Gestione degli accessi

SANtricity 11.5

NetApp
February 12, 2024

Sommario

Gestione degli accessi

Concetti

Come funziona Access Management

La gestione degli accessi è un metodo per stabilire l'autenticazione dell'utente in Gestione di sistema di SANtricity. L'autenticazione richiede agli utenti di accedere a questi sistemi con le credenziali assegnate.

La configurazione di Access Management e l'autenticazione dell'utente funzionano come segue:

1. Un amministratore accede a System Manager con un profilo utente che include le autorizzazioni di amministratore della 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.

2. L'amministratore accede a Access Management nell'interfaccia utente. Lo storage array è preconfigurato per l'utilizzo dei ruoli utente locali, ovvero 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 applicate nell'array di storage. I ruoli utente locali includono profili utente 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 esegue il mapping degli utenti LDAP ai ruoli utente locali incorporati nell'array di storage.
   - **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 System Manager.
5. Gli utenti accedono al sistema inserendo le proprie credenziali.

   > Se l'autenticazione viene gestita con SAML e SSO (Single Sign-on), il sistema potrebbe ignorare la finestra di dialogo di accesso di System Manager.

   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 attività nell'interfaccia utente.
   - Visualizza il nome utente nella parte superiore destra dell'interfaccia.

Attività disponibili in System Manager

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

- **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.

Un'attività non disponibile viene visualizzata in grigio o non viene visualizzata nell'interfaccia utente. Ad esempio, un utente con il ruolo Monitor può visualizzare tutte le informazioni sui volumi, ma non può accedere alle funzioni per la modifica di tale volume. Le schede relative a funzioni come **Copy Services** e **Add to workload** non saranno visualizzate; sono disponibili solo le impostazioni di visualizzazione/modifica.

Accesso dell'utente a Gestione storage SANtricity

Una volta configurati i ruoli utente locali e i servizi di directory, gli utenti devono immettere le credenziali prima di eseguire una delle seguenti funzioni nella finestra di gestione aziendale (EMW):

- Ridenominazione dello storage array
- Aggiornamento del firmware del controller
- Caricamento della configurazione di uno storage array
- Esecuzione di uno script
- Tentativo di eseguire un'operazione attiva quando una sessione non utilizzata è scaduta

Se SAML è configurato per un array di storage, gli utenti non possono utilizzare EMW per rilevare o gestire lo storage per tale array.

Terminologia per la gestione degli accessi

Scopri come si applicano i termini di Access Management al tuo storage array.

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.

Termine	Descrizione
CIRCA	Un'autorità di certificazione (CA) è un'entità attendibile che emette documenti elettronici, denominati certificati digitali, per la sicurezza di Internet. Questi certificati identificano i proprietari dei siti Web, consentendo connessioni sicure tra client e server.
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.
IDP	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.
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. I controlli RBAC vengono applicati all'array di storage e includono 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.

Termine	Descrizione
SP	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.
SSO	SSO (Single Sign-on) è un servizio di autenticazione che consente a un set di credenziali di accesso di accedere a più applicazioni.

Autorizzazioni per i ruoli mappati

Le funzionalità RBAC (role-based access control) applicate all'array di storage includono profili utente predefiniti con uno o più ruoli mappati. Ogni ruolo include le autorizzazioni per l'accesso alle attività in Gestore di sistema di SANtricity.

I profili utente e i ruoli mappati sono accessibili dal **Impostazioni › Gestione accessi › ruoli utente locali** nell'interfaccia utente di System Manager.

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

- **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.

Se un utente non dispone delle autorizzazioni per una determinata attività, tale attività viene visualizzata in grigio o non viene visualizzata nell'interfaccia utente.

Gestione degli accessi con ruoli utente locali

Per la gestione degli accessi, gli amministratori possono utilizzare le funzionalità RBAC (role-based access control) applicate nell'array di storage. Queste funzionalità sono denominate "ruoli utente locali".

