



Configura ONTAP tools for VMware vSphere

ONTAP tools for VMware vSphere 105

NetApp
July 24, 2026

Sommario

Configura ONTAP tools for VMware vSphere	1
Aggiungi istanze del server vCenter agli strumenti ONTAP	1
Registrare il provider VASA con un'istanza del server vCenter negli ONTAP tools	2
Installa il plug-in NFS VAAI usando ONTAP tools	3
Configurare le impostazioni dell'host ESXi negli ONTAP tools	4
Configura le impostazioni di multipath e timeout del server ESXi	4
Imposta i valori host di ESXi	4
Configurare i ruoli e i privilegi utente ONTAP per ONTAP tools	5
Requisiti di mappatura degli aggregate SVM	6
Crea manualmente l'utente e il ruolo ONTAP	6
Aggiorna ONTAP tools for VMware vSphere 10.1 user a 10.3 user	15
Aggiorna ONTAP tools for VMware vSphere utente 10.3 a utente 10.4	16
Aggiungi un backend di storage a ONTAP tools	17
Associare un backend di storage a un'istanza del vCenter Server negli ONTAP tools	19
Configurare l'accesso alla rete negli ONTAP tools	19
Creare un datastore in ONTAP tools	20

Configura ONTAP tools for VMware vSphere

Aggiungi istanze del server vCenter agli strumenti ONTAP

Aggiungi istanze vCenter Server a ONTAP tools for VMware vSphere per configurare, gestire e proteggere i tuoi datastore virtuali nell'ambiente vCenter Server. Quando aggiungi più istanze vCenter Server, sono necessari certificati CA personalizzati per una comunicazione sicura tra ONTAP tools e ciascuna istanza vCenter Server.

Informazioni su questa attività

ONTAP tools si integra con vCenter Server per eseguire attività di storage come provisioning, Snapshot e protezione dei dati direttamente dal client vSphere.

L'aggiunta di un'istanza del server vCenter agli ONTAP tools attiva automaticamente le seguenti azioni:

- ONTAP tools registra il plug-in client vCenter come plug-in remoto.
- I privilegi personalizzati per i plug-in e le API vengono applicati all'istanza del server vCenter.
- I ruoli personalizzati vengono creati per gestire gli utenti.
- Il plug-in appare come un collegamento rapido sull'interfaccia utente di vSphere.

Prima di iniziare

- Assicurarsi che il certificato del server vCenter includa un'estensione SAN (Subject Alternative Name) valida con voci sia DNS che indirizzo IP. Per esempio:

```
X509v3 extensions:  
    X509v3 Subject Alternative Name:  
        DNS: vcenter.example.com, DNS: vcenter, IP Address: 192.168.0.50
```

Se il certificato non include un'estensione SAN, o se l'estensione SAN non contiene i valori DNS o di indirizzo IP corretti, le operazioni di ONTAP tools potrebbero non riuscire a causa di errori di convalida del certificato.

- L'identificatore di rete primario (PNID) del vCenter Server deve essere incluso nei dettagli SAN. Il PNID e il nome DNS devono essere identici e risolvibili nel DNS.
- Si raccomanda di distribuire vCenter Server utilizzando il suo fully qualified domain name (FQDN), assicurandosi che il SAN nel certificato includa DNS Name=machine_FQDN per una compatibilità e un supporto ottimali.
- Per ulteriori informazioni, fare riferimento alla documentazione VMware:
 - ["vSphere Certificate Requirements per diversi percorsi di soluzione"](#)
 - ["Sostituisci il certificato SSL della macchina vCenter con un certificato firmato da un'autorità di certificazione personalizzata"](#)
 - ["Errore: il campo Subject Alternate Name \(SAN\) non contiene il PNID. Fornire un certificato valido"](#)



Se l'FQDN non è disponibile, puoi impostare il PNID sull'indirizzo IP e includere l'indirizzo IP nella SAN. Tuttavia, questo non è raccomandato da VMware.

Passaggi

1. Apri un browser web e vai all'URL: `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Accedi con le credenziali di amministratore degli ONTAP tools for VMware vSphere che hai fornito durante la distribuzione.
3. Seleziona **vCenters** > **Aggiungi** per eseguire l'onboarding delle istanze del server vCenter. Fornisci l'indirizzo IP o il nome host vCenter, il nome utente, la password e i dettagli della porta.
4. Nelle opzioni avanzate, recupera automaticamente il certificato del server vCenter (autorizzalo) oppure caricalo manualmente.



Non ti serve un account admin per aggiungere istanze vCenter agli ONTAP tools. Puoi creare un ruolo personalizzato senza l'account admin, con permessi limitati. Consulta "[Usa vCenter Server RBAC con ONTAP tools for VMware vSphere 10](#)" per i dettagli.

Registrare il provider VASA con un'istanza del server vCenter negli ONTAP tools

Usa ONTAP tools for VMware vSphere per registrare il VASA Provider con un'istanza del vCenter Server. Questo abilita la gestione basata su policy dello storage, il supporto vVols e l'integrazione con gli appliance VMware Live Site Recovery sui sistemi ONTAP.

Le impostazioni del provider VASA mostrano lo stato di registrazione per il vCenter Server selezionato.

Passaggi

1. Accedi al vSphere client.
2. Seleziona **Collegamenti** > **NetApp ONTAP tools** nella sezione dei plug-in.
3. Seleziona **Impostazioni** > **Impostazioni del provider VASA**. Gli ONTAP tools visualizzano lo stato di registrazione del VASA Provider come non registrato.
4. Seleziona il pulsante **Registra** per registrare il VASA Provider.
5. Inserisci un nome e le credenziali per il VASA Provider. Il nome utente può contenere solo lettere, numeri e trattini bassi. La password deve essere compresa tra 8 e 256 caratteri.
6. Seleziona **Register**.
7. Dopo una registrazione e un aggiornamento della pagina andati a buon fine, ONTAP tools visualizza lo stato, il nome e la versione del VASA Provider registrato.

Cosa c'è dopo

Verifica che il VASA Provider integrato sia elencato sotto VASA Provider dal client vCenter:

Passaggi

1. Vai all'istanza del server vCenter.
2. Accedi con le credenziali dell'amministratore.
3. Seleziona **Storage Providers** > **Configure**. Verifica che il VASA Provider onboarded sia elencato correttamente.

