Gestire i ruoli di controllo degli accessi

ONTAP 9

NetApp
February 12, 2026

This PDF was generated from https://docs.netapp.com/it-it/ontap/authentication/manage-access-control-roles-concept.html on February 12, 2026. Always check docs.netapp.com for the latest.

Sommario

Gestire i ruoli di controllo degli accessi . . . 1
- Scopri come gestire i ruoli di controllo degli accessi di ONTAP . . . 1
- Modificare il ruolo assegnato a un amministratore ONTAP . . . 1
- Definire ruoli personalizzati per gli amministratori di ONTAP . . . 1
- Ruoli predefiniti per gli amministratori del cluster ONTAP . . . 3
- Ruoli predefiniti per gli amministratori delle SVM di ONTAP . . . 5
- Gestire l’accesso di amministratore ONTAP con Gestione sistema . . . 7
  - Assegnazione di un ruolo a un amministratore . . . 8
  - Modifica del ruolo di amministratore . . . 8
- Elevazione dei privilegi JIT di accesso in ONTAP . . . 8
- Configurare l’elevazione dei privilegi JIT in ONTAP . . . 9
  - Modificare le impostazioni JIT globali . . . 10
  - Configurare l’accesso all’elevazione dei privilegi JIT per un utente . . . 11
  - Casi d’uso JIT comuni . . . 12

Gestire i ruoli di controllo degli accessi

Scopri come gestire i ruoli di controllo degli accessi di ONTAP

Il ruolo assegnato a un amministratore determina i comandi a cui l'amministratore ha accesso. Il ruolo viene assegnato quando si crea l'account per l'amministratore. È possibile assegnare un ruolo diverso o definire ruoli personalizzati in base alle esigenze.

Modificare il ruolo assegnato a un amministratore ONTAP

Puoi utilizzare `security login modify` il comando per modificare il ruolo di un account amministratore di cluster o SVM. È possibile assegnare un ruolo predefinito o personalizzato.

Prima di iniziare

Per eseguire questa attività, è necessario essere un amministratore del cluster.

Fase

1. Modificare il ruolo di un amministratore di cluster o SVM:

   ```
   security login modify -vserver SVM_name -user-or-group-name user_or_group_name
   -application application -authmethod authentication_method -role role -comment
   comment
   ```

   "Creazione o modifica degli account di accesso"

   Il seguente comando modifica il ruolo dell'account amministratore del cluster ad `DOMAIN1\guest1` al predefinito `readonly` ruolo.

   ```
   cluster1::>security login modify -vserver engCluster -user-or-group-name
   DOMAIN1\guest1 -application ssh -authmethod domain -role readonly
   ```

   Il seguente comando modifica il ruolo degli account amministratore SVM nell'account di gruppo ad `DOMAIN1\adgroup` al personalizzato `vol_role` ruolo.

   ```
   cluster1::>security login modify -vserver engData -user-or-group-name
   DOMAIN1\adgroup -application ssh -authmethod domain -role vol_role
   ```

   Ulteriori informazioni su `security login modify` nella "Riferimento al comando ONTAP".

Definire ruoli personalizzati per gli amministratori di ONTAP

È possibile utilizzare il `security login role create` comando per definire un ruolo

personalizzato. È possibile eseguire il comando tutte le volte necessarie per ottenere la combinazione esatta di funzionalità che si desidera associare al ruolo.

A proposito di questa attività

- Un ruolo, predefinito o personalizzato, concede o nega l'accesso ai comandi ONTAP o alle directory dei comandi.

  Una directory di comandi (`volume`, ad esempio) è un gruppo di sottodirectory di comandi e comandi correlati. Ad eccezione di quanto descritto in questa procedura, la concessione o il rifiuto dell'accesso a una directory di comandi concede o nega l'accesso a ciascun comando nella directory e nelle relative sottodirectory.

- L'accesso a comandi o sottodirectory specifici sovrascrive l'accesso alla directory principale.