Workflow di configurazione

I ruoli utente locali sono preconfigurati per lo storage array. Per utilizzare i ruoli utente locali per l'autenticazione, gli amministratori possono:

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

Per la gestione degli accessi, gli amministratori possono utilizzare un server LDAP (Lightweight Directory Access Protocol) e un servizio di directory, ad esempio Active Directory di Microsoft.

Workflow di configurazione

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

1. Un amministratore effettua l'accesso a Gestione di sistema di SANtricity con un profilo utente che include le autorizzazioni di amministratore della 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 lo storage array.
4. Una volta stabilita la connessione al server, l'amministratore associa i gruppi di utenti ai ruoli dell'array di storage. Questi ruoli sono predefiniti e non possono essere modificati.
5. L'amministratore verifica la connessione tra il server LDAP e lo storage array.
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.

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 accede a System Manager con un profilo utente che include le autorizzazioni di amministratore della sicurezza.

   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 System 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 System Manager per esportare un file di metadati del service provider per ciascun controller. Dal sistema IdP, l'amministratore importa i 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 System 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 System 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, i seguenti client non possono accedere ai servizi e alle risorse dell'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

Come fare

Visualizzare i ruoli utente locali

Dalla scheda Local User Roles (ruoli utente locali), è possibile visualizzare le mappature dei profili utente ai ruoli predefiniti. Questi mapping fanno parte del RBAC (role-based access control) applicato nell'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.

A proposito di questa attività

I profili utente e le mappature non possono essere modificati. È possibile modificare solo le password.

Fasi

1. Selezionare **Impostazioni › Gestione accessi**.
2. Selezionare la scheda **ruoli utente locali**.

   I profili utente sono mostrati nella tabella:

   - **Root admin** (admin) — Super amministratore che ha accesso a tutte le funzioni del sistema. Questo profilo utente include tutti i ruoli.
   - **Storage admin** (storage) — l'amministratore responsabile di tutto il provisioning dello storage. Questo profilo utente include i seguenti ruoli: Storage Admin, Support Admin e Monitor.
   - **Security admin** (sicurezza) — l'utente responsabile della configurazione della sicurezza, inclusa la gestione degli accessi, la gestione dei certificati e le funzioni dei dischi abilitati alla sicurezza. Questo profilo utente include i seguenti ruoli: Security Admin e Monitor.
   - **Support admin** (support) — l'utente responsabile delle risorse hardware, dei dati di guasto e degli aggiornamenti del firmware. Questo profilo utente include i seguenti ruoli: Support Admin e Monitor.
   - **Monitor** (monitor) — utente con accesso in sola lettura al sistema. Questo profilo utente include solo il ruolo Monitor.

Modificare le password

È possibile modificare le password utente per ciascun profilo 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.

> La modifica della password in System Manager viene modificata anche nell'interfaccia della riga di comando (CLI). Inoltre, le modifiche apportate alla password causano l'interruzione della sessione attiva dell'utente.

Fasi

1. Selezionare **Impostazioni › Gestione accessi**.
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 per richiedere all'utente selezionato di immettere una password per accedere all'array di storage, quindi digitare la nuova password per l'utente selezionato.
6. Immettere la password dell'amministratore locale, quindi fare clic su **Change** (Modifica).

Risultato

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 sull'array di storage. È inoltre possibile consentire agli utenti locali di accedere allo storage array 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 allo storage array senza immettere una password.

Fasi

1. Selezionare **Impostazioni › Gestione accessi**.
2. Selezionare la scheda **ruoli utente locali**.
3. Selezionare il pulsante **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 allo storage array *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 possibile stabilire comunicazioni tra lo storage array e un server LDAP, quindi mappare i gruppi di utenti LDAP ai ruoli predefiniti dell'array.

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 predefiniti dell’array di storage.

> Durante la procedura di aggiunta di un server LDAP, l’interfaccia di gestione legacy viene disattivata. L’interfaccia di gestione legacy (Symbol) è un metodo di comunicazione tra lo storage array e il client di gestione. Se disattivato, lo storage array e il client di gestione utilizzano un metodo di comunicazione più sicuro (REST API over https).

