



Utilice el inicio de sesión único (SSO)

StorageGRID software

NetApp

December 03, 2025

Tabla de contenidos

Utilice el inicio de sesión único (SSO)	1
Configurar el inicio de sesión único	1
Cómo funciona el inicio de sesión único	1
Requisitos y consideraciones para el inicio de sesión único	4
Requisitos del proveedor de identidad	4
Requisitos del certificado de servidor	5
Requisitos del puerto	6
Confirmar que los usuarios federados puedan iniciar sesión	6
Utilizar el modo sandbox	8
Acceder al modo sandbox	9
Introduzca los datos del proveedor de identidad	9
Configurar relaciones de confianza entre usuarios, aplicaciones empresariales o conexiones de SP ...	13
Probar conexiones SSO	14
Habilitar el inicio de sesión único	18
Crear relaciones de confianza entre usuarios autenticados en AD FS	18
Crear una relación de confianza de usuario autenticado mediante Windows PowerShell	19
Cree una relación de confianza entre usuarios autenticados mediante la importación de metadatos de la federación	20
Crear una relación de confianza de usuario confiado manualmente	21
Crear aplicaciones empresariales en Azure AD	23
Acceder a Azure AD	24
Cree aplicaciones empresariales y guarde la configuración de SSO de StorageGRID	24
Descargar metadatos SAML para cada nodo de administración	25
Cargar metadatos SAML a cada aplicación empresarial	25
Crear conexiones de proveedor de servicios (SP) en PingFederate	25
Requisitos previos completos en PingFederate	26
Crear una conexión SP en PingFederate	27
Deshabilitar el inicio de sesión único	30
Deshabilitar temporalmente y volver a habilitar el inicio de sesión único para un nodo de administración. .	30

Utilice el inicio de sesión único (SSO)

Configurar el inicio de sesión único

Cuando el inicio de sesión único (SSO) está habilitado, los usuarios solo pueden acceder a Grid Manager, Tenant Manager, Grid Management API o Tenant Management API si sus credenciales están autorizadas mediante el proceso de inicio de sesión SSO implementado por su organización. Los usuarios locales no pueden iniciar sesión en StorageGRID.

Cómo funciona el inicio de sesión único

El sistema StorageGRID admite el inicio de sesión único (SSO) mediante el estándar Security Assertion Markup Language 2.0 (SAML 2.0).

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

Sign in cuando el SSO esté habilitado

Cuando SSO está habilitado e inicia sesión en StorageGRID, se lo redirige a la página SSO de su organización para validar sus credenciales.

Pasos

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

Aparece la página de Sign in de StorageGRID .

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



Sign in

Account

Sign in

[NetApp support](#) | [NetApp.com](#)

- Si ya ha accedido al Administrador de red o al Administrador de inquilinos, se le solicitará que seleccione una cuenta reciente o que ingrese un ID de cuenta:



Tenant Manager

Recent

Account

Sign in

[NetApp support](#) | [NetApp.com](#)



La página de Sign in de StorageGRID no se muestra cuando ingresa la URL completa para 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 SSO de su organización, donde puede [Inicie sesión con sus credenciales de SSO](#).

2. Indique si desea acceder al Administrador de red o al Administrador de inquilinos:

- Para acceder al Administrador de cuadrícula, deje el campo **ID de cuenta** en blanco, ingrese **0** como ID de cuenta o seleccione **Administrador de cuadrícula** si aparece en la lista de cuentas recientes.
- Para acceder al Administrador de inquilinos, ingrese el ID de la cuenta del inquilino de 20 dígitos o seleccione un inquilino por nombre si aparece en la lista de cuentas recientes.

3. Seleccionar * Sign in*

StorageGRID lo redirecciona a la página de inicio de sesión SSO de su organización. Por ejemplo:

Sign in with your organizational account

someone@example.com

Password

Sign in

4. Sign in con sus credenciales SSO.

Si sus credenciales de SSO son correctas:

- El proveedor de identidad (IdP) proporciona una respuesta de autenticación a StorageGRID.
- StorageGRID valida la respuesta de autenticación.
- Si la respuesta es válida y usted pertenece a un grupo federado con permisos de acceso a StorageGRID, iniciará sesión en Grid Manager o en Tenant Manager, según la cuenta que haya seleccionado.



Si la cuenta de servicio no es accesible, aún puede iniciar sesión, siempre que sea un usuario existente que pertenezca a un grupo federado con permisos de acceso a StorageGRID.

5. Opcionalmente, acceda a otros nodos de administración, o acceda al Administrador de red o al Administrador de inquilinos, si tiene los permisos adecuados.

No es necesario volver a ingresar sus credenciales SSO.

Cerrar sesión cuando el SSO esté habilitado

Cuando SSO está habilitado para StorageGRID, lo que sucede cuando cierra sesión depende de dónde haya iniciado sesión y desde dónde cierre sesión.

Pasos

1. Localice el enlace **Cerrar sesión** en la esquina superior derecha de la interfaz de usuario.
2. Seleccione **Cerrar sesión**.

Aparece la página de Sign in de StorageGRID . El menú desplegable **Cuentas recientes** se actualiza para incluir **Grid Manager** o el nombre del inquilino, para que pueda acceder a estas interfaces de usuario más rápidamente en el futuro.

Si ha iniciado sesión en...	Y cierras sesión en...	Has cerrado sesión en...
Administrador de cuadrícula en uno o más nodos de administración	Administrador de cuadrícula en cualquier nodo de administración	Administrador de cuadrícula en todos los nodos de administración Nota: Si usa Azure para SSO, puede que lleve algunos minutos cerrar sesión en todos los nodos de administración.
Administrador de inquilinos en uno o más nodos de administración	Administrador de inquilinos en cualquier nodo de administración	Administrador de inquilinos en todos los nodos de administración
Tanto Grid Manager como Tenant Manager	Administrador de red	Sólo el administrador de cuadrícula. También debe cerrar sesión en el Administrador de inquilinos para cerrar sesión en SSO.



La tabla resume lo que sucede cuando cierras sesión si estás usando una sola sesión de navegador. Si ha iniciado sesión en StorageGRID en varias sesiones de navegador, deberá cerrar sesión en todas las sesiones de navegador por separado.

Requisitos y consideraciones para el inicio de sesión único

Antes de habilitar el inicio de sesión único (SSO) para un sistema StorageGRID , revise los requisitos y las consideraciones.

Requisitos del proveedor de identidad

StorageGRID admite los siguientes proveedores de identidad SSO (IdP):

- Servicio de federación de Active Directory (AD FS)
- Directorio activo de Azure (Azure AD)
- Federación de ping

Debe configurar la federación de identidad para su sistema StorageGRID antes de poder configurar un proveedor de identidad SSO. El tipo de servicio LDAP que utiliza para la federación de identidad controla qué tipo de SSO puede implementar.

