



多要素認証 API メソッド

Element Software

NetApp
January 15, 2024

目次

多要素認証 API メソッド	1
詳細については、こちらをご覧ください	1
AddIpdClusterAdmin	1
CreateIpdConfiguration を実行します	3
DeleteAuthSession の略	5
DeleteAuthSessionsByClusterAdmin	7
DeleteAuthSessionsByUsername のように入力します	8
DeleteIpdConfiguration	10
DisableIpdAuthentication の略	12
EnableIpdAuthentication の略	12
GetIpdAuthenticationState のこと	14
ListActiveAuthSessions を参照してください	15
ListIpdConfigurations の例を次に示します	16
UpdateIpdConfiguration	18

多要素認証 API メソッド

多要素認証（MFA）を使用して、Security Assertion Markup Language（SAML）を介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できます。

- [AddIdpClusterAdmin](#)
- [CreateIdpConfiguration](#) を実行します
- [DeleteAuthSession](#) の略
- [DeleteAuthSessionsByClusterAdmin](#)
- [DeleteAuthSessionsByUsername](#) のように入力します
- [DeleteIdpConfiguration](#)
- [DisableIdpAuthentication](#) の略
- [EnableIdpAuthentication](#) の略
- [GetIdpAuthenticationState](#) のこと
- [ListActiveAuthSessions](#) を参照してください
- [ListIdpConfigurations](#) の例を次に示します
- [UpdateIdpConfiguration](#)

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"](#)
- ["以前のバージョンの NetApp SolidFire 製品および Element 製品に関するドキュメント"](#)

AddIdpClusterAdmin

「AddIdpClusterAdmin」メソッドを使用して、サードパーティのアイデンティティプロバイダ（IdP）によって認証されたクラスタ管理者ユーザを追加できます。IdP クラスタ管理者アカウントは、ユーザに関連付けられた IdP の SAML アサーションで指定された SAML の属性と値の情報に基づいて設定されます。ユーザが IdP で認証され、複数の IdP クラスタ管理アカウントに一致する SAML アサーション内に SAML 属性ステートメントが含まれている場合、そのユーザは一致する IdP クラスタ管理アカウントのアクセスレベルを組み合わせ使用できます。

パラメータ

このメソッドの入力パラメータは次のとおりです。

名前	説明	を入力します	デフォルト値	必須
にアクセスします	この IdP クラスタ管理者が使用できるメソッドを制御します。	文字列の配列	なし	はい。
アクセトウーラ	エンドユーザライセンス契約に同意します。システムにクラスタ管理者アカウントを追加するには、true に設定します。省略するか false に設定すると、メソッド呼び出しは失敗します。	ブール値	なし	はい。
属性 (Attributes)	JSON オブジェクト形式の名前と値のペアのリスト。	JSON オブジェクト	なし	いいえ
ユーザ名	IdP クラスタ管理者への SAML の属性と値のマッピング (例: email=test@example.com)。これは、「NameID」を使用して特定の SAML サブジェクトを使用するか、「eduPersonアフィリーション」などの SAML 属性ステートメントのエントリとして定義できます。	文字列	なし	はい。

戻り値

このメソッドの戻り値は次のとおりです。

名前	説明	を入力します
clusterAdminID	作成されたクラスタ管理者の一意の識別子。	整数

要求例

このメソッドの要求例を次に示します。

```
{
  "method": "AddIdpClusterAdmin",
  "params": {
    "username": "email=test@example.com",
    "acceptEula": true,
    "access": ["administrator"]
  }
}
```

応答例

このメソッドの応答例を次に示します。

```
{
  "result": {
    "clusterAdminID": 13
  }
}
```

新規導入バージョン

12.0

CreateldpConfiguration を実行します

「CreateldpConfiguration」メソッドを使用すると、クラスタにサードパーティのアイデンティティプロバイダ（IdP）を使用して認証の信頼関係を作成できます。IdP 通信には SAML サービスプロバイダ証明書が必要です。この証明書は必要に応じて生成され、この API 呼び出しで返されます。

パラメータ

このメソッドの入力パラメータは次のとおりです。

名前	説明	を入力します	デフォルト値	必須
idpMetadata のことです	保存する IdP メタデータ。	文字列	なし	はい。
idpName	SAML 2.0 シングルサインオンの IdP プロバイダを識別するための名前。	文字列	なし	はい。

戻り値

このメソッドの戻り値は次のとおりです。

名前	説明	を入力します
idpConfigInfo	サードパーティのアイデンティティプロバイダ (IdP) の設定に関する情報。	"idpConfigInfo"

