Configurer les fédérations

NetApp Console setup and administration

NetApp
February 11, 2026

Sommaire

Configurer les fédérations

Fédérer la NetApp Console avec les services de fédération Active Directory (AD FS)

Fédérez vos services de fédération Active Directory (AD FS) avec la NetApp Console pour activer l'authentification unique (SSO) pour la NetApp Console. Cela permet aux utilisateurs de se connecter à la console en utilisant leurs identifiants d'entreprise.

Rôles requis

Le rôle d'administrateur de fédération est requis pour créer et gérer des fédérations. Le spectateur de la Fédération peut voir la page de la Fédération."En savoir plus sur les rôles d'accès."

> Vous pouvez vous fédérer avec votre IdP d'entreprise ou avec le site de support NetApp . NetApp recommande de choisir l'un ou l'autre, mais pas les deux.

NetApp prend uniquement en charge l'authentification unique initiée par le fournisseur de services (SP). Tout d'abord, configurez le fournisseur d'identité pour qu'il approuve la NetApp Console en tant que fournisseur de services. Ensuite, créez une connexion dans la console en utilisant la configuration de votre fournisseur d'identité.

Vous pouvez configurer la fédération avec votre serveur AD FS pour activer l'authentification unique (SSO) pour la NetApp Console. Le processus implique la configuration de votre AD FS pour approuver la console en tant que fournisseur de services, puis la création de la connexion dans la NetApp Console.