Tipo de servicio LDAP configurado	Opciones para el proveedor de identidad SSO
Directorio activo	• Directorio activo • Azur • Federación de ping
Azur	Azur

Requisitos de AD FS

Puede utilizar cualquiera de las siguientes versiones de AD FS:

- ADFS de Windows Server 2022
- Servidor AD FS de Windows 2019
- Servidor AD FS de Windows 2016



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

Requisitos adicionales

- Seguridad de la capa de transporte (TLS) 1.2 o 1.3
- Microsoft .NET Framework, versión 3.5.1 o superior

Consideraciones para Azure

Si usa Azure como tipo de SSO y los usuarios tienen nombres principales de usuario que no usan sAMAccountName como prefijo, pueden surgir problemas de inicio de sesión si StorageGRID pierde su conexión con el servidor LDAP. Para permitir que los usuarios inicien sesión, debe restaurar la conexión al servidor LDAP.

Requisitos del certificado de servidor

De forma predeterminada, StorageGRID utiliza un certificado de interfaz de administración en cada nodo de administración para proteger el acceso al Administrador de Grid, al Administrador de inquilinos, a la API de administración de Grid y a la API de administración de inquilinos. Cuando configura relaciones de confianza de usuario confiable (AD FS), aplicaciones empresariales (Azure) o conexiones de proveedor de servicios (PingFederate) para StorageGRID, utiliza el certificado del servidor como certificado de firma para las solicitudes de StorageGRID .

Si aún no lo has hecho "[Configuró un certificado personalizado para la interfaz de administración](#)" Deberías hacerlo ahora. Cuando instala un certificado de servidor personalizado, este se utiliza para todos los nodos de administración y puede usarlo en todas las relaciones de confianza de usuarios confiables de StorageGRID , aplicaciones empresariales o conexiones de SP .



No se recomienda utilizar el certificado de servidor predeterminado de un nodo de administración en una relación de confianza de usuario confiable, una aplicación empresarial o una conexión de SP . Si el nodo falla y lo recupera, se genera un nuevo certificado de servidor predeterminado. Antes de poder iniciar sesión en el nodo recuperado, debe actualizar la confianza de la parte confiable, la aplicación empresarial o la conexión del SP con el nuevo certificado.

Puede acceder al certificado de servidor de un nodo de administración iniciando sesión en el shell de comandos del nodo y yendo a `/var/local/mgmt-api` directorio. Un certificado de servidor personalizado se denomina `custom-server.crt` . El certificado de servidor predeterminado del nodo se llama `server.crt` .

Requisitos del puerto

El inicio de sesión único (SSO) no está disponible en los puertos restringidos de Grid Manager o Tenant Manager. Debe utilizar el puerto HTTPS predeterminado (443) si desea que los usuarios se autenticuen con inicio de sesión único. Ver "[Controlar el acceso al firewall externo](#)" .

Confirmar que los usuarios federados puedan iniciar sesión

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

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "[navegador web compatible](#)" .
- Tienes "[permisos de acceso específicos](#)" .
- Ya ha configurado la federación de identidad.

Pasos

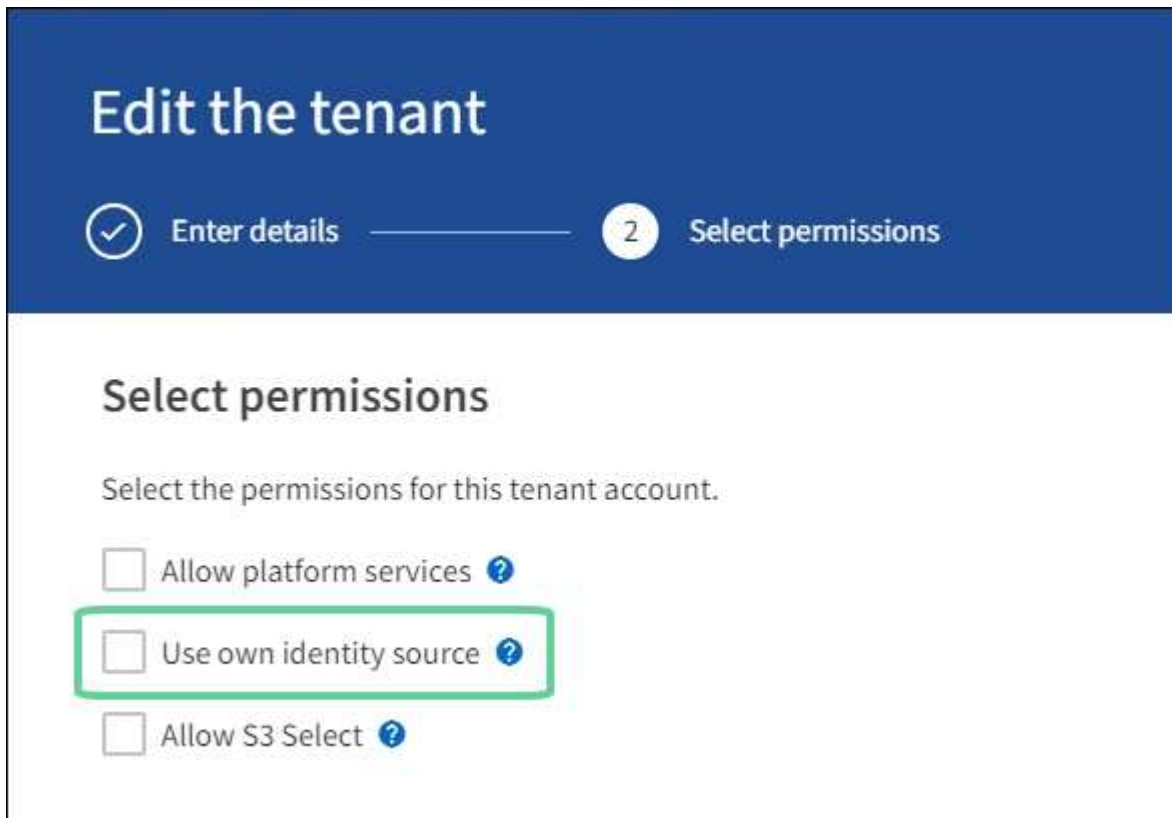
1. Si existen cuentas de inquilinos, confirme que ninguno de ellos esté usando su propia fuente de identidad.



Cuando habilita SSO, una fuente de identidad configurada en Tenant Manager se reemplaza por la fuente de identidad configurada en Grid Manager. Los usuarios que pertenecen a la fuente de identidad del inquilino ya no podrán iniciar sesión a menos que tengan una cuenta con la fuente de identidad de Grid Manager.

- a. Sign in en el Administrador de inquilinos para cada cuenta de inquilino.
 - b. Seleccione **GESTIÓN DE ACCESO > Federación de identidades**.
 - c. Confirme que la casilla de verificación **Habilitar federación de identidad** no esté seleccionada.
 - d. Si es así, confirme que cualquier grupo federado que pueda estar en uso para esta cuenta de inquilino ya no sea necesario, desmarque la casilla de verificación y seleccione **Guardar**.
2. Confirme que un usuario federado puede acceder al Administrador de Grid:
 - a. Desde Grid Manager, seleccione **CONFIGURACIÓN > Control de acceso > Grupos de administración**.
 - b. Asegúrese de que se haya importado al menos un grupo federado desde la fuente de identidad de Active Directory y que se le haya asignado el permiso de acceso raíz.

