Seguridad y cumplimiento

NetApp Console setup and administration

NetApp
February 11, 2026

Tabla de contenidos

Seguridad y cumplimiento . . . 1
- Federación de identidades . . . 1
  - Habilite el inicio de sesión único mediante la federación de identidades con la NetApp Console . . . 1
  - Verificación de dominio . . . 3
  - Configurar federaciones . . . 3
  - Administrar federaciones . . . 10
- Aplicar permisos de ONTAP para la Vista avanzada de ONTAP (Administrador del sistema ONTAP) . . . 13
- Habilitar el modo de solo lectura para una organización de NetApp Console . . . 14
  - Habilite el modo de solo lectura para su organización de la consola . . . 14
  - Regístrese en NetApp Console como administrador inicial de la organización . . . 15
  - Regístrese o inicie sesión en la NetApp Console cuando ya exista una organización . . . 15

Seguridad y cumplimiento

Federación de identidades

Habilite el inicio de sesión único mediante la federación de identidades con la NetApp Console

El inicio de sesión único (federación) simplifica el proceso de inicio de sesión y mejora la seguridad al permitir que los usuarios inicien sesión en la NetApp Console con sus credenciales corporativas. Puede habilitar el inicio de sesión único (SSO) con su proveedor de identidad (IdP) o con el sitio de soporte de NetApp .

Rol requerido

Administrador de la organización, administrador de la federación, visor de la federación."Obtenga más información sobre los roles de acceso."

Inicio de sesión único con NetApp Support Site

La federación con el sitio de soporte de NetApp permite a los usuarios iniciar sesión en la consola, Active IQ Digital Advisor y otras aplicaciones asociadas utilizando las mismas credenciales.

> Si se federa con el sitio de soporte de NetApp , no podrá federarse también con su proveedor de gestión de identidad corporativa. Elija cuál funciona mejor para su organización.

Pasos

1. Descargue y complete el "Formulario de solicitud de federación de NetApp" .
2. Envíe el formulario a la dirección de correo electrónico especificada en el formulario.

   El equipo de soporte de NetApp revisa y procesa su solicitud.

Inicio de sesión único con tu proveedor de identidades

Puede configurar una conexión federada con su proveedor de identidad para habilitar el inicio de sesión único (SSO) para la consola. El proceso implica configurar su proveedor de identidad para que confíe en NetApp como proveedor de servicios y luego crear la conexión en la consola.

> Si anteriormente configuró la federación usando NetApp Cloud Central (una aplicación externa a la consola), debe importar su federación usando la página Federación para administrarla dentro de la consola."Aprenda cómo importar su federación."

Proveedores de identidad compatibles

NetApp admite los siguientes protocolos y proveedores de identidad para la federación:

Protocolos

- Proveedores de identidad de lenguaje de marcado de aserción de seguridad (SAML)
- Servicios de federación de Active Directory (AD FS)

Proveedores de identidad

- Identificador de Microsoft Entra
- Federación de ping

Flujo de trabajo de la Federación con la NetApp Console

NetApp solo admite el inicio de sesión único (SSO) iniciado por el proveedor de servicios (SP). Primero debe configurar el proveedor de identidad para confiar en NetApp como proveedor de servicios. Luego, puede crear una conexión en la consola que utilice la configuración del proveedor de identidad.

Puedes federarlo con tu dominio de correo electrónico o con un dominio diferente que sea de tu propiedad. Para federarse con un dominio diferente de su dominio de correo electrónico, primero verifique que usted es el propietario del dominio.

Verifica tu dominio (si no utilizas tu dominio de correo electrónico)

Para federarse con un dominio diferente a su dominio de correo electrónico, verifique que sea su propietario. Puede federar su dominio de correo electrónico sin realizar pasos adicionales.

Configure su IdP para confiar en NetApp como proveedor de servicios

Configure su proveedor de identidad para que confíe en NetApp creando una nueva aplicación y proporcionando detalles como la URL de ACS, el ID de entidad u otra información de credenciales. La información del proveedor de servicios varía según el proveedor de identidad, por lo que consulte la documentación de su proveedor de identidad específico para obtener más detalles. Necesitará trabajar con el administrador de su IdP para completar este paso.

Crear la conexión federada en la consola

Proporcione la URL o el archivo de metadatos SAML de su proveedor de identidad para crear la conexión. Esta información se utiliza para establecer la relación de confianza entre la consola y su proveedor de identidad. La información que proporciones dependerá del IdP que estés utilizando. Por ejemplo, si utiliza Microsoft Entra ID, deberá proporcionar el ID de cliente, el secreto y el dominio.

