



# Gestione degli accessi

## SANtricity 11.7

NetApp  
February 12, 2024

# Sommario

- Gestione degli accessi ..... 1
  - Panoramica sulla gestione degli accessi ..... 1
  - Concetti ..... 1
  - Utilizzare ruoli utente locali ..... 5
  - Utilizzare i servizi di directory ..... 7
  - FAQ ..... 17

# Gestione degli accessi

## Panoramica sulla gestione degli accessi

Access Management è un metodo per configurare l'autenticazione dell'utente in Unified Manager.

### Quali metodi di autenticazione sono disponibili?

Sono disponibili i seguenti metodi di autenticazione:

- **Ruoli utente locali** — l'autenticazione viene gestita tramite funzionalità RBAC (role-based access control). I ruoli utente locali includono profili utente predefiniti e ruoli con autorizzazioni di accesso specifiche.
- **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.

Scopri di più:

- ["Come funziona Access Management"](#)
- ["Terminologia per la gestione degli accessi"](#)
- ["Autorizzazioni per i ruoli mappati"](#)

### Come si configura Access Management?

Il software SANtricity è preconfigurato per l'utilizzo dei ruoli utente locali. Se si desidera utilizzare LDAP, è possibile configurarlo nella pagina Gestione accessi.

Scopri di più:

- ["Gestione degli accessi con ruoli utente locali"](#)
- ["Gestione degli accessi con servizi di directory"](#)

## Concetti

### Come funziona Access Management

Utilizzare Access Management per stabilire l'autenticazione dell'utente in Unified Manager.

#### 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 Access Management a Unified Manager.

Termine	Descrizione
Active Directory	Active Directory (ad) è un servizio di directory Microsoft che utilizza LDAP per le reti di dominio Windows.

Termine	Descrizione
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.
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 Unified Manager.

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 Unified Manager. 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. Facoltativamente, 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 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. 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.

# Utilizzare ruoli utente locali

## 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 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 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 per i profili utente locali

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).

## Utilizzare i servizi di directory

### 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 Unified Manager. 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 del campo

Impostazione	Descrizione
<b>Impostazioni di configurazione</b>	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" style="border: 1px solid black; border-radius: 50%; width: 20px; height: 20px; display: flex; align-items: center; justify-content: center; margin-bottom: 10px;">i</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="212 793 513 1094">Fare clic su <b>Browse</b> (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="526 159 850 191">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 è chiamato "bindacct", è possibile immettere un valore come CN=bindacct, CN=Users, DC=cpoc, DC=local.</p>	<p data-bbox="526 1150 857 1182">Password bind (opzionale)</p>

Impostazione	Descrizione
<div style="display: flex; align-items: center;">  <p data-bbox="358 170 472 541">Questo campo viene visualizzato quando si immette un account BIND.</p> </div> <p data-bbox="212 590 500 653">Immettere la password per l'account BIND.</p>	<p data-bbox="529 159 1203 191">Verificare la connessione al server prima di aggiungerli</p>
<p data-bbox="212 709 511 1115">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 <b>Add</b> (Aggiungi) nella parte inferiore della finestra di dialogo.</p> <p data-bbox="212 1150 511 1524">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>	<p data-bbox="529 709 862 741"><b>Impostazioni dei privilegi</b></p>
<p data-bbox="212 1577 423 1608">Ricerca DN base</p>	<p data-bbox="529 1577 1377 1640">Immettere il contesto LDAP per la ricerca degli utenti, in genere sotto forma di <code>CN=Users, DC=cpoc, DC=local</code>.</p>
<p data-bbox="212 1698 456 1730">Attributo Username</p>	<p data-bbox="529 1698 1442 1761">Inserire l'attributo associato all'ID utente per l'autenticazione. Ad esempio: <code>sAMAccountName</code>.</p>
<p data-bbox="212 1820 456 1852">Attributo/i di gruppo</p>	<p data-bbox="529 1820 1442 1883">Inserire un elenco di attributi di gruppo nell'utente, che viene utilizzato per il mapping gruppo-ruolo. Ad esempio: <code>memberOf, managedObjects</code>.</p>