- c. Desconectar.
 - d. Confirme que puede volver a iniciar sesión en Grid Manager como usuario del grupo federado.
3. Si hay cuentas de inquilino existentes, confirme que un usuario federado que tenga permiso de acceso raíz pueda iniciar sesión:
 - a. Desde el Administrador de red, seleccione **INQUILINOS**.
 - b. Seleccione la cuenta del inquilino y seleccione **Acciones > Editar**.
 - c. En la pestaña Ingresar detalles, seleccione **Continuar**.
 - d. Si la casilla de verificación **Usar fuente de identidad propia** está seleccionada, desmarque la casilla y seleccione **Guardar**.



Aparece la página del inquilino.

- a. Seleccione la cuenta del inquilino, seleccione * Sign in* e inicie sesión en la cuenta del inquilino como usuario raíz local.
- b. Desde el Administrador de inquilinos, seleccione **ADMINISTRACIÓN DE ACCESO > Grupos**.
- c. Asegúrese de que al menos a un grupo federado del Administrador de Grid se le haya asignado el permiso de acceso raíz para este inquilino.
- d. Desconectar.
- e. Confirme que puede volver a iniciar sesión en el inquilino como usuario en el grupo federado.

Información relacionada

- ["Requisitos y consideraciones para el inicio de sesión único"](#)
- ["Administrar grupos de administradores"](#)

- ["Utilice una cuenta de inquilino"](#)

Utilizar el modo sandbox

Puede utilizar el modo sandbox para configurar y probar el inicio de sesión único (SSO) antes de habilitarlo para todos los usuarios de StorageGRID . Una vez habilitado el SSO, puede regresar al modo sandbox siempre que necesite cambiar o volver a probar la configuración.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tú tienes el ["Permiso de acceso root"](#) .
- Ha configurado la federación de identidad para su sistema StorageGRID .
- Para la federación de identidad **tipo de servicio LDAP**, seleccionó Active Directory o Azure, según el proveedor de identidad SSO que planea usar.

Tipo de servicio LDAP configurado	Opciones para el proveedor de identidad SSO
Directorio activo	• Directorio activo • Azur • Federación de ping
Azur	Azur

Acerca de esta tarea

Cuando SSO está habilitado y un usuario intenta iniciar sesión en un nodo de administración, StorageGRID envía una solicitud de autenticación al proveedor de identidad SSO. A su vez, el proveedor de identidad SSO envía una respuesta de autenticación a StorageGRID, indicando si la solicitud de autenticación fue exitosa. Para solicitudes exitosas:

- La respuesta de Active Directory o PingFederate incluye un identificador único universal (UUID) para el usuario.
- La respuesta de Azure incluye un nombre principal de usuario (UPN).

Para permitir que StorageGRID (el proveedor de servicios) y el proveedor de identidad SSO se comuniquen de forma segura acerca de las solicitudes de autenticación de usuarios, debe configurar ciertas configuraciones en StorageGRID. A continuación, debe utilizar el software del proveedor de identidad SSO para crear una relación de confianza de usuario confiable (AD FS), una aplicación empresarial (Azure) o un proveedor de servicios (PingFederate) para cada nodo de administración. Por último, debes regresar a StorageGRID para habilitar SSO.

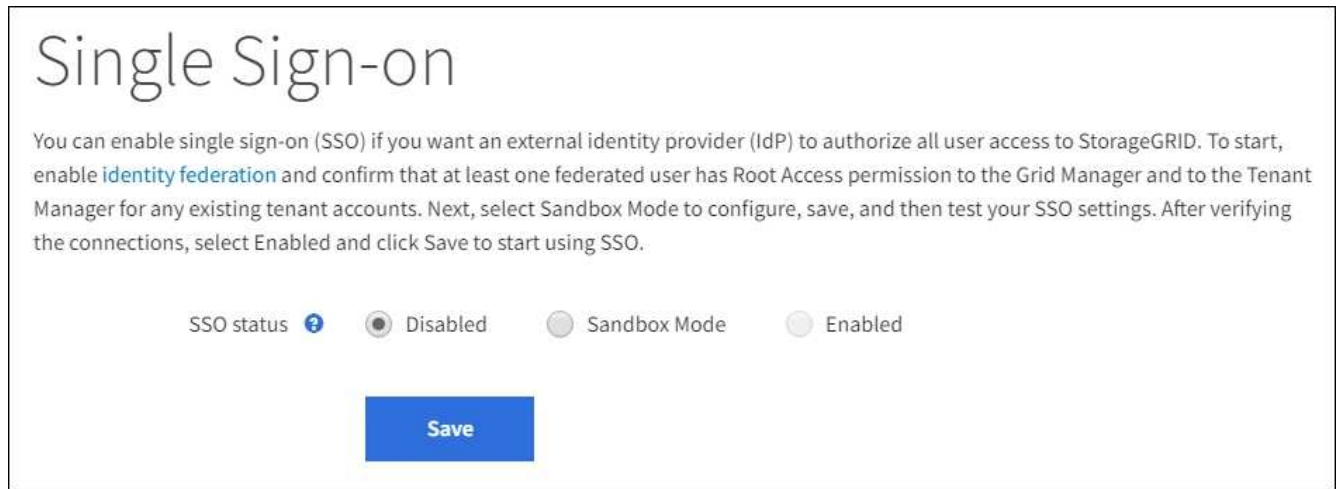
El modo Sandbox facilita la realización de esta configuración de ida y vuelta y permite probar todas las configuraciones antes de habilitar SSO. Cuando se utiliza el modo sandbox, los usuarios no pueden iniciar sesión mediante SSO.

Acceder al modo sandbox

Pasos

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

Aparece la página de inicio de sesión único, con la opción **Deshabilitado** 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 haya configurado el proveedor de identidad como fuente de identidad federada. Ver "[Requisitos y consideraciones para el inicio de sesión único](#)".

2. Seleccione **Modo Sandbox**.

Aparece la sección Proveedor de identidad.

Introduzca los datos del proveedor de identidad

Pasos

1. Seleccione el **tipo de SSO** de la lista desplegable.
2. Complete los campos en la sección Proveedor de identidad según el tipo de SSO que haya seleccionado.

Directorio activo

- a. Ingrese el **Nombre del servicio de federación** para el proveedor de identidad, exactamente como aparece en el Servicio de federación de Active Directory (AD FS).



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

- b. Especifique qué certificado TLS se utilizará para proteger la conexión cuando el proveedor de identidad envíe información de configuración de SSO en respuesta a las solicitudes de StorageGRID .

- **Usar certificado CA del sistema operativo:** utilice el certificado CA predeterminado instalado en el sistema operativo para proteger la conexión.
- **Usar certificado CA personalizado:** utilice un certificado CA personalizado para proteger la conexión.

Si selecciona esta configuración, copie el texto del certificado personalizado y péguelo en el cuadro de texto **Certificado CA**.

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



Si cambia el certificado de CA, inmediatamente [reiniciar el servicio mgmt-api en los nodos de administración](#) y comprobar que el inicio de sesión único (SSO) en Grid Manager es exitoso.

- c. En la sección Parte confiada, especifique el **Identificador de parte confiada** para StorageGRID. Este valor controla el nombre que utiliza para cada relación de confianza de usuario confiable en AD FS.