Pruebe su federación en la consola

Pruebe su conexión federada antes de habilitarla. Utilice la opción de prueba en la página Federación en la Consola para verificar que su usuario de prueba pueda autenticarse correctamente. Si la prueba es exitosa, puedes habilitar la conexión.

Habilite su conexión en la Consola

Después de habilitar la conexión, los usuarios pueden iniciar sesión en la consola utilizando sus credenciales corporativas.

Revise el tema de su respectivo protocolo o IdP para comenzar:

- "Configurar una conexión federada con AD FS"
- "Configurar una conexión federada con Microsoft Entra ID"

- "Configurar una conexión federada con PingFederate"
- "Configurar una conexión federada con un proveedor de identidad SAML"

Verificación de dominio

Verifique el dominio de correo electrónico para su conexión federada

Si desea federarse con un dominio diferente a su dominio de correo electrónico, primero debe verificar que es el propietario del dominio. Sólo se pueden utilizar dominios verificados para la federación.

Roles requeridos

El rol de administrador de la federación es necesario para crear y administrar federaciones. El espectador de la Federación puede ver la página de la Federación."Obtenga más información sobre los roles de acceso."

Para verificar su dominio es necesario agregar un registro TXT a la configuración de DNS de su dominio. Este registro se utiliza para demostrar que usted es el propietario del dominio y permite que la NetApp Console confíe en el dominio para la federación. Es posible que necesite coordinar con su administrador de TI o de red para completar este paso.

Pasos

1. Seleccione **Administración > Identidad y acceso**.
2. Seleccione **Federación** para ver la página **Federaciones**.
3. Seleccione **Configurar nueva federación**.
4. Seleccione **Verificar propiedad del dominio**.
5. Ingrese el dominio que desea verificar y seleccione **Continuar**.
6. Copie el registro TXT que se proporciona.
7. Vaya a la configuración de DNS de su dominio y configure el valor TXT que se proporcionó como registro TXT para su dominio. Trabaje con su administrador de TI o de red si es necesario.
8. Después de agregar el registro TXT, regrese a la Consola y seleccione **Verificar**.

Configurar federaciones

Federar la NetApp Console con los Servicios de federación de Active Directory (AD FS)

Federe sus Servicios de federación de Active Directory (AD FS) con la NetApp Console para habilitar el inicio de sesión único (SSO) para la NetApp Console. Esto permite a los usuarios iniciar sesión en la consola utilizando sus credenciales corporativas.

Roles requeridos

El rol de administrador de la federación es necesario para crear y administrar federaciones. El espectador de la Federación puede ver la página de la Federación."Obtenga más información sobre los roles de acceso."

Puede federarse con su IdP corporativo o con el sitio de soporte de NetApp . NetApp recomienda elegir uno u otro, pero no ambos.

NetApp solo admite el inicio de sesión único (SSO) iniciado por el proveedor de servicios (SP). Primero, configure el proveedor de identidad para que confíe en la NetApp Console como proveedor de servicios.

Luego, crea una conexión en la consola utilizando la configuración de tu proveedor de identidad.

Puede configurar la federación con su servidor AD FS para habilitar el inicio de sesión único (SSO) para NetApp Console. El proceso implica configurar AD FS para que confíe en la consola como proveedor de servicios y luego crear la conexión en la NetApp Console.

