Gestione degli accessi

SANtricity 11.8

NetApp
April 05, 2024

Sommario

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.
- **SAML** — l'autenticazione viene gestita tramite un provider di identità (IdP) utilizzando SAML 2.0.

Scopri di più:

- "Come funziona Access Management"
- "Terminologia per la gestione degli accessi"
- "Autorizzazioni per i ruoli mappati"
- "SAML"

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"
- "Configurare SAML"

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.
   - **SAML** — l'autenticazione viene gestita tramite un provider di identità (IdP) utilizzando il linguaggio SAML (Security Assertion Markup Language) 2.0. Un amministratore stabilisce la comunicazione tra il sistema IdP e l'array di storage, quindi mappa gli utenti IdP ai ruoli utente locali integrati nell'array di storage.
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.
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.
SAML	SAML (Security Assertion Markup Language) è uno standard basato su XML per l'autenticazione e l'autorizzazione tra due entità. SAML consente l'autenticazione a più fattori, in cui gli utenti devono fornire due o più elementi per dimostrare la propria identità (ad esempio, una password e un'impronta digitale). La funzionalità SAML integrata dello storage array è conforme a SAML2.0 per l'asserzione, l'autenticazione e l'autorizzazione dell'identità.
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.

Gestione degli accessi con SAML

Per la gestione degli accessi, gli amministratori possono utilizzare le funzionalità SAML (Security Assertion Markup Language) 2.0 integrate nell'array.

Workflow di configurazione

La configurazione SAML funziona come segue:

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

   Il `admin` L'utente ha accesso completo a tutte le funzioni di System Manager.

2. L'amministratore accede alla scheda **SAML** in Gestione accessi.

3. Un amministratore configura le comunicazioni con il provider di identità (IdP). Un IdP è un sistema esterno utilizzato per richiedere le credenziali a un utente e determinare se l'utente è autenticato correttamente. Per configurare le comunicazioni con lo storage array, l'amministratore scarica il file di metadati IdP dal sistema IdP, quindi utilizza Unified Manager per caricare il file nello storage array.
4. Un amministratore stabilisce una relazione di trust tra il service provider e l'IdP. Un service provider controlla l'autorizzazione dell'utente; in questo caso, il controller nell'array di storage agisce come service provider. Per configurare le comunicazioni, l'amministratore utilizza Unified Manager per esportare un file di metadati del provider di servizi per il controller. Dal sistema IdP, l'amministratore importa il file di metadati nell'IdP.

   Gli amministratori devono inoltre assicurarsi che IdP supporti la capacità di restituire un ID nome all'autenticazione.

5. L'amministratore associa i ruoli dell'array di storage agli attributi dell'utente definiti nell'IdP. A tale scopo, l'amministratore utilizza Unified Manager per creare le mappature.
6. L'amministratore verifica l'accesso SSO all'URL IdP. Questo test garantisce che lo storage array e IdP possano comunicare.

   Una volta abilitato SAML, non è possibile disattivarlo tramite l'interfaccia utente, né modificare le impostazioni IdP. Se è necessario disattivare o modificare la configurazione SAML, contattare il supporto tecnico per assistenza.

7. Da Unified Manager, l'amministratore abilita SAML per lo storage array.
8. Gli utenti accedono al sistema con le proprie credenziali SSO.

Gestione

Quando si utilizza SAML per l'autenticazione, gli amministratori possono eseguire le seguenti attività di gestione:

- Modificare o creare nuove mappature dei ruoli
- Esportare i file del provider di servizi

Restrizioni di accesso

Quando SAML è attivato, gli utenti non possono rilevare o gestire lo storage per quell'array dall'interfaccia precedente di Storage Manager.

