



# Certificati

## SANtricity 11.7

NetApp  
February 12, 2024

# Sommario

- Certificati ..... 1
  - Panoramica dei certificati ..... 1
  - Concetti ..... 1
  - Utilizzare i certificati firmati dalla CA per il sistema di gestione ..... 4
  - Reimpostare i certificati di gestione ..... 6
  - Utilizzare certificati array ..... 7
  - Gestire i certificati ..... 9

# Certificati

## Panoramica dei certificati

Gestione certificati consente di creare richieste di firma del certificato (CSR), importare certificati e gestire i certificati esistenti.

### Cosa sono i certificati?

I *certificati* sono file digitali che identificano entità online, come siti Web e server, per comunicazioni sicure su Internet. Esistono due tipi di certificati: Un *certificato firmato* viene validato da un'autorità di certificazione (CA) e un *certificato autofirmato* viene validato dal proprietario dell'entità anziché da una terza parte.

Scopri di più:

- ["Come funzionano i certificati"](#)
- ["Terminologia del certificato"](#)

### Come si configurano i certificati?

Da Certificate Management, è possibile configurare i certificati per la stazione di gestione che ospita Unified Manager e importare i certificati per i controller negli array.

Scopri di più:

- ["Utilizzare i certificati firmati dalla CA per il sistema di gestione"](#)
- ["Importare certificati per gli array"](#)

## Concetti

### Come funzionano i certificati

I certificati sono file digitali che identificano entità online, come siti Web e server, per comunicazioni sicure su Internet.

#### Certificati firmati

I certificati garantiscono che le comunicazioni web vengano trasmesse in forma crittografata, privatamente e inalterate, solo tra il server e il client specificati. Con Unified Manager, è possibile gestire i certificati per il browser su un sistema di gestione host e i controller negli array di storage rilevati.

Un certificato può essere firmato da un'autorità attendibile o autofirmato. "Firmare" significa semplicemente che qualcuno ha convalidato l'identità del proprietario e determinato che i loro dispositivi possono essere affidabili. Gli array di storage vengono forniti con un certificato autofirmato generato automaticamente su ciascun controller. È possibile continuare a utilizzare i certificati autofirmati oppure ottenere certificati firmati dalla CA per una connessione più sicura tra i controller e i sistemi host.



Sebbene i certificati firmati dalla CA forniscano una migliore protezione di sicurezza (ad esempio, prevenendo gli attacchi man-in-the-middle), richiedono anche tariffe che possono essere costose se si dispone di una rete di grandi dimensioni. Al contrario, i certificati autofirmati sono meno sicuri, ma sono gratuiti. Pertanto, i certificati autofirmati vengono utilizzati più spesso per ambienti di test interni, non in ambienti di produzione.

Un certificato firmato viene convalidato da un'autorità di certificazione (CA), un'organizzazione di terze parti fidata. I certificati firmati includono i dettagli sul proprietario dell'entità (in genere, un server o un sito Web), la data di emissione e scadenza del certificato, i domini validi per l'entità e una firma digitale composta da lettere e numeri.

Quando si apre un browser e si inserisce un indirizzo Web, il sistema esegue un processo di verifica dei certificati in background per determinare se si sta effettuando la connessione a un sito Web che include un certificato valido firmato dalla CA. In genere, un sito protetto con un certificato firmato include un'icona a forma di lucchetto e una designazione https nell'indirizzo. Se si tenta di connettersi a un sito Web che non contiene un certificato firmato dalla CA, il browser visualizza un avviso che indica che il sito non è sicuro.

La CA esegue le operazioni necessarie per verificare l'identità dell'utente durante il processo dell'applicazione. Potrebbero inviare un'e-mail all'azienda registrata, verificare l'indirizzo aziendale ed eseguire una verifica HTTP o DNS. Una volta completato il processo applicativo, la CA invia i file digitali da caricare su un sistema di gestione host. In genere, questi file includono una catena di attendibilità, come segue:

- **Root** — nella parte superiore della gerarchia si trova il certificato root, che contiene una chiave privata utilizzata per firmare altri certificati. La directory principale identifica un'organizzazione CA specifica. Se si utilizza la stessa CA per tutti i dispositivi di rete, è necessario un solo certificato root.
- **Intermedio** — i certificati intermedi si disconnettono dalla radice. La CA emette uno o più certificati intermedi per fungere da intermediario tra certificati di server e root protetti.
- **Server** — nella parte inferiore della catena si trova il certificato del server, che identifica l'entità specifica dell'utente, ad esempio un sito Web o un altro dispositivo. Ogni controller di uno storage array richiede un certificato server separato.