Installa il plug-in NFS VAAI usando ONTAP tools

Il plug-in NFS vStorage API for Array Integration (NFS VAAI) collega VMware vSphere agli array di storage NFS. Usa ONTAP tools for VMware vSphere per installare il plug-in VAAI. Questo permette all'array di storage NFS di gestire alcune operazioni di storage invece degli host ESXi.

Prima di iniziare

- Scarica il ["NetApp NFS Plug-in per VMware VAAI"](#) pacchetto di installazione.
- Assicurati di disporre di host ESXi con vSphere 7.0 U3 (ultima patch o successiva) e ONTAP 9.14.1 o successiva.
- Monta un datastore NFS.

Passaggi

1. Accedi al vSphere client.
2. Seleziona **Collegamenti** > **NetApp ONTAP tools** nella sezione dei plug-in.
3. Seleziona **Impostazioni** > **NFS VAAI Tools**.
4. Se hai già caricato il plug-in VAAI su vCenter Server, seleziona **Modifica** in **Versione esistente**. Se non lo hai fatto, seleziona **Carica**.
5. Sfoglia e seleziona il `.vib` file e seleziona **Carica** per caricare il file in ONTAP tools.
6. Seleziona **Installa sull'host ESXi**, seleziona l'host ESXi su cui desideri installare il plug-in NFS VAAI e quindi seleziona **Installa**.

Il vSphere Web Client mostra solo gli host ESXi che possono installare il plug-in. Puoi monitorare l'avanzamento dell'installazione nella sezione delle attività recenti.

7. Riavvia manualmente l'host ESXi dopo l'installazione.

Dopo il riavvio dell'host ESXi, ONTAP tools for VMware vSphere rileva e abilita automaticamente il plug-in NFS VAAI.

E ora?

Dopo aver installato il plug-in NFS VAAI e riavviato l'host ESXi, configura le policy di esportazione NFS per l'offload della copia VAAI. Assicurati che le regole della policy di esportazione soddisfino questi requisiti:

- Il volume ONTAP pertinente consente le chiamate NFSv4.
- L'utente root rimane root e NFSv4 è consentito in tutti i volumi padre di giunzione.
- L'opzione per il supporto VAAI è impostata sul server NFS pertinente.

Per ulteriori informazioni, consulta l' ["Configura le policy di esportazione NFS corrette per l'offload della copia VAAI"](#) articolo KB.

Informazioni correlate

["Supporto per VMware vStorage su NFS"](#)

["Abilita o disabilita NFSv4.0"](#)

["Supporto ONTAP per NFSv4.2"](#)

Configurare le impostazioni dell'host ESXi negli ONTAP tools

La configurazione delle impostazioni di multipath e timeout del server ESXi ti aiuta a mantenere la disponibilità e l'integrità dei dati. Ti permette il failover automatico su un percorso di storage per il backup se il percorso primario diventa non disponibile.

Configura le impostazioni di multipath e timeout del server ESXi

ONTAP tools for VMware vSphere verifica e imposta le configurazioni multipath dell'host ESXi e le impostazioni di timeout dell'HBA che funzionano al meglio con i sistemi storage NetApp.

Informazioni su questa attività

Questo processo potrebbe richiedere del tempo, a seconda della configurazione e del carico di sistema. Puoi visualizzare l'avanzamento nel pannello Attività recenti.

Passaggi

1. Dalla home page del client Web vSphere di VMware, seleziona **Host e cluster**.
2. Nella pagina dei collegamenti rapidi del client Web VMware vSphere, seleziona **NetApp ONTAP tools** nella sezione dei plug-in.
3. Vai alla scheda **Conformità host ESXi** nella panoramica (dashboard) del plug-in ONTAP tools for VMware vSphere.
4. Seleziona il link **Applica impostazioni consigliate**.
5. Nella finestra **Applica le impostazioni host consigliate**, seleziona gli host che vuoi aggiornare per usare le impostazioni consigliate NetApp e seleziona **Avanti**.



Puoi espandere l'host ESXi per vedere i valori attuali.

6. Nella pagina delle impostazioni, seleziona i valori consigliati come richiesto.
7. Nel riquadro di riepilogo, verifica i valori e seleziona **Fine**. Puoi monitorare l'avanzamento nel pannello delle attività recenti.

Imposta i valori host di ESXi

Utilizza ONTAP tools for VMware vSphere per impostare timeout e altri valori sugli host ESXi per prestazioni e failover ottimali. Imposta questi valori in base ai test NetApp.

Puoi impostare i seguenti valori su un host ESXi:

Impostazioni dell'adattatore HBA/CNA

Imposta i seguenti parametri sui valori predefiniti:

- Disk.QFullSampleSize
- Disk.QFullThreshold
- Timeout HBA Emulex FC
- Timeout dell'HBA QLogic FC

Impostazioni MPIO

Le impostazioni MPIO scelgono i percorsi migliori per i sistemi di archiviazione NetApp. Le impostazioni MPIO selezionano il percorso migliore e lo utilizzano.

Per ambienti dalle performance elevate o quando testi con un singolo datastore LUN, regola l'impostazione di bilanciamento del carico della policy di selezione del percorso round-robin (VMW_PSP_RR) (PSP) per migliorare le prestazioni. Imposta il valore IOPS predefinito da 1000 a 1.



Le impostazioni MPIO non si applicano ai protocolli NVMe, NVMe/FC e NVMe/TCP.

Impostazioni NFS

Parametro	Imposta questo valore su...
Net.TcpipHeapSize	32
Net.TcpipHeapMax	1024 MB
NFS.MaxVolumes	256
NFS41.MaxVolumes	256
NFS.MaxQueueDepth	128 o superiore
NFS.HeartbeatMaxFailures	10
NFS.HeartbeatFrequency	12
NFS.HeartbeatTimeout	5

Configurare i ruoli e i privilegi utente ONTAP per ONTAP tools

Usa questa sezione per configurare i ruoli utente e i privilegi ONTAP per i backend di storage con ONTAP tools for VMware vSphere e ONTAP System Manager. Puoi assegnare ruoli utilizzando i file JSON forniti, creare manualmente utenti e ruoli e applicare i privilegi minimi richiesti per gli account non admin.