要求例

このメソッドの要求例を次に示します。

```
{
  "method": "CreateIdpConfiguration",
  "params": {
    "idpMetadata": "<?xml version=\"1.0\" encoding=\"UTF-8\"?>
      <EntityDescriptor
        xmlns=\"urn:oasis:names:tc:SAML:2.0:metadata\"
        xmlns:ds=\"http://www.w3.org/2000/09/xmldsig#\"
        xmlns:shibmd=\"urn:mace:shibboleth:metadata:1.0\"
        xmlns:xml=\"http://www.w3.org/XML/1998/namespace\"
        ...</Organization>
      </EntityDescriptor>",
    "idpName": "https://provider.name.url.com"
  },
}
```

応答例

このメソッドの応答例を次に示します。

```

{
  "result": {
    "idpConfigInfo": {
      "enabled": false,
      "idpConfigurationID": "f983c602-12f9-4c67-b214-bf505185cfed",
      "idpMetadata": "<?xml version=\"1.0\" encoding=\"UTF-8\"?>\r\n
<EntityDescriptor
xmlns=\"urn:oasis:names:tc:SAML:2.0:metadata\"\r\n
xmlns:ds=\"http://www.w3.org/2000/09/xmldsig#\"\r\n
xmlns:shibmd=\"urn:mace:shibboleth:metadata:1.0\"\r\n
xmlns:xml=\"http://www.w3.org/XML/1998/namespace\"\r\n
... </Organization>\r\n
</EntityDescriptor>",
      "idpName": "https://priver.name.url.com",
      "serviceProviderCertificate": "-----BEGIN CERTIFICATE-----\n
MIID...SlBHi\n
-----END CERTIFICATE-----\n",
      "spMetadataUrl": "https://10.193.100.100/auth/ui/saml2"
    }
  }
}

```

新規導入バージョン

12.0

DeleteAuthSession の略

「DeleteAuthSession」メソッドを使用して、個々のユーザ認証セッションを削除できます。呼び出し元のユーザが ClusterAdmins/Administrator AccessGroup にない場合は、呼び出し元のユーザに属する認証セッションだけを削除できます。

パラメータ

このメソッドの入力パラメータは次のとおりです。

名前	説明	を入力します	デフォルト値	必須
SessionID	削除する認証セッションの一意的識別子。	UUID	なし	はい。

戻り値

このメソッドの戻り値は次のとおりです。

名前	説明	を入力します
セッション	削除認証セッションのセッション情報。	"authSessionInfo"

要求例

このメソッドの要求例を次に示します。

```
{
  "method": "DeleteAuthSession",
  "params": {
    "sessionID": "a862a8bb-2c5b-4774-a592-2148e2304713"
  },
  "id": 1
}
```

応答例

このメソッドの応答例を次に示します。

```
{
  "id": 1,
  "result": {
    "session": {
      "accessGroupList": [
        "administrator"
      ],
      "authMethod": "Cluster",
      "clusterAdminIDs": [
        1
      ],
      "finalTimeout": "2020-04-09T17:51:30Z",
      "idpConfigVersion": 0,
      "lastAccessTimeout": "2020-04-06T18:21:33Z",
      "sessionCreationTime": "2020-04-06T17:51:30Z",
      "sessionID": "a862a8bb-2c5b-4774-a592-2148e2304713",
      "username": "admin"
    }
  }
}
```


DeleteAuthSessionsByClusterAdmin

「DeleteAuthSessionsByClusterAdmin」メソッドを使用すると、指定した「ClusterAdminID」に関連付けられているすべての認証セッションを削除できます。指定したClusterAdminIDがユーザのグループにマッピングされている場合、そのグループのすべてのメンバーのすべての認証セッションが削除されます。削除可能なセッションのリストを表示するには'ClusterAdminID'パラメータを指定してListAuthSessionsByClusterAdminメソッドを使用します

パラメータ

このメソッドの入力パラメータは次のとおりです。

名前	説明	を入力します	デフォルト値	必須
clusterAdminID	クラスタ管理者の一意の識別子。	整数	なし	はい。

戻り値

このメソッドの戻り値は次のとおりです。

名前	説明	を入力します
セッション	削除された認証セッションのセッション情報。	"authSessionInfo"

要求例

このメソッドの要求例を次に示します。

```
{
  "method": "DeleteAuthSessionsByClusterAdmin",
  "params": {
    "clusterAdminID": 1
  }
}
```

