



# **Configurare la gestione esterna delle chiavi**

## **ONTAP 9**

NetApp  
April 24, 2024

# Sommario

- Configurare la gestione esterna delle chiavi ..... 1
  - Configurare una panoramica sulla gestione esterna delle chiavi ..... 1
  - Raccogliere le informazioni di rete in ONTAP 9.2 e versioni precedenti ..... 1
  - Installare i certificati SSL sul cluster ..... 2
  - Gestione esterna delle chiavi in ONTAP 9.6 e versioni successive (basato su hardware) ..... 3
  - Abilitare la gestione esterna delle chiavi in ONTAP 9.5 e versioni precedenti ..... 5
  - Configurare i server di chiavi esterne in cluster ..... 6
  - Creare chiavi di autenticazione in ONTAP 9.6 e versioni successive ..... 8
  - Creare chiavi di autenticazione in ONTAP 9.5 e versioni precedenti ..... 10
  - Assegnazione di una chiave di autenticazione dei dati a un disco FIPS o SED (gestione esterna delle chiavi) ..... 12

# Configurare la gestione esterna delle chiavi

## Configurare una panoramica sulla gestione esterna delle chiavi

È possibile utilizzare uno o più server di gestione delle chiavi esterni per proteggere le chiavi utilizzate dal cluster per accedere ai dati crittografati. Un server di gestione delle chiavi esterno è un sistema di terze parti nell'ambiente di storage che fornisce le chiavi ai nodi utilizzando il protocollo KMIP (Key Management Interoperability Protocol).

Per ONTAP 9.1 e versioni precedenti, è necessario assegnare le LIF di gestione dei nodi alle porte configurate con il ruolo di gestione dei nodi prima di poter utilizzare il gestore delle chiavi esterno.

La crittografia dei volumi NetApp (NVE) può essere implementata con Onboard Key Manager in ONTAP 9.1 e versioni successive. In ONTAP 9.3 e versioni successive, NVE può essere implementato con gestione delle chiavi esterna (KMIP) e Gestione delle chiavi integrata. A partire da ONTAP 9.11.1, è possibile configurare più Key Manager esterni in un cluster. Vedere [Configurare i server delle chiavi in cluster](#).

## Raccogliere le informazioni di rete in ONTAP 9.2 e versioni precedenti

Se si utilizza ONTAP 9.2 o versioni precedenti, compilare il foglio di lavoro per la configurazione di rete prima di attivare la gestione esterna delle chiavi.



A partire da ONTAP 9.3, il sistema rileva automaticamente tutte le informazioni di rete necessarie.

Elemento	Note	Valore
Nome dell'interfaccia di rete per la gestione delle chiavi		
Indirizzo IP dell'interfaccia di rete per la gestione delle chiavi	Indirizzo IP della LIF di gestione dei nodi, in formato IPv4 o IPv6	
Gestione delle chiavi interfaccia di rete IPv6 lunghezza prefisso di rete	Se si utilizza IPv6, la lunghezza del prefisso di rete IPv6	
Subnet mask dell'interfaccia di rete per la gestione delle chiavi		
Gestione delle chiavi Indirizzo IP del gateway dell'interfaccia di rete		

Indirizzo IPv6 per l'interfaccia di rete del cluster	Obbligatorio solo se si utilizza IPv6 per l'interfaccia di rete per la gestione delle chiavi	
Numero di porta per ciascun server KMIP	Opzionale. Il numero di porta deve essere lo stesso per tutti i server KMIP. Se non si specifica un numero di porta, per impostazione predefinita viene impostata la porta 5696, che corrisponde alla porta assegnata dall'autorità IANA (Internet Assigned Numbers Authority) per KMIP.	
Nome tag chiave	Opzionale. Il nome del tag della chiave viene utilizzato per identificare tutte le chiavi appartenenti a un nodo. Il nome predefinito del tag della chiave è il nome del nodo.	