Inoltre, i seguenti client non possono accedere ai servizi e alle risorse degli array di storage:

- Finestra Enterprise Management (EMW)
- Interfaccia a riga di comando (CLI)
- Client Software Developer Kit (SDK)
- Client in-band
- Client REST API per l'autenticazione di base HTTP
- Effettuare l'accesso utilizzando l'endpoint REST API standard

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
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. 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 è 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. 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=cpoc, 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 del campo

Impostazione	Descrizione
Mapping	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	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: • **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.

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
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

Impostazione	Descrizione
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**
Ricerca DN base	Il contesto LDAP per la ricerca degli utenti, in genere sotto forma di `CN=Users, DC=cpoc, 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.

Dettagli del campo

Impostazione	Descrizione
Mapping	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: • **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.

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.

Utilizzare SAML

Configurare SAML

Per configurare l'autenticazione per Access Management, è possibile utilizzare le funzionalità SAML (Security Assertion Markup Language) integrate nell'array di storage. Questa configurazione stabilisce una connessione tra un provider di identità e lo storage provider.

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 conoscere l'indirizzo IP o il nome di dominio del controller nell'array di storage.
- Un amministratore IdP ha configurato un sistema IdP.
- Un amministratore IdP ha garantito che IdP supporti la capacità di restituire un ID nome all'autenticazione.
- Un amministratore ha garantito la sincronizzazione del clock del controller e del server IdP (tramite un server NTP o regolando le impostazioni del clock del controller).
- Un file di metadati IdP viene scaricato dal sistema IdP ed è disponibile sul sistema locale utilizzato per accedere a Unified Manager.

A proposito di questa attività

Un provider di identità (IdP) è un sistema esterno utilizzato per richiedere le credenziali a un utente e per determinare se tale utente è autenticato correttamente. È possibile configurare IdP in modo da fornire l'autenticazione a più fattori e utilizzare qualsiasi database utente, ad esempio Active Directory. Il tuo team di sicurezza è responsabile della manutenzione dell'IdP. Un service provider (SP) è un sistema che controlla l'autenticazione e l'accesso degli utenti. Quando Access Management è configurato con SAML, lo storage array agisce come service provider per richiedere l'autenticazione al provider di identità. Per stabilire una connessione tra IdP e lo storage array, è necessario condividere i file di metadati tra queste due entità. Quindi, mappare le entità utente IdP ai ruoli degli array di storage. Infine, prima di attivare SAML, è necessario verificare la connessione e gli accessi SSO.

SAML e Directory Services. Se si attiva SAML quando Directory Services è configurato come metodo di autenticazione, SAML sostituisce Directory Services in Unified Manager. Se si disattiva SAML in un secondo momento, la configurazione dei servizi di directory torna alla configurazione precedente.

Modifica e disattivazione. una volta abilitato SAML, non è possibile disattivarlo tramite l'interfaccia utente, né modificare le impostazioni IdP. Se è necessario disattivare o modificare la configurazione SAML, contattare il supporto tecnico per assistenza.

La configurazione dell'autenticazione SAML è una procedura multi-step.

Fase 1: Caricare il file di metadati IdP

Per fornire allo storage array le informazioni di connessione IdP, importare i metadati IdP in Unified Manager. Il sistema IdP ha bisogno di questi metadati per reindirizzare le richieste di autenticazione all'URL corretto e per validare le risposte ricevute.

Fasi

1. Selezionare **Impostazioni › Gestione accessi**.
2. Selezionare la scheda **SAML**.

   La pagina visualizza una panoramica delle fasi di configurazione.

3. Fare clic sul collegamento **Import Identity Provider (IdP) file**.

   Viene visualizzata la finestra di dialogo Importa file provider di identità.

4. Fare clic su **Browse** (Sfoglia) per selezionare e caricare il file di metadati IdP copiato nel sistema locale.

   Dopo aver selezionato il file, viene visualizzato l'ID entità IdP.

