配置联合

NetApp Console setup and administration

NetApp
February 11, 2026

目录

配置联合 1
- 将NetApp Console与 Active Directory 联合服务 (AD FS) 联合起来 1
- 将NetApp Console与 Microsoft Entra ID 联合起来 2
- 使用 PingFederate 联合NetApp Console 4
- 与 SAML 身份提供商联合 5

配置联合

将NetApp Console与 Active Directory 联合服务 (AD FS) 联合起来

将您的 Active Directory 联合身份验证服务 (AD FS) 与NetApp Console联合起来，以便为NetApp Console启用单点登录 (SSO)。这允许用户使用他们的公司凭证登录控制台。

必需角色

需要联盟管理员角色来创建和管理联盟。联盟查看者可以查看联盟页面。"了解有关访问角色的更多信息。"

您可以与您的企业 IdP 或NetApp支持站点联合。 NetApp建议选择其中一个，但不要同时选择两者。

NetApp仅支持服务提供商发起的（SP发起的） SSO。首先，配置身份提供者以信任NetApp Console作为服务提供者。然后，使用您的身份提供商的配置在控制台中创建连接。

您可以与 AD FS 服务器建立联合，以启用NetApp Console的单点登录 (SSO)。该过程涉及配置您的 AD FS 以信任控制台作为服务提供商，然后在NetApp Console中创建连接。

步骤

1. 选择*管理>身份和访问*。
2. 选择“**Federation**”以查看“**Federations**”页面。
3. 选择*配置新联合*。
4. 输入您的域名详细信息：
   a. 选择您是否要使用已验证的域名或您的电子邮件域名。电子邮件域是与您登录的帐户关联的域。
   b. 输入您正在配置的联盟的名称。
   c. 如果您选择已验证的域，请从列表中选择该域。
5. 选择“下一步”。
6. 对于您的连接方法，选择*协议*，然后选择*Active Directory 联合身份验证服务 (AD FS)*。
7. 选择“下一步”。
8. 在您的 AD FS 服务器中创建依赖方信任。您可以使用 PowerShell 或在 AD FS 服务器上手动配置它。有关如何创建信赖方信任的详细信息，请参阅 AD FS 文档。
   a. 使用以下脚本通过 PowerShell 创建信任：

```
(new-object Net.WebClient -property @{Encoding = [Text.Encoding]
::UTF8}).DownloadString("https://raw.github.com/auth0/AD FS-
auth0/master/AD FS.ps1") | iex
AddRelyingParty "urn:auth0:netapp-cloud-account" "https://netapp-
cloud-account.auth0.com/login/callback"
```

b. 或者，您可以在 AD FS 管理控制台中手动创建信任。创建信任时使用以下NetApp Console值：

   - 创建依赖信任标识符时，使用 **YOUR_TENANT** 值： `netapp-cloud-account`
   - 当您选择 启用对 **WS-Federation** 的支持 时，请使用 **YOUR_AUTH0_DOMAIN** 值： `netapp-cloud-account.auth0.com`

c. 创建信任后，从 AD FS 服务器复制元数据 URL 或下载联合元数据文件。您需要此 URL 或文件来完成控制台中的连接。

NetApp建议使用元数据 URL 让NetApp Console自动检索最新的 AD FS 配置。如果您下载联合元数据文件，则每当 AD FS 配置发生更改时，都需要在NetApp Console中手动更新它。

9. 返回控制台，然后选择“下一步”来创建连接。
10. 创建与 AD FS 的连接。
    a. 输入您在上一步中从 AD FS 服务器复制的 **AD FS URL** 或上传您从 AD FS 服务器下载的联合元数据文件。
11. 选择*创建连接*。建立连接可能需要几秒钟。
12. 选择“下一步”。
13. 选择*测试连接*来测试您的连接。您将被引导至 IdP 服务器的登录页面。使用您的身份提供商凭据登录。登录后，返回控制台启用连接。

