Abilitare l'accesso all'account locale

ONTAP 9

NetApp
February 12, 2026

This PDF was generated from https://docs.netapp.com/it-it/ontap/authentication/create-local-user-accounts-task.html on February 12, 2026. Always check docs.netapp.com for the latest.

Sommario

Abilitare l’accesso all’account locale . . . 1
- Ulteriori informazioni sull’attivazione dell’accesso all’account ONTAP locale . . . 1
- Attiva l’accesso alla password dell’account ONTAP . . . 1
- Attiva l’accesso a chiave pubblica SSH dell’account ONTAP . . . 2
- Abilitare gli account MFA (Multiple Factor Authentication) . . . 3
  - Ulteriori informazioni sull’autenticazione a più fattori ONTAP . . . 3
  - Abilita l’autenticazione a più fattori ONTAP con SSH e TOTP . . . 4
  - Configurare gli account utente ONTAP locali per MFA con TOTP . . . 7
  - Reimpostare la chiave segreta TOTP per un account utente ONTAP . . . 8
  - Disattivare la chiave segreta TOTP per un account utente ONTAP . . . 9
- Attiva l’accesso all’account ONTAP del certificato SSL . . . 9

Abilitare l'accesso all'account locale

Ulteriori informazioni sull'attivazione dell'accesso all'account ONTAP locale

Un account locale è un account in cui le informazioni sull'account, la chiave pubblica o il certificato di protezione risiedono nel sistema di storage. Puoi utilizzare `security login create` il comando per abilitare gli account locali per l'accesso a un amministratore o a una SVM dati.

Informazioni correlate

- "creazione dell'accesso di sicurezza"

Attiva l'accesso alla password dell'account ONTAP

Puoi utilizzare `security login create` il comando per abilitare gli account amministratore per l'accesso a una SVM di amministrazione o dati con una password. La password viene richiesta dopo aver immesso il comando.

A proposito di questa attività

Se non si è certi del ruolo di controllo dell'accesso che si desidera assegnare all'account di accesso, è possibile utilizzare il `security login modify` comando per aggiungere il ruolo in un secondo momento.

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

Prima di iniziare

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

Fase

1. Abilitare gli account dell'amministratore locale per accedere a una SVM utilizzando una password:

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

   Il seguente comando attiva l'account amministratore del cluster `admin1` con il predefinito `backup` Ruolo di accesso alla SVM amministrativa`engCluster` utilizzo di una password. La password viene richiesta dopo aver immesso il comando.

   ```
   cluster1::>security login create -vserver engCluster -user-or-group-name
   admin1 -application ssh -authmethod password -role backup
   ```

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

Attiva l'accesso a chiave pubblica SSH dell'account ONTAP

Puoi utilizzare `security login create` il comando per abilitare gli account amministratore per l'accesso a una SVM di amministrazione o dati con una chiave pubblica SSH.

A proposito di questa attività

- Prima che l'account possa accedere a SVM, è necessario associare la chiave pubblica all'account.

  Associazione di una chiave pubblica a un account utente

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

- Se non si è certi del ruolo di controllo dell'accesso che si desidera assegnare all'account di accesso, è possibile utilizzare il `security login modify` comando per aggiungere il ruolo in un secondo momento.

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

Se si desidera attivare la modalità FIPS sul cluster, gli account a chiave pubblica SSH esistenti senza gli algoritmi a chiave supportati devono essere riconfigurati con un tipo di chiave supportato. Gli account devono essere riconfigurati prima di attivare FIPS, altrimenti l'autenticazione dell'amministratore non avrà esito positivo.

La seguente tabella indica gli algoritmi del tipo di chiave host supportati per le connessioni SSH ONTAP. Questi tipi di chiave non si applicano alla configurazione dell'autenticazione pubblica SSH.

Release di ONTAP	Tipi di chiave supportati in modalità FIPS	Tipi di chiave supportati in modalità non FIPS
9.11.1 e versioni successive	ecdsa-sha2-nistp256	ecdsa-sha2-nistp256 + rsa-sha2-512 + rsa-sha2-256 + ssh-ed25519 + ssh-dss + ssh-rsa
9.10.1 e versioni precedenti	ecdsa-sha2-nistp256 + ssh-ed25519	ecdsa-sha2-nistp256 + ssh-ed25519 + ssh-dss + ssh-rsa

Il supporto per l'algoritmo della chiave host ssh-ed25519 viene rimosso a partire da ONTAP 9.11.1.

