



Certificati e autenticazione

SANtricity 11.6

NetApp
February 12, 2024

Sommario

- Certificati e autenticazione 1
 - Gestione dei certificati 1
 - Gestione degli accessi 9

Certificati e autenticazione

Gestione dei certificati

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.

Termine	Descrizione
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.
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.
Proxy dei servizi Web	Il proxy dei servizi Web, che fornisce l'accesso tramite meccanismi HTTPS standard, consente agli amministratori di configurare i servizi di gestione per gli array di storage. Il proxy può essere installato su host Windows o Linux. L'interfaccia di Unified Manager viene fornita in bundle con il proxy dei servizi Web.

Come fare

USA certificati firmati dalla CA

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 due fasi.

Fase 1: Completare e inviare una CSR

È necessario innanzitutto generare un file CSR (Certificate Signing Request) e inviarlo alla CA.

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 descrive come generare il file CSR inviato a una CA per ricevere certificati di gestione firmati per il sistema che ospita Unified Manager e Web Services Proxy. È necessario fornire informazioni sull'organizzazione, oltre all'indirizzo IP o al nome DNS del sistema host.



Non generare una nuova CSR dopo l'invio alla CA. Quando si genera una CSR, il sistema crea una coppia di chiavi private e pubbliche. La chiave pubblica fa parte della CSR, mentre la chiave privata viene conservata nell'archivio chiavi. Quando si ricevono i certificati firmati e li si importano nel keystore, il sistema garantisce che sia le chiavi private che quelle pubbliche siano la coppia originale. Pertanto, non è necessario generare una nuova CSR dopo averla inoltrata alla CA. In tal caso, i controller generano nuove chiavi e i certificati ricevuti dalla CA non funzioneranno.

Fasi

1. Selezionare **Certificate Management** (Gestione certificati).
2. Dalla scheda **Gestione**, selezionare **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 relative al sistema host:
 - **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://.

- **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.

5. Fare clic su **fine**.

Un file CSR viene scaricato nel sistema locale. La posizione della cartella del download dipende dal browser in uso.

6. Inviare il file CSR a una CA e richiedere certificati firmati in formato PEM o DER.

Al termine

Attendere che la CA restituisca i file di certificato, quindi passare a. "[Fase 2: Importazione dei certificati di gestione](#)".

Fase 2: Importazione dei certificati di gestione

Una volta ricevuti i certificati firmati, importare la catena di certificati per il sistema host in cui è installata l'interfaccia di 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.
- È stata generata una richiesta di firma del certificato (file CSR) e inviata alla CA.
- La CA ha restituito file di certificato attendibili.
- I file dei certificati vengono installati nel sistema locale.
- Se la CA ha fornito un 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 **tutte le attività > Esporta**). Una volta completate le esportazioni, viene visualizzato un file CER per ciascun file di certificato nella catena.

Fasi

1. Selezionare **Certificate Management** (Gestione certificati).
2. Dalla scheda **Gestione**, selezionare **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 root e intermedi, quindi selezionare il certificato del server.

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 il proxy dei servizi Web e il gestore unificato di SANtricity. 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**, selezionare **Reset**.

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.

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 SANtricity 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 Gestione di sistema di SANtricity.

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 **Importa > certificati** per importare un certificato CA oppure **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.

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.

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 un array di storage tenta di stabilire una connessione sicura a Gestione unificata di SANtricity, 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 **Importa > certificati**. Per importare un certificato CA o **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.

Gestione degli accessi

Concetti

Come funziona Access Management

Utilizzare la gestione degli accessi per stabilire l'autenticazione dell'utente in Gestione unificata di SANtricity.

Workflow di configurazione

La configurazione di Access Management funziona come segue:

1. Un amministratore effettua l'accesso a Unified Manager con un profilo utente che include le autorizzazioni di amministratore di sicurezza.



Per il primo accesso, il nome utente `admin` viene visualizzato automaticamente e non può essere modificato. Il `admin` l'utente ha accesso completo a tutte le funzioni del sistema. La password deve essere impostata al primo accesso.