5. Fare clic su **Importa**.

Fase 2: Esportare i file del provider di servizi

Per stabilire una relazione di trust tra IdP e l'array di storage, importare i metadati del service provider nell'IdP. L'IdP ha bisogno di questi metadati per stabilire una relazione di trust con il controller ed elaborare le richieste di autorizzazione. Il file include informazioni come il nome di dominio del controller o l'indirizzo IP, in modo che l'IdP possa comunicare con i service provider.

Fasi

1. Fare clic sul collegamento **Export Service Provider Files**.

   Viene visualizzata la finestra di dialogo Esporta file provider di servizi.

2. Inserire l'indirizzo IP o il nome DNS del controller nel campo **Controller A**, quindi fare clic su **Export** per salvare il file di metadati nel sistema locale.

   Dopo aver fatto clic su **Esporta**, i metadati del provider di servizi vengono scaricati nel sistema locale. Prendere nota della posizione in cui è memorizzato il file.

3. Dal sistema locale, individuare il file di metadati del Service Provider in formato XML esportato.
4. Dal server IdP, importare il file di metadati del provider di servizi per stabilire la relazione di trust. È possibile importare il file direttamente o inserire manualmente le informazioni del controller dal file.

Fase 3: Mappare i ruoli

Per fornire agli utenti l'autorizzazione e l'accesso a Unified Manager, è necessario mappare gli attributi utente IdP e le appartenenze ai gruppi ai ruoli predefiniti dell'array di storage.

Prima di iniziare

- Un amministratore IdP ha configurato gli attributi utente e l'appartenenza al gruppo nel sistema IdP.
- Il file di metadati IdP viene importato in Unified Manager.
- Un file di metadati del service provider per il controller viene importato nel sistema IdP per la relazione di trust.

Fasi

1. Fare clic sul collegamento **mapping dei ruoli di Unified Manager**.

   Viene visualizzata la finestra di dialogo mappatura ruoli.

2. Assegnare gli attributi e i gruppi degli utenti IdP ai ruoli predefiniti. Un gruppo può avere più ruoli assegnati.

Dettagli del campo

Impostazione	Descrizione
Mapping	Attributo dell'utente
Specificare l'attributo (ad esempio, "membro di") per il gruppo SAML da mappare.	Valore dell'attributo
Specificare il valore dell'attributo per il gruppo 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	Fare clic nel campo e selezionare uno dei ruoli dell'array di storage da mappare all'attributo. È necessario selezionare singolarmente ciascun ruolo da includere. Per accedere a Unified Manager, è necessario il ruolo di monitoraggio in combinazione con gli altri ruoli. Il ruolo Security Admin è richiesto anche per almeno un gruppo. I ruoli mappati includono le seguenti autorizzazioni: • **Storage admin** — accesso completo in lettura/scrittura agli oggetti di storage (ad esempio, volumi e pool di dischi), ma nessun accesso alla configurazione di sicurezza. • **Security admin** — accesso alla configurazione della sicurezza in Access Management, gestione dei certificati, gestione dei registri di controllo e possibilità di attivare o disattivare l'interfaccia di gestione legacy (Symbol). • **Support admin** — accesso a tutte le risorse hardware dello storage array, dati di guasto, eventi MEL e aggiornamenti del firmware del controller. 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. Unified Manager non funzionerà correttamente per nessun utente senza il ruolo di monitoraggio presente.

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

   I mapping dei ruoli possono essere modificati dopo l'attivazione di SAML.

4. Una volta completate le mappature, fare clic su **Save** (Salva).

Fase 4: Verifica dell'accesso SSO

Per garantire che il sistema IdP e lo storage array possano comunicare, è possibile eseguire un test di accesso SSO. Questo test viene eseguito anche durante la fase finale per l'abilitazione di SAML.

Prima di iniziare

- Il file di metadati IdP viene importato in Unified Manager.
- Un file di metadati del service provider per il controller viene importato nel sistema IdP per la relazione di trust.

Fasi

1. Selezionare il collegamento **Test SSO Login**.

   Viene visualizzata una finestra di dialogo per l'immissione delle credenziali SSO.

