セキュリティとコンプライアンス

NetApp Console setup and administration

NetApp
February 26, 2026

This PDF was generated from https://docs.netapp.com/ja-jp/console-setup-admin/concept-federation.html on February 26, 2026. Always check docs.netapp.com for the latest.

目次

セキュリティとコンプライアンス

アイデンティティ連携

NetApp ConsoleでIDフェデレーションを使用してシングルサインオンを有効にする

シングル サインオン (フェデレーション) により、ユーザーは企業の認証情報を使用してNetApp Consoleにログインできるため、ログイン プロセスが簡素化され、セキュリティが強化されます。アイデンティティ プロバイダー (IdP) またはNetAppサポート サイトを使用してシングル サインオン (SSO) を有効にできます。

フェデレーションは、NetApp Consoleがプライベート モードの場合は使用できません。"NetApp Console モードの詳細"。

必要な役割

組織管理者、フェデレーション管理者、フェデレーション閲覧者。"アクセス ロールの詳細について説明します。"

NetApp Support Site でのシングルサインオン

NetAppサポート サイトと連携すると、ユーザーは同じ資格情報を使用してコンソール、 Active IQ Digital Advisor、およびその他の関連アプリケーションにログインできるようになります。

NetAppサポート サイトと連携する場合、企業の ID 管理プロバイダーとも連携することはできません。組織に最適なものを選択してください。

手順

1. ダウンロードして完了 "NetAppフェデレーション リクエスト フォーム"。
2. フォームに指定されたメールアドレスにフォームを送信します。

   NetAppサポート チームがお客様のリクエストを確認し、処理します。

IDプロバイダーによるシングルサインオン

コンソールのシングル サインオン (SSO) を有効にするには、ID プロバイダーとのフェデレーション接続を設定できます。このプロセスでは、 NetApp をサービス プロバイダーとして信頼するように ID プロバイダーを構成し、コンソールで接続を作成します。

以前にNetApp Cloud Central (コンソールの外部アプリケーション) を使用してフェデレーションを構成した場合は、コンソール内でフェデレーションを管理するために、フェデレーション ページを使用してフェデレーションをインポートする必要があります。"フェデレーションをインポートする方法を学びます。"

サポートされているIDプロバイダー

NetApp は、フェデレーション用に次のプロトコルと ID プロバイダーをサポートしています。

プロトコル

- セキュリティアサーションマークアップ言語（SAML）IDプロバイダー
- アクティブ ディレクトリ フェデレーション サービス (AD FS)

アイデンティティプロバイダー

- Microsoft Entra ID
- PingFederate

NetApp Consoleワークフローとの連携

NetApp は、サービス プロバイダー開始 (SP開始) SSO のみをサポートします。まず、 NetApp をサービス プロバイダーとして信頼するように ID プロバイダーを構成する必要があります。次に、コンソールで ID プロバイダーの構成を使用する接続を作成できます。

自分のメールドメインまたは自分が所有する別のドメインと連携できます。メール ドメインとは異なるドメインとフェデレーションするには、まずそのドメインを所有していることを確認します。

1 ドメインを確認する（メールドメインを使用していないとき）

メール ドメインとは異なるドメインとフェデレーションするには、そのドメインを所有していることを確認します。追加の手順なしで電子メールドメインを統合できます。

2 **IdP** を設定して、 **NetApp** をサービス プロバイダーとして信頼します。

新しいアプリケーションを作成し、ACS URL、エンティティ ID、その他の資格情報などの詳細を指定して、NetAppを信頼するように ID プロバイダーを構成します。サービス プロバイダー情報は ID プロバイダーによって異なるため、詳細については特定の ID プロバイダーのドキュメントを参照してください。この手順を完了するには、IdP 管理者と協力する必要があります。

3 コンソールでフェデレーション接続を作成する

接続を作成するには、ID プロバイダーからの SAML メタデータ URL またはファイルを指定します。この情報は、コンソールと ID プロバイダー間の信頼関係を確立するために使用されます。提供する情報は、使用している IdP によって異なります。たとえば、Microsoft Entra ID を使用している場合は、クライアント ID、シークレット、ドメインを指定する必要があります。

4 コンソールでフェデレーションをテストする

フェデレーション接続を有効にする前にテストしてください。コンソールのフェデレーション ページのテスト オプションを使用して、テスト ユーザーが正常に認証できることを確認します。テストが成功した場合は、接続を有効にできます。

