Configurare i tool ONTAP per VMware vSphere

ONTAP tools for VMware vSphere 10

NetApp
February 11, 2026

Sommario

Configurare i tool ONTAP per VMware vSphere

Aggiungere istanze di vCenter Server agli strumenti ONTAP

Aggiungi le istanze di vCenter Server ai tool ONTAP per VMware vSphere per configurare, gestire e proteggere i datastore virtuali nel tuo ambiente vCenter Server. Quando si aggiungono più istanze di vCenter Server, sono richiesti certificati CA personalizzati per la comunicazione sicura tra gli strumenti ONTAP e ciascun vCenter Server.

A proposito di questa attività

Gli strumenti ONTAP si integrano con vCenter Server per eseguire attività di archiviazione come provisioning, snapshot e protezione dei dati direttamente dal client 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. Ad 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 consiglia di distribuire vCenter Server utilizzando il suo fully qualified domain name (FQDN) e di assicurarsi 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.

Fasi

1. Apri un browser web e vai all'URL: `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Effettua l'accesso con i tool ONTAP per le credenziali di amministratore di VMware vSphere fornite durante l'implementazione.
3. Selezionare **vCenters** > **Add** per integrare le istanze di vCenter Server. Fornisci l'indirizzo IP vCenter o il

nome host, il nome utente, la password e i dettagli della porta.

4. Nelle opzioni avanzate, è possibile recuperare automaticamente il certificato di vCenter Server (autorizzarlo) oppure caricarlo manualmente.

> Non occorre un account di amministratore per aggiungere istanze vCenter agli strumenti ONTAP. È possibile creare un ruolo personalizzato senza l'account admin con autorizzazioni limitate. Per ulteriori informazioni, fare riferimento alla "USA vCenter Server RBAC con i tool ONTAP per VMware vSphere 10" sezione.

L'aggiunta di un'istanza di vCenter Server agli strumenti ONTAP attiva automaticamente le seguenti azioni:

- Gli strumenti ONTAP registrano il plug-in del client vCenter come plug-in remoto.
- All'istanza di vCenter Server vengono applicate le Privileges personalizzate per i plug-in e le API.
- Per gestire gli utenti vengono creati ruoli personalizzati.
- Il plug-in viene visualizzato come collegamento nell'interfaccia utente di vSphere.

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

Utilizzare gli ONTAP tools for VMware vSphere per registrare il provider VASA con un'istanza di vCenter Server. Ciò consente la gestione basata su policy di storage, il supporto vVols e l'integrazione con appliance VMware Live Site Recovery su sistemi ONTAP .

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

Fasi

1. Accedere al client vSphere.
2. Selezionare **tasti di scelta rapida** > **NetApp ONTAP tools** nella sezione dei plug-in.
3. Selezionare **Impostazioni** > **Impostazioni provider VASA**. Gli strumenti ONTAP visualizzano lo stato di registrazione del fornitore VASA come non registrato.
4. Selezionare il pulsante **Registra** per registrare il provider VASA.
5. Inserisci un nome e le credenziali per il fornitore VASA. Il nome utente può contenere solo lettere, numeri e caratteri di sottolineatura. Impostare la lunghezza della password tra 8 e 256 caratteri.
6. Selezionare **Registra**.
7. Dopo una registrazione riuscita e l'aggiornamento della pagina, gli strumenti ONTAP visualizzano lo stato, il nome e la versione del provider VASA registrato.

Cosa succederà

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

Fasi

1. Accedere all'istanza di vCenter Server.
2. Accedere con le credenziali di amministratore.
3. Selezionare **Storage Providers** > **Configure**. Verificare che il provider VASA incorporato sia elencato

correttamente.

Installare il plug-in NFS VAAI utilizzando gli strumenti ONTAP

Il plug-in NFS vStorage API for Array Integration (NFS VAAI) collega VMware vSphere agli array di archiviazione NFS. Utilizzare gli ONTAP tools for VMware vSphere per installare il plug-in VAAI. Ciò consente all'array di storage NFS di gestire determinate operazioni di storage al posto degli host ESXi.