  Se un ruolo viene definito con una directory di comandi e quindi viene definito nuovamente con un livello di accesso diverso per un comando specifico o per una sottodirectory della directory principale, il livello di accesso specificato per il comando o la sottodirectory sovrascrive quello della directory principale.

> Non è possibile assegnare a un amministratore SVM un ruolo che dia accesso a una directory di comandi o comandi disponibile solo per `admin` amministratore del cluster, ad esempio `security` directory dei comandi.

Prima di iniziare

Per eseguire questa attività, è necessario essere un amministratore del cluster.

Fase

1. Definire un ruolo personalizzato:

   ```
   security login role create -vserver SVM_name -role role -cmddirname
   command_or_directory_name -access access_level -query query
   ```

   I seguenti comandi assegnano a. `vol_role` accesso completo ai comandi in `volume` directory dei comandi e accesso in sola lettura ai comandi in `volume snapshot` sottodirectory.

   ```
   cluster1::>security login role create -role vol_role -cmddirname
   "volume" -access all

   cluster1::>security login role create -role vol_role -cmddirname "volume
   snapshot" -access readonly
   ```

   I seguenti comandi assegnano a. `SVM_storage` accesso in sola lettura ai comandi in `storage` directory dei comandi, nessun accesso ai comandi in `storage encryption` sottodirectory e accesso completo a `storage aggregate plex offline` comando non intrinseco.

```
cluster1::>security login role create -role SVM_storage -cmddirname
"storage" -access readonly

cluster1::>security login role create -role SVM_storage -cmddirname
"storage encryption" -access none

cluster1::>security login role create -role SVM_storage -cmddirname
"storage aggregate plex offline" -access all
```

Ulteriori informazioni su `security login role create` nella "Riferimento al comando ONTAP".

Informazioni correlate

- "creazione del ruolo di accesso di sicurezza"
- "plesso di aggregato di storage offline"
- "crittografia dello storage"

Ruoli predefiniti per gli amministratori del cluster ONTAP

I ruoli predefiniti per gli amministratori dei cluster devono soddisfare la maggior parte delle esigenze. È possibile creare ruoli personalizzati in base alle necessità. Per impostazione predefinita, a un amministratore del cluster viene assegnato il valore predefinito `admin` ruolo.

La seguente tabella elenca i ruoli predefiniti per gli amministratori del cluster:

Questo ruolo…	Dispone di questo livello di accesso…	Alle seguenti directory di comandi o comandi
amministratore	tutto	Tutte le directory dei comandi (`DEFAULT`)
admin-no-fsa (disponibile a partire da ONTAP 9.12.1)	Lettura/scrittura	• Tutte le directory dei comandi (`DEFAULT`) • `security login rest-role` • `security login role`

Di sola lettura	• `security login rest-role create` • `security login rest-role delete` • `security login rest-role modify` • `security login rest-role show` • `security login role create` • `security login role create` • `security login role delete` • `security login role modify` • `security login role show` • `volume activity-tracking` • `volume analytics`	Nessuno
`volume file show-disk-usage`	AutoSupport	tutto
• `set` • `system node autosupport`	nessuno	Tutte le altre directory di comando (`DEFAULT`)
backup	tutto	`vserver services ndmp`
readonly	`volume`	nessuno
Tutte le altre directory di comando (`DEFAULT`)	readonly	tutto

• `security login password` Solo per la gestione della password locale del proprio account utente e delle informazioni sulle chiavi • `set`	• A partire da ONTAP 9,8, sola lettura • Prima di ONTAP 9,8, nessuno	`security`
readonly	Tutte le altre directory di comando (`DEFAULT`)	SnapLock
tutto	• `set` • `volume create` • `volume modify` • `volume move` • `volume show`	nessuno
• `volume move governor` • `volume move recommend`	nessuno	Tutte le altre directory di comando (`DEFAULT`)
nessuno	nessuno	Tutte le directory dei comandi (`DEFAULT`)

Il `autosupport` il ruolo viene assegnato al predefinito `autosupport` Account, utilizzato da AutoSupport OnDemand. ONTAP impedisce di modificare o eliminare `autosupport` account. ONTAP impedisce inoltre l'assegnazione di `autosupport` ruolo per altri account utente.

