



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 (<i>nome utente@dominio</i>) per specificare il server di directory da autenticare.	URL server
Immettere l'URL per accedere al server LDAP nel formato <code>ldap[s]://host:port*</code> .	Carica certificato (opzionale)

Impostazione	Descrizione
<div data-bbox="245 432 302 485" data-label="Image"> </div> <p data-bbox="358 170 483 747">Questo campo viene visualizzato solo se è stato specificato un protocollo LDAPS nel campo URL server sopra riportato.</p> <p data-bbox="212 793 516 1094">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.</p>	<p data-bbox="526 159 850 191">Account BIND (opzionale)</p>
<p data-bbox="212 1150 505 1696">Inserire un account utente di sola lettura per le query di ricerca sul server LDAP e per la ricerca all'interno dei gruppi. Immettere il nome dell'account in formato LDAP. Ad esempio, se l'utente bind è chiamato "bindacct", è possibile immettere un valore come CN=bindacct, CN=Users, DC=cpoc, DC=local.</p>	<p data-bbox="526 1150 857 1182">Password bind (opzionale)</p>

Impostazione	Descrizione
<div style="display: flex; align-items: center;">  <p data-bbox="358 170 472 541">Questo campo viene visualizzato quando si immette un account BIND.</p> </div> <p data-bbox="212 590 500 653">Immettere la password per l'account BIND.</p>	<p data-bbox="529 159 1203 191">Verificare la connessione al server prima di aggiungerli</p>
<p data-bbox="212 711 511 1115">Selezionare questa casella di controllo per assicurarsi che il sistema possa comunicare con la configurazione del server LDAP immessa. Il test si verifica dopo aver fatto clic su Add (Aggiungi) nella parte inferiore della finestra di dialogo.</p> <p data-bbox="212 1150 505 1524">Se questa casella di controllo è selezionata e il test non riesce, la configurazione non viene aggiunta. È necessario risolvere l'errore o deselezionare la casella di controllo per saltare il test e aggiungere la configurazione.</p>	<p data-bbox="529 711 862 743">Impostazioni dei privilegi</p>
<p data-bbox="212 1577 423 1608">Ricerca DN base</p>	<p data-bbox="529 1577 1430 1640">Immettere il contesto LDAP per la ricerca degli utenti, generalmente sotto forma di <code>CN=Users, DC=cpoc, DC=local</code>.</p>
<p data-bbox="212 1698 456 1730">Attributo Username</p>	<p data-bbox="529 1698 1438 1761">Inserire l'attributo associato all'ID utente per l'autenticazione. Ad esempio: <code>sAMAccountName</code>.</p>
<p data-bbox="212 1820 456 1852">Attributo/i di gruppo</p>	<p data-bbox="529 1820 1438 1883">Inserire un elenco di attributi di gruppo nell'utente, che viene utilizzato per il mapping gruppo-ruolo. Ad esempio: <code>memberOf, managedObjects</code>.</p>

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

Dettagli del campo

Impostazione	Descrizione
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	<p>Fare clic nel campo e selezionare uno dei ruoli utente locali da mappare al DN del gruppo. È necessario selezionare singolarmente ciascun ruolo che si desidera includere per questo gruppo. Il ruolo di monitoraggio è necessario in combinazione con gli altri ruoli per accedere a Gestione unificata di SANtricity. I ruoli mappati includono le seguenti autorizzazioni:</p> <ul style="list-style-type: none"> • 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 (<i>nome utente@dominio</i>) per specificare il server di directory da autenticare.	URL server
L'URL per accedere al server LDAP sotto forma di <code>ldap[s]://host:port</code> .	Account BIND (opzionale)
L'account utente di sola lettura per le query di ricerca sul server LDAP e per la ricerca all'interno dei gruppi.	Password bind (opzionale)
La password per l'account BIND. (Questo campo viene visualizzato quando viene inserito un account BIND).	Verificare la connessione al server prima di salvare

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

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

Dettagli del campo

Impostazione	Descrizione
Mapping	DN gruppo
<p>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:</p> <p><code>[]{}()<>*+ -=! ? ^</code></p>	
Ruoli	<p>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:</p> <ul style="list-style-type: none">• 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

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.