Per ulteriori informazioni, vedere "Configurare la sicurezza di rete utilizzando FIPS".

Prima di iniziare

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

Fase

1. Abilitare gli account dell'amministratore locale per accedere a una SVM utilizzando una chiave pubblica SSH:

   ```
   security login create -vserver SVM_name -user-or-group-name user_or_group_name
   ```

`-application` *`application`* `-authmethod` *`authentication_method`* `-role` *`role`* `-comment` *`comment`*

Il seguente comando attiva l'account amministratore SVM `svmadmin1` con il predefinito `vsadmin-volume` Ruolo per accedere a SVM`engData1` Utilizzando una chiave pubblica SSH:

```
cluster1::>security login create -vserver engData1 -user-or-group-name
svmadmin1 -application ssh -authmethod publickey -role vsadmin-volume
```

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

Al termine

Se non è stata associata una chiave pubblica all'account amministratore, è necessario farlo prima che l'account possa accedere a SVM.

Associazione di una chiave pubblica a un account utente

Abilitare gli account MFA (Multiple Factor Authentication)

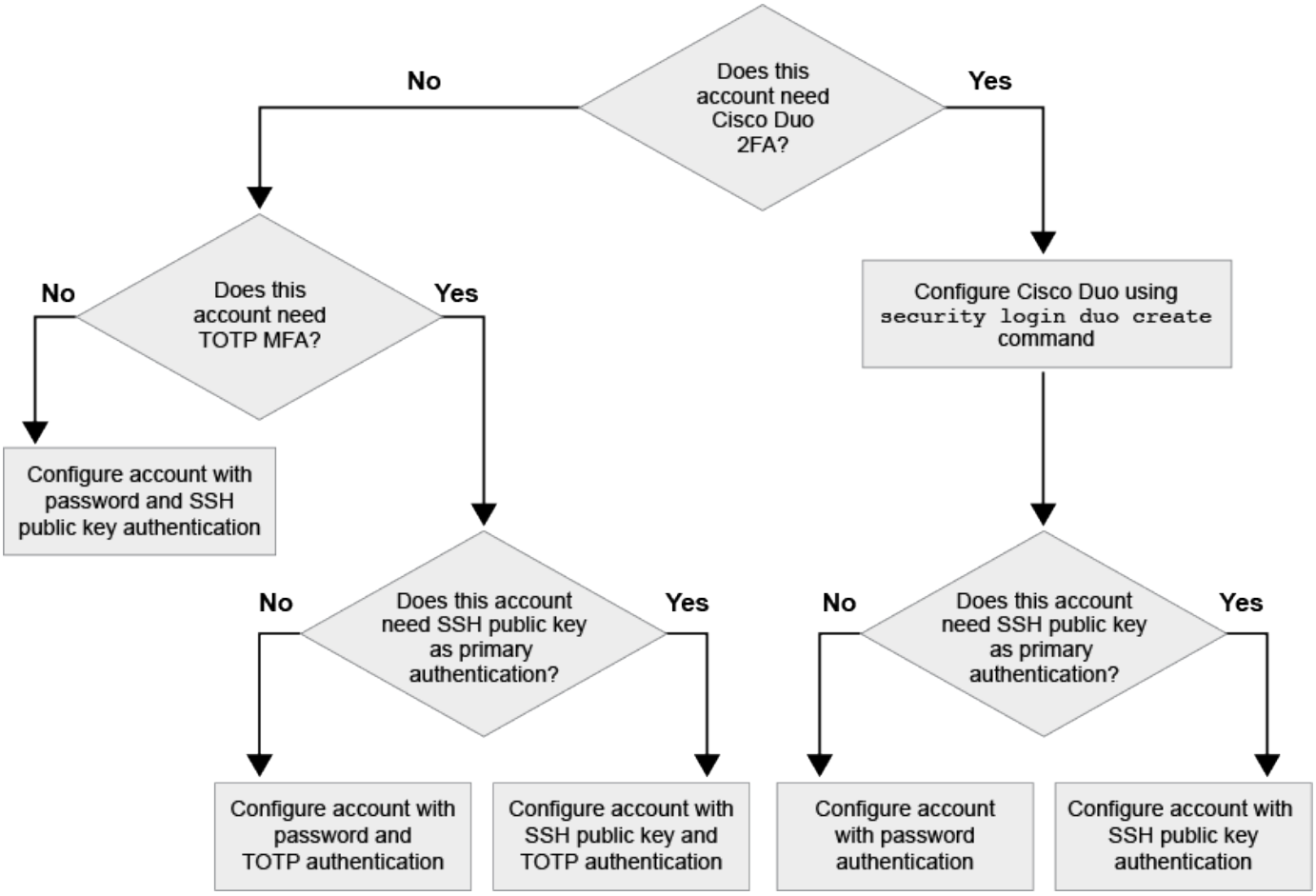
Ulteriori informazioni sull'autenticazione a più fattori ONTAP