Informazioni correlate

- "accesso di sicurezza"
- "partenza"
- "volume"
- "servizi vserver ndmp"

Ruoli predefiniti per gli amministratori delle SVM di ONTAP

I ruoli predefiniti per gli amministratori SVM devono soddisfare la maggior parte delle esigenze. È possibile creare ruoli personalizzati in base alle necessità. Per impostazione predefinita, a un amministratore SVM viene assegnato il valore predefinito `vsadmin` ruolo.

La seguente tabella elenca i ruoli predefiniti per gli amministratori SVM:

Nome del ruolo	Funzionalità
vsadmin	• Gestione delle informazioni relative alla password locale e alle chiavi del proprio account utente • Gestione dei volumi, ad eccezione degli spostamenti dei volumi • Gestione di quote, qtree, snapshot e file • Gestione delle LUN • Esecuzione delle operazioni SnapLock, ad eccezione dell'eliminazione con privilegi • Configurazione dei protocolli: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC e NVMe/TCP • Configurazione dei servizi: DNS, LDAP e NIS • Monitoraggio dei lavori • Monitoraggio delle connessioni di rete e dell'interfaccia di rete • Monitoraggio dello stato di salute di SVM
volume vsadmin	• Gestione delle informazioni relative alla password locale e alle chiavi del proprio account utente • Gestione dei volumi, ad eccezione degli spostamenti dei volumi • Gestione di quote, qtree, snapshot e file • Gestione delle LUN • Configurazione dei protocolli: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC e NVMe/TCP • Configurazione dei servizi: DNS, LDAP e NIS • Interfaccia di rete di monitoraggio • Monitoraggio dello stato di salute di SVM
protocollo vsadmin	• Gestione delle informazioni relative alla password locale e alle chiavi del proprio account utente • Configurazione dei protocolli: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC e NVMe/TCP • Configurazione dei servizi: DNS, LDAP e NIS • Gestione delle LUN • Interfaccia di rete di monitoraggio • Monitoraggio dello stato di salute di SVM

vsadmin-backup	• Gestione delle informazioni relative alla password locale e alle chiavi del proprio account utente • Gestione delle operazioni NDMP • Creazione di un volume ripristinato in lettura/scrittura • Gestione di relazioni e snapshot SnapMirror • Visualizzazione di volumi e informazioni di rete
vsadmin-snaplock	• Gestione delle informazioni relative alla password locale e alle chiavi del proprio account utente • Gestione dei volumi, ad eccezione degli spostamenti dei volumi • Gestione di quote, qtree, snapshot e file • Esecuzione di operazioni SnapLock, inclusa l'eliminazione con privilegi • Configurazione dei protocolli: NFS e SMB • Configurazione dei servizi: DNS, LDAP e NIS • Monitoraggio dei lavori • Monitoraggio delle connessioni di rete e dell'interfaccia di rete
vsadmin-readonly	• Gestione delle informazioni relative alla password locale e alle chiavi del proprio account utente • Monitoraggio dello stato di salute di SVM • Interfaccia di rete di monitoraggio • Visualizzazione di volumi e LUN • Visualizzazione di servizi e protocolli

Gestire l'accesso di amministratore ONTAP con Gestione sistema

Il ruolo assegnato a un amministratore determina le funzioni che l'amministratore può eseguire con System Manager. System Manager fornisce ruoli predefiniti per gli amministratori dei cluster e gli amministratori delle macchine virtuali dello storage. Il ruolo viene assegnato quando si crea l'account dell'amministratore oppure è possibile assegnarlo in un secondo momento.

A seconda di come è stato attivato l'accesso all'account, potrebbe essere necessario eseguire una delle seguenti operazioni:

- Associare una chiave pubblica a un account locale.
- Installare un certificato digitale del server firmato dalla CA.