5 コンソールで接続を有効にする

接続を有効にすると、ユーザーは企業の資格情報を使用してコンソールにログインできるようになります。

開始するには、それぞれのプロトコルまたは IdP のトピックを確認してください。

- "AD FSとのフェデレーション接続を設定する"
- "Microsoft Entra ID とのフェデレーション接続を設定する"
- "PingFederateでフェデレーション接続を設定する"
- "SAML ID プロバイダとのフェデレーション接続を設定する"

ドメイン検証

フェデレーション接続のメールドメインを確認する

電子メール ドメインとは異なるドメインとフェデレーションを行う場合は、まずそのドメインを所有していることを確認する必要があります。フェデレーションには検証済みのドメインのみを使用できます。

必要な役割

フェデレーションを作成および管理するには、フェデレーション管理者ロールが必要です。フェデレーションビューアーはフェデレーション ページを表示できます。"アクセス ロールの詳細について説明します。"

ドメインを確認するには、ドメインの DNS 設定に TXT レコードを追加する必要があります。このレコードは、ドメインを所有していることを証明するために使用され、 NetApp Consoleがフェデレーションのためにドメインを信頼できるようにします。この手順を完了するには、IT またはネットワーク管理者との調整が必要になる場合があります。

手順

1. *管理 > IDとアクセス*を選択します。
2. **Federation** ページを表示するには、**Federation** を選択します。
3. *新しいフェデレーションの構成*を選択します。
4. *ドメインの所有権を確認*を選択します。
5. 検証するドメインを入力し、「続行」を選択します。
6. 提供された TXT レコードをコピーします。
7. ドメインの DNS 設定に移動し、ドメインの TXT レコードとして提供された TXT 値を設定します。必要に応じて、IT 管理者またはネットワーク管理者と協力してください。
8. TXT レコードが追加されたら、コンソールに戻り、[検証] を選択します。

フェデレーションを構成する

NetApp Consoleを**Active Directory** フェデレーション サービス **(AD FS)** と連携する

Active Directory フェデレーション サービス (AD FS) をNetApp Consoleと連携させて、NetApp Consoleのシングル サインオン (SSO) を有効にします。これにより、ユーザーは企業の資格情報を使用してコンソールにログインできるようになります。

必要な役割

フェデレーションを作成および管理するには、フェデレーション管理者ロールが必要です。フェデレーションビューアーはフェデレーション ページを表示できます。"アクセス ロールの詳細について説明します。"

企業の IdP またはNetAppサポート サイトと連携できます。 NetApp、両方ではなく、どちらか一方を選択することを推奨しています。

NetApp は、サービス プロバイダー開始 (SP開始) SSO のみをサポートします。まず、 NetApp Consoleをサービス プロバイダーとして信頼するように ID プロバイダーを構成します。次に、ID プロバイダーの構成を使用してコンソールで接続を作成します。

AD FS サーバーとのフェデレーションを設定して、 NetApp Consoleのシングル サインオン (SSO) を有効にすることができます。このプロセスでは、コンソールをサービス プロバイダーとして信頼するように AD FS を構成し、 NetApp Consoleで接続を作成します。