    在受限模式下使用控制台时，请将 URL 复制到隐身浏览器窗口或单独的浏览器中，以登录到您的身份提供商 (IdP)。

14. 在控制台中，选择“下一步”以查看摘要页面。
15. 设置通知。

    您可以选择七天或三十天。系统会通过电子邮件向具有以下角色的任何用户发送到期通知，并在控制台中显示这些通知：超级管理员、组织管理员、联盟管理员和联盟查看者。

16. 查看联盟详细信息，然后选择“启用联盟”。
17. 选择“完成”以完成该过程。

启用联合身份验证后，用户可以使用其企业凭据登录NetApp Console。

将NetApp Console与 Microsoft Entra ID 联合起来

与您的 Microsoft Entra ID IdP 提供商联合，为NetApp Console启用单点登录 (SSO)。这允许用户使用他们的公司凭证登录。

必需角色

需要联盟管理员角色来创建和管理联盟。联盟查看者可以查看联盟页面。"了解有关访问角色的更多信息。"

您可以与您的企业 IdP 或NetApp支持站点联合。 NetApp建议选择其中一个，但不要同时选择两者。

NetApp仅支持服务提供商发起的（SP发起的） SSO。您需要首先配置身份提供者以信任NetApp作为服务提供

商。然后，您可以在控制台中创建使用身份提供者配置的连接。

您可以与 Microsoft Entra ID 建立联合连接，以启用控制台的单点登录 (SSO)。该过程涉及配置您的 Microsoft Entra ID 以信任控制台作为服务提供商，然后在控制台中创建连接。

步骤

1. 选择*管理>身份和访问*。
2. 选择“**Federation**”以查看“**Federations**”页面。
3. 选择*配置新联合*。

域名详细信息

1. 输入您的域名详细信息：
   a. 选择您是否要使用已验证的域名或您的电子邮件域名。电子邮件域是与您登录的帐户关联的域。
   b. 输入您正在配置的联盟的名称。
   c. 如果您选择已验证的域，请从列表中选择该域。
2. 选择“下一步”。

连接方法

1. 对于您的连接方法，选择*提供商*，然后选择*Microsoft Entra ID*。
2. 选择“下一步”。

配置说明

1. 配置您的 Microsoft Entra ID 以信任NetApp作为服务提供商。您需要在 Microsoft Entra ID 服务器上执行此步骤。
   a. 注册 Microsoft Entra ID 应用程序以信任控制台时，请使用以下值：
      - 对于 重定向 **URL** ，使用 `https://services.cloud.netapp.com`
      - 对于 回复 **URL**，使用 `https://netapp-cloud-account.auth0.com/login/callback`
   b. 为您的 Microsoft Entra ID 应用创建客户端机密。您需要提供客户端 ID、客户端密钥和 Entra ID 域名来完成联合。
2. 返回控制台，然后选择“下一步”来创建连接。

创建连接

1. 使用 Microsoft Entra ID 创建连接
   a. 输入您在上一步中创建的客户端 ID 和客户端密钥。
   b. 输入 Microsoft Entra ID 域名。
2. 选择*创建连接*。系统在几秒钟内建立连接。

测试并启用连接

1. 选择“下一步”。

2. 选择*测试连接*来测试您的连接。您将被引导至 IdP 服务器的登录页面。使用您的身份提供商凭据登录。登录后，返回控制台启用连接。

   在受限模式下使用控制台时，请将 URL 复制到隐身浏览器窗口或单独的浏览器中，以登录到您的身份提供商 (IdP)。

3. 在控制台中，选择“下一步”以查看摘要页面。
4. 设置通知。

   您可以选择七天或三十天。系统会通过电子邮件向具有以下角色的任何用户发送到期通知，并在控制台中显示这些通知：超级管理员、组织管理员、联盟管理员和联盟查看者。

5. 查看联盟详细信息，然后选择“启用联盟”。
6. 选择“完成”以完成该过程。

启用联合身份验证后，用户可以使用其企业凭据登录NetApp Console。

使用 PingFederate 联合NetApp Console

与您的 PingFederate IdP 提供商联合，为NetApp Console启用单点登录 (SSO)。这允许用户使用他们的公司凭证登录。

必需角色

需要联盟管理员角色来创建和管理联盟。联盟查看者可以查看联盟页面。"了解有关访问角色的更多信息。"

