



# Uso del inicio de sesión único (SSO) para StorageGRID

StorageGRID 11.5

NetApp  
April 11, 2024

# Tabla de contenidos

- Uso del inicio de sesión único (SSO) para StorageGRID ..... 1
  - Cómo funciona el inicio de sesión único ..... 1
  - Requisitos para usar el inicio de sesión único ..... 3
  - Configuración del inicio de sesión único ..... 4

# Uso del inicio de sesión único (SSO) para StorageGRID

El sistema StorageGRID admite el inicio de sesión único (SSO) con el estándar de lenguaje de marcado de aserción de seguridad 2.0 (SAML 2.0). Cuando se habilita SSO, todos los usuarios deben estar autenticados por un proveedor de identidades externo antes de poder acceder a Grid Manager, al Gestor de inquilinos, a la API de gestión de grid o a la API de gestión de inquilinos. Los usuarios locales no pueden iniciar sesión en StorageGRID.

- ["Cómo funciona el inicio de sesión único"](#)
- ["Requisitos para usar el inicio de sesión único"](#)
- ["Configuración del inicio de sesión único"](#)

## Cómo funciona el inicio de sesión único

Antes de habilitar el inicio de sesión único (SSO), revise cómo se ven afectados los procesos de inicio de sesión y cierre de sesión de StorageGRID cuando se habilita SSO.

### Inicio de sesión cuando SSO está habilitado

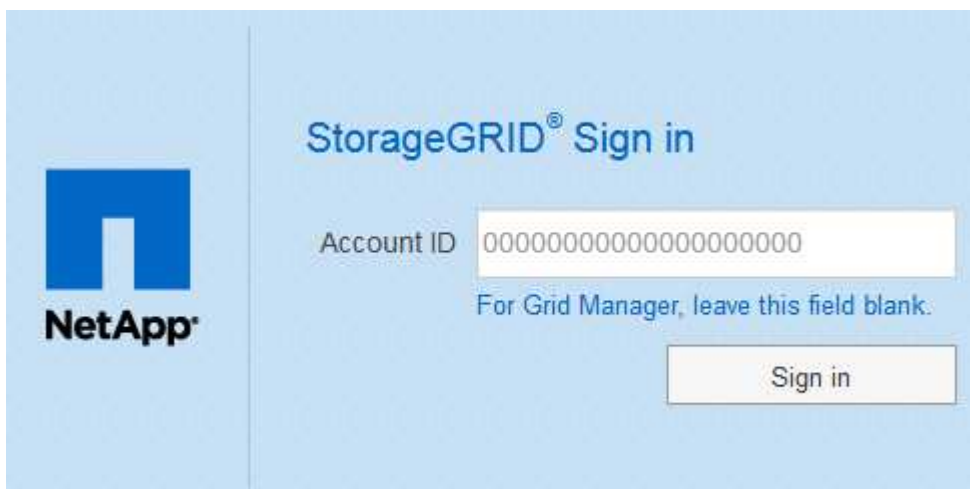
Cuando se habilita SSO y usted inicia sesión en StorageGRID, se le redirigirá a la página SSO de su organización para validar sus credenciales.

#### Pasos

1. Introduzca el nombre de dominio o la dirección IP completos de cualquier nodo de administración de StorageGRID en un navegador web.

Aparece la página Inicio de sesión de StorageGRID.

- Si es la primera vez que accede a la URL en este navegador, se le pedirá un ID de cuenta:



StorageGRID® Sign in

Account ID

For Grid Manager, leave this field blank.

Sign in

- Si anteriormente ha accedido al administrador de grid o al administrador de inquilinos, se le pedirá que seleccione una cuenta reciente o que introduzca un ID de cuenta:

The image shows the StorageGRID Sign in interface. On the left is the NetApp logo. The main area has the title "StorageGRID® Sign in". Below the title, there is a "Recent" dropdown menu with "S3 tenant" selected. Underneath is an "Account ID" text input field containing "27469746059057031822". A note below the field says "For Grid Manager, leave this field blank." At the bottom right is a "Sign in" button.

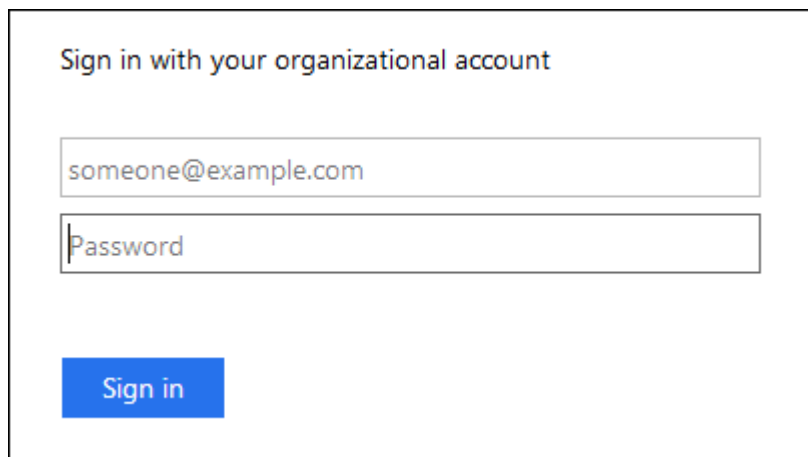
La página de inicio de sesión de StorageGRID no se muestra cuando introduce la URL completa de una cuenta de inquilino (es decir, un nombre de dominio completo o una dirección IP seguida de `/?accountId=20-digit-account-id`). En su lugar, se le redirige inmediatamente a la página de inicio de sesión con SSO de su organización, en la que puede hacerlo [Inicie sesión con sus credenciales de SSO](#).

2. Indique si desea acceder al administrador de grid o al responsable de inquilinos:

- Para acceder a Grid Manager, deje en blanco el campo **ID de cuenta**, introduzca **0** como ID de cuenta o seleccione **Grid Manager** si aparece en la lista de cuentas recientes.
- Para acceder al Administrador de arrendatarios, introduzca el ID de cuenta de arrendatario de 20 dígitos o seleccione un arrendatario por nombre si aparece en la lista de cuentas recientes.