Fasi

1. Selezionare **Impostazioni › Gestione accessi**.
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)
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 bind è chiamato "bindacct", è possibile immettere un valore come "CN=bindacct,CN=Users,DC=cpoc,DC=local".	Password bind (opzionale)
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 lo storage array 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**

Impostazione	Descrizione
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. System Manager non funzionerà correttamente per nessun utente senza il ruolo di monitoraggio presente.

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 **Impostazioni › Gestione accessi**.
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 lo storage array possa comunicare con la configurazione del server LDAP. Il test si verifica dopo aver fatto clic su Save (Salva) nella parte inferiore della finestra di dialogo. 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 saltare 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=copc, DC=local`.
Attributo Username	L'attributo associato all'ID utente per l'autenticazione. Ad esempio: `sAMAccountName`.

Impostazione	Descrizione
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. System Manager non funzionerà correttamente per nessun utente senza il ruolo di monitoraggio presente.

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).

Risultato

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 lo storage array, è possibile rimuovere le informazioni sul server dalla pagina Access Management. 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 **Impostazioni › Gestione accessi**.
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.

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.

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 System 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 a più fasi:

- Fase 1: Caricare il file di metadati IdP
- Fase 2: Esportare i file del provider di servizi
- Fase 3: Mappare i ruoli
- Fase 4: Verifica dell'accesso SSO
- Fase 5: Abilitare SAML

Fase 1: Caricare il file di metadati IdP

Per fornire allo storage array le informazioni di connessione IdP, importare i metadati IdP in System 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.

- 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 che i clock del server IdP e del controller siano sincronizzati (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 System Manager.

A proposito di questa attività

In questa attività, si carica un file di metadati da IdP in System Manager. Il sistema IdP ha bisogno di questi metadati per reindirizzare le richieste di autenticazione all'URL corretto e per validare le risposte ricevute. È necessario caricare un solo file di metadati per l'array di storage, anche se sono presenti due controller.

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 **Import Identity Provider file**.

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.

Prima di iniziare

- Si conosce l'indirizzo IP o il nome di dominio di ciascun controller dell'array di storage.

A proposito di questa attività

In questa attività, si esportano i metadati dai controller (un file per ciascun controller). L'IdP ha bisogno di questi metadati per stabilire una relazione di trust con i controller e per 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 **Export Service Provider Files** (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. Se lo storage array include due controller, ripetere questo passaggio per il secondo controller nel campo **Controller B**.

   Dopo aver fatto clic su Export (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 i file di metadati del provider di servizi esportati.

   Per ciascun controller è disponibile un file in formato XML.

4. Dal server IdP, importare i file di metadati del provider di servizi per stabilire la relazione di trust. È possibile importare i file direttamente o inserire manualmente le informazioni del controller dai file.

Fase 3: Mappare i ruoli

Per fornire agli utenti l'autorizzazione e l'accesso a System 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 System Manager.
- Un file di metadati del service provider per ciascun controller viene importato nel sistema IdP per la relazione di trust.

A proposito di questa attività

In questa attività, si utilizza System Manager per associare i gruppi IdP ai ruoli utente locali.

Fasi

1. Fare clic sul collegamento per la mappatura dei ruoli di System Manager.

   Viene visualizzata la finestra di dialogo **mappatura ruolo**.

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

   Dettagli 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. System 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 System Manager.
- Un file di metadati del service provider per ciascun 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.
   - Gli indirizzi del controller nei file di metadati SP sono corretti.

Fase 5: Abilitare SAML

Il passaggio finale consiste nell'abilitare l'autenticazione utente SAML.

Prima di iniziare

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

A proposito di questa attività

Questa attività descrive come 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.

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.

Risultato

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 ruolo**.

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 System Manager.

Dettagli 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. System 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).

Risultato

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 lo storage array e reimportare i 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 dai controller (un file per ciascun controller). L'IdP ha bisogno di questi metadati per stabilire una relazione di trust con i 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 **Export Service Provider Files** (Esporta file provider di servizi).

4. Per ciascun controller, fare clic su **Export** (Esporta) per salvare il file di metadati nel sistema locale.

I campi dei nomi di dominio per ciascun controller sono di sola lettura.