Prima di iniziare

- Scaricare il "Plug-in NetApp NFS per VMware VAAI" pacchetto di installazione.
- Assicurarsi di disporre dell'host ESXi e della patch più recente di vSphere 7.0U3 o versioni successive e di ONTAP 9.14.1 o versioni successive.
- Montare un datastore NFS.

Fasi

1. Accedere al client vSphere.
2. Selezionare **tasti di scelta rapida** > **NetApp ONTAP tools** nella sezione dei plug-in.
3. Selezionare **Impostazioni** > **NFS VAAI Tools**.
4. Se hai già caricato il plug-in VAAI su vCenter Server, seleziona **Modifica** in **Versione esistente**. In caso contrario, seleziona **Carica**.
5. Sfogliare e selezionare il `.vib` file e selezionare **carica** per caricare il file negli strumenti ONTAP.
6. Selezionare **Installa su host ESXI**, selezionare l'host ESXi su cui si desidera installare il plug-in NFS VAAI, quindi selezionare **Installa**.

   vSphere Web Client mostra solo gli host ESXi che possono installare il plug-in. È possibile monitorare l'avanzamento dell'installazione nella sezione Attività recenti.

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

   Dopo aver riavviato l'host ESXi, gli ONTAP tools for VMware vSphere rilevano e abilitano automaticamente il plug-in NFS VAAI.

Quali sono le prossime novità?

Dopo aver installato il plug-in NFS VAAI e riavviato l'host ESXi, configurare i criteri di esportazione NFS per l'offload della copia VAAI. Assicurarsi che le norme sulla politica di esportazione soddisfino questi requisiti:

- Il volume ONTAP pertinente consente 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 maggiori informazioni, fare riferimento a "Configura le policy di esportazione NFS corrette per l'offload delle copie VAAI" Articolo della Knowledge Base.

Informazioni correlate

"Supporto per VMware vStorage su NFS"

"Attivare o disattivare NFSv4.0"

"Supporto ONTAP per NFSv4.2"

Configurare le impostazioni dell'host ESXi negli ONTAP tools

La configurazione delle impostazioni multipath e timeout del server ESXi aiuta a mantenere la disponibilità e l'integrità dei dati. Abilita il failover automatico su un percorso di archiviazione di backup se il percorso primario non è più disponibile.

Configurare le impostazioni di multipath e timeout del server ESXi

I tool ONTAP per VMware vSphere controllano e impostano le impostazioni di multipath host ESXi e le impostazioni di timeout HBA che funzionano meglio con i sistemi storage NetApp.

A proposito di questa attività

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

Fasi

1. Dalla home page del client Web VMware vSphere, selezionare **host e cluster**.
2. Nella pagina dei collegamenti del client Web VMware vSphere, selezionare **NetApp ONTAP tools** nella sezione dei plug-in.
3. Andare alla scheda **ESXi host compliance** nella panoramica (dashboard) degli strumenti ONTAP per il plug-in VMware vSphere.
4. Selezionare il collegamento **Applica impostazioni consigliate**.
5. Nella finestra **Applica impostazioni host consigliate**, seleziona gli host che desideri aggiornare per utilizzare le impostazioni consigliate NetApp e seleziona **Avanti**.

   È possibile espandere l'host ESXi per visualizzare i valori correnti.

6. Nella pagina delle impostazioni, selezionare i valori consigliati secondo necessità.
7. Nel pannello di riepilogo, controllare i valori e selezionare **fine**. È possibile tenere traccia dell'avanzamento nel riquadro attività recenti.

Impostare i valori dell'host ESXi

Utilizzare gli 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 .

È possibile impostare i seguenti valori su un host ESXi:

Impostazioni adattatore HBA/CNA

Imposta i seguenti parametri sui valori predefiniti:

- Disk.QFullSampleSize

- Disk.QFullThreshold
- Timeout HBA FC Emulex
- Timeout HBA FC QLogic

Impostazioni MPIO

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

Per ambienti ad alte prestazioni o quando si esegue il test con un singolo datastore LUN, regolare l'impostazione del bilanciamento del carico del criterio di selezione del percorso (PSP) round-robin (VMW_PSP_RR) 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	Impostare questo valore su…
NET.TcpipelHeapSize	32
NET.TcpipelHeapMax	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

Utilizzare questa sezione per configurare i ruoli utente e i privilegi ONTAP per i backend di archiviazione con gli ONTAP tools for VMware vSphere e ONTAP System Manager. È possibile assegnare ruoli utilizzando i file JSON forniti, creare manualmente utenti e ruoli e applicare i privilegi minimi richiesti per gli account non amministratori.