Prima di iniziare

- Scarica il file ONTAP Privileges da ONTAP tools for VMware vSphere usando https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_roles.zip. Dopo aver scaricato il file zip, trovi due file JSON. Usa il file JSON specifico per ASA r2 quando configuri un sistema ASA r2.



Puoi creare utenti a livello di cluster o direttamente a livello di storage virtual machines (SVM). Se non usi il file `user_roles.json`, assicurati che l'utente abbia le autorizzazioni SVM minime richieste.

- Accedi con i privilegi di amministratore al backend di archiviazione.

Passaggi

- Estrai il file https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_roles.zip che hai scaricato.
- Accedi a ONTAP System Manager utilizzando l'indirizzo IP di gestione del cluster.

3. Accedi al cluster con privilegi di amministratore. Per configurare un utente:

- Per configurare un utente degli ONTAP tools per il cluster, seleziona **Cluster > Impostazioni > riquadro Utenti e ruoli**.
- Per configurare un utente ONTAP tools SVM, seleziona **Storage SVM > Impostazioni > riquadro Utenti e ruoli**.
- Seleziona **Aggiungi** sotto Utenti.
- Nella finestra di dialogo **Aggiungi utente**, seleziona **Prodotti di virtualizzazione**.
- Sfoggia** per selezionare e caricare il file JSON ONTAP Privileges. Per i sistemi non-ASA r2, seleziona il file `users_roles.json` e per i sistemi ASA r2, seleziona il file `users_roles_ASAr2.json`.

ONTAP tools compila automaticamente il campo Product.

- Seleziona la funzionalità del prodotto come **VSC, VASA Provider e SRA** dal menu a tendina.

ONTAP tools compila automaticamente il campo **Ruolo** in base alla funzionalità del prodotto che selezioni.

- Inserisci il nome utente e la password richiesti.
- Seleziona i privilegi (Rilevamento, Crea Storage, Modifica Storage, Elimina Storage, Ruolo NAS/SAN) di cui l'utente ha bisogno, quindi seleziona **Aggiungi**.

ONTAP tools aggiunge il nuovo ruolo e il nuovo utente. Puoi visualizzare i privilegi sotto il ruolo che hai configurato.

Requisiti di mappatura degli aggregate SVM

Quando esegui il provisioning dei datastore utilizzando le credenziali utente SVM, ONTAP tools for VMware vSphere crea volumi sull'aggregate specificato nell'API POST dei datastore. ONTAP impedisce agli utenti SVM di creare volumi su aggregate non mappati all'SVM. Mappa l'SVM agli aggregate richiesti utilizzando l'API REST o la CLI di ONTAP prima di creare i volumi.

API REST:

```
PATCH "/api/svm/svms/f16f0935-5281-11e8-b94d-005056b46485"
'{"aggregates":{"name":["aggr1","aggr2","aggr3"]}}'
```

CLI di ONTAP:

```
sti115_vsim_ucs630f_aggr1 vserver show-aggregates
AvailableVserver      Aggregate      State          Size Type      SnapLock
Type-----
-----svm_test      sti115_vsim_ucs630f_aggr1
online      10.11GB vmdisk  non-snaplock
```

Crea manualmente l'utente e il ruolo ONTAP

Crea utenti e ruoli manualmente senza il file JSON.

1. Accedi a ONTAP System Manager utilizzando l'indirizzo IP di gestione del cluster.
2. Accedi al cluster con privilegi di amministratore.
 - a. Per configurare i ruoli degli ONTAP tools per il cluster, seleziona **Cluster > Impostazioni > Utenti e ruoli**.
 - b. Per configurare i ruoli degli strumenti ONTAP SVM del cluster, seleziona **Storage SVM > Impostazioni > Utenti e ruoli**.
3. Crea ruoli:
 - a. Seleziona **Aggiungi** nella tabella **Ruoli**.
 - b. Inserisci i dettagli relativi al **nome del ruolo** e agli **attributi del ruolo**.

 Aggiungi il **Percorso REST API** e scegli l'accesso dall'elenco a discesa.
 - c. Aggiungi tutte le API necessarie e salva le modifiche.
4. Crea utenti:
 - a. Seleziona **Aggiungi** nella tabella **Users**.
 - b. Nella finestra di dialogo **Aggiungi utente**, seleziona **System Manager**.
 - c. Inserisci il **nome utente**.
 - d. Seleziona **Role** tra le opzioni create nella fase **Create Roles** descritta sopra.
 - e. Inserisci le applicazioni a cui desideri concedere l'accesso e il metodo di autenticazione. ONTAPI e HTTP sono le applicazioni richieste e il tipo di autenticazione è **Password**.
 - f. Imposta la **password per l'utente** e **salva** l'utente.

Elenco dei privilegi minimi richiesti per un utente cluster con ambito globale non amministratore

Questa pagina elenca i privilegi minimi richiesti per un utente di cluster con ambito globale non amministratore senza un file JSON. Se un cluster è in ambito locale, usa il file JSON per creare gli utenti perché ONTAP tools for VMware vSphere richiede più dei soli privilegi di lettura per il provisioning su ONTAP.

Puoi accedere alla funzionalità tramite le API:

API	Livello di accesso	Utilizzato per
/api/cluster	Sola lettura	Rilevamento della configurazione del cluster
/api/cluster/licensing/licenses	Sola lettura	Verifica delle licenze specifiche del protocollo
/api/cluster/nodes	Sola lettura	Rilevamento del tipo di piattaforma
/api/security/accounts	Sola lettura	Scoperta dei privilegi
/api/security/roles	Sola lettura	Scoperta dei privilegi
/api/storage/aggregates	Sola lettura	Verifica dello spazio aggregato durante il provisioning del datastore/volume
/api/storage/cluster	Sola lettura	Per ottenere i dati relativi allo spazio e all'efficienza a livello di cluster

/api/storage/disks	Sola lettura	Per ottenere i dischi associati in un aggregato
/api/storage/qos/policies	Leggi/Crea/Modifica	Gestione delle policy QoS e VM
/api/svm/svms	Sola lettura	Per ottenere la configurazione SVM quando il cluster viene aggiunto localmente.
/api/network/ip/interfaces	Sola lettura	Aggiungi backend di archiviazione - Per identificare l'ambito della LIF di gestione è cluster/SVM
/api/storage/availability-zones	Sola lettura	Rilevamento SAZ. Applicabile alla release ONTAP 9.16.1 e successive e ai sistemi ASA r2.
/api/cluster/metrocluster	Sola lettura	Recupera lo stato e i dettagli di configurazione di MetroCluster.

