



Identitätsföderation

NetApp Console setup and administration

NetApp
January 13, 2026

Inhalt

Identitätsföderation	1
Aktivieren Sie Single Sign-On durch die Verwendung der Identitätsföderation mit der NetApp Console	1
Identitätsföderation mit der NetApp -Support-Site	1
Richten Sie eine Verbundverbindung mit Ihrem Identitätsanbieter ein	1
Domänenüberprüfung	3
Überprüfen Sie die E-Mail-Domäne für Ihre Verbundverbindung	3
Konfigurieren von Föderationen	3
Verbinden Sie die NetApp Console mit Active Directory Federation Services (AD FS)	3
Verbinden Sie die NetApp Console mit der Microsoft Entra-ID	5
Föderieren Sie die NetApp Console mit PingFederate	7
Föderieren Sie mit einem SAML-Identitätsanbieter	9
Föderationen verwalten	11
Föderationen in der NetApp Console verwalten	11
Importieren Sie Ihre Föderation in die NetApp Console	13

Identitätsföderation

Aktivieren Sie Single Sign-On durch die Verwendung der Identitätsföderation mit der NetApp Console

Single-Sign-On (Föderation) vereinfacht den Anmeldevorgang und erhöht die Sicherheit, indem Benutzer sich mit ihren Unternehmensanmeldeinformationen bei der NetApp Console anmelden können. Sie können Single Sign-On (SSO) bei Ihrem Identitätsanbieter (IdP) oder über die NetApp Support-Site aktivieren.

Erforderliche Rolle

Organisationsadministrator, Föderationsadministrator, Föderationsbetrachter. "[Erfahren Sie mehr über Zugriffsrollen.](#)"

Identitätsföderation mit der NetApp -Support-Site

Durch die Verbindung mit der NetApp -Support-Site können sich Benutzer mit denselben Anmeldeinformationen bei der Konsole, Active IQ Digital Advisor und anderen zugehörigen Apps anmelden.



Wenn Sie eine Verbindung mit der NetApp -Support-Site herstellen, können Sie nicht gleichzeitig eine Verbindung mit Ihrem Corporate Identity Management-Anbieter herstellen. Wählen Sie die Option aus, die für Ihr Unternehmen am besten geeignet ist.

Schritte

1. Laden Sie die "[NetApp Federation-Antragsformular](#)".
2. Senden Sie das Formular an die im Formular angegebene E-Mail-Adresse.

Das NetApp Supportteam prüft und bearbeitet Ihre Anfrage.

Richten Sie eine Verbundverbindung mit Ihrem Identitätsanbieter ein

Sie können eine Verbundverbindung mit Ihrem Identitätsanbieter einrichten, um Single Sign-On (SSO) für die Konsole zu aktivieren. Der Vorgang umfasst die Konfiguration Ihres Identitätsanbieters, sodass dieser NetApp als Dienstanbieter vertraut, und die anschließende Herstellung der Verbindung in der Konsole.



Wenn Sie die Föderation zuvor mit NetApp Cloud Central (einer externen Anwendung der Konsole) konfiguriert haben, müssen Sie Ihre Föderation über die Föderationsseite importieren, um sie in der Konsole zu verwalten. "[Erfahren Sie, wie Sie Ihre Föderation importieren.](#)"

Unterstützte Identitätsanbieter

NetApp unterstützt die folgenden Protokolle und Identitätsanbieter für die Föderation:

Protokolle

- Security Assertion Markup Language (SAML)-Identitätsanbieter
- Active Directory-Verbunddienste (AD FS)

Identitätsanbieter

- Microsoft Entra ID
- PingFederate

Föderation mit NetApp Console -Workflow

NetApp unterstützt nur vom Dienstanbieter initiiertes (SP-initiiertes) SSO. Sie müssen zunächst den Identitätsanbieter so konfigurieren, dass er NetApp als Dienstanbieter vertraut. Anschließend können Sie in der Konsole eine Verbindung erstellen, die die Konfiguration des Identitätsanbieters verwendet.

Sie können eine Föderation mit Ihrer E-Mail-Domäne oder mit einer anderen Domäne, die Ihnen gehört, herstellen. Um eine Föderation mit einer anderen Domäne als Ihrer E-Mail-Domäne herzustellen, bestätigen Sie zunächst, dass Sie der Eigentümer der Domäne sind.

1

Bestätigen Sie Ihre Domäne (wenn Sie nicht Ihre E-Mail-Domäne verwenden)

Um eine Föderation mit einer anderen Domäne als Ihrer E-Mail-Domäne herzustellen, bestätigen Sie, dass Sie deren Eigentümer sind. Sie können Ihre E-Mail-Domäne ohne zusätzliche Schritte föderieren.

2

Konfigurieren Sie Ihren IdP so, dass er NetApp als Serviceprovider vertraut

Konfigurieren Sie Ihren Identitätsanbieter so, dass er NetApp vertraut, indem Sie eine neue Anwendung erstellen und Details wie die ACS-URL, die Entitäts-ID oder andere Anmeldeinformationen angeben. Die Informationen zum Dienstanbieter variieren je nach Identitätsanbieter. Weitere Informationen finden Sie in der Dokumentation Ihres spezifischen Identitätsanbieters. Sie müssen mit Ihrem IdP-Administrator zusammenarbeiten, um diesen Schritt abzuschließen.