Étapes

1. Sélectionnez **Administration > Identité et accès**.
2. Sélectionnez **Fédération** pour afficher la page **Fédérations**.
3. Sélectionnez **Configurer une nouvelle fédération**.
4. Entrez les détails de votre domaine :
    a. Choisissez si vous souhaitez utiliser un domaine vérifié ou votre domaine de messagerie. Le domaine de messagerie est le domaine associé au compte avec lequel vous êtes connecté.
    b. Entrez le nom de la fédération que vous configurez.
    c. Si vous choisissez un domaine vérifié, sélectionnez le domaine dans la liste.
5. Sélectionnez **Suivant**.
6. Pour votre méthode de connexion, choisissez **Protocole** puis sélectionnez **Active Directory Federation Services (AD FS)**.
7. Sélectionnez **Suivant**.
8. Créez une approbation de partie de confiance sur votre serveur AD FS. Vous pouvez utiliser PowerShell ou le configurer manuellement sur votre serveur AD FS. Consultez la documentation AD FS pour plus de détails sur la création d'une approbation de partie de confiance.
    a. Créez la confiance à l'aide de PowerShell en utilisant le script suivant :

```
(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. Vous pouvez également créer l'approbation manuellement dans la console de gestion AD FS. Utilisez les valeurs suivantes de la NetApp Console lors de la création de l'approbation :

   - Lors de la création de l'identifiant de confiance de confiance, utilisez la valeur **YOUR_TENANT** : `netapp-cloud-account`
   - Lorsque vous sélectionnez **Activer la prise en charge de WS-Federation**, utilisez la valeur **YOUR_AUTH0_DOMAIN** : `netapp-cloud-account.auth0.com`

c. Après avoir créé l'approbation, copiez l'URL des métadonnées à partir de votre serveur AD FS ou téléchargez le fichier de métadonnées de fédération. Vous aurez besoin de cette URL ou de ce fichier pour terminer la connexion dans la console.

NetApp recommande d'utiliser l'URL des métadonnées pour permettre à la NetApp Console de récupérer automatiquement la dernière configuration AD FS. Si vous téléchargez le fichier de métadonnées de fédération, vous devrez le mettre à jour manuellement dans la NetApp Console chaque fois que des modifications sont apportées à votre configuration AD FS.

9. Revenez à la console et sélectionnez **Suivant** pour créer la connexion.
10. Créez la connexion avec AD FS.
    a. Saisissez l'**URL AD FS** que vous avez copiée à partir de votre serveur AD FS à l'étape précédente ou téléchargez le fichier de métadonnées de fédération que vous avez téléchargé à partir de votre serveur AD FS.
11. Sélectionnez **Créer une connexion**. La création de la connexion peut prendre quelques secondes.
12. Sélectionnez **Suivant**.
13. Sélectionnez **Tester la connexion** pour tester votre connexion. Vous êtes dirigé vers une page de connexion pour votre serveur IdP. Connectez-vous avec vos identifiants IdP. Une fois connecté, retournez à la console pour activer la connexion.

    Lorsque vous utilisez la console en mode restreint, copiez l'URL dans une fenêtre de navigateur incognito ou dans un navigateur distinct pour vous connecter à votre fournisseur d'identité.

14. Dans la console, sélectionnez **Suivant** pour consulter la page récapitulative.
15. Configurer les notifications.

    Choisissez entre sept jours ou 30 jours. Le système envoie par courriel des notifications d'expiration et les affiche dans la console à tout utilisateur ayant les rôles suivants : super administrateur, administrateur d'organisation, administrateur de fédération et visionneur de fédération.

16. Vérifiez les détails de la fédération, puis sélectionnez **Activer la fédération**.
17. Sélectionnez **Terminer** pour terminer le processus.

Une fois la fédération activée, les utilisateurs se connectent à la NetApp Console à l'aide de leurs identifiants

d’entreprise.

Fédérer la NetApp Console avec Microsoft Entra ID

Fédérez-vous avec votre fournisseur IdP Microsoft Entra ID pour activer l’authentification unique (SSO) pour la NetApp Console. Cela permet aux utilisateurs de se connecter en utilisant leurs identifiants d’entreprise.

Rôles requis

Le rôle d’administrateur de fédération est requis pour créer et gérer des fédérations. Le spectateur de la Fédération peut voir la page de la Fédération."En savoir plus sur les rôles d’accès."

Vous pouvez vous fédérer avec votre IdP d’entreprise ou avec le site de support NetApp . NetApp recommande de choisir l’un ou l’autre, mais pas les deux.

NetApp prend uniquement en charge l’authentification unique initiée par le fournisseur de services (SP). Vous devez d’abord configurer le fournisseur d’identité pour qu’il approuve NetApp en tant que fournisseur de services. Ensuite, vous pouvez créer une connexion dans la console qui utilise la configuration du fournisseur d’identité.

Vous pouvez configurer une connexion fédérée avec Microsoft Entra ID pour activer l’authentification unique (SSO) pour la console. Le processus implique la configuration de votre identifiant Microsoft Entra pour approuver la console en tant que fournisseur de services, puis la création de la connexion dans la console.

Étapes

1. Sélectionnez **Administration > Identité et accès**.
2. Sélectionnez **Fédération** pour afficher la page **Fédérations**.
3. Sélectionnez **Configurer une nouvelle fédération**.

Détails du domaine

1. Entrez les détails de votre domaine :
   a. Choisissez si vous souhaitez utiliser un domaine vérifié ou votre domaine de messagerie. Le domaine de messagerie est le domaine associé au compte avec lequel vous êtes connecté.
   b. Entrez le nom de la fédération que vous configurez.
   c. Si vous choisissez un domaine vérifié, sélectionnez le domaine dans la liste.
2. Sélectionnez **Suivant**.

Méthode de connexion

1. Pour votre méthode de connexion, choisissez **Fournisseur** puis sélectionnez **Microsoft Entra ID**.
2. Sélectionnez **Suivant**.

Instructions de configuration

1. Configurez votre identifiant Microsoft Entra pour faire confiance à NetApp en tant que fournisseur de services. Vous devez effectuer cette étape sur votre serveur Microsoft Entra ID.
   a. Utilisez les valeurs suivantes lors de l’enregistrement de votre application Microsoft Entra ID pour faire confiance à la console :

- Pour l'**URL de redirection**, utilisez `https://services.cloud.netapp.com`
- Pour l'**URL de réponse**, utilisez `https://netapp-cloud-account.auth0.com/login/callback`

b. Créez un secret client pour votre application Microsoft Entra ID. Vous devrez fournir l'ID client, le secret client et le nom de domaine Entra ID pour terminer la fédération.

2. Revenez à la console et sélectionnez **Suivant** pour créer la connexion.

Créer une connexion

1. Créer la connexion avec Microsoft Entra ID
   a. Saisissez l'ID client et le secret client que vous avez créés à l'étape précédente.
   b. Saisissez le nom de domaine Microsoft Entra ID.
2. Sélectionnez **Créer une connexion**. Le système crée la connexion en quelques secondes.

Tester et activer la connexion

1. Sélectionnez **Suivant**.
2. Sélectionnez **Tester la connexion** pour tester votre connexion. Vous êtes dirigé vers une page de connexion pour votre serveur IdP. Connectez-vous avec vos identifiants IdP. Une fois connecté, retournez à la console pour activer la connexion.

   Lorsque vous utilisez la console en mode restreint, copiez l'URL dans une fenêtre de navigateur incognito ou dans un navigateur distinct pour vous connecter à votre fournisseur d'identité.

3. Dans la console, sélectionnez **Suivant** pour consulter la page récapitulative.
4. Configurer les notifications.