Crea un utente con ambito cluster basato su API ONTAP per ONTAP tools for VMware vSphere



Per le operazioni PATCH e il rollback automatico sui datastore sono necessari i privilegi di discovery, create, modify e destroy. La mancanza di tali privilegi potrebbe causare problemi al workflow e alla pulizia.

Un utente basato su API ONTAP con privilegi di individuazione, creazione, modifica ed eliminazione può gestire i workflow degli ONTAP tools.

Per creare un utente con ambito cluster dotato di tutti i privilegi sopra menzionati, esegui i seguenti comandi:

```
security login rest-role create -role <role-name> -api
/api/application/consistency-groups -access all

security login rest-role create -role <role-name> -api
/api/private/cli/snapmirror -access all

security login rest-role create -role <role-name> -api
/api/protocols/nfs/export-policies -access all

security login rest-role create -role <role-name> -api
/api/protocols/nvme/subsystem-maps -access all

security login rest-role create -role <role-name> -api
/api/protocols/nvme/subsystems -access all

security login rest-role create -role <role-name> -api
/api/protocols/san/igroups -access all

security login rest-role create -role <role-name> -api
/api/protocols/san/lun-maps -access all
```

```

security login rest-role create -role <role-name> -api
/api/protocols/san/vvol-bindings -access all

security login rest-role create -role <role-name> -api
/api/snapmirror/relationships -access all

security login rest-role create -role <role-name> -api
/api/storage/volumes -access all

security login rest-role create -role <role-name> -api
"/api/storage/volumes/*/snapshots" -access all

security login rest-role create -role <role-name> -api /api/storage/luns
-access all

security login rest-role create -role <role-name> -api
/api/storage/namespaces -access all

security login rest-role create -role <role-name> -api
/api/storage/qos/policies -access all

security login rest-role create -role <role-name> -api
/api/cluster/schedules -access read_create

security login rest-role create -role <role-name> -api
/api/snapmirror/policies -access read_create

security login rest-role create -role <role-name> -api
/api/storage/file/clone -access read_create

security login rest-role create -role <role-name> -api
/api/storage/file/copy -access read_create

security login rest-role create -role <role-name> -api
/api/support/ems/application-logs -access read_create

security login rest-role create -role <role-name> -api
/api/protocols/nfs/services -access read_modify

security login rest-role create -role <role-name> -api /api/cluster
-access readonly

security login rest-role create -role <role-name> -api /api/cluster/jobs
-access readonly

security login rest-role create -role <role-name> -api

```

```

/api/cluster/licensing/licenses -access readonly

security login rest-role create -role <role-name> -api /api/cluster/nodes
-access readonly

security login rest-role create -role <role-name> -api /api/cluster/peers
-access readonly

security login rest-role create -role <role-name> -api /api/name-
services/name-mappings -access readonly

security login rest-role create -role <role-name> -api
/api/network/ethernet/ports -access readonly

security login rest-role create -role <role-name> -api
/api/network/fc/interfaces -access readonly

security login rest-role create -role <role-name> -api
/api/network/fc/logins -access readonly

security login rest-role create -role <role-name> -api
/api/network/fc/ports -access readonly

security login rest-role create -role <role-name> -api
/api/network/ip/interfaces -access readonly

security login rest-role create -role <role-name> -api
/api/protocols/nfs/kerberos/interfaces -access readonly

security login rest-role create -role <role-name> -api
/api/protocols/nvme/interfaces -access readonly

security login rest-role create -role <role-name> -api
/api/protocols/san/fcp/services -access readonly

security login rest-role create -role <role-name> -api
/api/protocols/san/iscsi/services -access readonly

security login rest-role create -role <role-name> -api
/api/security/accounts -access readonly

security login rest-role create -role <role-name> -api /api/security/roles
-access readonly

security login rest-role create -role <role-name> -api
/api/storage/aggregates -access readonly

```

```
security login rest-role create -role <role-name> -api
/api/storage/cluster -access readonly

security login rest-role create -role <role-name> -api /api/storage/disks
-access readonly

security login rest-role create -role <role-name> -api /api/storage/qtrees
-access readonly

security login rest-role create -role <role-name> -api
/api/storage/quota/reports -access readonly

security login rest-role create -role <role-name> -api
/api/storage/snapshot-policies -access readonly

security login rest-role create -role <role-name> -api /api/svm/peers
-access readonly

security login rest-role create -role <role-name> -api /api/svm/svms
-access readonly

security login rest-role create -role <role-name> -api
/api/cluster/metrocluster -access readonly
```

Inoltre, per le versioni di ONTAP 9.16.0 e successive, eseguire il seguente comando:

```
security login rest-role create -role <role-name> -api
/api/storage/storage-units -access all
```

Per i sistemi ASA r2 con versioni di ONTAP 9.16.1 e successive, eseguire il seguente comando:

```
security login rest-role create -role <role-name> -api
/api/storage/availability-zones -access readonly
```

Crea un utente SVM con ambito basato su API ONTAP per ONTAP tools for VMware vSphere

Esegui i seguenti comandi per creare un utente con ambito SVM e tutti i privilegi:

```
security login rest-role create -role <role-name> -api
/api/application/consistency-groups -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/private/cli/snapmirror -access all -vserver <vserver-name>
```

```

security login rest-role create -role <role-name> -api
/api/protocols/nfs/export-policies -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/nvme/subsystem-maps -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/nvme/subsystems -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/san/igroups -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/san/lun-maps -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/san/vvol-bindings -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/snapmirror/relationships -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/volumes -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
"/api/storage/volumes/*/snapshots" -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/storage/luns
-access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/namespaces -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/cluster/schedules -access read_create -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/snapmirror/policies -access read_create -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/file/clone -access read_create -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/file/copy -access read_create -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/support/ems/application-logs -access read_create -vserver <vserver-

