



Multi-Faktor-Authentifizierung aktivieren

Element Software

NetApp
October 01, 2024

Inhalt

- Multi-Faktor-Authentifizierung aktivieren 1
 - Richten Sie die Multi-Faktor-Authentifizierung ein 1
 - Zusätzliche Informationen für Multi-Faktor-Authentifizierung 2

Multi-Faktor-Authentifizierung aktivieren

Multi-Faktor-Authentifizierung (MFA) verwendet zum Verwalten von Benutzersitzungen einen Drittanbieter-Identitätsanbieter (IdP) über die Security Assertion Markup Language (SAML). MFA ermöglicht Administratoren, zusätzliche Authentifizierungsfaktoren wie Passwort und Textnachricht, Kennwort und E-Mail-Nachricht nach Bedarf zu konfigurieren.

Richten Sie die Multi-Faktor-Authentifizierung ein

Sie können diese grundlegenden Schritte über die Element API verwenden, um Ihr Cluster zur Multi-Faktor-Authentifizierung einzurichten.

Details zu den einzelnen API-Methoden finden Sie im "[Element-API-Referenz](#)".

1. Erstellen Sie eine neue IdP-Konfiguration (Third Party Identity Provider) für das Cluster, indem Sie die folgende API-Methode aufrufen und die IdP-Metadaten im JSON-Format übergeben:

`CreateIdpConfiguration`

IdP-Metadaten werden im Klartextformat aus dem Drittanbieter-IdP abgerufen. Diese Metadaten müssen validiert werden, um sicherzustellen, dass sie korrekt in JSON formatiert sind. Es stehen zahlreiche JSON-Formatierer-Anwendungen zur Verfügung, zum Beispiel: <https://freeformatter.com/json-escape.html>.

2. Rufen Sie Cluster-Metadaten über `spMetadataUrl` ab, um sie in das IdP eines Drittanbieters zu kopieren, indem Sie die folgende API-Methode aufrufen: `ListIdpConfigurations`

`SpMetadataUrl` ist eine URL, mit der die Metadaten des Dienstanbieters für das IdP aus dem Cluster abgerufen werden, um eine Vertrauensbeziehung aufzubauen.

3. Konfigurieren Sie die SAML-Behauptungen auf dem IdP eines Drittanbieters so, dass das Attribut „NameID“ verwendet wird, dass ein Benutzer für die Prüfprotokollierung eindeutig identifiziert wird und dass Single Logout ordnungsgemäß funktioniert.
4. Erstellen Sie ein oder mehrere Cluster-Administrator-Benutzerkonten, die von einem IdP eines Drittanbieters zur Autorisierung authentifiziert wurden, indem Sie die folgende API-Methode aufrufen: `AddIdpClusterAdmin`



Der Benutzername für den IdP-Clusteradministrator muss mit dem SAML-Attribut Name/Wert-Mapping für den gewünschten Effekt übereinstimmen, wie in den folgenden Beispielen dargestellt:

- `Email=bob@company.com` — wobei das IdP so konfiguriert ist, dass es eine E-Mail-Adresse in den SAML-Attributen gibt.
- `Group=Cluster-Administrator` - wobei das IdP so konfiguriert ist, dass es eine Gruppeneigenschaft freigibt, in der alle Benutzer Zugriff haben sollen. Beachten Sie, dass die Paarung des SAML-Attributs Name/Wert zwischen Groß- und Kleinschreibung und Sicherheit beachtet wird.

5. Aktivieren Sie MFA für das Cluster, indem Sie die folgende API-Methode aufrufen:

`EnableIdpAuthentication`

Weitere Informationen

- ["Dokumentation von SolidFire und Element Software"](#)
- ["NetApp Element Plug-in für vCenter Server"](#)

Zusätzliche Informationen für Multi-Faktor-Authentifizierung

Beachten Sie die folgenden Einschränkungen bei der Multi-Faktor-Authentifizierung.

- Um nicht mehr gültige IdP-Zertifikate zu aktualisieren, müssen Sie einen nicht-IdP-Admin-Benutzer verwenden, um die folgende API-Methode aufzurufen: `UpdateIdpConfiguration`
- MFA ist nicht kompatibel mit Zertifikaten, die weniger als 2048 Bit lang sind. Standardmäßig wird auf dem Cluster ein 2048-Bit-SSL-Zertifikat erstellt. Sie sollten vermeiden, ein kleineres Zertifikat beim Aufruf der API-Methode festzulegen: `SetSSLCertificate`



Wenn das Cluster ein Zertifikat verwendet, das vor dem Upgrade weniger als 2048-Bit enthält, muss das Cluster-Zertifikat nach dem Upgrade auf Element 12.0 oder höher mit einem Zertifikat von mindestens 2048 Bit aktualisiert werden.

- IDP Admin-Benutzer können nicht dazu verwendet werden, API-Aufrufe direkt (beispielsweise über SDKs oder Postman) zu tätigen oder andere Integrationen (z. B. OpenStack Cinder oder vCenter Plug-in) zu verwenden. Fügen Sie entweder LDAP-Cluster-Administratorbenutzer oder lokale Cluster-Admin-Benutzer hinzu, wenn Sie Benutzer mit diesen Fähigkeiten erstellen müssen.

Weitere Informationen

- ["Storage-Management mit der Element API"](#)
- ["Dokumentation von SolidFire und Element Software"](#)
- ["NetApp Element Plug-in für vCenter Server"](#)

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFT SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.