Utilizzare i servizi di directory

SANtricity 11.8

NetApp
December 16, 2024

Sommario

Utilizzare i servizi di directory 1
Aggiungere il server di directory 1
Modificare le impostazioni del server di directory e le mappature dei ruoli 6
Rimuovere il server di directory 10

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 server
Immettere l'URL per accedere 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 bind 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, generalmente 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 server
L'URL per accedere al server LDAP sotto forma di `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	Contesto LDAP per la ricerca degli utenti, generalmente 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. Digitare `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.

Informazioni sul copyright

Informazioni sul marchio commerciale