## Certificati autofirmati

Ogni controller dell'array di storage include un certificato preinstallato e autofirmato. Un certificato autofirmato è simile a un certificato firmato dalla CA, ad eccezione del fatto che è convalidato dal proprietario dell'entità anziché da una terza parte. Come un certificato firmato dalla CA, un certificato autofirmato contiene una propria chiave privata e garantisce inoltre che i dati siano crittografati e inviati tramite una connessione HTTPS tra un server e un client.

I certificati autofirmati non sono "trusted" dai browser. Ogni volta che si tenta di connettersi a un sito Web che contiene solo un certificato autofirmato, il browser visualizza un messaggio di avviso. È necessario fare clic su un collegamento nel messaggio di avviso che consente di accedere al sito Web; in questo modo, si accetta essenzialmente il certificato autofirmato.

## Certificati per Unified Manager

L'interfaccia di Unified Manager viene installata con il proxy dei servizi Web su un sistema host. Quando si apre un browser e si tenta di connettersi a Unified Manager, il browser tenta di verificare che l'host sia un'origine attendibile verificando la presenza di un certificato digitale. Se il browser non individua un certificato firmato dalla CA per il server, viene visualizzato un messaggio di avviso. Da qui, è possibile accedere al sito Web per accettare il certificato autofirmato per la sessione. In alternativa, è possibile ottenere certificati digitali firmati da una CA in modo da non visualizzare più il messaggio di avviso.

## Certificati per i controller

Durante una sessione di Unified Manager, potrebbero essere visualizzati ulteriori messaggi di sicurezza quando si tenta di accedere a un controller che non dispone di un certificato firmato dalla CA. In questo caso, è possibile considerare attendibile in modo permanente il certificato autofirmato oppure importare i certificati firmati dalla CA per i controller in modo che il server Web Services Proxy possa autenticare le richieste client in entrata da questi controller.

## Terminologia del certificato

I seguenti termini si applicano alla gestione dei certificati.

Termine	Descrizione
CIRCA	Un'autorità di certificazione (CA) è un'entità attendibile che emette documenti elettronici, denominati certificati digitali, per la sicurezza di Internet. Questi certificati identificano i proprietari dei siti Web, consentendo connessioni sicure tra client e server.
CSR	Una richiesta di firma del certificato (CSR) è un messaggio inviato da un richiedente a un'autorità di certificazione (CA). La CSR convalida le informazioni richieste dalla CA per il rilascio di un certificato.
Certificato	Un certificato identifica il proprietario di un sito per motivi di sicurezza, impedendo agli autori degli attacchi di impersonare il sito. Il certificato contiene informazioni sul proprietario del sito e l'identità dell'entità attendibile che certifica (firma) queste informazioni.
Catena di certificati	Gerarchia di file che aggiunge un livello di protezione ai certificati. In genere, la catena include un certificato root nella parte superiore della gerarchia, uno o più certificati intermedi e i certificati server che identificano le entità.
Certificato intermedio	Uno o più certificati intermedi si diramano dalla directory principale nella catena di certificati. La CA emette uno o più certificati intermedi per fungere da intermediario tra certificati di server e root protetti.
Archivio chiavi	Un keystore è un repository sul sistema di gestione host che contiene chiavi private, insieme alle chiavi pubbliche e ai certificati corrispondenti. Queste chiavi e certificati identificano le proprie entità, ad esempio i controller.
Certificato root	Il certificato root si trova nella parte superiore della gerarchia nella catena del certificato e contiene una chiave privata utilizzata per firmare altri certificati. La directory principale identifica un'organizzazione CA specifica. Se si utilizza la stessa CA per tutti i dispositivi di rete, è necessario un solo certificato root.

Termine	Descrizione
Certificato firmato	Certificato convalidato da un'autorità di certificazione (CA). Questo file di dati contiene una chiave privata e garantisce che i dati vengano inviati in forma crittografata tra un server e un client tramite una connessione HTTPS. Inoltre, un certificato firmato include i dettagli relativi al proprietario dell'entità (in genere, un server o un sito Web) e una firma digitale composta da lettere e numeri. Un certificato firmato utilizza una catena di trust e quindi viene utilizzato più spesso negli ambienti di produzione. Definito anche "certificato firmato da CA" o "certificato di gestione".
Certificato autofirmato	Un certificato autofirmato viene validato dal proprietario dell'entità. Questo file di dati contiene una chiave privata e garantisce che i dati vengano inviati in forma crittografata tra un server e un client tramite una connessione HTTPS. Include anche una firma digitale composta da lettere e numeri. Un certificato autofirmato non utilizza la stessa catena di attendibilità di un certificato firmato dalla CA e, di conseguenza, viene spesso utilizzato negli ambienti di test. Detto anche certificato "preinstallato".
Certificato del server	Il certificato del server si trova nella parte inferiore della catena di certificati. Identifica l'entità specifica dell'utente, ad esempio un sito Web o un altro dispositivo. Ogni controller di un sistema storage richiede un certificato server separato.
Truststore	Un truststore è un repository che contiene certificati di terze parti attendibili, ad esempio CA.