応答例

このメソッドの応答例を次に示します。

```
{
  "sessions": [
    {
      "accessGroupList": [
        "administrator"
      ],
      "authMethod": "Cluster",
      "clusterAdminIDs": [
        1
      ],
      "finalTimeout": "2020-03-14T19:21:24Z",
      "idpConfigVersion": 0,
      "lastAccessTimeout": "2020-03-11T19:51:24Z",
      "sessionCreationTime": "2020-03-11T19:21:24Z",
      "sessionID": "b12bfc64-f233-44df-8b9f-6fb6c011abf7",
      "username": "admin"
    }
  ]
}
```

新規導入バージョン

12.0

DeleteAuthSessionsByUsername のように入力します

「deleteAuthSessionsByUsername」メソッドを使用して、特定のユーザのすべての認証セッションを削除できます。AccessGroup ClusterAdmins/Administrator がない発信者は、自身のセッションだけを削除できます。ClusterAdmins/Administrator 権限を持つ呼び出し側は、任意のユーザに属するセッションを削除できます。削除可能なセッションのリストを表示するには、同じパラメータで「ListAuthSessionsByUsername」を使用します。削除可能なセッションのリストを表示するには '同じパラメータを持つ ListAuthSessionsByUsername メソッドを使用します

パラメータ

このメソッドの入力パラメータは次のとおりです。

名前	説明	を入力します	デフォルト値	必須
使用します	<p>削除するユーザセッションの認証方式を指定します。このパラメータを指定できるのは、ClusterAdmins または Administrator AccessGroup 内の呼び出し元だけです。有効な値は次のとおりです。</p> <ul style="list-style-type: none"> • authMethod=Cluster は、ClusterAdmin ユーザ名を指定します。 • authMethod=LDAP には、ユーザの LDAP DN を指定します。 • * authMethod=IDP * には、ユーザの IdP UUID または NameID を指定します。どちらのオプションも返すように IdP が設定されていない場合は、セッションの作成時に発行されたランダム UUID を指定します。 	使用します	なし	いいえ
ユーザ名	ユーザの一意の識別子。	文字列	なし	いいえ

戻り値

このメソッドの戻り値は次のとおりです。

名前	説明	を入力します
セッション	削除された認証セッションのセッション情報。	"authSessionInfo"

要求例

このメソッドの要求例を次に示します。

```
{
  "method": "DeleteAuthSessionsByUsername",
  "params": {
    "authMethod": "Cluster",
    "username": "admin"
  }
}
```

応答例

このメソッドの応答例を次に示します。

```
{
  "sessions": [
    {
      "accessGroupList": [
        "administrator"
      ],
      "authMethod": "Cluster",
      "clusterAdminIDs": [
        1
      ],
      "finalTimeout": "2020-03-14T19:21:24Z",
      "idpConfigVersion": 0,
      "lastAccessTimeout": "2020-03-11T19:51:24Z",
      "sessionCreationTime": "2020-03-11T19:21:24Z",
      "sessionID": "b12bfc64-f233-44df-8b9f-6fb6c011abf7",
      "username": "admin"
    }
  ]
}
```

新規導入バージョン

12.0

DeleteldpConfiguration

「\[\\"leetldpConfiguration\"] メソッドを使用すると、クラスタのサードパーティ IdP の既存の設定を削除できます。最後の IdP 設定を削除すると、SAML サービスプロバイダ

証明書がクラスタから削除されます。

パラメータ

このメソッドの入力パラメータは次のとおりです。

名前	説明	を入力します	デフォルト値	必須
idpConfigurationID	サードパーティ IdP 設定の UUID。	UUID	なし	いいえ
idpName	SAML 2.0 シングルサインオンの IdP プロバイダを識別して取得するための名前。	文字列	なし	いいえ

戻り値

このメソッドには戻り値はありません。

要求例

このメソッドの要求例を次に示します。

```
{
  "method": "DeleteIdpConfiguration",
  "params": {
    "idpConfigurationID": "f983c602-12f9-4c67-b214-bf505185cfed",
    "idpName": "https://provider.name.url.com"
  }
}
```

応答例

このメソッドの応答例を次に示します。

```
{
  "result": {}
}
```

新規導入バージョン

12.0

DisableIdpAuthentication の略

「DisableIdpAuthentication」メソッドを使用すると、クラスタでサードパーティ IdP を使用した認証のサポートを無効にできます。無効にすると、サードパーティの IdP によって認証されたユーザはクラスタにアクセスできなくなり、アクティブな認証済みセッションは無効になるか切断されます。LDAP 管理者およびクラスタ管理者は、サポートされている UI からクラスタにアクセスできます。

