多因素身份驗證 API 方法

Element Software

NetApp
November 12, 2025

This PDF was generated from https://docs.netapp.com/zh-tw/element-software-128/api/reference_element_api_addidpclusteradmin.html on November 12, 2025. Always check docs.netapp.com for the latest.

目錄

多因素身份驗證 API 方法

新增IDP叢集管理員

你可以使用 `AddIpdClusterAdmin`新增由第三方身分提供者 (IdP) 進行驗證的叢集管理員使用者的方法。 IdP 叢集管理員帳戶是根據 IdP 的 SAML 斷言中提供的與使用者關聯的 SAML 屬性值資訊進行配置的。如果使用者成功透過身分識別提供者 (IdP) 的驗證，且 SAML 斷言中的 SAML 屬性語句與多個 IdP 叢集管理員帳戶相符，則該使用者將擁有與這些相符的 IdP 叢集管理員帳戶的合併存取等級。

參數

此方法有以下輸入參數：

Name	描述	類型	預設值	必需的
使用權	控制此身分提供者群集管理員可以使用的方法。	字串數組	沒有任何	是的
接受最終用戶許可協議	接受最終用戶許可協議。設定為 true 可向系統中新增叢集管理員帳戶。如果省略或設為 false，則方法呼叫失敗。	布林值	沒有任何	是的
屬性	JSON 物件格式的名稱-值對清單。	JSON 物件	沒有任何	不
使用者名稱	將 SAML 屬性值對應到 IdP 叢集管理員（例如，email=test@example.com）。這可以透過使用特定的 SAML 主題來定義。 `NameID`或作為 `SAML` 屬性語句中的一個條目，例如 `eduPersonAffiliation`。	細繩	沒有任何	是的

傳回值

此方法傳回以下值：

Name	描述	類型
叢集管理員ID	新建立的叢集管理員的唯一識別碼。	整數

請求範例

該方法的請求類似於以下範例：

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

回應範例

此方法傳回類似以下範例的回應：

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

自版本以來的新版本

12.0

建立身分保護配置

你可以使用 `CreateIpdConfiguration`使用第三方身分提供者 (IdP) 為叢集建立潛在的身分驗證信任關係的方法。身分提供者 (IdP) 通訊需要 SAML 服務提供者憑證。此證書是按需生成的，並透過此 API 呼叫返回。

參數

此方法有以下輸入參數：

Name	描述	類型	預設值	必需的
idpMetadata	要儲存的身分提供者元資料。	細繩	沒有任何	是的
idpName	用於識別 SAML 2.0 單一登入的身分提供者的名稱。	細繩	沒有任何	是的

傳回值

此方法傳回以下值：

Name	描述	類型
idp配置訊息	第三方身分提供者 (IdP) 配置資訊。	"idp配置訊息"

請求範例

該方法的請求類似於以下範例：

```
{
    "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"
    },
}
```

回應範例

此方法傳回類似以下範例的回應：

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

自版本以來的新版本

12.0

刪除授權會話

你可以使用 `DeleteAuthSession`刪除單一使用者身份驗證會話的方法。如果呼叫使用者不在 ClusterAdmins / Administrator AccessGroup 中，則只能刪除屬於呼叫使用者的驗證工作階段。

參數

此方法具有以下輸入參數：

Name	描述	類型	預設值	必需的
會話ID	要刪除的身份驗證會話的唯一識別碼。	唯一識別符	沒有任何	是的

傳回值

此方法傳回以下值：

Name	描述	類型
會議	刪除身份驗證會話的會話資訊。	"authSessionInfo"

請求範例

該方法的請求類似於以下範例：

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

回應範例

此方法傳回類似以下範例的回應：

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

自版本以來的新版本

12.0

DeleteAuthSessionsByClusterAdmin

你可以使用 `DeleteAuthSessionsByClusterAdmin`刪除與指定會話關聯的所有驗證會話的方法 `ClusterAdminID`。如果指定的 ClusterAdminID 對應到一組用戶，則該群組所有成員的所有驗證工作階段都會被刪除。若要查看可能刪除的會話列表，請使用 ListAuthSessionsByClusterAdmin 方法。 `ClusterAdminID`範圍。