您可以与您的企业 IdP 或NetApp支持站点联合。 NetApp建议选择其中一个，但不要同时选择两者。

NetApp仅支持服务提供商发起的（SP发起的） SSO。您需要首先配置身份提供者以信任NetApp作为服务提供商。然后，您可以在控制台中创建使用身份提供者配置的连接。

您可以使用 PingFederate 设置联合连接，以启用控制台的单点登录 (SSO)。该过程涉及配置您的 PingFederate 服务器以信任控制台作为服务提供商，然后在控制台中创建连接。

步骤

1. 选择*管理>身份和访问*。
2. 选择“**Federation**”以查看“**Federations**”页面。
3. 选择*配置新联合*。
4. 输入您的域名详细信息：
   a. 选择您是否要使用已验证的域名或您的电子邮件域名。电子邮件域是与您登录的帐户关联的域。
   b. 输入您正在配置的联盟的名称。
   c. 如果您选择已验证的域，请从列表中选择该域。
5. 选择“下一步”。
6. 对于您的连接方法，选择*提供商*，然后选择*PingFederate*。

7. 选择“下一步”。
8. 配置您的 PingFederate 服务器以信任NetApp作为服务提供商。您需要在 PingFederate 服务器上执行此步骤。
   a. 配置 PingFederate 以信任NetApp Console时，请使用以下值：
      - 对于 回复 **URL** 或 断言消费者服务 **(ACS) URL**，使用 `https://netapp-cloud-account.auth0.com/login/callback`
      - 对于*注销 URL*，使用 `https://netapp-cloud-account.auth0.com/logout`
      - 对于*受众/实体 ID*，使用 `urn:auth0:netapp-cloud-account:<fed-domain-name-saml>`其中 `<fed-domain-name-pingfederate>` 是联合的域名。例如，如果您的域名是 `example.com`，受众/实体 ID 将是 `urn:auth0:netappcloud-account:fed-example-com-pingfederate`。
   b. 复制 PingFederate 服务器 URL。在控制台中创建连接时，您将需要此 URL。
   c. 从您的 PingFederate 服务器下载 X.509 证书。它需要采用 Base64 编码的 PEM 格式（.pem、.crt、.cer）。
9. 返回控制台，然后选择“下一步”来创建连接。
10. 使用 PingFederate 创建连接
    a. 输入您在上一步中复制的 PingFederate 服务器 URL。
    b. 上传 X.509 签名证书。证书必须采用 PEM、CER 或 CRT 格式。
11. 选择*创建连接*。系统在几秒钟内建立连接。
12. 选择“下一步”。
13. 选择*测试连接*来测试您的连接。您将被引导至 IdP 服务器的登录页面。使用您的身份提供商凭据登录。登录后，返回控制台启用连接。

    在受限模式下使用控制台时，请将 URL 复制到隐身浏览器窗口或单独的浏览器中，以登录到您的身份提供商 (IdP)。

14. 在控制台中，选择“下一步”以查看摘要页面。
15. 设置通知。

    您可以选择七天或三十天。系统会通过电子邮件向具有以下角色的任何用户发送到期通知，并在控制台中显示这些通知：超级管理员、组织管理员、联盟管理员和联盟查看者。

16. 查看联盟详细信息，然后选择“启用联盟”。
17. 选择“完成”以完成该过程。

启用联合身份验证后，用户可以使用其企业凭据登录NetApp Console。

与 SAML 身份提供商联合

与您的 SAML 2.0 IdP 提供商联合，为 NEtApp 控制台启用单点登录 (SSO)。这允许用户使用他们的公司凭证登录。

所需角色

需要联盟管理员角色来创建和管理联盟。联盟查看者可以查看联盟页面。"了解有关访问角色的更多信息。"