3

Erstellen Sie die Verbundverbindung in der Konsole

Geben Sie die SAML-Metadaten-URL oder -Datei von Ihrem Identitätsanbieter an, um die Verbindung herzustellen. Diese Informationen werden verwendet, um die Vertrauensbeziehung zwischen der Konsole und Ihrem Identitätsanbieter herzustellen. Die von Ihnen bereitgestellten Informationen hängen von dem von Ihnen verwendeten IdP ab. Wenn Sie beispielsweise die Microsoft Entra ID verwenden, müssen Sie die Client-ID, das Geheimnis und die Domäne angeben.

4

Testen Sie Ihre Föderation in der Konsole

Testen Sie Ihre Verbundverbindung, bevor Sie sie aktivieren. Verwenden Sie die Testoption auf der Seite „Föderation“ in der Konsole, um zu überprüfen, ob sich Ihr Testbenutzer erfolgreich authentifizieren kann. Wenn der Test erfolgreich ist, können Sie die Verbindung aktivieren.

5

Aktivieren Sie Ihre Verbindung in der Konsole

Nachdem Sie die Verbindung aktiviert haben, können sich Benutzer mit ihren Unternehmensanmeldeinformationen bei der Konsole anmelden.

Lesen Sie zunächst das Thema für Ihr jeweiliges Protokoll oder Ihren IdP:

- ["Einrichten einer Verbundverbindung mit AD FS"](#)
- ["Einrichten einer Verbundverbindung mit der Microsoft Entra ID"](#)

- ["Einrichten einer Verbundverbindung mit PingFederate"](#)
- ["Einrichten einer Verbundverbindung mit einem SAML-Identitätsanbieter"](#)

Domänenüberprüfung

Überprüfen Sie die E-Mail-Domäne für Ihre Verbundverbindung

Wenn Sie eine Föderation mit einer Domäne durchführen möchten, die sich von Ihrer E-Mail-Domäne unterscheidet, müssen Sie zunächst bestätigen, dass Sie der Eigentümer der Domäne sind. Sie können für die Föderation nur verifizierte Domänen verwenden.

Erforderliche Rollen

Zum Erstellen und Verwalten von Föderationen ist die Rolle des Föderationsadministrators erforderlich. Der Federation-Viewer kann die Federation-Seite anzeigen. ["Erfahren Sie mehr über Zugriffsrollen."](#)

Zur Überprüfung Ihrer Domäne müssen Sie den DNS-Einstellungen Ihrer Domäne einen TXT-Eintrag hinzufügen. Dieser Datensatz dient als Nachweis dafür, dass Sie der Eigentümer der Domäne sind, und ermöglicht der NetApp Console, der Domäne für die Föderation zu vertrauen. Möglicherweise müssen Sie sich mit Ihrem IT- oder Netzwerkadministrator abstimmen, um diesen Schritt abzuschließen.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie **Föderation** aus, um die Seite **Föderationen** anzuzeigen.
3. Wählen Sie **Neue Föderation konfigurieren**.
4. Wählen Sie **Domänenbesitz bestätigen**.
5. Geben Sie die Domäne ein, die Sie verifizieren möchten, und wählen Sie **Weiter**.
6. Kopieren Sie den bereitgestellten TXT-Eintrag.
7. Gehen Sie zu den DNS-Einstellungen Ihrer Domäne und konfigurieren Sie den TXT-Wert, der als TXT-Eintrag für Ihre Domäne bereitgestellt wurde. Arbeiten Sie bei Bedarf mit Ihrem IT- oder Netzwerkadministrator zusammen.
8. Nachdem der TXT-Eintrag hinzugefügt wurde, kehren Sie zur Konsole zurück und wählen Sie **Überprüfen**.

Konfigurieren von Föderationen

Verbinden Sie die NetApp Console mit Active Directory Federation Services (AD FS).

Verbinden Sie Ihre Active Directory Federation Services (AD FS) mit der NetApp Console, um Single Sign-On (SSO) für die NetApp Console zu aktivieren. Dadurch können sich Benutzer mit ihren Unternehmensanmeldeinformationen bei der Konsole anmelden.

Erforderliche Rollen

Zum Erstellen und Verwalten von Föderationen ist die Rolle des Föderationsadministrators erforderlich. Der Federation-Viewer kann die Federation-Seite anzeigen. ["Erfahren Sie mehr über Zugriffsrollen."](#)



Sie können eine Föderation mit Ihrem Unternehmens-IdP oder mit der NetApp -Support-Site herstellen. NetApp empfiehlt, sich für das eine oder das andere zu entscheiden, aber nicht für beides.

NetApp unterstützt nur vom Dienstanbieter initiiertes (SP-initiiertes) SSO. Konfigurieren Sie zunächst den Identitätsanbieter so, dass er der NetApp Console als Dienstanbieter vertraut. Erstellen Sie dann mithilfe der Konfiguration Ihres Identitätsanbieters eine Verbindung in der Konsole.