Prendere nota della posizione in cui è memorizzato il file.

5. Dal sistema locale, individuare i file di metadati del provider di servizi esportati.

   Per ciascun controller è disponibile un file in formato XML.

6. Dal server IdP, importare i file di metadati del provider di servizi. È possibile importare i file direttamente o inserire manualmente le informazioni del controller.
7. Fare clic su **Chiudi**.

Visualizzare l'attività del registro di audit

Visualizzando i registri di controllo, gli utenti con autorizzazioni di amministratore della sicurezza possono monitorare le azioni degli utenti, gli errori di autenticazione, i tentativi di accesso non validi e la durata della sessione utente.

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.

Fasi

1. Selezionare **Impostazioni › Gestione accessi**.
2. Selezionare la scheda **Registro di controllo**.

   L'attività **Registro audit** viene visualizzata in formato tabulare, che include le seguenti colonne di informazioni:

   - **Data/ora** — Timestamp di quando lo storage array ha rilevato l'evento (in GMT).
   - **Username** — Nome utente associato all'evento. Per qualsiasi azione non autenticata sull'array di storage, viene visualizzato "N/A" come nome utente. Le azioni non autenticate potrebbero essere attivate dal proxy interno o da qualche altro meccanismo.
   - **Status Code** — Codice di stato HTTP dell'operazione (200, 400, ecc.) e testo descrittivo associato all'evento.
   - **URL a cui si accede** — URL completo (incluso host) e stringa di query.
   - **Client IP Address** — Indirizzo IP del client associato all'evento.
   - **Origine** — origine di registrazione associata all'evento, che può essere System Manager, CLI, Web Services o Support Shell.
3. Utilizzare le selezioni nella pagina Registro audit per visualizzare e gestire gli eventi.

Dettagli della selezione

Selezione	Descrizione
Mostra gli eventi del…	Limita gli eventi visualizzati in base all'intervallo di date (ultime 24 ore, ultimi 7 giorni, ultimi 30 giorni o un intervallo di date personalizzato).
Filtro	Limita gli eventi visualizzati dai caratteri immessi nel campo. Utilizzare le virgolette ("") per una corrispondenza esatta della parola, immettere `OR` per restituire una o più parole, oppure inserire un trattino (--) per omettere le parole.
Aggiornare	Selezionare **Refresh** (Aggiorna) per aggiornare la pagina agli eventi più recenti.
Visualizza/Modifica impostazioni	Selezionare **Visualizza/Modifica impostazioni** per aprire una finestra di dialogo che consente di specificare un criterio di log completo e il livello di azioni da registrare.
Eliminare gli eventi	Selezionare **Elimina** per aprire una finestra di dialogo che consente di rimuovere gli eventi precedenti dalla pagina.
Mostra/Nascondi colonne	Fare clic sull'icona della colonna **Mostra/Nascondi** per selezionare colonne aggiuntive da visualizzare nella tabella. Le colonne aggiuntive includono: • **Method** — il metodo HTTP (AD esempio, POST, GET, DELETE, ecc.). • **Comando CLI eseguito** — comando CLI (grammatica) eseguito per richieste CLI sicure. • **CLI Return Status** — un codice di stato CLI o una richiesta di file di input dal client. • **Symbol procedure** — procedura di simbolo eseguita. • **SSH Event Type** — tipo di eventi Secure Shell (SSH), come login, logout e login_fail. • **SSH Session PID** — numero ID del processo della sessione SSH. • **SSH Session Duration(s)** — il numero di secondi in cui l'utente ha effettuato l'accesso.
Attiva/disattiva filtri colonna	Fare clic sull'icona **Alterna** per aprire i campi di filtraggio per ciascuna colonna. Immettere i caratteri all'interno di un campo colonna per limitare gli eventi visualizzati da tali caratteri. Fare nuovamente clic sull'icona per chiudere i campi di filtraggio.
Annulla le modifiche	Fare clic sull'icona **Annulla** per ripristinare la configurazione predefinita della tabella.