手順

1. *管理 > IDとアクセス*を選択します。
2. **Federation** ページを表示するには、**Federation** を選択します。
3. *新しいフェデレーションの構成*を選択します。
4. ドメインの詳細を入力してください:
   a. 検証済みドメインを使用するか、メールドメインを使用するかを選択します。電子メール ドメインは、ログインしているアカウントに関連付けられているドメインです。
   b. 構成するフェデレーションの名前を入力します。
   c. 検証済みのドメインを選択する場合は、リストからドメインを選択します。
5. *次へ*を選択します。
6. 接続方法として、[プロトコル] を選択し、[**Active Directory** フェデレーション サービス **(AD FS)**] を選択します。
7. *次へ*を選択します。
8. AD FS サーバーに証明書利用者信頼を作成します。 PowerShell を使用することも、AD FS サーバー上で手動で構成することもできます。証明書利用者信頼を作成する方法の詳細については、AD FS のドキュメントを参照してください。
   a. 次のスクリプトを使用して PowerShell を使用して信頼を作成します。

```
(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. または、AD FS 管理コンソールで信頼を手動で作成することもできます。信頼を作成するときは、次のNetApp Consoleの値を使用します。
      - 信頼信頼識別子を作成するときは、**YOUR_TENANT** 値を使用します。 `netapp-cloud-account`
      - **WS-Federation** のサポートを有効にする を選択した場合は、**YOUR_AUTH0_DOMAIN** 値を使用します。 `netapp-cloud-account.auth0.com`

c. 信頼を作成した後、AD FS サーバーからメタデータ URL をコピーするか、フェデレーション メタデータ ファイルをダウンロードします。コンソールで接続を完了するには、この URL またはファイルが必要になります。

NetApp、メタデータ URL を使用してNetApp Consoleが最新の AD FS 構成を自動的に取得できるようにすることをお勧めします。フェデレーション メタデータ ファイルをダウンロードした場合は、AD FS 構成に変更があるたびに、 NetApp Consoleで手動で更新する必要があります。

9. コンソールに戻り、[次へ] を選択して接続を作成します。
10. AD FS との接続を作成します。
    a. 前の手順で AD FS サーバーからコピーした **AD FS URL** を入力するか、AD FS サーバーからダウンロードしたフェデレーション メタデータ ファイルをアップロードします。
11. *接続を作成*を選択します。接続の作成には数秒かかる場合があります。
12. *次へ*を選択します。
13. 接続をテストするには、[接続テスト] を選択します。IdP サーバーのログイン ページに移動します。IdP のクレデンシャルを使用してログインします。ログイン後、コンソールに戻って接続を有効にします。

    コンソールを制限モードで使用する場合は、URL をシークレット ブラウザ ウィンドウまたは別のブラウザにコピーして IdP にログインします。

14. コンソールで、[次へ] を選択して概要ページを確認します。
15. 通知を設定します。

    7日間または30日間を選択します。システムは、スーパー管理者、組織管理者、フェデレーション管理者、フェデレーション閲覧者の役割を持つすべてのユーザーに有効期限通知を電子メールで送信し、コンソールに表示します。

16. フェデレーションの詳細を確認し、[フェデレーションを有効にする] を選択します。
17. プロセスを完了するには、[完了] を選択します。

フェデレーションを有効にすると、ユーザーは企業の資格情報を使用してNetApp Consoleにログインします。

NetApp Consoleを**Microsoft Entra ID** と連携する

Microsoft Entra ID IdP プロバイダーと連携して、 NetApp Consoleのシングル サインオン (SSO) を有効にします。これにより、ユーザーは企業の資格情報を使用してログインできるようになります。

必要な役割

フェデレーションを作成および管理するには、フェデレーション管理者ロールが必要です。フェデレーション ビューアーはフェデレーション ページを表示できます。"アクセス ロールの詳細について説明します。"

企業の IdP またはNetAppサポート サイトと連携できます。 NetApp、両方ではなく、どちらか一方を選択することを推奨しています。

NetApp は、サービス プロバイダー開始 (SP開始) SSO のみをサポートします。まず、 NetApp をサービス プロバイダーとして信頼するように ID プロバイダーを構成する必要があります。次に、コンソールで ID プロ

バイダーの構成を使用する接続を作成できます。

Microsoft Entra ID とのフェデレーション接続を設定して、コンソールのシングル サインオン (SSO) を有効にすることができます。このプロセスでは、コンソールをサービス プロバイダーとして信頼するように Microsoft Entra ID を構成し、コンソールで接続を作成します。

手順

1. *管理 > IDとアクセス*を選択します。
2. **Federation** ページを表示するには、**Federation** を選択します。
3. *新しいフェデレーションの構成*を選択します。

ドメインの詳細

1. ドメインの詳細を入力してください:
   a. 検証済みドメインを使用するか、メールドメインを使用するかを選択します。電子メール ドメインは、ログインしているアカウントに関連付けられているドメインです。
   b. 構成するフェデレーションの名前を入力します。
   c. 検証済みのドメインを選択する場合は、リストからドメインを選択します。
2. *次へ*を選択します。

接続方法

1. 接続方法として、*プロバイダー*を選択し、*Microsoft Entra ID*を選択します。
2. *次へ*を選択します。

設定手順

1. NetApp をサービス プロバイダーとして信頼するように Microsoft Entra ID を構成します。この手順は Microsoft Entra ID サーバーで実行する必要があります。
   a. コンソールを信頼するには、Microsoft Entra ID アプリを登録するときに次の値を使用します。
      - *リダイレクトURL*には、 `https://services.cloud.netapp.com`
      - *返信URL*には、 `https://netapp-cloud-account.auth0.com/login/callback`
   b. Microsoft Entra ID アプリのクライアント シークレットを作成します。フェデレーションを完了するには、クライアント ID、クライアント シークレット、Entra ID ドメイン名を提供する必要があります。
2. コンソールに戻り、[次へ] を選択して接続を作成します。

接続を作成

1. Microsoft Entra IDで接続を作成する
   a. 前の手順で作成したクライアント ID とクライアント シークレットを入力します。
   b. Microsoft Entra ID ドメイン名を入力します。
2. *接続を作成*を選択します。システムは数秒で接続を作成します。

接続をテストして有効にする

1. *次へ*を選択します。
2. 接続をテストするには、[接続テスト] を選択します。IdP サーバーのログイン ページに移動します。IdP のクレデンシャルを使用してログインします。ログイン後、コンソールに戻って接続を有効にします。

   コンソールを制限モードで使用する場合は、URL をシークレット ブラウザ ウィンドウまたは別のブラウザにコピーして IdP にログインします。

3. コンソールで、[次へ] を選択して概要ページを確認します。
4. 通知を設定します。