- Configurare l'accesso ad, LDAP o NIS.

È possibile eseguire queste attività prima o dopo aver attivato l'accesso all'account.

Assegnazione di un ruolo a un amministratore

Assegnare un ruolo a un amministratore, come indicato di seguito:

Fasi

1. Selezionare **Cluster > Settings** (cluster > Impostazioni).
2. Selezionare → accanto a **utenti e ruoli**.
3. Selezionare + Add in **utenti**.
4. Specificare un nome utente e selezionare un ruolo nel menu a discesa per **ruolo**.
5. Specificare un metodo di accesso e una password per l'utente.

Modifica del ruolo di amministratore

Modificare il ruolo di amministratore, come segue:

Fasi

1. Fare clic su **Cluster > Settings** (Cluster > Impostazioni).
2. Selezionare il nome dell'utente di cui si desidera modificare il ruolo, quindi fare clic sul ⋮ che viene visualizzato accanto al nome utente.
3. Fare clic su **Edit** (Modifica).
4. Selezionare un ruolo nel menu a discesa per **ruolo**.

Elevazione dei privilegi JIT di accesso in ONTAP

A partire da ONTAP 9.17.1, gli amministratori del cluster possono "configurare l'elevazione dei privilegi just-in-time (JIT)" Per consentire agli utenti ONTAP di elevare temporaneamente i propri privilegi per eseguire determinate attività. Quando JIT è configurato per un utente, quest'ultimo può elevare temporaneamente i propri privilegi a un ruolo che dispone delle autorizzazioni necessarie per eseguire un'attività. Alla scadenza della sessione, l'utente torna al livello di accesso originale.

Gli amministratori del cluster possono configurare la durata di accesso di un utente all'elevazione JIT. Ad esempio, gli amministratori del cluster possono configurare l'accesso utente all'elevazione JIT con un limite di 30 minuti per sessione (il *periodo di validità della sessione*) per un periodo di 30 giorni (il *periodo di validità JIT*). Durante il periodo di 30 giorni, l'utente può elevare i propri privilegi tutte le volte che desidera, ma ogni sessione è limitata a 30 minuti.

A proposito di questa attività

- L'elevazione dei privilegi JIT è disponibile solo per gli utenti che accedono a ONTAP tramite SSH. L'elevazione dei privilegi è disponibile solo all'interno della sessione SSH corrente, ma è possibile elevare i privilegi in tutte le sessioni SSH simultanee necessarie.
- L'elevazione dei privilegi JIT è supportata solo per gli utenti che utilizzano l'autenticazione tramite password, nsswitch o dominio per l'accesso. L'autenticazione a più fattori (MFA) non è supportata per l'elevazione dei privilegi JIT.

- La sessione JIT di un utente verrà terminata se scade la sessione configurata o il periodo di validità JIT oppure se un amministratore del cluster revoca l'accesso JIT all'utente.

Prima di iniziare

- Per accedere all'elevazione dei privilegi JIT, un amministratore del cluster deve configurare l'accesso JIT per il tuo account. L'amministratore del cluster determina il ruolo a cui puoi elevare i tuoi privilegi e la durata per cui puoi accedere ai privilegi elevati.

Fasi

1. Eleva temporaneamente i tuoi privilegi al ruolo configurato:

   ```
   security jit-privilege elevate
   ```

   Dopo aver inserito questo comando, ti verrà richiesto di inserire la password di accesso. Se per il tuo account è configurato l'accesso JIT, ti verrà concesso un accesso elevato per la durata della sessione configurata. Al termine della sessione, tornerai al tuo livello di accesso originale. Puoi elevare i tuoi privilegi tutte le volte che vuoi entro il periodo di validità JIT configurato.

2. Visualizza il tempo rimanente della sessione JIT:

   ```
   security jit-privilege show-remaining-time
   ```

   Se ci si trova in una sessione JIT, questo comando visualizza il tempo rimanente.