Sie können eine Föderation mit Ihrem AD FS-Server einrichten, um Single Sign-On (SSO) für die NetApp Console zu aktivieren. Der Vorgang umfasst die Konfiguration Ihres AD FS, sodass es der Konsole als Dienstanbieter vertraut, und die anschließende Herstellung der Verbindung in der NetApp Console.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie **Föderation** aus, um die Seite **Föderationen** anzuzeigen.
3. Wählen Sie **Neue Föderation konfigurieren**.
4. Geben Sie Ihre Domänendetails ein:
 - a. Wählen Sie, ob Sie eine verifizierte Domäne oder Ihre E-Mail-Domäne verwenden möchten. Die E-Mail-Domäne ist die Domäne, die mit dem Konto verknüpft ist, mit dem Sie angemeldet sind.
 - b. Geben Sie den Namen der Föderation ein, die Sie konfigurieren.
 - c. Wenn Sie eine verifizierte Domäne auswählen, wählen Sie die Domäne aus der Liste aus.
5. Wählen Sie **Weiter**.
6. Wählen Sie als Verbindungsmethode **Protokoll** und dann **Active Directory Federation Services (AD FS)**.
7. Wählen Sie **Weiter**.
8. Erstellen Sie eine Vertrauensstellung der vertrauenden Seite auf Ihrem AD FS-Server. Sie können PowerShell verwenden oder es manuell auf Ihrem AD FS-Server konfigurieren. Weitere Informationen zum Erstellen einer Vertrauensstellung der vertrauenden Seite finden Sie in der AD FS-Dokumentation.
 - a. Erstellen Sie die Vertrauensstellung mithilfe von PowerShell und dem folgenden Skript:

```
(new-object Net.WebClient -property @{Encoding = [Text.Encoding]
::UTF8}).DownloadString("https://raw.githubusercontent.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. Alternativ können Sie die Vertrauensstellung manuell in der AD FS-Verwaltungskonsole erstellen. Verwenden Sie beim Erstellen der Vertrauensstellung die folgenden NetApp Console :
 - Verwenden Sie beim Erstellen der Relying Trust Identifier den Wert **YOUR_TENANT**: netapp-cloud-account
 - Wenn Sie **Unterstützung für WS-Federation aktivieren** auswählen, verwenden Sie den Wert **YOUR_AUTH0_DOMAIN**: netapp-cloud-account.auth0.com
- c. Kopieren Sie nach dem Erstellen der Vertrauensstellung die Metadaten-URL von Ihrem AD FS-Server oder laden Sie die Verbundmetadaten-datei herunter. Sie benötigen diese URL oder Datei, um die Verbindung in der Konsole herzustellen.

NetApp empfiehlt die Verwendung der Metadaten-URL, damit die NetApp Console automatisch die neueste AD FS-Konfiguration abrufen kann. Wenn Sie die Federation-Metadatendatei herunterladen, müssen Sie sie bei jeder Änderung Ihrer AD FS-Konfiguration manuell in der NetApp Console aktualisieren.

9. Kehren Sie zur Konsole zurück und wählen Sie **Weiter**, um die Verbindung herzustellen.
10. Stellen Sie die Verbindung mit AD FS her.
 - a. Geben Sie die **AD FS-URL** ein, die Sie im vorherigen Schritt von Ihrem AD FS-Server kopiert haben, oder laden Sie die Verbundmetadatendatei hoch, die Sie von Ihrem AD FS-Server heruntergeladen haben.
11. Wählen Sie **Verbindung erstellen**. Das Herstellen der Verbindung kann einige Sekunden dauern.
12. Wählen Sie **Weiter**.
13. Wählen Sie **Verbindung testen**, um Ihre Verbindung zu testen. Sie werden zu einer Anmeldeseite für Ihren IdP-Server weitergeleitet. Melden Sie sich mit Ihren IdP-Zugangsdaten an. Nach dem Einloggen müssen Sie zur Konsole zurückkehren, um die Verbindung zu aktivieren.



Wenn Sie die Konsole im eingeschränkten Modus verwenden, kopieren Sie die URL entweder in ein Inkognito-Browserfenster oder in einen separaten Browser, um sich bei Ihrem Identitätsanbieter anzumelden.

14. Wählen Sie in der Konsole **Weiter**, um die Zusammenfassungsseite anzuzeigen.
15. Benachrichtigungen einrichten.

Sie haben die Wahl zwischen sieben Tagen oder 30 Tagen. Das System versendet E-Mail-Benachrichtigungen über das Ablaufdatum und zeigt diese in der Konsole allen Benutzern mit den folgenden Rollen an: Super-Admin, Organisations-Admin, Verbund-Admin und Verbund-Viewer.

16. Überprüfen Sie die Föderationsdetails und wählen Sie dann **Föderation aktivieren**.
17. Wählen Sie **Fertig**, um den Vorgang abzuschließen.

Nach der Aktivierung der Föderation melden sich die Benutzer mit ihren Unternehmensanmeldeinformationen bei der NetApp Console an.

Verbinden Sie die NetApp Console mit der Microsoft Entra-ID

Verbinden Sie sich mit Ihrem Microsoft Entra ID IdP-Anbieter, um Single Sign-On (SSO) für die NetApp Console zu aktivieren. Dadurch können sich Benutzer mit ihren Unternehmensanmeldeinformationen anmelden.

Erforderliche Rollen

Zum Erstellen und Verwalten von Föderationen ist die Rolle des Föderationsadministrators erforderlich. Der Federation-Viewer kann die Federation-Seite anzeigen. ["Erfahren Sie mehr über Zugriffsrollen."](#)



Sie können eine Föderation mit Ihrem Unternehmens-IdP oder mit der NetApp -Support-Site herstellen. NetApp empfiehlt, sich für das eine oder das andere zu entscheiden, aber nicht für beides.

NetApp unterstützt nur vom Dienstanbieter initiiertes (SP-initiiertes) SSO. Sie müssen zunächst den Identitätsanbieter so konfigurieren, dass er NetApp als Dienstanbieter vertraut. Anschließend können Sie in

der Konsole eine Verbindung erstellen, die die Konfiguration des Identitätsanbieters verwendet.