2. L'amministratore accede a Access Management nell'interfaccia utente, che include ruoli utente locali preconfigurati. Questi ruoli sono un'implementazione delle funzionalità RBAC (role-based access control).
3. L'amministratore configura uno o più dei seguenti metodi di autenticazione:
 - **Ruoli utente locali** — l'autenticazione viene gestita tramite funzionalità RBAC. I ruoli utente locali includono utenti predefiniti e ruoli con autorizzazioni di accesso specifiche. Gli amministratori possono utilizzare questi ruoli utente locali come singolo metodo di autenticazione o in combinazione con un

servizio di directory. Non è necessaria alcuna configurazione, ad eccezione dell'impostazione delle password per gli utenti.

- **Servizi di directory** — l'autenticazione viene gestita tramite un server LDAP (Lightweight Directory Access Protocol) e un servizio di directory, ad esempio Active Directory di Microsoft. Un amministratore si connette al server LDAP, quindi associa gli utenti LDAP ai ruoli utente locali.

4. L'amministratore fornisce agli utenti le credenziali di accesso per Unified Manager.

5. Gli utenti accedono al sistema inserendo le proprie credenziali. Durante l'accesso, il sistema esegue le seguenti attività in background:

- Autentica il nome utente e la password rispetto all'account utente.
- Determina le autorizzazioni dell'utente in base ai ruoli assegnati.
- Fornisce all'utente l'accesso alle funzioni dell'interfaccia utente.
- Visualizza il nome utente nel banner superiore.

Funzioni disponibili in Unified Manager

L'accesso alle funzioni dipende dai ruoli assegnati a un utente, che includono:

- **Storage admin** — accesso completo in lettura/scrittura agli oggetti storage sugli array, ma nessun accesso alla configurazione di sicurezza.
- **Security admin** — accesso alla configurazione di sicurezza in Access Management e Certificate Management.
- **Support admin** — accesso a tutte le risorse hardware su storage array, dati di guasto ed eventi MEL. Nessun accesso agli oggetti di storage o alla configurazione di sicurezza.
- **Monitor** — accesso in sola lettura a tutti gli oggetti di storage, ma nessun accesso alla configurazione di sicurezza.

Una funzione non disponibile è disattivata o non viene visualizzata nell'interfaccia utente.

Terminologia per la gestione degli accessi

Scopri come si applicano i termini di gestione degli accessi a SANtricity Unified Manager.

Termine	Descrizione
Active Directory	Active Directory (ad) è un servizio di directory Microsoft che utilizza LDAP per le reti di dominio Windows.
Binding	Le operazioni BIND vengono utilizzate per autenticare i client nel server di directory. Il binding in genere richiede credenziali di account e password, ma alcuni server consentono operazioni di binding anonime.
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.

Termine	Descrizione
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.
LDAP	LDAP (Lightweight Directory Access Protocol) è un protocollo applicativo per l'accesso e la manutenzione dei servizi informativi di directory distribuiti. Questo protocollo consente a numerose applicazioni e servizi diversi di connettersi al server LDAP per la convalida degli utenti.
RBAC	RBAC (role-based access control) è un metodo per regolare l'accesso alle risorse di computer o di rete in base ai ruoli dei singoli utenti. Unified Manager include ruoli predefiniti.
SSO	SSO (Single Sign-on) è un servizio di autenticazione che consente a un set di credenziali di accesso di accedere a più applicazioni.
Proxy dei servizi Web	Il proxy dei servizi Web, che fornisce l'accesso tramite meccanismi HTTPS standard, consente agli amministratori di configurare i servizi di gestione per gli array di storage. Il proxy può essere installato su host Windows o Linux. L'interfaccia di Unified Manager è disponibile con Web Services Proxy.

Autorizzazioni per i ruoli mappati

Le funzionalità RBAC (role-based access control) includono utenti predefiniti con uno o più ruoli mappati. Ogni ruolo include le autorizzazioni per l'accesso alle attività in Gestione unificata di SANtricity.

I ruoli forniscono agli utenti l'accesso alle attività, come segue:

- **Storage admin** — accesso completo in lettura/scrittura agli oggetti storage sugli array, ma nessun accesso alla configurazione di sicurezza.
- **Security admin** — accesso alla configurazione di sicurezza in Access Management e Certificate Management.
- **Support admin** — accesso a tutte le risorse hardware su storage array, dati di guasto ed eventi MEL. Nessun accesso agli oggetti di storage o alla configurazione di sicurezza.
- **Monitor** — accesso in sola lettura a tutti gli oggetti di storage, ma nessun accesso alla configurazione di sicurezza.