3. Se necessario, termina la sessione JIT in anticipo:

   ```
   security jit-privilege reset
   ```

   Se ci si trova in una sessione JIT, questo comando termina la sessione JIT e ripristina il livello di accesso originale.

Configurare l'elevazione dei privilegi JIT in ONTAP

A partire da ONTAP 9.17.1, gli amministratori di cluster possono configurare l'elevazione dei privilegi just-in-time (JIT) per consentire agli utenti ONTAP di elevare temporaneamente i propri privilegi per eseguire determinate attività. Quando JIT è configurato per un utente, questi può temporaneamente "elevare il loro privilegio" a un ruolo che dispone delle autorizzazioni necessarie per eseguire un'attività. Al termine della sessione, l'utente torna al suo livello di accesso originale.

Gli amministratori del cluster possono configurare la durata di accesso di un utente all'elevazione JIT. Ad esempio, è possibile configurare l'accesso utente all'elevazione JIT con un limite di 30 minuti per sessione (il *periodo di validità della sessione*) per un periodo di 30 giorni (il *periodo di validità JIT*). Durante il periodo di 30 giorni, l'utente può elevare i propri privilegi tutte le volte che desidera, ma ogni sessione è limitata a 30 minuti.

L'elevazione dei privilegi JIT supporta il principio del privilegio minimo, consentendo agli utenti di eseguire attività che richiedono privilegi elevati senza concederli in modo permanente. Questo contribuisce a ridurre il

rischio di accessi non autorizzati o modifiche accidentali al sistema. I seguenti esempi descrivono alcuni casi d'uso comuni per l'elevazione dei privilegi JIT:

- Consentire l'accesso temporaneo al `security login create` E `security login delete` comandi per abilitare l'onboarding e l'offboarding degli utenti.
- Consentire l'accesso temporaneo a `system node image update` E `system node upgrade-revert` Durante una finestra di aggiornamento. Al termine dell'aggiornamento, l'accesso ai comandi viene revocato.
- Consentire l'accesso temporaneo a `cluster add-node` , `cluster remove-node` , E `cluster modify` Per abilitare l'espansione o la riconfigurazione del cluster. Una volta completate le modifiche al cluster, l'accesso ai comandi viene revocato.
- Consentire l'accesso temporaneo a `volume snapshot restore` Per abilitare le operazioni di ripristino e la gestione delle destinazioni di backup. Una volta completato il ripristino o la configurazione, l'accesso ai comandi viene revocato.
- Consentire l'accesso temporaneo a `security audit log show` per abilitare la revisione e l'esportazione del registro di controllo durante un controllo di conformità.

Per un elenco più ampio dei casi d'uso JIT più comuni, fare riferimento a Casi d'uso JIT comuni .

Gli amministratori del cluster possono impostare l'accesso JIT per gli utenti ONTAP e configurare i periodi di validità JIT predefiniti a livello globale nel cluster o per SVM specifiche.

A proposito di questa attività

- L'elevazione dei privilegi JIT è disponibile solo per gli utenti che accedono a ONTAP tramite SSH. I privilegi elevati sono disponibili solo all'interno della sessione SSH corrente dell'utente, ma possono essere elevati in tutte le sessioni SSH simultanee necessarie.
- L'elevazione dei privilegi JIT è supportata solo per gli utenti che utilizzano l'autenticazione tramite password, nsswitch o dominio per l'accesso. L'autenticazione a più fattori (MFA) non è supportata per l'elevazione dei privilegi JIT.

Prima di iniziare

- Devi essere un amministratore del cluster ONTAP presso `admin` livello di privilegio per eseguire le seguenti attività.

Modificare le impostazioni JIT globali

È possibile modificare le impostazioni JIT predefinite a livello globale, per l'intero cluster ONTAP o per una specifica SVM. Queste impostazioni determinano il periodo di validità predefinito della sessione e il periodo di validità JIT massimo per gli utenti configurati per l'accesso JIT.