#### Informazioni correlate

["Report tecnico di NetApp 3954: Requisiti e procedure di preinstallazione di NetApp Storage Encryption per IBM Tivoli Lifetime Key Manager"](#)

["Report tecnico di NetApp 4074: Requisiti e procedure di preinstallazione di NetApp Storage Encryption per SafeNet KeySecure"](#)

## Installare i certificati SSL sul cluster

Il cluster e il server KMIP utilizzano i certificati SSL KMIP per verificare l'identità reciproca e stabilire una connessione SSL. Prima di configurare la connessione SSL con il server KMIP, è necessario installare i certificati SSL del client KMIP per il cluster e il certificato pubblico SSL per l'autorità di certificazione principale (CA) del server KMIP.

#### A proposito di questa attività

In una coppia ha, entrambi i nodi devono utilizzare gli stessi certificati SSL KMIP pubblici e privati. Se si collegano più coppie ha allo stesso server KMIP, tutti i nodi delle coppie ha devono utilizzare gli stessi certificati SSL KMIP pubblici e privati.

#### Prima di iniziare

- L'ora deve essere sincronizzata sul server che crea i certificati, sul server KMIP e sul cluster.
- È necessario avere ottenuto il certificato del client KMIP SSL pubblico per il cluster.
- È necessario aver ottenuto la chiave privata associata al certificato del client SSL KMIP per il cluster.
- Il certificato del client SSL KMIP non deve essere protetto da password.
- È necessario aver ottenuto il certificato pubblico SSL per l'autorità di certificazione principale (CA) del server KMIP.
- In un ambiente MetroCluster, è necessario installare gli stessi certificati SSL KMIP su entrambi i cluster.



È possibile installare i certificati client e server sul server KMIP prima o dopo l'installazione dei certificati sul cluster.

## Fasi

1. Installare i certificati del client KMIP SSL per il cluster:

```
security certificate install -vserver admin_svm_name -type client
```

Viene richiesto di immettere i certificati SSL KMIP pubblici e privati.

```
cluster1::> security certificate install -vserver cluster1 -type client
```

2. Installare il certificato pubblico SSL per l'autorità di certificazione principale (CA) del server KMIP:

```
security certificate install -vserver admin_svm_name -type server-ca
```

```
cluster1::> security certificate install -vserver cluster1 -type server-ca
```

## Gestione esterna delle chiavi in ONTAP 9.6 e versioni successive (basato su hardware)

È possibile utilizzare uno o più server KMIP per proteggere le chiavi utilizzate dal cluster per accedere ai dati crittografati. È possibile collegare fino a quattro server KMIP a un nodo. Si consiglia di utilizzare almeno due server per la ridondanza e il disaster recovery.

A partire da ONTAP 9.11.1, è possibile aggiungere fino a 3 server di chiavi secondari per ogni server di chiavi primario per creare un server di chiavi in cluster. Per ulteriori informazioni, vedere [Configurare i server di chiavi esterne in cluster](#).

### Prima di iniziare

- I certificati del server e del client SSL KMIP devono essere stati installati.
- Per eseguire questa attività, è necessario essere un amministratore del cluster.
- È necessario configurare l'ambiente MetroCluster prima di configurare un gestore di chiavi esterno.
- In un ambiente MetroCluster, è necessario installare il certificato SSL KMIP su entrambi i cluster.

## Fasi

1. Configurare la connettività del gestore delle chiavi per il cluster:

```
security key-manager external enable -vserver admin_SVM -key-servers  
host_name|IP_address:port,... -client-cert client_certificate -server-ca-cert  
server_CA_certificates
```



- Il `security key-manager external enable` il comando **sostituisce** `security key-manager setup` comando. È possibile eseguire `security key-manager external modify` comando per modificare la configurazione di gestione delle chiavi esterne. Per la sintassi completa dei comandi, vedere le pagine man.
- In un ambiente MetroCluster, se si sta configurando la gestione esterna delle chiavi per la SVM amministrativa, è necessario ripetere `security key-manager external enable` sul cluster partner.