Sie können eine Verbundverbindung mit der Microsoft Entra ID einrichten, um Single Sign-On (SSO) für die Konsole zu aktivieren. Der Vorgang umfasst die Konfiguration Ihrer Microsoft Entra-ID, um der Konsole als Dienstanbieter zu vertrauen, und das anschließende Erstellen der Verbindung in der Konsole.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie **Föderation** aus, um die Seite **Föderationen** anzuzeigen.
3. Wählen Sie **Neue Föderation konfigurieren**.

Domänendetails

1. Geben Sie Ihre Domänendetails ein:
 - a. Wählen Sie, ob Sie eine verifizierte Domäne oder Ihre E-Mail-Domäne verwenden möchten. Die E-Mail-Domäne ist die Domäne, die mit dem Konto verknüpft ist, mit dem Sie angemeldet sind.
 - b. Geben Sie den Namen der Föderation ein, die Sie konfigurieren.
 - c. Wenn Sie eine verifizierte Domäne auswählen, wählen Sie die Domäne aus der Liste aus.
2. Wählen Sie **Weiter**.

Verbindungsmethode

1. Wählen Sie als Verbindungsmethode **Anbieter** und dann **Microsoft Entra ID**.
2. Wählen Sie **Weiter**.

Konfigurationshinweise

1. Konfigurieren Sie Ihre Microsoft Entra-ID, um NetApp als Dienstanbieter zu vertrauen. Sie müssen diesen Schritt auf Ihrem Microsoft Entra ID-Server ausführen.
 - a. Verwenden Sie beim Registrieren Ihrer Microsoft Entra ID-App die folgenden Werte, um der Konsole zu vertrauen:
 - Verwenden Sie für die **Umleitungs-URL** <https://services.cloud.netapp.com>
 - Verwenden Sie für die **Antwort-URL** <https://netapp-cloud-account.auth0.com/login/callback>
 - b. Erstellen Sie ein Clientgeheimnis für Ihre Microsoft Entra ID-App. Sie müssen die Client-ID, das Client-Geheimnis und den Entra-ID-Domännennamen angeben, um die Föderation abzuschließen.
2. Kehren Sie zur Konsole zurück und wählen Sie **Weiter**, um die Verbindung herzustellen.

Verbindung erstellen

1. Erstellen Sie die Verbindung mit der Microsoft Entra ID
 - a. Geben Sie die Client-ID und das Client-Geheimnis ein, die Sie im vorherigen Schritt erstellt haben.
 - b. Geben Sie den Domännennamen der Microsoft Entra ID ein.
2. Wählen Sie **Verbindung erstellen**. Das System stellt die Verbindung in wenigen Sekunden her.

Testen und aktivieren Sie die Verbindung

1. Wählen Sie **Weiter**.
2. Wählen Sie **Verbindung testen**, um Ihre Verbindung zu testen. Sie werden zu einer Anmeldeseite für Ihren IdP-Server weitergeleitet. Melden Sie sich mit Ihren IdP-Zugangsdaten an. Nach dem Einloggen müssen Sie zur Konsole zurückkehren, um die Verbindung zu aktivieren.



Wenn Sie die Konsole im eingeschränkten Modus verwenden, kopieren Sie die URL entweder in ein Inkognito-Browserfenster oder in einen separaten Browser, um sich bei Ihrem Identitätsanbieter anzumelden.

3. Wählen Sie in der Konsole **Weiter**, um die Zusammenfassungsseite anzuzeigen.
4. Benachrichtigungen einrichten.

Sie haben die Wahl zwischen sieben Tagen oder 30 Tagen. Das System versendet E-Mail-Benachrichtigungen über das Ablaufdatum und zeigt diese in der Konsole allen Benutzern mit den folgenden Rollen an: Super-Admin, Organisations-Admin, Verbund-Admin und Verbund-Viewer.

5. Überprüfen Sie die Föderationsdetails und wählen Sie dann **Föderation aktivieren**.
6. Wählen Sie **Fertig**, um den Vorgang abzuschließen.

Nach der Aktivierung der Föderation melden sich die Benutzer mit ihren Unternehmensanmeldeinformationen bei der NetApp Console an.

Föderieren Sie die NetApp Console mit PingFederate

Verbinden Sie sich mit Ihrem PingFederate IdP-Anbieter, um Single Sign-On (SSO) für die NetApp Console zu aktivieren. Dadurch können sich Benutzer mit ihren Unternehmensanmeldeinformationen anmelden.

Erforderliche Rollen

Zum Erstellen und Verwalten von Föderationen ist die Rolle des Föderationsadministrators erforderlich. Der Federation-Viewer kann die Federation-Seite anzeigen. ["Erfahren Sie mehr über Zugriffsrollen."](#)



Sie können eine Föderation mit Ihrem Unternehmens-IdP oder mit der NetApp -Support-Site herstellen. NetApp empfiehlt, sich für das eine oder das andere zu entscheiden, aber nicht für beides.

NetApp unterstützt nur vom Dienstanbieter initiiertes (SP-initiiertes) SSO. Sie müssen zunächst den Identitätsanbieter so konfigurieren, dass er NetApp als Dienstanbieter vertraut. Anschließend können Sie in der Konsole eine Verbindung erstellen, die die Konfiguration des Identitätsanbieters verwendet.

Sie können mit PingFederate eine Verbundverbindung einrichten, um Single Sign-On (SSO) für die Konsole zu aktivieren. Der Vorgang umfasst die Konfiguration Ihres PingFederate-Servers, sodass dieser der Konsole als Dienstanbieter vertraut, und die anschließende Herstellung der Verbindung in der Konsole.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie **Föderation** aus, um die Seite **Föderationen** anzuzeigen.
3. Wählen Sie **Neue Föderation konfigurieren**.
4. Geben Sie Ihre Domänendetails ein:

- a. Wählen Sie, ob Sie eine verifizierte Domäne oder Ihre E-Mail-Domäne verwenden möchten. Die E-Mail-Domäne ist die Domäne, die mit dem Konto verknüpft ist, mit dem Sie angemeldet sind.
 - b. Geben Sie den Namen der Föderation ein, die Sie konfigurieren.
 - c. Wenn Sie eine verifizierte Domäne auswählen, wählen Sie die Domäne aus der Liste aus.