Pasos

1. Seleccione **Administración > Identidad y acceso**.
2. Seleccione **Federación** para ver la página **Federaciones**.
3. Seleccione **Configurar nueva federación**.
4. Introduzca los detalles de su dominio:
   a. Elija si desea utilizar un dominio verificado o su dominio de correo electrónico. El dominio de correo electrónico es el dominio asociado con la cuenta con la que ha iniciado sesión.
   b. Introduzca el nombre de la federación que está configurando.
   c. Si elige un dominio verificado, seleccione el dominio de la lista.
5. Seleccione **Siguiente**.
6. Para su método de conexión, elija **Protocolo** y luego seleccione **Servicios de federación de Active Directory (AD FS)**.
7. Seleccione **Siguiente**.
8. Cree una relación de confianza de usuario autenticado en su servidor AD FS. Puede usar PowerShell o configurarlo manualmente en su servidor AD FS. Consulte la documentación de AD FS para obtener detalles sobre cómo crear una relación de confianza entre usuarios.
   a. Cree la confianza mediante PowerShell mediante el siguiente script:

```
(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. Alternativamente, puede crear la confianza manualmente en la consola de administración de AD FS. Utilice los siguientes valores de la NetApp Console al crear la confianza:
      - Al crear el identificador de confianza confiable, utilice el valor **YOUR_TENANT**: `netapp-cloud-account`
      - Cuando seleccione **Habilitar soporte para WS-Federation**, utilice el valor **YOUR_AUTH0_DOMAIN**: `netapp-cloud-account.auth0.com`
   c. Después de crear la confianza, copie la URL de metadatos de su servidor AD FS o descargue el archivo de metadatos de federación. Necesitará esta URL o archivo para completar la conexión en la consola.

NetApp recomienda utilizar la URL de metadatos para permitir que la NetApp Console recupere automáticamente la última configuración de AD FS. Si descarga el archivo de metadatos de federación, deberá actualizarlo manualmente en la NetApp Console cada vez que haya cambios en su configuración de AD FS.

9. Regrese a la consola y seleccione **Siguiente** para crear la conexión.
10. Cree la conexión con AD FS.
    a. Ingrese la **URL de AD FS** que copió de su servidor de AD FS en el paso anterior o cargue el archivo de metadatos de federación que descargó de su servidor de AD FS.
11. Seleccione **Crear conexión**. La creación de la conexión puede tardar unos segundos.
12. Seleccione **Siguiente**.
13. Seleccione **Probar conexión** para probar su conexión. Se le dirigirá a una página de inicio de sesión para su servidor IdP. Inicie sesión con sus credenciales de IdP. Después de iniciar sesión, regrese a la Consola para habilitar la conexión.

    Al utilizar la consola en modo restringido, copie la URL en una ventana de incógnito del navegador o en un navegador separado para iniciar sesión en su IdP.

14. En la consola, seleccione **Siguiente** para revisar la página de resumen.
15. Configurar notificaciones.

    Elija entre siete días o 30 días. El sistema envía notificaciones de vencimiento por correo electrónico y las muestra en la consola a cualquier usuario con los siguientes roles: superadministrador, administrador de la organización, administrador de la federación y visor de la federación.

16. Revise los detalles de la federación y luego seleccione **Habilitar federación**.
17. Seleccione **Finalizar** para completar el proceso.

Después de habilitar la federación, los usuarios inician sesión en la NetApp Console con sus credenciales corporativas.

Federar la NetApp Console con el ID de Microsoft Entra

Fedérese con su proveedor de IdP de Microsoft Entra ID para habilitar el inicio de sesión único (SSO) para la NetApp Console. Esto permite a los usuarios iniciar sesión utilizando sus credenciales corporativas.

Roles requeridos

El rol de administrador de la federación es necesario para crear y administrar federaciones. El espectador de la Federación puede ver la página de la Federación."Obtenga más información sobre los roles de acceso."

Puede federarse con su IdP corporativo o con el sitio de soporte de NetApp . NetApp recomienda elegir uno u otro, pero no ambos.

NetApp solo admite el inicio de sesión único (SSO) iniciado por el proveedor de servicios (SP). Primero debe configurar el proveedor de identidad para confiar en NetApp como proveedor de servicios. Luego, puede crear una conexión en la consola que utilice la configuración del proveedor de identidad.

Puede configurar una conexión federada con Microsoft Entra ID para habilitar el inicio de sesión único (SSO) para la consola. El proceso implica configurar su ID de Microsoft Entra para confiar en la consola como proveedor de servicios y luego crear la conexión en la consola.

Pasos

1. Seleccione **Administración > Identidad y acceso**.

2. Seleccione **Federación** para ver la página **Federaciones**.
3. Seleccione **Configurar nueva federación**.

Detalles del dominio

1. Introduzca los detalles de su dominio:
   a. Elija si desea utilizar un dominio verificado o su dominio de correo electrónico. El dominio de correo electrónico es el dominio asociado con la cuenta con la que ha iniciado sesión.
   b. Introduzca el nombre de la federación que está configurando.
   c. Si elige un dominio verificado, seleccione el dominio de la lista.
2. Seleccione **Siguiente**.

Método de conexión

1. Para su método de conexión, elija **Proveedor** y luego seleccione **Microsoft Entra ID**.
2. Seleccione **Siguiente**.

Instrucciones de configuración

1. Configure su ID de Microsoft Entra para confiar en NetApp como proveedor de servicios. Debe realizar este paso en su servidor Microsoft Entra ID.
   a. Utilice los siguientes valores al registrar su aplicación Microsoft Entra ID para confiar en la consola:
      - Para la **URL de redirección**, utilice `https://services.cloud.netapp.com`
      - Para la **URL de respuesta**, utilice `https://netapp-cloud-account.auth0.com/login/callback`
   b. Cree un secreto de cliente para su aplicación Microsoft Entra ID. Necesitará proporcionar el ID del cliente, el secreto del cliente y el nombre de dominio de Entra ID para completar la federación.
2. Regrese a la consola y seleccione **Siguiente** para crear la conexión.

Crear conexión

1. Crear la conexión con Microsoft Entra ID
   a. Ingrese el ID de cliente y el secreto de cliente que creó en el paso anterior.
   b. Introduzca el nombre de dominio de Microsoft Entra ID.
2. Seleccione **Crear conexión**. El sistema crea la conexión en unos segundos.

Probar y habilitar la conexión

1. Seleccione **Siguiente**.
2. Seleccione **Probar conexión** para probar su conexión. Se le dirigirá a una página de inicio de sesión para su servidor IdP. Inicie sesión con sus credenciales de IdP. Después de iniciar sesión, regrese a la Consola para habilitar la conexión.

> Al utilizar la consola en modo restringido, copie la URL en una ventana de incógnito del navegador o en un navegador separado para iniciar sesión en su IdP.

3. En la consola, seleccione **Siguiente** para revisar la página de resumen.
4. Configurar notificaciones.