2. Immettere le credenziali di accesso per un utente con permessi di amministratore della sicurezza e di monitoraggio.

   Viene visualizzata una finestra di dialogo durante il test dell'accesso.

3. Cercare il messaggio Test Successful (Test riuscito). Se il test viene completato correttamente, passare alla fase successiva per l'abilitazione di SAML.

   Se il test non viene completato correttamente, viene visualizzato un messaggio di errore con ulteriori informazioni. Assicurarsi che:

   - L'utente appartiene a un gruppo con autorizzazioni per Security Admin e Monitor.
   - I metadati caricati per il server IdP sono corretti.
   - L'indirizzo del controller nei file di metadati SP è corretto.

Fase 5: Abilitare SAML

Il passaggio finale consiste nel completare la configurazione SAML per l'autenticazione dell'utente. Durante questo processo, il sistema richiede anche di verificare un accesso SSO. Il processo di test di accesso SSO è descritto nel passaggio precedente.

Prima di iniziare

- Il file di metadati IdP viene importato in Unified Manager.
- Un file di metadati del service provider per il controller viene importato nel sistema IdP per la relazione di trust.
- È stata configurata almeno una mappatura dei ruoli Monitor e Security Admin.

Modifica e disattivazione. una volta abilitato SAML, non è possibile disattivarlo tramite l'interfaccia utente, né modificare le impostazioni IdP. Se è necessario disattivare o modificare la configurazione SAML, contattare il supporto tecnico per assistenza.

Fasi

1. Dalla scheda **SAML**, selezionare il collegamento **Enable SAML** (attiva SAML).

   Viene visualizzata la finestra di dialogo Conferma abilitazione SAML.

2. Tipo `enable`, Quindi fare clic su **Enable** (attiva).
3. Immettere le credenziali utente per un test di accesso SSO.

Risultati

Una volta attivato SAML, il sistema termina tutte le sessioni attive e inizia l'autenticazione degli utenti tramite SAML.

Modificare le mappature dei ruoli SAML

Se in precedenza è stato configurato SAML per Access Management, è possibile modificare le mappature dei ruoli tra i gruppi IdP e i ruoli predefiniti dell'array di storage.

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.
- Un amministratore IdP ha configurato gli attributi utente e l'appartenenza al gruppo nel sistema IdP.
- SAML è configurato e abilitato.

Fasi

1. Selezionare **Impostazioni › Gestione accessi**.
2. Selezionare la scheda **SAML**.
3. Selezionare **mappatura ruolo**.

   Viene visualizzata la finestra di dialogo mappatura ruoli.

4. Assegnare gli attributi e i gruppi degli utenti IdP ai ruoli predefiniti. Un gruppo può avere più ruoli assegnati.

   Prestare attenzione a non rimuovere le autorizzazioni mentre SAML è attivato, altrimenti si perde l'accesso a Unified Manager.

Dettagli del campo

Impostazione	Descrizione
Mapping	Attributo dell'utente
Specificare l'attributo (ad esempio, "membro di") per il gruppo SAML da mappare.	Valore dell'attributo
Specificare il valore dell'attributo per il gruppo da mappare.	Ruoli

> Il ruolo Monitor è necessario per tutti gli utenti, incluso l'amministratore. Unified Manager non funzionerà correttamente per nessun utente senza il ruolo di monitoraggio presente.

5. Facoltativamente, fare clic su **Add another mapping** (Aggiungi un'altra mappatura) per immettere più mappature gruppo-ruolo.
6. 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.

Esportare i file del provider di servizi SAML

Se necessario, è possibile esportare i metadati del service provider per l'array di storage e reimportare il file nel sistema IdP (Identity Provider).

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.
- SAML è configurato e abilitato.

A proposito di questa attività

In questa attività, si esportano i metadati dal controller. L'IdP ha bisogno di questi metadati per stabilire una relazione di trust con il controller ed elaborare le richieste di autenticazione. Il file include informazioni come il nome di dominio del controller o l'indirizzo IP che IdP può utilizzare per l'invio delle richieste.