3. Haga clic en **Iniciar sesión**

StorageGRID le redirige a la página de inicio de sesión con SSO de su organización. Por ejemplo:

The image shows a sign-in form for an organizational account. The title is "Sign in with your organizational account". There are two input fields: the first contains the email address "someone@example.com" and the second is labeled "Password". Below the fields is a blue "Sign in" button.

4. Inicia sesión con sus credenciales de SSO.

Si sus credenciales de SSO son correctas:

- a. El proveedor de identidades (IDP) ofrece una respuesta de autenticación a StorageGRID.
- b. StorageGRID valida la respuesta de autenticación.
- c. Si la respuesta es válida y pertenece a un grupo federado que tiene el permiso de acceso adecuado, se ha iniciado sesión en el Gestor de grid o en el Gestor de inquilinos, según la cuenta seleccionada.

- Opcionalmente, acceda a otros nodos de administración o acceda al administrador de grid o al administrador de inquilinos, si dispone de los permisos adecuados.

No es necesario volver a introducir sus credenciales de SSO.

## Cerrar sesión cuando SSO está habilitado

Cuando se habilita SSO en StorageGRID, lo que sucede cuando se inicia sesión depende de lo que se haya iniciado sesión y del lugar en el que se está cerrando sesión.

### Pasos

- Busque el enlace **Cerrar sesión** en la esquina superior derecha de la interfaz de usuario.
- Haga clic en **Cerrar sesión**.

Aparece la página Inicio de sesión de StorageGRID. La lista desplegable **Cuentas recientes** se actualiza para incluir **Grid Manager** o el nombre del inquilino, por lo que puede acceder a estas interfaces de usuario más rápidamente en el futuro.

Si ha iniciado sesión en...	Y salir de...	Se ha cerrado sesión en...
Grid Manager en uno o varios nodos de administrador	Grid Manager en cualquier nodo de administrador	Grid Manager en todos los nodos de administración
Administrador de inquilinos en uno o varios nodos de administrador	Inquilino Manager en cualquier nodo de administrador	Administrador de inquilinos en todos los nodos de administrador
Tanto Grid Manager como Inquilino Manager	Administrador de grid	Sólo Grid Manager. También debe cerrar sesión en el Administrador de inquilinos para cerrar la sesión de SSO.



La tabla resume lo que sucede cuando se inicia sesión si está utilizando una sola sesión del navegador. Si ha iniciado sesión en StorageGRID en varias sesiones de explorador, debe cerrar la sesión en todas las sesiones de explorador por separado.

## Requisitos para usar el inicio de sesión único

Antes de habilitar el inicio de sesión único (SSO) para un sistema StorageGRID, revise los requisitos en esta sección.



El inicio de sesión único (SSO) no está disponible en los puertos de administrador de grid restringido o de administrador de inquilinos. Debe utilizar el puerto HTTPS predeterminado (443) si desea que los usuarios se autenticuen con inicio de sesión único.

## Requisitos del proveedor de identidades

El proveedor de identidades (IDP) para SSO debe cumplir los siguientes requisitos:

- Cualquiera de las siguientes versiones del servicio de Federación de Active Directory (AD FS):
  - AD FS 4.0, incluido en Windows Server 2016



Windows Server 2016 debe utilizar "[Actualización KB3201845](#)", o superior.

- AD FS 3.0, incluido con la actualización de Windows Server 2012 R2 o superior.
- Seguridad de la capa de transporte (TLS) 1.2 ó 1.3
- Microsoft .NET Framework, versión 3.5.1 o posterior

## Requisitos de certificado de servidor

StorageGRID utiliza un certificado de servidor de interfaz de gestión en cada nodo de administración para garantizar el acceso al administrador de grid, al administrador de inquilinos, a la API de gestión de grid y a la API de gestión de inquilinos. Cuando configura las confianzas de la parte de confianza de SSO para StorageGRID en AD FS, el certificado de servidor se utiliza como el certificado de firma para las solicitudes de StorageGRID a AD FS.

Si todavía no ha instalado un certificado de servidor personalizado para la interfaz de gestión, debe hacerlo ahora. Cuando se instala un certificado de servidor personalizado, se utiliza para todos los nodos de administración y se puede usar en todas las confianzas de parte que confía de StorageGRID.



No se recomienda utilizar el certificado de servidor predeterminado de un nodo de administración en la confianza de parte de confianza de AD FS. Si el nodo falla y lo recupera, se genera un nuevo certificado de servidor predeterminado. Antes de iniciar sesión en el nodo recuperado, debe actualizar la confianza de la parte que confía en AD FS con el nuevo certificado.

Para acceder a la certificación de servidor de un nodo de administrador, inicie sesión en el shell de comandos del nodo y vaya al `/var/local/mgmt-api` directorio. Se denomina certificado de servidor personalizado `custom-server.crt`. El certificado de servidor predeterminado del nodo se denomina `server.crt`.

### Información relacionada

["Controlar el acceso mediante firewalls"](#)

["Configuración de un certificado de servidor personalizado para el administrador de grid y el administrador de inquilinos"](#)

## Configuración del inicio de sesión único

Cuando se habilita el inicio de sesión único (SSO), los usuarios solo pueden acceder a Grid Manager, al arrendatario Manager, a la API de gestión de grid o a la API de gestión de inquilinos si sus credenciales están autorizadas mediante el proceso de inicio de sesión SSO implementado por la organización.