   Elija entre siete días o 30 días. El sistema envía notificaciones de vencimiento por correo electrónico y las muestra en la consola a cualquier usuario con los siguientes roles: superadministrador, administrador de la organización, administrador de la federación y visor de la federación.

5. Revise los detalles de la federación y luego seleccione **Habilitar federación**.
6. Seleccione **Finalizar** para completar el proceso.

Después de habilitar la federación, los usuarios inician sesión en la NetApp Console con sus credenciales corporativas.

Federar la NetApp Console con PingFederate

Fedérese con su proveedor de IdP de PingFederate para habilitar el inicio de sesión único (SSO) para la NetApp Console. Esto permite a los usuarios iniciar sesión utilizando sus credenciales corporativas.

Roles requeridos

El rol de administrador de la federación es necesario para crear y administrar federaciones. El espectador de la Federación puede ver la página de la Federación."Obtenga más información sobre los roles de acceso."

Puede federarse con su IdP corporativo o con el sitio de soporte de NetApp . NetApp recomienda elegir uno u otro, pero no ambos.

NetApp solo admite el inicio de sesión único (SSO) iniciado por el proveedor de servicios (SP). Primero debe configurar el proveedor de identidad para confiar en NetApp como proveedor de servicios. Luego, puede crear una conexión en la consola que utilice la configuración del proveedor de identidad.

Puede configurar una conexión federada con PingFederate para habilitar el inicio de sesión único (SSO) para la consola. El proceso implica configurar su servidor PingFederate para que confíe en la consola como proveedor de servicios y luego crear la conexión en la consola.

Pasos

1. Seleccione **Administración > Identidad y acceso**.
2. Seleccione **Federación** para ver la página **Federaciones**.
3. Seleccione **Configurar nueva federación**.
4. Introduzca los detalles de su dominio:
   a. Elija si desea utilizar un dominio verificado o su dominio de correo electrónico. El dominio de correo electrónico es el dominio asociado con la cuenta con la que ha iniciado sesión.
   b. Introduzca el nombre de la federación que está configurando.
   c. Si elige un dominio verificado, seleccione el dominio de la lista.
5. Seleccione **Siguiente**.
6. Para su método de conexión, elija **Proveedor** y luego seleccione **PingFederate**.
7. Seleccione **Siguiente**.
8. Configure su servidor PingFederate para confiar en NetApp como proveedor de servicios. Debes realizar

este paso en tu servidor PingFederate.

a. Utilice los siguientes valores al configurar PingFederate para confiar en la NetApp Console:
   - Para la **URL de respuesta** o la **URL del servicio de consumidor de afirmaciones (ACS)**, utilice `https://netapp-cloud-account.auth0.com/login/callback`
   - Para la **URL de cierre de sesión**, utilice `https://netapp-cloud-account.auth0.com/logout`
   - Para **ID de audiencia/entidad**, utilice `urn:auth0:netapp-cloud-account:<fed-domain-name-saml>` donde <fed-domain-name-pingfederate> es el nombre de dominio de la federación. Por ejemplo, si su dominio es `example.com` , el ID de audiencia/entidad sería `urn:auth0:netappcloud-account:fed-example-com-pingfederate` .

b. Copie la URL del servidor PingFederate. Necesitará esta URL al crear la conexión en la consola.

c. Descargue el certificado X.509 de su servidor PingFederate. Debe estar en formato PEM codificado en Base64 (.pem, .crt, .cer).

9. Regrese a la consola y seleccione **Siguiente** para crear la conexión.
10. Crea la conexión con PingFederate
    a. Ingrese la URL del servidor PingFederate que copió en el paso anterior.
    b. Cargue el certificado de firma X.509. El certificado debe estar en formato PEM, CER o CRT.
11. Seleccione **Crear conexión**. El sistema crea la conexión en unos segundos.
12. Seleccione **Siguiente**.
13. Seleccione **Probar conexión** para probar su conexión. Se le dirigirá a una página de inicio de sesión para su servidor IdP. Inicie sesión con sus credenciales de IdP. Después de iniciar sesión, regrese a la Consola para habilitar la conexión.

    Al utilizar la consola en modo restringido, copie la URL en una ventana de incógnito del navegador o en un navegador separado para iniciar sesión en su IdP.

14. En la consola, seleccione **Siguiente** para revisar la página de resumen.
15. Configurar notificaciones.

    Elija entre siete días o 30 días. El sistema envía notificaciones de vencimiento por correo electrónico y las muestra en la consola a cualquier usuario con los siguientes roles: superadministrador, administrador de la organización, administrador de la federación y visor de la federación.

16. Revise los detalles de la federación y luego seleccione **Habilitar federación**.
17. Seleccione **Finalizar** para completar el proceso.

Después de habilitar la federación, los usuarios inician sesión en la NetApp Console con sus credenciales corporativas.

Federarse con un proveedor de identidad SAML

Fedérese con su proveedor de IdP SAML 2.0 para habilitar el inicio de sesión único (SSO) para la consola NEtApp. Esto permite a los usuarios iniciar sesión utilizando sus credenciales corporativas.

Rol requerido

El rol de administrador de la federación es necesario para crear y administrar federaciones. El espectador de la Federación puede ver la página de la Federación."Obtenga más información sobre los roles de acceso."

Puede federarse con su IdP corporativo o con el sitio de soporte de NetApp . No es posible federarse con ambos.

NetApp solo admite el inicio de sesión único (SSO) iniciado por el proveedor de servicios (SP). Primero debe configurar el proveedor de identidad para confiar en NetApp como proveedor de servicios. Luego, puede crear una conexión en la consola que utilice la configuración del proveedor de identidad.

Puede configurar una conexión federada con su proveedor de SAML 2.0 para habilitar el inicio de sesión único (SSO) para la consola. El proceso implica configurar su proveedor para que confíe en NetApp como proveedor de servicios y luego crear la conexión en la consola.

Pasos

1. Seleccione **Administración > Identidad y acceso**.
2. Seleccione **Federación** para ver la página **Federaciones**.
3. Seleccione **Configurar nueva federación**.
4. Introduzca los detalles de su dominio:
   a. Elija si desea utilizar un dominio verificado o su dominio de correo electrónico. El dominio de correo electrónico es el dominio asociado con la cuenta con la que ha iniciado sesión.
   b. Introduzca el nombre de la federación que está configurando.
   c. Si elige un dominio verificado, seleccione el dominio de la lista.
5. Seleccione **Siguiente**.
6. Para su método de conexión, elija **Protocolo** y luego seleccione **Proveedor de identidad SAML**.
7. Seleccione **Siguiente**.
8. Configure su proveedor de identidad SAML para confiar en NetApp como proveedor de servicios. Debe realizar este paso en su servidor proveedor SAML.
   a. Asegúrese de que su IdP tenga el atributo `email` establecer en la dirección de correo electrónico del usuario. Esto es necesario para que la consola identifique correctamente a los usuarios:

