# Come fare

SANtricity 11.6

NetApp
February 12, 2024

# Sommario

# 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 (*nome utente@dominio*) per specificare il server di directory da autenticare. | URL del server |
| Immettere l'URL per l'accesso al server LDAP nel formato `ldap[s]://host:port`. | Carica certificato (opzionale) |

| Impostazione | Descrizione |
| --- | --- |
| Questo campo viene visualizzato solo se è stato specificato un protocollo LDAPS nel campo URL server sopra riportato.<br><br>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. | Account BIND (opzionale) |
| 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`. | Password bind (opzionale) |

| Impostazione | Descrizione |
| --- | --- |
| Questo campo viene visualizzato quando si immette un account BIND.<br><br>Immettere la password per l'account BIND. | Verificare la connessione al server prima di aggiungerli |
| 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. | **Impostazioni dei privilegi** |
| Ricerca DN base | Immettere il contesto LDAP per la ricerca degli utenti, in genere sotto forma di `CN=Users, DC=copc, DC=local`. |
| Attributo Username | Inserire l'attributo associato all'ID utente per l'autenticazione. Ad esempio: `sAMAccountName`. |
| Attributo/i di gruppo | Inserire un elenco di attributi di gruppo nell'utente, che viene utilizzato per il mapping gruppo-ruolo. Ad esempio: `memberOf, managedObjects`. |

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 (*nome utente @dominio*) per specificare il server di directory da autenticare. | URL del server |
| L'URL per l'accesso al server LDAP nel formato `ldap[s]://host:port`. | 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 `CN=Users, DC=copc, DC=local`. |
| Attributo Username | L'attributo associato all'ID utente per l'autenticazione. Ad esempio: `sAMAccountName`. |
| Attributo/i di gruppo | Un elenco di attributi di gruppo sull'utente, utilizzato per il mapping gruppo-ruolo. Ad esempio: `memberOf, managedObjects`. |

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.