



多因素身份验证 **API** 方法

Element Software

NetApp
October 01, 2024

目录

多因素身份验证 API 方法	1
了解更多信息	1
AddIdpClusterAdmin	1
CreateIdpConfiguration	3
DeleteAuthSession	5
DeleteAuthSessionsByClusterAdmin	6
DeleteAuthSessionsByUsername	8
DeleteIdpConfiguration	10
DisableIdpAuthentication	11
EnableIdpAuthentication	11
GetIdpAuthenticationState	13
ListActiveAuthSessions	13
ListIdpConfigurations	15
UpdateIdpConfiguration	16

多因素身份验证 API 方法

您可以使用多因素身份验证（Multi-Factor Authentication，MFA）通过安全断言标记语言（Security Assertion Markup Language，SAML）使用第三方身份提供程序（IdP）管理用户会话。

- [AddIdpClusterAdmin](#)
- [CreateIdpConfiguration](#)
- [DeleteAuthSession](#)
- [DeleteAuthSessionsByClusterAdmin](#)
- [DeleteAuthSessionsByUsername](#)
- [DeleteIdpConfiguration](#)
- [DisableIdpAuthentication](#)
- [EnableIdpAuthentication](#)
- [GetIdpAuthenticationState](#)
- [ListActiveAuthSessions](#)
- [ListIdpConfigurations](#)
- [UpdateIdpConfiguration](#)

了解更多信息

- ["SolidFire 和 Element 软件文档"](#)
- ["早期版本的 NetApp SolidFire 和 Element 产品的文档"](#)

AddIdpClusterAdmin

您可以使用 `AddIdpClusterAdmin` 方法添加通过第三方身份提供程序 (Identity Provider、Idp) 身份验证的集群管理员用户。IdP 集群管理员帐户是根据 IdP 与用户关联的 SAML 断言中提供的 SAML 属性值信息进行配置的。如果用户成功通过 IdP 身份验证，并且 SAML 断言中的 SAML 属性语句与多个 IdP 集群管理员帐户匹配，则用户将具有这些匹配的 IdP 集群管理员帐户的组合访问级别。

参数

此方法具有以下输入参数：

名称	说明	键入	默认值	必填
访问	控制此 IdP 集群管理员可以使用的方法。	string array	无	是

名称	说明	键入	默认值	必填
接受 Eula	接受最终用户许可协议。设置为 true 可向系统添加集群管理员帐户。如果省略或设置为 false，则方法调用将失败。	boolean	无	是
属性	名称 - 值对列表，采用 JSON 对象格式。	JSON 对象	无	否
用户名	映射到 IdP 集群管理员的 SAML 属性值（例如，EEmail=test@example.com）。可以使用特定的SAML主题进行定义，也可以在SAML属性语句中作为条目进行定义 NameID，例如 eduPersonAffiliation。	string	无	是

返回值

此方法具有以下返回值：

名称	说明	键入
clusterAdminID	新创建的集群管理员的唯一标识符。	整型

请求示例

此方法的请求类似于以下示例：

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

响应示例

此方法返回类似于以下示例的响应：

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

自版本以来的新增功能

12.0

CreateIdpConfiguration

您可以使用 `CreateIdpConfiguration` 方法通过第三方身份提供程序(Idp)为集群创建潜在的身份验证信任关系。IdP 通信需要 SAML 服务提供商证书。此证书将根据需要生成，并由此 API 调用返回。

参数

此方法具有以下输入参数：

名称	说明	键入	默认值	必填
idpMetadata	要存储的 IdP 元数据。	string	无	是
idpName	用于标识 SAML 2.0 单点登录的 IdP 提供程序的名称。	string	无	是

返回值

此方法具有以下返回值：

名称	说明	键入
idpConfigInfo	有关第三方身份提供程序 (IdP) 配置的信息。	"idpConfigInfo"

请求示例

此方法的请求类似于以下示例：

```

{
  "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"
  },
}

```

响应示例

此方法返回类似于以下示例的响应：

```

{
  "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://privider.name.url.com",
      "serviceProviderCertificate": "-----BEGIN CERTIFICATE-----\n
MIID...SlBHi\n
-----END CERTIFICATE-----\n",
      "spMetadataUrl": "https://10.193.100.100/auth/ui/saml2"
    }
  }
}

```

自版本以来的新增功能

12.0

DeleteAuthSession

您可以使用 `DeleteAuthSession` 方法删除单个用户身份验证会话。如果调用用户不在 ClusterAdmins/Administrator AccessGroup 中，则只能删除属于调用用户的身份验证会话。

