione del cluster.



Prima di implementare una delle due soluzioni, verifica che la tua versione di ONTAP, la configurazione di sincronizzazione attiva di MetroCluster o SnapMirror e la versione di Proxmox VE siano elencate insieme in "[NetApp Interoperability Matrix Tool \(IMT\)](#)".

MetroCluster architettura con Proxmox VE

Il diagramma seguente mostra un cluster esteso Proxmox VE con una configurazione IP MetroCluster a quattro nodi e storage condiviso NFS.



MetroCluster cluster IP

Ogni sito ha una coppia HA con aggregati mirrorati. La rete IP di back-end di MetroCluster replica i dati (SyncMirror) e NVRAM sul sito partner in modo sincrono.

SVM in entrambi i siti

Ciascun sito può gestire le proprie SVM. Per ogni SVM, MetroCluster mantiene una SVM mirrorata arrestata con il suffisso `-mc` nel sito partner, con la stessa configurazione e gli stessi indirizzi LIF.

Accesso NFS da tutti i nodi

Ogni nodo Proxmox VE monta lo storage condiviso di entrambe le SVM attive, SVM A1 e SVM B1, in modo che l'HA possa riavviare qualsiasi VM su qualsiasi nodo. I nodi del sito B accedono a SVM A1 e i nodi del sito A accedono a SVM B1 attraverso la rete intersito. Questo è lo stesso modello di accesso di SnapMirror active sync.

Commutazione

Se un sito si guasta, ONTAP Mediator o MetroCluster Tiebreaker nel sito C abilita uno switchover automatico. Le SVM mirror nel sito superstite si avviano e servono tutto lo storage condiviso con gli stessi indirizzi NFS, e Proxmox VE HA riavvia le VM dal sito guasto. Un guasto di un singolo controller viene gestito da un takeover HA locale, senza switchover. Dopo aver riparato il sito guasto, risani gli aggregati e torni indietro.

Come MetroCluster reagisce ai guasti

La tabella seguente mostra come una configurazione IP MetroCluster e il cluster esteso Proxmox VE rispondono agli stessi guasti mostrati in [Come la soluzione reagisce ai guasti](#). In questo esempio, SVM A1 è attivo nel sito A e SVM B1 è attivo nel sito B.

Evento	Comportamento di ONTAP	Comportamento di Proxmox VE
Il sito A ha un guasto	ONTAP Mediator o MetroCluster Tiebreaker conferma il guasto e ONTAP esegue lo switchover del sito A. SVM A1-mc si avvia nel sito B con lo stesso indirizzo NFS LIF. SVM B1 continua a servire i dati.	I nodi del sito B e il QDevice mantengono il quorum. L'HA isola i nodi del sito A e riavvia le relative VM sui nodi del sito B. Le VM già in esecuzione sui nodi del sito B continuano a funzionare, mentre quelle su SVM A1 riprendono le operazioni di I/O dopo lo switchover.
Il cluster IP MetroCluster A si blocca, i nodi Proxmox VE del sito A continuano a funzionare	ONTAP Mediator o MetroCluster Tiebreaker conferma che il cluster A non è raggiungibile e ONTAP esegue lo switchover del sito A. L'SVM A1-mc si avvia nel sito B con lo stesso indirizzo LIF NFS.	Nessuna modifica al quorum e nessun riavvio della VM. Le VM su SVM A1 riprendono le operazioni di I/O dopo lo switchover, con i nodi del sito A che raggiungono il sito B attraverso la rete tra i siti.
Un controller del sito A si guasta	Il partner HA del sito A subentra in un takeover HA locale. Non si verifica alcuno switchover.	Nessun impatto. Le macchine virtuali interrompono brevemente le operazioni di I/O durante il takeover.
Il sito B si guasta	ONTAP effettua il passaggio al sito B. SVM B1-mc si avvia nel sito A con lo stesso indirizzo LIF NFS. SVM A1 continua a servire i dati.	I nodi del sito A e il QDevice mantengono il quorum. L'HA riavvia le VM del sito B sui nodi del sito A, dove accedono alla SVM B1 del sito A.

Evento	Comportamento di ONTAP	Comportamento di Proxmox VE
Il collegamento tra siti non funziona	Non si verifica alcuno switchover, perché entrambi i cluster sono ancora in esecuzione. Ogni sito continua a servire le proprie SVM e il mirroring verso il sito partner resta sospeso finché il collegamento non viene ripristinato.	Il QDevice assegna il proprio voto alla partizione del sito A quando l'interruttore è allineato con il sito A. I nodi del sito B perdono il quorum e si isolano automaticamente. L'HA riavvia le VM sull'SVM A1 sui nodi del sito A. Le VM sull'SVM B1 non possono essere riavviate finché il collegamento non viene ripristinato, perché i nodi del sito A non riescono a raggiungere l'SVM B1.
Il sito C si guasta	Il mirroring continua senza perdita di dati, ma lo switchover automatico non è possibile finché il witness non è disponibile. Puoi comunque eseguire lo switchover manualmente.	Il cluster mantiene il quorum grazie ai voti dei quattro nodi. Nessuna VM è interessata.
Un nodo Proxmox VE non funziona	Nessun impatto.	HA riavvia le VM da quel nodo su altri nodi, privilegiando i nodi nello stesso sito.

Il guasto del collegamento tra i siti è la principale differenza rispetto a una progettazione con un solo sito primario. Ogni volta che entrambi i siti ospitano SVM attive, con MetroCluster o con due SVM SnapMirror active sync in direzioni opposte, il tie breaker di corosync può favorire un solo sito. Le VM il cui SVM attivo si trova nell'altro sito restano inattive finché il collegamento non viene ripristinato. Per limitare l'impatto, usa collegamenti inter-sito ridondanti su percorsi fisici separati e posiziona le VM più critiche sull'SVM del sito favorito dal tie breaker.

Confronto delle funzionalità

Considerazione	SnapMirror active sync per NAS	MetroCluster IP
Ambito di protezione	SVM e volumi selezionati	Tutti gli aggregati mirrorati e tutte le SVM nella configurazione
Granularità del failover	Ogni SVM in modo indipendente	L'intero sito, tramite switchover
Carichi di lavoro non protetti	Esegui su SVM non protette negli stessi cluster	Puoi usare aggregati non mirrorati, che vanno offline dopo uno switchover finché non li riporti online
Progettazione del cluster	Due cluster indipendenti, collegati tramite una rete IP	Una configurazione di due cluster partner, con una rete back-end IP dedicata MetroCluster
Witness nel sito C	ONTAP Mediator o ONTAP Cloud Mediator	ONTAP Mediator o MetroCluster Tiebreaker
Copie dei dati protetti	Uno per ogni sito	Uno in ogni sito, in aggregati mirrorati
Percorso di replica	SnapMirror sincrono su LIF intercluster	SyncMirror e mirroring NVRAM sulla rete back-end IP di MetroCluster
Indirizzo NFS in entrambe le sedi	VLAN di livello 2 estesa. LIF VIP con qualificazione BGP in sospeso	VLAN Layer 2 estesa o LIF VIP con BGP

Considerazione	SnapMirror active sync per NAS	MetroCluster IP
Ripristino dopo un guasto del sito	Esegui il failback di ogni SVM	Ripara gli aggregati, quindi ripristina il sito

Guida alla selezione

- Scegli MetroCluster quando tutti, o quasi tutti, i carichi di lavoro sullo storage necessitano di un RPO pari a zero, ad esempio quando un'azienda esegue solo macchine virtuali mission-critical sul cluster o quando un service provider offre lo stesso livello di disponibilità a ogni tenant. Ottieni un dominio di protezione unico senza configurazione per singolo carico di lavoro.
- Scegli la sincronizzazione attiva di SnapMirror quando solo un sottoinsieme di carichi di lavoro richiede RPO zero, ad esempio un livello premium per alcuni tenant, oppure quando devi eseguire il failover o testare il disaster recovery per un tenant o un'applicazione alla volta.
- SnapMirror active sync per NAS non è supportato in una configurazione MetroCluster. Usa una soluzione per ogni coppia di cluster.
- Le linee guida relative a corosync, QDevice e HA in questa soluzione si applicano a entrambi. Con MetroCluster, allinea il tie breaker di QDevice con il sito che continua a servire i dati quando il collegamento tra i siti si interrompe e utilizza le regole di affinità dei nodi HA per mantenere le VM nello stesso sito della loro SVM attiva.
- MetroCluster IP supporta anche VIP LIF con BGP per le reti di livello 3 tra i siti.

Considerazioni su Corosync per un cluster esteso Proxmox VE

Proxmox VE utilizza corosync per l'appartenenza al cluster e il quorum. Corosync è più sensibile alla rete tra i siti rispetto a SnapMirror active sync, quindi pianifica prima la rete del cluster.

Latenza e progettazione di rete

- SnapMirror active sync richiede un tempo di andata e ritorno (RTT) tra cluster inferiore a 10 ms. Proxmox raccomanda una latenza di corosync inferiore a 5 ms tra tutti i nodi, quindi il requisito di corosync definisce il limite di distanza per la soluzione.
- Corosync richiede una latenza bassa e costante piuttosto che un'elevata larghezza di banda. Utilizza una rete dedicata per corosync, separata dal traffico di storage e di migrazione live, in modo che i picchi di traffico dello storage non causino timeout di corosync.
- Configura almeno due collegamenti corosync (ad esempio, collegamento 0 e collegamento 1) su percorsi fisici separati tra i siti. Corosync utilizza Kronosnet per commutare automaticamente i collegamenti in caso di guasto di uno di essi.

Quorum con un QDevice presso una terza sede

Suddividi equamente i nodi Proxmox VE tra il sito A e il sito B e aggiungi un QDevice al sito C. Con quattro nodi e un QDevice, il cluster ha cinque voti e ne richiede tre per il quorum, quindi uno dei due siti può guastarsi senza perdere il quorum. Il QDevice si connette al cluster tramite la porta TCP 5403 e non ha il requisito di bassa latenza di corosync, quindi può condividere il sito C con ONTAP Mediator. Se usi ONTAP Cloud Mediator, hai comunque bisogno di una terza posizione per il QDevice, ma può trattarsi di un piccolo host Linux che non ospita anche un mediatore.

Allineamento del tie breaker con il cluster primario

Quando il collegamento tra i siti si interrompe, ma entrambi i siti possono ancora raggiungere il sito C, ONTAP

mantiene il cluster primario nel sito A a servire i dati. Il QDevice deve assegnare il proprio voto allo stesso sito. Per impostazione predefinita, il QDevice sceglie la partizione che contiene l'ID nodo più basso.

PRATICA CONSIGLIATA: Crea il cluster Proxmox VE su un nodo del sito A e unisci gli altri nodi del sito A prima di unire i nodi del sito B, in modo che il sito A mantenga gli ID nodo più bassi. Se lo storage primario viene spostato sul sito B per un periodo prolungato, aggiorna l'impostazione QDevice `tie_breaker` con un ID nodo del sito B.

Se il QDevice avesse preferito il sito B, i nodi del sito A si sarebbero autoisolati e l'HA avrebbe riavviato le VM sui nodi del sito B che non riescono a raggiungere lo storage attivo nel sito A.

Comportamento HA e posizionamento delle VM

- In genere, Proxmox VE HA rileva un nodo guasto e ripristina le sue VM in circa due minuti, incluso un timeout di 60 secondi per il watchdog fencing. In caso di guasto del sito, il failover di SnapMirror active sync e il ripristino di Proxmox VE HA vengono eseguiti in parallelo.
- Utilizza le regole di affinità dei nodi HA con priorità dei nodi per posizionare le VM sui nodi nello stesso sito del loro storage primario e per consentire il failover sull'altro sito.
- Dopo un failover del sito, imposta la proprietà HA `failback` su 0 per le VM interessate finché non ripristini lo storage. In caso contrario, HA migra di nuovo le VM ai nodi del sito A non appena tornano disponibili, mentre lo storage attivo è ancora nel sito B.
- Assicurati che i timeout del disco del sistema operativo guest siano più lunghi del tempo di failover previsto, in modo che i guest non segnalino errori di I/O durante un failover dello storage.

Integrazione con Storage Manager per Proxmox

Storage Manager for Proxmox (SMP) offre agli amministratori di Proxmox VE un'unica interfaccia per eseguire il provisioning dello storage condiviso ONTAP e per eseguire il backup, il ripristino e la clonazione delle VM utilizzando gli snapshot ONTAP e la tecnologia FlexClone. SMP si connette al cluster Proxmox VE e a ONTAP tramite le rispettive API, quindi non richiede agenti sui nodi Proxmox VE.

SMP e SnapMirror active sync proteggono da diversi tipi di guasti. SnapMirror active sync mantiene le VM in esecuzione anche in caso di guasto dello storage o del sito, ma replica ogni scrittura in modo sincrono, inclusi una cancellazione accidentale, un aggiornamento guest non riuscito o dati crittografati da ransomware. Gli snapshot SMP ti offrono copie point-in-time per il ripristino da questi guasti logici. Insieme, offrono disponibilità continua e un rapido ripristino operativo dallo stesso storage ONTAP.

Livello di protezione	Protegge da	Punto di ripristino	Gestito con
Sincronizzazione attiva SnapMirror	Guasto del sistema di storage e guasto del sito	Nessuna perdita di dati	ONTAP
Backup SMP (snapshot ONTAP)	Cancellazione accidentale, corruzione dei dati, aggiornamenti non riusciti e ransomware	Ultimo backup pianificato o su richiesta	SMP
SnapMirror fan-out asincrono o Proxmox Backup Server	Perdita di entrambi i siti e mantenimento a lungo termine	Ultima replica o backup	ONTAP o Proxmox Backup Server

Backup e ripristino

SMP crea backup coerenti in caso di crash o coerenti a livello di file come snapshot di ONTAP dei volumi di storage, su richiesta o in base a criteri, e ripristina singole VM, storage o gruppi di risorse:

- Utilizza i gruppi di risorse e le policy di backup per applicare la stessa pianificazione e gli stessi criteri di conservazione alle macchine virtuali di un tenant o di un'applicazione.
- Usa backup coerenti a livello di file per le VM che eseguono il guest agent QEMU, in modo che i file system guest vengano messi in quiescenza prima che ONTAP crei lo snapshot.
- SMP gestisce lo storage attivo. Dopo un failover di SnapMirror active sync, esegui un rilevamento in SMP in modo che associ lo storage al cluster B prima di eseguire operazioni di backup o ripristino.
- Per una terza copia al di fuori dei due siti, o per una conservazione più lunga, aggiungi una relazione fan-out asincrona SnapMirror dai volumi protetti oppure utilizza Proxmox Backup Server.
- Gli snapshot a prova di manomissione non sono supportati con SnapMirror active sync, quindi non abilitare il blocco degli snapshot in SMP per i volumi protetti.

Clonazione delle VM

SMP utilizza la tecnologia ONTAP FlexClone per creare cloni di macchine virtuali efficienti in termini di spazio per lo sviluppo, i test e il provisioning rapido. I cloni che crei nello storage protetto consumano larghezza di banda di replica e capacità in entrambi i siti. Escludi dalla protezione di sincronizzazione attiva di SnapMirror i cloni e lo storage di test che non richiedono continuità operativa.

Posizionamento SMP

- Esegui la VM SMP come risorsa HA su uno storage condiviso protetto da SnapMirror active sync, in modo che SMP rimanga disponibile dopo un guasto dello storage o del sito.
- Registra il cluster Proxmox VE e entrambi i cluster ONTAP in SMP, in modo che SMP possa raggiungere lo storage attivo in entrambi i siti.

Storage condiviso NFS con SnapMirror active sync per NAS

A partire da ONTAP 9.19.1, SnapMirror active sync protegge i carichi di lavoro NAS. Le seguenti considerazioni si applicano solo allo storage condiviso NFS. Per implementare la soluzione con storage NFS, segui ["Workflow di configurazione NAS"](#).

Protezione a livello SVM e identità di rete

- SnapMirror active sync per NAS protegge un'intera macchina virtuale di storage (SVM). Puoi proteggere tutti i volumi nella SVM o escludere i volumi selezionati. Sono supportati solo i volumi FlexVol e la SVM non può contenere LUN.
- La SVM secondaria rimane inattiva, con i relativi LIF disattivati, fino a un failover. ONTAP replica la configurazione della SVM, inclusi gli indirizzi IP dei LIF, le policy di esportazione e le impostazioni NFS, in modo che la SVM secondaria presenti lo stesso endpoint NFS dopo un failover.
- Il failover non interrompe il funzionamento per NFSv3 e versioni successive.
- SnapMirror active sync per NAS è di tipo attivo/passivo, quindi le VM sui nodi del sito B leggono e scrivono attraverso la rete intersito verso l'SVM primario. Per i carichi di lavoro attivi in entrambi i siti, usa due SVM con direzioni di replica opposte, una primaria in ciascun sito, e allinea la regola di affinità del nodo di ogni VM al sito del relativo SVM primario.
- SnapMirror active sync per NAS è supportato sui cluster AFF A-Series e C-Series a due nodi.

Impostazioni del client NFS

Utilizza NFSv3 o NFSv4.1 per lo storage NFS. Mantieni il comportamento predefinito di hard mount e non aggiungere l'opzione di montaggio, in modo che le operazioni di I/O NFS vengano ritentate anziché non

riuscire durante un failover.

Usa più connessioni TCP allo storage per prestazioni migliori e una maggiore tolleranza ai guasti. Usa nConnect oppure il trunking di sessione, non entrambi:

- **nConnect.** Apre più connessioni TCP a un singolo indirizzo LIF NFS, ad esempio `nconnect=4`. nConnect funziona con NFSv3 e NFSv4.1 e con un singolo indirizzo LIF VIP, quindi è l'opzione consigliata per SnapMirror active sync per NAS, incluse le reti layer 3.
- **Session trunking.** Raggruppa più LIF di dati in una sessione NFSv4.1, ad esempio `vers=4.1, trunkdiscovery, max_connect=16`. Il session trunking richiede NFSv4.1 o versione successiva. Utilizzalo solo quando la SVM protetta dispone di più LIF di dati raggiungibili dai client in entrambi i siti, come in una rete layer 2 estesa. Per i dettagli, consulta ["Trunking NFS"](#).

Per i comandi delle opzioni di montaggio e i passaggi di verifica, vedi ["Configurare l'archiviazione NFS per Proxmox VE"](#).

Provisioning dello storage NFS con SMP

SMP esegue il provisioning di un volume ONTAP, crea o seleziona una policy di esportazione e monta il volume come storage condiviso NFS sui nodi Proxmox VE che selezioni. Per lo storage in una SVM protetta:

- Esegui il provisioning del volume nella SVM primaria e seleziona la LIF NFS, oppure la LIF VIP in una rete di livello 3, come LIF preferita. La SVM secondaria utilizza lo stesso indirizzo dopo un failover, quindi la definizione dello storage rimane valida.
- Monta lo storage su tutti i nodi Proxmox VE in entrambi i siti in modo che l'HA possa riavviare le VM su qualsiasi nodo.
- Assicurati che la policy di esportazione consenta i nodi Proxmox VE in entrambi i siti. ONTAP replica la policy di esportazione sull'SVM secondario.
- Dopo il provisioning, verifica che il volume sia incluso nella protezione di sincronizzazione attiva di SnapMirror.