5. Wählen Sie **Weiter**.
 6. Wählen Sie als Verbindungsmethode **Provider** und dann **PingFederate**.
 7. Wählen Sie **Weiter**.
 8. Konfigurieren Sie Ihren PingFederate-Server so, dass er NetApp als Dienstanbieter vertraut. Sie müssen diesen Schritt auf Ihrem PingFederate-Server ausführen.
 - a. Verwenden Sie die folgenden Werte, wenn Sie PingFederate so konfigurieren, dass es der NetApp Console vertraut:
 - Für die **Antwort-URL** oder **Assertion Consumer Service (ACS)-URL** verwenden Sie <https://netapp-cloud-account.auth0.com/login/callback>
 - Verwenden Sie für die **Abmelde-URL** <https://netapp-cloud-account.auth0.com/logout>
 - Verwenden Sie für **Zielgruppen-/Entitäts-ID** `urn:auth0:netapp-cloud-account:<fed-domain-name-saml>` wobei `<fed-domain-name-pingfederate>` der Domänenname für die Föderation ist. Wenn Ihre Domäne beispielsweise `example.com`, wäre die Zielgruppen-/Entitäts-ID `urn:auth0:netappcloud-account:fed-example-com-pingfederate`.
 - b. Kopieren Sie die URL des PingFederate-Servers. Sie benötigen diese URL, wenn Sie die Verbindung in der Konsole herstellen.
 - c. Laden Sie das X.509-Zertifikat von Ihrem PingFederate-Server herunter. Es muss im Base64-codierten PEM-Format (.pem, .crt, .cer) vorliegen.
 9. Kehren Sie zur Konsole zurück und wählen Sie **Weiter**, um die Verbindung herzustellen.
 10. Erstellen Sie die Verbindung mit PingFederate
 - a. Geben Sie die PingFederate-Server-URL ein, die Sie im vorherigen Schritt kopiert haben.
 - b. Laden Sie das X.509-Signaturzertifikat hoch. Das Zertifikat muss im PEM-, CER- oder CRT-Format vorliegen.
 11. Wählen Sie **Verbindung erstellen**. Das System stellt die Verbindung in wenigen Sekunden her.
 12. Wählen Sie **Weiter**.
 13. Wählen Sie **Verbindung testen**, um Ihre Verbindung zu testen. Sie werden zu einer Anmeldeseite für Ihren IdP-Server weitergeleitet. Melden Sie sich mit Ihren IdP-Zugangsdaten an. Nach dem Einloggen müssen Sie zur Konsole zurückkehren, um die Verbindung zu aktivieren.



Wenn Sie die Konsole im eingeschränkten Modus verwenden, kopieren Sie die URL entweder in ein Inkognito-Browserfenster oder in einen separaten Browser, um sich bei Ihrem Identitätsanbieter anzumelden.

14. Wählen Sie in der Konsole **Weiter**, um die Zusammenfassungsseite anzuzeigen.
15. Benachrichtigungen einrichten.

Sie haben die Wahl zwischen sieben Tagen oder 30 Tagen. Das System versendet E-Mail-Benachrichtigungen über das Ablaufdatum und zeigt diese in der Konsole allen Benutzern mit den folgenden Rollen an: Super-Admin, Organisations-Admin, Verbund-Admin und Verbund-Viewer.

16. Überprüfen Sie die Föderationsdetails und wählen Sie dann **Föderation aktivieren**.

17. Wählen Sie **Fertig**, um den Vorgang abzuschließen.

Nach der Aktivierung der Föderation melden sich die Benutzer mit ihren Unternehmensanmeldeinformationen bei der NetApp Console an.

Föderieren Sie mit einem SAML-Identitätsanbieter

Verbinden Sie sich mit Ihrem SAML 2.0-IdP-Anbieter, um Single Sign-On (SSO) für die NtApp-Konsole zu aktivieren. Dadurch können sich Benutzer mit ihren Unternehmensanmeldeinformationen anmelden.

Erforderliche Rolle

Zum Erstellen und Verwalten von Föderationen ist die Rolle des Föderationsadministrators erforderlich. Der Federation-Viewer kann die Federation-Seite anzeigen. ["Erfahren Sie mehr über Zugriffsrollen."](#)



Sie können eine Föderation mit Ihrem Unternehmens-IdP oder mit der NetApp -Support-Site herstellen. Sie können nicht mit beiden eine Föderation bilden.

NetApp unterstützt nur vom Dienstanbieter initiiertes (SP-initiiertes) SSO. Sie müssen zunächst den Identitätsanbieter so konfigurieren, dass er NetApp als Dienstanbieter vertraut. Anschließend können Sie in der Konsole eine Verbindung erstellen, die die Konfiguration des Identitätsanbieters verwendet.

Sie können eine Verbundverbindung mit Ihrem SAML 2.0-Anbieter einrichten, um Single Sign-On (SSO) für die Konsole zu aktivieren. Der Vorgang umfasst die Konfiguration Ihres Providers, sodass dieser NetApp als Serviceprovider vertraut, und die anschließende Herstellung der Verbindung in der Konsole.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie **Föderation** aus, um die Seite **Föderationen** anzuzeigen.
3. Wählen Sie **Neue Föderation konfigurieren**.
4. Geben Sie Ihre Domänendetails ein:
 - a. Wählen Sie, ob Sie eine verifizierte Domäne oder Ihre E-Mail-Domäne verwenden möchten. Die E-Mail-Domäne ist die Domäne, die mit dem Konto verknüpft ist, mit dem Sie angemeldet sind.
 - b. Geben Sie den Namen der Föderation ein, die Sie konfigurieren.
 - c. Wenn Sie eine verifizierte Domäne auswählen, wählen Sie die Domäne aus der Liste aus.
5. Wählen Sie **Weiter**.
6. Wählen Sie als Verbindungsmethode **Protokoll** und dann **SAML-Identitätsanbieter**.
7. Wählen Sie **Weiter**.
8. Konfigurieren Sie Ihren SAML-Identitätsanbieter so, dass er NetApp als Dienstanbieter vertraut. Sie müssen diesen Schritt auf dem Server Ihres SAML-Anbieters ausführen.
 - a. Stellen Sie sicher, dass Ihr IdP das Attribut `email` auf die E-Mail-Adresse des Benutzers eingestellt. Dies ist erforderlich, damit die Konsole Benutzer korrekt identifizieren kann:

```
<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. Verwenden Sie die folgenden Werte, wenn Sie Ihre SAML-Anwendung bei der Konsole registrieren:
 - Für die **Antwort-URL** oder **Assertion Consumer Service (ACS)-URL** verwenden Sie <https://netapp-cloud-account.auth0.com/login/callback>
 - Verwenden Sie für die **Abmelde-URL** <https://netapp-cloud-account.auth0.com/logout>
 - Verwenden Sie für **Zielgruppen-/Entitäts-ID** `urn:auth0:netapp-cloud-account:<fed-domain-name-saml>` wobei `<fed-domain-name-saml>` der Domänenname ist, den Sie für die Föderation verwenden möchten. Wenn Ihre Domäne beispielsweise `example.com`, wäre die Zielgruppen-/Entitäts-ID `urn:auth0:netapp-cloud-account:fed-example-com-samlp`.
2. Kopieren Sie nach dem Erstellen des Vertrauens die folgenden Werte vom Server Ihres SAML-Anbieters:
 - Anmelde-URL
 - Abmelde-URL (optional)
3. Laden Sie das X.509-Zertifikat vom Server Ihres SAML-Anbieters herunter. Es muss im PEM-, CER- oder CRT-Format vorliegen.
 - a. Kehren Sie zur Konsole zurück und wählen Sie **Weiter**, um die Verbindung herzustellen.
 - b. Stellen Sie die Verbindung mit SAML her.
4. Geben Sie die **Anmelde-URL** Ihres SAML-Servers ein.
5. Laden Sie das X.509-Zertifikat hoch, das Sie vom Server Ihres SAML-Anbieters heruntergeladen haben.
6. Geben Sie optional die **Abmelde-URL** Ihres SAML-Servers ein.
 - a. Wählen Sie **Verbindung erstellen**. Das System stellt die Verbindung in wenigen Sekunden her.
 - b. Wählen Sie **Weiter**.
 - c. Wählen Sie **Verbindung testen**, um Ihre Verbindung zu testen. Sie werden zu einer Anmeldeseite für Ihren IdP-Server weitergeleitet. Melden Sie sich mit Ihren IdP-Zugangsdaten an. Nach dem Einloggen müssen Sie zur Konsole zurückkehren, um die Verbindung zu aktivieren.