Se un utente non dispone delle autorizzazioni per una determinata funzione, tale funzione non è disponibile per la selezione o non viene visualizzata nell'interfaccia utente.

Gestione degli accessi con ruoli utente locali

Gli amministratori possono utilizzare le funzionalità RBAC (role-based access control) applicate in Gestione unificata di SANtricity. Queste funzionalità sono denominate "ruoli utente locali".

Workflow di configurazione

I ruoli utente locali sono preconfigurati nel sistema. Per utilizzare i ruoli utente locali per l'autenticazione, gli amministratori possono:

1. Un amministratore effettua l'accesso a Unified Manager con un profilo utente che include le autorizzazioni di amministratore di sicurezza.



Il `admin` l'utente ha accesso completo a tutte le funzioni del sistema.

2. Un amministratore esamina i profili utente predefiniti e non modificabili.
3. **Opzionale:** l'amministratore assegna nuove password per ogni profilo utente.
4. Gli utenti accedono al sistema con le credenziali assegnate.

Gestione

Quando si utilizzano solo ruoli utente locali per l'autenticazione, gli amministratori possono eseguire le seguenti attività di gestione:

- Modificare le password.
- Impostare una lunghezza minima per le password.
- Consentire agli utenti di effettuare l'accesso senza password.

Gestione degli accessi con servizi di directory

Gli amministratori possono utilizzare un server LDAP (Lightweight Directory Access Protocol) e un servizio di directory, ad esempio Active Directory di Microsoft.

Workflow di configurazione

Se nella rete vengono utilizzati un server LDAP e un servizio di directory, la configurazione funziona come segue:

1. Un amministratore effettua l'accesso a Gestione unificata di SANtricity con un profilo utente che include le autorizzazioni di amministratore di sicurezza.



Il `admin` l'utente ha accesso completo a tutte le funzioni del sistema.

2. L'amministratore inserisce le impostazioni di configurazione per il server LDAP. Le impostazioni includono il nome di dominio, l'URL e le informazioni sull'account di binding.
3. Se il server LDAP utilizza un protocollo sicuro (LDAPS), l'amministratore carica una catena di certificati CA (Certificate Authority) per l'autenticazione tra il server LDAP e il sistema host in cui è installato il proxy dei servizi Web.
4. Una volta stabilita la connessione al server, l'amministratore associa i gruppi di utenti ai ruoli utente locali. Questi ruoli sono predefiniti e non possono essere modificati.
5. L'amministratore verifica la connessione tra il server LDAP e il proxy dei servizi Web.
6. Gli utenti accedono al sistema con le credenziali LDAP/Directory Services assegnate.

Gestione

Quando si utilizzano i servizi di directory per l'autenticazione, gli amministratori possono eseguire le seguenti attività di gestione:

- Aggiungere un server di directory.
- Modificare le impostazioni del server di directory.
- Associare gli utenti LDAP ai ruoli utente locali.
- Rimuovere un server di directory.
- Modificare le password.
- Impostare una lunghezza minima per le password.
- Consentire agli utenti di effettuare l'accesso senza password.

Come fare

Visualizzare i ruoli utente locali

Dalla scheda Local User Roles (ruoli utente locali), è possibile visualizzare le mappature degli utenti ai ruoli predefiniti. Questi mapping fanno parte del RBAC (role-based access control) applicato nel proxy dei servizi Web per il gestore unificato di SANtricity.

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 di gestione degli accessi non vengono visualizzate.

A proposito di questa attività

Gli utenti e le mappature non possono essere modificati. È possibile modificare solo le password.

Fasi

1. Selezionare **Access Management**.
2. Selezionare la scheda **ruoli utente locali**.

Gli utenti sono mostrati nella tabella:

- **Admin** — Amministratore eccellente che ha accesso a tutte le funzioni del sistema. Questo utente include tutti i ruoli.
- **Storage** — l'amministratore responsabile di tutto il provisioning dello storage. Questo utente include i seguenti ruoli: Storage Admin, Support Admin e Monitor.
- **Security** — l'utente responsabile della configurazione della sicurezza, inclusi Access Management e Certificate Management. Questo utente include i seguenti ruoli: Security Admin e Monitor.
- **Support** — l'utente responsabile delle risorse hardware, dei dati di guasto e degli aggiornamenti del firmware. Questo utente include i seguenti ruoli: Support Admin e Monitor.
- **Monitor** — un utente con accesso in sola lettura al sistema. Questo utente include solo il ruolo Monitor.
- **rw** (lettura/scrittura) — questo utente include i seguenti ruoli: Amministratore dello storage, amministratore del supporto e monitor.
- **Ro** (sola lettura) — questo utente include solo il ruolo Monitor.