Selezione	Descrizione
Esportare	Fare clic su **Export** (Esporta) per salvare i dati della tabella in un file CSV (comma Separated Value).

Definire i criteri del registro di controllo

È possibile modificare il criterio di sovrascrittura e i tipi di eventi registrati nel registro di controllo.

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

Questa attività descrive come modificare le impostazioni del registro di controllo, che includono il criterio per la sovrascrittura degli eventi precedenti e il criterio per la registrazione dei tipi di evento.

Fasi

1. Selezionare **Impostazioni › Gestione accessi**.
2. Selezionare la scheda **Registro di controllo**.
3. Selezionare **Visualizza/Modifica impostazioni**.

   Viene visualizzata la finestra di dialogo **Impostazioni registro di controllo**.

4. Modificare il criterio di sovrascrittura o i tipi di eventi registrati.

Dettagli campo

Impostazione	Descrizione
Sovrascrivere il criterio	Determina il criterio per la sovrascrittura di eventi precedenti quando viene raggiunta la capacità massima: • **Consente di sovrascrivere gli eventi meno recenti nel registro di controllo quando il registro di controllo è pieno** — sovrascrive gli eventi precedenti quando il registro di controllo raggiunge 50,000 record. • **Richiedere l'eliminazione manuale degli eventi del registro di controllo** — specifica che gli eventi non verranno cancellati automaticamente; viene invece visualizzato un avviso di soglia in corrispondenza della percentuale impostata. Gli eventi devono essere cancellati manualmente. Se il criterio di sovrascrittura è disattivato e le voci del registro di controllo raggiungono il limite massimo, l'accesso a System Manager viene negato agli utenti senza autorizzazioni di amministratore della sicurezza. Per ripristinare l'accesso al sistema agli utenti senza autorizzazioni di amministratore della sicurezza, un utente assegnato al ruolo di amministratore della protezione deve eliminare i vecchi record di eventi. I criteri di sovrascrittura non si applicano se un server syslog è configurato per l'archiviazione dei registri di controllo.

Impostazione	Descrizione
Livello di azioni da registrare	Determina i tipi di eventi da registrare: • **Registra solo eventi di modifica** — Mostra solo gli eventi in cui un'azione dell'utente comporta la modifica del sistema. • **Registra tutti gli eventi di modifica e di sola lettura** — Mostra tutti gli eventi, inclusa un'azione dell'utente che comporta la lettura o il download delle informazioni.

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

Eliminare gli eventi dal registro di controllo

È possibile cancellare il registro di controllo degli eventi precedenti, rendendo più gestibile la ricerca tra gli eventi. È possibile salvare gli eventi precedenti in un file CSV (comma-Separated Values) al momento dell'eliminazione.

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

Questa attività descrive come rimuovere i vecchi eventi dal registro di controllo.

Fasi

1. Selezionare **Impostazioni › Gestione accessi**.
2. Selezionare la scheda **Registro di controllo**.
3. Selezionare **Delete** (Elimina).

   Viene visualizzata la finestra di dialogo **Delete Audit Log** (Elimina registro di controllo).

4. Selezionare o immettere il numero di eventi meno recenti che si desidera eliminare.
5. Se si desidera esportare gli eventi cancellati in un file CSV (scelta consigliata), mantenere la casella di controllo selezionata. Quando si fa clic su **Delete** (Elimina) nella fase successiva, viene richiesto di inserire un nome e una posizione per il file. In caso contrario, se non si desidera salvare gli eventi in un file CSV, fare clic sulla casella di controllo per deselezionarla.
6. Fare clic su **Delete** (Elimina).

   Viene visualizzata una finestra di dialogo di conferma.

7. Tipo `delete` Nel campo, quindi fare clic su **Delete** (Elimina).

   Gli eventi meno recenti vengono rimossi dalla pagina Registro di controllo.

Configurare il server syslog per i registri di controllo

Se si desidera archiviare i registri di controllo su un server syslog esterno, è possibile configurare le comunicazioni tra tale server e lo storage array. Una volta stabilita la connessione, i registri di controllo vengono salvati automaticamente nel server syslog.