A proposito di questa attività

- Il valore predefinito `default-session-validity-period` Il valore è un'ora. Questa impostazione determina per quanto tempo un utente può accedere ai privilegi elevati in una sessione JIT prima di doverli riassegnare.
- Il valore predefinito `max-jit-validity-period` Il valore è 90 giorni. Questa impostazione determina il periodo massimo durante il quale un utente può accedere all'elevazione JIT dopo la data di inizio configurata. È possibile configurare il periodo di validità JIT per singoli utenti, ma non può superare il periodo di validità JIT massimo.

Fasi

1. Controllare le impostazioni JIT correnti:

```
security jit-privilege show -vserver <svm_name>
```

`-vserver` è facoltativo. Se non si specifica una SVM, il comando mostra le impostazioni JIT globali.

2. Modificare le impostazioni JIT a livello globale o per una SVM:

```
security jit-privilege modify -vserver <svm_name> -default-session
-validity-period <period> -max-jit-validity-period <period>
```

Se non si specifica una SVM, il comando modifica le impostazioni JIT globali. L'esempio seguente imposterà la durata predefinita della sessione JIT a 45 minuti e la durata massima a 30 giorni per la SVM. `svm1` :
`security jit-privilege modify -vserver svm1 -default-session-validity-period 45m -max-jit-validity-period 30d`

In questo esempio, gli utenti potranno accedere all'elevazione JIT per 45 minuti alla volta e potranno avviare sessioni JIT per un massimo di 30 giorni dopo la data di inizio configurata.

Configurare l'accesso all'elevazione dei privilegi JIT per un utente

È possibile assegnare l'accesso con privilegi di elevazione JIT agli utenti ONTAP .

Fasi

1. Controlla l'accesso JIT corrente per un utente:

```
security jit-privilege user show -username <username>
```

`-username` è facoltativo. Se non si specifica un nome utente, il comando mostra l'accesso JIT per tutti gli utenti.

2. Assegna un nuovo accesso JIT per un utente:

```
security jit-privilege create -username <username> -vserver <svm_name>
-role <rbac_role> -session-validity-period <period> -jit-validity-period
<period> -start-time <date>
```

- Se `-vserver` non è specificato, l'accesso JIT viene assegnato a livello di cluster.
- `-role` è il ruolo RBAC a cui l'utente verrà elevato. Se non specificato, `-role` predefinito su `admin` .
- `-session-validity-period` è la durata per cui l'utente può accedere al ruolo elevato prima di dover avviare una nuova sessione JIT. Se non specificato, il valore globale o SVM `default-session-validity-period` viene utilizzato.
- `-jit-validity-period` è la durata massima per la quale un utente può avviare sessioni JIT dopo

la data di inizio configurata. Se non specificato, `session-validity-period` viene utilizzato. Questo parametro non può superare il valore globale o SVM `max-jit-validity-period` .

- `-start-time` Indica la data e l'ora dopo le quali l'utente può avviare sessioni JIT. Se non specificato, vengono utilizzate la data e l'ora correnti.

  L'esempio seguente consentirà `ontap_user` per accedere al `admin` ruolo per 1 ora prima di dover iniziare una nuova sessione JIT. `ontap_user` potrà avviare sessioni JIT per un periodo di 60 giorni a partire dalle 13:00 del 1° luglio 2025:
  `security jit-privilege user create -username ontap_user -role admin -session -validity-period 1h -jit-validity-period 60d -start-time "7/1/25 13:00:00"`

3. Se necessario, revocare l'accesso JIT di un utente:

```
security jit-privilege user delete -username <username> -vserver
<svm_name>
```

Questo comando revocherà l'accesso JIT di un utente, anche se il suo accesso non è scaduto. Se `-vserver` Se non è specificato, l'accesso JIT viene revocato a livello di cluster. Se l'utente è in una sessione JIT attiva, la sessione verrà terminata.