Prima di iniziare

- Scaricare il file ONTAP Privileges dagli ONTAP tools for VMware vSphere utilizzando *https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_roles.zip*. Dopo aver scaricato il file zip, troverai due file JSON. Utilizzare il file JSON specifico di ASA r2 durante la configurazione di un sistema ASA r2.

È possibile creare utenti a livello di cluster o direttamente a livello di macchine virtuali di archiviazione (SVM). Se non si utilizza il file user_roles.json, assicurarsi che l'utente disponga delle autorizzazioni SVM minime richieste.

- Accedi con privilegi di amministratore per il backend di archiviazione.

Fasi

1. Estrarre il file *https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_roles.zip* scaricato.
2. Accedere a ONTAP System Manager utilizzando l'indirizzo IP di gestione del cluster del cluster.
3. Accedi al cluster con privilegi di amministratore. Per configurare un utente:
   a. Per configurare un utente degli strumenti ONTAP del cluster, selezionare il riquadro **Cluster** > **Impostazioni** > **Utenti e ruoli**.
   b. Per configurare un utente degli strumenti SVM ONTAP , selezionare il riquadro **Storage SVM** > **Impostazioni** > **Utenti e ruoli**.
   c. Selezionare **Aggiungi** in utenti.
   d. Nella finestra di dialogo **Aggiungi utente**, selezionare **prodotti di virtualizzazione**.
   e. **Sfoglia** per selezionare e caricare il file JSON Privileges ONTAP . Per i sistemi non ASA r2, selezionare il file users_roles.json e per i sistemi ASA r2, selezionare il file users_roles_ASAr2.json.

      Gli strumenti ONTAP popolano automaticamente il campo Prodotto.

   f. Selezionare la funzionalità del prodotto come **VSC, VASA Provider e SRA** dal menu a discesa.

      Gli strumenti ONTAP popolano automaticamente il campo **Ruolo** in base alla funzionalità del prodotto selezionata.

   g. Immettere il nome utente e la password richiesti.
   h. Selezionare i privilegi (Discovery, Create Storage, Edit Storage, Destroy Storage, NAS/SAN Role) di cui l'utente ha bisogno, quindi selezionare **Aggiungi**.

Gli strumenti ONTAP aggiungono il nuovo ruolo e utente. Puoi visualizzare i privilegi relativi al ruolo configurato.

Requisiti di mappatura degli aggregati delle SVM

Durante il provisioning degli archivi dati utilizzando le credenziali utente SVM, gli ONTAP tools for VMware vSphere creano volumi sull'aggregato specificato nell'API POST degli archivi dati. ONTAP impedisce agli utenti SVM di creare volumi su aggregati non mappati sull'SVM. Prima di creare i volumi, mappare l'SVM sugli aggregati richiesti utilizzando l'API REST o la CLI ONTAP .

API REST:

