



Concetti

SANtricity 11.8

NetApp
December 16, 2024

Sommario

- Concetti 1
 - Come funziona Access Management. 1
 - Terminologia per la gestione degli accessi. 2
 - Autorizzazioni per i ruoli mappati 3
 - Gestione degli accessi con ruoli utente locali 3
 - Gestione degli accessi con servizi di directory. 4
 - Gestione degli accessi con SAML 5

Concetti

Come funziona Access Management

Utilizzare Access Management per stabilire l'autenticazione dell'utente in Unified Manager.

Workflow di configurazione

La configurazione di Access Management funziona come segue:

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



Per il primo accesso, il nome utente `admin` viene visualizzato automaticamente e non può essere modificato. L'utente `admin` ha accesso completo a tutte le funzioni del sistema. La password deve essere impostata al primo accesso.

2. L'amministratore accede a Access Management nell'interfaccia utente, che include ruoli utente locali preconfigurati. Questi ruoli sono un'implementazione delle funzionalità RBAC (role-based access control).
3. L'amministratore configura uno o più dei seguenti metodi di autenticazione:
 - **Ruoli utente locali** — l'autenticazione viene gestita tramite funzionalità RBAC. I ruoli utente locali includono utenti predefiniti e ruoli con autorizzazioni di accesso specifiche. Gli amministratori possono utilizzare questi ruoli utente locali come singolo metodo di autenticazione o in combinazione con un servizio di directory. Non è necessaria alcuna configurazione, ad eccezione dell'impostazione delle password per gli utenti.
 - **Servizi di directory** — l'autenticazione viene gestita tramite un server LDAP (Lightweight Directory Access Protocol) e un servizio di directory, ad esempio Active Directory di Microsoft. Un amministratore si connette al server LDAP, quindi associa gli utenti LDAP ai ruoli utente locali.
 - **SAML** — l'autenticazione viene gestita tramite un provider di identità (IdP) utilizzando il linguaggio SAML (Security Assertion Markup Language) 2.0. Un amministratore stabilisce la comunicazione tra il sistema IdP e l'array di storage, quindi mappa gli utenti IdP ai ruoli utente locali integrati nell'array di storage.
4. L'amministratore fornisce agli utenti le credenziali di accesso per Unified Manager.
5. Gli utenti accedono al sistema inserendo le proprie credenziali. Durante l'accesso, il sistema esegue le seguenti attività in background:
 - Autentica il nome utente e la password rispetto all'account utente.
 - Determina le autorizzazioni dell'utente in base ai ruoli assegnati.
 - Fornisce all'utente l'accesso alle funzioni dell'interfaccia utente.
 - Visualizza il nome utente nel banner superiore.

Funzioni disponibili in Unified Manager

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

- **Storage admin** — accesso completo in lettura/scrittura agli oggetti storage sugli array, ma nessun accesso alla configurazione di sicurezza.

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

Una funzione non disponibile è disattivata o non viene visualizzata nell'interfaccia utente.

Terminologia per la gestione degli accessi

Scopri come si applicano i termini di Access Management a Unified Manager.

Termine	Descrizione
Active Directory	Active Directory (ad) è un servizio di directory Microsoft che utilizza LDAP per le reti di dominio Windows.
Binding	Le operazioni BIND vengono utilizzate per autenticare i client nel server di directory. Il binding in genere richiede credenziali di account e password, ma alcuni server consentono operazioni di binding anonime.
CIRCA	Un'autorità di certificazione (CA) è un'entità attendibile che emette documenti elettronici, denominati certificati digitali, per la sicurezza di Internet. Questi certificati identificano i proprietari dei siti Web, consentendo connessioni sicure tra client e server.
Certificato	Un certificato identifica il proprietario di un sito per motivi di sicurezza, impedendo agli autori degli attacchi di impersonare il sito. Il certificato contiene informazioni sul proprietario del sito e l'identità dell'entità attendibile che certifica (firma) queste informazioni.
LDAP	LDAP (Lightweight Directory Access Protocol) è un protocollo applicativo per l'accesso e la manutenzione dei servizi informativi di directory distribuiti. Questo protocollo consente a numerose applicazioni e servizi diversi di connettersi al server LDAP per la convalida degli utenti.
RBAC	RBAC (role-based access control) è un metodo per regolare l'accesso alle risorse di computer o di rete in base ai ruoli dei singoli utenti. Unified Manager include ruoli predefiniti.
SAML	SAML (Security Assertion Markup Language) è uno standard basato su XML per l'autenticazione e l'autorizzazione tra due entità. SAML consente l'autenticazione a più fattori, in cui gli utenti devono fornire due o più elementi per dimostrare la propria identità (ad esempio, una password e un'impronta digitale). La funzionalità SAML integrata dello storage array è conforme a SAML2.0 per l'asserzione, l'autenticazione e l'autorizzazione dell'identità.

