Abilitare l'autenticazione a più fattori

Element Software

NetApp
November 12, 2025

This PDF was generated from https://docs.netapp.com/it-it/element-software/storage/task_system_manage_mfa_set_up_multi_factor_authentication.html on November 12, 2025. Always check docs.netapp.com for the latest.

Sommario

Abilitare l’autenticazione a più fattori 1
Impostare l’autenticazione a più fattori 1
Trova ulteriori informazioni 1
Ulteriori informazioni per l’autenticazione a più fattori 2
Trova ulteriori informazioni 2

Abilitare l’autenticazione a più fattori

Impostare l’autenticazione a più fattori

L’autenticazione a più fattori (MFA) utilizza un provider di identità (IdP) di terze parti tramite il linguaggio SAML (Security Assertion Markup Language) per gestire le sessioni utente. MFA consente agli amministratori di configurare ulteriori fattori di autenticazione, come password e SMS, password e messaggi di posta elettronica.

È possibile utilizzare questi passaggi di base tramite l’API Element per configurare il cluster in modo che utilizzi l’autenticazione a più fattori.

I dettagli di ciascun metodo API possono essere trovati in "Riferimento API dell’elemento".

1. Creare una nuova configurazione IdP (Identity Provider) di terze parti per il cluster chiamando il seguente metodo API e passando i metadati IdP in formato JSON: `CreateIdpConfiguration`

   I metadati IDP, in formato testo normale, vengono recuperati da IdP di terze parti. Questi metadati devono essere validati per garantire che siano formattati correttamente in JSON. Sono disponibili numerose applicazioni per formatter JSON, ad esempio:https://freeformatter.com/json-escape.html.

2. Recuperare i metadati del cluster, tramite spMetadataUrl, da copiare nell’IdP di terze parti chiamando il seguente metodo API: `ListIdpConfigurations`

   SpMetadataUrl è un URL utilizzato per recuperare i metadati del provider di servizi dal cluster per IdP al fine di stabilire una relazione di trust.

3. Configurare le asserzioni SAML sull’IdP di terze parti in modo che includa l’attributo “NameID” per identificare in modo univoco un utente per la registrazione dell’audit e per il corretto funzionamento della disconnessione singola.
4. Creare uno o più account utente amministratore del cluster autenticati da un IdP di terze parti per l’autorizzazione chiamando il seguente metodo API:`AddIdpClusterAdmin`

   > Il nome utente per l’amministratore del cluster IdP deve corrispondere alla mappatura nome/valore attributo SAML per l’effetto desiderato, come mostrato negli esempi seguenti:

   - Email=bob@company.com — dove IdP è configurato per rilasciare un indirizzo email negli attributi SAML.
   - Group=cluster-Administrator - dove IdP è configurato per rilasciare una proprietà di gruppo in cui tutti gli utenti devono avere accesso. Tenere presente che l’associazione nome attributo/valore SAML è sensibile alla distinzione tra maiuscole e minuscole per motivi di sicurezza.
5. Abilitare MFA per il cluster chiamando il seguente metodo API: `EnableIdpAuthentication`

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Ulteriori informazioni per l'autenticazione a più fattori

È necessario conoscere le seguenti avvertenze relative all'autenticazione a più fattori.

- Per aggiornare i certificati IdP non più validi, è necessario utilizzare un utente amministratore non IdP per chiamare il seguente metodo API: `UpdateIdpConfiguration`
- MFA non è compatibile con i certificati di lunghezza inferiore a 2048 bit. Per impostazione predefinita, nel cluster viene creato un certificato SSL a 2048 bit. Evitare di impostare un certificato di dimensioni inferiori quando si chiama il metodo API: `SetSSLCertificate`

> Se il cluster utilizza un certificato precedente all'aggiornamento a meno di 2048 bit, il certificato del cluster deve essere aggiornato con un certificato a 2048 bit o superiore dopo l'aggiornamento all'elemento 12.0 o successivo.

- Gli utenti amministratori IDP non possono essere utilizzati per effettuare chiamate API direttamente (ad esempio, tramite SDK o Postman) o per altre integrazioni (ad esempio, OpenStack Cinder o vCenter Plug-in). Aggiungere utenti amministratori cluster LDAP o utenti amministratori cluster locali se si desidera creare utenti con queste funzionalità.

Trova ulteriori informazioni

- "Gestione dello storage con l'API Element"
- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Informazioni sul copyright

Copyright © 2025 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 COMMERCIABILITÀ 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 CONSEQUENZIALE (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.