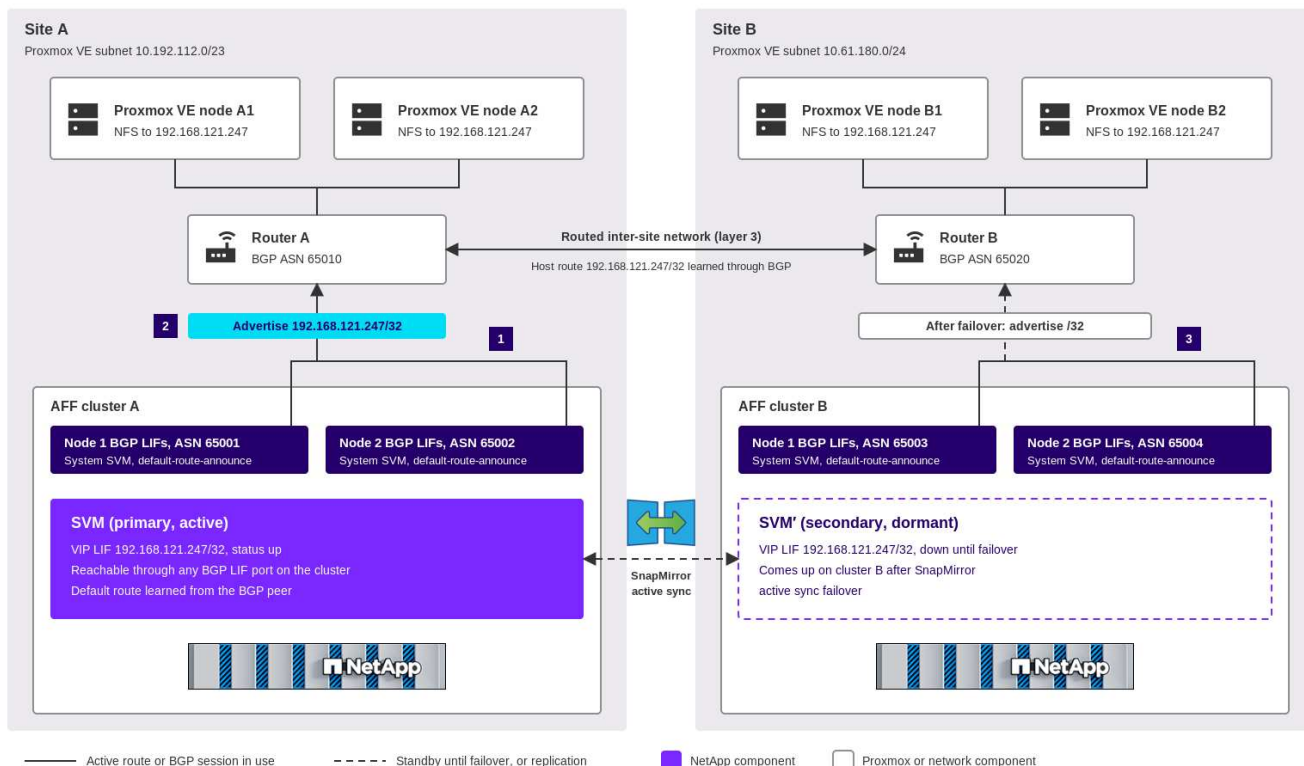
Reti di livello 3 con VIP LIFs e BGP

SnapMirror active sync per NAS richiede lo stesso indirizzo IP sulle SVM primaria e secondaria. Quando la VLAN NFS viene estesa tra i siti, l'indirizzo IP della LIF si sposta con la SVM. Quando i siti sono connessi tramite una rete instradata di livello 3, la sottorete di una LIF del sito A non esiste nel sito B.



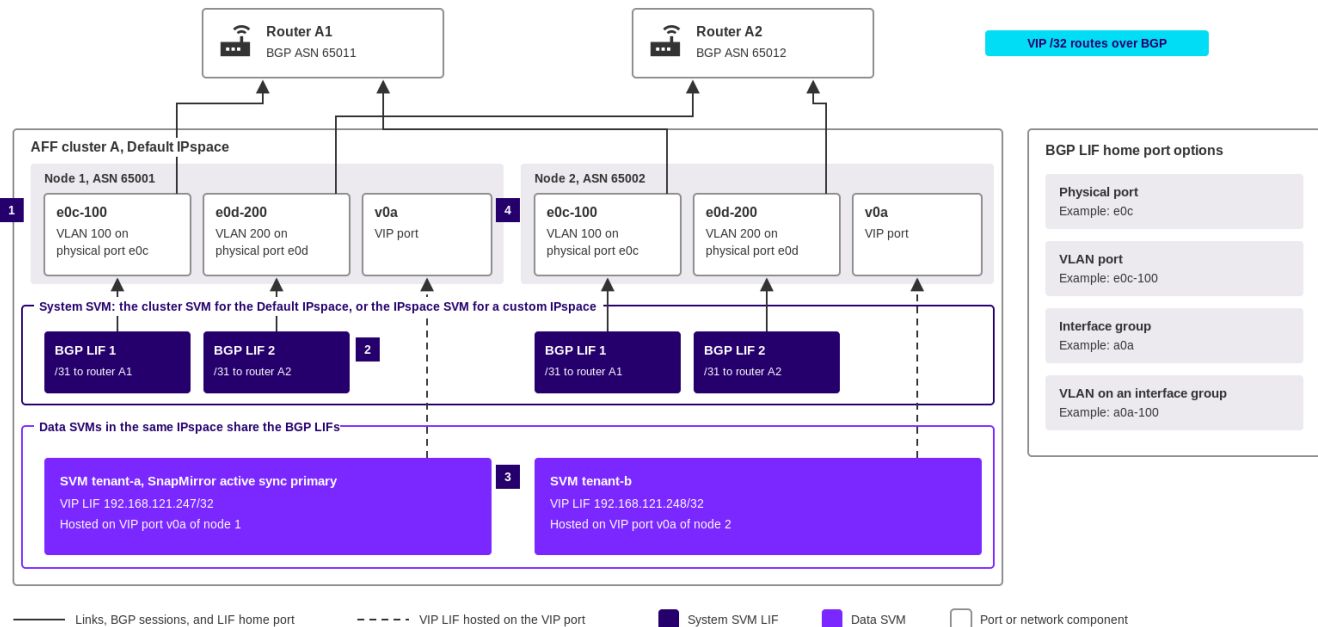
Al momento della pubblicazione, NetApp non ha documentato le VIP LIF con BGP come configurazione qualificata per la sincronizzazione attiva di SnapMirror per NAS. Prima di pianificare una progettazione di livello 3, conferma il supporto attuale con NetApp. In caso contrario, estendi la VLAN NFS tra i siti. Le configurazioni IP di MetroCluster supportano le VIP LIF con BGP.

Le LIF con IP virtuale (VIP) di ONTAP risolvono questo problema. Una LIF VIP non appartiene ad alcuna sottorete. ONTAP pubblicizza l'indirizzo VIP ai router peer come una rotta host /32 utilizzando Border Gateway Protocol (BGP), in modo che l'indirizzo possa spostarsi tra i siti senza una VLAN estesa.



1. Ogni nodo in entrambi i siti dispone di BGP LIF nella SVM di sistema che sono in peering con i router del sito. I BGP LIF sono specifici del nodo e non vengono replicati, quindi devi configurarli su entrambi i cluster.
2. L'SVM primaria ospita la LIF VIP NFS. Il cluster A pubblicizza la rotta host /32 e i nodi Proxmox VE in entrambi i siti raggiungono lo storage attraverso la rete instradata.
3. Dopo un failover di SnapMirror active sync, il VIP LIF si attiva sulla SVM secondaria, il cluster B pubblicizza la route host e i router convergono sul sito B.

Quando pianifichi BGP in ONTAP per la prima volta, è utile sapere quale SVM possiede ciascuna LIF. Le LIF BGP appartengono alla SVM di sistema dell'IPspace, non alle SVM dati. Un set di LIF BGP su ciascun cluster serve le LIF VIP di ogni SVM dati in quell'IPspace, quindi non crei LIF BGP per ogni tenant. Il diagramma seguente mostra il layout di LIF e porte su un cluster, con le LIF BGP sulle porte VLAN.



1. Ogni nodo ha due porte per BGP, in questo esempio le porte VLAN e0c-100 e e0d-200. Ogni porta si connette direttamente a un router diverso.
2. Ogni nodo ha due BGP LIF nell'SVM di sistema, una su ciascuna porta, con una sottorete /31 e un gruppo peer BGP verso un router. Per l'IPspace predefinito, l'SVM di sistema è la cluster SVM. Per un IPspace personalizzato, è l'SVM con lo stesso nome dell'IPspace.
3. Le SVM di dati nello stesso IPspace ospitano VIP LIFs e non richiedono BGP LIFs proprie. I gruppi di peer BGP pubblicizzano le route VIP per tutte le SVM nell'IPspace.
4. ONTAP crea una porta VIP, ad esempio v0a, su ciascun nodo quando crei il primo gruppo di peer BGP. Le LIF VIP sono ospitate sulla porta VIP e sono raggiungibili tramite ogni porta del nodo che ospita una LIF BGP nell'IPspace.

La porta home di un BGP LIF può essere una porta fisica, una porta VLAN, un gruppo di interfacce o una VLAN su un gruppo di interfacce. Un gruppo di interfacce non è obbligatorio. NetApp Technical Report TR-4949 raccomanda due BGP LIF su due porte separate per ogni IPspace, ciascuna connessa direttamente a un router first-hop diverso.

Tenete presenti le seguenti linee guida:

- Le BGP LIF non sono soggette a failover. La ridondanza deriva da due BGP LIF per nodo, ognuna in peering con un router diverso. Se un nodo perde tutte le sessioni BGP per una SVM, ONTAP sposta la VIP LIF su un altro nodo che ha una sessione BGP attiva per quella SVM.
- Usa il protocollo BGP esterno (eBGP) con un numero di sistema autonomo privato (ASN) univoco per ogni nodo ONTAP e per ogni router.
- Usa una sottorete /31 (maschera di sottorete 255.255.255.254) per ogni BGP LIF e il relativo router. Assegna l'indirizzo dispari al BGP LIF e l'indirizzo pari al router.
- ONTAP non elabora le rotte provenienti dai router. Configura i router in modo che accettino le rotte host /32 da ONTAP e non inviino aggiornamenti di rotta al cluster.
- I nodi Proxmox VE non devono condividere una subnet con l'indirizzo VIP. Un router di livello 3 ridondante, ad esempio con VRRP o HSRP, deve trovarsi nel percorso tra i nodi e lo storage.
- Configura i gruppi peer BGP con `-use-peer-as-next-hop true` in modo che ogni cluster apprenda la

propria rotta predefinita dai router locali. Le rotte che puntano al gateway del sito A non sono valide nel sito B dopo un failover.

- Abilita il routing multipath in modo che il traffico VIP in uscita utilizzi tutte le porte LIF BGP disponibili.
- Riduci il tempo di hold BGP dal valore predefinito di 180 secondi. TR-4949 raccomanda un tempo di hold di 3 secondi. Un router ritira la route da un cluster guasto solo quando scade il timer di hold e, durante un guasto del sistema storage, il router nel sito A rimane online.

Informazioni correlate

- ["Architettura di ONTAP SnapMirror active sync"](#)
- ["Prerequisiti per la sincronizzazione attiva di ONTAP SnapMirror"](#)
- ["Preparati a configurare ONTAP Cloud Mediator"](#)
- ["Configura ONTAP Cloud Mediator per SnapMirror active sync"](#)
- ["Considerazioni su ONTAP MetroCluster per IP virtuale e BGP"](#)
- ["MetroCluster protezione dei dati e ripristino di emergenza"](#)
- ["Configurare e utilizzare Storage Manager per Proxmox"](#)
- ["TR-4949: BGP/VIP con ONTAP nel Datacenter"](#)
- ["cluster manager Proxmox VE"](#)
- ["Proxmox VE ad alta disponibilità"](#)

Configura la continuità operativa di Proxmox VE con storage NAS

Proteggi le VM di Proxmox Virtual Environment (VE) da un guasto del sito combinando ONTAP SnapMirror active sync per NAS con un cluster esteso di Proxmox VE. Configuri un mediatore, ONTAP Mediator oppure ONTAP Cloud Mediator in NetApp Console, proteggi la storage VM (SVM) NFS, opzionalmente rendi il suo indirizzo NFS portabile attraverso una rete instradata con una LIF con IP virtuale (VIP) e Border Gateway Protocol (BGP), crei il cluster esteso con un QDevice e poi esegui il provisioning dello storage condiviso e configuri l'alta disponibilità (HA) e i backup delle VM con Storage Manager for Proxmox. Il risultato è zero perdita di dati e il ripristino automatico delle VM nel sito superstite.

Informazioni su questo flusso di lavoro

Prima di iniziare, rivedi ["Architettura della soluzione, comportamento in caso di guasto e considerazioni sulla progettazione di corosync"](#). Sostituisci i valori tra parentesi angolari, come `<primary_svm>`, con i valori relativi al tuo ambiente.

Prima di iniziare

- Due cluster AFF A-Series o C-Series a due nodi devono eseguire ONTAP 9.19.1 o versione successiva, uno nel sito A e uno nel sito B.
- SnapMirror e le licenze sincrone di SnapMirror, incluse in ONTAP One, devono essere installate su entrambi i cluster.
- I cluster devono essere collegati tramite peering nell'IPspace predefinito, con un tempo di andata e ritorno

inter-cluster (RTT) inferiore a 10 ms.

- Devi scegliere un'opzione di mediazione. Per un confronto, vedi ["Opzioni del mediatore"](#).
 - Per ONTAP Mediator, devi installare un host Linux nel sito C o in un altro terzo dominio di guasto e renderlo raggiungibile dalle LIF di gestione del cluster e dei nodi di entrambi i cluster.
 - Per ONTAP Cloud Mediator, entrambi i cluster devono avere accesso HTTPS outbound a NetApp Console, direttamente o tramite un proxy, con una latenza inferiore a 200 ms. Hai inoltre bisogno di un'organizzazione NetApp Console e dell'autorizzazione per creare un account di servizio.
- Un SVM nel sito A deve fornire NFS ai nodi Proxmox VE. L'SVM deve contenere solo volumi FlexVol per NAS, senza LUN, e la sua policy di esportazione deve consentire l'accesso a tutti i nodi Proxmox VE.
- Devi installare un numero pari di nodi Proxmox VE 9.0 o versioni successive, equamente suddivisi tra il sito A e il sito B, con una latenza corosync inferiore a 5 ms tra tutti i nodi.
- Un host Linux presso il sito C, o presso un'altra terza sede, deve essere disponibile per il demone corosync QDevice e raggiungibile da tutti i nodi Proxmox VE sulla porta TCP 5403. Ti serve questo host con una delle due opzioni del mediatore.
- La VLAN NFS deve essere estesa tra il sito A e il sito B. Per una rete instradata di livello 3, deve essere disponibile un router compatibile con BGP in ciascun sito e devi confermare con NetApp che le VIP LIF con BGP siano supportate con SnapMirror active sync per NAS.
- Le tue versioni di ONTAP e Proxmox VE devono essere elencate insieme in ["NetApp Interoperability Matrix Tool \(IMT\)"](#).
- Per configurare lo storage condiviso ed eseguire il backup delle macchine virtuali, Storage Manager per Proxmox deve essere installato con accesso di rete ai nodi Proxmox VE e a entrambi i cluster ONTAP.

Passaggio 1: Configura il mediatore

Aggiungi un mediatore alla cluster peer relationship prima di inizializzare la relazione di sincronizzazione attiva SnapMirror. ONTAP necessita del mediatore per eseguire i failover pianificati e automatici. Puoi aggiungere il mediatore da uno dei due cluster e ONTAP lo aggiunge automaticamente all'altro cluster. Utilizza una sola opzione per il mediatore, non entrambe.

Scegli una delle seguenti opzioni.

ONTAP Mediator

Usa questa opzione se installi il mediatore su un host Linux nel sito C. Per l'installazione, vedi ["Installa o aggiorna ONTAP Mediator"](#).

Passi

1. Su entrambi i cluster, aggiungi il mediatore:

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

Inserisci la password del mediatore quando richiesto.

2. Verifica che il mediatore sia connesso e che lo stato del quorum sia true:

```
snapmirror mediator show
```

ONTAP Cloud Mediator

Usa questa opzione per ospitare il mediatore come servizio in NetApp Console, in modo da non aver bisogno di un host del mediatore in un terzo sito.

Prima di iniziare

- I firewall di entrambi i siti devono consentire il traffico HTTPS da entrambi i cluster all'endpoint API di NetApp Console. Per il nome host dell'endpoint corrente, vedi "[Preparati a configurare ONTAP Cloud Mediator](#)".
- Se i cluster utilizzano proxy server, tieni a disposizione l'indirizzo IP del proxy, la porta e le credenziali. Usa un proxy server diverso per ciascun cluster. Il certificato CA root del proxy deve essere installato in ONTAP.
- ONTAP include certificati CA radice noti, quindi in genere non devi installare il certificato NetApp Console. Per verificarlo, esegui `security certificate show -common-name Sectigo*|USERTrust*|AAA*`.

Passi

1. Nella NetApp Console, copia l'ID della tua organizzazione.
2. Nella NetApp Console, crea un account di servizio membro:
 - a. Imposta l'organizzazione su quella in cui utilizzi ONTAP Cloud Mediator.
 - b. Imposta la categoria su **Application**.
 - c. Imposta il ruolo su **ONTAP Mediator Setup Role**.
 - d. Salva il client ID e il client secret quando crei l'account.
3. Su entrambi i cluster, aggiungi il mediatore:

```
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>
```

Inserisci il client secret quando richiesto.

Puoi anche usare System Manager. Seleziona **Protection > Overview > Mediator > Add**, seleziona **Cloud** come tipo di mediatore e inserisci organization ID, client ID e client secret.

4. Verifica che il tipo di mediatore sia `cloud`, lo stato della connessione sia `connected` e lo stato del quorum sia `true`:

```
snapmirror mediator show
```

Passaggio 2: Proteggi la SVM NFS con SnapMirror active sync

Crea una SVM di destinazione inattiva sul cluster del sito B e replica su di essa la SVM del sito A. ONTAP replica i dati in modo sincrono e replica la configurazione della SVM, inclusi gli indirizzi LIF NFS e le policy di esportazione. Puoi anche completare questo passaggio in System Manager selezionando **Protect** per la SVM e scegliendo la policy `AutomatedFailOver`.

Passi

1. Sul cluster del sito B, crea la SVM di destinazione:

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

2. Sul cluster del sito B, crea una relazione peer SVM con l'SVM primario:

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

3. Sul cluster del sito A, accetta la richiesta di peering dell'SVM:

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

4. Sul cluster del sito B, crea la relazione di sincronizzazione attiva di SnapMirror:

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

5. Inizializza la relazione:

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

6. Verifica che la relazione sia sincronizzata:

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

Il Mirror State è Snapmirrored, e il Relationship Status è InSync.

7. Facoltativamente, escludi i volumi che non necessitano di protezione, come i volumi scratch o di test:

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

Passaggio 3: Configura un VIP LIF con BGP per le reti di livello 3



Al momento della pubblicazione, NetApp non ha documentato le VIP LIF con BGP come configurazione qualificata per la sincronizzazione attiva di SnapMirror per NAS. Conferma il supporto attuale con NetApp prima di completare questo passaggio. In caso contrario, estendi la VLAN NFS tra i siti e salta questo passaggio.

Se la VLAN NFS è estesa tra il sito A e il sito B, salta questo passaggio. Se i siti sono connessi tramite una rete con routing, crea LIF BGP su ogni nodo di entrambi i cluster e quindi ospita l'indirizzo NFS su una LIF VIP nell'SVM primario. L'indirizzo VIP non deve appartenere alla sottorete dei nodi Proxmox VE.

Prima di iniziare

- Ciascun router deve essere configurato per accettare una sessione BGP dalle LIF BGP presenti nel suo sito, per accettare le route host /32 e per non inviare aggiornamenti di route a ONTAP.
- Ogni nodo ONTAP e ogni router devono avere un ASN privato univoco e ogni coppia di LIF BGP e router deve avere una sottorete /31.

Passi

1. Su ciascun cluster, passa al livello di privilegio avanzato:

```
set -privilege advanced
```

2. Su ciascun nodo di entrambi i cluster, crea una configurazione BGP con un ASN ONTAP univoco per il nodo, un hold time di 3 secondi e l'indirizzo IP di gestione del nodo come ID del router:

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

3. Facoltativamente, su ciascun nodo di entrambi i cluster, crea una porta VLAN su ciascuna delle due porte che si connettono ai router:

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

Puoi anche utilizzare porte fisiche, gruppi di interfacce o VLAN su gruppi di interfacce come porte home di BGP LIF. Le porte devono appartenere a un dominio di broadcast nell'IPspace.

4. Su ciascun nodo di entrambi i cluster, crea due LIF BGP nell'SVM di sistema, una per ogni porta, con una sottorete /31 verso il router su quella porta:

```
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
```

Per l'IPspace predefinito, `<system\_svm>` è il nome del cluster. Per un IPspace personalizzato, è il nome

dell'IPspace. Crei le LIF BGP una volta per ogni nodo e queste gestiscono le LIF VIP di tutti gli SVM di dati nell'IPspace.