您可以与您的企业 IdP 或NetApp支持站点联合。你不能与两者结成联盟。

NetApp仅支持服务提供商发起的（SP发起的） SSO。您需要首先配置身份提供者以信任NetApp作为服务提供商。然后，您可以在控制台中创建使用身份提供者配置的连接。

您可以与 SAML 2.0 提供商建立联合连接，以便为控制台启用单点登录 (SSO)。该过程涉及配置您的提供商以信任NetApp作为服务提供商，然后在控制台中创建连接。

步骤

1. 选择*管理>身份和访问*。
2. 选择“**Federation**”以查看“**Federations**”页面。
3. 选择*配置新联合*。
4. 输入您的域名详细信息：
   a. 选择您是否要使用已验证的域名或您的电子邮件域名。电子邮件域是与您登录的帐户关联的域。
   b. 输入您正在配置的联盟的名称。
   c. 如果您选择已验证的域，请从列表中选择该域。
5. 选择“下一步”。
6. 对于您的连接方法，选择*协议*，然后选择*SAML 身份提供者*。
7. 选择“下一步”。
8. 配置您的 SAML 身份提供商以信任NetApp作为服务提供商。您需要在 SAML 提供商服务器上执行此步骤。
   a. 确保您的 IdP 具有属性 `email`设置为用户的电子邮件地址。这是控制台正确识别用户所必需的：

```
<saml:AttributeStatement
xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <saml:Attribute Name="email"
NameFormat="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
        <saml:AttributeValue
xsi:type="xs:string">email@domain.com</saml:AttributeValue>
    </saml:Attribute>
</saml:AttributeStatement>
```

1. 在控制台中注册 SAML 应用程序时，请使用以下值：
   - 对于 回复 **URL** 或 断言消费者服务 **(ACS) URL**，使用 `https://netapp-cloud-account.auth0.com/login/callback`
   - 对于*注销 URL*，使用 `https://netapp-cloud-account.auth0.com/logout`
   - 对于*受众/实体 ID*，使用 `urn:auth0:netapp-cloud-account:<fed-domain-name-saml>`其

中 `<fed-domain-name-saml>` 是您想要用于联合的域名。例如，如果您的域名是 `example.com，受众/实体 ID 将是 `urn:auth0:netapp-cloud-account:fed-example-com-samlp。

2. 创建信任后，从 SAML 提供商服务器复制以下值：
   - 登录网址
   - 退出 URL（可选）
3. 从您的 SAML 提供商服务器下载 X.509 证书。它需要采用 PEM、CER 或 CRT 格式。
   a. 返回控制台，然后选择“下一步”来创建连接。
   b. 使用 SAML 创建连接。
4. 输入您的 SAML 服务器的 登录 **URL**。
5. 上传从 SAML 提供商服务器下载的 X.509 证书。
6. 或者，输入您的 SAML 服务器的 退出 **URL**。
   a. 选择*创建连接*。系统在几秒钟内建立连接。
   b. 选择“下一步”。
   c. 选择*测试连接*来测试您的连接。您将被引导至 IdP 服务器的登录页面。使用您的身份提供商凭据登录。登录后，返回控制台启用连接。

      在受限模式下使用控制台时，请将 URL 复制到隐身浏览器窗口或单独的浏览器中，以登录到您的身份提供商 (IdP)。

   d. 在控制台中，选择“下一步”以查看摘要页面。
   e. 设置通知。

      您可以选择七天或三十天。系统会通过电子邮件向具有以下角色的任何用户发送到期通知，并在控制台中显示这些通知：超级管理员、组织管理员、联盟管理员和联盟查看者。

   f. 查看联盟详细信息，然后选择“启用联盟”。
   g. 选择“完成”以完成该过程。

启用联合身份验证后，用户可以使用其企业凭据登录NetApp Console。