Termine	Descrizione
SSO	SSO (Single Sign-on) è un servizio di autenticazione che consente a un set di credenziali di accesso di accedere a più applicazioni.
Proxy dei servizi Web	Il proxy dei servizi Web, che fornisce l'accesso tramite meccanismi HTTPS standard, consente agli amministratori di configurare i servizi di gestione per gli array di storage. Il proxy può essere installato su host Windows o Linux. L'interfaccia di Unified Manager è disponibile con Web Services Proxy.

Autorizzazioni per i ruoli mappati

Le funzionalità RBAC (role-based access control) includono utenti predefiniti con uno o più ruoli mappati. Ogni ruolo include le autorizzazioni per l'accesso alle attività in Unified Manager.

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

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

Se un utente non dispone delle autorizzazioni per una determinata funzione, tale funzione non è disponibile per la selezione o non viene visualizzata nell'interfaccia utente.

Gestione degli accessi con ruoli utente locali

Gli amministratori possono utilizzare le funzionalità RBAC (role-based access control) applicate in Unified Manager. Queste funzionalità sono denominate "ruoli utente locali".

Workflow di configurazione

I ruoli utente locali sono preconfigurati nel sistema. Per utilizzare i ruoli utente locali per l'autenticazione, gli amministratori possono:

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



L'`admin`utente ha accesso completo a tutte le funzioni del sistema.

2. Un amministratore esamina i profili utente predefiniti e non modificabili.
3. Facoltativamente, l'amministratore assegna nuove password per ogni profilo utente.

4. Gli utenti accedono al sistema con le credenziali assegnate.

Gestione

Quando si utilizzano solo ruoli utente locali per l'autenticazione, gli amministratori possono eseguire le seguenti attività di gestione:

- Modificare le password.
- Impostare una lunghezza minima per le password.
- Consentire agli utenti di effettuare l'accesso senza password.

Gestione degli accessi con servizi di directory

Gli amministratori possono utilizzare un server LDAP (Lightweight Directory Access Protocol) e un servizio di directory, ad esempio Active Directory di Microsoft.

Workflow di configurazione

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

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



L'`admin`utente ha accesso completo a tutte le funzioni del sistema.

2. L'amministratore inserisce le impostazioni di configurazione per il server LDAP. Le impostazioni includono il nome di dominio, l'URL e le informazioni sull'account di binding.
3. Se il server LDAP utilizza un protocollo sicuro (LDAPS), l'amministratore carica una catena di certificati CA (Certificate Authority) per l'autenticazione tra il server LDAP e il sistema host in cui è installato il proxy dei servizi Web.
4. Una volta stabilita la connessione al server, l'amministratore associa i gruppi di utenti ai ruoli utente locali. Questi ruoli sono predefiniti e non possono essere modificati.
5. L'amministratore verifica la connessione tra il server LDAP e il proxy dei servizi Web.
6. Gli utenti accedono al sistema con le credenziali LDAP/Directory Services assegnate.

Gestione

Quando si utilizzano i servizi di directory per l'autenticazione, gli amministratori possono eseguire le seguenti attività di gestione:

- Aggiungere un server di directory.
- Modificare le impostazioni del server di directory.
- Associare gli utenti LDAP ai ruoli utente locali.
- Rimuovere un server di directory.
- Modificare le password.
- Impostare una lunghezza minima per le password.

- Consentire agli utenti di effettuare l'accesso senza password.

Gestione degli accessi con SAML

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

Workflow di configurazione

La configurazione SAML funziona come segue:

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



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

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



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

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



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

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

Gestione

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

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

Restrizioni di accesso

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

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

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

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.