## Utilizzare i certificati firmati dalla CA per il sistema di gestione

È possibile ottenere e importare certificati firmati dalla CA per un accesso sicuro al sistema di gestione che ospita Unified Manager.

### Prima di iniziare

È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni del certificato non vengono visualizzate.

### A proposito di questa attività

L'utilizzo dei certificati firmati dalla CA è una procedura in tre fasi.

### Fase 1: Completare un file CSR

È necessario innanzitutto generare un file CSR (Certificate Signing Request) che identifichi l'organizzazione e il sistema host in cui sono installati Web Services Proxy e Unified Manager.



In alternativa, è possibile generare un file CSR utilizzando uno strumento come OpenSSL e passare a [Fase 2: Inviare il file CSR](#).

### Fasi

1. Selezionare **Certificate Management** (Gestione certificati).
2. Dalla scheda Management (Gestione), selezionare **complete CSR** (completa CSR).
3. Inserire le seguenti informazioni, quindi fare clic su **Avanti**:
  - **Organizzazione** — il nome completo e legale della tua azienda o organizzazione. Includere i suffissi, ad esempio Inc. O Corp.
  - **Unità organizzativa (opzionale)** — la divisione dell'organizzazione che gestisce il certificato.
  - **Città/Località** — la città in cui si trova il sistema host o l'azienda.
  - **Stato/Regione (opzionale)** — Stato o regione in cui si trova il sistema host o l'azienda.
  - **Codice ISO del Paese** — Codice ISO (International Organization for Standardization) a due cifre del Paese, ad esempio USA.
4. Inserire le seguenti informazioni sul sistema host in cui è installato il proxy dei servizi Web:
  - **Nome comune** — Indirizzo IP o nome DNS del sistema host in cui è installato il proxy dei servizi Web. Assicurarsi che l'indirizzo sia corretto; deve corrispondere esattamente a quello immesso per accedere a Unified Manager nel browser. Non includere http:// o https://. Il nome DNS non può iniziare con un carattere jolly.
  - **Indirizzi IP alternativi** — se il nome comune è un indirizzo IP, è possibile inserire eventuali indirizzi IP o alias aggiuntivi per il sistema host. Per più voci, utilizzare un formato delimitato da virgole.
  - **Nomi DNS alternativi** — se il nome comune è un nome DNS, immettere eventuali nomi DNS aggiuntivi per il sistema host. Per più voci, utilizzare un formato delimitato da virgole. Se non sono presenti nomi DNS alternativi, ma è stato immesso un nome DNS nel primo campo, copiarlo qui. Il nome DNS non può iniziare con un carattere jolly.
5. Assicurarsi che le informazioni sull'host siano corrette. In caso contrario, i certificati restituiti dalla CA non avranno esito positivo quando si tenta di importarli.
6. Fare clic su **fine**.
7. Passare a. [Fase 2: Inviare il file CSR](#).

## Fase 2: Inviare il file CSR

Dopo aver creato un file di richiesta di firma del certificato (CSR), lo si invia a un'autorità di certificazione (CA) per ricevere certificati di gestione firmati per il sistema che ospita Unified Manager e Web Services Proxy.



I sistemi e-Series richiedono il formato PEM (codifica ASCII Base64) per i certificati firmati, che include i seguenti tipi di file: .Pem, .crt, .cer o .key.

### Fasi

1. Individuare il file CSR scaricato.

La posizione della cartella del download dipende dal browser in uso.

2. Inviare il file CSR a una CA (ad esempio, VeriSign o DigiCert) e richiedere certificati firmati in formato PEM.



**Dopo aver inviato un file CSR alla CA, NON rigenerare un altro file CSR.** ogni volta che si genera una CSR, il sistema crea una coppia di chiavi privata e pubblica. La chiave pubblica fa parte della CSR, mentre la chiave privata viene conservata nell'archivio chiavi del sistema. Quando si ricevono i certificati firmati e li si importano, il sistema garantisce che sia la chiave privata che la chiave pubblica siano la coppia originale. Se le chiavi non corrispondono, i certificati firmati non funzioneranno ed è necessario richiedere nuovi certificati alla CA.