Modificare le password

È possibile modificare le password utente per ciascun utente in Gestione accessi.

Prima di iniziare

- Devi essere connesso come amministratore locale, che include le autorizzazioni di amministratore root.
- È necessario conoscere la password dell'amministratore locale.

A proposito di questa attività

Quando si sceglie una password, tenere presenti le seguenti linee guida:

- Le nuove password utente locali devono soddisfare o superare l'impostazione corrente per una password minima (in Visualizza/Modifica impostazioni).
- Le password distinguono tra maiuscole e minuscole.
- Gli spazi finali non vengono rimossi dalle password quando vengono impostati. Fare attenzione a includere spazi se inclusi nella password.
- Per una maggiore sicurezza, utilizzare almeno 15 caratteri alfanumerici e modificare la password frequentemente.

Fasi

1. Selezionare **Access Management**.
2. Selezionare la scheda **ruoli utente locali**.
3. Selezionare un utente dalla tabella.

Il pulsante **Change Password** (Modifica password) diventa disponibile.

4. Selezionare **Change Password** (Modifica password).

Viene visualizzata la finestra di dialogo **Change Password** (Modifica password).

5. Se non è stata impostata alcuna lunghezza minima per le password utente locali, selezionare la casella di controllo per richiedere all'utente di immettere una password per accedere al sistema.
6. Immettere la nuova password per l'utente selezionato nei due campi.
7. Immettere la password dell'amministratore locale per confermare l'operazione, quindi fare clic su **Change** (Modifica).

Risultati

Se l'utente è attualmente connesso, la modifica della password provoca l'interruzione della sessione attiva dell'utente.

Modificare le impostazioni della password utente locale

È possibile impostare la lunghezza minima richiesta per tutte le password utente locali nuove o aggiornate. È inoltre possibile consentire agli utenti locali di accedere al sistema senza inserire una password.

Prima di iniziare

- Devi essere connesso come amministratore locale, che include le autorizzazioni di amministratore root.

A proposito di questa attività

Tenere presenti queste linee guida quando si imposta la lunghezza minima per le password utente locali:

- Le modifiche apportate non influiscono sulle password utente locali esistenti.
- La lunghezza minima richiesta per le password utente locali deve essere compresa tra 0 e 30 caratteri.
- Le nuove password utente locali devono soddisfare o superare l'impostazione di lunghezza minima corrente.
- Non impostare una lunghezza minima per la password se si desidera che gli utenti locali accedano al sistema senza immettere una password.

Fasi

1. Selezionare **Access Management**.
2. Selezionare la scheda **ruoli utente locali**.
3. Selezionare **Visualizza/Modifica impostazioni**.

Viene visualizzata la finestra di dialogo **Local User Password Settings** (Impostazioni password utente locale).

4. Effettuare una delle seguenti operazioni:
 - Per consentire agli utenti locali di accedere al sistema *senza* inserire una password, deselezionare la casella di controllo "Richiedi almeno tutte le password utente locali".
 - Per impostare una lunghezza minima della password per tutte le password utente locali, selezionare la casella di controllo "Richiedi almeno tutte le password utente locali", quindi utilizzare la casella di selezione per impostare la lunghezza minima richiesta per tutte le password utente locali.

Le nuove password utente locali devono soddisfare o superare l'impostazione corrente.

5. Fare clic su **Save** (Salva).

Aggiungere il server di directory

Per configurare l'autenticazione per la gestione degli accessi, è necessario stabilire le comunicazioni tra un server LDAP e l'host che esegue il proxy dei servizi Web per la gestione unificata di SANtricity. Quindi, associare i gruppi di utenti LDAP ai ruoli utente locali.

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 di gestione degli accessi non vengono visualizzate.
- I gruppi di utenti devono essere definiti nel servizio di directory.
- Le credenziali del server LDAP devono essere disponibili, inclusi il nome di dominio, l'URL del server e, facoltativamente, il nome utente e la password dell'account BIND.
- Per i server LDAPS che utilizzano un protocollo sicuro, la catena di certificati del server LDAP deve essere installata sul computer locale.