- ["Confirmación de que los usuarios federados pueden iniciar sesión"](#)
- ["Uso del modo de recinto de seguridad"](#)
- ["Creación de confianzas de parte de confianza en AD FS"](#)
- ["Prueba de fideicomisos de la parte de confianza"](#)

- "Habilitar el inicio de sesión único"
- "Desactivar el inicio de sesión único"
- "Desactive y vuelva a habilitar temporalmente el inicio de sesión único para un nodo de administración"

## Confirmación de que los usuarios federados pueden iniciar sesión

Antes de habilitar el inicio de sesión único (SSO), debe confirmar que al menos un usuario federado puede iniciar sesión en Grid Manager y en el Gestor de inquilinos para cualquier cuenta de inquilino existente.

### Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener permisos de acceso específicos.
- Está utilizando Active Directory como origen de identidad federado y AD FS como proveedor de identidades.

["Requisitos para usar el inicio de sesión único"](#)

### Pasos

1. Si hay cuentas de inquilino existentes, confirme que ninguno de los inquilinos utiliza su propio origen de identidad.



Al habilitar SSO, el origen de identidad configurado en el Administrador de inquilinos se anula mediante el origen de identidades configurado en Grid Manager. Los usuarios que pertenezcan al origen de identidad del arrendatario ya no podrán iniciar sesión a menos que tengan una cuenta con el origen de identidad de Grid Manager.

- a. Inicie sesión en el Administrador de arrendatarios para cada cuenta de arrendatario.
  - b. Seleccione **Control de acceso > Federación de identidades**.
  - c. Confirme que la casilla de verificación **Activar Federación de identidades** no está activada.
  - d. Si es así, confirme que los grupos federados que podrían estar en uso para esta cuenta de arrendatario ya no son necesarios, anule la selección de la casilla de verificación y haga clic en **Guardar**.
2. Confirme que un usuario federado puede acceder a Grid Manager:
    - a. En Grid Manager, seleccione **Configuración > Control de acceso > grupos de administración**.
    - b. Asegúrese de que al menos un grupo federado se ha importado del origen de identidad de Active Directory y de que se le ha asignado el permiso acceso raíz.
    - c. Cierre la sesión.
    - d. Confirme que puede volver a iniciar sesión en Grid Manager como usuario en el grupo federado.
  3. Si hay cuentas de inquilino existentes, confirme que un usuario federado con permiso de acceso raíz puede iniciar sesión:
    - a. En Grid Manager, seleccione **arrendatarios**.
    - b. Seleccione la cuenta de arrendatario y haga clic en **Editar cuenta**.
    - c. Si la casilla de verificación **Usos own Identity Source** está activada, desmarque la casilla y haga clic

en **Guardar**.

### Edit Tenant Account

#### Tenant Details

Display Name

**Uses Own Identity Source**

Allow Platform Services

Storage Quota (optional)

Aparece la página Cuentas de arrendatario.

- Seleccione la cuenta de arrendatario, haga clic en **Iniciar sesión** e inicie sesión en la cuenta de arrendatario como usuario raíz local.
- En el Administrador de arrendatarios, haga clic en **Control de acceso > grupos**.
- Asegúrese de que al menos un grupo federado de Grid Manager ha sido asignado el permiso acceso raíz para este arrendatario.
- Cierre la sesión.
- Confirme que puede volver a iniciar sesión en el inquilino como usuario en el grupo federado.

#### Información relacionada

["Requisitos para usar el inicio de sesión único"](#)

["Gestión de los grupos de administración"](#)

["Usar una cuenta de inquilino"](#)

## Uso del modo de recinto de seguridad

Puede utilizar el modo de recinto de seguridad para configurar y probar las confianzas de partes de Active Directory Federation Services (AD FS) antes de aplicar el inicio de sesión único (SSO) para los usuarios de StorageGRID. Una vez habilitado SSO, puede volver a habilitar el modo Sandbox para configurar o probar confianzas de partes de confianza nuevas y existentes. Al volver a habilitar el modo de recinto limitado, se deshabilita temporalmente SSO para los usuarios de StorageGRID.

#### Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener permisos de acceso específicos.

#### Acerca de esta tarea



Cuando se habilita SSO y un usuario intenta iniciar sesión en un nodo de administración, StorageGRID envía una solicitud de autenticación a AD FS. A su vez, AD FS envía una respuesta de autenticación a StorageGRID, indicando si la solicitud de autorización se ha realizado correctamente. En el caso de las solicitudes correctas, la respuesta incluye un identificador único universal (UUID) para el usuario.

Para permitir que StorageGRID (el proveedor de servicios) y AD FS (el proveedor de identidades) se comuniquen de forma segura acerca de las solicitudes de autenticación de usuario, debe configurar determinados ajustes en StorageGRID. A continuación, debe utilizar AD FS para crear una confianza de parte de confianza para cada nodo de administración. Por último, debe volver a StorageGRID para habilitar SSO.

El modo de recinto de seguridad facilita la realización de esta configuración de fondo y la realización de pruebas de todos los ajustes antes de habilitar SSO.



Se recomienda utilizar el modo de recinto de seguridad, pero no estrictamente necesario. Si está preparado para crear confianzas de parte de confianza de AD FS inmediatamente después de configurar SSO en StorageGRID, Además, no es necesario probar los procesos de inicio de sesión único (SLO) y cierre de sesión único (SLO) para cada nodo de administración, haga clic en **habilitado**, introduzca la configuración de StorageGRID, cree una confianza de parte de confianza para cada nodo de administración en AD FS y, a continuación, haga clic en **Guardar** para habilitar SSO.

## Pasos

1. Seleccione **Configuración > Control de acceso > Inicio de sesión único**.

Aparece la página Inicio de sesión único, con la opción **Desactivado** seleccionada.

### Single Sign-on

You can enable single sign-on (SSO) if you want an external identity provider (IdP) to authorize all user access to StorageGRID. To start, enable [identity federation](#) and confirm that at least one federated user has Root Access permission to the Grid Manager and to the Tenant Manager for any existing tenant accounts. Next, select Sandbox Mode to configure, save, and then test your SSO settings. After verifying the connections, select Enabled and click Save to start using SSO.