- Por ejemplo, si su red tiene solo un nodo de administración y no prevé agregar más nodos de administración en el futuro, ingrese `SG` o `StorageGRID` .
- Si su cuadrícula incluye más de un nodo de administración, incluya la cadena `[HOSTNAME]` en el identificador. Por ejemplo, `SG-[HOSTNAME]` . Esto genera una tabla que muestra el identificador de la parte confiable para cada nodo de administración en su sistema, según el nombre de host del nodo.



Debe crear una relación de confianza de usuario autenticado para cada nodo de administración en su sistema StorageGRID . Tener una relación de confianza de parte confiable para cada nodo de administración garantiza que los usuarios puedan iniciar y cerrar sesión de forma segura en cualquier nodo de administración.

- d. Seleccione **Guardar**.

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



Azur

- a. Especifique qué certificado TLS se utilizará para proteger la conexión cuando el proveedor de identidad envíe información de configuración de SSO en respuesta a las solicitudes de StorageGRID .

- **Usar certificado CA del sistema operativo:** utilice el certificado CA predeterminado instalado en el sistema operativo para proteger la conexión.
- **Usar certificado CA personalizado:** utilice un certificado CA personalizado para proteger la conexión.

Si selecciona esta configuración, copie el texto del certificado personalizado y péguelo en el cuadro de texto **Certificado CA**.

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



Si cambia el certificado de CA, inmediatamente ["reiniciar el servicio mgmt-api en los nodos de administración"](#) y comprobar que el inicio de sesión único (SSO) en Grid Manager es exitoso.

- b. En la sección Aplicación empresarial, especifique el **nombre de la aplicación empresarial** para StorageGRID. Este valor controla el nombre que utiliza para cada aplicación empresarial en Azure AD.

- Por ejemplo, si su red tiene solo un nodo de administración y no prevé agregar más nodos de administración en el futuro, ingrese SG o StorageGRID .
- Si su cuadrícula incluye más de un nodo de administración, incluya la cadena [HOSTNAME] en el identificador. Por ejemplo, SG-[HOSTNAME] . Esto genera una tabla que muestra un nombre de aplicación empresarial para cada nodo de administración en su sistema, según el nombre de host del nodo.



Debe crear una aplicación empresarial para cada nodo de administración en su sistema StorageGRID . Tener una aplicación empresarial para cada nodo de administración garantiza que los usuarios puedan iniciar y cerrar sesión de forma segura en cualquier nodo de administración.

- c. Siga los pasos en ["Crear aplicaciones empresariales en Azure AD"](#) para crear una aplicación empresarial para cada nodo de administración enumerado en la tabla.
- d. Desde Azure AD, copie la URL de metadatos de federación para cada aplicación empresarial. Luego, pegue esta URL en el campo **URL de metadatos de federación** correspondiente en StorageGRID.
- e. Después de haber copiado y pegado una URL de metadatos de federación para todos los nodos de administración, seleccione **Guardar**.

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



Federación de ping

- a. Especifique qué certificado TLS se utilizará para proteger la conexión cuando el proveedor de identidad envíe información de configuración de SSO en respuesta a las solicitudes de

StorageGRID .

- **Usar certificado CA del sistema operativo:** utilice el certificado CA predeterminado instalado en el sistema operativo para proteger la conexión.
- **Usar certificado CA personalizado:** utilice un certificado CA personalizado para proteger la conexión.

Si selecciona esta configuración, copie el texto del certificado personalizado y péguelo en el cuadro de texto **Certificado CA**.

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



Si cambia el certificado de CA, inmediatamente ["reiniciar el servicio mgmt-api en los nodos de administración"](#) y comprobar que el inicio de sesión único (SSO) en Grid Manager es exitoso.

- b. En la sección Proveedor de servicios (SP), especifique el *ID de conexión de SP * para StorageGRID. Este valor controla el nombre que utiliza para cada conexión SP en PingFederate.

- Por ejemplo, si su red tiene solo un nodo de administración y no prevé agregar más nodos de administración en el futuro, ingrese SG o StorageGRID .
- Si su cuadrícula incluye más de un nodo de administración, incluya la cadena [HOSTNAME] en el identificador. Por ejemplo, SG-[HOSTNAME] . Esto genera una tabla que muestra el ID de conexión de SP para cada nodo de administración en su sistema, según el nombre de host del nodo.



Debe crear una conexión SP para cada nodo de administración en su sistema StorageGRID . Tener una conexión SP para cada nodo de administración garantiza que los usuarios puedan iniciar y cerrar sesión de forma segura en cualquier nodo de administración.

- c. Especifique la URL de metadatos de la federación para cada nodo de administración en el campo **URL de metadatos de la federación**.

Utilice el siguiente formato:

```
https://<Federation Service  
Name>:<port>/pf/federation_metadata.ping?PartnerSpId=<SP  
Connection ID>
```

- d. Seleccione **Guardar**.

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

Save 

Configurar relaciones de confianza entre usuarios, aplicaciones empresariales o conexiones de SP

Cuando se guarda la configuración, aparece el aviso de confirmación del modo Sandbox. Este aviso confirma que el modo sandbox ahora está habilitado y proporciona instrucciones generales.

StorageGRID puede permanecer en modo sandbox tanto tiempo como sea necesario. Sin embargo, cuando se selecciona **Modo Sandbox** en la página de Inicio de sesión único, el SSO se deshabilita para todos los usuarios de StorageGRID . Sólo los usuarios locales pueden iniciar sesión.

Siga estos pasos para configurar relaciones de confianza de usuarios autenticados (Active Directory), completar aplicaciones empresariales (Azure) o configurar conexiones de SP (PingFederate).

Directorio activo

Pasos

1. Vaya a Servicios de federación de Active Directory (AD FS).
2. Cree una o más relaciones de confianza de usuario confiable para StorageGRID, utilizando cada identificador de usuario confiable que se muestra en la tabla de la página de inicio de sesión único de StorageGRID .

Debe crear una confianza para cada nodo de administración que se muestra en la tabla.

Para obtener instrucciones, vaya a ["Crear relaciones de confianza entre usuarios autenticados en AD FS"](#) .

Azur

Pasos

1. Desde la página de inicio de sesión único del nodo de administración en el que está conectado actualmente, seleccione el botón para descargar y guardar los metadatos SAML.
2. Luego, para cualquier otro nodo de administración en su red, repita estos pasos:
 - a. Sign in en el nodo.
 - b. Seleccione **CONFIGURACIÓN > Control de acceso > Inicio de sesión único**.
 - c. Descargue y guarde los metadatos SAML para ese nodo.
3. Vaya al Portal de Azure.
4. Siga los pasos en ["Crear aplicaciones empresariales en Azure AD"](#) para cargar el archivo de metadatos SAML para cada nodo de administración en su aplicación empresarial de Azure correspondiente.