5. Per ogni LIF BGP, crea un gruppo di peer BGP con il relativo router e apprendi la rotta predefinita da quel 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. Verifica che ogni gruppo peer sia attivo:

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

7. Su ciascun cluster, abilita il routing multipath:

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

8. Nel cluster del sito A, crea la LIF VIP NFS nella SVM primaria:

```
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. Sul cluster del sito A, verifica che lo stato BGP sia up per l'SVM primaria su ogni nodo:

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

10. Su entrambi i router, verifica che la rotta /32 per l'indirizzo VIP venga appresa dal cluster A.

Passaggio 4: Crea il Proxmox VE stretch cluster con un QDevice

Crea il cluster da un nodo del sito A in modo che i nodi del sito A ricevano gli ID dei nodi più bassi e aggiungi un QDevice al sito C. Il QDevice assegna il voto al sito A quando il collegamento tra i siti si interrompe, in linea con la SVM che ONTAP mantiene attiva.

Passi

1. Sul primo nodo del sito A, crea il cluster con due collegamenti corosync su reti separate:

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

2. Su ciascun nodo A rimanente e poi su ciascun nodo B, unisciti al cluster:

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

3. Verifica che i nodi del sito A abbiano gli ID nodo più bassi:

```
pvecm nodes
```

4. Sul server host QDevice nel sito C o in un'altra terza posizione, installa il demone QDevice:

```
apt install corosync-qnetd
```

5. Su ogni nodo Proxmox VE, installa il client QDevice:

```
apt install corosync-qdevice
```

6. Su un nodo Proxmox VE, aggiungi il QDevice al cluster:

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

7. Verifica che il cluster sia in quorum con il voto del QDevice:

```
pvecm status
```

Per un cluster a quattro nodi, Expected votes`è `5, Quorum`è `3, e Flags includono Quorate Qdevice.

Passaggio 5: Esegui il provisioning dello storage condiviso NFS protetto

Esegui il provisioning dello storage NFS nell'SVM primario e montalo su tutti i nodi Proxmox VE in entrambi i siti, utilizzando l'indirizzo NFS LIF o VIP condiviso da entrambe le SVM. Storage Manager for Proxmox (SMP) crea il volume ONTAP, la policy di esportazione e la definizione dello storage Proxmox VE in un unico flusso di lavoro. Se non utilizzi SMP, crea il volume in ONTAP e aggiungilo come storage NFS tramite la CLI di Proxmox VE.

Scegli uno dei seguenti metodi per predisporre lo storage.

Storage Manager per Proxmox

Usa SMP per il provisioning dello storage. SMP deve essere installato, con il cluster Proxmox VE e entrambi i cluster ONTAP aggiunti come piani. Per i dettagli, vedi ["Configurare e utilizzare Storage Manager per Proxmox"](#).

1. In SMP, seleziona **Provision > Add Volume**, quindi seleziona **NFS**.
2. In **ONTAP Details**, seleziona la SVM primaria, inserisci il nome e la dimensione del volume e seleziona la NFS LIF o la VIP LIF come LIF preferita.
3. Seleziona una policy di esportazione che consenta i nodi Proxmox VE in entrambi i siti, oppure creane una.
4. In **Dettagli Proxmox**, seleziona il cluster e tutti i nodi in entrambi i siti, seleziona NFS v3 o NFS v4.1 e seleziona i tipi di contenuto.
5. Assicurati che **Mount the datastore** sia selezionato, quindi seleziona **Provision**.
6. Sul cluster del sito A, verifica che il volume sia incluso nella protezione active sync di SnapMirror:

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

CLI

Utilizza la CLI di Proxmox VE per aggiungere un volume già presente nell'SVM primario come storage NFS.

1. Su un nodo Proxmox VE, aggiungi lo storage NFS:

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

Usa 3 o 4.1 per <nfs_version>. Non aggiungere l' `soft` opzione di mount.

2. Verifica che lo storage sia attivo su ogni nodo:

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

Imposta le opzioni di montaggio NFS

Usa nConnect per aprire più connessioni TCP verso l'indirizzo NFS LIF o VIP per ottenere prestazioni migliori e una maggiore tolleranza ai guasti. Se l'SVM protetta dispone di più LIF dati che i client possono raggiungere in entrambi i siti, puoi invece usare il trunking di sessione NFSv4.1. Usa nConnect oppure il trunking di sessione, non entrambi. Per i dettagli, vedi ["Configurare l'archiviazione NFS per Proxmox VE"](#).

Passi

1. Se hai configurato lo storage con SMP o senza nConnect, imposta le opzioni di montaggio su un nodo Proxmox VE:

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

Per utilizzare invece il trunking di sessione, imposta:

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

Proxmox VE applica nuove opzioni di montaggio al successivo montaggio dello storage. Rimonta lo storage su ciascun nodo durante una finestra di manutenzione, dopo aver migrato le VM da quel nodo.

2. Verifica le opzioni in `/etc/pve/storage.cfg`.
3. Su ciascun nodo Proxmox VE, verifica che siano presenti più connessioni all'indirizzo del server NFS:

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

Passaggio 6: Configura HA e i backup delle VM

Aggiungi le VM all'HA con regole di affinità dei nodi che privilegiano il sito A, dove la SVM primaria gestisce i dati. Quindi proteggi le VM da guasti logici, come l'eliminazione accidentale o il ransomware, con policy di backup SMP. SnapMirror active sync replica questi guasti in modo sincrono, quindi non sostituisce i backup point-in-time.

Passi

1. Aggiungi ogni VM protetta a HA:

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

2. Crea una regola di affinità dei nodi che dia la preferenza ai nodi del sito A e consenta il failover ai nodi del sito B:

```
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. Facoltativamente, puoi aumentare il timeout del disco in ciascun sistema operativo guest in modo che sia più lungo del tempo di failover dello storage previsto.
4. In SMP, seleziona **Proteggi > Backup > Gruppo di risorse** e crea un gruppo di risorse per le VM o lo storage di ciascun tenant o applicazione.
5. Seleziona **Proteggi > Backup > Criteri > Aggiungi**, e crea un criterio con la frequenza di backup e la conservazione per il gruppo di risorse.

Seleziona **Coerenza VM** in **Opzioni avanzate** per le macchine virtuali che eseguono QEMU guest agent.

6. Esegui un backup su richiesta, quindi ripristina una VM di test per verificare la policy.

Passaggio 7: Verifica del failover pianificato

Convalida la progettazione prima di posizionare le VM di produzione sullo storage condiviso. Un failover pianificato sposta la SVM attiva nel sito B senza perdita di dati, così puoi testarla durante una finestra di manutenzione e tornare indietro in seguito.

Passi

1. Esegui la migrazione live delle VM di test ai nodi del sito B.
2. Prima del failover, impedisce che l'HA sposti di nuovo le VM sui nodi del sito A:

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

3. Sul cluster del sito B, avvia un failover pianificato:

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

4. Monitora il failover fino al completamento:

```
snapmirror failover show
```

5. Verifica che l'I/O delle VM continui e che lo storage rimanga attivo su tutti i nodi Proxmox VE.
6. Se utilizzi un VIP LIF, verifica che entrambi i router apprendano la route /32 dal cluster B.
7. In SMP, esegui un rilevamento per i piani ONTAP, quindi esegui un backup on-demand per verificare che SMP protegga le VM dalla SVM nel sito B.
8. Al termine del test, torna al sito A e poi imposta `failback` di nuovo su 1 per le VM di test.

Risultato

Le macchine virtuali Proxmox VE continuano a funzionare sullo stesso storage condiviso NFS mentre la SVM attiva si sposta tra i siti e il cluster si ripristina automaticamente in caso di guasto imprevisto di un sito.

Informazioni correlate

- ["Proteggi con ONTAP SnapMirror active sync per NAS"](#)
- ["Configura le LIF VIP di ONTAP"](#)
- ["Preparati a installare ONTAP Mediator"](#)
- ["Preparati a configurare ONTAP Cloud Mediator"](#)
- ["Configura ONTAP Cloud Mediator per SnapMirror active sync"](#)
- ["snapmirror mediator add"](#)
- ["Configurare l'archiviazione NFS per Proxmox VE"](#)
- ["Supporto del voto esterno corosync di Proxmox VE"](#)

Configurare e utilizzare Storage Manager per Proxmox

Storage Manager for Proxmox (SMP) offre provisioning dello storage e gestione del ciclo di vita completi per le macchine virtuali negli ambienti Proxmox che utilizzano sistemi storage NetApp ONTAP. SMP consente agli amministratori di gestire lo storage direttamente, semplificando le operazioni grazie a funzionalità automatizzate di

provisioning, backup, ripristino e clonazione.

Scopri Storage Manager per Proxmox

Storage Manager for Proxmox (SMP) offre una gestione end-to-end dello storage per le macchine virtuali all'interno degli ambienti Proxmox che utilizzano NetApp storage systems. Consentendo agli amministratori di gestire direttamente lo storage, SMP semplifica sia le attività di gestione dello storage che quelle di gestione dei dati negli ambienti Proxmox.

Caratteristiche principali

- **Gestione completa dello storage:** SMP offre una gestione completa del ciclo di vita delle macchine virtuali, dal provisioning dello storage al backup e al ripristino.
- **Gestione diretta dello storage:** gli amministratori di Proxmox possono gestire lo storage direttamente, semplificando le operazioni e riducendo la complessità.
- **Programma di installazione autonomo:** SMP viene fornito come programma di installazione autonomo che si connette senza problemi ai nodi Proxmox tramite API.

Capacità

Ogni componente di SMP è progettato per migliorare l'efficienza della gestione dello storage:

- **Provisioning dello storage:** Assegna e gestisci facilmente risorse di storage per gli host Proxmox e le macchine virtuali associate.
 - **Provisioning dello storage NFS:** Configura e imposta lo storage NFS di ONTAP da utilizzare con il tuo ambiente Proxmox.
 - **iSCSI provisioning dello storage:** Implementare LVM thick con multipath per una gestione dello storage iSCSI robusta ed efficiente.
- **Backup e ripristino:** Esegui backup affidabili e ripristini rapidi per garantire l'integrità e la disponibilità dei dati.
 - **Backup coerenti con gli arresti anomali e con i file:** Garantisci l'integrità dei dati configurando meccanismi di backup sia coerenti con gli arresti anomali che con i file.
 - **Operazioni di ripristino delle macchine virtuali:** Esegui i processi di ripristino delle macchine virtuali per recuperare i dati e mantenere la disponibilità del sistema.
- **Efficienza dello storage:** ONTAP offre una suite completa di tecnologie per l'efficienza dello storage, progettate per ridurre al minimo lo storage necessario per i dati. Queste tecnologie non solo riducono il consumo di storage, ma migliorano anche le prestazioni del sistema, offrendo:
 - **Provisioning rapido delle macchine virtuali:** Semplifica il provisioning delle macchine virtuali per una distribuzione più rapida.
 - **Copie dei dataset più rapide:** velocizza la duplicazione dei dataset per una gestione efficiente dei dati.

Prerequisiti

Assicurati di aver completato i seguenti passaggi prima di procedere:

- Cluster Proxmox Virtual Environment (PVE) 9.x o versione successiva funzionante.
- Storage ONTAP All Flash FAS (AFF) con protocollo NFS e iSCSI abilitati a livello SVM. Per istruzioni, vedere ["Configura i datastore NFS con ONTAP"](#) e ["Configurare Proxmox VE 9.x per iSCSI con storage"](#)

ONTAP".

Per la configurazione di una LUN iSCSI, è necessario abilitare quanto segue:

Installare multipath e iSCSI su tutti gli host Proxmox:

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

Configura iSCSI initiator e connettiti tramite iSCSI (sugli host Proxmox):

Crea o aggiorna /etc/multipath.conf:



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

Oppure usa:

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

- Gli host Proxmox e lo storage ONTAP sono raggiungibili in rete dall'host SMP.

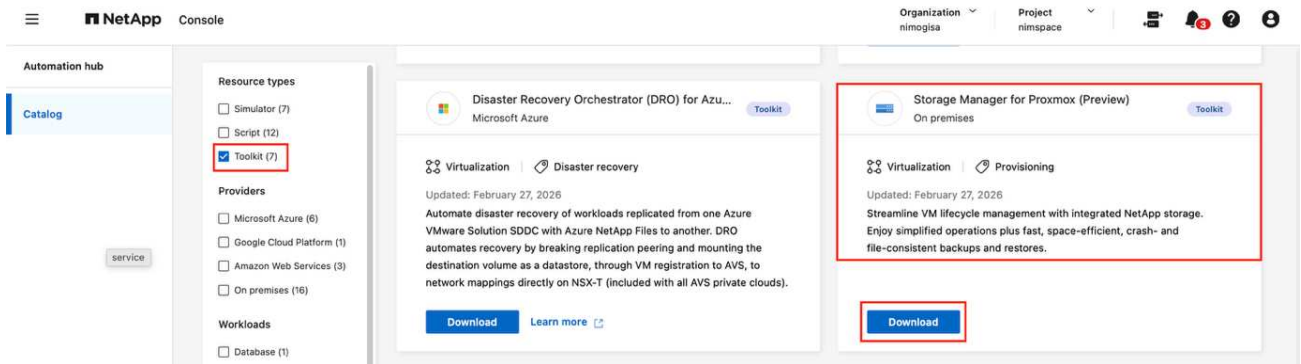
Installare e configurare Storage Manager per Proxmox

Per iniziare a utilizzare SMP, è necessario un sistema operativo Windows su una macchina virtuale dedicata. SMP può essere eseguito su Windows Server 2019, 2022 e 2025.

Passi

1. Scarica il pacchetto SMP (~17MB) da ["Hub di automazione NetApp Console"](#).

▼ **Visualizza la pagina di download di SMP**

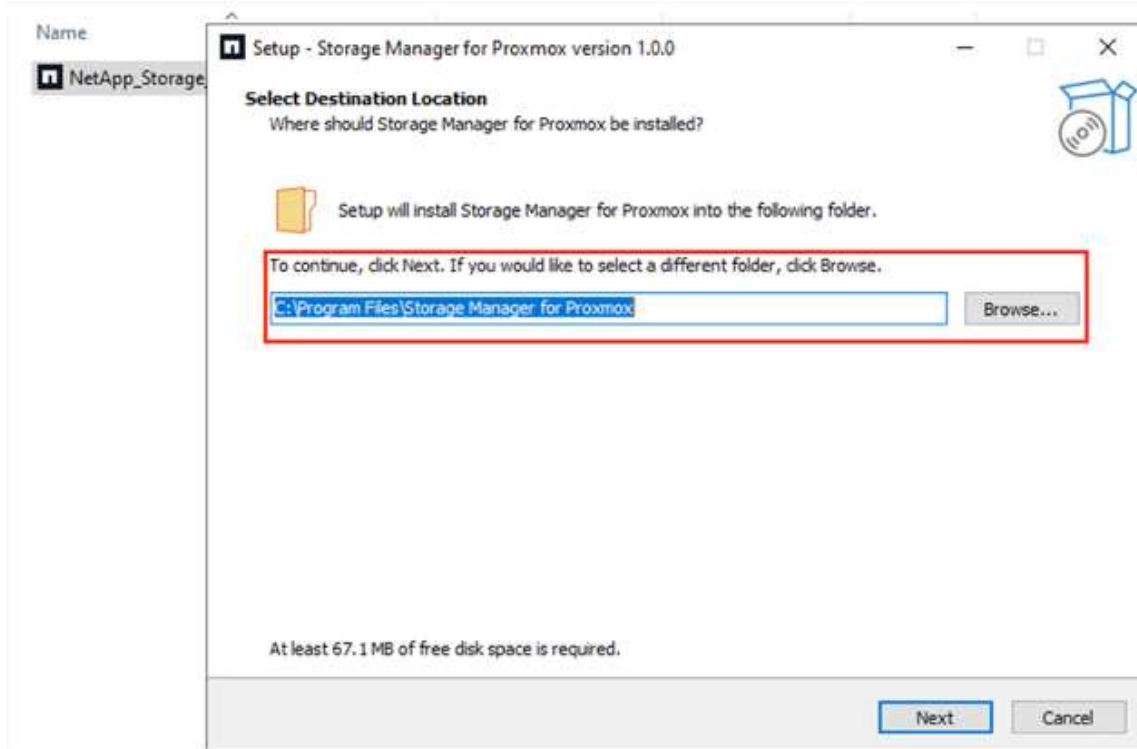


2. Decomprimi il pacchetto.
3. Eseguire il file eseguibile per installare e avviare il servizio.



Non sono necessarie dipendenze da pacchetti aggiuntivi perché SMP sfrutta le API disponibili per orchestrare i flussi di lavoro di provisioning e protezione dei dati.

▼ Visualizza la procedura guidata di installazione di SMP



Installazione alternativa tramite Shift toolkit

In alternativa al programma di installazione autonomo, è possibile installare Proxmox VE Storage Manager utilizzando Shift toolkit:

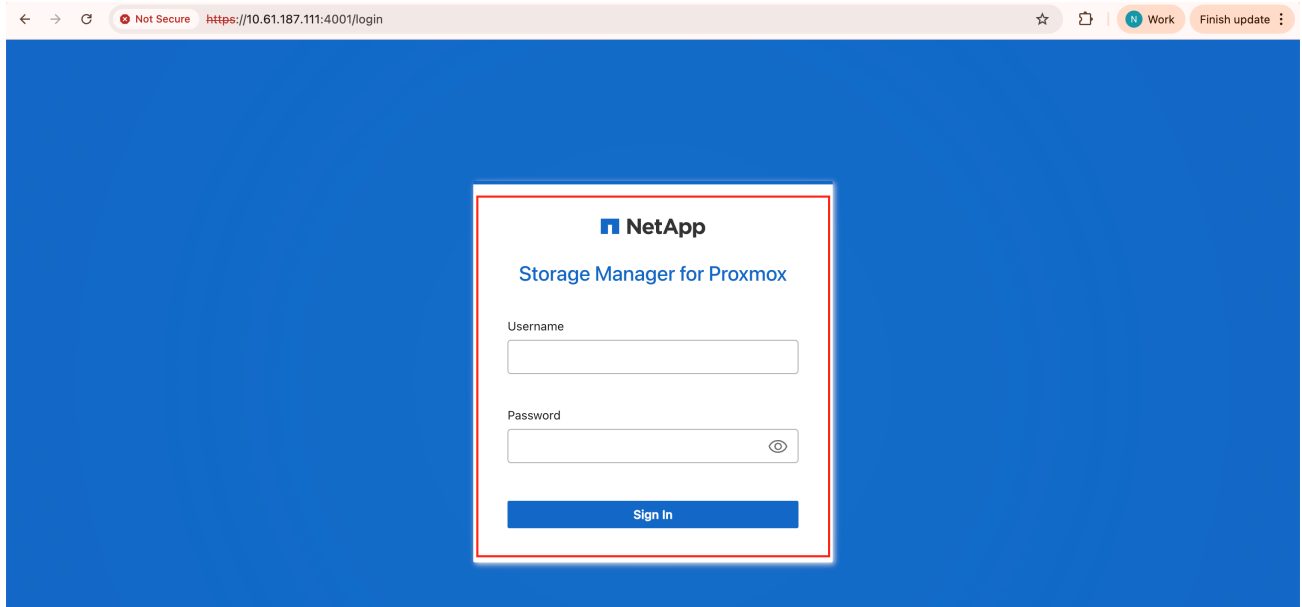
- Open Shift Toolkit.
- Accedere a **Impostazioni > Avanzate > Gestione archiviazione**.
- Attiva Proxmox VE tramite l'interruttore.
- Attendi che il sistema installi automaticamente i componenti necessari.
- Al termine dell'installazione, accedi a Storage Manager facendo clic su **Visualizza** oppure aprendo un

browser web per `https://<Shift_server_IP>:4001`

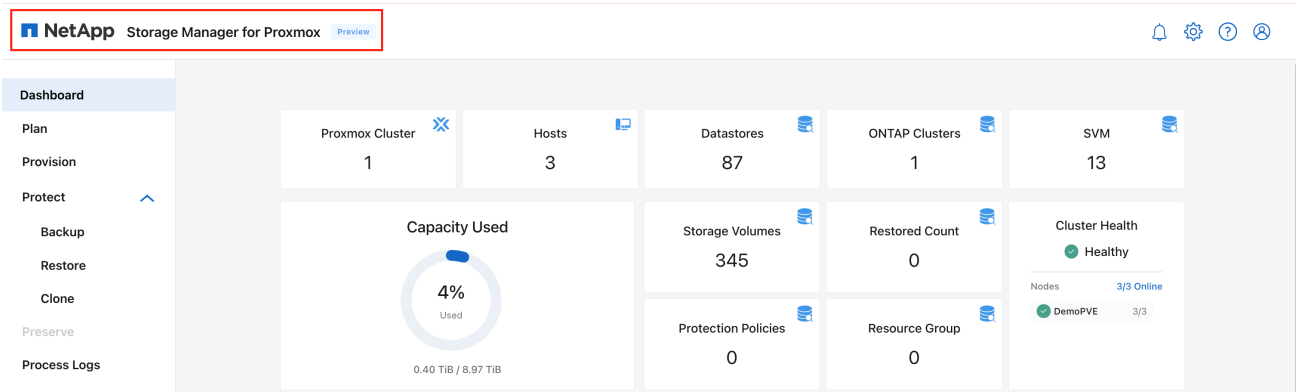
Ad esempio: `https://10.61.187.117:4001`

4. Apri un browser web e accedi all'interfaccia utente SMP inserendo `http://<IP address specified during installation>:4001`

▼ Visualizza la schermata di accesso SMP



▼ Visualizza la schermata iniziale di SMP



Configurare Storage Manager per Proxmox

Una volta configurati correttamente lo storage e la connettività sia ai nodi di storage che ai nodi Proxmox, configura SMP per automatizzare il provisioning e la protezione delle macchine virtuali sfruttando le funzionalità ONTAP Snapshot e FlexClone.

Il primo passo consiste nell'individuare e aggiungere l'endpoint di storage ONTAP e poi i nodi Proxmox di destinazione all'SMP.