Fasi

1. Selezionare **Impostazioni › Gestione accessi**.
2. Selezionare la scheda **SAML**.
3. Selezionare **Esporta**.

   Viene visualizzata la finestra di dialogo Esporta file provider di servizi.

4. Fare clic su **Export** (Esporta) per salvare il file di metadati nel sistema locale.

   Il campo del nome di dominio è di sola lettura.

   Prendere nota della posizione in cui è memorizzato il file.

5. Dal sistema locale, individuare il file di metadati del Service Provider in formato XML esportato.
6. Dal server IdP, importare il file di metadati del provider di servizi. È possibile importare il file direttamente o inserire manualmente le informazioni del controller.
7. Fare clic su **Chiudi**.

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.
- L'autenticazione SAML è attivata. Aggiornare il browser per accedere.

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.

SAML

Se si utilizzano le funzionalità SAML (Security Assertion Markup Language) integrate nell'array di storage, assicurarsi che:

- Un amministratore del provider di identità (IdP) ha configurato gli attributi utente e l'appartenenza al gruppo nel sistema IdP.
- Conosci i nomi dei membri del gruppo.
- Si conosce il valore dell'attributo per il gruppo 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:

  ```
  \.[]{}()<>*+-=!?^$|
  ```

- Il ruolo Monitor è necessario per tutti gli utenti, incluso l'amministratore. Unified Manager non funzionerà correttamente per nessun utente senza il ruolo di monitoraggio presente.

Cosa occorre sapere prima di configurare e abilitare SAML?

Prima di configurare e attivare le funzionalità SAML (Security Assertion Markup Language) per l'autenticazione, assicurarsi di soddisfare i seguenti requisiti e comprendere le restrizioni SAML.

Requisiti

Prima di iniziare, assicurarsi che:

- Nella rete è configurato un provider di identità (IdP). Un IdP è un sistema esterno utilizzato per richiedere le credenziali a un utente e determinare se l'utente è autenticato correttamente. Il tuo team di sicurezza è responsabile della manutenzione dell'IdP.
- Un amministratore IdP ha configurato gli attributi e i gruppi utente nel sistema IdP.
- Un amministratore IdP ha garantito che IdP supporti la capacità di restituire un ID nome all'autenticazione.
- Un amministratore ha garantito la sincronizzazione del clock del controller e del server IdP (tramite un server NTP o regolando le impostazioni del clock del controller).
- Un file di metadati IdP viene scaricato dal sistema IdP e disponibile sul sistema locale utilizzato per accedere a Unified Manager.
- Si conosce l'indirizzo IP o il nome di dominio del controller nell'array di storage.

Restrizioni

Oltre ai requisiti sopra indicati, assicurati di comprendere le seguenti restrizioni:

- Una volta abilitato SAML, non è possibile disattivarlo tramite l'interfaccia utente, né modificare le impostazioni IdP. Se è necessario disattivare o modificare la configurazione SAML, contattare il supporto tecnico per assistenza. Si consiglia di testare gli accessi SSO prima di attivare SAML nella fase finale di configurazione. (Il sistema esegue anche un test di accesso SSO prima di attivare SAML).
- Se si disattiva SAML in futuro, il sistema ripristina automaticamente la configurazione precedente (ruoli utente locali e/o servizi di directory).
- Se i servizi di directory sono attualmente configurati per l'autenticazione dell'utente, SAML sovrascrive tale configurazione.
- Quando SAML è configurato, i seguenti client non possono accedere alle risorse degli array di storage:
  - Finestra Enterprise Management (EMW)
  - Interfaccia a riga di comando (CLI)
  - Client Software Developer Kit (SDK)
  - Client in-band
  - Client REST API per l'autenticazione di base HTTP
  - Effettuare l'accesso utilizzando l'endpoint REST API standard

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.