



Aktivieren Sie die Multi-Faktor-Authentifizierung

Element Software

NetApp
November 12, 2025

Inhalt

- Aktivieren Sie die Multi-Faktor-Authentifizierung 1
 - Multifaktor-Authentifizierung einrichten 1
 - Weitere Informationen 2
- Zusätzliche Informationen zur Multi-Faktor-Authentifizierung 2
 - Weitere Informationen 2

Aktivieren Sie die Multi-Faktor-Authentifizierung

Multifaktor-Authentifizierung einrichten

Die Multi-Faktor-Authentifizierung (MFA) nutzt einen Drittanbieter-Identitätsanbieter (IdP) über die Security Assertion Markup Language (SAML), um Benutzersitzungen zu verwalten. Die Multi-Faktor-Authentifizierung (MFA) ermöglicht es Administratoren, bei Bedarf zusätzliche Authentifizierungsfaktoren zu konfigurieren, wie beispielsweise Passwort und SMS oder Passwort und E-Mail-Nachricht.

Mithilfe dieser grundlegenden Schritte können Sie über die Element API Ihren Cluster für die Verwendung der Multi-Faktor-Authentifizierung einrichten.

Einzelheiten zu jeder API-Methode finden Sie in der "[Element-API-Referenz](#)".

1. Erstellen Sie eine neue Konfiguration eines Drittanbieter-Identitätsanbieters (IdP) für den Cluster, indem Sie die folgende API-Methode aufrufen und die IdP-Metadaten im JSON-Format übergeben:

`CreateIdpConfiguration`

Die IdP-Metadaten werden im Klartextformat vom Drittanbieter-IdP abgerufen. Diese Metadaten müssen validiert werden, um sicherzustellen, dass sie korrekt im JSON-Format vorliegen. Es gibt zahlreiche JSON-Formatierungsanwendungen, die Sie verwenden können, zum Beispiel: <https://freeformatter.com/json-escape.html>.

2. Rufen Sie die Cluster-Metadaten über `spMetadataUrl` ab, um sie durch Aufruf der folgenden API-Methode an den Drittanbieter-IdP zu kopieren: `ListIdpConfigurations`

`spMetadataUrl` ist eine URL, die verwendet wird, um Dienstanbieter-Metadaten aus dem Cluster für den IdP abzurufen, um eine Vertrauensbeziehung herzustellen.

3. Konfigurieren Sie SAML-Assertions auf dem Drittanbieter-IdP so, dass sie das Attribut "NameID" enthalten, um einen Benutzer für die Audit-Protokollierung eindeutig zu identifizieren und damit Single Logout ordnungsgemäß funktioniert.
4. Erstellen Sie ein oder mehrere Cluster-Administrator-Benutzerkonten, die von einem Drittanbieter-IdP zur Autorisierung authentifiziert werden, indem Sie die folgende API-Methode aufrufen: `AddIdpClusterAdmin`



Der Benutzername des IdP-Clusteradministrators muss mit der SAML-Attribut-Name/Wert-Zuordnung übereinstimmen, um den gewünschten Effekt zu erzielen, wie in den folgenden Beispielen gezeigt:

- `email=bob@company.com` — wobei der IdP so konfiguriert ist, dass er eine E-Mail-Adresse in den SAML-Attributen freigibt.
- `group=cluster-administrator` - wobei der IdP so konfiguriert ist, dass er eine Gruppeneigenschaft freigibt, auf die alle Benutzer Zugriff haben sollen. Beachten Sie, dass bei der SAML-Attribut-Name/Wert-Zuordnung aus Sicherheitsgründen zwischen Groß- und Kleinschreibung unterschieden wird.

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

`EnableIdpAuthentication`

Weitere Informationen

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

Zusätzliche Informationen zur Multi-Faktor-Authentifizierung

Beachten Sie bitte die folgenden Einschränkungen im Zusammenhang mit der Multi-Faktor-Authentifizierung.

- Um abgelaufene IdP-Zertifikate zu aktualisieren, müssen Sie mit einem Nicht-IdP-Administratorbenutzer die folgende API-Methode aufrufen: `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, beim Aufruf der API-Methode ein kleineres Zertifikat zu verwenden: `SetSSLCertificate`



Wenn der Cluster vor dem Upgrade ein Zertifikat mit weniger als 2048 Bit verwendet, muss das Clusterzertifikat nach dem Upgrade auf Element 12.0 oder höher durch ein Zertifikat mit mindestens 2048 Bit ersetzt werden.

- IdP-Administratorbenutzer können nicht verwendet werden, um API-Aufrufe direkt durchzuführen (z. B. über SDKs oder Postman) oder für andere Integrationen (z. B. OpenStack Cinder oder vCenter Plug-in) verwendet zu werden. Fügen Sie entweder LDAP-Cluster-Administratorbenutzer oder lokale Cluster-Administratorbenutzer hinzu, wenn Sie Benutzer erstellen müssen, die über diese Berechtigungen verfügen.

Weitere Informationen

- ["Speicherverwaltung mit der Element-API"](#)
- ["SolidFire und Element-Softwaredokumentation"](#)
- ["NetApp Element Plug-in für vCenter Server"](#)

Copyright-Informationen

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers 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.