Prima di iniziare

Assicurarsi che siano soddisfatti i seguenti prerequisiti:

- SMP è installato

- L'istanza SMP dispone di connettività ai nodi Proxmox e ai sistemi storage
- ONTAP cluster per fornire pool di storage NFS o iSCSI
- La risoluzione DNS è attiva quando si utilizzano i nomi DNS. In caso contrario, utilizzare gli indirizzi IP per l'individuazione.
- L'ambiente dispone di versioni supportate dei server Proxmox Virtual Environment

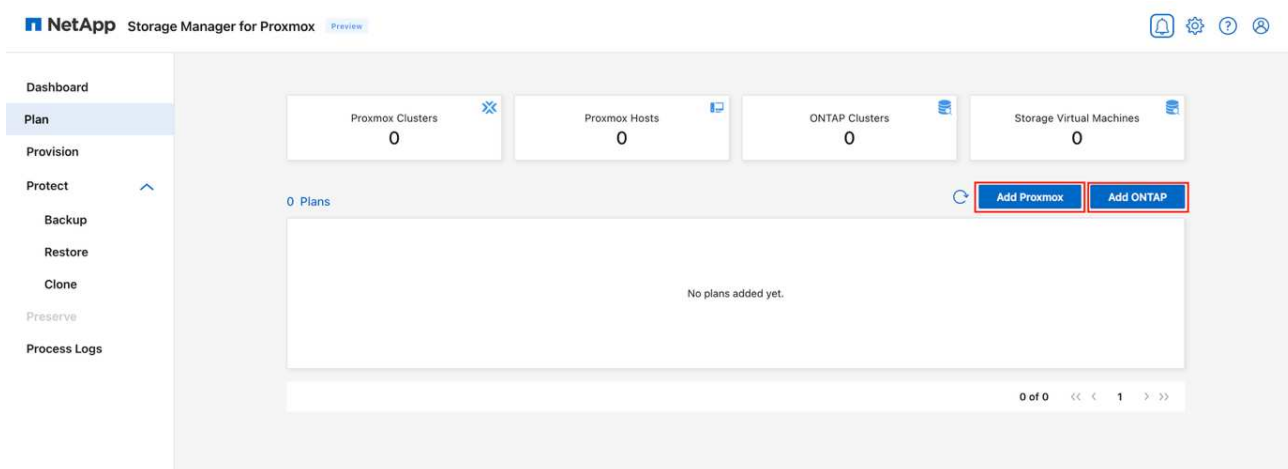
Informazioni su questa attività

Una volta stabilita la connettività tra l'hypervisor e lo storage, la configurazione richiede un paio di clic e circa 2 minuti.

Passi

1. Accedi a SMP.
2. Dal menu di navigazione a sinistra di SMP, selezionare **Plan**.
3. Fai clic su **Aggiungi piano**.

▼ Visualizza Aggiungi piano



4. Fare clic su **Aggiungi ONTAP** per aggiungere le credenziali di un sistema storage ONTAP.

È possibile aggiungere ONTAP utilizzando l'endpoint del cluster o il LIF di gestione SVM.

5. Per aggiungere utilizzando il cluster endpoint, fornire i seguenti dettagli:
 - a. Indirizzo IP del cluster o FQDN
 - b. Nome utente per accedere al cluster ONTAP
 - c. Password per accedere al cluster ONTAP
 - d. Seleziona **Accetta certificato autofirmato** e fai clic su **Aggiungi storage cluster**

▼ Visualizza Aggiungi ONTAP: cluster endpoint

NetApp Storage Manager for Proxmox

Dashboard

Plan

Provision

Protect

Backup

Restore

Clone

Preserve

Process Logs

ONTAP Cluster Details

Connection Type

Cluster

SVM

Connect to cluster management IP to access all SVMs

Cluster Name

SMPProxClus

Cluster Management IP

10.192.102.41

Admin Username

admin

Password

Accept self-signed certificates

Cancel Add Storage Cluster

6. Per aggiungere utilizzando il LIF di gestione SVM, fornire i seguenti dettagli:
 - a. LIF o FQDN di gestione SVM
 - b. Nome utente per accedere alla SVM
 - c. Password per accedere all'SVM
 - d. Seleziona **Accetta certificato autofirmato** e fai clic su **Aggiungi storage cluster**

▼ Visualizza Aggiungi ONTAP: SVM management LIF

NetApp Storage Manager for Proxmox

Dashboard

Plan

Provision

Protect

Backup

Restore

Clone

Preserve

Process Logs

ONTAP SVM Details

Connection Type

Cluster

SVM

Connect directly to a single SVM using its management LIF

SVM Name

SMPProxSVM

SVM Management LIF IP

10.61.187.155

Admin Username

vasadmin

Password

Accept self-signed certificates

Cancel Add Storage SVM

7. Fai clic su **Aggiungi Proxmox** per aggiungere le credenziali di un nodo Proxmox da registrare con SMP.

Per aggiungere nodi Proxmox, specificare l'indirizzo IP di uno dei nodi Proxmox esistenti. Il processo di rilevamento interroga automaticamente il cluster per raccogliere tutti i dettagli di configurazione essenziali.

8. Fornire i seguenti dettagli:

- Indirizzo IP o FQDN autonomo di Proxmox
- Nome utente per accedere a Proxmox
- Password per accedere all'host Proxmox per eseguire l'inventario delle risorse
- Seleziona **Accetta certificato autofirmato** e fai clic su **Continua**

▼ Visualizza Aggiungi Proxmox: credenziali del nodo

NetApp Storage Manager for Proxmox

Proxmox Details

Node

Plan Name
SMPProxmox-Username

Proxmox Endpoint
10.193.172.225

Authentication Method
☒ Username / Password ☐ API Token

Proxmox Username
root

Proxmox Password
NetApp123

☒ Accept self-signed certificates

Cancel Add Site

In alternativa, è possibile utilizzare un token API per accedere alle API fornendo:

- ID token API
- segreto del token API



In questa versione, il token API è consentito solo per le operazioni NFS.

▼ Visualizza Aggiungi Proxmox: token API

Proxmox Details

Plan Name: SMPProxmox-ApiToken

Proxmox Endpoint: 10.193.172.221

Authentication Method: ☒ API Token

API Token ID: root@pam!My_Token_123

API Token Secret: [Masked]

☒ Accept self-signed certificates

Buttons: Cancel, Add Site

9. Verifica che i processi di rilevamento siano andati a buon fine e che lo stato di ciascun piano sia contrassegnato come **Success**.

Una volta aggiunto, SMP esegue automaticamente una scansione di rilevamento e visualizza le VM insieme ai relativi metadati. Vengono rilevati anche eventuali volumi di storage o LUN mappati esistenti.

▼ Visualizza i risultati della scoperta del piano

3 Plans

Name	Endpoint	Type	Discover Status
SMPProxClus	10.192.102.41	ONTAP	Success
SMPProxmox-ApiToken	10.193.172.221:8006	Proxmox	In Progress
SMPProxmox-Username	10.193.172.225:8006	Proxmox	Success

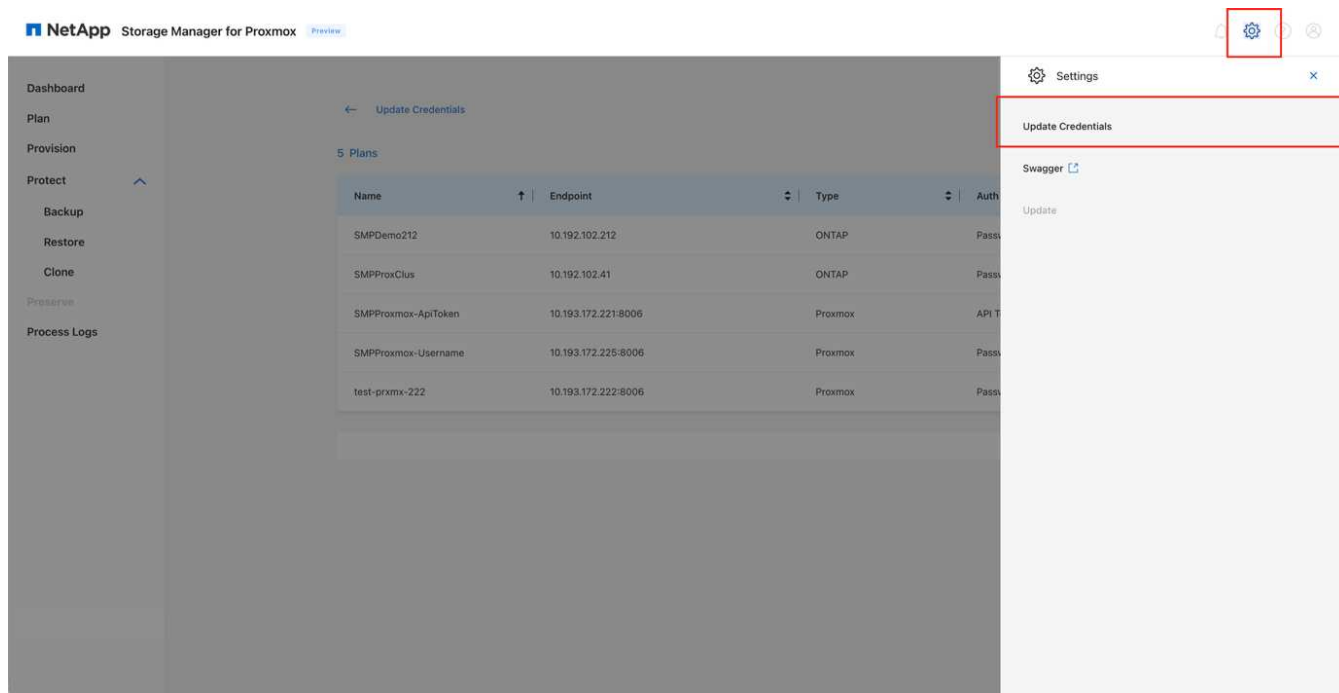
1 - 3 of 3

Dopo aver finito

- Se vengono apportate modifiche ai nodi o allo storage di Proxmox, esegui la procedura di rilevamento per recuperare le informazioni più recenti. Fai clic sui tre puntini accanto al nome del piano e quindi su **Rileva**.
- Assicurarsi che il sistema storage ONTAP venga aggiunto per primo, in modo che il processo di rilevamento possa mappare le risorse esistenti di conseguenza. Se Proxmox viene aggiunto per primo, eseguire un processo di rilevamento su ONTAP.

- Se in seguito fosse necessario aggiornare le credenziali o il token API, accedere a **Impostazioni** e selezionare l'opzione **Aggiorna credenziali**.

▼ Visualizza le credenziali di aggiornamento



Provisioning dello storage

Il provisioning di un volume come pool di storage, comunemente denominato datastore, crea un container logico per le macchine virtuali e i relativi dischi virtuali (QCOW2 o RAW). SMP consente di effettuare il provisioning di un datastore e di collegarlo a un singolo host o a tutti gli host all'interno di un cluster.

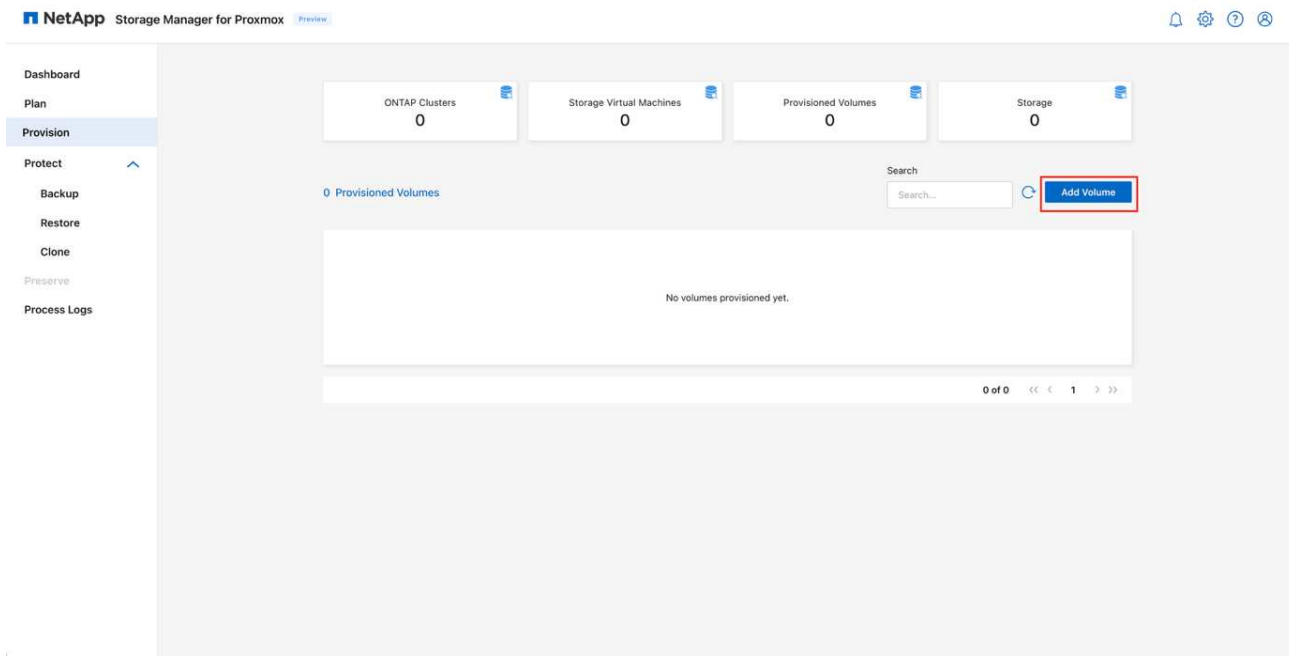
Provisioning dello storage NFS

Utilizzare SMP per eseguire il provisioning e il montaggio di un volume ONTAP come datastore NFS.

Passi

1. Nell'interfaccia grafica di SMP, vai alla scheda **Provision**.
2. Accedere alla sezione **Aggiungi volume**.

▼ Visualizza la scheda Provision: Aggiungi Volume

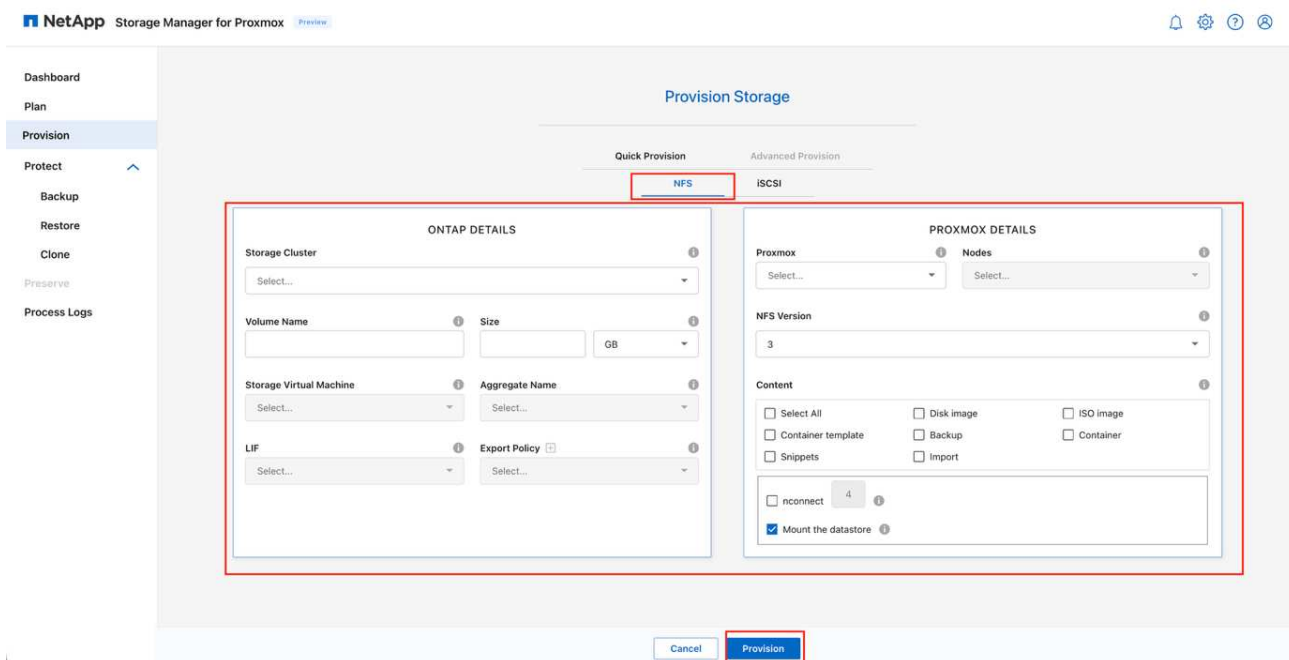


3. Nella procedura guidata Nuovo volume, nella fase di provisioning rapido, selezionare **NFS**.



NFS è selezionato per impostazione predefinita. Il provisioning rapido offre una configurazione più veloce utilizzando le impostazioni predefinite per le implementazioni standard. Il provisioning avanzato offre opzioni estese per le funzionalità di HA e BCDR, che saranno introdotte nelle versioni future.

▼ Visualizza la procedura guidata Nuovo Volume: NFS

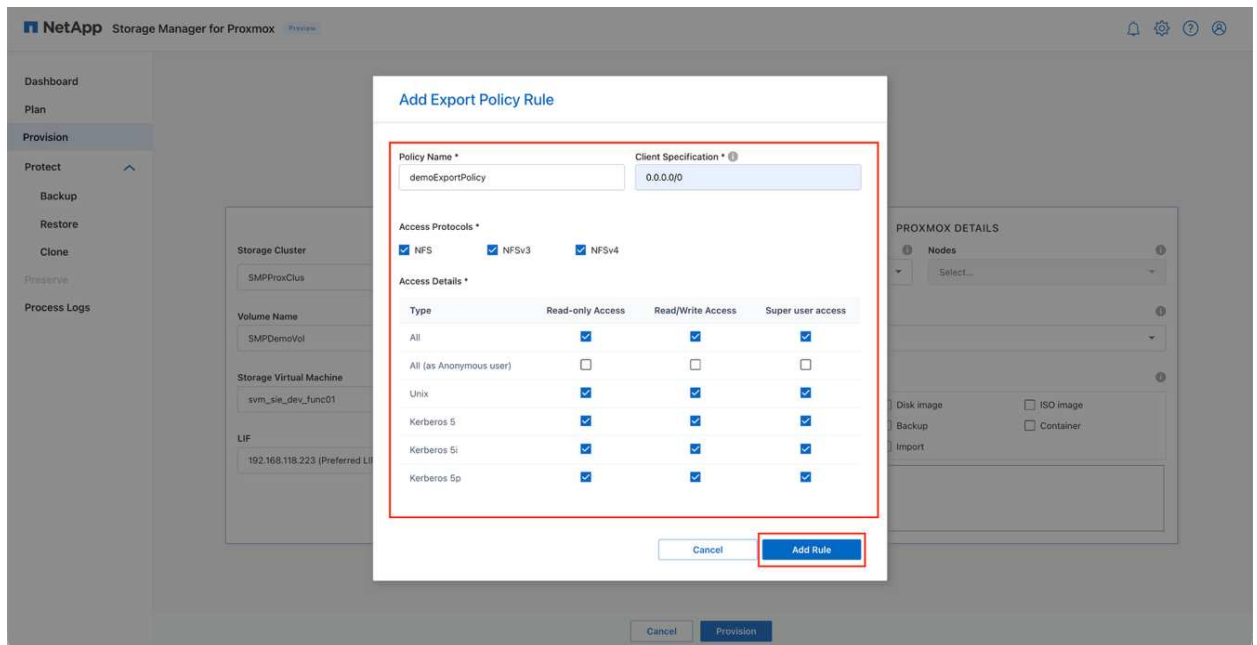


4. Nella sezione **Dettagli ONTAP**, fornire le seguenti informazioni:

- Selezionare l'ONTAP cluster o la Storage Virtual Machine (SVM) designata dal menu a tendina **Storage Cluster**
- Inserisci un valore univoco nel campo **Nome del volume**