Federación de ping

Pasos

1. Desde la página de inicio de sesión único del nodo de administración en el que está conectado actualmente, seleccione el botón para descargar y guardar los metadatos SAML.
2. Luego, para cualquier otro nodo de administración en su red, repita estos pasos:
 - a. Sign in en el nodo.
 - b. Seleccione **CONFIGURACIÓN > Control de acceso > Inicio de sesión único**.
 - c. Descargue y guarde los metadatos SAML para ese nodo.
3. Vaya a PingFederate.
4. ["Cree una o más conexiones de proveedor de servicios \(SP\) para StorageGRID"](#) . Utilice el ID de conexión de SP para cada nodo de administración (que se muestra en la tabla de la página de inicio de sesión único de StorageGRID) y los metadatos SAML que descargó para ese nodo de administración.

Debe crear una conexión SP para cada nodo de administración que se muestra en la tabla.

Probar conexiones SSO

Antes de implementar el uso del inicio de sesión único para todo el sistema StorageGRID , debe confirmar que

el inicio de sesión único y el cierre de sesión único estén configurados correctamente para cada nodo de administración.

Directorio activo

Pasos

1. Desde la página de inicio de sesión único de StorageGRID , busque el enlace en el mensaje del modo Sandbox.

La URL se deriva del valor ingresado en el campo **Nombre del servicio de federación**.

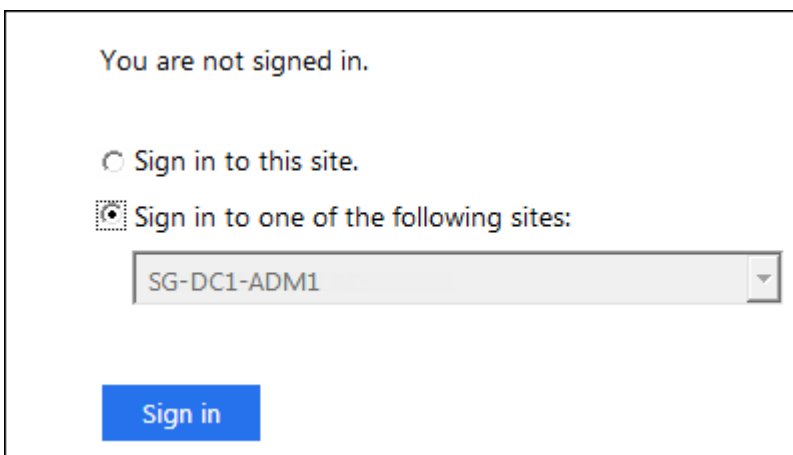
Sandbox mode

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.

2. Seleccione el enlace o copie y pegue la URL en un navegador para acceder a la página de inicio de sesión de su proveedor de identidad.
3. Para confirmar que puede usar SSO para iniciar sesión en StorageGRID, seleccione * Sign in en uno de los siguientes sitios , **seleccione el identificador de parte confiable para su nodo de administración principal y seleccione * Sign in**.



You are not signed in.

☐ Sign in to this site.

☒ Sign in to one of the following sites:

SG-DC1-ADM1

Sign in

4. Introduzca su nombre de usuario y contraseña federados.
 - Si las operaciones de inicio y cierre de sesión SSO son exitosas, aparece un mensaje de éxito.

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

- Si la operación SSO no se realiza correctamente, aparece un mensaje de error. Solucione el problema, borre las cookies del navegador y vuelva a intentarlo.
5. Repita estos pasos para verificar la conexión SSO para cada nodo de administración en su red.

Azur

Pasos

1. Vaya a la página de inicio de sesión único en el portal de Azure.
2. Seleccione **Probar esta aplicación**.
3. Introduzca las credenciales de un usuario federado.
 - Si las operaciones de inicio y cierre de sesión SSO son exitosas, aparece un mensaje de éxito.

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

- Si la operación SSO no se realiza correctamente, aparece un mensaje de error. Solucione el problema, borre las cookies del navegador y vuelva a intentarlo.
4. Repita estos pasos para verificar la conexión SSO para cada nodo de administración en su red.

Federación de ping

Pasos

1. Desde la página de inicio de sesión único de StorageGRID , seleccione el primer enlace en el mensaje del modo Sandbox.

Seleccione y pruebe un enlace a la vez.

Sandbox mode

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

1. Use Ping Federate to create SP connections for StorageGRID. Create one SP connection for each Admin Node, using the relying party identifier(s) shown below.
2. Test SSO and SLO by selecting the link for each Admin Node:
 - [https://\[redacted\]/idp/startSSO.ping?PartnerSpId=SG-DC1-ADM1-106-69](https://[redacted]/idp/startSSO.ping?PartnerSpId=SG-DC1-ADM1-106-69)
 - [https://\[redacted\]/idp/startSSO.ping?PartnerSpId=SG-DC2-ADM1-106-73](https://[redacted]/idp/startSSO.ping?PartnerSpId=SG-DC2-ADM1-106-73)
3. StorageGRID displays a success or error message for each test.

When you have confirmed SSO for each SP connection and you are ready to enforce the use of SSO for StorageGRID, change the SSO Status to Enabled, and select **Save**.

2. Introduzca las credenciales de un usuario federado.
 - Si las operaciones de inicio y cierre de sesión SSO son exitosas, aparece un mensaje de éxito.

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

- Si la operación SSO no se realiza correctamente, aparece un mensaje de error. Solucione el problema, borre las cookies del navegador y vuelva a intentarlo.
3. Seleccione el siguiente enlace para verificar la conexión SSO para cada nodo de administración en su red.

Si ve un mensaje de Página expirada, seleccione el botón **Atrás** en su navegador y vuelva a enviar sus credenciales.

Habilitar el inicio de sesión único

Cuando haya confirmado que puede usar SSO para iniciar sesión en cada nodo de administración, podrá habilitar SSO para todo su sistema StorageGRID .



Cuando SSO está habilitado, todos los usuarios deben usar SSO para acceder al Administrador de Grid, al Administrador de inquilinos, a la API de administración de Grid y a la API de administración de inquilinos. Los usuarios locales ya no pueden acceder a StorageGRID.

Pasos

1. Seleccione **CONFIGURACIÓN > Control de acceso > Inicio de sesión único**.
2. Cambie el estado de SSO a **Habilitado**.
3. Seleccione **Guardar**.
4. Revise el mensaje de advertencia y seleccione **Aceptar**.

El inicio de sesión único ahora está habilitado.



Si usa Azure Portal y accede a StorageGRID desde la misma computadora que usa para acceder a Azure, asegúrese de que el usuario de Azure Portal también sea un usuario autorizado de StorageGRID (un usuario en un grupo federado que se haya importado a StorageGRID) o cierre la sesión en Azure Portal antes de intentar iniciar sesión en StorageGRID.

Crear relaciones de confianza entre usuarios autenticados en AD FS

Debe utilizar los Servicios de federación de Active Directory (AD FS) para crear una relación de confianza de usuario autenticado para cada nodo de administración en su sistema. Puede crear relaciones de confianza de usuario autenticado mediante comandos de PowerShell, importando metadatos SAML desde StorageGRID o ingresando los datos manualmente.