La Multifactor Authentication (MFA) consente di migliorare la sicurezza richiedendo agli utenti di fornire due metodi di autenticazione per l'accesso a una VM di amministrazione o per lo storage dei dati.

A seconda della versione di ONTAP in uso, è possibile utilizzare una combinazione di chiave pubblica SSH, una password utente e una password monouso (TOTP) basata sul tempo per l'autenticazione multifattore. Quando si attiva e si configura Cisco Duo (ONTAP 9.14.1 e versioni successive), questo metodo funge da metodo di autenticazione aggiuntivo, che integra i metodi esistenti per tutti gli utenti.

Disponibile a partire da…	Primo metodo di autenticazione	Secondo metodo di autenticazione
ONTAP 9.14.1	Chiave pubblica SSH	TTP
	User Password (Password utente)	TTP
	Chiave pubblica SSH	Cisco Duo
	Password utente	Cisco Duo
ONTAP 9.13.1	Chiave pubblica SSH	TTP
	Password utente	TTP
ONTAP 9.3	Chiave pubblica SSH	Password utente

Se MFA è configurato, l'amministratore del cluster deve prima abilitare l'account utente locale, quindi l'account deve essere configurato dall'utente locale.



Abilita l'autenticazione a più fattori ONTAP con SSH e TOTP

L'autenticazione a più fattori (MFA) consente di migliorare la sicurezza richiedendo agli utenti di fornire due metodi di autenticazione per accedere a un'SVM amministrativa o di dati.

A proposito di questa attività

- Per eseguire questa attività, è necessario essere un amministratore del cluster.
- Se non si è certi del ruolo di controllo dell'accesso che si desidera assegnare all'account di accesso, è possibile utilizzare il `security login modify` comando per aggiungere il ruolo in un secondo momento.

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

  "Modifica del ruolo assegnato a un amministratore"

- Se si utilizza una chiave pubblica per l'autenticazione, è necessario associare la chiave pubblica all'account prima che l'account possa accedere a SVM.

  "Associare una chiave pubblica a un account utente"

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

- A partire da ONTAP 9.12.1, è possibile utilizzare i dispositivi di autenticazione hardware di Yubikey per l'autenticazione MFA del client SSH utilizzando gli standard di autenticazione FIDO2 (Fast Identity Online)

o Personal Identity Verification (PIV).

Abilitare MFA con chiave pubblica SSH e password utente

A partire da ONTAP 9.3, un amministratore del cluster può configurare account utente locali per l'accesso con MFA utilizzando una chiave pubblica SSH e una password utente.

1. Abilitare MFA sull'account utente locale con chiave pubblica SSH e password utente:

```
security login create -vserver <svm_name> -user-or-group-name
<user_name> -application ssh -authentication-method <password|publickey>
-role admin -second-authentication-method <password|publickey>
```

Il seguente comando richiede l'account amministratore SVM `admin2` con il predefinito `admin` Ruolo di accesso a SVM`engData1` Con una chiave pubblica SSH e una password utente:

```
cluster-1::> security login create -vserver engData1 -user-or-group-name
admin2 -application ssh -authentication-method publickey -role admin
-second-authentication-method password

Please enter a password for user 'admin2':
Please enter it again:
Warning: To use public-key authentication, you must create a public key
for user "admin2".
```

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

Abilitare MFA con TOTP

A partire da ONTAP 9.13.1, è possibile migliorare la sicurezza richiedendo agli utenti locali di accedere a un server di amministrazione o a una SVM di dati con una chiave pubblica SSH o una password utente e una password monouso (TOTP) basata sul tempo. Una volta abilitato l'account MFA con TOTP, l'utente locale deve effettuare l'accesso a. "completare la configurazione".

