



FAQ

SANtricity 11.8

NetApp
April 05, 2024

Sommario

- FAQ 1
 - Perché non riesco ad accedere? 1
 - Cosa occorre sapere prima di aggiungere un server di directory? 1
 - Cosa occorre sapere sulla mappatura dei ruoli degli array di storage? 1
 - Cosa occorre sapere prima di configurare e abilitare SAML? 2
 - Quali sono gli utenti locali? 3

FAQ

Perché non riesco ad accedere?

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

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

- Il nome utente o la password immessi non sono corretti.
- Privilegi insufficienti.
- Si è tentato di accedere più volte senza successo, attivando la modalità di blocco. Attendere 10 minuti per eseguire nuovamente l'accesso.
- L'autenticazione SAML è attivata. Aggiornare il browser per accedere.

Cosa occorre sapere prima di aggiungere un server di directory?

Prima di aggiungere un server di directory in Access Management, è necessario soddisfare determinati requisiti.

- I gruppi di utenti devono essere definiti nel servizio di directory.
- Le credenziali del server LDAP devono essere disponibili, inclusi il nome di dominio, l'URL del server e, facoltativamente, il nome utente e la password dell'account BIND.
- Per i server LDAPS che utilizzano un protocollo sicuro, la catena di certificati del server LDAP deve essere installata sul computer locale.

Cosa occorre sapere sulla mappatura dei ruoli degli array di storage?

Prima di mappare i gruppi ai ruoli, rivedere le linee guida.

Le funzionalità RBAC (role-based access control) includono i seguenti ruoli:

- **Storage admin** — accesso completo in lettura/scrittura agli oggetti storage sugli array, ma nessun accesso alla configurazione di sicurezza.
- **Security admin** — accesso alla configurazione di sicurezza in Access Management e Certificate Management.
- **Support admin** — accesso a tutte le risorse hardware su storage array, dati di guasto ed eventi MEL. Nessun accesso agli oggetti di storage o alla configurazione di sicurezza.
- **Monitor** — accesso in sola lettura a tutti gli oggetti di storage, ma nessun accesso alla configurazione di sicurezza.



Il ruolo Monitor è necessario per tutti gli utenti, incluso l'amministratore.

Se si utilizza un server LDAP (Lightweight Directory Access Protocol) e servizi di directory, assicurarsi che:

- Un amministratore ha definito i gruppi di utenti nel servizio di directory.
- Si conoscono i nomi di dominio del gruppo per i gruppi di utenti LDAP.

SAML

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

- Un amministratore del provider di identità (IdP) ha configurato gli attributi utente e l'appartenenza al gruppo nel sistema IdP.
- Conosci i nomi dei membri del gruppo.
- Si conosce il valore dell'attributo per il gruppo da mappare. Sono supportate le espressioni regolari. Questi caratteri speciali di espressione regolare devono essere escapati con una barra rovesciata (\) se non fanno parte di un modello di espressione regolare:

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

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

Cosa occorre sapere prima di configurare e abilitare SAML?

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

Requisiti

Prima di iniziare, assicurarsi che:

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

Restrizioni

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

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

tecnico per assistenza. Si consiglia di testare gli accessi SSO prima di attivare SAML nella fase finale di configurazione. (Il sistema esegue anche un test di accesso SSO prima di attivare SAML).

- Se si disattiva SAML in futuro, il sistema ripristina automaticamente la configurazione precedente (ruoli utente locali e/o servizi di directory).
- Se i servizi di directory sono attualmente configurati per l'autenticazione dell'utente, SAML sovrascrive tale configurazione.
- Quando SAML è configurato, i seguenti client non possono accedere alle risorse degli array di storage:
 - Finestra Enterprise Management (EMW)
 - Interfaccia a riga di comando (CLI)
 - Client Software Developer Kit (SDK)
 - Client in-band
 - Client REST API per l'autenticazione di base HTTP
 - Effettuare l'accesso utilizzando l'endpoint REST API standard

Quali sono gli utenti locali?

Gli utenti locali sono predefiniti nel sistema e includono autorizzazioni specifiche.

Gli utenti locali includono:

- **Admin** — Amministratore eccellente che ha accesso a tutte le funzioni del sistema. Questo utente include tutti i ruoli. La password deve essere impostata al primo accesso.
- **Storage** — l'amministratore responsabile di tutto il provisioning dello storage. Questo utente include i seguenti ruoli: Storage Admin, Support Admin e Monitor. Questo account viene disattivato fino a quando non viene impostata una password.
- **Security** — l'utente responsabile della configurazione della sicurezza, inclusi Access Management e Certificate Management. Questo utente include i seguenti ruoli: Security Admin e Monitor. Questo account viene disattivato fino a quando non viene impostata una password.
- **Support** — l'utente responsabile delle risorse hardware, dei dati di guasto e degli aggiornamenti del firmware. Questo utente include i seguenti ruoli: Support Admin e Monitor. Questo account viene disattivato fino a quando non viene impostata una password.
- **Monitor** — un utente con accesso in sola lettura al sistema. Questo utente include solo il ruolo Monitor. Questo account viene disattivato fino a quando non viene impostata una password.
- **rw** (lettura/scrittura) — questo utente include i seguenti ruoli: Amministratore dello storage, amministratore del supporto e monitor. Questo account viene disattivato fino a quando non viene impostata una password.
- **Ro** (sola lettura) — questo utente include solo il ruolo Monitor. Questo account viene disattivato fino a quando non viene impostata una password.

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.