參數

此方法具有以下輸入參數：

Name	描述	類型	預設值	必需的
叢集管理員ID	群集管理員的唯一識別碼。	整數	沒有任何	是的

傳回值

此方法傳回以下值：

Name	描述	類型
會議	已刪除身份驗證會話的會話資訊。	"authSessionInfo"

請求範例

該方法的請求類似於以下範例：

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

回應範例

此方法傳回類似以下範例的回應：

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


自版本以來的新版本

12.0

按使用者名稱刪除身份驗證會話

你可以使用 `DeleteAuthSessionsByUsername`刪除給定使用者的所有身份驗證會話的方法。不在 AccessGroup ClusterAdmins/Administrator 中的呼叫者只能刪除自己的會話。擁有 ClusterAdmins/Administrator 權限的呼叫者可以刪除屬於任何使用者的會話。若要查看可以刪除的會話列表，請使用 `ListAuthSessionsByUsername`參數相同。若要查看可刪除的會話列表，請使用下列方法： `ListAuthSessionsByUsername`使用相同參數的方法。

參數

此方法有以下輸入參數：

Name	描述	類型	預設值	必需的
認證方法	要刪除的使用者會話的身份驗證方法。只有屬於 ClusterAdmins/Administrator AccessGroup 的呼叫者才能提供此參數。可能的值有： • **authMethod=Cluster** 指定叢集管理員使用者名稱。 • **authMethod=Ldap** 指定使用者的 LDAP DN。 • **authMethod=Idp** 指定使用者的 IdP UUID 或 NameID。如果 IdP 未配置為傳回任一選項，則此設定會指定在建立工作階段時所發出的隨機 UUID。	認證方法	沒有任何	不
使用者名稱	用戶的唯一識別碼。	細繩	沒有任何	不

傳回值

此方法傳回以下值：

Name	描述	類型
會議	已刪除身份驗證會話的會話資訊。	"authSessionInfo"

請求範例

該方法的請求類似於以下範例：

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

回應範例

此方法傳回類似以下範例的回應：

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

自版本以來的新版本

12.0

刪除Idp配置

你可以使用 `DeleteIdpConfiguration`刪除叢集中第三方身分提供者 (IdP) 的現有配置的方法。刪除最後一個 IdP 設定會從叢集中移除 SAML 服務提供者憑證。

參數

此方法有以下輸入參數：

Name	描述	類型	預設值	必需的
idp配置ID	由第三方身分提供者配置的 UUID。	唯一識別符	沒有任何	不
idpName	用於識別和檢索 SAML 2.0 單一登入的身份提供者的名稱。	細繩	沒有任何	不

傳回值

此方法沒有傳回值。

請求範例

該方法的請求類似於以下範例：

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

回應範例

此方法傳回類似以下範例的回應：

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

自版本以來的新版本

12.0

禁用身份提供者身份驗證

你可以使用 `DisableIdpAuthentication`停用叢集使用第三方身分提供者進行身分驗證支援

的方法。一旦停用，透過第三方身分提供者 (IdP) 進行身份驗證的使用者將無法再存取集群，並且任何活動的已驗證會話都將失效/斷開連接。 LDAP 和叢集管理員可以透過支援的使用者介面存取叢集。

參數

此方法沒有輸入參數。

傳回值

此方法沒有傳回值。

請求範例

該方法的請求類似於以下範例：

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

回應範例

此方法傳回類似以下範例的回應：

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

自版本以來的新版本

12.0

啟用身份提供者身份驗證

你可以使用 `EnableIdpAuthentication`啟用對叢集使用第三方身分提供者進行身份驗證的支援的方法。啟用 IdP 身份驗證後，LDAP 和集群管理員將無法再透過受支援的 UI 存取集群，並且任何活動的已驗證會話都將失效/斷開連接。只有透過第三方身分提供者 (IdP) 認證的使用者才能透過支援的使用者介面存取叢集。