TOTP è un algoritmo per computer che utilizza l'ora corrente per generare una password monouso. Se si utilizza il protocollo TOTP, si tratta sempre della seconda forma di autenticazione dopo la chiave pubblica SSH o la password dell'utente.

Prima di iniziare

Per eseguire queste attività, è necessario essere un amministratore dello storage.

Fasi

È possibile impostare MFA su con una password utente o una chiave pubblica SSH come primo metodo di autenticazione e TOTP come secondo metodo di autenticazione.

Abilitare MFA con password utente e TOTP

1. Abilitare un account utente per l'autenticazione a più fattori con una password utente e TOTP.

   Per nuovi account utente

   ```
   security login create -vserver <svm_name> -user-or-group-name
   <user_or_group_name> -application ssh -authentication-method
   password -second-authentication-method totp -role <role> -comment
   <comment>
   ```

   Per gli account utente esistenti

   ```
   security login modify -vserver <svm_name> -user-or-group-name
   <user_or_group_name> -application ssh -authentication-method
   password -second-authentication-method totp -role <role> -comment
   <comment>
   ```

2. Verificare che MFA con TOTP sia attivato:

   ```
   security login show
   ```

Abilitare MFA con chiave pubblica SSH e TOTP

1. Abilitare un account utente per l'autenticazione a più fattori con una chiave pubblica SSH e TOTP.

   Per nuovi account utente

   ```
   security login create -vserver <svm_name> -user-or-group-name
   <user_or_group_name> -application ssh -authentication-method
   publickey -second-authentication-method totp -role <role> -comment
   <comment>
   ```

   Per gli account utente esistenti

   ```
   security login modify -vserver <svm_name> -user-or-group-name
   <user_or_group_name> -application ssh -authentication-method
   publickey -second-authentication-method totp -role <role> -comment
   <comment>
   ```

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

2. Verificare che MFA con TOTP sia attivato:

```
security login show
```

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

Al termine

- Se non è stata associata una chiave pubblica all'account amministratore, è necessario farlo prima che l'account possa accedere a SVM.

  "Associazione di una chiave pubblica a un account utente"

- L'utente locale deve effettuare l'accesso per completare la configurazione MFA con TOTP.

  "Configurare l'account utente locale per MFA con TOTP"

Informazioni correlate

- "Autenticazione multifattore in ONTAP 9 (TR-4647)"
- "Riferimento al comando ONTAP"

Configurare gli account utente ONTAP locali per MFA con TOTP

A partire da ONTAP 9.13.1, gli account utente possono essere configurati con Multifactor Authentication (MFA) utilizzando una password monouso basata sul tempo (TOTP).

Prima di iniziare

- L'amministratore dello storage deve "Abilitare MFA con TOTP" come secondo metodo di autenticazione per l'account utente.
- Il metodo di autenticazione dell'account utente principale deve essere una password utente o una chiave SSH pubblica.
- È necessario configurare l'applicazione TOTP per il funzionamento con lo smartphone e creare la chiave segreta TOTP.

  Sono supportati Microsoft Authenticator, Google Authenticator, Authy e qualsiasi altro autenticatore compatibile con TOTP.

Fasi

1. Accedere all'account utente con il metodo di autenticazione corrente.

   Il metodo di autenticazione corrente deve essere una password utente o una chiave pubblica SSH.

2. Creare la configurazione TOTP sull'account:

   ```
   security login totp create -vserver "<svm_name>" -username
   "<account_username >"
   ```

3. Verificare che la configurazione TOTP sia attivata sull'account:

```
security login totp show -vserver "<svm_name>" -username
"<account_username>"
```

Informazioni correlate

- "creazione di accesso di sicurezza tottop"
- "accesso di sicurezza tottop show"

Reimpostare la chiave segreta TOTP per un account utente ONTAP

Per proteggere la sicurezza del tuo account, se la tua chiave segreta TOTP viene compromessa o persa, devi disattivarla e crearne una nuova.