   7日間または30日間を選択します。システムは、スーパー管理者、組織管理者、フェデレーション管理者、フェデレーション閲覧者の役割を持つすべてのユーザーに有効期限通知を電子メールで送信し、コンソールに表示します。

5. フェデレーションの詳細を確認し、[フェデレーションを有効にする] を選択します。
6. プロセスを完了するには、[完了] を選択します。

フェデレーションを有効にすると、ユーザーは企業の資格情報を使用してNetApp Consoleにログインします。

PingFederateで**NetApp Console**を連携

PingFederate IdP プロバイダーと連携して、 NetApp Consoleのシングル サインオン (SSO) を有効にします。これにより、ユーザーは企業の資格情報を使用してログインできるようになります。

必要な役割

フェデレーションを作成および管理するには、フェデレーション管理者ロールが必要です。フェデレーション ビューアーはフェデレーション ページを表示できます。"アクセス ロールの詳細について説明します。"

企業の IdP またはNetAppサポート サイトと連携できます。 NetApp、両方ではなく、どちらか一方を選択することを推奨しています。

NetApp は、サービス プロバイダー開始 (SP開始) SSO のみをサポートします。まず、 NetApp をサービス プロバイダーとして信頼するように ID プロバイダーを構成する必要があります。次に、コンソールで ID プロバイダーの構成を使用する接続を作成できます。

PingFederate とのフェデレーション接続を設定して、コンソールのシングル サインオン (SSO) を有効にすることができます。このプロセスでは、コンソールをサービス プロバイダーとして信頼するように PingFederate サーバーを構成し、コンソールで接続を作成します。

手順

1. *管理 > IDとアクセス*を選択します。
2. **Federation** ページを表示するには、**Federation** を選択します。
3. *新しいフェデレーションの構成*を選択します。
4. ドメインの詳細を入力してください:
   a. 検証済みドメインを使用するか、メールドメインを使用するかを選択します。電子メール ドメイン

は、ログインしているアカウントに関連付けられているドメインです。

b. 構成するフェデレーションの名前を入力します。

c. 検証済みのドメインを選択する場合は、リストからドメインを選択します。

5. *次へ*を選択します。

6. 接続方法として、*プロバイダー*を選択し、次に*PingFederate*を選択します。

7. *次へ*を選択します。

8. PingFederate サーバーを、サービス プロバイダーとしてNetApp を信頼するように構成します。この手順は PingFederate サーバーで実行する必要があります。

a. PingFederate を構成してNetApp Consoleを信頼する場合は、次の値を使用します。

- *返信URL*または*アサーションコンシューマーサービス（ACS）URL*の場合は、`https://netapp-cloud-account.auth0.com/login/callback`
- *ログアウトURL*には、`https://netapp-cloud-account.auth0.com/logout`
- *オーディエンス/エンティティID*には、`urn:auth0:netapp-cloud-account:<fed-domain-name-saml>`ここで、`<fed-domain-name-pingfederate>` はフェデレーションのドメイン名です。たとえば、ドメインが `example.com`オーディエンス/エンティティIDは次のようになります。 `urn:auth0:netappcloud-account:fed-example-com-pingfederate`。

b. PingFederate サーバーの URL をコピーします。コンソールで接続を作成するときに、この URL が必要になります。

c. PingFederate サーバーから X.509 証明書をダウンロードします。 Base64 でエンコードされた PEM 形式 (.pem、.crt、.cer) である必要があります。

9. コンソールに戻り、[次へ] を選択して接続を作成します。

10. PingFederateで接続を作成する

a. 前の手順でコピーした PingFederate サーバーの URL を入力します。

b. X.509 署名証明書をアップロードします。証明書は PEM、CER、または CRT 形式である必要があります。

11. *接続を作成*を選択します。システムは数秒で接続を作成します。

12. *次へ*を選択します。

13. 接続をテストするには、[接続テスト] を選択します。IdP サーバーのログイン ページに移動します。IdP のクレデンシャルを使用してログインします。ログイン後、コンソールに戻って接続を有効にします。

コンソールを制限モードで使用する場合は、URL をシークレット ブラウザ ウィンドウまたは別のブラウザにコピーして IdP にログインします。

14. コンソールで、[次へ] を選択して概要ページを確認します。

15. 通知を設定します。

7日間または30日間を選択します。システムは、スーパー管理者、組織管理者、フェデレーション管理者、フェデレーション閲覧者の役割を持つすべてのユーザーに有効期限通知を電子メールで送信し、コンソールに表示します。

16. フェデレーションの詳細を確認し、[フェデレーションを有効にする] を選択します。
17. プロセスを完了するには、[完了] を選択します。

フェデレーションを有効にすると、ユーザーは企業の資格情報を使用してNetApp Consoleにログインします。

SAML ID プロバイダとの連携

SAML 2.0 IdP プロバイダーと連携して、NEtApp コンソールのシングル サインオン (SSO) を有効にします。これにより、ユーザーは企業の資格情報を使用してログインできるようになります。

必要な役割

フェデレーションを作成および管理するには、フェデレーション管理者ロールが必要です。フェデレーション ビューアーはフェデレーション ページを表示できます。"アクセス ロールの詳細について説明します。"

企業の IdP またはNetAppサポート サイトと連携できます。両方と連携することはできません。

NetApp は、サービス プロバイダー開始 (SP開始) SSO のみをサポートします。まず、 NetApp をサービス プロバイダーとして信頼するように ID プロバイダーを構成する必要があります。次に、コンソールで ID プロバイダーの構成を使用する接続を作成できます。

SAML 2.0 プロバイダーとのフェデレーション接続を設定して、コンソールのシングル サインオン (SSO) を有効にすることができます。このプロセスでは、プロバイダーがNetApp をサービス プロバイダーとして信頼するように構成し、コンソールで接続を作成します。

手順

1. *管理 > IDとアクセス*を選択します。
2. **Federation** ページを表示するには、**Federation** を選択します。
3. *新しいフェデレーションの構成*を選択します。
4. ドメインの詳細を入力してください:
    a. 検証済みドメインを使用するか、メールドメインを使用するかを選択します。電子メール ドメインは、ログインしているアカウントに関連付けられているドメインです。
    b. 構成するフェデレーションの名前を入力します。
    c. 検証済みのドメインを選択する場合は、リストからドメインを選択します。
5. *次へ*を選択します。
6. 接続方法として、*プロトコル*を選択し、*SAML ID プロバイダー*を選択します。
7. *次へ*を選択します。
8. SAML ID プロバイダーを構成して、 NetApp をサービス プロバイダーとして信頼します。この手順は SAML プロバイダー サーバーで実行する必要があります。
    a. IdPに属性があることを確認する `email`ユーザーのメールアドレスに設定されます。これは、コンソールがユーザーを正しく識別するために必要です。