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

#### Dettagli del campo

Impostazione	Descrizione
<b>Mapping</b>	DN gruppo
Specificare il nome distinto del gruppo (DN) per il gruppo di utenti LDAP da mappare. Sono supportate le espressioni regolari. Questi caratteri speciali di espressione regolare devono essere escapati con una barra rovesciata ( ) se non fanno parte di un modello di espressione regolare: []{}()<>*+.=!?^	
Ruoli	<p>Fare clic nel campo e selezionare uno dei ruoli utente locali da mappare al DN del gruppo. È necessario selezionare singolarmente ciascun ruolo che si desidera includere per questo gruppo. Il ruolo di monitoraggio è necessario in combinazione con gli altri ruoli per accedere a Gestione unificata di SANtricity. I ruoli mappati includono le seguenti autorizzazioni:</p> <ul style="list-style-type: none"> <li>• <b>Storage admin</b> — accesso completo in lettura/scrittura agli oggetti storage sugli array, ma nessun accesso alla configurazione di sicurezza.</li> <li>• <b>Security admin</b> — accesso alla configurazione di sicurezza in Access Management e Certificate Management.</li> <li>• <b>Support admin</b> — 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.</li> <li>• <b>Monitor</b> — accesso in sola lettura a tutti gli oggetti di storage, ma nessun accesso alla configurazione di sicurezza.</li> </ul>



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.

## Dettagli del campo

Impostazione	Descrizione
<b>Impostazioni di configurazione</b>	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

Impostazione	Descrizione
<p>Verifica che il sistema possa comunicare con la configurazione del server LDAP. Il test si verifica dopo aver fatto clic su <b>Save</b> (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.</p>	<p><b>Impostazioni dei privilegi</b></p>
<p>Ricerca DN base</p>	<p>Il contesto LDAP per la ricerca degli utenti, in genere sotto forma di <code>CN=Users, DC=cpoc, DC=local</code>.</p>
<p>Attributo Username</p>	<p>L'attributo associato all'ID utente per l'autenticazione. Ad esempio: <code>sAMAccountName</code>.</p>
<p>Attributo/i di gruppo</p>	<p>Un elenco di attributi di gruppo sull'utente, utilizzato per il mapping gruppo-ruolo. Ad esempio: <code>memberOf, managedObjects</code>.</p>

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

## Dettagli del campo

Impostazione	Descrizione
<b>Mapping</b>	DN gruppo
Il nome di dominio del gruppo di utenti LDAP da mappare. Sono supportate le espressioni regolari. Questi caratteri speciali di espressione regolare devono essere escapati con una barra rovesciata ( ) se non fanno parte di un modello di espressione regolare:  []{}()<>*+ -=! ? ^	
Ruoli	I ruoli da mappare al DN del gruppo. È necessario selezionare singolarmente ciascun ruolo che si desidera includere per questo gruppo. Il ruolo di monitoraggio è necessario in combinazione con gli altri ruoli per accedere a Gestione unificata di SANtricity. I ruoli includono: <ul style="list-style-type: none"><li>• <b>Storage admin</b> — accesso completo in lettura/scrittura agli oggetti storage sugli array, ma nessun accesso alla configurazione di sicurezza.</li><li>• <b>Security admin</b> — accesso alla configurazione di sicurezza in Access Management e Certificate Management.</li><li>• <b>Support admin</b> — 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.</li><li>• <b>Monitor</b> — accesso in sola lettura a tutti gli oggetti di storage, ma nessun accesso alla configurazione di sicurezza.</li></ul>



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, esaminare queste possibili cause.

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

- Il nome utente o la password immessi non sono corretti.
- Privilegi insufficienti.
- Si è tentato di accedere più volte senza successo, attivando la modalità di blocco. Attendere 10 minuti per eseguire nuovamente l'accesso.

### 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.