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

CLI 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
```

Creare manualmente un utente e un ruolo ONTAP

Creare manualmente utenti e ruoli senza il file JSON.

1. Accedere a ONTAP System Manager utilizzando l'indirizzo IP di gestione del cluster del cluster.
2. Accedere al cluster con admin Privileges.
   a. Per configurare i ruoli degli strumenti ONTAP del cluster, selezionare **Cluster** > **Impostazioni** > **Utenti e ruoli**.
   b. Per configurare i ruoli degli strumenti SVM ONTAP del cluster, selezionare **Storage SVM** > **Impostazioni** > **Utenti e ruoli**.
3. Crea ruoli:
   a. Selezionare **Aggiungi** nella tabella **ruoli**.
   b. Immettere i dettagli **nome ruolo** e **attributi ruolo**.

      Aggiungere il **Percorso API REST** e scegliere l'accesso dall'elenco a discesa.

   c. Aggiungere tutte le API necessarie e salvare le modifiche.
4. Crea utenti:
   a. Selezionare **Aggiungi** nella tabella **utenti**.
   b. Nella finestra di dialogo **Aggiungi utente**, selezionare **System Manager**.
   c. Immettere il **Nome utente**.
   d. Selezionare **ruolo** dalle opzioni create nel passaggio **Crea ruoli** riportato sopra.
   e. Immettere le applicazioni a cui assegnare l'accesso e il metodo di autenticazione. ONTAPI e HTTP sono le applicazioni richieste e il tipo di autenticazione è **Password**.
   f. Impostare **Password per l'utente** e **Salva** l'utente.

Elenco dei privilegi minimi richiesti per gli utenti cluster con ambito globale non amministratori

Questa pagina elenca i privilegi minimi richiesti per un utente del cluster con ambito globale non amministratore senza un file JSON. Se un cluster si trova nell'ambito locale, utilizzare il file JSON per creare gli utenti, poiché gli ONTAP tools for VMware vSphere necessitano di più dei semplici privilegi di lettura per il provisioning su ONTAP.

È possibile accedere alle funzionalità tramite API:

API	Livello di accesso	Utilizzato per
/api/cluster	Sola lettura	Rilevamento della configurazione del cluster

/api/cluster/licenze/licenze	Sola lettura	Controllo della licenza per licenze specifiche del protocollo
/api/cluster/nodi	Sola lettura	Rilevamento del tipo di piattaforma
/api/security/accounts	Sola lettura	Scoperta dei privilegi
/api/security/ruoli	Sola lettura	Scoperta dei privilegi
/api/storage/aggregati	Sola lettura	Controllo dello spazio aggregato durante il provisioning del datastore/volume
/api/storage/cluster	Sola lettura	Per ottenere i dati sullo spazio e sull'efficienza a livello di cluster
/api/storage/dischi	Sola lettura	Per ottenere i dischi associati in un aggregato
/api/storage/qos/policy	Lettura/creazione/Modifica	Gestione delle policy QoS e VM
/api/svm/svm	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 di gestione LIF è cluster/SVM
/api/storage/availability-zones	Sola lettura	Scoperta SAZ. Applicabile alla versione ONTAP 9.16.1 e successive e ai sistemi ASA r2.
/api/cluster/metrocluster	Sola lettura	Ottiene lo stato e i dettagli di configurazione MetroCluster .

Crea tool ONTAP per l'utente con ambito cluster basato su API VMware vSphere ONTAP

Per le operazioni PATCH e il rollback automatico sui datastore sono richiesti privilegi di individuazione, creazione, modifica ed eliminazione. La mancanza di autorizzazioni potrebbe causare problemi di flusso di lavoro e di pulizia.

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

Per creare un utente soggetto all'ambito del cluster con tutti gli Privileges 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 ONTAP versione 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 su ONTAP versione 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 tool ONTAP per l'utente con ambito SVM basato su API di VMware vSphere ONTAP

Eseguire i seguenti comandi per creare un utente con ambito SVM dotato di 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 ONTAP versione 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 comando seguente:

```
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_sti160-cluster_
```

Eseguire 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_sti160-cluster
```

Aggiorna i tool ONTAP per VMware vSphere 10,1 a un utente 10,3

Per i tool ONTAP per gli utenti di VMware vSphere 10,1 con un utente impostato su cluster creato utilizzando il file JSON, utilizzare i seguenti comandi dell'interfaccia della riga di comando di ONTAP con l'Privileges dell'amministratore utente per eseguire l'aggiornamento alla release 10,3.

Per le funzionalità del prodotto:

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

Privileges 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 i tool ONTAP per l'utente di VMware vSphere 10,1 con un utente con ambito SVM creato utilizzando il file json, utilizza i comandi dell'interfaccia della riga di comando di ONTAP con l'utente admin Privileges per eseguire l'upgrade alla release 10,3.

Privileges 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, aggiungere 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 i tool ONTAP per VMware vSphere 10,3 a un utente 10,4

A partire da ONTAP 9.16.1, aggiornare gli ONTAP tools for VMware vSphere 10.3 alla versione 10.4.

Per i tool ONTAP per l'utente VMware vSphere 10,3 con un utente sottoposto a cluster creato utilizzando il file JSON e ONTAP versione 9.16.1 o successiva, utilizza il comando CLI ONTAP con admin user Privileges per eseguire l'upgrade alla release 10,4.