Reimpostare il TOTP se la chiave viene compromessa

Se la chiave segreta TOTP è compromessa, ma si dispone ancora dell'accesso, è possibile rimuovere la chiave compromessa e crearne una nuova.

1. Accedere all'account utente con la password utente o la chiave pubblica SSH e la chiave segreta TOTP compromessa.
2. Rimuovere la chiave segreta TOTP compromessa:

```
security login totp delete -vserver <svm_name> -username
<account_username>
```

3. Creare una nuova chiave segreta TOTP:

```
security login totp create -vserver <svm_name> -username
<account_username>
```

4. Verificare che la configurazione TOTP sia attivata sull'account:

```
security login totp show -vserver <svm_name> -username
<account_username>
```

Ripristinare il TOTP se la chiave viene persa

Se la chiave segreta TOTP viene persa, contattare l'amministratore dello storage per "disattivare la chiave". Una volta disattivata la chiave, è possibile utilizzare il primo metodo di autenticazione per accedere e configurare un nuovo TOTP.

Prima di iniziare

La chiave segreta TOTP deve essere disattivata da un amministratore dello storage. Se non si dispone di un account amministratore dello storage, contattare l'amministratore dello storage per disattivare la chiave.

Fasi

1. Una volta disattivato il segreto TOTP da un amministratore dello storage, utilizzare il metodo di autenticazione principale per accedere all'account locale.
2. Creare una nuova chiave segreta TOTP:

```
security login totp create -vserver <svm_name> -username
<account_username >
```

3. Verificare che la configurazione TOTP sia attivata sull'account:

```
security login totp show -vserver <svm_name> -username
<account_username>
```

Informazioni correlate

- "creazione di accesso di sicurezza tottop"
- "accesso di sicurezza tottop elimina"
- "accesso di sicurezza tottop show"

Disattivare la chiave segreta TOTP per un account utente ONTAP

Se la chiave segreta TOTP (Time-Based One-Time Password) di un utente locale viene persa, la chiave persa deve essere disattivata da un amministratore dello storage prima che l'utente possa creare una nuova chiave segreta TOTP.

A proposito di questa attività

Questa attività può essere eseguita solo da un account amministratore del cluster.

Fase

1. Disattivare la chiave segreta TOTP:

```
security login totp modify -vserver <svm_name> -username
<account_username> -enabled false
```

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

Attiva l'accesso all'account ONTAP del certificato SSL

Puoi utilizzare `security login create` il comando per abilitare gli account amministratore ad accedere a una SVM di amministrazione o dati con un certificato SSL.

A proposito di questa attività

- È necessario installare un certificato digitale del server firmato dalla CA prima che l'account possa accedere alla SVM.

Creazione e installazione di un certificato server firmato dalla CA

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

- Se non si è sicuri del ruolo di controllo degli accessi che si desidera assegnare all'account di accesso, è possibile aggiungerlo successivamente con `security login modify` comando.

Modifica del ruolo assegnato a un amministratore

> Per gli account degli amministratori del cluster, l'autenticazione del certificato è supportata con `http`, `ontapi`, e. `rest` applicazioni. Per gli account amministratore SVM, l'autenticazione del certificato è supportata solo con `ontapi` e. `rest` applicazioni.

Fase

1. Abilitare gli account dell'amministratore locale per accedere a una SVM utilizzando un certificato SSL:

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

   Il seguente comando attiva l'account amministratore SVM `svmadmin2` con l'impostazione predefinita `vsadmin` Ruolo per accedere a SVM`engData2` Utilizzando un certificato digitale SSL.

   ```
   cluster1::>security login create -vserver engData2 -user-or-group-name
   svmadmin2 -application ontapi -authmethod cert
   ```

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

Al termine

Se non è stato installato un certificato digitale del server firmato dalla CA, è necessario farlo prima che l'account possa accedere alla SVM.

Creazione e installazione di un certificato server firmato dalla CA

Per ulteriori informazioni sui comandi descritti in questa procedura, consultare la "Riferimento al comando ONTAP".

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.