```
<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. SAML アプリケーションをコンソールに登録するときは、次の値を使用します。
   - *返信URL*または*アサーションコンシューマーサービス（ACS）URL*の場合は、 https://netapp-cloud-account.auth0.com/login/callback
   - *ログアウトURL*には、 https://netapp-cloud-account.auth0.com/logout
   - *オーディエンス/エンティティID*には、 `urn:auth0:netapp-cloud-account:<fed-domain-name-saml>`ここで、<fed-domain-name-saml> はフェデレーションに使用するドメイン名です。たとえば、ドメインが `example.com`オーディエンス/エンティティIDは次のようになります。 `urn:auth0:netapp-cloud-account:fed-example-com-samlp`。
2. 信頼を作成したら、SAML プロバイダー サーバーから次の値をコピーします。
   - サインインURL
   - サインアウトURL（オプション）
3. SAML プロバイダー サーバーから X.509 証明書をダウンロードします。 PEM、CER、または CRT 形式である必要があります。
   a. コンソールに戻り、[次へ] を選択して接続を作成します。
   b. SAML を使用して接続を作成します。
4. SAML サーバーの サインイン **URL** を入力します。
5. SAML プロバイダー サーバーからダウンロードした X.509 証明書をアップロードします。
6. 必要に応じて、SAML サーバーの サインアウト **URL** を入力します。
   a. *接続を作成*を選択します。システムは数秒で接続を作成します。
   b. *次へ*を選択します。
   c. 接続をテストするには、[接続テスト] を選択します。IdP サーバーのログイン ページに移動します。IdPのクレデンシャルを使用してログインします。ログイン後、コンソールに戻って接続を有効にします。