Il seguente comando abilita la gestione esterna delle chiavi per `cluster1` con tre key server esterni. Il primo server chiavi viene specificato utilizzando il nome host e la porta, il secondo viene specificato utilizzando un indirizzo IP e la porta predefinita, mentre il terzo viene specificato utilizzando un indirizzo IPv6 e una porta:

```
cluster1::> security key-manager external enable -key-servers
ks1.local:15696,10.0.0.10,[fd20:8b1e:b255:814e:32bd:f35c:832c:5a09]:1234
-client-cert AdminVserverClientCert -server-ca-certs
AdminVserverServerCaCert
```

## 2. Verificare che tutti i server KMIP configurati siano connessi:

```
security key-manager external show-status -node node_name -vserver SVM -key
-server host_name|IP_address:port -key-server-status available|not-
responding|unknown
```



Il `security key-manager external show-status` il comando **sostituisce** `security key-manager show -status` comando. Per la sintassi completa dei comandi, vedere la pagina man.

```
cluster1::> security key-manager external show-status
```

Node	Vserver	Key Server	Status
-----			
node1			
	cluster1	10.0.0.10:5696	available
		fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234	available
		ks1.local:15696	available
node2			
	cluster1	10.0.0.10:5696	available
		fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234	available
		ks1.local:15696	available

6 entries were displayed.

# Abilitare la gestione esterna delle chiavi in ONTAP 9.5 e versioni precedenti

È possibile utilizzare uno o più server KMIP per proteggere le chiavi utilizzate dal cluster per accedere ai dati crittografati. È possibile collegare fino a quattro server KMIP a un nodo. Si consiglia di utilizzare almeno due server per la ridondanza e il disaster recovery.

## A proposito di questa attività

ONTAP configura la connettività del server KMIP per tutti i nodi del cluster.

## Prima di iniziare

- I certificati del server e del client SSL KMIP devono essere stati installati.
- Per eseguire questa attività, è necessario essere un amministratore del cluster.
- È necessario configurare l'ambiente MetroCluster prima di configurare un gestore di chiavi esterno.
- In un ambiente MetroCluster, è necessario installare il certificato SSL KMIP su entrambi i cluster.

## Fasi

1. Configurare la connettività del gestore delle chiavi per i nodi del cluster:

```
security key-manager setup
```

Viene avviata la configurazione di Key Manager.



In un ambiente MetroCluster, è necessario eseguire questo comando su entrambi i cluster.

2. Immettere la risposta appropriata a ogni richiesta.
3. Aggiunta di un server KMIP:

```
security key-manager add -address key_management_server_ipaddress
```

```
cluster1::> security key-manager add -address 20.1.1.1
```



In un ambiente MetroCluster, è necessario eseguire questo comando su entrambi i cluster.

4. Aggiungere un server KMIP aggiuntivo per la ridondanza:

```
security key-manager add -address key_management_server_ipaddress
```

```
cluster1::> security key-manager add -address 20.1.1.2
```



In un ambiente MetroCluster, è necessario eseguire questo comando su entrambi i cluster.

5. Verificare che tutti i server KMIP configurati siano connessi:

```
security key-manager show -status
```

Per la sintassi completa dei comandi, vedere la pagina man.

```
cluster1::> security key-manager show -status
```

Node	Port	Registered Key Manager	Status
-----	----	-----	-----
cluster1-01	5696	20.1.1.1	available
cluster1-01	5696	20.1.1.2	available
cluster1-02	5696	20.1.1.1	available
cluster1-02	5696	20.1.1.2	available

6. Facoltativamente, convertire volumi di testo normale in volumi crittografati.

```
volume encryption conversion start
```

Prima di convertire i volumi, è necessario configurare completamente un gestore di chiavi esterno. In un ambiente MetroCluster, è necessario configurare un gestore di chiavi esterno su entrambi i siti.

## Configurare i server di chiavi esterne in cluster

A partire da ONTAP 9.11.1, è possibile configurare la connettività ai server di gestione delle chiavi esterni in cluster su una SVM. Con i key server in cluster, è possibile designare i key server primari e secondari su una SVM. Durante la registrazione delle chiavi, ONTAP tenta innanzitutto di accedere a un server principale prima di tentare di accedere in sequenza ai server secondari fino al completamento dell'operazione, evitando la duplicazione delle chiavi.

I Key server esterni possono essere utilizzati per le chiavi NSE, NVE, NAE e SED. Una SVM può supportare fino a quattro server KMIP esterni primari. Ciascun server primario può supportare fino a tre server secondari per le chiavi.