   Choisissez entre sept jours ou 30 jours. Le système envoie par courriel des notifications d'expiration et les affiche dans la console à tout utilisateur ayant les rôles suivants : super administrateur, administrateur d'organisation, administrateur de fédération et visionneur de fédération.

5. Vérifiez les détails de la fédération, puis sélectionnez **Activer la fédération**.
6. Sélectionnez **Terminer** pour terminer le processus.

Une fois la fédération activée, les utilisateurs se connectent à la NetApp Console à l'aide de leurs identifiants d'entreprise.

Fédérer la NetApp Console avec PingFederate

Fédérez-vous avec votre fournisseur IdP PingFederate pour activer l'authentification unique (SSO) pour la NetApp Console. Cela permet aux utilisateurs de se connecter en utilisant leurs identifiants d'entreprise.

Rôles requis

Le rôle d'administrateur de fédération est requis pour créer et gérer des fédérations. Le spectateur de la Fédération peut voir la page de la Fédération."En savoir plus sur les rôles d'accès."

Vous pouvez vous fédérer avec votre IdP d'entreprise ou avec le site de support NetApp . NetApp recommande de choisir l'un ou l'autre, mais pas les deux.

NetApp prend uniquement en charge l'authentification unique initiée par le fournisseur de services (SP). Vous devez d'abord configurer le fournisseur d'identité pour qu'il approuve NetApp en tant que fournisseur de services. Ensuite, vous pouvez créer une connexion dans la console qui utilise la configuration du fournisseur d'identité.

Vous pouvez configurer une connexion fédérée avec PingFederate pour activer l'authentification unique (SSO) pour la console. Le processus implique la configuration de votre serveur PingFederate pour faire confiance à la console en tant que fournisseur de services, puis la création de la connexion dans la console.

Étapes

1. Sélectionnez **Administration > Identité et accès**.
2. Sélectionnez **Fédération** pour afficher la page **Fédérations**.
3. Sélectionnez **Configurer une nouvelle fédération**.
4. Entrez les détails de votre domaine :
   a. Choisissez si vous souhaitez utiliser un domaine vérifié ou votre domaine de messagerie. Le domaine de messagerie est le domaine associé au compte avec lequel vous êtes connecté.
   b. Entrez le nom de la fédération que vous configurez.
   c. Si vous choisissez un domaine vérifié, sélectionnez le domaine dans la liste.
5. Sélectionnez **Suivant**.
6. Pour votre méthode de connexion, choisissez **Fournisseur** puis sélectionnez **PingFederate**.
7. Sélectionnez **Suivant**.
8. Configurez votre serveur PingFederate pour faire confiance à NetApp en tant que fournisseur de services. Vous devez effectuer cette étape sur votre serveur PingFederate.
   a. Utilisez les valeurs suivantes lors de la configuration de PingFederate pour approuver la NetApp Console:
      - Pour l'**URL de réponse** ou l'**URL du service client d'assertion (ACS)**, utilisez `https://netapp-cloud-account.auth0.com/login/callback`
      - Pour l'**URL de déconnexion**, utilisez `https://netapp-cloud-account.auth0.com/logout`
      - Pour **ID d'audience/d'entité**, utilisez `urn:auth0:netapp-cloud-account:<fed-domain-name-saml>` où <fed-domain-name-pingfederate> est le nom de domaine de la fédération. Par exemple, si votre domaine est `example.com` , l'ID d'audience/d'entité serait `urn:auth0:netappcloud-account:fed-example-com-pingfederate` .
   b. Copiez l'URL du serveur PingFederate. Vous aurez besoin de cette URL lors de la création de la connexion dans la console.
   c. Téléchargez le certificat X.509 depuis votre serveur PingFederate. Il doit être au format PEM codé en Base64 (.pem, .crt, .cer).
9. Revenez à la console et sélectionnez **Suivant** pour créer la connexion.
10. Créer la connexion avec PingFederate
    a. Saisissez l'URL du serveur PingFederate que vous avez copiée à l'étape précédente.
    b. Téléchargez le certificat de signature X.509. Le certificat doit être au format PEM, CER ou CRT.

11. Sélectionnez **Créer une connexion**. Le système crée la connexion en quelques secondes.
12. Sélectionnez **Suivant**.
13. Sélectionnez **Tester la connexion** pour tester votre connexion. Vous êtes dirigé vers une page de connexion pour votre serveur IdP. Connectez-vous avec vos identifiants IdP. Une fois connecté, retournez à la console pour activer la connexion.

    Lorsque vous utilisez la console en mode restreint, copiez l'URL dans une fenêtre de navigateur incognito ou dans un navigateur distinct pour vous connecter à votre fournisseur d'identité.

14. Dans la console, sélectionnez **Suivant** pour consulter la page récapitulative.
15. Configurer les notifications.

    Choisissez entre sept jours ou 30 jours. Le système envoie par courriel des notifications d'expiration et les affiche dans la console à tout utilisateur ayant les rôles suivants : super administrateur, administrateur d'organisation, administrateur de fédération et visionneur de fédération.

16. Vérifiez les détails de la fédération, puis sélectionnez **Activer la fédération**.
17. Sélectionnez **Terminer** pour terminer le processus.

Une fois la fédération activée, les utilisateurs se connectent à la NetApp Console à l'aide de leurs identifiants d'entreprise.

Fédérer avec un fournisseur d'identité SAML

Fédérez-vous avec votre fournisseur IdP SAML 2.0 pour activer l'authentification unique (SSO) pour la console NEtApp. Cela permet aux utilisateurs de se connecter en utilisant leurs identifiants d'entreprise.

Rôle requis

Le rôle d'administrateur de fédération est requis pour créer et gérer des fédérations. Le spectateur de la Fédération peut voir la page de la Fédération."En savoir plus sur les rôles d'accès."

Vous pouvez vous fédérer avec votre IdP d'entreprise ou avec le site de support NetApp . Vous ne pouvez pas vous fédérer avec les deux.

NetApp prend uniquement en charge l'authentification unique initiée par le fournisseur de services (SP). Vous devez d'abord configurer le fournisseur d'identité pour qu'il approuve NetApp en tant que fournisseur de services. Ensuite, vous pouvez créer une connexion dans la console qui utilise la configuration du fournisseur d'identité.

Vous pouvez configurer une connexion fédérée avec votre fournisseur SAML 2.0 pour activer l'authentification unique (SSO) pour la console. Le processus implique la configuration de votre fournisseur pour qu'il fasse confiance à NetApp en tant que fournisseur de services, puis la création de la connexion dans la console.

Étapes

1. Sélectionnez **Administration > Identité et accès**.
2. Sélectionnez **Fédération** pour afficher la page **Fédérations**.
3. Sélectionnez **Configurer une nouvelle fédération**.

4. Entrez les détails de votre domaine :
    a. Choisissez si vous souhaitez utiliser un domaine vérifié ou votre domaine de messagerie. Le domaine de messagerie est le domaine associé au compte avec lequel vous êtes connecté.
    b. Entrez le nom de la fédération que vous configurez.
    c. Si vous choisissez un domaine vérifié, sélectionnez le domaine dans la liste.
5. Sélectionnez **Suivant**.
6. Pour votre méthode de connexion, choisissez **Protocole** puis sélectionnez **Fournisseur d'identité SAML**.
7. Sélectionnez **Suivant**.
8. Configurez votre fournisseur d'identité SAML pour faire confiance à NetApp en tant que fournisseur de services. Vous devez effectuer cette étape sur votre serveur fournisseur SAML.
    a. Assurez-vous que votre IdP possède l'attribut `email` définir sur l'adresse e-mail de l'utilisateur. Ceci est nécessaire pour que la console identifie correctement les utilisateurs :