A proposito di questa attività

L'aggiunta di un server di directory è un processo in due fasi. Immettere innanzitutto il nome di dominio e l'URL. Se il server utilizza un protocollo sicuro, è necessario caricare anche un certificato CA per

l'autenticazione se è firmato da un'autorità di firma non standard. Se si dispone delle credenziali per un account BIND, è anche possibile immettere il nome e la password dell'account utente. Quindi, mappare i gruppi di utenti del server LDAP ai ruoli utente locali.

Fasi


1. Selezionare **Access Management**.
2. Dalla scheda **Directory Services**, selezionare **Add Directory Server** (Aggiungi server di directory).


Viene visualizzata la finestra di dialogo **Add Directory Server** (Aggiungi server di directory).

3. Nella scheda **Server Settings** (Impostazioni server), immettere le credenziali per il server LDAP.

Dettagli campo

Impostazione	Descrizione
Impostazioni di configurazione	Dominio/i
Immettere il nome di dominio del server LDAP. Per più domini, inserire i domini in un elenco separato da virgole. Il nome di dominio viene utilizzato nel login (<i>nome utente@dominio</i>) per specificare il server di directory da autenticare.	URL del server
Immettere l'URL per l'accesso al server LDAP nel formato <code>ldap[s]://host:port</code> .	Carica certificato (opzionale)

Impostazione	Descrizione
<div data-bbox="245 432 302 485"></div> <p data-bbox="358 170 483 747">Questo campo viene visualizzato solo se è stato specificato un protocollo LDAPS nel campo URL server sopra riportato.</p> <p data-bbox="212 793 516 1098">Fare clic su Browse (Sfoglia) e selezionare un certificato CA da caricare. Si tratta del certificato attendibile o della catena di certificati utilizzata per l'autenticazione del server LDAP.</p>	<p data-bbox="529 159 850 191">Account BIND (opzionale)</p>
<p data-bbox="212 1150 505 1696">Inserire un account utente di sola lettura per le query di ricerca sul server LDAP e per la ricerca all'interno dei gruppi. Immettere il nome dell'account in formato LDAP. Ad esempio, se l'utente bindacct viene chiamato "bindacct", è possibile immettere un valore come CN=bindacct,CN=Users,DC=cpoc,DC=local.</p>	<p data-bbox="529 1150 857 1182">Password bind (opzionale)</p>

Impostazione		Descrizione
 <p>Questo campo viene visualizzato quando si immette un account BIND.</p>	Immettere la password per l'account BIND.	Verificare la connessione al server prima di aggiungerli
	<p>Selezionare questa casella di controllo per assicurarsi che il sistema possa comunicare con la configurazione del server LDAP immessa. Il test si verifica dopo aver fatto clic su Add (Aggiungi) nella parte inferiore della finestra di dialogo. Se questa casella di controllo è selezionata e il test non riesce, la configurazione non viene aggiunta. È necessario risolvere l'errore o deselezionare la casella di controllo per saltare il test e aggiungere la configurazione.</p>	Impostazioni dei privilegi
Ricerca DN base		Immettere il contesto LDAP per la ricerca degli utenti, in genere sotto forma di <code>CN=Users, DC=copc, DC=local</code> .
Attributo Username		Inserire l'attributo associato all'ID utente per l'autenticazione. Ad esempio: <code>sAMAccountName</code> .
Attributo/i di gruppo		Inserire un elenco di attributi di gruppo nell'utente, che viene utilizzato per il mapping gruppo-ruolo. Ad esempio: <code>memberOf, managedObjects</code> .

4. Fare clic sulla scheda **mappatura ruolo**.
5. Assegnare i gruppi LDAP ai ruoli predefiniti. Un gruppo può avere più ruoli assegnati.

Dettagli campo

Impostazione	Descrizione
Mapping	DN gruppo
Specificare il nome distinto del gruppo (DN) per il gruppo di utenti LDAP da mappare.	Ruoli



Il ruolo Monitor è necessario per tutti gli utenti, incluso l'amministratore.

6. Se lo si desidera, fare clic su **Add another mapping** (Aggiungi un'altra mappatura) per immettere più mappature gruppo-ruolo.
7. Al termine delle mappature, fare clic su **Aggiungi**.