      コンソールを制限モードで使用する場合は、URL をシークレット ブラウザ ウィンドウまたは別のブラウザにコピーして IdP にログインします。

   d. コンソールで、[次へ] を選択して概要ページを確認します。
   e. 通知を設定します。

7日間または30日間を選択します。システムは、スーパー管理者、組織管理者、フェデレーション管理者、フェデレーション閲覧者の役割を持つすべてのユーザーに有効期限通知を電子メールで送信し、コンソールに表示します。

f. フェデレーションの詳細を確認し、[フェデレーションを有効にする] を選択します。

g. プロセスを完了するには、[完了] を選択します。

フェデレーションを有効にすると、ユーザーは企業の資格情報を使用してNetApp Consoleにログインします。

フェデレーションの管理

NetApp Consoleでフェデレーションを管理する

NetApp Consoleでフェデレーションを管理できます。無効にしたり、期限切れの資格情報を更新したり、不要になった場合に無効にしたりすることができます。

必要な役割

フェデレーションを作成および管理するには、フェデレーション管理者ロールが必要です。フェデレーションビューアーはフェデレーション ページを表示できます。"アクセス ロールの詳細について説明します。"

既存のフェデレーションに検証済みのドメインを追加することもできます。これにより、フェデレーション接続に複数のドメインを使用できるようになります。

- NetApp Cloud Central を使用してフェデレーションを構成した場合は、フェデレーション ページからインポートして、コンソールで管理します。"フェデレーションをインポートする方法を学ぶ"
- 監査ページでは、フェデレーションの有効化、無効化、更新などのフェデレーション管理イベントを表示できます。 "NetApp Consoleでの操作の監視について詳しく学習します。"

フェデレーションを有効にする

フェデレーションを作成したが有効になっていない場合は、フェデレーション ページから有効にすることができます。フェデレーションを有効にすると、フェデレーションに関連付けられたユーザーは、企業の資格情報を使用してコンソールにログインできるようになります。フェデレーションを有効にする前に、フェデレーションを作成してテストしてください。

手順

1. *管理 > IDとアクセス*を選択します。
2. *Federation*タブを選択します。
3. アクションメニューを選択 ••• 有効にするフェデレーションの横にある をクリックし、[有効] を選択します。

検証済みのドメインを既存のフェデレーションに追加する

コンソールで既存のフェデレーションに検証済みのドメインを追加して、同じ ID プロバイダー (IdP) で複数のドメインを使用できます。

ドメインをフェデレーションに追加する前に、コンソールでドメインを検証しておく必要があります。ドメイ

ンをまだ確認していない場合は、以下の手順に従って確認することができます。"コンソールでドメインを確認する" 。

手順

1. *管理 > IDとアクセス*を選択します。
2. *Federation*タブを選択します。
3. アクションメニューを選択:検証済みドメインを追加するフェデレーションの横にある をクリックし、[ドメインの更新] を選択します。 ドメインの更新 ダイアログ ボックスには、このフェデレーションにすでに関連付けられているドメインが表示されます。
4. 利用可能なドメインのリストから検証済みのドメインを選択します。
5. *更新*を選択します。新しいドメイン ユーザーは、30 秒以内にフェデレーション コンソール アクセスを取得できます。

期限切れのフェデレーション接続の更新

コンソールでフェデレーションの詳細を更新できます。たとえば、証明書やクライアント シークレットなどの資格情報の有効期限が切れた場合は、フェデレーションを更新する必要があります。必要に応じて通知日を更新し、接続が期限切れになる前に更新するよう通知します。

ログインの問題を回避するには、IdP を更新する前にまずコンソールを更新してください。プロセス中はコンソールにログインしたままにしてください。

手順

1. *管理 > IDとアクセス*を選択します。
2. *Federation*タブを選択します。
3. 更新するフェデレーションの横にあるアクション メニュー (縦に並んだ 3 つのドット) を選択し、フェデレーションの更新 を選択します。
4. 必要に応じてフェデレーションの詳細を更新します。
5. *更新*を選択します。

既存のフェデレーションをテストする

既存のフェデレーションの接続をテストして、それが機能することを確認します。これにより、フェデレーションに関する問題を特定し、トラブルシューティングすることができます。

手順

1. *管理 > IDとアクセス*を選択します。
2. *Federation*タブを選択します。
3. アクションメニューを選択:検証済みドメインを追加するフェデレーションの横にある をクリックし、[テスト接続] を選択します。
4. *テスト*を選択します。システムは、企業の資格情報を使用してログインするように要求します。接続が成功すると、 NetApp Consoleにリダイレクトされます。接続に失敗した場合は、フェデレーションの問題を示すエラー メッセージが表示されます。
5. *完了*を選択して*連合*タブに戻ります。

フェデレーションを無効にする

フェデレーションが不要になった場合は、無効にすることができます。これにより、フェデレーションに関連付けられたユーザーが企業の資格情報を使用してコンソールにログインできなくなります。必要に応じて、後でフェデレーションを再度有効にすることができます。