```

name>

```
security login rest-role create -role <role-name> -api  
/api/protocols/nfs/services -access read_modify -vserver <vserver-name>
```

```
security login rest-role create -role <role-name> -api /api/cluster  
-access readonly -vserver <vserver-name>
```

```
security login rest-role create -role <role-name> -api /api/cluster/jobs  
-access readonly -vserver <vserver-name>
```

```
security login rest-role create -role <role-name> -api /api/cluster/peers  
-access readonly -vserver <vserver-name>
```

```
security login rest-role create -role <role-name> -api /api/name-  
services/name-mappings -access readonly -vserver <vserver-name>
```

```
security login rest-role create -role <role-name> -api  
/api/network/ethernet/ports -access readonly -vserver <vserver-name>
```

```
security login rest-role create -role <role-name> -api  
/api/network/fc/interfaces -access readonly -vserver <vserver-name>
```

```
security login rest-role create -role <role-name> -api  
/api/network/fc/logins -access readonly -vserver <vserver-name>
```

```
security login rest-role create -role <role-name> -api  
/api/network/ip/interfaces -access readonly -vserver <vserver-name>
```

```
security login rest-role create -role <role-name> -api  
/api/protocols/nfs/kerberos/interfaces -access readonly -vserver <vserver-  
name>
```

```
security login rest-role create -role <role-name> -api  
/api/protocols/nvme/interfaces -access readonly -vserver <vserver-name>
```

```
security login rest-role create -role <role-name> -api  
/api/protocols/san/fcp/services -access readonly -vserver <vserver-name>
```

```
security login rest-role create -role <role-name> -api  
/api/protocols/san/iscsi/services -access readonly -vserver <vserver-name>
```

```
security login rest-role create -role <role-name> -api  
/api/security/accounts -access readonly -vserver <vserver-name>
```

```
security login rest-role create -role <role-name> -api /api/security/roles  
-access readonly -vserver <vserver-name>
```

```
security login rest-role create -role <role-name> -api /api/storage/qtrees
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/quota/reports -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/snapshot-policies -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/svm/peers
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/svm/svms
-access readonly -vserver <vserver-name>
```

Inoltre, per le versioni di ONTAP 9.16.0 e successive, eseguire il seguente comando:

```
security login rest-role create -role <role-name> -api
/api/storage/storage-units -access all -vserver <vserver-name>
```

Per creare un nuovo utente basato su API utilizzando i ruoli basati su API creati in precedenza, eseguire il seguente comando:

```
security login create -user-or-group-name <user-name> -application http
-authentication-method password -role <role-name> -vserver <cluster-or-
vserver-name>
```

Esempio:

```
security login create -user-or-group-name testvpsraall -application http
-authentication-method password -role
OTV_10_VP_SRA_Discovery_Create_Modify_Destroy -vserver C1_stil60-cluster_
```

Esegui il seguente comando per sbloccare l'account e abilitare l'accesso all'interfaccia di gestione:

```
security login unlock -user <user-name> -vserver <cluster-or-vserver-name>
```

Esempio:

```
security login unlock -username testvpsraall -vserver C1_stil60-cluster
```


Aggiorna ONTAP tools for VMware vSphere 10.1 user a 10.3 user

Per gli utenti di ONTAP tools for VMware vSphere 10.1 con un utente a livello di cluster creato tramite file JSON, usa i seguenti comandi ONTAP CLI con privilegi admin per eseguire l'aggiornamento alla release 10.3.

Per le funzionalità del prodotto:

- VSC
- VSC e VASA Provider
- VSC e SRA
- VSC, VASA Provider e SRA.

Privilegi del cluster:

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme namespace show" -access all
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem show" -access all
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host show" -access all
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map show" -access all
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme show-interface" -access read
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host add" -access all
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map add" -access all
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme namespace delete" -access all
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem delete" -access all
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host remove" -access all
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map remove" -access all
```

Per gli utenti di ONTAP tools for VMware vSphere 10.1 con un utente con ambito SVM creato tramite file json, usa i comandi CLI di ONTAP con privilegi di amministratore per eseguire l'aggiornamento alla release 10.3.

Privilegi SVM:

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme namespace show" -access all -vserver <vserver-name>
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem show" -access all -vserver <vserver-name>
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host show"  
-access all -vserver <vserver-name>
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map show"  
-access all -vserver <vserver-name>
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme show-interface" -access read  
-vserver <vserver-name>
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host add" -access  
all -vserver <vserver-name>
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map add" -access  
all -vserver <vserver-name>
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme namespace delete" -access  
all -vserver <vserver-name>
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem delete" -access all  
-vserver <vserver-name>
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host remove"  
-access all -vserver <vserver-name>
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map remove"  
-access all -vserver <vserver-name>
```

Per abilitare i seguenti comandi, aggiungi i comandi *vserver nvme namespace show* e *vserver nvme subsystem show* al ruolo esistente.

```
vserver nvme namespace create  
  
vserver nvme namespace modify  
  
vserver nvme subsystem create  
  
vserver nvme subsystem modify
```

Aggiorna ONTAP tools for VMware vSphere utente 10.3 a utente 10.4

A partire da ONTAP 9.16.1, aggiorna l'utente di ONTAP tools for VMware vSphere 10.3 a utente 10.4.

Per ONTAP tools for VMware vSphere 10.3, se hai un utente con ambito cluster creato tramite file JSON e versione di ONTAP 9.16.1 o superiore, usa il comando ONTAP CLI con privilegi di amministratore per eseguire l'aggiornamento alla release 10.4.

Per le funzionalità del prodotto:

- VSC
- VSC e VASA Provider
- VSC e SRA

- VSC, VASA Provider e SRA.

Privilegi del cluster:

```
security login role create -role <existing-role-name> -cmddirname "storage  
availability-zone show" -access all
```

Aggiungi un backend di storage a ONTAP tools

Usa ONTAP tools per VMware vSphere per aggiungere e gestire i backend di storage per i tuoi host ESXi. Puoi aggiungere cluster o SVM, abilitare il supporto MetroCluster e convalidare i certificati per una connettività sicura. Puoi configurare i backend di storage usando ONTAP tools Manager o il client vSphere, monitorare lo stato dei certificati e riscoprire manualmente le risorse dopo le modifiche al cluster.

