Activez l'authentification multifacteur

Element Software

NetApp
March 01, 2023

Table des matières

Activez l’authentification multifacteur

L’authentification multifacteur (MFA) fait appel à un fournisseur d’identités tiers via le langage SAML pour gérer les sessions utilisateur. L’authentification multifacteur permet aux administrateurs de configurer d’autres facteurs d’authentification, tels que le mot de passe et l’e-mail, ainsi que le mot de passe et l’e-mail.

Configuration de l’authentification multifacteur

Vous pouvez utiliser ces étapes de base avec l’API Element pour configurer votre cluster afin qu’il utilise l’authentification multifacteur.

Vous trouverez des détails sur chaque méthode API dans le "Référence de l’API d’élément".

1. Créez une nouvelle configuration IDP pour le cluster en appelant la méthode d’API suivante et en transmettant les métadonnées IDP au format JSON : `CreateIdpConfiguration`

   Les métadonnées IDP, au format texte brut, sont extraites du IDP tiers. Ces métadonnées doivent être validées pour être correctement formatées dans JSON. De nombreuses applications de formateur JSON sont disponibles, par exemple :https://freeformatter.com/json-escape.html.

2. Récupérez les métadonnées du cluster, via spMetadaUrl, pour les copier vers le IDP tiers en appelant la méthode d’API suivante : `ListIdpConfigurations`

   SpMetadaUrl est une URL utilisée pour récupérer les métadonnées du fournisseur de services du cluster pour le PDI afin d’établir une relation de confiance.

3. Configurez les assertions SAML sur l’IDP tiers pour inclure l’attribut « NameID » afin d’identifier de manière unique un utilisateur pour la journalisation d’audit et pour que Single Logout fonctionne correctement.
4. Créez un ou plusieurs comptes utilisateur administrateur de cluster authentifiés par un IDP tiers pour autorisation en appelant la méthode API suivante :`AddIdpClusterAdmin`

   > Le nom d’utilisateur de l’administrateur de cluster IDP doit correspondre au mappage de nom/valeur de l’attribut SAML pour l’effet souhaité, comme indiqué dans les exemples suivants :

   - Email=bob@company.com — où le IDP est configuré pour publier une adresse électronique dans les attributs SAML.
   - Group=cluster-Administrator - où le IDP est configuré pour libérer une propriété de groupe dans laquelle tous les utilisateurs doivent avoir accès. Notez que le couplage nom/valeur de l’attribut SAML est sensible à la casse à des fins de sécurité.
5. Activez l’authentification multifacteur pour le cluster en appelant la méthode API suivante : `EnableIdpAuthentication`

Trouvez plus d’informations

- "Page Ressources SolidFire et Element"
- "Plug-in NetApp Element pour vCenter Server"

Informations supplémentaires pour l’authentification multifacteur

Concernant l’authentification multifacteur, vous devez connaître les mises en garde suivantes.

- Pour actualiser les certificats IDP qui ne sont plus valides, vous devez utiliser un utilisateur non-IDP admin pour appeler la méthode API suivante : `UpdateIdpConfiguration`
- MFA est incompatible avec des certificats d’une longueur inférieure à 2048 bits. Par défaut un certificat SSL 2048 bits est créé sur le cluster. Évitez de définir un certificat de taille plus petite lors de l’appel de la méthode API : `SetSSLCertificate`

  Si le cluster utilise un certificat dont la pré-mise à niveau est inférieure à 2048 bits, le certificat du cluster doit être mis à jour avec un certificat de 2048 bits ou plus après la mise à niveau vers l’élément 12.0 ou version ultérieure.

- Les utilisateurs admin IDP ne peuvent pas être utilisés directement pour effectuer des appels d’API (par exemple, via des kits de développement logiciel ou Postman) ou pour d’autres intégrations (par exemple, OpenStack Cinder ou le plug-in vCenter). Ajoutez soit des utilisateurs d’administrateur de cluster LDAP, soit des utilisateurs d’administrateur de cluster local si vous avez besoin de créer des utilisateurs qui ont ces capacités.

Trouvez plus d’informations

- "Gestion du stockage avec l’API Element"
- "Page Ressources SolidFire et Element"
- "Plug-in NetApp Element pour vCenter Server"

Informations sur le copyright

Informations sur les marques commerciales