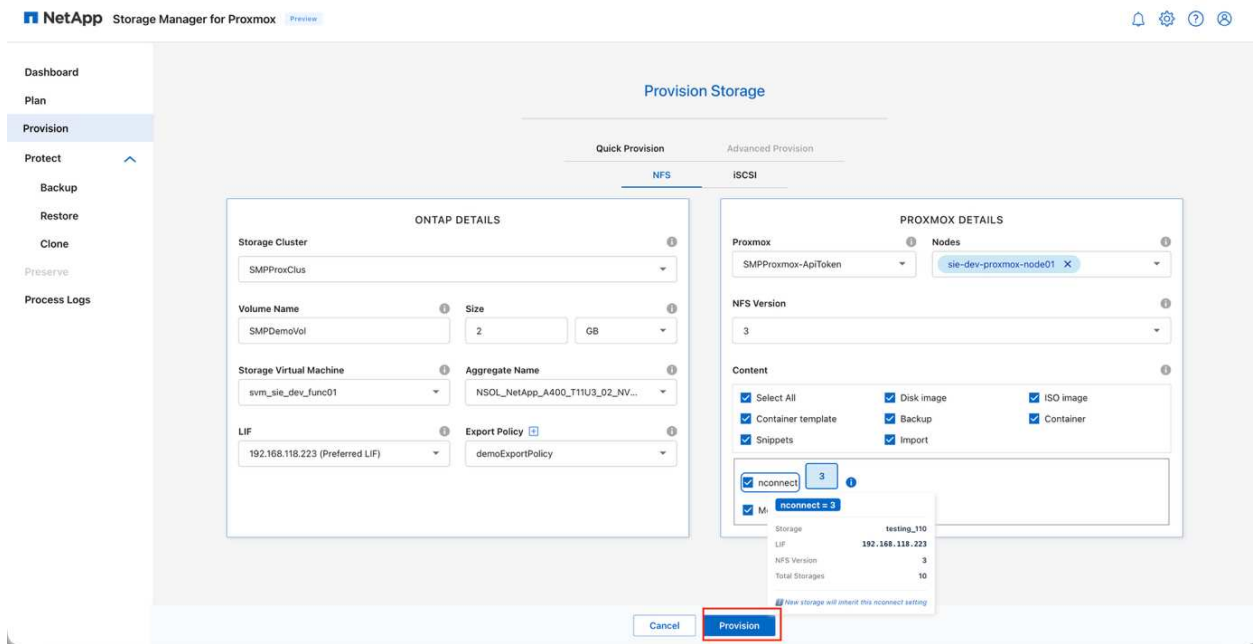
- c. Inserisci la capacità richiesta per il volume del datastore nel campo **Size**
- d. Scegli le risorse di storage ONTAP selezionando le opzioni appropriate per:
 - Nome aggregato
 - Storage Virtual Machine (SVM)
 - LIF preferito da utilizzare per l'accesso al datastore
- e. Seleziona una **policy di esportazione** esistente oppure crea una policy personalizzata facendo clic sul (+) a seconda delle necessità

▼ Visualizza dettagli ONTAP: NFS



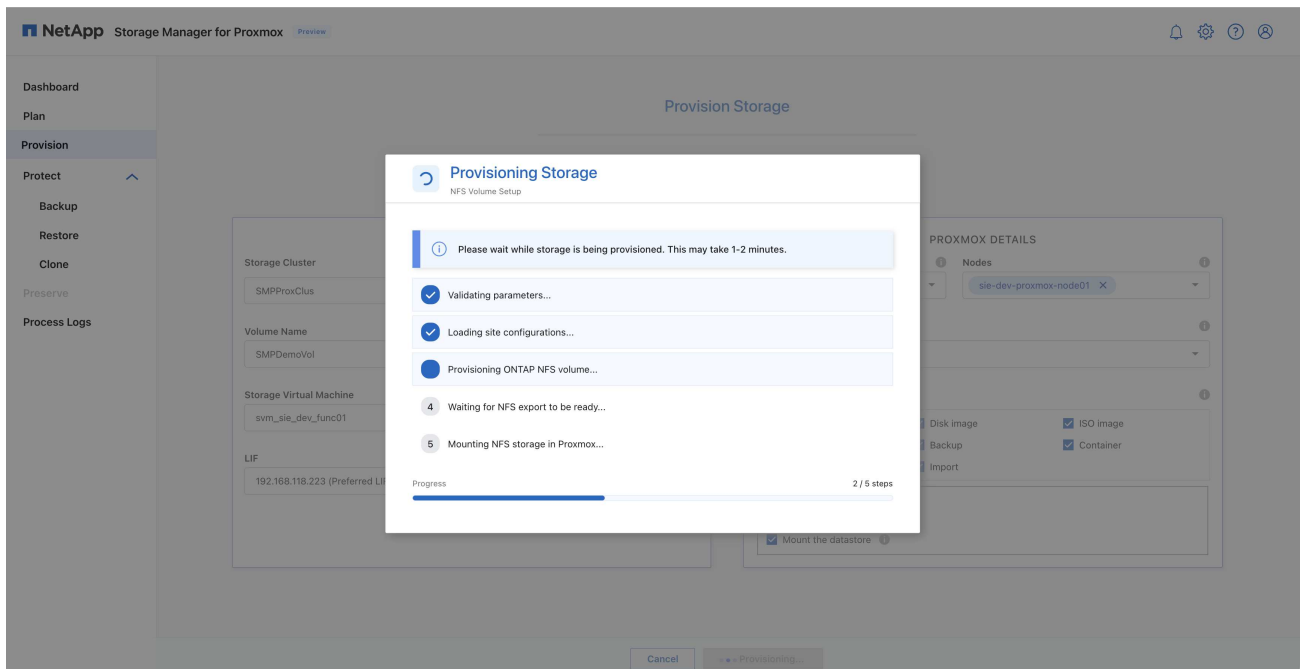
5. Nella sezione **Dettagli Proxmox**, fornire le seguenti informazioni:
 - a. Nel campo **Proxmox**, scegli il cluster di destinazione, quindi seleziona tutti i nodi che necessitano di accedere al datastore
 - b. Nel campo **Versione NFS**, selezionare il protocollo NFS preferito (NFS v3 o NFS v4.1)
 - c. Nella sezione **Contenuto**, selezionare i tipi di contenuto da abilitare per questo datastore:
 - Immagine del disco
 - immagine ISO
 - Modello di container
 - Backup
 - Frammenti
 - Importare
 - Oppure seleziona **Tutti** i tipi di contenuto
 - d. (Facoltativo) Attivare l'opzione **nconnect** se si desiderano più connessioni TCP
 - e. Assicurati che **Monta il datastore** sia selezionato, in modo che il datastore venga montato sui nodi Proxmox selezionati

▼ Visualizza i dettagli di Proxmox: NFS



- Fai clic su **Provision** per creare il volume ONTAP e registrare il datastore (pool di storage) all'interno del cluster Proxmox selezionato.

▼ Visualizza il risultato del provisioning NFS



NetApp Storage Manager for Proxmox

Dashboard

Plan

Provision

Protect

Backup

Restore

Clone

Preserve

Process Logs

ONTAP Clusters: 1

Storage Virtual Machines: 21

Provisioned Volumes: 111

Storage: 2030

111 Provisioned Volumes

Search

Add Volume

Storage Name	Protocol	Capacity	Mount Path	Proxmox Cluster	Mount Status
sie_dev_vol_aakashgupta...	NFS	1075.20 GB	/mnt/pve/sie_dev_vol_aakash	SMPProxmox-Username	Mounted
sie_dev_vol_aakashgupta	NFS	1.00 GB	/mnt/pve/sie_dev_vol_aakash	SMPProxmox-ApiToken	Mounted
sie_dev_vol_aakashgupta	NFS	1075.20 GB	/mnt/pve/sie_vol_aka_tst_1	SMPProxmox-Username	Mounted
sie_dev_proxmox_varsinil_1	NFS	105.26 GB	/mnt/pve/varsinil_proxmox_vo	SMPProxmox-Username	Mounted
sie_dev_proxmox_varsinil	NFS	200.00 GB	/mnt/pve/varsinil_proxmox_vo	SMPProxmox-Username	Mounted
sie_dev_aka_test1	NFS	2.00 GB	/mnt/pve/sie_dev_aka_test1	SMPProxmox-ApiToken	Mounted
sie_dev_aka_demo_3	NFS	7.00 GB	/mnt/pve/sie_dev_aka_demo_3	SMPProxmox-Username	Mounted
sie_dev_aka_demo	NFS	5.00 GB	/mnt/pve/sie_dev_aka_demo	SMPProxmox-Username	Mounted
abcd9876	NFS	6.00 GB	/mnt/pve/abcd9876	SMPProxmox-ApiToken	Mounted
SMPDemoVol	NFS	2.00 GB	/mnt/pve/SMPDemoVol	SMPProxmox-ApiToken	Mounted

▼ Visualizzare il datastore NFS in Proxmox

PROXMOX Virtual Environment 9.1.1

Search

Documentation

Create VM

Create CT

root@pam

Server View

Datacenter

Datacenter (nimravprox)

proxmox9-vm01

101 (nimrfs01)

102 (TVM-U18)

103 (ewaflead)

104 (testscsi)

107 (nim03)

112 (nimrfs06-88737)

113 (nimrfs01-1c20a)

Search

Summary

Notes

Cluster

Ceph

Options

ID	Type	Content	Path/Target	Shared	Enabled	Bandwidth Limit
DNDdemo	NFS	Disk image	/mnt/pve/DNDdemo	Yes	Yes	
ISO_Proxmox	NFS	ISO image	/mnt/pve/ISO_Proxmox	Yes	Yes	
SMPDemoLVM	LVM	Disk image	/mnt/pve/SMPDemoLVM	Yes	Yes	
SMPDemoVol	NFS	Disk image	/mnt/pve/SMPDemoVol	Yes	Yes	
dnstst	NFS	Disk image	/mnt/pve/dnstst	Yes	Yes	

Modificare un volume di cui è stato effettuato il provisioning

Utilizzare SMP per modificare le impostazioni del volume dopo il provisioning.

Passi

1. Nell'interfaccia grafica di SMP, individuare il volume nella scheda **Provision**.
2. Fai clic sui tre puntini verticali (**:**) accanto al volume.
3. Seleziona **Modifica** dal menu contestuale per aprire le impostazioni del volume.

▼ Finestra di dialogo Visualizza Modifica Volume

4. Modifica le impostazioni del volume secondo necessità:

- **Ridimensiona volume:** Regola la capacità di storage del volume



Il ridimensionamento è applicabile solo ai volumi NFS.

- **Snapshot Locking:** Attiva per impedire che gli snapshot vengano eliminati o modificati



Ciò richiede che la licenza SnapLock sia installata sul cluster e che l'orologio di conformità del cluster sia inizializzato.

- **Protezione anti-ransomware:** Consente di rilevare e segnalare in modo proattivo attività insolite che potrebbero indicare un attacco ransomware
- **Policy di esportazione:** Aggiorna o modifica la policy di esportazione

5. Fai clic su **Salva** per applicare le modifiche.

Provisioning dello storage iSCSI

Utilizza SMP per configurare un backend iSCSI per le macchine virtuali.

Passi

1. Nell'interfaccia grafica di SMP, vai alla scheda **Provision**.
2. Accedere alla sezione **Aggiungi volume**.
3. Nella procedura guidata Nuovo volume, nella fase di provisioning rapido, selezionare **iSCSI**.

▼ Visualizza la procedura guidata Nuovo Volume: iSCSI

NetApp Storage Manager for Proxmox

Provision Storage

Quick Provision | **iSCSI** | Advanced Provision

ONTAP DETAILS

Storage Cluster: Select...

Storage Virtual Machine: Select... | Aggregate Name: Select...

LUN Name: | Number of LUNs: 1

Capacity per LUN: | GB | Initiator Group: Select...

PROXMOX DETAILS

Proxmox: Select... | Nodes: Select...

LVM ID: | Storage VLAN: Select...

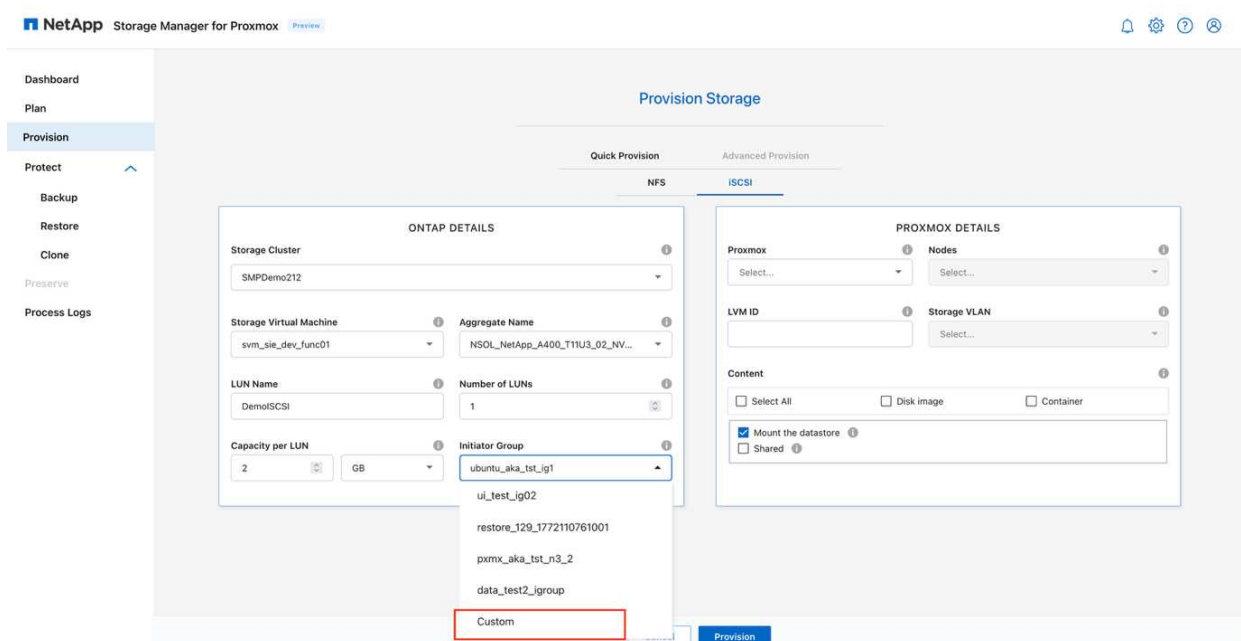
Content: ☐ Select All ☐ Disk image ☐ Container

☒ Mount the datastore ☐ Shared

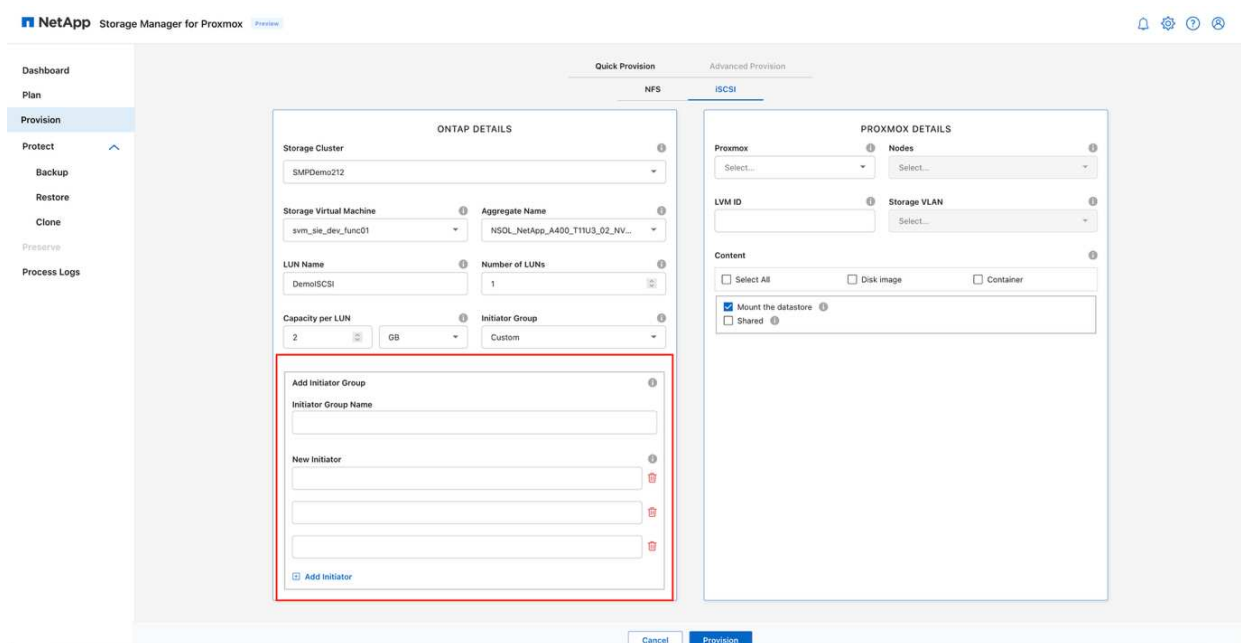
Cancel | **Provision**

4. Nel protocollo iSCSI, nella sezione **Dettagli ONTAP**, fornire le seguenti informazioni:
- Scegli il cluster ONTAP appropriato o la Storage Virtual Machine (SVM) designata dal menu a discesa **Storage Cluster**
 - Seleziona le opzioni per:
 - Nome aggregato
 - Storage Virtual Machine (SVM)
 - Inserisci un valore univoco nel campo **Nome LUN**
 - Specificare il numero di LUN richiesto nel campo **Numero di LUN** (il valore predefinito è 1; è possibile creare in parallelo LUN aggiuntivi della stessa dimensione)
 - Inserisci la dimensione desiderata per ogni LUN nel campo **Capacità per LUN**
 - Scegliere un **gruppo iniziatore** (igroup) per il controllo degli accessi iSCSI. È possibile selezionare un igroup esistente oppure crearne uno nuovo.

▼ **Visualizza dettagli ONTAP: configurazione LUN iSCSI**



▼ Visualizza la selezione igroup iSCSI



5. Nella sezione **Dettagli Proxmox**, fornire le seguenti informazioni:

- Dal menu a tendina **Proxmox**, scegli il cluster di destinazione, quindi seleziona tutti i nodi che richiedono l'accesso allo storage
- Seleziona l'**ID LVM** appropriato che rappresenterà il pool di storage iSCSI all'interno di Proxmox
- Nel campo **Nodi**, selezionare tutti i nodi che necessitano di accedere alle destinazioni iSCSI presentate
- (Facoltativo) Se è necessaria la segmentazione VLAN, scegliere la **VLAN di archiviazione** desiderata
- Nella sezione **Contenuto**, selezionare i tipi di contenuto supportati da questo datastore:
 - Immagine del disco
 - container
 - Oppure seleziona **Tutti** i tipi di contenuto

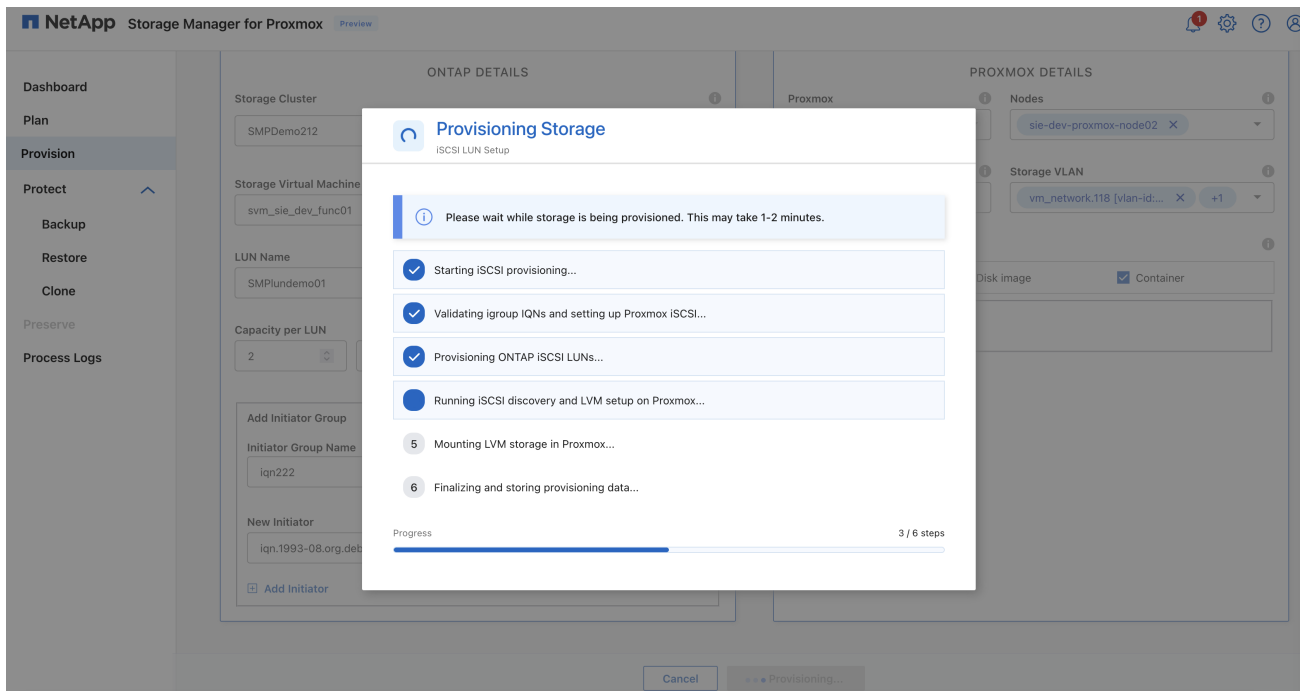
- f. Assicurati che **Mount the datastore** sia selezionato, in modo che lo storage sia disponibile sui nodi Proxmox scelti
- g. (Opzionale) Abilita **Condiviso** se il pool di storage verrà acceduto contemporaneamente da più nodi