```
<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. Utilice los siguientes valores al registrar su aplicación SAML con la consola:
   - Para la **URL de respuesta** o la **URL del servicio de consumidor de afirmaciones (ACS)**, utilice `https://netapp-cloud-account.auth0.com/login/callback`

- Para la **URL de cierre de sesión**, utilice `https://netapp-cloud-account.auth0.com/logout`
- Para **ID de audiencia/entidad**, utilice `urn:auth0:netapp-cloud-account:<fed-domain-name-saml>` donde <fed-domain-name-saml> es el nombre de dominio que desea utilizar para la federación. Por ejemplo, si su dominio es `example.com` , el ID de audiencia/entidad sería `urn:auth0:netapp-cloud-account:fed-example-com-samlp` .

2. Después de crear la confianza, copie los siguientes valores de su servidor de proveedor SAML:
   - URL de inicio de sesión
   - URL de cierre de sesión (opcional)
3. Descargue el certificado X.509 de su servidor proveedor SAML. Debe estar en formato PEM, CER o CRT.
   a. Regrese a la consola y seleccione **Siguiente** para crear la conexión.
   b. Crear la conexión con SAML.
4. Introduzca la **URL de inicio de sesión** de su servidor SAML.
5. Cargue el certificado X.509 que descargó de su servidor de proveedor SAML.
6. Opcionalmente, ingrese la **URL de cierre de sesión** de su servidor SAML.
   a. Seleccione **Crear conexión**. El sistema crea la conexión en unos segundos.
   b. Seleccione **Siguiente**.
   c. Seleccione **Probar conexión** para probar su conexión. Se le dirigirá a una página de inicio de sesión para su servidor IdP. Inicie sesión con sus credenciales de IdP. Después de iniciar sesión, regrese a la Consola para habilitar la conexión.