SSO Status  Disabled  Sandbox Mode  Enabled

Save



Si las opciones de estado de SSO no aparecen, confirme que ha configurado Active Directory como origen de identidad federado. Véase «requisitos para el uso de la entrada única».

2. Seleccione la opción **modo Sandbox**.

Aparece la configuración del proveedor de identidades y de la parte de confianza. En la sección Proveedor de identidades, el campo **Tipo de servicio** es de sólo lectura. Muestra el tipo de servicio de federación de identidades que está utilizando (por ejemplo, Active Directory).

3. En la sección Proveedor de identidades:

- a. Escriba el nombre del Servicio de Federación, exactamente como aparece en AD FS.



Para buscar el nombre del servicio de Federación, vaya al Administrador del servidor de Windows. Seleccione **Herramientas > Administración AD FS**. En el menú Acción, seleccione **Editar propiedades del servicio de Federación**. El nombre del servicio de Federación se muestra en el segundo campo.

b. Especifique si desea utilizar TLS (Seguridad de la capa de transporte) para proteger la conexión cuando el proveedor de identidades envíe información de configuración de SSO en respuesta a solicitudes de StorageGRID.

- **Utilizar certificado CA** del sistema operativo: Utilice el certificado CA predeterminado instalado en el sistema operativo para asegurar la conexión.
- **Utilizar certificado de CA personalizado**: Utilice un certificado de CA personalizado para proteger la conexión.

Si selecciona este ajuste, copie y pegue el certificado en el cuadro de texto **Certificado CA**.

- **No utilice TLS**: No utilice un certificado TLS para garantizar la conexión.

4. En la sección parte de confianza , especifique el identificador de parte de confianza que utilizará para los nodos de administración de StorageGRID cuando configure confianzas de parte de confianza.

- Por ejemplo, si el grid solo tiene un nodo de administrador y no prevé añadir más nodos de administrador en el futuro, introduzca `SG` o `StorageGRID`.
- Si el grid incluye más de un nodo de administración, incluya la cadena `[HOSTNAME]` en el identificador. Por ejemplo: `SG-[HOSTNAME]` . Esto genera una tabla que incluye un identificador de parte de confianza para cada nodo de administración, en función del nombre de host del nodo. +  
NOTA: Debe crear una confianza de parte de confianza para cada nodo de administración en su sistema StorageGRID. Tener una confianza de parte que confía en cada nodo de administración garantiza que los usuarios puedan iniciar sesión de forma segura desde y hacia cualquier nodo de administración.

5. Haga clic en **Guardar**.

- Aparece una Marca de verificación verde en el botón **Guardar** durante unos segundos.



- Aparece el aviso de confirmación del modo Sandbox, que confirma que el modo Sandbox está habilitado. Puede utilizar este modo mientras utiliza AD FS para configurar una confianza de parte de confianza para cada nodo de administración y probar los procesos de inicio de sesión único (SSO) y cierre de sesión único (SLO).

## Single Sign-on

You can enable single sign-on (SSO) if you want an external identity provider (IdP) to authorize all user access to StorageGRID. To start, enable [identity federation](#) and confirm that at least one federated user has Root Access permission to the Grid Manager and to the Tenant Manager for any existing tenant accounts. Next, select Sandbox Mode to configure, save, and then test your SSO settings. After verifying the connections, select Enabled and click Save to start using SSO.

SSO Status    Disabled    Sandbox Mode    Enabled

### Sandbox mode

Sandbox mode is currently enabled. Use this mode to configure relying party trusts and to confirm that single sign-on (SSO) and single logout (SLO) are correctly configured for the StorageGRID system.

1. Use Active Directory Federation Services (AD FS) to create relying party trusts for StorageGRID. Create one trust for each Admin Node, using the relying party identifier(s) shown below.
2. Go to your identity provider's sign-on page: <https://ad2016.saml.sgws/adfs/ls/idpinitiatedsignon.htm>
3. From this page, sign in to each StorageGRID relying party trust. If the SSO operation is successful, StorageGRID displays a page with a success message. Otherwise, an error message is displayed.

When you have confirmed SSO for each of the relying party trusts and you are ready to enforce the use of SSO for StorageGRID, change the SSO Status to Enabled, and click Save.

## Información relacionada

["Requisitos para usar el inicio de sesión único"](#)

## Creación de confianzas de parte de confianza en AD FS

Debe utilizar los Servicios de Federación de Active Directory (AD FS) para crear una confianza de parte de confianza para cada nodo de administración del sistema. Puede crear confianzas de parte confiando mediante comandos de PowerShell, importando los metadatos de SAML desde StorageGRID o introduciendo los datos manualmente.

### Crear una confianza de parte de confianza mediante Windows PowerShell

Puede utilizar Windows PowerShell para crear rápidamente una o más confianzas de parte que dependan.

#### Lo que necesitará

- Configuró SSO en StorageGRID y conoce el nombre de dominio completo (o la dirección IP) y el identificador de la parte que confía para cada nodo de administrador del sistema.



Debe crear una confianza de parte de confianza para cada nodo de administrador en el sistema StorageGRID. Tener una confianza de parte que confía en cada nodo de administración garantiza que los usuarios puedan iniciar sesión de forma segura desde y hacia cualquier nodo de administración.

- Tiene experiencia en la creación de confianzas de parte de confianza en AD FS o tiene acceso a la documentación de Microsoft AD FS.
- Está utilizando el complemento Administración de AD FS y pertenece al grupo Administradores.

#### Acerca de esta tarea

Estas instrucciones se aplican a AD FS 4.0, que se incluye en Windows Server 2016. Si está utilizando AD FS

3.0, que se incluye con Windows 2012 R2, notará ligeras diferencias en el procedimiento. Consulte la documentación de Microsoft AD FS si tiene alguna pregunta.