パラメータ

このメソッドには入力パラメータはありません。

戻り値

このメソッドには戻り値はありません。

要求例

このメソッドの要求例を次に示します。

```
{
  "method": "DisableIdpAuthentication",
  "params": {}
}
```

応答例

このメソッドの応答例を次に示します。

```
{
  "result": {}
}
```

新規導入バージョン

12.0

EnableIdpAuthentication の略

「EnableIdpAuthentication」メソッドを使用すると、クラスタにサードパーティの IdP を使用した認証のサポートを有効にできます。IdP 認証を有効にすると、LDAP 管理者およびクラスタ管理者は、サポートされている UI からクラスタにアクセスできなくなり、アクティブな認証されたセッションが無効化 / 切断されます。サポートされている

UI からクラスタにアクセスできるのは、サードパーティの IdP で認証されたユーザだけです。

パラメータ

このメソッドの入力パラメータは次のとおりです。

名前	説明	を入力します	デフォルト値	必須
idpConfigurationID	サードパーティ IdP 設定の UUID。IdP 設定が 1 つしかない場合は、その設定がデフォルトで有効になります。IDpConfiguration が 1 つしかない場合は、idpConfigurationID パラメータを指定する必要はありません。	UUID	なし	いいえ

戻り値

このメソッドには戻り値はありません。

要求例

このメソッドの要求例を次に示します。

```
{
  "method": "EnableIdpAuthentication",
  "params": {
    "idpConfigurationID": "f983c602-12f9-4c67-b214-bf505185cfed",
  }
}
```

応答例

このメソッドの応答例を次に示します。

```
{
  "result": {}
}
```

新規導入バージョン

12.0

GetIdpAuthenticationState のこと

「GetIdpAuthenticationState」メソッドを使用すると、サードパーティ IdP を使用した認証の状態に関する情報を返すことができます。

パラメータ

このメソッドには入力パラメータはありません。

戻り値

このメソッドの戻り値は次のとおりです。

名前	説明	を入力します
有効	サードパーティの IdP 認証が有効になっているかどうかを示します。	ブール値

要求例

このメソッドの要求例を次に示します。

```
{
  "method": "GetIdpAuthenticationState"
}
```

応答例

このメソッドの応答例を次に示します。

```
{
  "result": {"enabled": true}
}
```

新規導入バージョン

12.0

ListActiveAuthSessions を参照してください

「ListActiveAuthSessions」メソッドを使用して、アクティブな認証済みセッションをすべて一覧表示できます。このメソッドを呼び出すことができるのは、管理者アクセス権を持つユーザーだけです。

パラメータ

このメソッドには入力パラメータはありません。

戻り値

このメソッドの戻り値は次のとおりです。

名前	説明	を入力します
セッション	認証セッションのセッション情報。	"authSessionInfo"

要求例

このメソッドの要求例を次に示します。

```
{
  "method": "ListActiveAuthSessions"
}
```

応答例

このメソッドの応答例を次に示します。

```

{
  "sessions": [
    {
      "accessGroupList": [
        "administrator"
      ],
      "authMethod": "Cluster",
      "clusterAdminIDs": [
        1
      ],
      "finalTimeout": "2020-03-14T19:21:24Z",
      "idpConfigVersion": 0,
      "lastAccessTimeout": "2020-03-11T19:51:24Z",
      "sessionCreationTime": "2020-03-11T19:21:24Z",
      "sessionID": "b12bfc64-f233-44df-8b9f-6fb6c011abf7",
      "username": "admin"
    }
  ]
}

```

新規導入バージョン

12.0

ListIdpConfigurations の例を次に示します

「ListIdpConfigurations」メソッドを使用すると、サードパーティ製 IdP の設定を一覧表示できます。必要に応じて、「enabledOnly」フラグを指定して現在有効になっている IdP 設定を取得したり、IdP メタデータ UUID または IdP 名を指定して特定の IdP 設定の情報を照会したりできます。

パラメータ

このメソッドの入力パラメータは次のとおりです。

名前	説明	を入力します	デフォルト値	必須
enabledOnly を有効にします	結果をフィルタして、現在有効な IdP 設定を返します。	ブール値	なし	いいえ
idpConfigurationID	サードパーティ IdP 設定の UUID。	UUID	なし	いいえ