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.
- L'indirizzo del server syslog, il protocollo e il numero di porta devono essere disponibili. L'indirizzo del server può essere un nome di dominio completo, un indirizzo IPv4 o un indirizzo IPv6.
- Se il server utilizza un protocollo sicuro (ad esempio TLS), è necessario che nel sistema locale sia disponibile un certificato dell'autorità di certificazione (CA). I certificati CA identificano i proprietari dei siti Web per connessioni sicure tra server e client.

Fasi

1. Selezionare **Impostazioni › Gestione accessi**.
2. Dalla scheda **Registro di controllo**, selezionare **Configura server Syslog**.

   Viene visualizzata la finestra di dialogo **Configura server Syslog**.

3. Fare clic su **Aggiungi**.

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

4. Inserire le informazioni relative al server, quindi fare clic su **Aggiungi**.
   - Server address (Indirizzo server) - immettere un nome di dominio completo, un indirizzo IPv4 o un indirizzo IPv6.
   - Protocol (protocollo) - selezionare un protocollo dall'elenco a discesa (ad esempio TLS, UDP o TCP).
   - Carica certificato (opzionale) — se è stato selezionato il protocollo TLS e non è stato ancora caricato un certificato CA firmato, fare clic su Sfoglia per caricare un file di certificato. I registri di controllo non vengono archiviati in un server syslog senza un certificato attendibile.

     > Se il certificato diventa non valido in un secondo momento, l'handshake TLS avrà esito negativo. Di conseguenza, un messaggio di errore viene inviato al registro di controllo e i messaggi non vengono più inviati al server syslog. Per risolvere questo problema, è necessario correggere il certificato sul server syslog e accedere al **Impostazioni › Registro audit › Configura server Syslog › Test tutti**.

   - Port (porta) — inserire il numero di porta del ricevitore syslog. Dopo aver fatto clic su **Add** (Aggiungi), viene visualizzata la finestra di dialogo **Configure Syslog Servers** (Configura server Syslog) e il server syslog configurato.
5. Per verificare la connessione del server con lo storage array, selezionare **Test All**.

Risultato

Dopo la configurazione, tutti i nuovi registri di controllo vengono inviati al server syslog. I registri precedenti non vengono trasferiti.

Modificare le impostazioni del server syslog per i record del registro di controllo

È possibile modificare le impostazioni del server syslog utilizzato per l'archiviazione dei registri di controllo e caricare un nuovo certificato CA per il server.

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.
- L'indirizzo del server syslog, il protocollo e il numero di porta devono essere disponibili. L'indirizzo del server può essere un nome di dominio completo, un indirizzo IPv4 o un indirizzo IPv6.
- Se si sta caricando un nuovo certificato CA, il certificato deve essere disponibile nel sistema locale.

Fasi

1. Selezionare **Impostazioni › Gestione accessi**.
2. Dalla scheda **Registro di controllo**, selezionare **Configura server Syslog**.

   I server syslog configurati vengono visualizzati nella pagina.

3. Per modificare le informazioni sul server, selezionare l'icona **Edit** (matita) a destra del nome del server, quindi apportare le modifiche desiderate nei seguenti campi:
   - Server Address (Indirizzo server) - immettere un nome di dominio completo, un indirizzo IPv4 o un indirizzo IPv6.
   - Protocol (protocollo) - selezionare un protocollo dall'elenco a discesa (ad esempio TLS, UDP o TCP).
   - Port (porta) — inserire il numero di porta del ricevitore syslog.
4. Se il protocollo è stato modificato nel protocollo TLS sicuro (da UDP o TCP), fare clic su **Import Trusted Certificate** (Importa certificato attendibile) per caricare un certificato CA.
5. Per verificare la nuova connessione con lo storage array, selezionare **Test All**.

Risultato

Dopo la configurazione, tutti i nuovi registri di controllo vengono inviati al server syslog. I registri precedenti non vengono trasferiti.

FAQ

Perché non riesco ad accedere?

