多要素認証を有効にします

Element Software

NetApp
November 19, 2025

This PDF was generated from https://docs.netapp.com/ja-jp/element-software-123/storage/task_system_manage_mfa_set_up_multi_factor_authentication.html on November 19, 2025. Always check docs.netapp.com for the latest.

目次

多要素認証を有効にします 1
多要素認証をセットアップします 1
詳細については、こちらをご覧ください 1
多要素認証のための追加情報 2
詳細については、こちらをご覧ください 2

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

Copyright © 2025 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用権を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用権については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、http://www.netapp.com/TMに記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。