      Al utilizar la consola en modo restringido, copie la URL en una ventana de incógnito del navegador o en un navegador separado para iniciar sesión en su IdP.

   d. En la consola, seleccione **Siguiente** para revisar la página de resumen.
   e. Configurar notificaciones.

      Elija entre siete días o 30 días. El sistema envía notificaciones de vencimiento por correo electrónico y las muestra en la consola a cualquier usuario con los siguientes roles: superadministrador, administrador de la organización, administrador de la federación y visor de la federación.

   f. Revise los detalles de la federación y luego seleccione **Habilitar federación**.
   g. Seleccione **Finalizar** para completar el proceso.

Después de habilitar la federación, los usuarios inician sesión en la NetApp Console con sus credenciales corporativas.

Administrar federaciones

Administrar federaciones en la NetApp Console

Puede administrar su federación en la NetApp Console. Puede desactivarlo, actualizar credenciales vencidas, así como desactivarlo si ya no lo necesita.

Roles requeridos

El rol de administrador de la federación es necesario para crear y administrar federaciones. El espectador de la Federación puede ver la página de la Federación."Obtenga más información sobre los roles de acceso."

También puede agregar un dominio verificado adicional a una federación existente, lo que le permite utilizar múltiples dominios para su conexión federada.

- Si configuró la federación mediante NetApp Cloud Central, impórtela a través de la página **Federación** para administrarla en la consola."Aprenda a importar su federación"
- Puede ver eventos de administración de la federación, como habilitar, deshabilitar y actualizar federaciones en la página Auditoría. "Obtenga más información sobre la supervisión de operaciones en la NetApp Console."

Habilitar una federación

Si ha creado una federación pero no está habilitada, puede habilitarla a través de la página **Federación**. Habilitar una federación permite que los usuarios asociados con la federación inicien sesión en la Consola usando sus credenciales corporativas. Cree y pruebe la federación con éxito antes de habilitarla.

Pasos

1. Seleccione **Administración > Identidad y acceso**.
2. Seleccione la pestaña **Federación**.
3. Seleccione el menú de acciones ••• junto a la federación que desea habilitar y seleccione **Habilitar**.

Agregar un dominio verificado a una federación existente

Puede agregar un dominio verificado a una federación existente en la Consola para usar múltiples dominios con el mismo proveedor de identidad (IdP).

Debes haber verificado ya el dominio en la consola antes de poder agregarlo a una federación. Si aún no ha verificado el dominio, puede hacerlo siguiendo los pasos en"Verifica tu dominio en la consola" .

Pasos

1. Seleccione **Administración > Identidad y acceso**.
2. Seleccione la pestaña **Federación**.
3. Seleccione el menú de acciones ⋮ junto a la federación a la que desea agregar un dominio verificado y seleccione **Actualizar dominios**. El cuadro de diálogo **Actualizar dominios** muestra el dominio ya asociado con esta federación.
4. Seleccione un dominio verificado de la lista de dominios disponibles.
5. Seleccione **Actualizar**. Los nuevos usuarios del dominio pueden obtener acceso a la consola federada en 30 segundos.

Actualización de una conexión federada que está a punto de expirar

Puede actualizar los detalles de una federación en la Consola. Por ejemplo, necesitará actualizar la federación si las credenciales, como un certificado o un secreto de cliente, expiran. Cuando sea necesario, actualice la fecha de notificación para recordarle que debe actualizar la conexión antes de que expire.

Actualice la consola primero antes de actualizar su IdP para evitar problemas de inicio de sesión. Manténgase conectado a la consola durante el proceso.

Pasos

1. Seleccione **Administración > Identidad y acceso**.

2. Seleccione la pestaña **Federación**.
3. Seleccione el menú de acciones (tres puntos verticales) junto a la federación que desea actualizar y seleccione **Actualizar federación**.
4. Actualice los detalles de la federación según sea necesario.
5. Seleccione **Actualizar**.

Probar una federación existente

Pruebe la conexión de una federación existente para verificar que funciona. Esto puede ayudarle a identificar cualquier problema con la federación y solucionarlo.

Pasos

1. Seleccione **Administración > Identidad y acceso**.
2. Seleccione la pestaña **Federación**.
3. Seleccione el menú de acciones junto a la federación a la que desea agregar un dominio verificado y seleccione **Probar conexión**.
4. Seleccione **Prueba**. El sistema le solicita que inicie sesión con sus credenciales corporativas. Si la conexión es exitosa, será redirigido a la NetApp Console. Si falla la conexión, verá un mensaje de error que indica el problema con la federación.
5. Seleccione **Listo** para regresar a la pestaña **Federación**.

