多要素認証を有効にする
Element Software

NetApp
November 12, 2025

目次

多要素認証を有効にする

多要素認証を設定する

多要素認証 (MFA) は、セキュリティアサーションマークアップ言語 (SAML) を介してサードパーティの ID プロバイダー (IdP) を使用してユーザーセッションを管理します。MFA を使用すると、管理者は必要に応じて、パスワードとテキスト メッセージ、パスワードと電子メール メッセージなどの追加の認証要素を構成できます。

Element API 経由でこれらの基本的な手順を使用して、多要素認証を使用するようにクラスターを設定できます。

各APIメソッドの詳細については、 "要素APIリファレンス"。

1. 次の API メソッドを呼び出して、IdP メタデータを JSON 形式で渡すことで、クラスターの新しいサードパーティ ID プロバイダー (IdP) 構成を作成します。 `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 で正しくフォーマットされていることを確認するため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数多くあります。例えば、次のとおりです。https://freeformatter.com/json-escape.html.

2. 次の API メソッドを呼び出して、spMetadataUrl を介してクラスター メタデータを取得し、サードパーティの IdP にコピーします。 `ListIdpConfigurations`

   spMetadataUrl は、信頼関係を確立するために IdP のクラスターからサービス プロバイダー メタデータを取得するために使用される URL です。

3. 監査ログとシングル ログアウトが適切に機能するために、ユーザーを一意に識別するための “NameID” 属性を含めるようにサードパーティの IdP で SAML アサーションを構成します。
4. 次の API メソッドを呼び出して、承認のためにサードパーティの IdP によって認証された 1 つ以上のクラスター管理者ユーザー アカウントを作成します。`AddIdpClusterAdmin`

   > ⓘ 次の例に示すように、目的の効果を得るには、IdP クラスタ管理者のユーザー名が SAML 属性の名前/値のマッピングと一致する必要があります。

   - email=bob@company.com - ここで、IdP は SAML 属性で電子メール アドレスを解放するように構成されています。
   - group=cluster-administrator - ここで、IdP は、すべてのユーザー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構成されます。セキュリティ上の理由から、SAML 属性の名前と値のペアでは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、クラスターの MFA を有効にします。 `EnableIdpAuthentication`

詳細情報の参照

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

多要素認証に関する追加情報

多要素認証に関しては、次の注意事項に注意する必要があります。

- 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ーを使用して次の API メソッドを呼び出す必要があります。 `UpdateIdpConfiguration`
- MFA は、長さが 2048 ビット未満の証明書とは互換性がありません。デフォルトでは、クラスター上に 2048 ビットの SSL 証明書が作成されます。 API メソッドを呼び出すときは、小さいサイズの証明書の設定を避ける必要があります。 `SetSSLCertificate`

> アップグレード前にクラスターが 2048 ビット未満の証明書を使用している場合は、Element 12.0 以降にアップグレードした後、クラスター証明書を 2048 ビット以上の証明書に更新する必要があります。

- IdP 管理ユーザーは、API 呼び出しを直接行うために使用することはできません (たとえば、SDK または Postman 経由)。また、他の統合 (たとえば、OpenStack Cinder または vCenter プラグイン) に使用することもできません。これらの権限を持つユーザーを作成する必要がある場合は、LDAP クラスター管理者ユーザーまたはローカル クラスター管理者ユーザーのいずれかを追加します。

詳細情報の参照

- "Element API によるストレージの管理"
- "SolidFireおよびElementソフトウェアのドキュメント"
- "vCenter Server 用NetApp Elementプラグイン"

著作権に関する情報

商標に関する情報