名前	説明	を入力します	デフォルト値	必須
idpName	特定の IdP 名の IdP 設定情報を取得します。	文字列	なし	いいえ

戻り値

このメソッドの戻り値は次のとおりです。

名前	説明	を入力します
idpConfigInfos	サードパーティの IdP 設定に関する情報。	"idpConfigInfo" 配列

要求例

このメソッドの要求例を次に示します。

```
{
  "method": "ListIdpConfigurations",
  "params": {}
}
```

応答例

このメソッドの応答例を次に示します。

```

{
  "result": {
    "idpConfigInfo": {
      "enabled": true,
      "idpConfigurationID": "f983c602-12f9-4c67-b214-bf505185cfed",
      "idpMetadata": "<?xml version=\"1.0\" encoding=\"UTF-8\"?>\r\n
<EntityDescriptor
xmlns=\"urn:oasis:names:tc:SAML:2.0:metadata\"\r\n
xmlns:ds=\"http://www.w3.org/2000/09/xmldsig#\"\r\n
xmlns:shibmd=\"urn:mace:shibboleth:metadata:1.0\"\r\n
xmlns:xml=\"http://www.w3.org/XML/1998/namespace\"\r\n
...</Organization>\r\n
</EntityDescriptor>",
      "idpName": "https://priver.name.url.com",
      "serviceProviderCertificate": "-----BEGIN CERTIFICATE-----\n
MI...BHi\n
-----END CERTIFICATE-----\n",
      "spMetadataUrl": "https://10.193.100.100/auth/ui/saml2"
    }
  }
}

```

新規導入バージョン

12.0

UpdateIdpConfiguration

「UpdateIdpConfiguration」メソッドを使用すると、クラスタの既存の構成をサードパーティ IdP で更新できます。

パラメータ

このメソッドの入力パラメータは次のとおりです。

名前	説明	を入力します	デフォルト値	必須
GenerateNewCertificate	true を指定すると、新しい SAML キーと証明書が生成されて既存のペアが置き換えられます。メモ：既存の証明書を交換すると、IdP でクラスタのサービスプロバイダメタデータがリロードされるまで、クラスタと IdP 間の確立された信頼が損なわれます。指定しない場合や false に設定した場合、SAML 証明書とキーは変更されません。	ブール値	なし	いいえ
idpConfigurationID	サードパーティ IdP 設定の UUID。	UUID	なし	いいえ
idpMetadata のことです	SAML 2.0 シングルサインオンの設定および統合の詳細用の IdP メタデータ。	文字列	なし	いいえ
idpName	SAML 2.0 シングルサインオンの IdP プロバイダを識別して取得するための名前。	文字列	なし	いいえ
newIdpName の略	この名前を指定すると、古い IdP 名が置き換えられます。	文字列	なし	いいえ

戻り値

このメソッドの戻り値は次のとおりです。

名前	説明	を入力します
idpConfigInfo	サードパーティ IdP 設定に関する情報。	"idpConfigInfo"

要求例

このメソッドの要求例を次に示します。

```
{
  "method": "UpdateIdpConfiguration",
  "params": {
    "idpConfigurationID": "f983c602-12f9-4c67-b214-bf505185cfed",
    "generateNewCertificate": true
  }
}
```

応答例

このメソッドの応答例を次に示します。

```
{
  "result": {
    "idpConfigInfo": {
      "enabled": true,
      "idpConfigurationID": "f983c602-12f9-4c67-b214-bf505185cfed",
      "idpMetadata": "<?xml version=\"1.0\" encoding=\"UTF-8\"?>\r\n
<EntityDescriptor
xmlns=\"urn:oasis:names:tc:SAML:2.0:metadata\"\r\n
xmlns:ds=\"http://www.w3.org/2000/09/xmldsig#\"\r\n
xmlns:shibmd=\"urn:mace:shibboleth:metadata:1.0\"\r\n
xmlns:xml=\"http://www.w3.org/XML/1998/namespace\"\r\n
...</Organization>\r\n
</EntityDescriptor>",
      "idpName": "https://priver.name.url.com",
      "serviceProviderCertificate": "-----BEGIN CERTIFICATE-----\n
MI...BHi\n
-----END CERTIFICATE-----\n",
      "spMetadataUrl": "https://10.193.100.100/auth/ui/saml2"
    }
  }
}
```

新規導入バージョン

12.0

著作権に関する情報

Copyright © 2024 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权を有し、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权については、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。