IdP を廃止する場合やフェデレーションを中止する場合など、フェデレーションを削除する前に無効にします。これにより、必要に応じて後で再度有効にすることができます。

手順

1. *管理 > IDとアクセス*を選択します。
2. *Federation*タブを選択します。
3. アクションメニューを選択:検証済みドメインを追加するフェデレーションの横にある をクリックし、[無効にする] を選択します。

フェデレーションを削除する

フェデレーションが不要になった場合は、削除できます。これにより、フェデレーションが削除され、フェデレーションに関連付けられたすべてのユーザーが企業の資格情報を使用してコンソールにログインできなくなります。たとえば、IdP が廃止される場合や、フェデレーションが不要になった場合などです。

フェデレーションを削除した後は、回復することはできません。新しいフェデレーションを作成する必要があります。

フェデレーションを削除する前に無効にする必要があります。フェデレーションを削除した後で、元に戻すことはできません。

手順

1. *管理 > IDとアクセス*を選択します。
2. **Federations** ページを表示するには、**Federations** を選択します。
3. アクションメニューを選択:検証済みドメインを追加するフェデレーションの横にある をクリックし、[削除] を選択します。

NetApp Consoleにフェデレーションをインポートする

以前にNetApp Cloud Central (NetApp Consoleの外部アプリケーション) を通じてフェデレーションを設定したことがある場合は、フェデレーション ページで、既存のフェデレーション接続をコンソールにインポートして、新しいインターフェイスで管理できるようにするように求められます。そうすれば、フェデレーション接続を再作成しなくても、最新の拡張機能を活用できるようになります。

既存のフェデレーションをインポートした後、フェデレーション ページからフェデレーションを管理できます。"フェデレーションの管理について詳しく学びます。"

必要な役割

組織管理者またはフェデレーション管理者。"アクセス ロールの詳細について説明します。"

手順

1. *管理 > IDとアクセス*を選択します。
2. *Federation*タブを選択します。
3. *インポートフェデレーション*を選択します。

ONTAP Advanced View（ONTAP System Manager）のONTAP権限を適用する

デフォルトでは、コンソール エージェントの認証情報により、ユーザーは詳細ビュー (ONTAP System Manager) にアクセスできます。代わりに、ユーザーにONTAP認証情報の入力を求めることもできます。これにより、ユーザーが Cloud Volumes ONTAP とONTAPオンプレミス クラスターの両方でONTAPクラスターを操作するときに、ユーザーのONTAP権限が確実に適用されます。

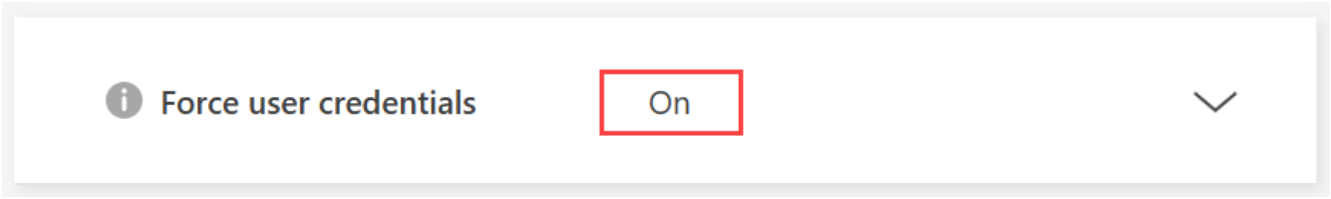
コンソール エージェントの設定を編集するには、組織管理者のロールが必要です。

手順

1. *管理 > エージェント*を選択します。
2. *概要*ページで、コンソール エージェントのアクション メニューを選択し、*エージェントの編集*を選択します。

   編集するには、コンソール エージェントがアクティブである必要があります。

3. *資格情報の強制*オプションを展開します。
4. *資格情報の強制*オプションを有効にするにはチェックボックスをオンにして、*保存*を選択します。
5. *資格情報の強制*オプションが有効になっていることを確認します。



NetApp Console組織の読み取り専用モードを有効にする

セキュリティ上の予防措置として、 NetApp Console組織に対して読み取り専用モードを有効にすることができます。読み取り専用モードでは、ユーザーはリソースと設定を表示できますが、変更することはできません。