Per le funzionalità del prodotto:

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

Privileges cluster:

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

Aggiungi un backend di storage a ONTAP tools

Utilizza gli ONTAP tools for VMware vSphere per aggiungere e gestire i backend di storage per i tuoi host ESXi. È possibile integrare cluster o SVM, abilitare il supporto MetroCluster e convalidare i certificati per una connettività sicura. È possibile configurare i backend di archiviazione utilizzando 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 archiviazione in locale, utilizzare le credenziali del cluster o SVM nell'interfaccia degli strumenti ONTAP . I backend di archiviazione locale sono disponibili solo per il vCenter Server selezionato. Gli strumenti ONTAP mappano le SVM sul vCenter Server per la gestione dei datastore vVols o VMFS. Per i datastore VMFS e i flussi di lavoro SRA, è possibile utilizzare le credenziali SVM senza mappare un cluster a livello globale.

Per aggiungere un backend di archiviazione globale, utilizzare le credenziali del cluster ONTAP in ONTAP Tools Manager. I backend di archiviazione globali consentono ai flussi di lavoro di individuazione di identificare le risorse del cluster necessarie per la gestione vVol. Negli ambienti multitenant, è possibile aggiungere un

utente SVM localmente per gestire i datastore vVols .

Se il supporto MetroCluster è abilitato in ONTAP, integrare sia i cluster di origine che quelli di destinazione come backend di archiviazione locali o globali.

Prima di iniziare

Verificare che il certificato includa un campo Subject Alternative Name (SAN) valido. I sistemi ONTAP utilizzano il campo SAN per identificare i LIF di gestione del cluster e dell'SVM.

Utilizzo di ONTAP Tools Manager

In un setup multi-tenant, puoi aggiungere un cluster backend storage a livello globale e una SVM locale per utilizzare le credenziali utente della SVM.

Fasi

1. Avviare Gestione strumenti ONTAP da un browser Web:
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Effettua l'accesso con i tool ONTAP per le credenziali di amministratore di VMware vSphere fornite durante l'implementazione.
3. Selezionare **backend di archiviazione** dalla barra laterale.
4. Aggiungere il backend di archiviazione e fornire l'indirizzo IP del server o i dettagli FQDN, nome utente e password.

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

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

   Se necessario, è possibile disabilitare la convalida del nome alternativo del soggetto (SAN) dalla console di manutenzione. Per le istruzioni, vedere"Cambia il flag di convalida del certificato" .

6. Se il backend di archiviazione aggiunto fa parte di una configurazione MetroCluster , ONTAP Tools Manager mostra un messaggio pop-up per aggiungere il cluster peered. Selezionare **Aggiungi** e fornire i dettagli per il backend di archiviazione peer MetroCluster .

   Dopo che il sistema ONTAP ha eseguito uno switchover e uno switchback, eseguire manualmente la scoperta degli strumenti ONTAP .

Utilizzo dell'interfaccia utente del client vSphere

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

1. Accedere al client vSphere.
2. Nella pagina Collegamenti, selezionare **NetApp ONTAP tools** nella sezione dei plug-in.
3. Selezionare **backend di archiviazione** dalla barra laterale.
4. Aggiungere il backend di archiviazione e fornire l'indirizzo IP del server, il nome utente, la password e i dettagli della porta.

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

5. Recupera automaticamente i certificati del cluster ONTAP e autorizza il certificato oppure caricalo

manualmente navigando fino alla sua posizione.

6. Se il backend di archiviazione aggiunto fa parte della configurazione MetroCluster , gli strumenti ONTAP visualizzano la schermata **Aggiungi peer MetroCluster *. Selezionare *Aggiungi peer** per aggiungere il backend di archiviazione peer.

   Dopo che il sistema ONTAP ha eseguito uno switchover e uno switchback, eseguire manualmente la scoperta degli strumenti ONTAP .

Cosa succederà?

Gli strumenti ONTAP aggiornano l'elenco per mostrare il nuovo backend di archiviazione.