Il sistema esegue una convalida, assicurandosi che lo storage array e il server LDAP possano comunicare. Se viene visualizzato un messaggio di errore, selezionare le credenziali inserite nella finestra di dialogo e, se necessario, immettere nuovamente le informazioni.

Modificare le impostazioni del server di directory e le mappature dei ruoli

Se in precedenza è stato configurato un server di directory in Access Management, è possibile modificarne le impostazioni in qualsiasi momento. Le impostazioni includono le informazioni di connessione al server e i mapping gruppo-ruolo.

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 di gestione degli accessi non vengono visualizzate.
- È necessario definire un server di directory.

Fasi

1. Selezionare **Access Management**.
2. Selezionare la scheda **Directory Services**.
3. Se sono stati definiti più server, selezionare il server che si desidera modificare dalla tabella.
4. Selezionare **Visualizza/Modifica impostazioni**.

Viene visualizzata la finestra di dialogo **Directory Server Settings** (Impostazioni server directory).

5. Nella scheda **Server Settings** (Impostazioni server), modificare le impostazioni desiderate.

Impostazione	Descrizione
Impostazioni di configurazione	Dominio/i
I nomi di dominio dei server LDAP. Per più domini, inserire i domini in un elenco separato da virgole. Il nome di dominio viene utilizzato nel login (<i>nome utente @dominio</i>) per specificare il server di directory da autenticare.	URL del server
L'URL per l'accesso al server LDAP nel formato <code>ldap[s]://host:port</code> .	Account BIND (opzionale)
L'account utente di sola lettura per le query di ricerca sul server LDAP e per la ricerca all'interno dei gruppi.	Password bind (opzionale)
La password per l'account BIND. (Questo campo viene visualizzato quando viene inserito un account BIND).	Verificare la connessione al server prima di salvare
Verifica che il sistema possa comunicare con la configurazione del server LDAP. Il test si verifica dopo aver fatto clic su Save (Salva). Se questa casella di controllo è selezionata e il test non riesce, la configurazione non viene modificata. È necessario risolvere l'errore o deselezionare la casella di controllo per ignorare il test e modificare nuovamente la configurazione.	Impostazioni dei privilegi

Impostazione	Descrizione
Ricerca DN base	Il contesto LDAP per la ricerca degli utenti, in genere sotto forma di <code>CN=Users, DC=copc, DC=local</code> .
Attributo Username	L'attributo associato all'ID utente per l'autenticazione. Ad esempio: <code>sAMAccountName</code> .
Attributo/i di gruppo	Un elenco di attributi di gruppo sull'utente, utilizzato per il mapping gruppo-ruolo. Ad esempio: <code>memberOf, managedObjects</code> .

6. Nella scheda **role Mapping**, modificare la mappatura desiderata.

Impostazione	Descrizione
Mapping	DN gruppo
Il nome di dominio del gruppo di utenti LDAP da mappare.	Ruoli



Il ruolo Monitor è necessario per tutti gli utenti, incluso l'amministratore.

7. Se lo si desidera, fare clic su **Add another mapping** (Aggiungi un'altra mappatura) per immettere più mappature gruppo-ruolo.

8. Fare clic su **Save** (Salva).

Risultati

Una volta completata questa attività, tutte le sessioni utente attive vengono terminate. Viene conservata solo la sessione utente corrente.

Rimuovere il server di directory

Per interrompere la connessione tra un server di directory e il proxy dei servizi Web, è possibile rimuovere le informazioni sul server dalla pagina Gestione accessi. È possibile eseguire questa attività se è stato configurato un nuovo server e si desidera rimuovere quello precedente.

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 di gestione degli accessi non vengono visualizzate.

A proposito di questa attività

Una volta completata questa attività, tutte le sessioni utente attive vengono terminate. Viene conservata solo la sessione utente corrente.

Fasi

1. Selezionare **Access Management**.

2. Selezionare la scheda **Directory Services**.
3. Dall'elenco, selezionare il server di directory che si desidera eliminare.
4. Fare clic su **Rimuovi**.

Viene visualizzata la finestra di dialogo **Remove Directory Server** (Rimuovi server di directory).

5. Tipo `remove` Nel campo, quindi fare clic su **Rimuovi**.

Le impostazioni di configurazione del server di directory, le impostazioni dei privilegi e i mapping dei ruoli vengono rimossi. Gli utenti non possono più accedere con le credenziali da questo server.