Deshabilitar una federación

Si ya no necesita una federación, puede desactivarla. Esto evita que los usuarios asociados a la federación inicien sesión en la consola utilizando sus credenciales corporativas. Puede volver a habilitar la federación más tarde si es necesario.

Deshabilite una federación antes de eliminarla, como por ejemplo al desmantelar el IdP o discontinuar la federación. Esto le permitirá volver a habilitarlo más tarde si es necesario.

Pasos

1. Seleccione **Administración > Identidad y acceso**.
2. Seleccione la pestaña **Federación**.
3. Seleccione el menú de acciones junto a la federación a la que desea agregar un dominio verificado y seleccione **Deshabilitar**.

Eliminar una federación

Si ya no necesita una federación, puede eliminarla. Esto elimina la federación y evita que cualquier usuario asociado con la federación inicie sesión en la consola usando sus credenciales corporativas. Por ejemplo, si se está desmantelando el IdP o si la federación ya no es necesaria.

No es posible recuperar una federación después de eliminarla. Debes crear una nueva federación.

Debes deshabilitar una federación antes de poder eliminarla. No es posible recuperar una federación después de eliminarla.

Pasos

1. Seleccione **Administración > Identidad y acceso** .

2. Seleccione **Federaciones** para ver la página **Federaciones**.
3. Seleccione el menú de acciones ⋮ junto a la federación a la que desea agregar un dominio verificado y seleccione **Eliminar**.

Importe su federación a la NetApp Console

Si previamente ha configurado la federación a través de NetApp Cloud Central (una aplicación externa a la NetApp Console), la página Federación le solicitará que importe su conexión federada existente a la consola para que pueda administrarla en la nueva interfaz. Luego podrá aprovechar las últimas mejoras sin tener que recrear su conexión federada.

Después de importar su federación existente, puede administrarla desde la página **Federaciones**."Obtenga más información sobre la gestión de federaciones."

Rol requerido

Administrador de la organización o administrador de la federación."Obtenga más información sobre los roles de acceso."

Pasos

1. Seleccione **Administración > Identidad y acceso**.
2. Seleccione la pestaña **Federación**.
3. Seleccione **Importar federación**.

Aplicar permisos de ONTAP para la Vista avanzada de ONTAP (Administrador del sistema ONTAP)

De forma predeterminada, las credenciales del agente de la consola permiten a los usuarios acceder a la Vista avanzada (ONTAP System Manager). En su lugar, puede solicitar a los usuarios sus credenciales de ONTAP . Esto garantiza que los permisos de ONTAP de un usuario se apliquen cuando trabaja con clústeres de ONTAP tanto en Cloud Volumes ONTAP como en clústeres locales de ONTAP .

Debe tener el rol de administrador de la organización para editar la configuración del agente de la consola.

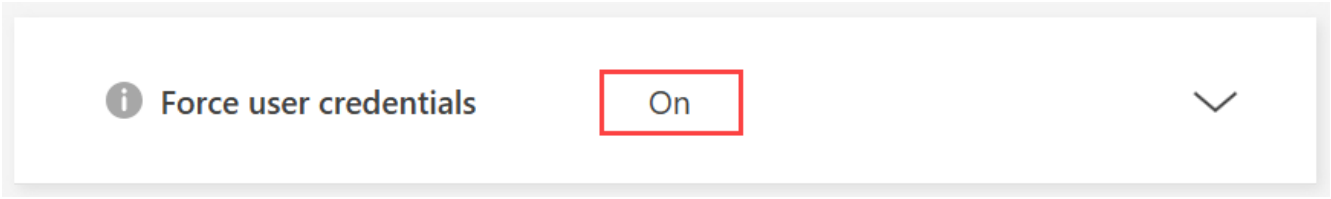
Pasos

1. Seleccione **Administración > Agentes**.
2. En la página **Descripción general**, seleccione el menú de acciones para un agente de consola y seleccione **Editar agente**.

   El agente de la consola debe estar activo para editarlo.

3. Expande la opción **Forzar Credenciales**.
4. Seleccione la casilla de verificación para habilitar la opción **Forzar credenciales** y luego seleccione **Guardar**.

5. Verifique que la opción **Forzar Credenciales** esté habilitada.



Habilitar el modo de solo lectura para una organización de NetApp Console

Como medida de seguridad, puede habilitar el modo de solo lectura para su organización de NetApp Console . En el modo de solo lectura, los usuarios pueden ver recursos y configuraciones, pero no pueden realizar cambios.

En el modo de solo lectura, los usuarios con roles de administrador deben elevar manualmente sus permisos para realizar cambios, lo que garantiza que los cambios sean intencionales.

Roles de acceso requeridos

Superadministrador o administrador de la organización.