```
<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. Utilisez les valeurs suivantes lors de l'enregistrement de votre application SAML auprès de la console :
    - Pour l'**URL de réponse** ou l'**URL du service client d'assertion (ACS)**, utilisez `https://netapp-cloud-account.auth0.com/login/callback`
    - Pour l'**URL de déconnexion**, utilisez `https://netapp-cloud-account.auth0.com/logout`
    - Pour **ID d'audience/d'entité**, utilisez `urn:auth0:netapp-cloud-account:<fed-domain-name-saml>` où <fed-domain-name-saml> est le nom de domaine que vous souhaitez utiliser pour la fédération. Par exemple, si votre domaine est `example.com` , l'ID d'audience/d'entité serait `urn:auth0:netapp-cloud-account:fed-example-com-samlp` .
2. Après avoir créé la confiance, copiez les valeurs suivantes à partir de votre serveur fournisseur SAML :
    - URL de connexion
    - URL de déconnexion (facultatif)
3. Téléchargez le certificat X.509 depuis le serveur de votre fournisseur SAML. Il doit être au format PEM, CER ou CRT.
    a. Revenez à la console et sélectionnez **Suivant** pour créer la connexion.
    b. Créez la connexion avec SAML.
4. Saisissez l'**URL de connexion** de votre serveur SAML.
5. Téléchargez le certificat X.509 que vous avez téléchargé depuis le serveur de votre fournisseur SAML.