Per aggiungere un backend di storage in locale, usa le credenziali del cluster o dell'SVM nell'interfaccia di ONTAP tools. I backend di storage locali sono disponibili solo per il vCenter Server selezionato. ONTAP tools mappa gli SVM al vCenter Server per la gestione dei datastore vVols o VMFS. Per i datastore VMFS e i workflow SRA, puoi usare le credenziali dell'SVM senza mappare un cluster a livello globale.

Per aggiungere un backend di storage globale, usa le credenziali del cluster ONTAP in ONTAP tools Manager. I backend di storage globali abilitano i workflow di discovery per identificare le risorse del cluster necessarie per la gestione dei vVol. Negli ambienti multi-tenant, puoi aggiungere localmente un utente SVM per gestire i datastore vVols.

Consultare l'articolo della Knowledge Base: ["OTV 10: Cos'è l'ambito globale e locale del backend di archiviazione"](#) per ulteriori informazioni sui backend di archiviazione globali e locali.

Se il supporto MetroCluster è abilitato in ONTAP, integra sia il cluster di origine che quello di destinazione come backend di storage locali o globali.

Prima di iniziare

Verifica che il certificato includa un campo Subject Alternative Name (SAN) valido. I sistemi ONTAP utilizzano il campo SAN per identificare le LIF di gestione del cluster e delle SVM.

Usare ONTAP tools Manager



In una configurazione multi-tenant, puoi aggiungere un cluster di backend dello storage a livello globale e SVM a livello locale per usare le credenziali utente di SVM.

Passaggi

1. Avvia ONTAP tools Manager da un browser web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Accedi con le credenziali di amministratore degli ONTAP tools for VMware vSphere che hai fornito durante la distribuzione.
3. Seleziona **Storage Backends** dalla barra laterale.
4. Aggiungi il backend di storage e fornisci l'indirizzo IP del server o il FQDN, il nome utente e la password.



Sono supportate le LIF di gestione degli indirizzi IPv4 e IPv6.

5. Recupera automaticamente i certificati del cluster ONTAP e autorizza il certificato, oppure caricalo manualmente accedendo alla sua posizione.



Se necessario, puoi disabilitare la convalida del Subject Alternative Name (SAN) dalla console di manutenzione. Per istruzioni, vedi ["Modifica il flag di convalida del certificato"](#).

6. Se il backend di storage che aggiungi fa parte di una configurazione MetroCluster, ONTAP tools Manager mostra un messaggio pop-up per aggiungere il cluster peer. Seleziona **Aggiungi** e inserisci i dettagli per il backend di storage peer MetroCluster.



Dopo che il sistema ONTAP ha eseguito uno switchover e uno switchback, esegui manualmente la discovery degli ONTAP tools.

Utilizzando l'interfaccia utente del client vSphere



I datastore vVols non supportano l'aggiunta diretta di un utente SVM tramite l'interfaccia utente client vSphere.

1. Accedi al vSphere client.
2. Nella pagina dei collegamenti rapidi, seleziona **NetApp ONTAP tools** nella sezione dei plug-in.
3. Seleziona **Storage Backends** dalla barra laterale.
4. Aggiungi il backend di storage e fornisci l'indirizzo IP del server, il nome utente, la password e i dettagli della porta.



Puoi aggiungere un backend di storage utilizzando credenziali basate su cluster con LIF di gestione IPv4 o IPv6. Per aggiungere direttamente un utente SVM, fornisci credenziali basate su SVM insieme a un LIF di gestione SVM. Se un cluster è già stato integrato, non puoi integrare nuovamente un utente SVM da quel cluster.

5. Recupera automaticamente i certificati del cluster ONTAP e autorizza il certificato, oppure caricalo manualmente accedendo alla sua posizione.

6. Se il backend di storage aggiunto fa parte della configurazione MetroCluster, ONTAP tools visualizza la schermata **Add MetroCluster peer**. Seleziona **Add peer** per aggiungere il backend di storage peer.



Dopo che il sistema ONTAP ha eseguito uno switchover e uno switchback, esegui manualmente la discovery degli ONTAP tools.

ONTAP tools elenca il nuovo storage backend aggiunto nella pagina **Storage backends**. Se un certificato scade entro 30 giorni o meno, ONTAP tools mostra un avviso nella colonna della data di scadenza del certificato. Dopo la scadenza, ONTAP tools segna lo storage backend come sconosciuto perché non può connettersi al sistema storage.

Informazioni correlate

["OTV 10: Cos'è l'ambito globale e locale del backend di archiviazione"](#)

["Configurare i cluster in una configurazione MetroCluster"](#)

Associare un backend di storage a un'istanza del vCenter Server negli ONTAP tools

Associa un backend di storage a un'istanza vCenter Server per consentire l'accesso a tutte le istanze vCenter Server. Per la configurazione MetroCluster, quando associ un cluster di backend di storage, assicurati di associare anche il relativo cluster peer al vCenter Server.

Passaggi

1. Avvia ONTAP tools Manager da un browser web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Accedi con le credenziali di amministratore degli ONTAP tools for VMware vSphere che hai fornito durante la distribuzione.
3. Seleziona vCenter dalla barra laterale.
4. Seleziona i puntini di sospensione verticali accanto all'istanza del vCenter Server che vuoi connettere ai backend di storage.
5. Dal menu a tendina, scegli il backend di storage che vuoi associare all'istanza di vCenter Server selezionata.

Configurare l'accesso alla rete negli ONTAP tools

Per impostazione predefinita, tutti gli indirizzi IP rilevati dall'host ESXi vengono aggiunti automaticamente alla policy di esportazione, a meno che tu non configuri l'accesso di rete. Puoi modificare la policy di esportazione per consentire l'accesso solo da specifici indirizzi IP. Se un host ESXi escluso tenta un'operazione di mount, l'operazione fallisce.

Passaggi

1. Accedi al vSphere client.
2. Seleziona **NetApp ONTAP tools** nella pagina dei collegamenti rapidi, nella sezione dei plug-in.