### Prima di iniziare

- ["La gestione delle chiavi di KMIP deve essere abilitata per la SVM"](#).
- Questo processo supporta solo i server chiave che utilizzano KMIP. Per un elenco dei server delle chiavi supportati, consultare ["Tool di matrice di interoperabilità NetApp"](#).
- Tutti i nodi del cluster devono eseguire ONTAP 9.11.1 o versione successiva.
- L'ordine dei server elenca gli argomenti in `-secondary-key-servers`. Il parametro riflette l'ordine di accesso dei server KMIP (gestione delle chiavi esterne).

### Creare un server di chiavi in cluster

La procedura di configurazione dipende dal fatto che sia stato configurato o meno un server di chiavi primario.



### Aggiunta di server di chiavi primari e secondari a una SVM

1. Verificare che non sia stata attivata alcuna gestione delle chiavi per il cluster:

```
security key-manager external show -vserver svm_name
```

Se SVM ha già attivato un massimo di quattro server principali, è necessario rimuovere uno dei server principali esistenti prima di aggiungerne uno nuovo.

2. Attivare il gestore delle chiavi primario:

```
security key-manager external enable -vserver svm_name -key-servers  
server_ip -client-cert client_cert_name -server-ca-certs  
server_ca_cert_names
```

3. Modificare il server delle chiavi primario per aggiungere i server delle chiavi secondari. Il `-secondary-key-servers` parameter accetta un elenco separato da virgole di un massimo di tre server chiave.

```
security key-manager external modify-server -vserver svm_name -key-servers  
primary_key_server -secondary-key-servers list_of_key_servers
```

### Aggiungere i server di chiavi secondari a un server di chiavi primario esistente

1. Modificare il server delle chiavi primario per aggiungere i server delle chiavi secondari. Il `-secondary-key-servers` parameter accetta un elenco separato da virgole di un massimo di tre server chiave.

```
security key-manager external modify-server -vserver svm_name -key-servers  
primary_key_server -secondary-key-servers list_of_key_servers
```

Per ulteriori informazioni sui server di chiavi secondari, vedere [\[mod-secondary\]](#).

## Modificare i server delle chiavi in cluster

È possibile modificare i cluster di Key Server esterni modificando lo stato (primario o secondario) di determinati Key Server, aggiungendo e rimuovendo i Key Server secondari o modificando l'ordine di accesso dei Key Server secondari.

### Convertire i server chiavi primari e secondari

Per convertire un server di chiavi primario in un server di chiavi secondario, è necessario prima rimuoverlo dalla SVM con `security key-manager external remove-servers` comando.

Per convertire un server chiavi secondario in un server chiavi primario, è necessario prima rimuovere il server chiavi secondario dal server chiavi primario esistente. Vedere [\[mod-secondary\]](#). Se si converte un server chiavi secondario in un server primario durante la rimozione di una chiave esistente, il tentativo di aggiungere un nuovo server prima di completare la rimozione e la conversione può comportare la duplicazione delle chiavi.

### Modificare i server chiavi secondari

I server di chiavi secondari vengono gestiti con `-secondary-key-servers` del parametro `security key-manager external modify-server` comando. Il `-secondary-key-servers` parameter accetta un elenco separato da virgole. L'ordine specificato dei server di chiavi secondari nell'elenco determina la sequenza di accesso per i server di chiavi secondari. L'ordine di accesso può essere modificato eseguendo il comando `security key-manager external modify-server` con i server di chiavi secondari inseriti in una sequenza diversa.

Per rimuovere un server di chiavi secondario, la `-secondary-key-servers` gli argomenti devono includere i server chiave che si desidera conservare mentre si omette quello da rimuovere. Per rimuovere tutti i server di

chiavi secondari, utilizzare l'argomento `-`, non significa nessuno.

Per ulteriori informazioni, fare riferimento a `security key-manager external` nella ["Riferimento al comando ONTAP"](#).

## Creare chiavi di autenticazione in ONTAP 9.6 e versioni successive

È possibile utilizzare `security key-manager key create` Per creare le chiavi di autenticazione per un nodo e memorizzarle nei server KMIP configurati.