Wenn Sie die Konsole im eingeschränkten Modus verwenden, kopieren Sie die URL entweder in ein Inkognito-Browserfenster oder in einen separaten Browser, um sich bei Ihrem Identitätsanbieter anzumelden.

- d. Wählen Sie in der Konsole **Weiter**, um die Zusammenfassungsseite anzuzeigen.
- e. Benachrichtigungen einrichten.

Sie haben die Wahl zwischen sieben Tagen oder 30 Tagen. Das System versendet E-Mail-

Benachrichtigungen über das Ablaufdatum und zeigt diese in der Konsole allen Benutzern mit den folgenden Rollen an: Super-Admin, Organisations-Admin, Verbund-Admin und Verbund-Viewer.

- f. Überprüfen Sie die Föderationsdetails und wählen Sie dann **Föderation aktivieren**.
- g. Wählen Sie **Fertig**, um den Vorgang abzuschließen.

Nach der Aktivierung der Föderation melden sich die Benutzer mit ihren Unternehmensanmeldeinformationen bei der NetApp Console an.

Föderationen verwalten

Föderationen in der NetApp Console verwalten

Sie können Ihre Föderation in der NetApp Console verwalten. Sie können es deaktivieren, abgelaufene Anmeldeinformationen aktualisieren und es deaktivieren, wenn Sie es nicht mehr benötigen.

Erforderliche Rollen

Zum Erstellen und Verwalten von Föderationen ist die Rolle des Föderationsadministrators erforderlich. Der Federation-Viewer kann die Federation-Seite anzeigen. ["Erfahren Sie mehr über Zugriffsrollen."](#)

Sie können einer bestehenden Föderation auch eine zusätzliche verifizierte Domäne hinzufügen, wodurch Sie mehrere Domänen für Ihre föderierte Verbindung nutzen können.



- Wenn Sie die Föderation mit NetApp Cloud Central konfiguriert haben, importieren Sie sie über die Seite **Föderation**, um sie in der Konsole zu verwalten. ["Erfahren Sie, wie Sie Ihre Föderation importieren"](#)
- Auf der Seite „Überwachung“ können Sie Ereignisse der Föderationsverwaltung wie das Aktivieren, Deaktivieren und Aktualisieren von Föderationen einsehen. ["Erfahren Sie mehr über die Überwachung von Vorgängen in der NetApp Console."](#)

Aktivieren einer Föderation

Wenn Sie eine Föderation erstellt haben, diese aber nicht aktiviert ist, können Sie sie über die Seite **Föderation** aktivieren. Durch die Aktivierung einer Föderation können sich die mit der Föderation verknüpften Benutzer mit ihren Unternehmensanmeldeinformationen bei der Konsole anmelden. Erstellen und testen Sie die Föderation erfolgreich, bevor Sie sie aktivieren.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie die Registerkarte **Föderation** aus.
3. Wählen Sie das Aktionsmenü **...** neben der Föderation, die Sie aktivieren möchten, und wählen Sie **Aktivieren** aus.

Hinzufügen einer verifizierten Domäne zu einer vorhandenen Föderation

Sie können einer vorhandenen Föderation in der Konsole eine verifizierte Domäne hinzufügen, um mehrere Domänen mit demselben Identitätsanbieter (IdP) zu verwenden.

Sie müssen die Domäne bereits in der Konsole verifiziert haben, bevor Sie sie zu einer Föderation hinzufügen

können. Wenn Sie die Domäne noch nicht verifiziert haben, können Sie dies tun, indem Sie die Schritte in ["Überprüfen Sie Ihre Domäne in der Konsole"](#) .

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie die Registerkarte **Föderation** aus.
3. Wählen Sie das Aktionsmenü neben dem Verbund, dem Sie eine verifizierte Domäne hinzufügen möchten, und wählen Sie **Domänen aktualisieren** aus. Im Dialogfeld **Domänen aktualisieren** wird die Domäne angezeigt, die bereits mit dieser Föderation verknüpft ist.
4. Wählen Sie eine verifizierte Domäne aus der Liste der verfügbaren Domänen aus.
5. Wählen Sie **Aktualisieren**. Neue Domänenbenutzer können innerhalb von 30 Sekunden föderierten Konsolenzugriff erhalten.