Antes de empezar

- Ha configurado el inicio de sesión único para StorageGRID y seleccionó **AD FS** como tipo de SSO.
- El **modo Sandbox** está seleccionado en la página de inicio de sesión único en Grid Manager. Ver "[Utilizar el modo sandbox](#)".
- Conoce el nombre de dominio completo (o la dirección IP) y el identificador de la parte confiable para cada nodo de administración en su sistema. Puede encontrar estos valores en la tabla de detalles de Nodos de administración en la página de inicio de sesión único de StorageGRID .



Debe crear una relación de confianza de usuario autenticado para cada nodo de administración en su sistema StorageGRID . Tener una relación de confianza de parte confiable para cada nodo de administración garantiza que los usuarios puedan iniciar y cerrar sesión de forma segura en cualquier nodo de administración.

- Tiene experiencia en la creación de relaciones de confianza de usuario autenticado 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.
- Si está creando la confianza de usuario confiable manualmente, tiene el certificado personalizado que se cargó para la interfaz de administración de StorageGRID o sabe cómo iniciar sesión en un nodo de administración desde el shell de comandos.

Acerca de esta tarea

Estas instrucciones se aplican a Windows Server 2016 AD FS. Si está utilizando una versión diferente de AD FS, notará ligeras diferencias en el procedimiento. Si tiene preguntas, consulte la documentación de Microsoft AD FS.

Crear una relación de confianza de usuario autenticado mediante Windows PowerShell

Puede utilizar Windows PowerShell para crear rápidamente una o más relaciones de confianza de usuario autenticado.

Pasos

1. Desde el menú de inicio de Windows, seleccione con el botón derecho el ícono de PowerShell y seleccione **Ejecutar como administrador**.
2. En el símbolo del sistema de PowerShell, ingrese el siguiente comando:

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

- Para *Admin_Node_Identifier*, ingrese el Identificador de parte confiable para el Nodo de administración, exactamente como aparece en la página de Inicio de sesión único. Por ejemplo, SG-DC1-ADM1.
- Para *Admin_Node_FQDN*, ingrese el nombre de dominio completo para el mismo nodo de administración. (Si es necesario, puede utilizar la dirección IP del nodo en su lugar. Sin embargo, si ingresa una dirección IP aquí, tenga en cuenta que debe actualizar o volver a crear esta confianza de parte confiable si esa dirección IP alguna vez cambia).

3. Desde el Administrador de servidor de Windows, seleccione **Herramientas > Administración de AD FS**.

Aparece la herramienta de administración de AD FS.

4. Seleccione **AD FS > Confianzas de usuario autenticado**.

Aparece la lista de fideicomisos de partes confiantes.

5. Agregue una Política de control de acceso a la confianza de usuario autenticado recién creada:

- a. Localice el fideicomiso de parte confiante que acaba de crear.
- b. Haga clic derecho en la confianza y seleccione **Editar política de control de acceso**.
- c. Seleccione una política de control de acceso.
- d. Seleccione **Aplicar** y seleccione **Aceptar**

6. Agregue una Política de emisión de reclamaciones al fideicomiso de parte confiada recién creado:

- a. Localice el fideicomiso de parte confiante que acaba de crear.
- b. Haga clic derecho en el fideicomiso y seleccione **Editar política de emisión de reclamaciones**.
- c. Seleccione **Agregar regla**.

- d. En la página Seleccionar plantilla de regla, seleccione **Enviar atributos LDAP como reclamaciones** de la lista y seleccione **Siguiente**.
- e. En la página Configurar regla, ingrese un nombre para mostrar para esta regla.

Por ejemplo, **ObjectGUID a ID de nombre** o **UPN a ID de nombre**.

- f. Para el almacén de atributos, seleccione **Active Directory**.
 - g. En la columna Atributo LDAP de la tabla Mapeo, escriba **objectGUID** o seleccione **User-Principal-Name**.
 - h. En la columna Tipo de reclamo saliente de la tabla de mapeo, seleccione **ID de nombre** de la lista desplegable.
 - i. Seleccione **Finalizar** y seleccione **Aceptar**.
7. Confirme que los metadatos se importaron correctamente.
- a. Haga clic con el botón derecho en la confianza del usuario confiado para abrir sus propiedades.
 - b. Confirme que los campos en las pestañas **Puntos finales**, **Identificadores** y **Firma** estén completos.

Si faltan los metadatos, confirme que la dirección de metadatos de la Federación sea correcta o ingrese los valores manualmente.

8. Repita estos pasos para configurar una relación de confianza de usuario confiable para todos los nodos de administración en su sistema StorageGRID .
9. Cuando haya terminado, regrese a StorageGRID y pruebe todas las relaciones de confianza de usuarios autenticados para confirmar que estén configuradas correctamente. Ver "[Utilizar el modo Sandbox](#)" para obtener instrucciones.

Cree una relación de confianza entre usuarios autenticados mediante la importación de metadatos de la federación

Puede importar los valores para cada entidad de confianza accediendo a los metadatos SAML de cada nodo de administración.

Pasos

1. En el Administrador de servidor de Windows, seleccione **Herramientas** y, a continuación, seleccione **Administración de AD FS**.
2. En Acciones, seleccione **Agregar confianza de usuario autenticado**.
3. En la página de bienvenida, seleccione **Reclamos conscientes** y seleccione **Iniciar**.
4. Seleccione **Importar datos sobre la parte confiante publicados en línea o en una red local**.
5. En **Dirección de metadatos de la 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*, ingrese el nombre de dominio completo para el mismo nodo de administración. (Si es necesario, puede utilizar la dirección IP del nodo en su lugar. Sin embargo, si ingresa una dirección IP aquí, tenga en cuenta que debe actualizar o volver a crear esta confianza de parte confiable si esa dirección IP alguna vez cambia).

6. Complete el asistente de confianza de usuario autenticado, guarde la confianza de usuario autenticado y cierre el asistente.



Al ingresar el nombre para mostrar, utilice el Identificador de usuario confiado para el Nodo de administración, exactamente como aparece en la página de Inicio de sesión único en el Administrador de Grid. Por ejemplo, SG-DC1-ADM1 .

7. Agregar una regla de reclamación:

- Haga clic derecho en el fideicomiso y seleccione **Editar política de emisión de reclamaciones**.
- Seleccione **Agregar regla**:
- En la página Seleccionar plantilla de regla, seleccione **Enviar atributos LDAP como reclamaciones** de la lista y seleccione **Siguiente**.
- En la página Configurar regla, ingrese un nombre para mostrar para esta regla.

Por ejemplo, **ObjectGUID a ID de nombre** o **UPN a ID de nombre**.

- Para el almacén de atributos, seleccione **Active Directory**.
- En la columna Atributo LDAP de la tabla Mapeo, escriba **objectGUID** o seleccione **User-Principal-Name**.
- En la columna Tipo de reclamo saliente de la tabla de mapeo, seleccione **ID de nombre** de la lista desplegable.
- Seleccione **Finalizar** y seleccione **Aceptar**.

8. Confirme que los metadatos se importaron correctamente.

- Haga clic con el botón derecho en la confianza del usuario confiado para abrir sus propiedades.
- Confirme que los campos en las pestañas **Puntos finales**, **Identificadores** y **Firma** estén completos.

Si faltan los metadatos, confirme que la dirección de metadatos de la Federación sea correcta o ingrese los valores manualmente.