### A proposito di questa attività

Se la configurazione della protezione richiede l'utilizzo di chiavi diverse per l'autenticazione dei dati e l'autenticazione FIPS 140-2, è necessario creare una chiave separata per ciascuna di esse. In caso contrario, è possibile utilizzare la stessa chiave di autenticazione per la conformità FIPS utilizzata per l'accesso ai dati.

ONTAP crea chiavi di autenticazione per tutti i nodi del cluster.

- Questo comando non è supportato quando Onboard Key Manager è attivato. Tuttavia, quando Onboard Key Manager è attivato, vengono create automaticamente due chiavi di autenticazione. I tasti possono essere visualizzati con il seguente comando:

```
security key-manager key query -key-type NSE-AK
```

- Viene visualizzato un avviso se i server di gestione delle chiavi configurati memorizzano già più di 128 chiavi di autenticazione.
- È possibile utilizzare `security key-manager key delete` per eliminare le chiavi inutilizzate. Il comando non riesce se la chiave è attualmente in uso da ONTAP. Per utilizzare questo comando, è necessario disporre di privilegi superiori a "admin".



In un ambiente MetroCluster, prima di eliminare una chiave, è necessario assicurarsi che la chiave non sia in uso nel cluster partner. È possibile utilizzare i seguenti comandi sul cluster partner per verificare che la chiave non sia in uso:

- ° `storage encryption disk show -data-key-id key-id`
- ° `storage encryption disk show -fips-key-id key-id`

### Prima di iniziare

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

### Fasi

1. Creare le chiavi di autenticazione per i nodi del cluster:

```
security key-manager key create -key-tag passphrase_label -prompt-for-key true|false
```



Impostazione `prompt-for-key=true` fa in modo che il sistema richieda all'amministratore del cluster la passphrase da utilizzare per l'autenticazione dei dischi crittografati. In caso contrario, il sistema genera automaticamente una passphrase da 32 byte. Il `security key-manager key create` il comando sostituisce `security key-manager create-key` comando. Per la sintassi completa dei comandi, vedere la pagina `man`.

Nell'esempio seguente vengono create le chiavi di autenticazione per `cluster1`, che genera automaticamente una passphrase da 32 byte:

```
cluster1::> security key-manager key create
Key ID:
000000000000000000002000000000001006268333f870860128fbe17d393e5083b00000000
00000000
```

## 2. Verificare che le chiavi di autenticazione siano state create:

```
security key-manager key query -node node
```



Il `security key-manager key query` il comando sostituisce `security key-manager query key` comando. Per la sintassi completa dei comandi, vedere la pagina `man`. L'ID della chiave visualizzato nell'output è un identificatore utilizzato per fare riferimento alla chiave di autenticazione. Non si tratta della chiave di autenticazione effettiva o della chiave di crittografia dei dati.

Nell'esempio seguente viene verificata la creazione di chiavi di autenticazione per `cluster1`:

```
cluster1::> security key-manager key query
      Vserver: cluster1
      Key Manager: external
      Node: node1
```

Key Tag	Key Type	Restored
node1	NSE-AK	yes
Key ID: 000000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e00000000 00000000		
node1	NSE-AK	yes
Key ID: 000000000000000000002000000000001006f4e2513353a674305872a4c9f3bf79700000000 00000000		

```
      Vserver: cluster1
      Key Manager: external
      Node: node2
```

Key Tag	Key Type	Restored
node2	NSE-AK	yes
Key ID: 000000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e00000000 00000000		
node2	NSE-AK	yes
Key ID: 000000000000000000002000000000001006f4e2513353a674305872a4c9f3bf79700000000 00000000		

## Creare chiavi di autenticazione in ONTAP 9.5 e versioni precedenti

È possibile utilizzare `security key-manager create-key` Per creare le chiavi di autenticazione per un nodo e memorizzarle nei server KMIP configurati.