3. Quando la CA restituisce i certificati firmati, passare a. [Fase 3: Importazione dei certificati di gestione.](#)

## Fase 3: Importazione dei certificati di gestione

Dopo aver ricevuto i certificati firmati dall'autorità di certificazione (CA), importare i certificati nel sistema host in cui sono installati Web Services Proxy e l'interfaccia di Unified Manager.

### Prima di iniziare

- Sono stati ricevuti certificati firmati dalla CA. Questi file includono il certificato di origine, uno o più certificati intermedi e il certificato del server.
- Se la CA ha fornito un file di certificato concatenato (ad esempio, un file .p7b), è necessario decomprimere il file concatenato in singoli file: il certificato root, uno o più certificati intermedi e il certificato del server. È possibile utilizzare Windows `certmgr` Utility per disimballare i file (fare clic con il pulsante destro del mouse e selezionare **All Tasks > Export**). Si consiglia la codifica base-64. Una volta completate le esportazioni, viene visualizzato un file CER per ciascun file di certificato nella catena.
- I file dei certificati sono stati copiati nel sistema host in cui è in esecuzione il proxy dei servizi Web.

### Fasi

1. Selezionare **Certificate Management** (Gestione certificati).
2. Dalla scheda Management (Gestione), selezionare **Import** (Importa).

Viene visualizzata una finestra di dialogo per l'importazione dei file dei certificati.

3. Fare clic su **Browse** (Sfoglia) per selezionare prima i file dei certificati root e intermedi, quindi selezionare il certificato del server. Se la CSR è stata generata da uno strumento esterno, è necessario importare anche il file della chiave privata creato insieme alla CSR.

I nomi dei file vengono visualizzati nella finestra di dialogo.

4. Fare clic su **Importa**.

### Risultati

I file vengono caricati e validati. Le informazioni sul certificato vengono visualizzate nella pagina Gestione certificati.

## Reimpostare i certificati di gestione

È possibile ripristinare lo stato originale autofirmato del certificato di gestione.

### Prima di iniziare

È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni del certificato non vengono visualizzate.



## A proposito di questa attività

Questa attività elimina il certificato di gestione corrente dal sistema host in cui sono installati Web Services Proxy e Unified Manager. Una volta ripristinato il certificato, il sistema host torna a utilizzare il certificato autofirmato.

### Fasi

1. Selezionare **Certificate Management** (Gestione certificati).
2. Dalla scheda Management (Gestione), selezionare **Reset** (Ripristina).

Viene visualizzata la finestra di dialogo Conferma ripristino certificato di gestione.

3. Tipo `reset` Nel campo, quindi fare clic su **Reset**.

Dopo l'aggiornamento del browser, il browser potrebbe bloccare l'accesso al sito di destinazione e segnalare che il sito utilizza HTTP Strict Transport Security. Questa condizione si verifica quando si torna ai certificati autofirmati. Per eliminare la condizione che sta bloccando l'accesso alla destinazione, è necessario cancellare i dati di navigazione dal browser.

### Risultati

Il sistema torna a utilizzare il certificato autofirmato dal server. Di conseguenza, il sistema richiede agli utenti di accettare manualmente il certificato autofirmato per le sessioni.

## Utilizzare certificati array

### Importare certificati per gli array

Se necessario, è possibile importare i certificati per gli array di storage in modo che possano autenticarsi con il sistema che ospita Unified Manager. I certificati possono essere firmati da un'autorità di certificazione (CA) o autofirmati.

#### Prima di iniziare

- È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni del certificato non vengono visualizzate.
- Se si importano certificati attendibili, è necessario importarli per i controller degli array di storage utilizzando System Manager.

### Fasi

1. Selezionare **Certificate Management** (Gestione certificati).
2. Selezionare la scheda **Trusted**.

Questa pagina mostra tutti i certificati segnalati per gli array di storage.

3. Selezionare il **Importa > certificati** per importare un certificato CA oppure il **Importa > certificati array storage autofirmati** per importare un certificato autofirmato.

Per limitare la visualizzazione, è possibile utilizzare il campo di filtraggio **Mostra certificati...** oppure ordinare le righe dei certificati facendo clic su una delle intestazioni di colonna.

4. Nella finestra di dialogo, selezionare il certificato e fare clic su **Importa**.

Il certificato viene caricato e validato.

## Eliminare i certificati attendibili

È possibile eliminare uno o più certificati non più necessari, ad esempio un certificato scaduto.

### Prima di iniziare

Importare il nuovo certificato prima di eliminarlo.



