Multi-Faktor-Authentifizierung aktivieren

Element Software

NetApp
October 01, 2024

Inhalt

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"