Abilitare l'autenticazione a più fattori

Element Software

NetApp
October 01, 2024

Sommario

Abilitare 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.

Impostare l’autenticazione a più fattori

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 sono disponibili nella "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, per 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 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 che non sono 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. Si consiglia di 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

Informazioni sul marchio commerciale