## Pasos

1. En el menú de inicio de Windows, haga clic con el botón derecho del ratón en el icono de PowerShell y seleccione **Ejecutar como administrador**.
2. En el símbolo del sistema de PowerShell, introduzca el siguiente comando:

```
Add-AdfsRelyingPartyTrust -Name "Admin_Node_Identifer" -MetadataURL  
"https://Admin_Node_FQDN/api/saml-metadata"
```

- Para *Admin\_Node\_Identifer*, Escriba el identificador de parte que confía para el nodo de administración, exactamente como aparece en la página Single Sign-On. Por ejemplo: SG-DC1-ADM1.
  - Para *Admin\_Node\_FQDN*, Escriba el nombre de dominio completo para el mismo nodo de administración. (Si es necesario, puede usar la dirección IP del nodo en su lugar. Sin embargo, si introduce una dirección IP aquí, tenga en cuenta que debe actualizar o volver a crear la confianza de esta parte que confía si esa dirección IP cambia alguna vez.)
3. En Windows Server Manager, seleccione **Herramientas > Administración de AD FS**.

Aparece la herramienta de administración de AD FS.

4. Seleccione **AD FS > fideicomisos de la parte**.

Aparece la lista de confianzas de parte de confianza.

5. Agregar una directiva de control de acceso a la confianza de parte de confianza recién creada:

- a. Busque la parte de confianza que acaba de crear.
- b. Haga clic con el botón derecho del ratón en la confianza y seleccione **Editar directiva de control de acceso**.
- c. Seleccione una Política de control de acceso.
- d. Haga clic en **aplicar** y haga clic en **Aceptar**

6. Agregar una política de emisión de reclamaciones a la nueva confianza de parte de confianza creada:

- a. Busque la parte de confianza que acaba de crear.
- b. Haga clic con el botón derecho del ratón en la confianza y seleccione **Editar política de emisión de reclamaciones**.
- c. Haga clic en **Agregar regla**.
- d. En la página Seleccionar plantilla de regla, seleccione **Enviar atributos LDAP como reclamaciones** en la lista y haga clic en **Siguiente**.
- e. En la página Configurar regla, introduzca un nombre para mostrar para esta regla.

Por ejemplo, **ObjectGUID to Name ID**.

- f. Para el almacén de atributos, seleccione **Active Directory**.
- g. En la columna atributo LDAP de la tabla Mapping, escriba **objectGUID**.
- h. En la columna Tipo de reclamación saliente de la tabla asignación, seleccione **ID de nombre** en la lista desplegable.
- i. Haga clic en **Finalizar** y haga clic en **Aceptar**.

7. Confirme que los metadatos se han importado correctamente.
  - a. Haga clic con el botón derecho del ratón en la confianza de la parte que confía para abrir sus propiedades.
  - b. Confirme que los campos de las fichas **puntos finales**, **identificadores** y **firma** se han rellenado.

Si faltan metadatos, confirme que la dirección de metadatos de la Federación es correcta o simplemente introduzca los valores manualmente.
8. Repita estos pasos para configurar una confianza de parte que confía para todos los nodos de administración del sistema StorageGRID.
9. Cuando haya terminado, vuelva a StorageGRID y. "[pruebe todos los fideicomisos de la parte de confianza](#)" para confirmar que están correctamente configurados.

## Crear una confianza de parte de confianza mediante la importación de metadatos de federación

Puede importar los valores de cada una de las partes que confía mediante el acceso a los metadatos de SAML de cada nodo de administrador.

### Lo que necesitará

- Configuró SSO en StorageGRID y conoce el nombre de dominio completo (o la dirección IP) y el identificador de la parte que confía para cada nodo de administrador del sistema.



Debe crear una confianza de parte de confianza para cada nodo de administrador en el sistema StorageGRID. Tener una confianza de parte que confía en cada nodo de administración garantiza que los usuarios puedan iniciar sesión de forma segura desde y hacia cualquier nodo de administración.

- Tiene experiencia en la creación de confianzas de parte de confianza en AD FS o tiene acceso a la documentación de Microsoft AD FS.
- Está utilizando el complemento Administración de AD FS y pertenece al grupo Administradores.

### Acerca de esta tarea

Estas instrucciones se aplican a AD FS 4.0, que se incluye en Windows Server 2016. Si está utilizando AD FS 3.0, que se incluye con Windows 2012 R2, notará ligeras diferencias en el procedimiento. Consulte la documentación de Microsoft AD FS si tiene alguna pregunta.

### Pasos

1. En Windows Server Manager, haga clic en **Herramientas** y, a continuación, seleccione **Administración de AD FS**.
2. En acciones, haga clic en **Agregar confianza de parte de confianza**.
3. En la página de bienvenida, elija **Claims aware** y haga clic en **Inicio**.
4. Seleccione **Importar datos sobre la parte que confía publicada en línea o en una red local**.
5. En **Dirección de metadatos de Federación (nombre de host o URL)**, escriba la ubicación de los metadatos SAML para este nodo de administración:

```
https://Admin_Node_FQDN/api/saml-metadata
```

Para *Admin\_Node\_FQDN*, Escriba el nombre de dominio completo para el mismo nodo de administración. (Si es necesario, puede usar la dirección IP del nodo en su lugar. Sin embargo, si introduce una dirección IP aquí, tenga en cuenta que debe actualizar o volver a crear la confianza de esta parte que confía si esa

dirección IP cambia alguna vez.)

6. Complete el asistente Trust Party Trust, guarde la confianza de la parte que confía y cierre el asistente.



Al introducir el nombre para mostrar, utilice el identificador de parte de confianza para el nodo de administración, exactamente como aparece en la página Single Sign-On en Grid Manager. Por ejemplo: SG-DC1-ADM1.

7. Agregar una regla de reclamación:

- a. Haga clic con el botón derecho del ratón en la confianza y seleccione **Editar política de emisión de reclamaciones**.
- b. Haga clic en **Agregar regla**:
- c. En la página Seleccionar plantilla de regla, seleccione **Enviar atributos LDAP como reclamaciones** en la lista y haga clic en **Siguiente**.
- d. En la página Configurar regla, introduzca un nombre para mostrar para esta regla.

