多因素身份验证 API 方法

Element Software

NetApp
January 15, 2024

目录

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 `AddIpdClusterAdmin` 方法添加经过第三方身份提供程序（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。

Parameters

此方法具有以下输入参数：

Name	Description	Type	默认值	Required
访问	控制此 IdP 集群管理员可以使用的方法。	string array	无	是的。

Name	Description	Type	默认值	Required
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	是的。
属性	名称 - 值对列表，采用 JSON 对象格式。	JSON 对象	无	否
username	映射到 IdP 集群管理员的 SAML 属性值（例如，EMail=test@example.com ）。这可以使用使用 `NameID` 的特定 SAML 主题进行定义，也可以作为 SAML 属性语句中的条目进行定义，例如 `eduPersonAffinor` 。	string	无	是的。

返回值

此方法具有以下返回值：

Name	Description	Type
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 `CreateIpdConfiguration` 方法为集群创建使用第三方身份提供程序（IdP）进行身份验证的潜在信任关系。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。

Parameters

此方法具有以下输入参数：

Name	Description	Type	默认值	Required
idpMetadata	要存储的 IdP 元数据。	string	无	是的。
idpName	用于标识 SAML 2.0 单点登录的 IdP 提供程序的名称。	string	无	是的。

返回值

此方法具有以下返回值：

Name	Description	Type
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 `DDeleteAuthSession` 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。

Parameters

此方法具有以下输入参数：

Name	Description	Type	默认值	Required
会话 ID	要删除的身份验证会话的唯一标识符。	UUID	无	是的。

返回值

此方法具有以下返回值：

Name	Description	Type
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 `DDeleteAuthSessionsByClusterAdmin` 方法删除与指定的 `ClusterAdminID` 关联的所有身份验证会话。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，请使用带有 `ClusterAdminID` 参数的 ListAuthSessionsByClusterAdmin 方法。

Parameters

此方法具有以下输入参数：

Name	Description	Type	默认值	Required
clusterAdminID	集群管理员的唯一标识符。	整型	无	是的。

返回值

此方法具有以下返回值：

Name	Description	Type
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 `DDeleteAuthSessionsByUsername` 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，请使用具有相同参数的 `ListAuthSessionsByUsername` 。要查看可能删除的会话列表，请使用具有相同参数的 `ListAuthSessionsByUsername` 方法。

Parameters

此方法具有以下输入参数：

Name	Description	Type	默认值	Required
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： • * authMethod=Cluster* 指定 ClusterAdmin 用户名。 • * authMethod=ldap* 用于指定用户的 LDAP DN 。 • * authMethod=Idp * 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
username	用户的唯一标识符。	string	无	否

返回值

此方法具有以下返回值：

Name	Description	Type

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 `DDeleteIdpConfiguration` 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。

Parameters

此方法具有以下输入参数：

Name	Description	Type	默认值	Required
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。

Parameters

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` 方法为集群启用使用第三方 IdP 进行身份验证的支持。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。

Parameters

此方法具有以下输入参数：

Name	Description	Type	默认值	Required
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 的身份验证状态的信息。

Parameters

此方法没有输入参数。

返回值

此方法具有以下返回值：

Name	Description	Type
enabled	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。

Parameters

此方法没有输入参数。

返回值

此方法具有以下返回值：

Name	Description	Type
会话	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": "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 `enabledOnly` 标志来检索当前启用的 IdP 配置，或者提供 IdP 元数据 UUID 或 IdP 名称来查询特定 IdP 配置的信息。

Parameters

此方法具有以下输入参数：

Name	Description	Type	默认值	Required
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：

Name	Description	Type
idpConfigInfo	有关第三方 IdP 配置的信息。	"idpConfigInfo" 数组

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://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

UpdateIdpConfiguration

您可以使用 `UpdateIdpConfiguration` 方法使用集群的第三方 IdP 更新现有配置。

Parameters

此方法具有以下输入参数：

Name	Description	Type	默认值	Required
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：

Name	Description	Type
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