9. Repita estos pasos para configurar una relación de confianza de usuario confiable para todos los nodos de administración en su sistema StorageGRID .

10. Cuando haya terminado, regrese a StorageGRID y pruebe todas las relaciones de confianza de usuarios autenticados para confirmar que estén configuradas correctamente. Ver "[Utilizar el modo Sandbox](#)" para obtener instrucciones.

Crear una relación de confianza de usuario confiado manualmente

Si decide no importar los datos de las confianzas de las partes confiables, puede ingresar los valores manualmente.

Pasos

- En el Administrador de servidor de Windows, seleccione **Herramientas** y, a continuación, seleccione **Administración de AD FS**.
- En Acciones, seleccione **Agregar confianza de usuario autenticado**.
- En la página de bienvenida, seleccione **Reclamos conscientes** y seleccione **Iniciar**.
- Seleccione **Ingresar datos sobre la parte confiada manualmente** y seleccione **Siguiente**.
- Complete el Asistente de confianza de usuario autenticado:
 - Introduzca un nombre para mostrar para este nodo de administración.

Para mantener la coherencia, utilice el Identificador de usuario autenticado para el Nodo de administración, exactamente como aparece en la página de Inicio de sesión único en el Administrador de Grid. Por ejemplo, SG-DC1-ADM1 .

- b. Omita el paso para configurar un certificado de cifrado de token opcional.
- c. En la página Configurar URL, seleccione la casilla de verificación **Habilitar soporte para el protocolo SAML 2.0 WebSSO**.
- d. Escriba la URL del punto final del servicio SAML para el nodo de administración:

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

Para *Admin_Node_FQDN* , ingrese el nombre de dominio completo para el nodo de administración. (Si es necesario, puede utilizar la dirección IP del nodo en su lugar. Sin embargo, si ingresa una dirección IP aquí, tenga en cuenta que debe actualizar o volver a crear esta confianza de parte confiable si esa dirección IP alguna vez cambia).

- e. En la página Configurar identificadores, especifique el identificador de usuario de confianza para el mismo nodo de administración:

Admin_Node_Identifier

Para *Admin_Node_Identifier* , ingrese el Identificador de parte confiable para el Nodo de administración, exactamente como aparece en la página de Inicio de sesión único. Por ejemplo, SG-DC1-ADM1 .

- f. Revise la configuración, guarde la confianza del usuario autenticado y cierre el asistente.

Aparece el cuadro de diálogo Editar política de emisión de reclamaciones.



Si el cuadro de diálogo no aparece, haga clic con el botón derecho en el fideicomiso y seleccione **Editar política de emisión de reclamaciones**.

- 6. Para iniciar el asistente de reglas de reclamación, seleccione **Agregar regla**:
 - a. En la página Seleccionar plantilla de regla, seleccione **Enviar atributos LDAP como reclamaciones** de la lista y seleccione **Siguiente**.
 - b. En la página Configurar regla, ingrese un nombre para mostrar para esta regla.

Por ejemplo, **ObjectGUID a ID de nombre** o **UPN a ID de nombre**.
 - c. Para el almacén de atributos, seleccione **Active Directory**.
 - d. En la columna Atributo LDAP de la tabla Mapeo, escriba **objectGUID** o seleccione **User-Principal-Name**.
 - e. En la columna Tipo de reclamo saliente de la tabla de mapeo, seleccione **ID de nombre** de la lista desplegable.
 - f. Seleccione **Finalizar** y seleccione **Aceptar**.
- 7. Haga clic con el botón derecho en la confianza del usuario confiado para abrir sus propiedades.
- 8. En la pestaña **Puntos finales**, configure el punto final para el cierre de sesión único (SLO):
 - a. Seleccione **Agregar SAML**.

b. Seleccione **Tipo de punto final > Cerrar sesión SAML**.

c. Seleccione **Enlace > Redireccionar**.

d. En el campo **URL de confianza**, ingrese la URL utilizada para el cierre de sesión único (SLO) desde este nodo de administración:

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

Para *Admin_Node_FQDN*, ingrese el nombre de dominio completo del nodo de administración. (Si es necesario, puede utilizar la dirección IP del nodo en su lugar. Sin embargo, si ingresa una dirección IP aquí, tenga en cuenta que debe actualizar o volver a crear esta confianza de parte confiable si esa dirección IP alguna vez cambia).

a. Seleccione **Aceptar**.

9. En la pestaña **Firma**, especifique el certificado de firma para esta relación de confianza de usuario autenticado:

a. Agregue el certificado personalizado:

- Si tiene el certificado de administración personalizado que cargó en StorageGRID, seleccione ese certificado.
- Si no tiene el certificado personalizado, inicie sesión en el Nodo de administración, vaya a `/var/local/mgmt-api` directorio del nodo de administración y agregue el `custom-server.crt` archivo de certificado.



Uso del certificado predeterminado del nodo de administración(`server.crt`) no se recomienda. Si el nodo de administración falla, se regenerará el certificado predeterminado cuando recupere el nodo y deberá actualizar la confianza de la parte confiable.

b. Seleccione **Aplicar** y seleccione **Aceptar**.

Las propiedades de la parte confiada se guardan y cierran.

10. Repita estos pasos para configurar una relación de confianza de usuario confiable para todos los nodos de administración en su sistema StorageGRID .

11. Cuando haya terminado, regrese a StorageGRID y pruebe todas las relaciones de confianza de usuarios autenticados para confirmar que estén configuradas correctamente. Ver "[Utilizar el modo sandbox](#)" para obtener instrucciones.

Crear aplicaciones empresariales en Azure AD

Utilice Azure AD para crear una aplicación empresarial para cada nodo de administración en su sistema.

Antes de empezar

- Ha comenzado a configurar el inicio de sesión único para StorageGRID y seleccionó **Azure** como tipo de SSO.
- El **modo Sandbox** está seleccionado en la página de inicio de sesión único en Grid Manager. Ver "[Utilizar el modo sandbox](#)".
- Tiene el **nombre de la aplicación empresarial** para cada nodo de administración en su sistema. Puede

copiar estos valores de la tabla de detalles del nodo de administración en la página de inicio de sesión único de StorageGRID .



Debe crear una aplicación empresarial para cada nodo de administración en su sistema StorageGRID . Tener una aplicación empresarial para cada nodo de administración garantiza que los usuarios puedan iniciar y cerrar sesión de forma segura en cualquier nodo de administración.

- Tiene experiencia en la creación de aplicaciones empresariales en Azure Active Directory.
- Tiene una cuenta de Azure con una suscripción activa.
- Tiene uno de los siguientes roles en la cuenta de Azure: Administrador global, Administrador de aplicaciones en la nube, Administrador de aplicaciones o propietario de la entidad de servicio.

Acceder a Azure AD

Pasos

1. Iniciar sesión en el "[Portal de Azure](#)" .
2. Navegar a "[Directorio activo de Azure](#)" .
3. Seleccionar "[Aplicaciones empresariales](#)" .