Por ejemplo, **ObjectGUID to Name ID**.

- e. Para el almacén de atributos, seleccione **Active Directory**.
- f. En la columna atributo LDAP de la tabla Mapping, escriba **objectGUID**.
- g. En la columna Tipo de reclamación saliente de la tabla asignación, seleccione **ID de nombre** en la lista desplegable.
- h. Haga clic en **Finalizar** y haga clic en **Aceptar**.

8. Confirme que los metadatos se han importado correctamente.

- a. Haga clic con el botón derecho del ratón en la confianza de la parte que confía para abrir sus propiedades.
- b. Confirme que los campos de las fichas **puntos finales**, **identificadores** y **firma** se han rellenado.

Si faltan metadatos, confirme que la dirección de metadatos de la Federación es correcta o simplemente introduzca los valores manualmente.

9. Repita estos pasos para configurar una confianza de parte que confía para todos los nodos de administración del sistema StorageGRID.

10. Cuando haya terminado, vuelva a StorageGRID y. "[pruebe todos los fideicomisos de la parte de confianza](#)" para confirmar que están correctamente configurados.

### Crear una confianza de parte de confianza manualmente

Si elige no importar los datos de las confianzas de la pieza de confianza, puede introducir los valores manualmente.

#### Lo que necesitará

- Configuró SSO en StorageGRID y conoce el nombre de dominio completo (o la dirección IP) y el identificador de la parte que confía para cada nodo de administrador del sistema.



Debe crear una confianza de parte de confianza para cada nodo de administrador en el sistema StorageGRID. Tener una confianza de parte que confía en cada nodo de administración garantiza que los usuarios puedan iniciar sesión de forma segura desde y hacia cualquier nodo de administración.

- Tiene el certificado personalizado que se cargó para la interfaz de gestión StorageGRID, o bien sabe cómo iniciar sesión en un nodo de administrador desde el shell de comandos.
- Tiene experiencia en la creación de confianzas de parte de confianza en AD FS o tiene acceso a la documentación de Microsoft AD FS.
- Está utilizando el complemento Administración de AD FS y pertenece al grupo Administradores.

### Acerca de esta tarea

Estas instrucciones se aplican a AD FS 4.0, que se incluye en Windows Server 2016. Si está utilizando AD FS 3.0, que se incluye con Windows 2012 R2, notará ligeras diferencias en el procedimiento. Consulte la documentación de Microsoft AD FS si tiene alguna pregunta.

### Pasos

1. En Windows Server Manager, haga clic en **Herramientas** y, a continuación, seleccione **Administración de AD FS**.
2. En acciones, haga clic en **Agregar confianza de parte de confianza**.
3. En la página de bienvenida, elija **Claims aware** y haga clic en **Inicio**.
4. Seleccione **introducir datos sobre la parte que confía manualmente** y haga clic en **Siguiente**.
5. Complete el asistente Trust Party Trust:

- a. Introduzca un nombre de visualización para este nodo de administración.

Para obtener coherencia, utilice el identificador de parte de confianza para el nodo de administración, exactamente como aparece en la página de inicio de sesión único en Grid Manager. Por ejemplo: SG-DC1-ADM1.

- b. Omitir el paso para configurar un certificado de cifrado de token opcional.
- c. En la página Configurar URL, active la casilla de verificación **Activar compatibilidad con el protocolo WebSSO** de SAML 2.0.
- d. Escriba la URL del extremo de servicio SAML para el nodo de administración:

```
https://Admin_Node_FQDN/api/saml-response
```

Para *Admin\_Node\_FQDN*, Escriba el nombre de dominio completo para el nodo de administración. (Si es necesario, puede usar la dirección IP del nodo en su lugar. Sin embargo, si introduce una dirección IP aquí, tenga en cuenta que debe actualizar o volver a crear la confianza de esta parte que confía si esa dirección IP cambia alguna vez.)

- e. En la página Configurar identificadores, especifique el identificador de parte que confía para el mismo nodo de administración:

```
Admin_Node_Identifier
```

Para *Admin\_Node\_Identifier*, Escriba el identificador de parte que confía para el nodo de administración, exactamente como aparece en la página Single Sign-On. Por ejemplo: SG-DC1-ADM1.

f. Revise la configuración, guarde la confianza de la parte que confía y cierre el asistente.

Aparecerá el cuadro de diálogo Editar directiva de emisión de reclamaciones.



Si el cuadro de diálogo no aparece, haga clic con el botón derecho del ratón en la confianza y seleccione **Editar directiva de emisión de reclamaciones**.

6. Para iniciar el asistente para reglas de reclamación, haga clic en **Agregar regla**:
  - a. En la página Seleccionar plantilla de regla, seleccione **Enviar atributos LDAP como reclamaciones** en la lista y haga clic en **Siguiente**.
  - b. En la página Configurar regla, introduzca un nombre para mostrar para esta regla.  
  
Por ejemplo, **ObjectGUID to Name ID**.
  - c. Para el almacén de atributos, seleccione **Active Directory**.
  - d. En la columna atributo LDAP de la tabla Mapping, escriba **objectGUID**.
  - e. En la columna Tipo de reclamación saliente de la tabla asignación, seleccione **ID de nombre** en la lista desplegable.
  - f. Haga clic en **Finalizar** y haga clic en **Aceptar**.
7. Haga clic con el botón derecho del ratón en la confianza de la parte que confía para abrir sus propiedades.
8. En la ficha **endpoints**, configure el extremo para un único cierre de sesión (SLO):
  - a. Haga clic en **Agregar SAML**.
  - b. Seleccione **Tipo de extremo > SAML Logout**.
  - c. Seleccione **enlace > Redirigir**.
  - d. En el campo **Trusted URL**, introduzca la dirección URL utilizada para cerrar sesión único (SLO) desde este nodo de administración:

```
https://Admin_Node_FQDN/api/saml-logout
```

Para *Admin\_Node\_FQDN*, Escriba el nombre de dominio completo del nodo de administración. (Si es necesario, puede usar la dirección IP del nodo en su lugar. Sin embargo, si introduce una dirección IP aquí, tenga en cuenta que debe actualizar o volver a crear la confianza de esta parte que confía si esa dirección IP cambia alguna vez.)