参数

此方法具有以下输入参数：

名称	说明	键入	默认值	必填
会话ID	要删除的身份验证会话的唯一标识符。	UUID	无	是

返回值

此方法具有以下返回值：

名称	说明	键入
会话	删除身份验证会话的会话信息。	"authSessionInfo"

请求示例

此方法的请求类似于以下示例：

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

响应示例

此方法返回类似于以下示例的响应：

```

{
  "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"
    }
  }
}

```

自版本以来的新增功能

12.0

DeleteAuthSessionsByClusterAdmin

您可以使用 `DeleteAuthSessionsByClusterAdmin` 方法删除与指定关联的所有身份验证会话 `ClusterAdminID`。如果指定的 `ClusterAdminID` 映射到一组用户，则该组中所有成员的所有身份验证会话都将被删除。要查看可能删除的会话列表、请使用 `ListAuthSessionsByClusterAdmin` 方法和参数。 `ClusterAdminID`

参数

此方法具有以下输入参数：

名称	说明	键入	默认值	必填
clusterAdminID	集群管理员的唯一标识符。	整型	无	是

返回值

此方法具有以下返回值：

名称	说明	键入
会话	已删除身份验证会话的会话信息。	"authSessionInfo"

请求示例

此方法的请求类似于以下示例：

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

响应示例

此方法返回类似于以下示例的响应：

```
{
  "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"
    }
  ]
}
```

自版本以来的新增功能

12.0

DeleteAuthSessionsByUsername

您可以使用 `DeleteAuthSessionsByUsername` 方法删除给定用户的所有身份验证会话。不在访问组集群管理员 / 管理员中的调用方只能删除自己的会话。具有 ClusterAdmins/Administrator 权限的调用程序可以删除属于任何用户的会话。要查看可删除的会话列表、请使用 `ListAuthSessionsByUsername` 相同的参数。要查看可能删除的会话列表、请使用 `ListAuthSessionsByUsername` 具有相同参数的方法。

参数

此方法具有以下输入参数：

名称	说明	键入	默认值	必填
authMethod	要删除的用户会话的身份验证方法。只有 ClusterAdmins/Administrator AccessGroup 中的调用程序才能提供此参数。可能值包括： <ul style="list-style-type: none">* authMethod=Cluster* 指定 ClusterAdmin 用户名。* authMethod=ldap* 用于指定用户的 LDAP DN。* authMethod=ldp* 指定用户的 IdP UUID 或 NameID。如果 IdP 未配置为返回任一选项，则此选项将指定创建会话时发出的随机 UUID。	authMethod	无	否
用户名	用户的唯一标识符。	string	无	否

返回值

此方法具有以下返回值：

名称	说明	键入
----	----	----

会话	已删除身份验证会话的会话信息。	"authSessionInfo"
----	-----------------	-----------------------------------

请求示例

此方法的请求类似于以下示例：

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

响应示例

此方法返回类似于以下示例的响应：

```
{
  "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"
    }
  ]
}
```

自版本以来的新增功能

12.0

DeleteIdpConfiguration

您可以使用 `DeleteIdpConfiguration` 方法删除集群的第三方 IdP 的现有配置。删除最后一个 IdP 配置会从集群中删除 SAML 服务提供程序证书。

参数

此方法具有以下输入参数：

名称	说明	键入	默认值	必填
idpConfigurationID	第三方 IdP 配置的 UUID 。	UUID	无	否
idpName	用于标识和检索 SAML 2.0 单点登录的 IdP 提供程序的名称。	string	无	否

返回值

此方法没有返回值。

请求示例

此方法的请求类似于以下示例：

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

响应示例

此方法返回类似于以下示例的响应：

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

自版本以来的新增功能

12.0

DisableIdpAuthentication

您可以使用 `DisableIdpAuthentication` 方法禁用对集群使用第三方IDP进行身份验证的支持。禁用后，经过第三方 IdP 身份验证的用户将无法再访问集群，并且任何经过身份验证的活动会话都将失效 / 断开连接。LDAP 和集群管理员可以通过支持的 UI 访问集群。

参数

此方法没有输入参数。

返回值

此方法没有返回值。

请求示例

此方法的请求类似于以下示例：

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

响应示例

此方法返回类似于以下示例的响应：

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

自版本以来的新增功能

12.0

EnableIdpAuthentication

您可以使用 `EnableIdpAuthentication` 方法为集群启用对使用第三方IDP的身份验证的支持。启用 IdP 身份验证后，LDAP 和集群管理员将无法再通过支持的 UI 访问集群，并且任何经过身份验证的活动会话都将失效 / 断开连接。只有经过第三方 IdP 身份验证的用户