3. Nel riquadro sinistro di ONTAP tools, vai su **Impostazioni > Gestisci accesso alla rete > Modifica**.

Per aggiungere più indirizzi IP, separa l'elenco con virgole, intervalli, Classless Inter-Domain Routing (CIDR) o una combinazione di tutti e tre.

4. Seleziona **Salva**.

Creare un datastore in ONTAP tools

Quando crei un datastore a livello di cluster host, ONTAP tools lo monta su tutti gli host di destinazione e abilita l'azione solo se hai i privilegi necessari.

Interoperabilità tra datastore nativi con vCenter Server e datastore gestiti dagli ONTAP tools

A partire da ONTAP tools per VMware vSphere 10.4, ONTAP tools crea igroup nidificati per i datastore, con igroup padre specifici per i datastore e igroup figlio mappati agli host. Puoi creare igroup flat da ONTAP System Manager e usarli per creare datastore VMFS senza usare ONTAP tools. Consulta ["Gestisci gli iniziatori SAN e gli igroup"](#) per ulteriori informazioni.

Dopo aver integrato lo storage ed eseguito il rilevamento dei datastore, ONTAP tools converte gli igroup flat nei datastore VMFS in igroup nidificati. Non puoi utilizzare gli igroup flat precedenti per creare nuovi datastore. Usa l'interfaccia di ONTAP tools o la REST API per riutilizzare gli igroup nidificati.

Crea un datastore vVols

A partire da ONTAP tools for VMware vSphere 10.3, puoi creare un datastore vVols su sistemi ASA r2 con efficienza dello spazio impostata su thin vVol. Il VASA Provider crea un container e gli endpoint di protocollo desiderati durante la creazione del datastore vVol. Il VASA Provider non assegna alcun volume di supporto a questo container.

Prima di iniziare

- Assicurarsi che gli aggregati radice non siano mappati sull'SVM.
- Assicurati che il VASA Provider sia registrato con il vCenter selezionato.
- Nel sistema storage ASA r2, l'SVM deve essere mappato all'aggregato per l'utente SVM.

Passaggi

1. Accedi al vSphere client.
2. Fai clic con il pulsante destro del mouse su un sistema host, un cluster o un data center e seleziona **NetApp ONTAP tools > Create Datastore**.
3. Selezionare vVols come **Tipo di archivio dati**.
4. Inserisci il **nome del datastore** e le informazioni sul **protocollo**.



Il sistema ASA r2 supporta i protocolli iSCSI e FC per vVols.

5. Seleziona la storage VM in cui vuoi creare il datastore.
6. Nelle opzioni avanzate:
 - Se selezioni la **Custom export policy**, assicurati di eseguire il rilevamento in vCenter per tutti gli oggetti. Si consiglia di non usare questa opzione.
 - È possibile selezionare un nome **Custom initiator group** per i protocolli iSCSI e FC.



Nel sistema storage ASA di tipo SVM, le unità di storage (LUN/namespace) non vengono create perché il datastore è solo un container logico.

7. Nel riquadro **Attributi di archiviazione**, puoi creare nuovi volumi o utilizzare quelli esistenti. Tuttavia, non puoi combinare questi due tipi di volumi per creare un datastore vVols.

Quando si crea un nuovo volume, è possibile abilitare il QoS sul datastore. Per impostazione predefinita, viene creato un volume per ogni richiesta di creazione di LUN. Saltare questo passaggio per i datastore vVols sui sistemi di storage ASA r2.

8. Rivedi la tua selezione nel riquadro **Riepilogo** e seleziona **Fine**.

Crea un datastore NFS

Un datastore NFS collega gli host ESXi allo storage condiviso utilizzando il protocollo NFS. Sono semplici e flessibili e vengono utilizzati negli ambienti VMware vSphere.

Passaggi

1. Accedi al vSphere client.
2. Fai clic con il pulsante destro del mouse su un sistema host, un cluster o un data center e seleziona **NetApp ONTAP tools > Create datastore**.
3. Seleziona NFS nel campo **Tipo di datastore**.

4. Nel riquadro **Nome e protocollo**, inserisci il nome del datastore, le dimensioni e le informazioni sul protocollo. Nelle opzioni avanzate, seleziona **Datastore cluster** e **Kerberos authentication**.



L'autenticazione Kerberos è disponibile solo quando il protocollo NFS 4.1 è selezionato.

5. Nel riquadro **Storage**, seleziona **Platform** e **Storage VM**.
6. Se selezioni **Custom export policy** nelle opzioni avanzate, esegui la discovery in vCenter per tutti gli oggetti. Si consiglia di non usare questa opzione.



Non puoi creare un datastore NFS utilizzando la policy predefinita o di volume root della SVM.

- Nelle opzioni avanzate, il pulsante di attivazione **Asimmetrico** è visibile solo se sono selezionate prestazioni o capacità nel menu a tendina della piattaforma.
 - Quando scegli l'opzione **Any** nel menu a tendina della piattaforma, puoi vedere tutti gli SVM nel vCenter. La piattaforma e il flag asimmetrico non influiscono sulla visibilità.
7. Seleziona l'aggregato per la creazione del volume nel riquadro **Attributi di storage**. Nelle opzioni avanzate, scegli **Riserva spazio** e **Abilita QoS** come richiesto.
8. Rivedi le selezioni nel riquadro **Riepilogo** e seleziona **Fine**.

ONTAP tools crea il datastore NFS e lo monta su tutti gli host.

Crea un datastore VMFS

VMFS è un file system cluster per l'archiviazione dei file delle macchine virtuali. Più host ESXi possono accedere simultaneamente agli stessi file VM per le funzionalità vMotion e High Availability.

Su un cluster protetto:

- Puoi creare solo datastore VMFS. Aggiungendo un datastore VMFS a un cluster protetto, viene automaticamente protetto.
- Non puoi creare un datastore in un data center con uno o più cluster host protetti.
- Non puoi creare un datastore su un host ESXi se il cluster host principale è protetto da una "Automated Failover Duplex policy" (configurazione uniforme o non uniforme).
- Puoi creare un datastore VMFS solo su un host ESXi protetto da una relazione asincrona. Non puoi creare e montare un datastore su un host ESXi che fa parte di un cluster protetto dalla policy "Automated Failover Duplex".