- a. Haga clic en **Aceptar**.
9. En la ficha **firma**, especifique el certificado de firma para esta confianza de parte de confianza:
  - a. Agregue el certificado personalizado:
    - Si posee el certificado de gestión personalizado cargado en StorageGRID, seleccione ese certificado.
    - Si no tiene el certificado personalizado, inicie sesión en el nodo de administrador, vaya al `/var/local/mgmt-api` directorio del nodo Admin y añada el `custom-server.crt` archivo de certificado.

**Nota:** utilizando el certificado predeterminado del nodo de administración (`server.crt`) no es recomendable. Si falla el nodo de administración, el certificado predeterminado se regenerará al recuperar el nodo y deberá actualizar la confianza de la parte de confianza.



- b. Haga clic en **aplicar** y haga clic en **Aceptar**.

Las propiedades de la parte de confianza se guardan y cierran.

10. Repita estos pasos para configurar una confianza de parte que confía para todos los nodos de administración del sistema StorageGRID.
11. Cuando haya terminado, vuelva a StorageGRID y. "[pruebe todos los fideicomisos de la parte de confianza](#)" para confirmar que están correctamente configurados.

## Prueba de fideicomisos de la parte de confianza

Antes de aplicar el uso de inicio de sesión único (SSO) para StorageGRID, confirme que el inicio de sesión único y el cierre de sesión único (SLO) se han configurado correctamente. Si ha creado una confianza de parte de confianza para cada nodo de administrador, confirme que puede usar SSO y SLO para cada nodo de administración.

### Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener permisos de acceso específicos.
- Ha configurado una o más confianzas de parte de confianza en AD FS.

### Pasos

1. Seleccione **Configuración > Control de acceso > Inicio de sesión único**.

Aparece la página Single Sign-On, con la opción **modo Sandbox** seleccionada.

2. En las instrucciones para el modo de recinto de seguridad, busque el vínculo a la página de inicio de sesión del proveedor de identidades.

La dirección URL se deriva del valor especificado en el campo **Nombre de servicio federado**.

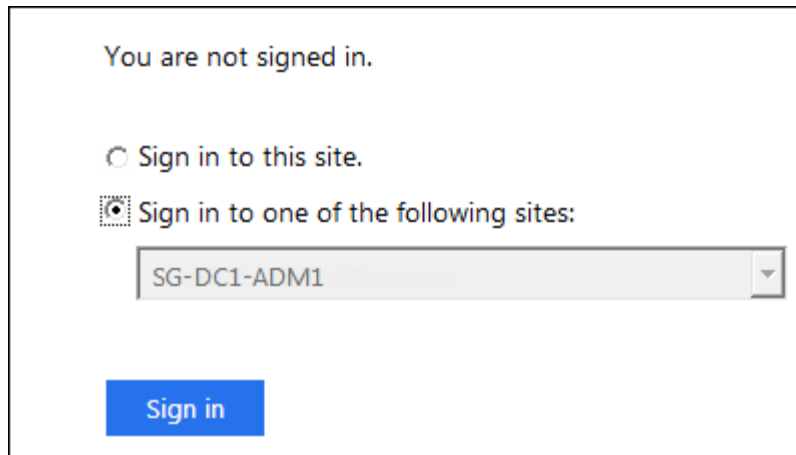
**Sandbox mode**

Sandbox mode is currently enabled. Use this mode to configure relying party trusts and to confirm that single sign-on (SSO) and single logout (SLO) are correctly configured for the StorageGRID system.

1. Use Active Directory Federation Services (AD FS) to create relying party trusts for StorageGRID. Create one trust for each Admin Node, using the relying party identifier(s) shown below.
2. Go to your identity provider's sign-on page: <https://ad2016.saml.sgws/adfs/ls/idpinitiatedsignon.htm>
3. From this page, sign in to each StorageGRID relying party trust. If the SSO operation is successful, StorageGRID displays a page with a success message. Otherwise, an error message is displayed.

When you have confirmed SSO for each of the relying party trusts and you are ready to enforce the use of SSO for StorageGRID, change the SSO Status to Enabled, and click Save.

3. Haga clic en el vínculo o copie y pegue la URL en un navegador para acceder a la página de inicio de sesión del proveedor de identidades.
4. Para confirmar que puede utilizar SSO para iniciar sesión en StorageGRID, seleccione **Iniciar sesión en uno de los siguientes sitios**, seleccione el identificador de la parte que confía para su nodo de administración principal y haga clic en **Iniciar sesión**.



Se le solicitará que introduzca su nombre de usuario y contraseña.

5. Introduzca el nombre de usuario y la contraseña federados.

- Si las operaciones de inicio de sesión y cierre de sesión SSO se realizan correctamente, se muestra un mensaje de éxito.

✓ Single sign-on authentication and logout test completed successfully.

- Si la operación de SSO se realiza sin errores, se muestra un mensaje de error. Solucione el problema, borre las cookies del navegador e inténtelo de nuevo.

6. Repita los pasos anteriores para confirmar que puede iniciar sesión en cualquier otro nodo de administrador.

Si todas las operaciones de inicio de sesión y cierre de sesión SSO se realizan correctamente, estará listo para habilitar SSO.

## Habilitar el inicio de sesión único

Después de usar el modo de Sandbox para probar todas sus confianzas de partes de confianza de StorageGRID, estará listo para habilitar el inicio de sesión único (SSO).

### Lo que necesitará

- Debe haber importado al menos un grupo federado del origen de identidades y los permisos de administración de acceso raíz asignados al grupo. Debe confirmar que al menos un usuario federado tiene permiso de acceso raíz al administrador de grid y al administrador de inquilinos para las cuentas de arrendatario existentes.
- Debe haber probado todas las confianzas de partes de confianza mediante el modo de Sandbox.