▼ Visualizza i dettagli di Proxmox: iSCSI

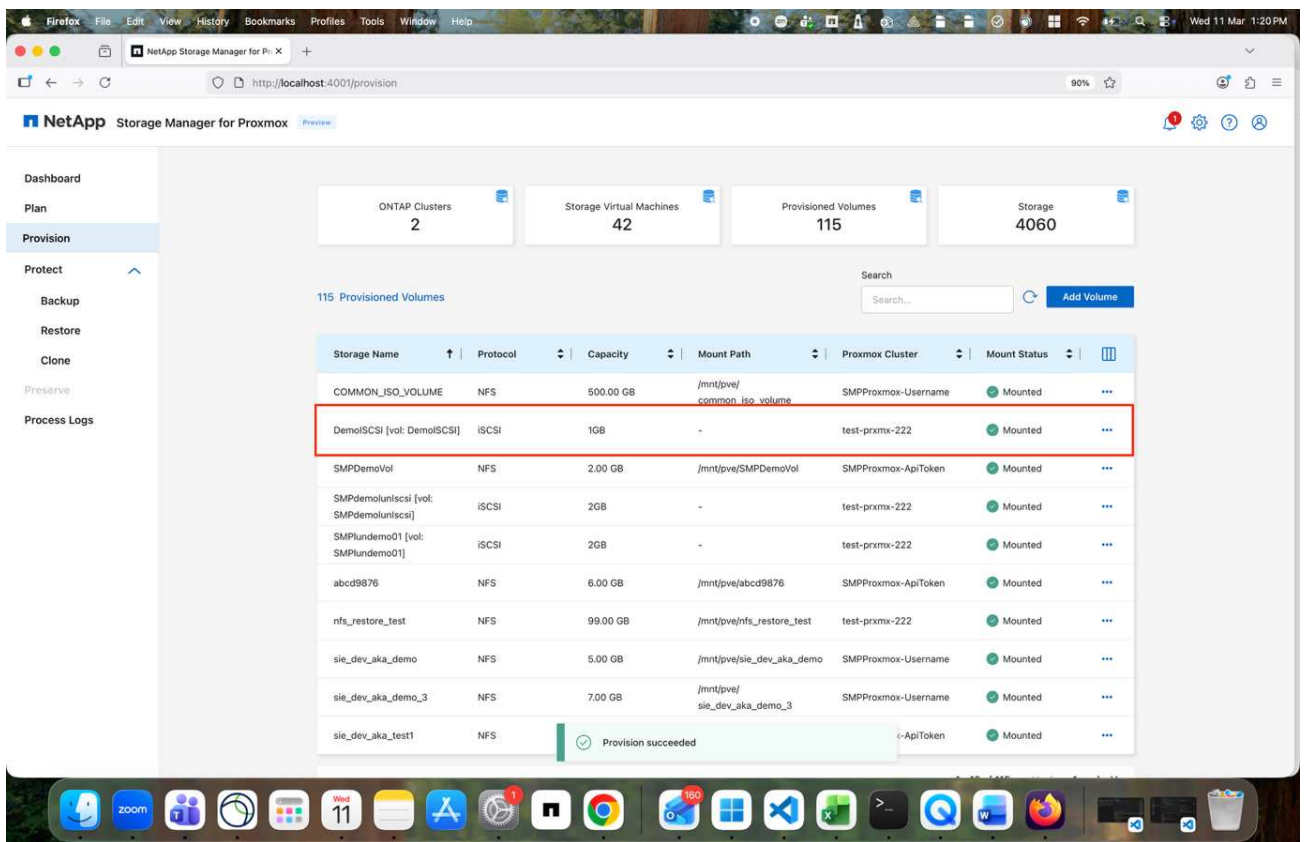
6. Fai clic su **Provision** per creare la LUN ONTAP e registrare il datastore (pool di storage) all'interno del cluster Proxmox selezionato.

▼ Visualizza il provisioning delle LUN iSCSI

▼ Visualizza provisioning iSCSI completato



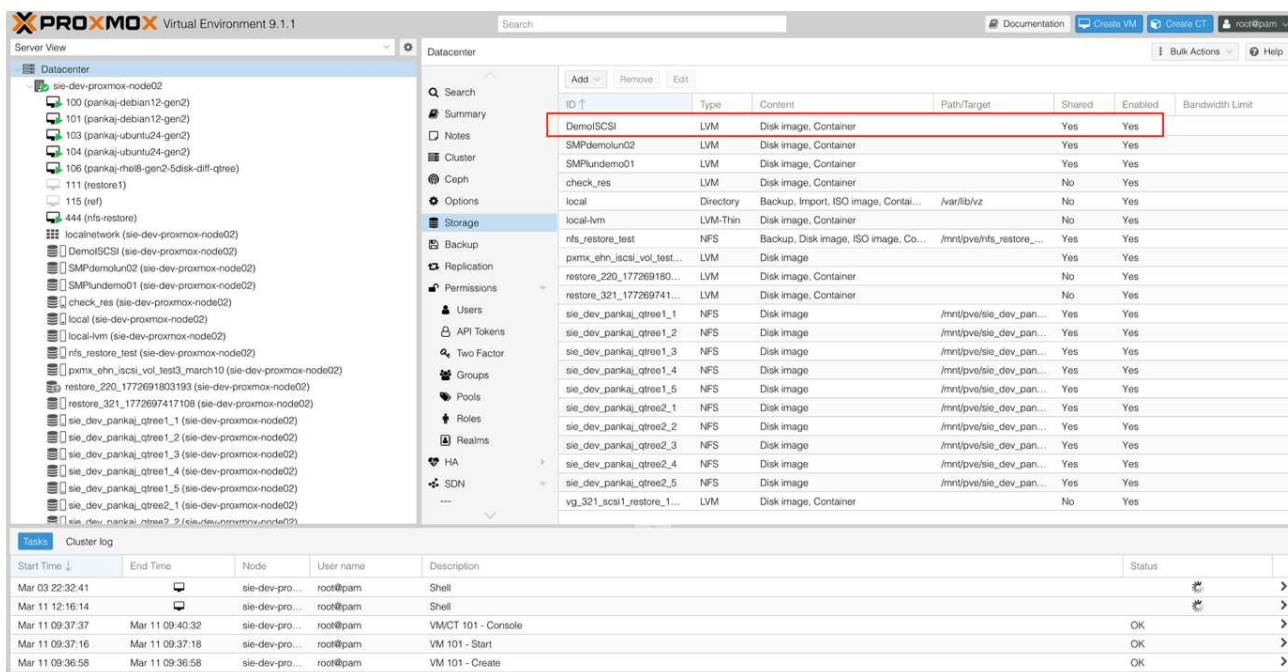
▼ Visualizza il datastore iSCSI in Proxmox



7. Verificare che le LUN NFS e iSCSI siano state connesse accedendo all'endpoint di Proxmox.

Lo spazio di archiviazione collegato è ora disponibile per il provisioning di macchine virtuali.

▼ Visualizza la vista dello storage di Proxmox



Opzioni di configurazione del volume

Quando SMP esegue il provisioning di nuovi ONTAP FlexVol volumi e LUN, vengono applicati automaticamente diversi valori di configurazione predefiniti:

Impostazione ONTAP	Valore predefinito
riserva di Snapshot (-percent-snapshot-space)	0%
Riserva frazionaria (-fractional-reserve)	0%
Aggiornamento dell'ora di accesso (-atime-update)	Disattivato
Previsione minima (-min-readahead)	Disattivato
Snapshot programmati	Nessuno
efficienza di storage	Abilitato
Garanzia di volume	Nessuno (thin provisioned)
dimensionamento automatico	aumenta_riduci
Riserva di spazio LUN	Disattivato
allocazione dello spazio LUN	Abilitato

Comportamento di NConnect

Quando si utilizza lo storage NFS con Proxmox VE, è importante tenere presente il comportamento specifico del client NFS (come utilizzato da Debian, il sistema operativo di base di Proxmox VE). Il kernel Linux potrebbe riutilizzare i parametri di montaggio dalla prima volta che un'esportazione NFS viene montata su un nodo. Se la stessa esportazione viene montata nuovamente con opzioni di montaggio diverse, queste nuove opzioni potrebbero non essere applicate.

Come best practice, crea e monta esportazioni separate e utilizza indirizzi IP del server NFS diversi, come LIF di dati distinti. SMP rileva automaticamente le connessioni esistenti insieme ai relativi valori nconnect e applica il valore nconnect appropriato a qualsiasi nuova connessione.

Proteggere le macchine virtuali

Quando le macchine virtuali vengono eseguite su datastore NFS supportati da ONTAP, l'approccio di protezione più efficiente consiste nel lasciare che Proxmox stabilisca la coerenza del filesystem, mentre ONTAP acquisisce il punto di backup effettivo a livello di storage. Le Snapshot ONTAP forniscono copie point-in-time rapide ed efficienti in termini di spazio del volume del datastore e possono essere utilizzate successivamente per ripristinare interi datastore, singoli file o contenuti di VM.

SMP offre un semplice orchestratore per la protezione dei dati coerente con i crash e con le macchine virtuali e la gestione dei cloni. Questo software semplifica i cicli di vita di backup, ripristino e clonazione attraverso la creazione di policy di backup applicabili a più processi. Queste policy possono definire pianificazione, conservazione, replica e altre funzionalità. Consentono la selezione facoltativa di snapshot coerenti con i file; questo approccio sfrutta la capacità di QEMU di sospendere le operazioni di I/O prima di acquisire una Snapshot ONTAP.

SMP consente di proteggere un intero datastore, dove un volume NFS ONTAP contiene più macchine virtuali, gruppi di macchine virtuali che possono estendersi su più datastore, oppure a livello di singola macchina virtuale.

Eseguire il backup delle macchine virtuali

Una volta che i volumi ONTAP sono stati predisposti, utilizzare l'opzione Backup per elencare tutte le VM in esecuzione sul cluster Proxmox ed eseguire un backup crash-consistent o file-consistent delle macchine virtuali.

Passi

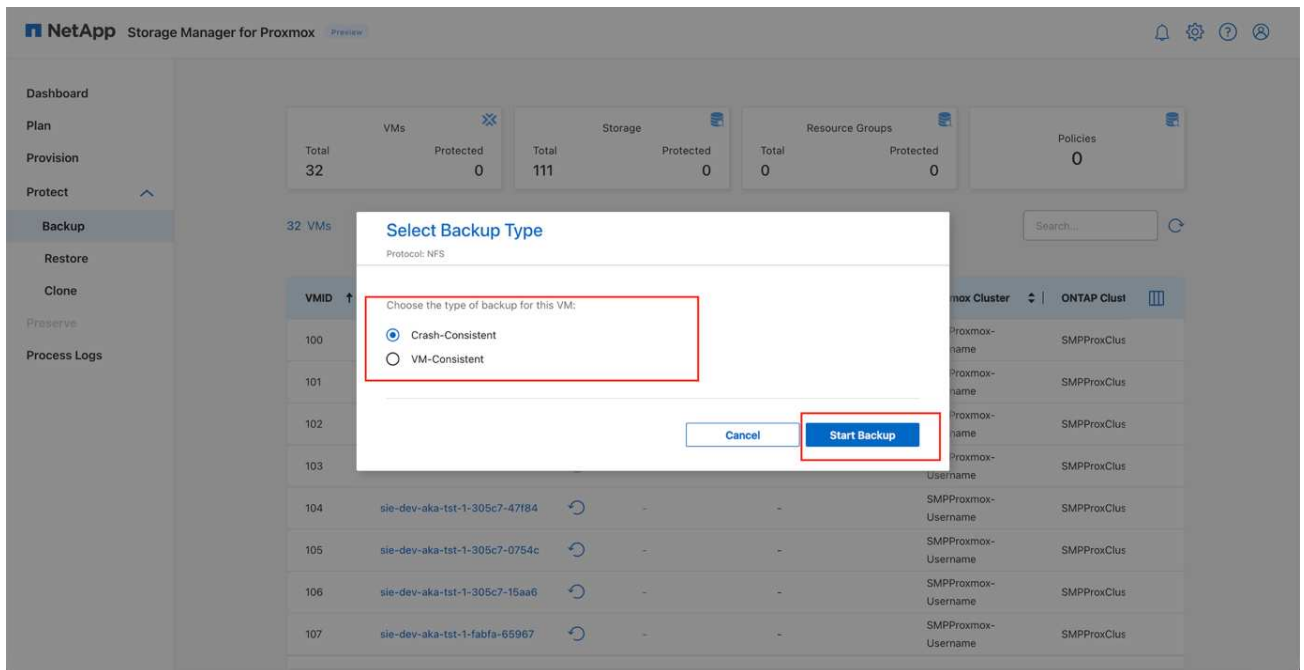
1. Accedi a **Proteggi > Backup** dal riquadro di navigazione a sinistra.

▼ Visualizza la pagina Protect Backup

VMID	Name	Backup	Backup Status	Last Backup Date	Proxmox Cluster	ONTAP Clust
100	sie-dev-aka-tst-1-89a2e	🔄	-	-	SMPProxmox-Username	SMPProxClus
101	sie-dev-aka-tst-1-fc39f	🔄	-	-	SMPProxmox-Username	SMPProxClus
102	sie-dev-aka-tst-1-ce32c	🔄	-	-	SMPProxmox-Username	SMPProxClus
103	sie-dev-aka-tst-1	🔄	-	-	SMPProxmox-Username	SMPProxClus
104	sie-dev-aka-tst-1-305c7-47f84	🔄	-	-	SMPProxmox-Username	SMPProxClus
105	sie-dev-aka-tst-1-305c7-0754c	🔄	-	-	SMPProxmox-Username	SMPProxClus
106	sie-dev-aka-tst-1-305c7-15aa6	🔄	-	-	SMPProxmox-Username	SMPProxClus
107	sie-dev-aka-tst-1-fabfa-65967	🔄	-	-	SMPProxmox-Username	SMPProxClus

2. Seleziona la macchina virtuale di cui eseguire il backup e fai clic su **Backup**.

▼ Visualizzazione della finestra di dialogo Backup: selezione VM



- Il flusso di lavoro di backup consente di scegliere tra protezione coerente in caso di arresto anomalo e protezione coerente a livello di file.

La modalità di coerenza dei file utilizza facoltativamente QEMU fsfreeze per garantire la quiescenza del filesystem all'interno della macchina virtuale prima della creazione dello Snapshot. Se fsfreeze fallisce, il sistema ripiega sull'utilizzo di uno Snapshot Proxmox.



Questo meccanismo di fallback si applica solo alle macchine virtuali archiviate su volumi NFS.

▼ Visualizza la finestra di dialogo Backup: opzioni di coerenza

Cluster log						
Start Time	End Time	Node	User name	Description	Status	
Feb 25 02:55:28		proxmox9-...	root@pam	Shell		
Mar 10 08:51:01	Mar 10 08:51:01	proxmox9-...	root@pam	VM 116 - Delete Snapshot	OK	
Mar 10 08:50:56	Mar 10 08:50:57	proxmox9-...	root@pam	VM 116 - Snapshot	OK	

▼ Visualizza l'avanzamento del backup

NetApp Storage Manager for Proxmox Preview

Dashboard

Plan

Provision

Protect

Backup

Restore

Clone

Preserve

Process Logs

VMs

Total 32 Protected 0

Storage

Total 111 Protected 0

Resource Groups

Total 0 Protected 0

Policies

Total 0 Protected 0

32 VMs

VMs Storage Resource groups Policies

Search...

VMID	Name	Backup	Backup Status	Last Backup Date	Proxmox Cluster	ONTAP Clust
100	sie-dev-aka-tst-1-89a2e		Success	11/03/2026, 11:44:00	SMPProxmox-Username	SMPProxClus
101	sie-dev-aka-tst-1-fc39f		-	-	SMPProxmox-Username	SMPProxClus
102	sie-dev-aka-tst-1-ce32c		-	-	SMPProxmox-Username	SMPProxClus
103	sie-dev-aka-tst-1		-	-	SMPProxmox-Username	SMPProxClus
104	sie-dev-aka-tst-1-305c7-47f84		-	-	SMPProxmox-Username	SMPProxClus
105	sie-dev-aka-tst-1-305c7-0754c		-	-	SMPProxmox-Username	SMPProxClus
106	sie-dev-aka-tst-1-305c7-15aa6		-	-	SMPProxmox-Username	SMPProxClus
107	sie-dev-aka-tst-1-fabfa-65967		VM backup completed: 1 successful, 0 failed		SMPProxmox-Username	SMPProxClus



Gli snapshot ONTAP vengono creati a livello di volume, acquisendo tutti i dischi delle VM e i file di configurazione all'interno del datastore NFS in un singolo snapshot. Quando è selezionata la protezione coerente con le VM, fsfreeze viene eseguito solo sulle VM selezionate; tutte le altre VM presenti nel volume vengono incluse come crash-consistent nello stesso snapshot ONTAP.

Opzioni di backup aggiuntive

- Per eseguire il backup di un singolo datastore, selezionare la scheda **Storage** e scegliere l'opzione **Backup**.
- Per eseguire il backup di più datastore come un'unica unità o per proteggere gruppi di macchine virtuali che si estendono su datastore diversi, utilizzare l'opzione **Gruppo di risorse**. I gruppi di risorse consentono di organizzare datastore o macchine virtuali in set di protezione logici.

▼ Visualizza la scheda Gruppo di risorse

NetApp Storage Manager for Proxmox Preview

Dashboard
Plan
Provision
Protect
Backup
Restore
Clone
Preserve
Process Logs

Total VMs: 32 Protected: 0
Total Storage: 111 Protected: 0
Total Resource Groups: 0 Protected: 0
Total Policies: 0

32 VMs **Storage** **Resource groups** Policies

VMID	Name	Backup	Backup Status	Last Backup Date	Proxmox Cluster	ONTAP Clust
100	sie-dev-aka-tst-1-89a2e	Success	Success	11/03/2026, 11:44:00	SMPProxmox-Username	SMPProxClus
101	sie-dev-aka-tst-1-fc39f	-	-	-	SMPProxmox-Username	SMPProxClus
102	sie-dev-aka-tst-1-ce32c	-	-	-	SMPProxmox-Username	SMPProxClus
103	sie-dev-aka-tst-1	-	-	-	SMPProxmox-Username	SMPProxClus
104	sie-dev-aka-tst-1-305c7-47f84	-	-	-	SMPProxmox-Username	SMPProxClus
105	sie-dev-aka-tst-1-305c7-0754c	-	-	-	SMPProxmox-Username	SMPProxClus
106	sie-dev-aka-tst-1-305c7-15aa6	-	-	-	SMPProxmox-Username	SMPProxClus
107	sie-dev-aka-tst-1-fabfa-65967	-	-	-	SMPProxmox-Username	SMPProxClus

Crea un gruppo di risorse

1. Apri la scheda **Gruppo di risorse** e seleziona **Aggiungi**.
2. Inserisci un nome per il nuovo gruppo di risorse.
3. Scegli il tipo di risorsa: **VM** o **Datastore**.
4. Selezionare il **Protocol** appropriato.
5. Scegli le macchine virtuali o i datastore specifici da includere, in base al tipo di risorsa selezionato.
6. Fai clic su **Crea gruppo di risorse** per completare la configurazione.

▼ Visualizza la finestra di dialogo Crea gruppo di risorse

NetApp Storage Manager for Proxmox Preview

Dashboard
Plan
Provision
Protect
Backup
Restore
Clone
Preserve
Process Logs

Add Resource Group

Resource Group Name

VM Datastore

Select Protocol Type

NFS (30) ISCSI (2)

Select the storage protocol for this VM resource group

Search VMs by name, ID, node, plan, or protocol...

	VMID	Name	Proxmox Cluster	Protocol	Node
☐	100	sie-dev-aka-tst-1-89a2e	SMPProxmox-Username	NFS	sie-dev-proxmox-...
☐	101	sie-dev-aka-tst-1-fc39f	SMPProxmox-Username	NFS	sie-dev-proxmox-...
☐	102	sie-dev-aka-tst-1-ce32c	SMPProxmox-Username	NFS	sie-dev-proxmox-...
☐	103	sie-dev-aka-tst-1	SMPProxmox-Username	NFS	sie-dev-proxmox-...

Cancel Create Resource Group



I backup eseguiti a livello di datastore (volume) sono sempre coerenti in caso di crash. Un gruppo di risorse può contenere un solo tipo di risorsa: o macchine virtuali o datastore. Per lo

storage basato su iSCSI, i backup sono sempre coerenti in caso di crash.

Dettagli del flusso di lavoro di backup

Il flusso di lavoro di backup high-level comprende:

1. **Definisci l'ambito di protezione:** Seleziona se la destinazione della protezione è un datastore (volume ONTAP), un gruppo di risorse (più volumi o VM) o una singola VM.
2. **Conferma il metodo di coerenza:** Scegli come viene creata la coerenza prima dello snapshot ONTAP:
 - Blocco/sblocco dell'agente guest QEMU per la quiescenza del filesystem all'interno della macchina virtuale e l'integrazione con Windows VSS.
3. **Esegui il dump dei file di configurazione della macchina virtuale.**
4. **Crea una Snapshot ONTAP:** acquisisci una Snapshot ONTAP del volume del datastore mentre le VM si trovano in uno stato coerente. Questa diventa la copia di backup conservata.
5. **Rimuovi gli snapshot temporanei di Proxmox:** Elimina gli snapshot di Proxmox dopo il completamento dello snapshot ONTAP per evitare la crescita dei file delta.
6. **Applica le policy di conservazione e replica (utilizzando le policy):** applica la policy di conservazione ONTAP configurata e replica il set di Snapshot se la replica per il disaster recovery è abilitata.