參數

此方法具有以下輸入參數：

Name	描述	類型	預設值	必需的
idp配置ID	由第三方身分提供者配置的 UUID。如果只有一個身分提供者配置，則預設啟用該配置。如果只有一個IdpConfiguration，則無需提供idpConfigurationID參數。	唯一識別符	沒有任何	不

傳回值

此方法沒有傳回值。

請求範例

該方法的請求類似於以下範例：

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

回應範例

此方法傳回類似以下範例的回應：

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

自版本以來的新版本

12.0

取得 IdP 驗證狀態

你可以使用 `GetIdpAuthenticationState`傳回有關使用第三方身分提供者進行身分驗證狀態的資訊的方法。

參數

此方法沒有輸入參數。

傳回值

此方法傳回以下值：

Name	描述	類型
已啟用	指示是否啟用第三方身分提供者身份驗證。	布林值

請求範例

該方法的請求類似於以下範例：

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

回應範例

此方法傳回類似以下範例的回應：

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

自版本以來的新版本

12.0

列出活動身份驗證會話

你可以使用 `ListActiveAuthSessions`列出所有已驗證的活動會話的方法。只有具有管理員權限的使用者才能呼叫此方法。

參數

此方法沒有輸入參數。

傳回值

此方法傳回以下值：

Name	描述	類型
會議	身份驗證會話的會話資訊。	"authSessionInfo"

請求範例

該方法的請求類似於以下範例：

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

回應範例

此方法傳回類似以下範例的回應：

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

自版本以來的新版本

12.0

列出 Idp 配置

你可以使用 `ListIdpConfigurations`列出第三方身分提供者配置的方法。您也可以選擇提供以下任一資訊： `enabledOnly`標誌用於擷取目前啟用的身分識別提供者 (IdP) 配置，或使用 IdP 元資料 UUID 或 IdP 名稱來查詢特定身分提供者 (IdP) 配置的資訊。

參數

此方法有以下輸入參數：

Name	描述	類型	預設值	必需的
僅啟用	篩選結果，傳回目前啟用的身分提供者配置。	布林值	沒有任何	不
idp配置ID	由第三方身分提供者配置的 UUID。	唯一識別符	沒有任何	不
idpName	取得指定身分提供者 (IdP) 名稱的身分提供者設定資訊。	細繩	沒有任何	不

傳回值

此方法傳回以下值：

Name	描述	類型
idp配置訊息	第三方身分提供者配置資訊。	"idp配置訊息"大批

請求範例

該方法的請求類似於以下範例：

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

回應範例

此方法傳回類似以下範例的回應：

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


自版本以來的新版本

12.0

更新Idp配置

你可以使用 `UpdateIdpConfiguration`使用第三方身分提供者 (IdP) 更新叢集現有配置的方法。

參數

此方法有以下輸入參數：

Name	描述	類型	預設值	必需的
產生新證書	如果指定為 true，則會產生新的 SAML 金鑰和證書，並取代現有的金鑰和證書對。注意：取代現有憑證將破壞叢集與身分提供者 (IdP) 之間已建立的信任關係，直到叢集的服務提供者元資料在身分提供者重新載入為止。如果未提供或設定為 false，則 SAML 憑證和金鑰保持不變。	布林值	沒有任何	不
idp配置ID	由第三方身分提供者配置的 UUID。	唯一識別符	沒有任何	不
idpMetadata	用於 SAML 2.0 單一登入的設定和整合詳細資訊的 IdP 元資料。	細繩	沒有任何	不
idpName	用於識別和檢索 SAML 2.0 單一登入的身份提供者的名稱。	細繩	沒有任何	不
新身分提供者名稱	如果指定，此名稱將取代舊的身分提供者名稱。	細繩	沒有任何	不

傳回值

此方法傳回以下值：

Name	描述	類型
idp配置訊息	有關第三方身分提供者配置的資訊。	"idp配置訊息"

請求範例

該方法的請求類似於以下範例：

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

回應範例

此方法傳回類似以下範例的回應：

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

自版本以來的新版本

12.0

版權資訊

Copyright © 2025 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變更本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。 美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 http://www.netapp.com/TM 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。