多要素認証を有効にします

Element Software

NetApp
January 15, 2024

目次

多要素認証を有効にします

多要素認証（ MFA ）では、 Security Assertion Markup Language （ SAML ）を使用してサードパーティのアイデンティティプロバイダ（ IdP ）を使用してユーザセッションを管理します。MFA を使用することで、管理者は、パスワードとテキストメッセージ、パスワードと E メールメッセージなど、必要に応じて認証のその他の要素を設定できます。

多要素認証をセットアップします

以下の Element API による基本的な手順を使用して、マルチファクタ認証を使用するようにクラスタをセットアップできます。

各 API メソッドの詳細については、を参照してください "Element API リファレンス"。

1. 次の API メソッドを呼び出し、 IdP メタデータを JSON 形式で渡して、クラスタの新しいサードパーティのアイデンティティプロバイダ（ IdP ）設定を作成します：「 CreateIdpConfiguration 」

   IdP メタデータはプレーンテキスト形式で、サードパーティの IdP から取得されます。このメタデータは、 JSON 形式で正しくフォーマットされるように検証する必要があります。使用できる JSON フォーマッタアプリケーションは多数あります。たとえば、 https://freeformatter.com/json-escape.html です。

2. 次の API メソッド「 ListIdpConfigurations 」を呼び出して、 spMetadataUrl を使用してクラスタメタデータを取得し、サードパーティ IdP にコピーします

   spMetadataUrl は、信頼関係を確立するために、 IdP のクラスタからサービスプロバイダのメタデータを取得するために使用する URL です。

3. 監査ログのユーザを一意に識別し、 Single Logout が適切に機能するように、サードパーティ IdP に SAML アサーションを設定して「 NameID 」属性を含めます。
4. 次の API メソッド「 AddIdpClusterAdmin 」を呼び出して、サードパーティ IdP によって認証された 1 つ以上のクラスタ管理者ユーザアカウントを作成します

   次の例に示すように、 IdP クラスタ管理者のユーザ名が、目的の効果の SAML 属性の名前 / 値のマッピングと一致している必要があります。

   - EMAIL=bob@company.com — SAML 属性の電子メールアドレスを解放するように IdP を設定します。
   - Group = cluster-administrator - すべてのユーザがアクセスできるグループプロパティを解放するように IdP が設定されている場合SAML 属性の名前と値のペアは、セキュリティ上の理由から大文字と小文字が区別されることに注意してください。
5. 次の API メソッドを呼び出して、クラスタに対して MFA を有効にします。 'EnableIdpAuthentication'

詳細については、こちらをご覧ください

- "SolidFire および Element ソフトウェアのドキュメント"
- "vCenter Server 向け NetApp Element プラグイン"

多要素認証のための追加情報

多要素認証については、次の点に注意してください。

- 有効ではなくなった IdP 証明書を更新するには、 IdP 以外の管理者ユーザを使用して次の API メソッド「 UpdateIdpConfiguration 」を呼び出す必要があります
- MFA は、 2048 ビット未満の長さの証明書と互換性がありません。デフォルトでは、クラスタ上に 2 、 048 ビット SSL 証明書が作成されます。API メソッド「 SSL 証明書」を呼び出すときは、小さいサイズの証明書を設定しないでください

> アップグレード前に 2048 ビット未満の証明書をクラスタが使用している場合は、 Element 12.0 以降にアップグレードしたあとに、クラスタ証明書を 2048 ビット以上の証明書で更新する必要があります。

- IDP 管理者ユーザは、 API 呼び出しを直接実行する（ SDK や Postman などで）ことも、他の統合機能（ OpenStack Cinder や vCenter Plug-in など）で使用することもできません。これらの機能を持つユーザを作成する必要がある場合は、 LDAP クラスタ管理者ユーザまたはローカルクラスタ管理者ユーザを追加します。

詳細については、こちらをご覧ください

- "Element API を使用してストレージを管理する"
- "SolidFire および Element ソフトウェアのドキュメント"
- "vCenter Server 向け NetApp Element プラグイン"

著作権に関する情報

商標に関する情報