Questo approccio riduce al minimo lo spazio di storage e la larghezza di banda memorizzando solo le informazioni modificate. Utilizza le copie Snapshot per creare copie rapide della macchina virtuale o del datastore senza influire sulle prestazioni e poi inviale a un sistema secondario utilizzando la tecnologia NetApp SnapMirror per la protezione dei dati a lungo termine e fuori sede.

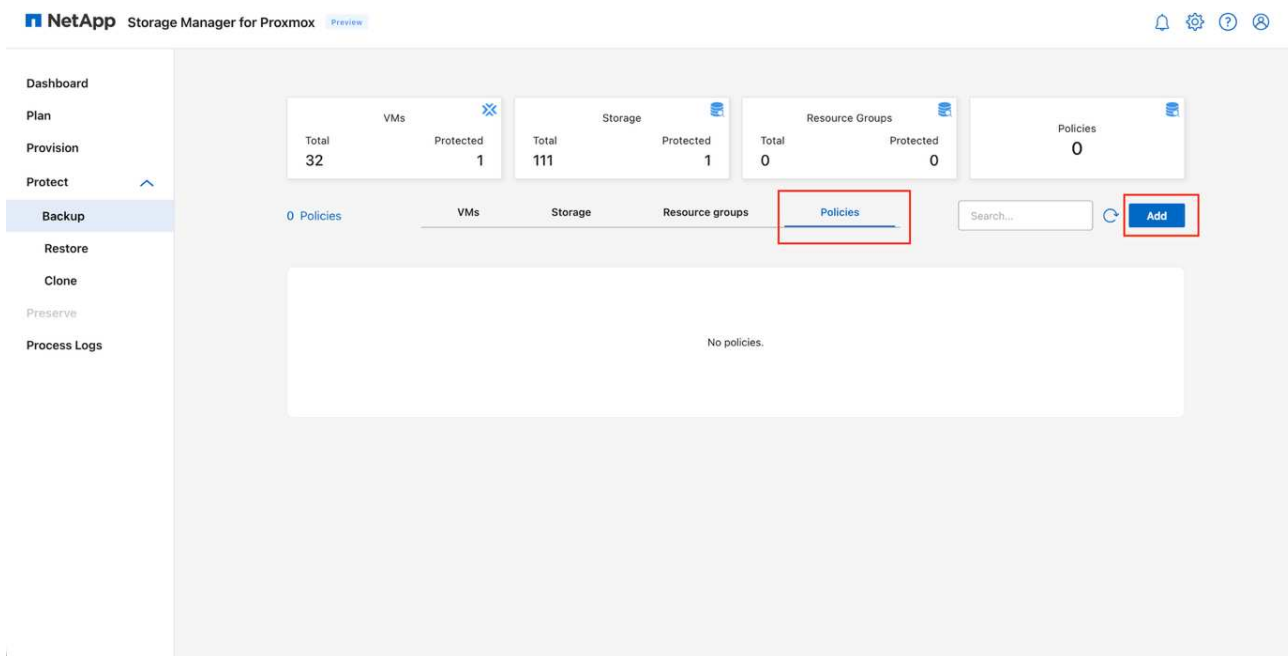
Automatizzare le attività di backup delle macchine virtuali

Automatizza i backup delle macchine virtuali Proxmox configurando una pianificazione. Creare backup regolari è fondamentale per la protezione dei dati e il ripristino di emergenza.

Passi

1. Vai su **Protezione > Backup > Policy** e fai clic su **Aggiungi** per aggiungere una nuova policy di backup e una pianificazione.

▼ **Visualizza la pagina delle policy di backup**



2. Configura le impostazioni generali:

- a. Inserisci un nome per la policy
- b. Seleziona il **tipo di policy** (volume o gruppo di risorse)
- c. Scegli il **Target** in base al tipo selezionato
- d. Imposta la **frequenza di backup** (oraria, giornaliera, settimanale o mensile)
- e. Configura la **conservazione**, utilizzando "Giorni di conservazione" o "Numero di elementi da conservare" (il valore di conservazione predefinito è 7)
- f. Seleziona la **Modalità di replica** (disabilitata nella versione attuale):
 - Aggiorna SnapMirror dopo il backup
 - Aggiorna SnapVault dopo il backup



SnapMirror replication deve essere configurata in ONTAP utilizzando la CLI o System Manager.

3. In **Opzioni avanzate**, abilita **Coerenza VM** se devono essere utilizzati gli snapshot di Proxmox o fsfreeze prima di avviare lo snapshot ONTAP.
4. Fai clic su **Crea policy** per salvare la configurazione.

▼ **Visualizza policy di backup: pianificazione e conservazione**

NetApp Storage Manager for Proxmox [Preview](#)

Dashboard
Plan
Provision
Protect
Backup
Restore
Clone
Preserve
Process Logs

Add Policy

Name

demoPolicy01

Policy Type

Volume

Select Volume

SMPDemoVol

Frequency

Hourly

Retention

Days to keep

7

Replication

☐ Update SnapMirror after backup

☐ Update SnapVault after backup

Advanced Options

Cancel

Create Policy

▼ Visualizza policy di backup: replica e opzioni avanzate

NetApp Storage Manager for Proxmox [Preview](#)

Dashboard
Plan
Provision
Protect
Backup
Restore
Clone
Preserve
Process Logs

VMs

Total 32

Protected 1

Storage

Total 111

Protected 1

Resource Groups

Total 0

Protected 0

Policies

Total 1

1 Policies

VMs Storage Resource groups Policies

Search... Add

Policy Name	Type	Target	Schedule	Retention	Status	Last Backup
demoPolicy01	datastore	SMPDemoVol	hourly	7 days	Enabled	-

1 - 1 of 1 << < 1 > >>



È possibile avviare immediatamente un'attività di backup di una macchina virtuale facendo clic su **Backup**, anziché attendere l'orario di esecuzione pianificato per un gruppo di risorse.

Ripristinare macchine virtuali o datastore

Utilizza SMP per ripristinare una VM Proxmox da backup.

Prima di iniziare

Le macchine virtuali devono essere spente prima di eseguire un'operazione di ripristino.

Passi

1. Seleziona l'opzione **Ripristina** dal riquadro di navigazione sul lato sinistro dell'interfaccia web.
2. Selezionare la macchina virtuale, lo storage o il gruppo di risorse da ripristinare.

▼ Visualizza la pagina Ripristina

The screenshot shows the NetApp Storage Manager for Proxmox interface. On the left sidebar, the 'Restore' option is highlighted with a red box. The main content area displays a summary of resources: VMs (Total 32, Protected 1), Storage (Total 111, Protected 1), Resource Groups (Total 0, Protected 0), and Policies (1). Below this, there are tabs for 'VMs', 'Storage', and 'Resource groups', with 'VMs' selected and highlighted with a red box. A table of VMs is shown with columns: VMID, Name, Proxmox Cluster, ONTAP Cluster, Protocol, Restore, Restore Status, and Last I. The 'Restore' column for the first VM (VMID 100) is highlighted with a red box, showing a restore icon.

VMID	Name	Proxmox Cluster	ONTAP Cluster	Protocol	Restore	Restore Status	Last I
100	sie-dev-aka-tst-1-89a2e	SMPProxox-Username	SMPProxClus	NFS	🔄	-	-
101	sie-dev-aka-tst-1-fc39f	SMPProxox-Username	SMPProxClus	NFS	🔄	-	-
102	sie-dev-aka-tst-1-ce32c	SMPProxox-Username	SMPProxClus	NFS	🔄	-	-
103	sie-dev-aka-tst-1	SMPProxox-Username	SMPProxClus	NFS	🔄	-	-
104	sie-dev-aka-tst-1-305c7-47f84	SMPProxox-Username	SMPProxClus	NFS	🔄	-	-
105	sie-dev-aka-tst-1-305c7-0754c	SMPProxox-Username	SMPProxClus	NFS	🔄	-	-
106	sie-dev-aka-tst-1-305c7-15aa6	SMPProxox-Username	SMPProxClus	NFS	🔄	-	-
107	sie-dev-aka-tst-1-fabfa-65967	SMPProxox-Username	SMPProxClus	NFS	🔄	-	-
108	sie-dev-aka-tst-1-1fbb1	SMPProxox-Username	SMPProxClus	NFS	🔄	-	-
111	sie-dev-aka-tst-1-350aa	SMPProxox-Username	SMPProxClus	NFS	🔄	-	-

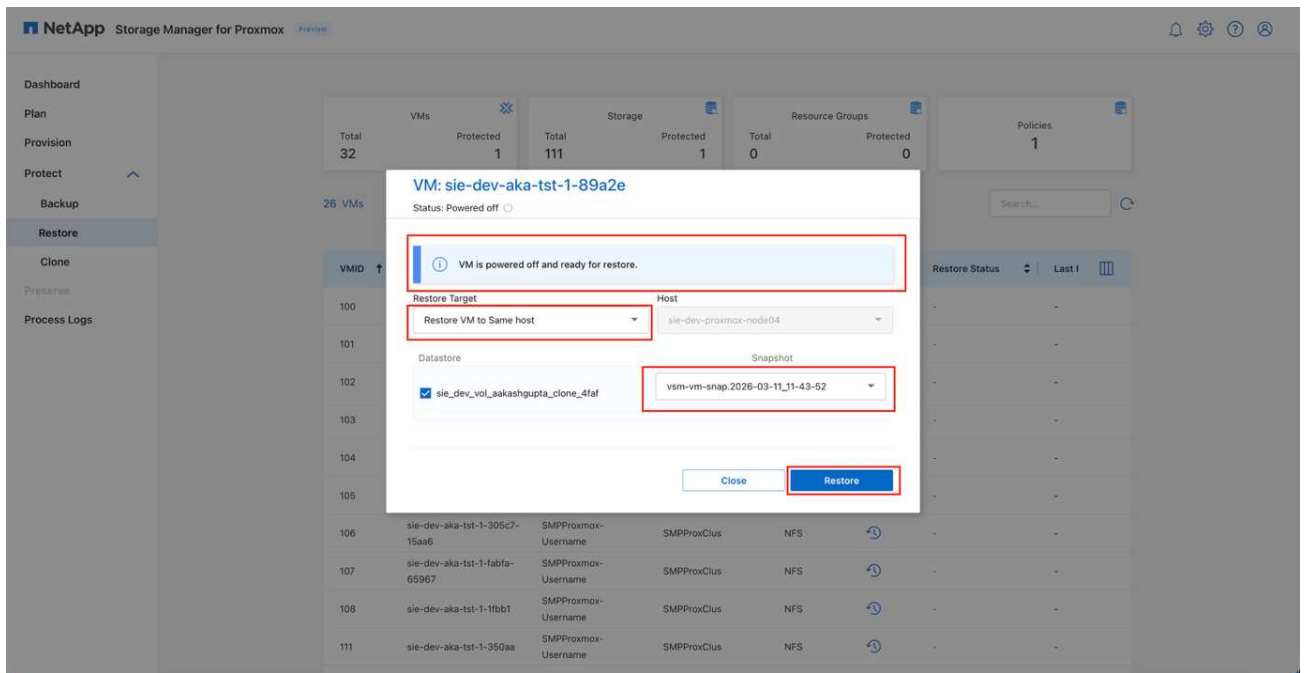
3. Fai clic sull'icona **Ripristina**.

A seconda della selezione (VM, storage o gruppo di risorse), si aprirà la finestra a comparsa per il ripristino.



A seconda della risorsa selezionata, verranno mostrati gli snapshot creati per i rispettivi componenti. Ad esempio, gli snapshot creati a livello di gruppo di risorse verranno visualizzati solo quando si seleziona un gruppo di risorse. Lo stesso vale per lo storage. Tuttavia, per le macchine virtuali, verranno visualizzati tutti gli snapshot creati per i vari componenti, consentendone la selezione.

▼ Visualizza la finestra di dialogo Ripristina: selezione Snapshot

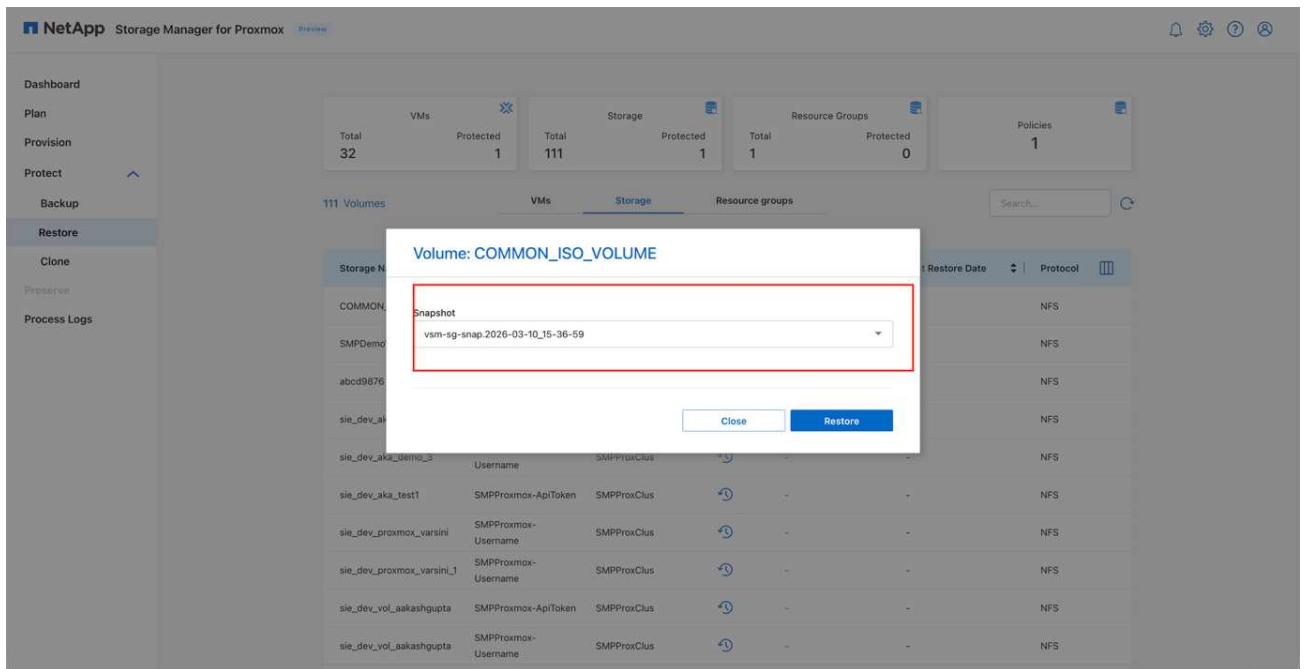


4. Seleziona le opzioni desiderate:

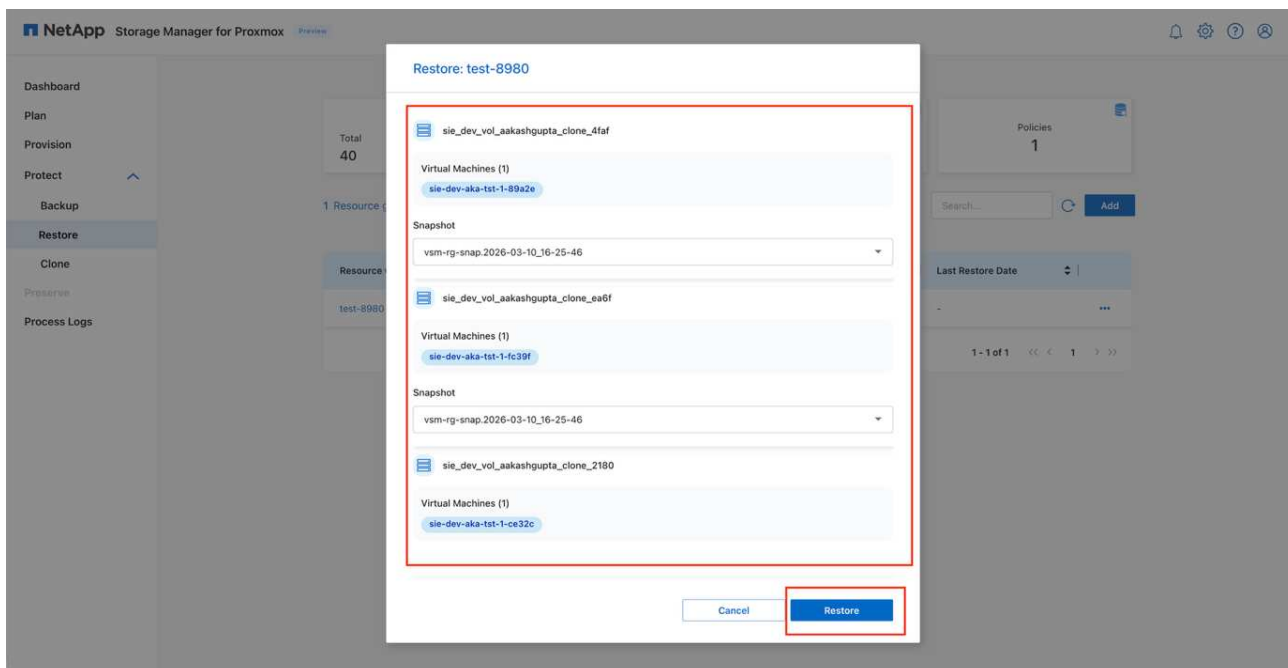
- Destinazione di ripristino:** opzione per ripristinare sullo stesso host o su un host alternativo
- Host:** Se si seleziona un host alternativo, il menu a tendina consente di selezionare un host qualsiasi disponibile all'interno del cluster
- Snapshot:** Scegli lo snapshot appropriato per ripristino point-in-time

5. Fai clic su **Ripristina**.

▼ Visualizza ripristino in corso

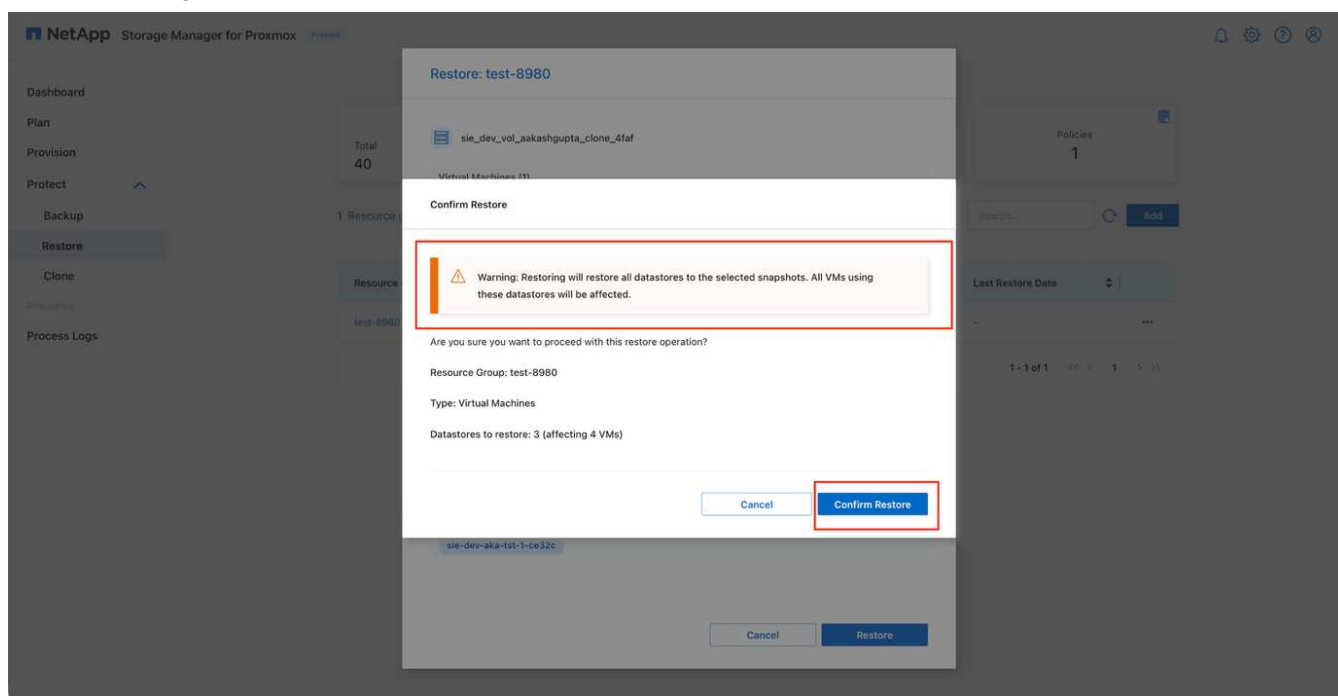


▼ Visualizza ripristino completato



Quando viene avviato un ripristino a livello di storage, tutte le macchine virtuali presenti su quel volume o LUN vengono spente e il sistema ripristina l'intera entità di storage nella sua interezza.