Tenere presente che l'eliminazione di un certificato root o intermedio può influire su più array di storage, poiché questi array possono condividere gli stessi file di certificato.

### Fasi

1. Selezionare **Certificate Management** (Gestione certificati).
2. Selezionare la scheda **Trusted**.
3. Selezionare uno o più certificati nella tabella, quindi fare clic su **Elimina**.



La funzione **Delete** non è disponibile per i certificati preinstallati.

Viene visualizzata la finestra di dialogo Conferma eliminazione certificato attendibile.

4. Confermare l'eliminazione, quindi fare clic su **Delete** (Elimina).

Il certificato viene rimosso dalla tabella.

## Risolvi i certificati non attendibili

I certificati non attendibili si verificano quando uno storage array tenta di stabilire una connessione sicura a Unified Manager, ma la connessione non viene confermata come sicura.

Dalla pagina Certificate (certificato), è possibile risolvere i certificati non attendibili importando un certificato autofirmato dall'array di storage o importando un certificato dell'autorità di certificazione (CA) emesso da una terza parte attendibile.

### Prima di iniziare

- È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore della sicurezza.
- Se si intende importare un certificato firmato dalla CA:
  - È stata generata una richiesta di firma del certificato (file CSR) per ciascun controller nell'array di storage e inviata alla CA.
  - La CA ha restituito file di certificato attendibili.
  - I file dei certificati sono disponibili nel sistema locale.

### A proposito di questa attività

Potrebbe essere necessario installare altri certificati CA attendibili se si verifica una delle seguenti condizioni:

- Di recente è stato aggiunto uno storage array.
- Uno o entrambi i certificati sono scaduti.
- Uno o entrambi i certificati vengono revocati.
- Uno o entrambi i certificati non dispongono di un certificato root o intermedio.

#### Fasi

1. Selezionare **Certificate Management** (Gestione certificati).
2. Selezionare la scheda **Trusted**.

Questa pagina mostra tutti i certificati segnalati per gli array di storage.

3. Selezionare il **Importa > certificati** per importare un certificato CA oppure il **Importa > certificati array storage autofirmati** per importare un certificato autofirmato.

Per limitare la visualizzazione, è possibile utilizzare il campo di filtraggio **Mostra certificati...** oppure ordinare le righe dei certificati facendo clic su una delle intestazioni di colonna.

4. Nella finestra di dialogo, selezionare il certificato, quindi fare clic su **Importa**.

Il certificato viene caricato e validato.

## Gestire i certificati

### Visualizzare i certificati

È possibile visualizzare informazioni riepilogative per un certificato, che includono l'organizzazione che utilizza il certificato, l'autorità che ha emesso il certificato, il periodo di validità e le impronte digitali (identificatori univoci).

#### Prima di iniziare

È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni del certificato non vengono visualizzate.

#### Fasi

1. Selezionare **Certificate Management** (Gestione certificati).
2. Selezionare una delle seguenti schede:
  - **Gestione** — Mostra il certificato per il sistema che ospita il proxy dei servizi Web. Un certificato di gestione può essere autofirmato o approvato da un'autorità di certificazione (CA). Consente un accesso sicuro a Unified Manager.
  - **Trusted** — Mostra i certificati a cui Unified Manager può accedere per storage array e altri server remoti, come un server LDAP. I certificati possono essere emessi da un'autorità di certificazione (CA) o autofirmati.
3. Per visualizzare ulteriori informazioni su un certificato, selezionare la relativa riga, selezionare i puntini di sospensione alla fine della riga, quindi fare clic su **Visualizza** o **Esporta**.

### Esportare i certificati

È possibile esportare un certificato per visualizzarne i dettagli completi.

## Prima di iniziare

Per aprire il file esportato, è necessario disporre di un'applicazione per il visualizzatore dei certificati.

## Fasi

1. Selezionare **Certificate Management** (Gestione certificati).
2. Selezionare una delle seguenti schede:
  - **Gestione** — Mostra il certificato per il sistema che ospita il proxy dei servizi Web. Un certificato di gestione può essere autofirmato o approvato da un'autorità di certificazione (CA). Consente un accesso sicuro a Unified Manager.
  - **Trusted** — Mostra i certificati a cui Unified Manager può accedere per storage array e altri server remoti, come un server LDAP. I certificati possono essere emessi da un'autorità di certificazione (CA) o autofirmati.
3. Selezionare un certificato dalla pagina, quindi fare clic sui puntini di sospensione alla fine della riga.
4. Fare clic su **Esporta**, quindi salvare il file del certificato.
5. Aprire il file nell'applicazione di visualizzazione dei certificati.

## 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.