Aktualisieren einer ablaufende Verbundverbindung

Sie können die Details einer Föderation in der Konsole aktualisieren. Sie müssen beispielsweise die Föderation aktualisieren, wenn Anmeldeinformationen wie ein Zertifikat oder ein Client-Geheimnis ablaufen. Aktualisieren Sie bei Bedarf das Benachrichtigungsdatum, um Sie daran zu erinnern, die Verbindung zu aktualisieren, bevor sie abläuft.



Aktualisieren Sie zuerst die Konsole, bevor Sie Ihren IdP aktualisieren, um Anmeldeprobleme zu vermeiden. Bleiben Sie während des Vorgangs bei der Konsole angemeldet.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie die Registerkarte **Föderation** aus.
3. Wählen Sie das Aktionsmenü (drei vertikale Punkte) neben der Föderation, die Sie aktualisieren möchten, und wählen Sie **Föderation aktualisieren**.
4. Aktualisieren Sie die Details der Föderation nach Bedarf.
5. Wählen Sie **Aktualisieren**.

Testen einer vorhandenen Föderation

Testen Sie die Verbindung einer vorhandenen Föderation, um sicherzustellen, dass sie funktioniert. Auf diese Weise können Sie etwaige Probleme mit der Föderation erkennen und beheben.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie die Registerkarte **Föderation** aus.
3. Wählen Sie das Aktionsmenü neben dem Verbund, dem Sie eine verifizierte Domäne hinzufügen möchten, und wählen Sie **Verbindung testen** aus.
4. Wählen Sie **Test**. Das System fordert Sie auf, sich mit Ihren Unternehmensanmeldeinformationen anzumelden. Wenn die Verbindung erfolgreich ist, werden Sie zur NetApp Console weitergeleitet. Wenn die Verbindung fehlschlägt, wird eine Fehlermeldung angezeigt, die auf das Problem mit der Föderation hinweist.
5. Wählen Sie **Fertig**, um zur Registerkarte **Föderation** zurückzukehren.

Deaktivieren einer Föderation

Wenn Sie eine Föderation nicht mehr benötigen, können Sie sie deaktivieren. Dadurch wird verhindert, dass sich mit der Föderation verknüpfte Benutzer mit ihren Unternehmensanmeldeinformationen bei der Konsole anmelden. Sie können die Föderation bei Bedarf später wieder aktivieren.

Deaktivieren Sie eine Föderation, bevor Sie sie löschen, beispielsweise wenn Sie den IdP außer Betrieb nehmen oder die Föderation beenden. Auf diese Weise können Sie es bei Bedarf später wieder aktivieren.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie die Registerkarte **Föderation** aus.
3. Wählen Sie das Aktionsmenü neben dem Verbund, dem Sie eine verifizierte Domäne hinzufügen möchten, und wählen Sie **Deaktivieren** aus.

Löschen einer Föderation

Wenn Sie eine Föderation nicht mehr benötigen, können Sie sie löschen. Dadurch wird die Föderation entfernt und alle mit der Föderation verknüpften Benutzer können sich nicht mehr mit ihren Unternehmensanmeldeinformationen bei der Konsole anmelden. Beispielsweise, wenn der IdP außer Betrieb genommen wird oder die Föderation nicht mehr benötigt wird.

Sie können eine Föderation nicht wiederherstellen, nachdem Sie sie gelöscht haben. Sie müssen eine neue Föderation erstellen.



Sie müssen eine Föderation deaktivieren, bevor Sie sie löschen können. Sie können eine Föderation nach dem Löschen nicht wiederherstellen.

Schritte

1. Wählen Sie **Administration > Identität und Zugriff**.
2. Wählen Sie **Föderationen** aus, um die Seite **Föderationen** anzuzeigen.
3. Wählen Sie das Aktionsmenü neben dem Verbund, dem Sie eine verifizierte Domäne hinzufügen möchten, und wählen Sie **Löschen** aus.

Importieren Sie Ihre Föderation in die NetApp Console

Wenn Sie zuvor die Föderation über NetApp Cloud Central (eine externe Anwendung der NetApp Console) eingerichtet haben, werden Sie auf der Föderationsseite aufgefordert, Ihre vorhandene föderierte Verbindung in die Konsole zu importieren, damit Sie sie in der neuen Schnittstelle verwalten können. Sie können dann die neuesten Verbesserungen nutzen, ohne Ihre Verbundverbindung neu erstellen zu müssen.



Nachdem Sie Ihre vorhandene Föderation importiert haben, können Sie die Föderation auf der Seite **Föderationen** verwalten. ["Erfahren Sie mehr über die Verwaltung von Föderationen."](#)

Erforderliche Rolle

Organisationsadministrator oder Föderationsadministrator. ["Erfahren Sie mehr über Zugriffsrollen."](#)

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie die Registerkarte **Föderation** aus.
3. Wählen Sie **Föderation importieren**.

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.