Gli strumenti ONTAP elencano il backend di archiviazione appena aggiunto nella pagina **Backend di archiviazione**. Se un certificato scade entro 30 giorni o meno, gli strumenti ONTAP mostrano un avviso nella colonna della data di scadenza del certificato. Dopo la scadenza, gli strumenti ONTAP contrassegnano il backend di archiviazione come sconosciuto perché non riesce a connettersi al sistema di archiviazione.

Informazioni correlate

"Configurazione dei cluster in una configurazione MetroCluster"

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

Associare un backend di archiviazione a un'istanza di vCenter Server per consentire l'accesso a tutte le istanze di vCenter Server. Per la configurazione MetroCluster , quando si associa un cluster backend di archiviazione, assicurarsi di associare anche il suo cluster peer al vCenter Server.

Fasi

1. Avviare Gestione strumenti ONTAP da un browser Web:
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Effettua l'accesso con i tool ONTAP per le credenziali di amministratore di VMware vSphere fornite durante l'implementazione.
3. Seleziona vCenter dalla barra laterale.
4. Selezionare le ellissi verticali accanto all'istanza di vCenter Server che si desidera connettere ai backend di storage.
5. Dal menu a discesa, seleziona il backend di archiviazione che desideri 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 al criterio di esportazione, a meno che non si configuri l'accesso alla rete. È possibile modificare i criteri di esportazione per consentire l'accesso solo da indirizzi IP specifici. Se un host ESXi escluso tenta un'operazione di montaggio, l'operazione fallisce.

Fasi

1. Accedere al client vSphere.
2. Selezionare **NetApp ONTAP tools** nella pagina dei collegamenti nella sezione dei plug-in.
3. Nel riquadro sinistro degli strumenti ONTAP , vai su **Impostazioni** > **Gestisci accesso alla rete** > **Modifica**.

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

4. Selezionare **Salva**.

Creare un datastore in ONTAP tools

Quando si crea un datastore a livello di cluster host, gli strumenti ONTAP lo montano su tutti gli host di destinazione e abilitano l'azione solo se si dispone dei privilegi richiesti.

Interoperabilità tra datastore nativi con vCenter Server e datastore gestiti da strumenti ONTAP

A partire dagli ONTAP tools for VMware vSphere 10.4, gli strumenti ONTAP creano igroup annidati per gli archivi dati, con igroup padre specifici per gli archivi dati e igroup figlio mappati agli host. È possibile creare igroup piatti da ONTAP System Manager e utilizzarli per creare datastore VMFS senza ricorrere agli strumenti ONTAP . Fare riferimento a "Gestire gli iniziatori SAN e gli igroup" per maggiori informazioni.

Dopo aver integrato l'archiviazione ed eseguito la scoperta del datastore, gli strumenti ONTAP trasformano gli igroup piatti nei datastore VMFS in igroup annidati. Non è possibile utilizzare igroup piatti precedenti per creare nuovi datastore. Utilizzare l'interfaccia degli strumenti ONTAP o l'API REST per riutilizzare gli igroup annidati.

Creare un datastore vVol

A partire dagli ONTAP tools for VMware vSphere 10.3, è possibile creare un datastore vVols su sistemi ASA r2 con efficienza di spazio come thin.vVol. Il provider VASA crea un contenitore e gli endpoint del protocollo desiderati durante la creazione del datastore vVol. Il provider VASA non assegna alcun volume di supporto a questo contenitore.

Prima di iniziare

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

Fasi

1. Accedere al client vSphere.
2. Fare clic con il pulsante destro del mouse su un sistema host, un cluster host o un data center e selezionare **Strumenti NetApp ONTAP * > *Crea datastore**.
3. Selezionare vVol **tipo di datastore**.
4. Immettere le informazioni **Nome datastore** e **protocollo**.

   Il sistema ASA R2 supporta i protocolli iSCSI e FC per i vVol.

5. Seleziona la macchina virtuale storage in cui desideri creare il datastore.
6. In Opzioni avanzate:
   - Se selezioni **Criterio di esportazione personalizzato**, assicurati di eseguire l'individuazione in vCenter per tutti gli oggetti. Si consiglia di non utilizzare questa opzione.
   - È possibile selezionare il nome **Custom Initiator group** per i protocolli iSCSI e FC.