読み取り専用モードでは、管理者ロールを持つユーザーは変更を行うために手動で権限を昇格する必要があり、これにより変更が意図的なものであることが保証されます。

読み取り専用モードは、NetApp Console がプライベート モードの場合は使用できません。"NetApp Console モードの詳細"。

必要なアクセスロール

スーパー管理者または組織管理者。

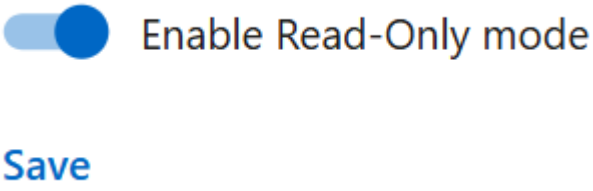
コンソール組織で読み取り専用モードを有効にする

コンソール組織への変更を制限するには、読み取り専用モードを有効にします。すべてのユーザーは引き続きリソースを表示できます。管理者ロールを持つユーザーは、権限を手動で昇格させなければ、コンソールでアクションを実行することはできません。

読み取り専用モードが有効になっている場合、組織が読み取り専用モードであることを通知するバナーがユーザーに表示されます。ユーザーは、役割を昇格するにはユーザー設定に移動する必要があります。

手順

1. *管理 > IDとアクセス*を選択します。
2. *組織*タブから、読み取り専用モードに設定する組織の*組織設定の編集*を選択します。
3. *読み取り専用モード*セクションで、トグルを*オン*の位置に移動して読み取り専用モードを有効にし、*保存*を選択します。



NetApp Consoleに初期組織管理者としてサインアップする

会社にNetApp Console組織がない場合は、サインアップして作成してください。最初のユーザーは管理者であり、アカウントと権限を管理します。後でロールを更新したり、管理者を追加したりできます。

手順

1. ウェブブラウザを開いて、 "NetApp Console"
2. NetApp Support Siteのアカウントをお持ちの場合は、ログイン ページでアカウントに関連付けられている電子メール アドレスを直接入力します。

   コンソールは、この最初のログインの一部として、NetApp Support Siteの資格情報を使用してサインアップします。

3. コンソール ログインを作成してサインアップする場合は、[サインアップ] を選択します。
   a. *サインアップ*ページで必要な情報を入力し、*次へ*を選択します。

      サインアップフォームでは英語の文字のみ使用できます。

   b. 受信トレイで、電子メール アドレスを確認するための手順が記載されたNetAppからの電子メールを確認してください。

      サインアップを完了するには、メールアドレスを確認してください。

4. ログイン後、エンドユーザー使用許諾契約書を確認して同意します。
5. *ようこそ*ページで組織を作成します。
6. *始めましょう*を選択します。

+ 初めての管理者は、ガイド付きのプロセスに従ってストレージの追加、コンソール エージェントの作成などを行います。 "コンソール アシスタントの使用について説明します。"

次のステップ

管理者は、コンソール アシスタントに含まれる手順を完了した後、ID とアクセス戦略を計画し、組織にユーザーを追加し、ロールを割り当てる必要があります。 "NetApp ConsoleのIDとアクセス管理について学ぶ"

組織がすでに存在する場合は、 NetApp Consoleにサインアップまたはログインしてください

会社にすでにNetApp Console組織がある場合は、サインアップまたはログインしてアクセスしてください。サインアップまたはログインの方法は、会社が ID フェデレーションを使用しているか、 NetApp Support Site の認証情報を持っているかによって異なります。そうでない場合は、 NetApp Consoleログインを作成します。

手順

1. ウェブブラウザを開いて、 "NetApp Console"
2. NetApp Support Siteのアカウントをお持ちの場合、または会社でシングル サインオン(SSO) を設定している場合は、[ログイン] ページに関連付けられている電子メール アドレスまたは SSO 資格情報を入力します。指示に従ってログインを完了してください。

   どちらの場合も、最初のログインの一環としてコンソールにサインアップされます。
3. コンソール ログインを作成してサインアップする場合は、[サインアップ] を選択します。
   a. *サインアップ*ページで必要な情報を入力し、*次へ*を選択します。

      サインアップフォームでは英語の文字のみ使用できます。

   b. 受信トレイで、電子メール アドレスを確認するための手順が記載されたNetAppからの電子メールを確認してください。

      サインアップを完了するには、メールアドレスを確認してください。
4. ログイン後、エンドユーザー使用許諾契約書を確認して同意します。
5. システムから組織の作成を求められた場合は、ダイアログ ボックスを閉じてコンソール管理者に伝え、コンソール組織に追加してアクセス権を付与してもらいます。 "組織管理者に連絡する方法について説明します。"

次のステップ

組織へのアクセス権が付与されると、ストレージの管理と割り当てられたデータ サービスの使用を開始できます。

著作権に関する情報

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用権を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用権については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、http://www.netapp.com/TMに記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。