Se si riceve un errore durante il tentativo di accesso a System Manager, esaminare queste possibili cause.

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

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

- È stata attivata una condizione di blocco e il registro di controllo potrebbe essere pieno. Accedere a Gestione accessi ed eliminare i vecchi eventi dal registro di controllo.
- L'autenticazione SAML è attivata. Aggiornare il browser per accedere.

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

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

Cosa occorre sapere prima di aggiungere un server di directory?

Prima di aggiungere un server di directory in Access Management, assicurarsi di soddisfare i seguenti 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, consultare le seguenti linee guida.

Le funzionalità RBAC (role-based access control) integrate dello storage array includono i seguenti ruoli:

- **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.

Servizi di directory

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

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

Quali strumenti di gestione esterni potrebbero essere interessati da questa modifica?

Quando si apportano alcune modifiche in System Manager, ad esempio la commutazione dell'interfaccia di gestione o l'utilizzo di SAML per un metodo di autenticazione, l'utilizzo di alcuni strumenti e funzionalità esterni potrebbe essere limitato.

Interfaccia di gestione

Gli strumenti che comunicano direttamente con l'interfaccia di gestione legacy (Symbol), come il provider SMI-S SANtricity o OnCommand Insight (OCI), non funzionano se non è attivata l'impostazione dell'interfaccia di gestione legacy. Inoltre, non è possibile utilizzare i comandi CLI legacy o eseguire operazioni di mirroring se questa impostazione è disattivata.

Per ulteriori informazioni, contatta il supporto tecnico.

Autenticazione SAML

Quando SAML è attivato, i seguenti client non possono accedere ai servizi e alle risorse dell'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

Per ulteriori informazioni, contatta il supporto tecnico.

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 che i clock del server IdP e del controller siano sincronizzati (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 System Manager.
- Si conosce l'indirizzo IP o il nome di dominio di ciascun controller dell'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 tipi di eventi vengono registrati nel registro di controllo?

Il registro di controllo può registrare gli eventi di modifica o gli eventi di modifica e di sola lettura.

A seconda delle impostazioni del criterio, vengono visualizzati i seguenti tipi di eventi:

- **Eventi di modifica** — azioni dell'utente da System Manager che comportano modifiche al sistema, come il provisioning dello storage.
- **Eventi di modifica e sola lettura** — azioni dell'utente che comportano modifiche al sistema, nonché eventi che comportano la visualizzazione o il download di informazioni, come la visualizzazione delle assegnazioni dei volumi.

Cosa occorre sapere prima di configurare un server syslog?

È possibile archiviare i registri di controllo su un server syslog esterno.

Prima di configurare un server syslog, tenere presenti le seguenti linee guida.

- Assicurarsi di conoscere l'indirizzo del server, il protocollo e il numero della porta. L'indirizzo del server può essere un nome di dominio completo, un indirizzo IPv4 o un indirizzo IPv6.
- Se il server utilizza un protocollo sicuro (ad esempio TLS), è necessario che nel sistema locale sia disponibile un certificato dell'autorità di certificazione (CA). I certificati CA identificano i proprietari dei siti Web per connessioni sicure tra server e client.
- Dopo la configurazione, tutti i nuovi registri di controllo vengono inviati al server syslog. I registri precedenti non vengono trasferiti.
- Le impostazioni di **Overwrite Policy** (disponibili in View/Edit Settings) non influiscono sulla gestione dei log con una configurazione del server syslog.
- I registri di controllo seguono il formato di messaggistica RFC 5424.

Il server syslog non riceve più registri di controllo. Cosa devo fare?

Se è stato configurato un server syslog con un protocollo TLS, il server non può ricevere messaggi se il certificato non è valido per qualsiasi motivo. Nel registro di controllo viene visualizzato un messaggio di errore relativo al certificato non valido.

Per risolvere questo problema, è necessario innanzitutto correggere il certificato per il server syslog. Una volta stabilita una catena di certificati valida, accedere al **Impostazioni › Registro audit › Configura server Syslog › Test tutti**.

Informazioni sul copyright

Informazioni sul marchio commerciale