   Nel sistema di archiviazione ASA r2 di tipo SVM, le unità di archiviazione (LUN/namespace) non vengono create perché l'archivio dati è solo un contenitore logico.

7. Nel riquadro **attributi archiviazione** è possibile creare nuovi volumi o utilizzare i volumi esistenti. Tuttavia, non è possibile combinare questi due tipi di volumi per creare un datastore vVol.

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

8. Controllare la selezione nel riquadro **Riepilogo** e selezionare **fine**.

Creare 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.

Fasi

1. Accedere al client vSphere.
2. Fare clic con il pulsante destro del mouse su un sistema host, un cluster host o un data center e selezionare **Strumenti NetApp ONTAP * > *Crea datastore**.

3. Selezionare NFS nel campo **tipo datastore**.
4. Immettere il nome del datastore, le dimensioni e le informazioni sul protocollo nel riquadro **Nome e protocollo**. Selezionare **Datastore cluster** e **autenticazione Kerberos** nelle opzioni avanzate.

   L'autenticazione Kerberos è disponibile solo quando è selezionato il protocollo NFS 4,1.

5. Selezionare **piattaforma** e **Storage VM** nel riquadro **Storage**.
6. Se si seleziona **Criterio di esportazione personalizzato** nelle opzioni avanzate, eseguire l'individuazione in vCenter per tutti gli oggetti. Si consiglia di non utilizzare questa opzione.

   Non è possibile creare un datastore NFS utilizzando il criterio del volume predefinito o root dell'SVM.

   - Nelle opzioni avanzate, il pulsante di commutazione **asimmetrico** è visibile solo se nel menu a discesa della piattaforma sono selezionate prestazioni o capacità.
   - Selezionando l'opzione **Qualsiasi** nel menu a discesa della piattaforma, è possibile visualizzare tutte le SVM in vCenter. La piattaforma e la bandiera asimmetrica non influiscono sulla visibilità.
7. Selezionare l'aggregato per la creazione del volume nel riquadro **attributi archiviazione**. Nelle opzioni avanzate, scegliere **Riserva spazio** e **attiva QoS** come richiesto.
8. Controllare le selezioni nel riquadro **Riepilogo** e selezionare **fine**.

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

Creare un datastore VMFS

VMFS è un file system clusterizzato 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.

In un cluster protetto:

- È possibile creare solo datastore VMFS. L'aggiunta di un datastore VMFS a un cluster protetto ne determina automaticamente la protezione.
- Non è possibile creare un datastore in un data center con uno o più cluster host protetti.
- Non è possibile creare un datastore su un host ESXi se il cluster host padre è protetto da una "policy di failover duplex automatizzato" (configurazione uniforme o non uniforme).
- È possibile creare un datastore VMFS solo su un host ESXi protetto da una relazione asincrona. Non è possibile creare e montare un datastore su un host ESXi che fa parte di un cluster host protetto dal criterio "Automated failover Duplex".

Prima di iniziare

- Abilitare servizi e LIF per ogni protocollo da parte dello storage ONTAP.
- Mappare la SVM per l'aggregato dell'utente SVM nel sistema storage ASA R2.
- Configurare l'host ESXi se si utilizza il protocollo NVMe/TCP:
  a. Esaminare "Guida alla compatibilità VMware"

  VMware vSphere 7,0 U3 e le versioni successive supportano il protocollo NVMe/TCP. Tuttavia, si consiglia VMware vSphere 8,0 e versioni successive.

b. Verificare se il fornitore della scheda di interfaccia di rete (NIC) supporta la NIC ESXi con il protocollo NVMe/TCP.

c. Configurare la scheda di rete ESXi per NVMe/TCP in base alle specifiche del fornitore della scheda di rete.

d. Quando si utilizza VMware vSphere 7 release, seguire le istruzioni sul sito VMware "Configurare il binding VMkernel per NVMe over TCP Adapter" per configurare il binding della porta NVMe/TCP. Quando si utilizza VMware vSphere 8 release, seguire "Configurazione di NVMe su TCP su ESXi", per configurare il binding della porta NVMe/TCP.

e. Per VMware vSphere 7 release, seguire le istruzioni a pagina "Abilita gli adattatori software NVMe su RDMA o NVMe su TCP" per configurare gli adattatori software NVMe/TCP. Per la release VMware vSphere 8, seguire "Aggiunta di adattatori software NVMe su RDMA o NVMe su TCP" questa procedura per configurare gli adattatori software NVMe/TCP.

f. Eseguire "Rilevamento di host e sistemi storage" l'azione sull'host ESXi. Per ulteriori informazioni, fare riferimento a "Come configurare NVMe/TCP con vSphere 8,0 Update 1 e ONTAP 9.13,1 per datastore VMFS".