才能通过受支持的 UI 访问集群。

参数

此方法具有以下输入参数：

名称	说明	键入	默认值	必填
idpConfigurationID	第三方 IdP 配置的 UUID。如果仅存在一个 IdP 配置，则默认为启用此配置。如果只有一个 IdpConfiguration，则无需提供 idpConfigurationID 参数。	UUID	无	否

返回值

此方法没有返回值。

请求示例

此方法的请求类似于以下示例：

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

响应示例

此方法返回类似于以下示例的响应：

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

自版本以来的新增功能

12.0

GetIdpAuthenticationState

您可以使用 `GetIdpAuthenticationState` 方法返回有关使用第三方IDP进行身份验证的状态的信息。

参数

此方法没有输入参数。

返回值

此方法具有以下返回值：

名称	说明	键入
已启用	指示是否已启用第三方 IdP 身份验证。	boolean

请求示例

此方法的请求类似于以下示例：

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

响应示例

此方法返回类似于以下示例的响应：

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

自版本以来的新增功能

12.0

ListActiveAuthSessions

您可以使用 `ListActiveAuthSessions` 方法列出所有经过身份验证的活动会话。只有具有管理访问权限的用户才能调用此方法。

参数

此方法没有输入参数。

返回值

此方法具有以下返回值：

名称	说明	键入
会话	身份验证会话的会话信息。	<code>"authSessionInfo"</code>

请求示例

此方法的请求类似于以下示例：

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

响应示例

此方法返回类似于以下示例的响应：

```
{
  "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"
    }
  ]
}
```

自版本以来的新增功能

12.0

ListIdpConfigurations

您可以使用 `ListIdpConfigurations` 方法列出第三方IDP的配置。或者、您也可以提供用于检索当前已启用的Idp配置的标志、或者提供 `enabledOnly` Idp元数据UUID或Idp名称来查询特定Idp配置的信息。

参数

此方法具有以下输入参数：

名称	说明	键入	默认值	必填
enabledOnly	筛选结果以返回当前已启用的 IdP 配置。	boolean	无	否
idpConfigurationID	第三方 IdP 配置的 UUID 。	UUID	无	否
idpName	检索特定 IdP 名称的 IdP 配置信息。	string	无	否

返回值

此方法具有以下返回值：

名称	说明	键入
idpConfigInfo	有关第三方 IdP 配置的信息。	"idpConfigInfo"阵列

请求示例

此方法的请求类似于以下示例：

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

响应示例

此方法返回类似于以下示例的响应：

```

{
  "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"
    }
  }
}

```

自版本以来的新增功能

12.0

UpdateIdpConfiguration

您可以使用 `UpdateIdpConfiguration` 方法使用第三方Idp更新集群的现有配置。

参数

此方法具有以下输入参数：

名称	说明	键入	默认值	必填
生成 NewCertificate	如果指定为 true ，则会生成新的 SAML 密钥和证书并替换现有对。注意：替换现有证书将中断集群与 IdP 之间建立的信任，直到在 IdP 处重新加载集群的服务提供商元数据为止。如果未提供 SAML 证书和密钥或将其设置为 false ，则 SAML 证书和密钥保持不变。	boolean	无	否
idpConfigurationID	第三方 IdP 配置的 UUID 。	UUID	无	否
idpMetadata	用于获取 SAML 2.0 单点登录配置和集成详细信息的 IdP 元数据。	string	无	否
idpName	用于标识和检索 SAML 2.0 单点登录的 IdP 提供程序的名称。	string	无	否
newIdpName	如果指定此名称，则此名称将替换旧的 IdP 名称。	string	无	否

返回值

此方法具有以下返回值：

名称	说明	键入
idpConfigInfo	有关第三方 IdP 配置的信息。	"idpConfigInfo"

请求示例

此方法的请求类似于以下示例：

```

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

```

响应示例

此方法返回类似于以下示例的响应：

```

{
  "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://privider.name.url.com\",
      "serviceProviderCertificate": "-----BEGIN CERTIFICATE-----\n
MI...BHi\n
-----END CERTIFICATE-----\n\",
      "spMetadataUrl": "https://10.193.100.100/auth/ui/saml2"
    }
  }
}

```

自版本以来的新增功能

12.0

版权信息

版权所有 © 2024 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。