### A proposito di questa attività

Se la configurazione della protezione richiede l'utilizzo di chiavi diverse per l'autenticazione dei dati e l'autenticazione FIPS 140-2, è necessario creare una chiave separata per ciascuna di esse. In caso contrario, è possibile utilizzare la stessa chiave di autenticazione per la conformità FIPS utilizzata per l'accesso ai dati.

ONTAP crea chiavi di autenticazione per tutti i nodi del cluster.

- Questo comando non è supportato quando è attivata la gestione delle chiavi integrate.

- Viene visualizzato un avviso se i server di gestione delle chiavi configurati memorizzano già più di 128 chiavi di autenticazione.

È possibile utilizzare il software del server di gestione delle chiavi per eliminare le chiavi inutilizzate, quindi eseguire nuovamente il comando.

## Prima di iniziare

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

## Fasi

1. Creare le chiavi di autenticazione per i nodi del cluster:

```
security key-manager create-key
```

Per la sintassi completa dei comandi, vedere la pagina man del comando.



L'ID della chiave visualizzato nell'output è un identificatore utilizzato per fare riferimento alla chiave di autenticazione. Non si tratta della chiave di autenticazione effettiva o della chiave di crittografia dei dati.

Nell'esempio seguente vengono create le chiavi di autenticazione per `cluster1`:

```
cluster1::> security key-manager create-key
(security key-manager create-key)
Verifying requirements...

Node: cluster1-01
Creating authentication key...
Authentication key creation successful.
Key ID: F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C

Node: cluster1-01
Key manager restore operation initialized.
Successfully restored key information.

Node: cluster1-02
Key manager restore operation initialized.
Successfully restored key information.
```

2. Verificare che le chiavi di autenticazione siano state create:

```
security key-manager query
```

Per la sintassi completa dei comandi, vedere la pagina man.

Nell'esempio seguente viene verificata la creazione di chiavi di autenticazione per `cluster1`:

```
cluster1::> security key-manager query

(security key-manager query)

Node: cluster1-01
Key Manager: 20.1.1.1
Server Status: available

Key Tag          Key Type  Restored
-----
cluster1-01      NSE-AK    yes
Key ID:
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C

Node: cluster1-02
Key Manager: 20.1.1.1
Server Status: available

Key Tag          Key Type  Restored
-----
cluster1-02      NSE-AK    yes
Key ID:
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
```

## Assegnazione di una chiave di autenticazione dei dati a un disco FIPS o SED (gestione esterna delle chiavi)

È possibile utilizzare `storage encryption disk modify` Comando per assegnare una chiave di autenticazione dei dati a un'unità FIPS o SED. I nodi del cluster utilizzano questa chiave per bloccare o sbloccare i dati crittografati sul disco.

### A proposito di questa attività

Un'unità con crittografia automatica è protetta da accessi non autorizzati solo se l'ID della chiave di autenticazione è impostato su un valore non predefinito. L'ID sicuro del produttore (MSID), con ID chiave 0x0, è il valore predefinito standard per i dischi SAS. Per i dischi NVMe, il valore predefinito standard è una chiave nulla, rappresentata come ID chiave vuoto. Quando si assegna l'ID della chiave a un'unità con crittografia automatica, il sistema modifica l'ID della chiave di autenticazione in un valore non predefinito.

Questa procedura non comporta interruzioni.

### Prima di iniziare

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

### Fasi

1. Assegnare una chiave di autenticazione dei dati a un'unità FIPS o SED:

```
storage encryption disk modify -disk disk_ID -data-key-id key_ID
```

Per la sintassi completa dei comandi, vedere la pagina man del comando.



È possibile utilizzare `security key-manager query -key-type NSE-AK` Per visualizzare gli ID chiave.

```
cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id  
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
```

```
Info: Starting modify on 14 disks.  
View the status of the operation by using the  
storage encryption disk show-status command.
```

2. Verificare che le chiavi di autenticazione siano state assegnate:

```
storage encryption disk show
```

Per la sintassi completa dei comandi, vedere la pagina man.

```
cluster1::> storage encryption disk show  
Disk      Mode Data Key ID  
-----  
-----  
0.0.0     data  
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C  
0.0.1     data  
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C  
[...]
```

## Informazioni sul copyright

Copyright © 2024 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.