6. Si vous le souhaitez, saisissez l'**URL de déconnexion** de votre serveur SAML.
   a. Sélectionnez **Créer une connexion**. Le système crée la connexion en quelques secondes.
   b. Sélectionnez **Suivant**.
   c. Sélectionnez **Tester la connexion** pour tester votre connexion. Vous êtes dirigé vers une page de connexion pour votre serveur IdP. Connectez-vous avec vos identifiants IdP. Une fois connecté, retournez à la console pour activer la connexion.

      Lorsque vous utilisez la console en mode restreint, copiez l'URL dans une fenêtre de navigateur incognito ou dans un navigateur distinct pour vous connecter à votre fournisseur d'identité.

   d. Dans la console, sélectionnez **Suivant** pour consulter la page récapitulative.
   e. Configurer les notifications.

      Choisissez entre sept jours ou 30 jours. Le système envoie par courriel des notifications d'expiration et les affiche dans la console à tout utilisateur ayant les rôles suivants : super administrateur, administrateur d'organisation, administrateur de fédération et visionneur de fédération.

   f. Vérifiez les détails de la fédération, puis sélectionnez **Activer la fédération**.
   g. Sélectionnez **Terminer** pour terminer le processus.

Une fois la fédération activée, les utilisateurs se connectent à la NetApp Console à l'aide de leurs identifiants d'entreprise.