Casi d'uso JIT comuni

La tabella seguente contiene casi d'uso comuni per l'elevazione dei privilegi JIT. Per ogni caso d'uso, è necessario configurare un ruolo RBAC per fornire l'accesso ai comandi pertinenti. Ogni comando è collegato al riferimento ai comandi ONTAP , con ulteriori informazioni sul comando e sui relativi parametri.

Caso d'utilizzo	Comandi	Dettagli
Gestione degli utenti e dei ruoli	• `security login create` • `security login delete`	Esegui l'elevazione temporanea per aggiungere/rimuovere utenti o modificare ruoli durante l'onboarding o l'offboarding.
Gestione dei certificati	• `security certificate create` • `security certificate install`	Concedi l'accesso a breve termine per l'installazione o il rinnovo del certificato.
Controllo di accesso SSH/CLI	• `security login create -application ssh`	Concedere temporaneamente l'accesso SSH per la risoluzione dei problemi o per il supporto del fornitore.
Gestione delle licenze	• `system license add` • `system license delete`	Concedi i diritti per aggiungere o rimuovere licenze durante l'attivazione o la disattivazione delle funzionalità.

Caso d'utilizzo	Comandi	Dettagli
Aggiornamenti e patch di sistema	• `system node image update` • `system node upgrade-revert`	Eleva per la finestra di aggiornamento, quindi revoca.
Impostazioni di sicurezza della rete	• `security login role create` • `security login role modify`	Consenti modifiche temporanee ai ruoli di sicurezza correlati alla rete.
Gestione dei cluster	• `cluster add-node` • `cluster remove-node` • `cluster modify`	Elevate per l'espansione o la riconfigurazione del cluster.
Gestione SVM	• `vserver create` • `vserver delete` • `vserver modify`	Concedere temporaneamente a un SVM i diritti di amministratore per il provisioning o la dismissione.
Gestione del volume	• `volume create` • `volume delete` • `volume modify`	Elevate per il provisioning, il ridimensionamento o la rimozione del volume.
Gestione degli snapshot	• `volume snapshot create` • `volume snapshot delete` • `volume snapshot restore`	Elevate per l'eliminazione degli snapshot o il ripristino durante il ripristino.
Configurazione di rete	• `network interface create` • `network port vlan create`	Concedere diritti per modifiche alla rete durante le finestre di manutenzione.
Gestione dischi/aggregati	• `storage disk assign` • `storage aggregate create` • `storage aggregate add-disks`	Elevate per aggiungere o rimuovere dischi o gestire aggregati.

Caso d'utilizzo	Comandi	Dettagli
Protezione dei dati	• `snapmirror create` • `snapmirror modify` • `snapmirror restore`	Eleva temporaneamente per configurare o ripristinare le relazioni SnapMirror .
Ottimizzazione delle prestazioni	• `qos policy-group create` • `qos policy-group modify`	Elevate per la risoluzione dei problemi o l'ottimizzazione delle prestazioni.
Accesso al registro di controllo	• `security audit log show`	Elevare temporaneamente per la revisione del registro di controllo o per l'esportazione durante i controlli di conformità.
Gestione di eventi e avvisi	• `event notification create` • `event notification modify`	Elevate per configurare o testare le notifiche degli eventi o le trap SNMP.
Accesso ai dati basato sulla conformità	• `volume show` • `security audit log show`	Concedere ai revisori l'accesso temporaneo in sola lettura per esaminare dati o registri sensibili.
Recensioni di accesso privilegiato	• `security login show` • `security login role show`	Eleva temporaneamente i privilegi per rivedere e segnalare gli accessi privilegiati. Concedi l'accesso elevato in sola lettura per un periodo di tempo limitato.

Informazioni correlate

- "cluster"
- "notifica di evento"
- "rete"
- "gruppo di policy QOS"
- "sicurezza"
- "snapmirror"
- "magazzinaggio"
- "sistema"
- "volume"
- "server virtuale"

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 COMMERCIABILITÀ 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 CONSEQUENZIALE (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.