- Se si utilizza il protocollo NVME/FC, procedere come segue per configurare l'host ESXi:

a. Se non è già abilitato, abilitare NVMe over Fabrics (NVMe-of) sugli host ESXi.

b. Zoning SCSI completo.

c. Verificare che gli host ESXi e il sistema ONTAP siano connessi a un livello fisico e logico.

Per configurare una SVM ONTAP per il protocollo FC, fare riferimento alla "Configurare una SVM per FC".

Per ulteriori informazioni sull'utilizzo del protocollo NVMe/FC con VMware vSphere 8,0, consultare "Configurazione host NVMe-of per ESXi 8.x con ONTAP" .

Per ulteriori informazioni sull'utilizzo di NVMe/FC con VMware vSphere 7,0, consultare "Guida alla configurazione degli host NVMe/FC di ONTAP" e "TR-4684".

Fasi

1. Accedere al client vSphere.
2. Fare clic con il pulsante destro del mouse su un sistema host, un cluster host o un data center e selezionare **Strumenti NetApp ONTAP * > *Crea datastore**.
3. Selezionare il tipo di datastore VMFS.
4. Immettere il nome del datastore, le dimensioni e le informazioni sul protocollo nel riquadro **Nome e protocollo**. Per aggiungere il nuovo datastore a un cluster VMFS esistente, selezionare il cluster del datastore in Opzioni avanzate.
5. Selezionare Storage VM nel riquadro **Storage**. Specificare il **nome gruppo iniziatore personalizzato** nella sezione **Opzioni avanzate** secondo necessità. È possibile scegliere un igroup esistente per il datastore o creare un nuovo igroup con un nome personalizzato.

   Quando si seleziona il protocollo NVMe/FC o NVMe/TCP, viene creato un nuovo sottosistema di namespace che viene utilizzato per la mappatura degli spazi dei nomi. Gli strumenti ONTAP creano il sottosistema dello spazio dei nomi utilizzando il nome generato automaticamente che include il nome del datastore. È possibile rinominare il sottosistema dello spazio dei nomi nel campo **nome del sottosistema dello spazio dei nomi personalizzato** nelle opzioni avanzate del riquadro **Archiviazione**.

6. Dal riquadro **attributi di archiviazione**:

a. Selezionare **aggregate** dalle opzioni a discesa.

> Per i sistemi di archiviazione ASA r2, l'opzione **Aggregate** non viene visualizzata perché l'archiviazione è disaggregata. Quando si sceglie un sistema di storage ASA r2 di tipo SVM, la pagina degli attributi di storage mostra le opzioni per abilitare la 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 * di performance per i sistemi storage ASA R2 con SVM a 12 nodi, che è un cluster eterogeneo. Questa opzione non è disponibile se la SVM selezionata è un cluster omogeneo o utilizza un utente SVM.

   'Qualsiasi' è il valore predefinito del livello di servizio delle prestazioni (PSL). Questa impostazione crea l'unità di memorizzazione utilizzando l'algoritmo di posizionamento bilanciato ONTAP. Tuttavia, è possibile selezionare l'opzione prestazioni o estreme in base alle esigenze.

d. Selezionare **Usa volume esistente**, **attiva QoS** come richiesto e fornire i dettagli.

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

> Non è possibile utilizzare il volume esistente per creare un datastore VMFS con protocollo NVMe/FC o NVMe/TCP. Creare un nuovo volume per il datastore VMFS.

7. Rivedere i dettagli del datastore nel riquadro **Riepilogo** e selezionare **fine**.

> Se si crea il datastore su un cluster protetto, viene visualizzato un messaggio di sola lettura: "Il datastore viene montato su un cluster protetto".

Risultato

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

Informazioni sul copyright

Informazioni sul marchio commerciale