FAQ

Perché non riesco ad accedere?

Se si riceve un errore durante il tentativo di accesso a Gestione unificata di SANtricity, esaminare queste possibili cause.

Gli errori di accesso a Unified Manager possono verificarsi per uno dei seguenti motivi:

- Il nome utente o la password immessi non sono corretti.
- Privilegi insufficienti.
- Il server di directory (se configurato) potrebbe non essere disponibile. In questo caso, provare ad accedere con un ruolo utente locale.
- Si è tentato di accedere più volte senza successo, attivando la modalità di blocco. Attendere 10 minuti per eseguire nuovamente l'accesso.

Gli errori di accesso a un array di storage remoto per le attività di mirroring possono verificarsi per uno dei seguenti motivi:

- La password immessa non è corretta.
- Si è tentato di accedere più volte senza successo, attivando la modalità di blocco. Attendere 10 minuti per effettuare nuovamente l'accesso.
- È stato raggiunto il numero massimo di connessioni client utilizzate sul controller. Verificare la presenza di più utenti o client.

Cosa occorre sapere prima di aggiungere un server di directory?

Prima di aggiungere un server di directory in Access Management, è necessario soddisfare determinati requisiti.

- I gruppi di utenti devono essere definiti nel servizio di directory.
- Le credenziali del server LDAP devono essere disponibili, inclusi il nome di dominio, l'URL del server e, facoltativamente, il nome utente e la password dell'account BIND.
- Per i server LDAPS che utilizzano un protocollo sicuro, la catena di certificati del server LDAP deve essere installata sul computer locale.

Cosa occorre sapere sulla mappatura dei ruoli degli array di storage?

Prima di mappare i gruppi ai ruoli, rivedere le linee guida.

Le funzionalità RBAC (role-based access control) includono i seguenti ruoli:

- **Storage admin** — accesso completo in lettura/scrittura agli oggetti storage sugli array, ma nessun accesso alla configurazione di sicurezza.
- **Security admin** — accesso alla configurazione di sicurezza in Access Management e Certificate Management.
- **Support admin** — accesso a tutte le risorse hardware su storage array, dati di guasto ed eventi MEL. Nessun accesso agli oggetti di storage o alla configurazione di sicurezza.
- **Monitor** — accesso in sola lettura a tutti gli oggetti di storage, ma nessun accesso alla configurazione di sicurezza.



Il ruolo Monitor è necessario per tutti gli utenti, incluso l'amministratore.

Se si utilizza un server LDAP (Lightweight Directory Access Protocol) e servizi di directory, assicurarsi che:

- Un amministratore ha definito i gruppi di utenti nel servizio di directory.
- Si conoscono i nomi di dominio del gruppo per i gruppi di utenti LDAP.

Quali sono gli utenti locali?

Gli utenti locali sono predefiniti nel sistema e includono autorizzazioni specifiche.

Gli utenti locali includono:

- **Admin** — Amministratore eccellente che ha accesso a tutte le funzioni del sistema. Questo utente include tutti i ruoli. La password deve essere impostata al primo accesso.
- **Storage** — l'amministratore responsabile di tutto il provisioning dello storage. Questo utente include i seguenti ruoli: Storage Admin, Support Admin e Monitor. Questo account viene disattivato fino a quando non viene impostata una password.
- **Security** — l'utente responsabile della configurazione della sicurezza, inclusi Access Management e Certificate Management. Questo utente include i seguenti ruoli: Security Admin e Monitor. Questo account viene disattivato fino a quando non viene impostata una password.
- **Support** — l'utente responsabile delle risorse hardware, dei dati di guasto e degli aggiornamenti del firmware. Questo utente include i seguenti ruoli: Support Admin e Monitor. Questo account viene disattivato fino a quando non viene impostata una password.
- **Monitor** — un utente con accesso in sola lettura al sistema. Questo utente include solo il ruolo Monitor. Questo account viene disattivato fino a quando non viene impostata una password.
- **rw** (lettura/scrittura) — questo utente include i seguenti ruoli: Amministratore dello storage, amministratore del supporto e monitor. Questo account viene disattivato fino a quando non viene impostata una password.
- **Ro** (sola lettura) — questo utente include solo il ruolo Monitor. Questo account viene disattivato fino a quando non viene impostata una password.

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.