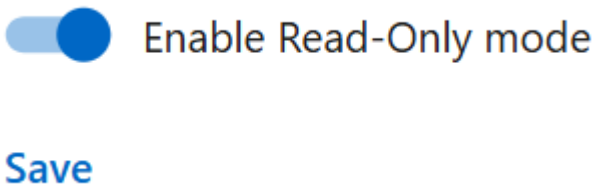
Habilite el modo de solo lectura para su organización de la consola

Habilite el modo de solo lectura para restringir los cambios en la organización de su consola. Todos los usuarios aún pueden ver los recursos. Los usuarios con roles de administrador no pueden realizar ninguna acción en la consola sin elevar manualmente sus permisos.

Cuando el modo de solo lectura está habilitado, los usuarios ven un banner que les notifica que la organización está en modo de solo lectura. Los usuarios deben ir a Configuración de usuario para elevar su rol.

Pasos

1. Seleccione **Administración > Identidad y acceso**.
2. Desde la pestaña **Organizaciones**, seleccione **Editar configuración de la organización** para la organización que desea configurar en modo de solo lectura.
3. En la sección **Modo de solo lectura**, habilite el modo de solo lectura moviendo el interruptor a la posición **Activado** y luego seleccione **Guardar**.



Regístrese en NetApp Console como administrador inicial de la organización

Si su empresa no tiene una organización de NetApp Console , regístrese para crear una. El primer usuario es el administrador y gestiona las cuentas y los permisos. Puede actualizar roles y agregar administradores más tarde.

Pasos

1. Abra un navegador web y vaya a "NetApp Console"
2. Si tiene una cuenta del sitio de soporte de NetApp , ingrese la dirección de correo electrónico asociada a su cuenta directamente en la página **Iniciar sesión**.

   La consola lo registra como parte de este inicio de sesión inicial con sus credenciales del sitio de soporte de NetApp .

3. Si desea registrarse creando un inicio de sesión de consola, seleccione **Registrarse**.
   a. En la página **Registrarse**, ingrese la información requerida y seleccione **Siguiente**.

      Sólo se permiten caracteres ingleses en el formulario de registro.

   b. Revise su bandeja de entrada en busca de un correo electrónico de NetApp que incluye instrucciones para verificar su dirección de correo electrónico.

      Verifique su dirección de correo electrónico para completar el registro.

4. Después de iniciar sesión, revise y acepte el Acuerdo de licencia de usuario final.
5. En la página **Bienvenido**, crea una organización.
6. Seleccione **Comencemos**.

+ Como administrador por primera vez, siga el proceso guiado para agregar almacenamiento, crear un agente de consola y más. "Obtenga información sobre cómo utilizar el Asistente de consola."

Próximos pasos

Como administrador, después de completar los pasos incluidos en el Asistente de consola, debe planificar su estrategia de identidad y acceso, agregar usuarios a su organización y asignar roles. "Obtenga información sobre la gestión de identidad y acceso para la NetApp Console"

Regístrese o inicie sesión en la NetApp Console cuando ya exista una organización

Si su empresa ya tiene una organización de NetApp Console , regístrese o inicie sesión para acceder a ella. Su método de registro o inicio de sesión depende de si su empresa utiliza la federación de identidad o tiene credenciales del sitio de soporte de NetApp . De lo contrario, cree un inicio de sesión en la NetApp Console .

Pasos

1. Abra un navegador web y vaya a "NetApp Console"
2. Si tiene una cuenta del sitio de soporte de NetApp o si su empresa ha configurado el inicio de sesión único (SSO), ingrese su dirección de correo electrónico asociada o sus credenciales de SSO en la página **Iniciar sesión**. Siga las instrucciones para completar el inicio de sesión.

   En ambos casos, usted se registra en la Consola como parte de este inicio de sesión inicial.

3. Si desea registrarse creando un inicio de sesión de consola, seleccione **Registrarse**.
   a. En la página **Registrarse**, ingrese la información requerida y seleccione **Siguiente**.

      Sólo se permiten caracteres ingleses en el formulario de registro.

   b. Revise su bandeja de entrada en busca de un correo electrónico de NetApp que incluye instrucciones para verificar su dirección de correo electrónico.

      Verifique su dirección de correo electrónico para completar el registro.

4. Después de iniciar sesión, revise y acepte el Acuerdo de licencia de usuario final.
5. Si el sistema le solicita que cree una organización, cierre el cuadro de diálogo e infórmeselo a un administrador de la consola para que pueda agregarlo a su organización de la consola y brindarle acceso. "Aprenda cómo comunicarse con un administrador de la organización."

Próximos pasos

Una vez que tenga acceso a su organización, podrá comenzar a administrar el almacenamiento y utilizar los servicios de datos que se le hayan asignado.