Prima di iniziare

- Abilita i servizi e i LIF per ciascun protocollo sul lato storage ONTAP.
- Mappa SVM all'aggregato per l'utente SVM nel sistema storage ASA.
- Configura l'host ESXi se usi il protocollo NVMe/TCP:
 - a. Esaminare il ["Guida alla compatibilità VMware"](#)



VMware vSphere 7.0 U3 e versioni successive supportano il protocollo NVMe/TCP. Tuttavia, si consiglia di utilizzare VMware vSphere 8.0 e versioni successive.

- b. Verifica se il fornitore della scheda di interfaccia di rete (NIC) supporta la NIC ESXi con il

protocollo NVMe/TCP.

- c. Configura la scheda di rete ESXi per NVMe/TCP secondo le specifiche del fornitore della scheda di rete.
 - d. Quando si utilizza VMware vSphere 7, seguire le istruzioni sul sito VMware ["Configura il binding VMkernel per l'adattatore NVMe over TCP"](#) per configurare il binding della porta NVMe/TCP. Quando si utilizza VMware vSphere 8, seguire ["Configurare NVMe over TCP su ESXi"](#) per configurare il binding della porta NVMe/TCP.
 - e. Per la release di VMware vSphere 7, segui le istruzioni nella pagina ["Abilita gli adattatori software NVMe over RDMA o NVMe over TCP"](#) per configurare gli adattatori software NVMe/TCP. Per la release di VMware vSphere 8, segui ["Aggiungi adattatori software NVMe over RDMA o NVMe over TCP"](#) per configurare gli adattatori software NVMe/TCP.
 - f. Eseguire ["Scopri i sistemi storage e gli host"](#) l'azione sull'host ESXi. Per ulteriori informazioni, consulta ["Come configurare NVMe/TCP con vSphere 8.0 Update 1 e ONTAP 9.13.1 per i datastore VMFS"](#).
- Se usi il protocollo NVMe/FC, segui questi passaggi per configurare l'host ESXi:
 - a. Se non è già abilitato, abilita NVMe over Fabrics (NVMe-oF) sul tuo host ESXi.
 - b. Zonizzazione SCSI completa.
 - c. Assicurati che gli host ESXi e il sistema ONTAP siano connessi sia a livello fisico che logico.

Per configurare un ONTAP SVM per il protocollo FC, fare riferimento a ["Configura un SVM per FC"](#).

Per ulteriori informazioni sull'utilizzo del protocollo NVMe/FC con VMware vSphere 8.0, fare riferimento a ["Configurazione host NVMe-oF per ESXi 8.x con ONTAP"](#).

Per ulteriori informazioni sull'utilizzo di NVMe/FC con VMware vSphere 7.0, fare riferimento a ["Guida alla configurazione dell'host ONTAP NVMe/FC"](#) e ["TR-4684"](#).

Passaggi

1. Accedi al vSphere client.
2. Fai clic con il pulsante destro del mouse su un sistema host, un cluster o un data center e seleziona **NetApp ONTAP tools > Create Datastore**.
3. Selezionare il tipo di datastore VMFS.
4. Nel riquadro **Nome e protocollo**, inserisci il nome, le dimensioni e le informazioni sul protocollo del datastore. Per aggiungere il nuovo datastore a un cluster VMFS esistente, seleziona il cluster di datastore in Opzioni avanzate.
5. Seleziona una VM di archiviazione nel riquadro **Archiviazione**. Fornisci il **Custom initiator group name** nella sezione **Advanced options** se necessario. Puoi scegliere un igroup esistente per il datastore oppure crearne uno nuovo con un nome personalizzato.

Quando selezioni il protocollo NVMe/FC o NVMe/TCP, viene creato un nuovo sottosistema di namespace che viene utilizzato per la mappatura dei namespace. ONTAP tools crea il sottosistema di namespace utilizzando il nome generato automaticamente che include il nome del datastore. Puoi rinominare il sottosistema di namespace nel campo **custom namespace subsystem name** nelle opzioni avanzate del pannello **Storage**.

6. Dal riquadro **attributi dello storage**:
 - a. Seleziona **Aggregate** dal menu a tendina.



Per i sistemi di storage ASA r2, l'opzione **Aggregate** non viene visualizzata perché lo storage è disaggregato. Quando scegli un sistema di storage ASA r2 di tipo SVM, la pagina degli attributi di storage mostra le opzioni per abilitare il QoS.

- b. Gli strumenti ONTAP creano un'unità di archiviazione (LUN/Namespace) con una riserva di spazio ridotta in base al protocollo selezionato.



A partire da ONTAP 9.16.1, i sistemi storage ASA r2 supportano fino a 12 nodi per cluster.

- c. Seleziona il **livello di servizio Prestazioni** per i sistemi storage ASA r2 con SVM a 12 nodi che fanno parte di un cluster eterogeneo. Questa opzione non è disponibile se l'SVM selezionato è un cluster omogeneo o utilizza un utente SVM.

'Any' è il valore predefinito del livello di servizio prestazionale (PSL). Questa impostazione crea l'unità di storage utilizzando l'algoritmo di posizionamento bilanciato di ONTAP. Tuttavia, puoi selezionare l'opzione "performance" o "extreme" a seconda delle esigenze.

- d. Seleziona **Usa volume esistente, Abilita QoS** se necessario e fornisci i dettagli.



Nel tipo di storage ASA r2, la creazione o la selezione del volume non si applica alla creazione dell'unità di storage (LUN/Namespace). Pertanto, queste opzioni non vengono visualizzate.



Non puoi utilizzare il volume esistente per creare un datastore VMFS con protocollo NVMe/FC o NVMe/TCP. Crea un nuovo volume per il datastore VMFS.

7. Esamina i dettagli del datastore nel riquadro **Riepilogo** e seleziona **Fine**.



Se crei il datastore su un cluster protetto, puoi vedere un messaggio di sola lettura: "Il datastore è in fase di montaggio su un cluster protetto."

Risultato

Gli strumenti ONTAP creano il datastore VMFS e lo montano su tutti gli host.

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.