▼ Visualizza il ripristino a livello di archiviazione



Dettagli del flusso di lavoro di ripristino

Il flusso di lavoro di ripristino varia a seconda del tipo di storage sottostante e prevede i seguenti passaggi chiave:

1. **Definisci l'ambito del ripristino:** Seleziona se la destinazione della protezione è un datastore (volume ONTAP), un gruppo di risorse (più volumi o VM) o una singola VM.
2. **Eseguire l'operazione di ripristino:** Il processo di ripristino della macchina virtuale varia a seconda del

protocollo storage:

- **Ripristini basati su NFS:** Quando si ripristina un volume o un datastore su NFS, SMP avvia un'operazione di ripristino dello snapshot del volume sul volume di destinazione. Per le VM ospitate su volumi NFS, SMP convalida i parametri di ripristino, inclusi l'ID della VM, il nome dello snapshot, gli ID del sito e il tipo di storage. Se la VM è in esecuzione, SMP la arresta verificandone lo stato ed emettendo un comando di arresto. Il sistema ripristina quindi i dischi della VM dallo snapshot utilizzando un'operazione di ripristino a livello di file.
- **Ripristini basati su iSCSI:** Per i datastore o i LUN iSCSI, SMP ripristina il LUN dallo snapshot, verifica il dispositivo ripristinato, esegue una nuova scansione iSCSI sui nodi Proxmox e garantisce l'accessibilità del dispositivo. Per le VM residenti su storage iSCSI, SMP clona i LUN dello snapshot, mappa i LUN clonati sull'host Proxmox ed esegue il rilevamento iSCSI per importarli. Lo storage ripristinato viene quindi aggiunto e le configurazioni delle VM vengono aggiornate. I dischi delle VM vengono spostati nuovamente nello storage originale e l'avanzamento viene monitorato per ogni VM. Il processo si conclude con attività di pulizia, tra cui la rimozione dello storage temporaneo e l'eliminazione dei LUN clonati.

Clonare macchine virtuali

Utilizza SMP per creare cloni di macchine virtuali per lo sviluppo, il test o il provisioning rapido.

Passi

1. Apri la sezione **Proteggi** e seleziona **Clona** dal menu di navigazione a sinistra.
2. Dall'elenco delle macchine virtuali, individua la macchina virtuale desiderata e fai clic su **Clona** nella colonna Azioni.
3. Nella finestra Clone VM, scegli il **Target Node** in cui verrà creato il clone.

▼ Visualizza la finestra di dialogo Clona VM

The screenshot shows the NetApp Storage Manager for Proxmox interface. On the left is a navigation menu with options: Dashboard, Plan, Provision, Protect (selected), Backup, Restore, Clone, Preserve, and Process Logs. The main area displays a summary of resources: 40 VMs, 113 Provisioned Volumes, 1 Resource Group, and 1 Policy. Below this is a table titled '27 VMs' with columns: VMID, Name, Proxmox Cluster, ONTAP Cluster, Protocol, and Actions. The table lists 11 VMs. In the 'Actions' column, the 'Clone' button for each VM is highlighted with a red rectangle.

VMID	Name	Proxmox Cluster	ONTAP Cluster	Protocol	Actions
100	sie-dev-aka-tst-1-89a2e	SMPProxmox-Username	SMPDemo212	NFS	Clone
101	sie-dev-aka-tst-1-fc39f	SMPProxmox-Username	SMPDemo212	NFS	Clone
102	sie-dev-aka-tst-1-ce32c	SMPProxmox-Username	SMPDemo212	NFS	Clone
103	sie-dev-aka-tst-1	SMPProxmox-Username	SMPDemo212	NFS	Clone
104	sie-dev-aka-tst-1-305c7-47f84	SMPProxmox-Username	SMPDemo212	NFS	Clone
105	sie-dev-aka-tst-1-305c7-0754c	SMPProxmox-Username	SMPDemo212	NFS	Clone
106	sie-dev-aka-tst-1-305c7-15aa6	SMPProxmox-Username	SMPDemo212	NFS	Clone
107	sie-dev-aka-tst-1-fabfa-65967	SMPProxmox-Username	SMPDemo212	NFS	Clone
108	sie-dev-aka-tst-1-1fbb1	SMPProxmox-Username	SMPDemo212	NFS	Clone
111	sie-dev-aka-tst-1-350aa	SMPProxmox-Username	SMPDemo212	NFS	Clone

4. Seleziona la **Snapshot** da utilizzare come origine per il clone.



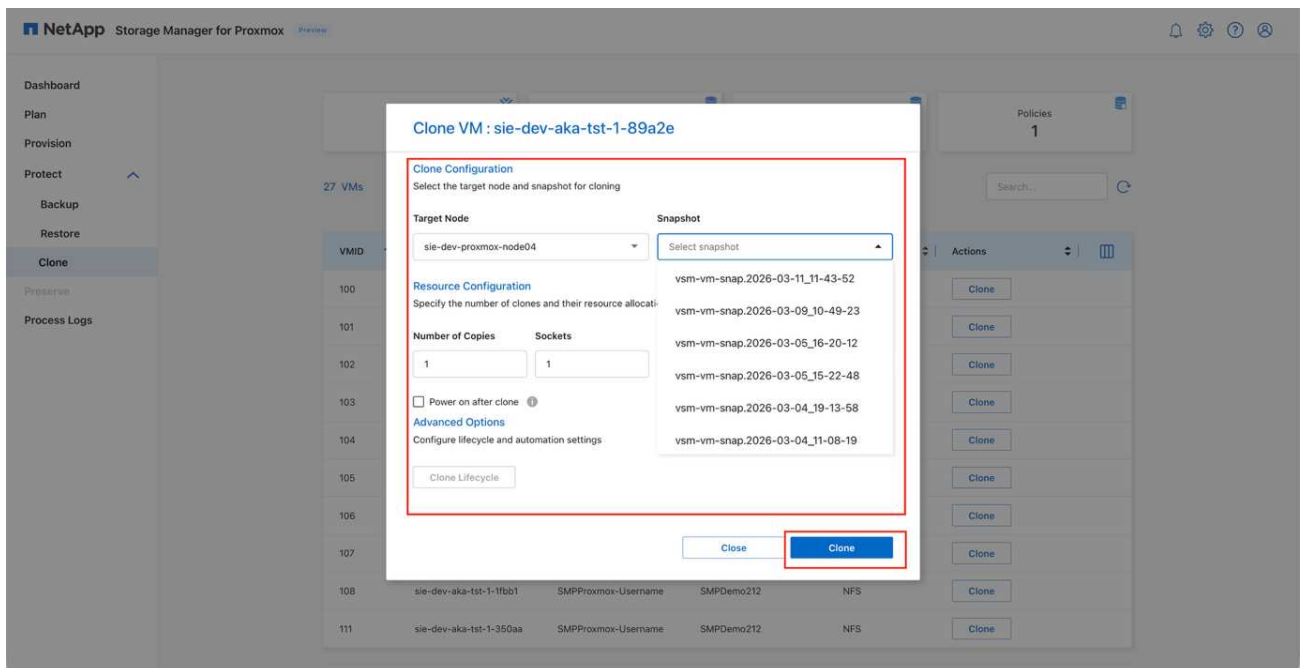
Nella versione attuale, la clonazione viene eseguita sul file system attivo. In una prossima versione, il flusso di lavoro di clonazione consentirà la selezione di uno Snapshot, nel qual

caso i cloni dei file verranno eseguiti utilizzando un nuovo volume creato dallo Snapshot selezionato.

5. Specificare il **numero di copie**, i **core della CPU**, i **socket** e la **memoria** per la macchina virtuale clonata.
6. (Facoltativo) Abilita **Avvia dopo la clonazione** se la macchina virtuale clonata deve avviarsi automaticamente dopo la creazione.
7. (Facoltativo) Selezionare **Crea un nuovo datastore** se il clone deve essere posizionato su un datastore appena creato.
8. Nella sezione **Opzioni avanzate**, abilita **Configurazione di rete** se desideri che le impostazioni di rete vengano applicate automaticamente al clone.
9. Fai clic su **Clona** per avviare il processo di cloning.

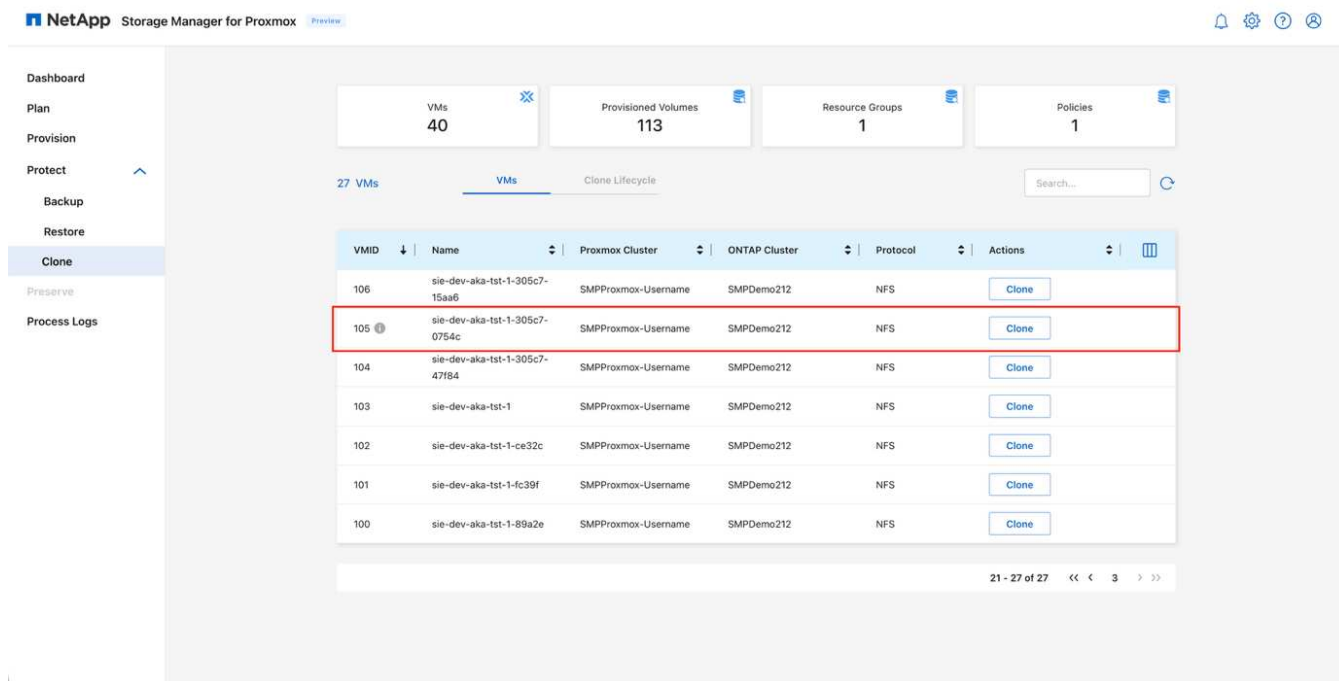
Il flusso di lavoro di clonazione predispone la nuova macchina virtuale utilizzando le API di clonazione rapida di ONTAP e assegna un GUID univoco di cinque cifre all'istanza clonata.

▼ Visualizza l'operazione di clonazione



La macchina virtuale clonata viene visualizzata sia nell'elenco Backup che nell'elenco Clona e può essere protetta utilizzando le policy di backup esistenti. Per rendere visibili le macchine virtuali clonate in questi elenchi, eseguire una scansione dei piani Proxmox e ONTAP.

▼ Visualizza le VM clonate negli elenchi



Dettagli del flusso di lavoro di clonazione

SMP automatizza la clonazione rapida delle macchine virtuali delegando le operazioni più complesse a ONTAP, che esegue cloni lato storage anziché copie di file lato host. A livello interno, SMP sfrutta la semantica FlexClone di ONTAP (cloni basati su snapshot, scrivibili ed efficienti in termini di spazio) in modo che i cloni vengano creati rapidamente e consumino inizialmente poca capacità; inoltre, evita, ove possibile, operazioni di lettura/scrittura dei dati tramite l'host Proxmox.

Questo approccio accelera il provisioning delle macchine virtuali spostando il lavoro di clonazione in ONTAP, fornendo cloni veloci, leggeri ed efficienti in termini di spazio, adatti a Dev/Test, laboratori e cicli di aggiornamento rapidi.

Per impostazione predefinita, la clonazione viene eseguita sul file system attivo. Il flusso di lavoro di clonazione consente anche la selezione di uno Snapshot, nel qual caso i cloni dei file vengono eseguiti utilizzando un nuovo volume creato dallo Snapshot selezionato.

Operazioni di monitoraggio

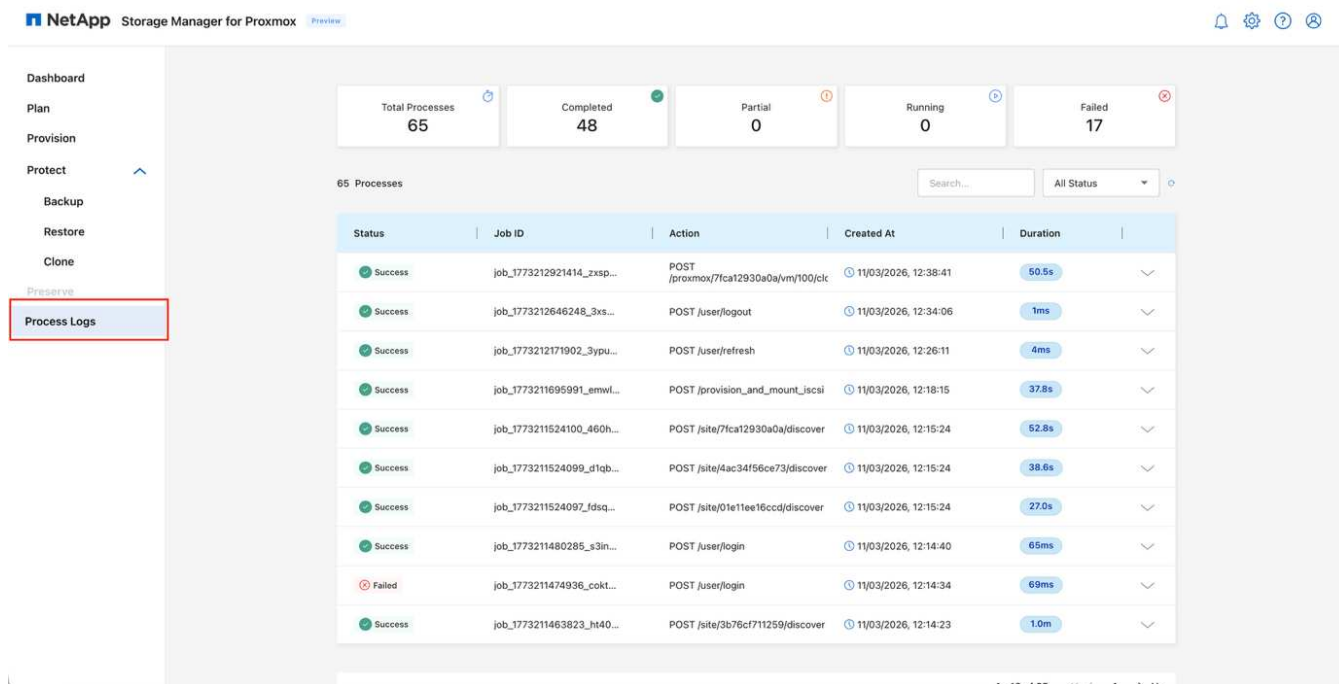
Utilizza le viste Registri di processo e Dashboard per monitorare e tracciare le operazioni SMP.

Registri di processo

La vista Registri processi fornisce un registro consolidato di tutte le operazioni eseguite tramite Storage Manager per Proxmox. Ogni voce mostra lo stato del processo, l'ID del processo, l'azione eseguita, l'ora di inizio e la durata. Ciò semplifica il monitoraggio delle attività completate, l'identificazione di eventuali operazioni non riuscite o incomplete e la revisione della sequenza di azioni eseguite nell'ambiente.

Sono disponibili filtri e opzioni di ricerca per individuare rapidamente job specifici o restringere l'elenco in base allo stato.

▼ Visualizza i registri di processo

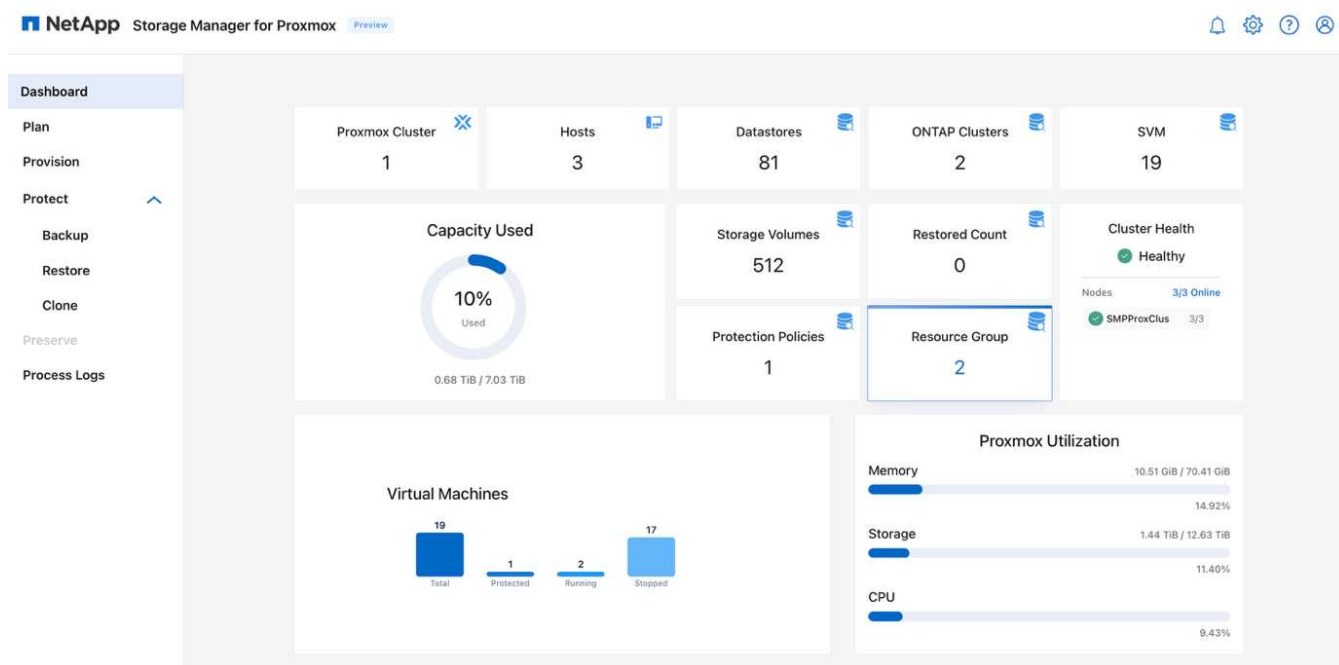


Pannello di controllo

La dashboard offre una panoramica immediata dell'intero ambiente Storage Manager per Proxmox. Riepiloga le informazioni chiave, come il numero di cluster Proxmox, host, datastore, cluster ONTAP e macchine virtuali protette. Vengono inoltre visualizzati l'utilizzo della capacità, i volumi di storage totali, le policy di protezione e i gruppi di risorse, per fornire un quadro chiaro dell'utilizzo del sistema.

Lo stato di salute del cluster è visualizzato in modo evidente, indicando lo stato di tutti i nodi connessi. La sezione inferiore della dashboard evidenzia la distribuzione delle VM (totale, in esecuzione e arrestate) e fornisce l'utilizzo in tempo reale delle risorse Proxmox per memoria, storage e CPU. Questa visualizzazione consente di valutare rapidamente lo stato di salute del sistema, identificare le pressioni sulle risorse e monitorare lo stato operativo generale.

▼ Visualizza la dashboard



Riepilogo

Storage Manager per Proxmox offre un modo semplificato e unificato per gestire le operazioni di protezione, clonazione e ripristino negli ambienti Proxmox. Integrandosi direttamente con ONTAP, la soluzione porta l'efficienza, l'affidabilità e le prestazioni dello storage di livello enterprise nei flussi di lavoro quotidiani delle VM. Le snapshot efficienti in termini di spazio di ONTAP, le capacità di clonazione rapida e la replica integrata offrono una protezione dei dati coerente e prevedibile, mentre SMP semplifica queste funzionalità in un'interfaccia intuitiva e focalizzata sulle attività.

Informazioni sul copyright

Copyright © 2026 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.