### Pasos

1. Seleccione **Configuración > Control de acceso > Inicio de sesión único**.

Aparece la página Single Sign-On con **modo Sandbox** seleccionado.

2. Cambie el estado de SSO a **habilitado**.

3. Haga clic en **Guardar**.

Aparecerá un mensaje de advertencia.

## Warning

### Enable single sign-on

After you enable SSO, no local users—including the root user—will be able to sign in to the Grid Manager, the Tenant Manager, the Grid Management API, or the Tenant Management API.

Before proceeding, confirm the following:

- You have imported at least one federated group from the identity source and assigned Root Access management permissions to the group. You must confirm that at least one federated user has Root Access permission to the Grid Manager and to the Tenant Manager for any existing tenant accounts.
- You have tested all relying party trusts using sandbox mode.

Are you sure you want to enable single sign-on?

Cancel

OK

4. Revise la advertencia y haga clic en **Aceptar**.

El inicio de sesión único ahora está activado.



Todos los usuarios deben utilizar SSO para acceder a Grid Manager, al Gestor de inquilinos, a la API de gestión de grid y a la API de gestión de inquilinos. Los usuarios locales ya no pueden acceder a StorageGRID.

## Desactivar el inicio de sesión único

Si ya no desea usar esta funcionalidad, puede deshabilitar el inicio de sesión único (SSO). Debe deshabilitar el inicio de sesión único antes de poder deshabilitar la federación de identidades.

### Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener permisos de acceso específicos.

### Pasos

1. Seleccione **Configuración > Control de acceso > Inicio de sesión único**.

Aparece la página Single Sign-On.

2. Seleccione la opción **Desactivado**.
3. Haga clic en **Guardar**.

Aparece un mensaje de advertencia que indica que los usuarios locales podrán iniciar sesión.

## Warning

### Disable single sign-on

After you disable SSO or switch to sandbox mode, local users will be able to sign in. Are you sure you want to proceed?

Cancel

OK

#### 4. Haga clic en **Aceptar**.

La próxima vez que inicie sesión en StorageGRID, aparecerá la página Inicio de sesión en StorageGRID, donde deberá introducir el nombre de usuario y la contraseña de un usuario de StorageGRID local o federado.

## Desactive y vuelva a habilitar temporalmente el inicio de sesión único para un nodo de administración

Es posible que no pueda iniciar sesión en Grid Manager si se desactiva el sistema de inicio de sesión único (SSO). En este caso, puede deshabilitar y volver a habilitar SSO para un nodo de administración. Para deshabilitar y, a continuación, volver a habilitar SSO, debe acceder al shell de comandos del nodo.

### Lo que necesitará

- Debe tener permisos de acceso específicos.
- Debe tener la `Passwords.txt` archivo.
- Debe conocer la contraseña del usuario raíz local.

### Acerca de esta tarea

Después de deshabilitar SSO para un nodo de administración, puede iniciar sesión en Grid Manager como usuario raíz local. Para proteger el sistema StorageGRID, tiene que utilizar el shell de comandos del nodo para volver a habilitar SSO en el nodo de administración tan pronto como cierre la sesión.



La deshabilitación de SSO para un nodo de administrador no afecta la configuración de SSO para ningún otro nodo de administrador que esté en el grid. La casilla de verificación **Activar SSO** de la página de inicio de sesión único de Grid Manager permanece seleccionada y se mantienen todas las configuraciones de SSO existentes a menos que se actualicen.

### Pasos

1. Inicie sesión en un nodo de administrador:
  - a. Introduzca el siguiente comando: `ssh admin@Admin_Node_IP`
  - b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
  - c. Introduzca el siguiente comando para cambiar a la raíz: `su -`
  - d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

Cuando ha iniciado sesión como root, el símbolo del sistema cambia de \$ para #.

2. Ejecute el siguiente comando:`disable-saml`

Un mensaje indica que el comando se aplica únicamente a este nodo de administrador.

3. Confirme que desea deshabilitar SSO.

Un mensaje indica que el inicio de sesión único está deshabilitado en el nodo.

4. Desde un explorador web, acceda a Grid Manager en el mismo nodo de administración.

Ahora se muestra la página de inicio de sesión de Grid Manager porque SSO se ha desactivado.

5. Inicie sesión con la raíz del nombre de usuario y la contraseña del usuario raíz local.

6. Si deshabilitó temporalmente SSO debido a que debe corregir la configuración de SSO:

- a. Seleccione **Configuración > Control de acceso > Inicio de sesión único**.
- b. Cambie la configuración incorrecta o obsoleta de SSO.
- c. Haga clic en **Guardar**.

Al hacer clic en **Guardar** en la página de inicio de sesión único, se vuelve a activar SSO automáticamente para toda la cuadrícula.

7. Si ha desactivado SSO temporalmente porque necesita acceder a Grid Manager por algún otro motivo:

- a. Realice cualquier tarea o tarea que necesite realizar.
- b. Haga clic en **Cerrar sesión** y cierre Grid Manager.
- c. Vuelva a habilitar SSO en el nodo de administrador. Puede realizar cualquiera de los siguientes pasos:
  - Ejecute el siguiente comando: `enable-saml`

Un mensaje indica que el comando se aplica únicamente a este nodo de administrador.

Confirme que desea habilitar SSO.

Un mensaje indica que el inicio de sesión único está habilitado en el nodo.

- Reinicie el nodo de cuadrícula: `reboot`

8. Desde un explorador web, acceda a Grid Manager desde el mismo nodo de administración.

9. Confirme que aparece la página de inicio de sesión de StorageGRID y que debe introducir sus credenciales de SSO para acceder a Grid Manager.

## Información relacionada

["Configuración del inicio de sesión único"](#)

## Información de copyright

Copyright © 2024 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

## Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.