Cree aplicaciones empresariales y guarde la configuración de SSO de StorageGRID

Para guardar la configuración de SSO para Azure en StorageGRID, debe usar Azure para crear una aplicación empresarial para cada nodo de administración. Copiará las URL de metadatos de federación de Azure y las pegará en los campos **URL de metadatos de federación** correspondientes en la página de inicio de sesión único de StorageGRID .

Pasos

1. Repita los siguientes pasos para cada nodo de administración.
 - a. En el panel de aplicaciones empresariales de Azure, seleccione **Nueva aplicación**.
 - b. Seleccione **Crea tu propia aplicación**.
 - c. Para el nombre, ingrese el **nombre de la aplicación empresarial** que copió de la tabla de detalles del nodo de administración en la página de inicio de sesión único de StorageGRID .
 - d. Deje seleccionado el botón de opción **Integrar cualquier otra aplicación que no encuentre en la galería (No galería)**.
 - e. Seleccione **Crear**.
 - f. Seleccione el enlace **Comenzar** en el **2. Configurar el cuadro de inicio de sesión único** o seleccione el enlace **Inicio de sesión único** en el margen izquierdo.
 - g. Seleccione la casilla **SAML**.
 - h. Copie la **URL de metadatos de federación de aplicaciones**, que puede encontrar en el **Paso 3 Certificado de firma SAML**.
 - i. Vaya a la página de inicio de sesión único de StorageGRID y pegue en el campo **URL de metadatos de federación** la URL que corresponde al **nombre de la aplicación empresarial** que utilizó.
2. Después de haber pegado una URL de metadatos de federación para cada nodo de administración y realizado todos los demás cambios necesarios en la configuración de SSO, seleccione **Guardar** en la página de inicio de sesión único de StorageGRID .

Descargar metadatos SAML para cada nodo de administración

Una vez guardada la configuración de SSO, puede descargar un archivo de metadatos SAML para cada nodo de administración en su sistema StorageGRID .

Pasos

1. Repita estos pasos para cada nodo de administración.
 - a. Sign in en StorageGRID desde el nodo de administración.
 - b. Seleccione **CONFIGURACIÓN > Control de acceso > Inicio de sesión único**.
 - c. Seleccione el botón para descargar los metadatos SAML para ese nodo de administración.
 - d. Guarde el archivo que cargará en Azure AD.

Cargar metadatos SAML a cada aplicación empresarial

Después de descargar un archivo de metadatos SAML para cada nodo de administración de StorageGRID , realice los siguientes pasos en Azure AD:

Pasos

1. Regresar al Portal de Azure.
2. Repita estos pasos para cada aplicación empresarial:



Es posible que necesites actualizar la página de aplicaciones empresariales para ver las aplicaciones que agregaste previamente a la lista.

- a. Vaya a la página Propiedades de la aplicación empresarial.
 - b. Establezca **Tarea requerida** en **No** (a menos que desee configurar las asignaciones por separado).
 - c. Vaya a la página de inicio de sesión único.
 - d. Complete la configuración de SAML.
 - e. Seleccione el botón **Cargar archivo de metadatos** y seleccione el archivo de metadatos SAML que descargó para el nodo de administración correspondiente.
 - f. Después de cargar el archivo, seleccione **Guardar** y luego seleccione **X** para cerrar el panel. Regresará a la página Configurar inicio de sesión único con SAML.
3. Siga los pasos en "[Utilizar el modo sandbox](#)" para probar cada aplicación.

Crear conexiones de proveedor de servicios (SP) en PingFederate

Utilice PingFederate para crear una conexión de proveedor de servicios (SP) para cada nodo de administración en su sistema. Para acelerar el proceso, importará los metadatos SAML desde StorageGRID.

Antes de empezar

- Ha configurado el inicio de sesión único para StorageGRID y seleccionó **Ping Federate** como tipo de SSO.
- El **modo Sandbox** está seleccionado en la página de inicio de sesión único en Grid Manager. Ver "[Utilizar el modo sandbox](#)".

- Tienes el *ID de conexión SP* para cada nodo de administración en tu sistema. Puede encontrar estos valores en la tabla de detalles de Nodos de administración en la página de inicio de sesión único de StorageGRID.
- Ha descargado los **metadatos SAML** para cada nodo de administración en su sistema.
- Tiene experiencia en la creación de conexiones SP en PingFederate Server.
- Tú tienes [el](https://docs.pingidentity.com/pingfederate/latest/administrators_reference_guide/pf_administrators_reference_guide.html) https://docs.pingidentity.com/pingfederate/latest/administrators_reference_guide/pf_administrators_reference_guide.html ["Guía de referencia del administrador"] para el servidor PingFederate. La documentación de PingFederate proporciona instrucciones y explicaciones detalladas paso a paso.
- Tú tienes el **"Permiso de administrador"** para el servidor PingFederate.

Acerca de esta tarea

Estas instrucciones resumen cómo configurar PingFederate Server versión 10.3 como proveedor de SSO para StorageGRID. Si está utilizando otra versión de PingFederate, es posible que deba adaptar estas instrucciones. Consulte la documentación del servidor PingFederate para obtener instrucciones detalladas para su versión.

Requisitos previos completos en PingFederate

Antes de poder crear las conexiones SP que utilizará para StorageGRID, debe completar las tareas previas requeridas en PingFederate. Utilizará la información de estos requisitos previos cuando configure las conexiones del SP.

Crear almacén de datos[[almacén de datos]]

Si aún no lo ha hecho, cree un almacén de datos para conectar PingFederate al servidor LDAP de AD FS. Utilice los valores que utilizó cuando **"configuración de la federación de identidades"** en StorageGRID.

- **Tipo:** Directorio (LDAP)
- **Tipo LDAP:** Directorio activo
- **Nombre del atributo binario:** Ingrese **objectGUID** en la pestaña Atributos binarios LDAP exactamente como se muestra.

Crear un validador de credenciales de contraseña

Si aún no lo ha hecho, cree un validador de credenciales de contraseña.

- **Tipo:** LDAP Nombre de usuario Contraseña Credencial Validador
- **Almacén de datos:** seleccione el almacén de datos que creó.
- **Base de búsqueda:** Ingrese información de LDAP (por ejemplo, DC=saml,DC=sgws).
- **Filtro de búsqueda:** sAMAccountName=\${username}
- **Alcance:** Subárbol

Crear una instancia de adaptador de IdP

Si aún no lo ha hecho, cree una instancia de adaptador IdP.

Pasos

1. Vaya a **Autenticación > Integración > Adaptadores IdP**.

2. Seleccione **Crear nueva instancia**.
3. En la pestaña Tipo, seleccione **Adaptador IdP de formulario HTML**.
4. En la pestaña Adaptador IdP, seleccione **Agregar una nueva fila a 'Validadores de credenciales'**.
5. Seleccione el [validador de credenciales de contraseña](#) que cree.
6. En la pestaña Atributos del adaptador, seleccione el atributo **nombre de usuario** para **Seudónimo**.
7. Seleccione **Guardar**.

Crear o importar certificado de firma

Si aún no lo ha hecho, cree o importe el certificado de firma.

Pasos

1. Vaya a **Seguridad > Claves y certificados de firma y descifrado**.
2. Cree o importe el certificado de firma.

Crear una conexión SP en PingFederate

Cuando crea una conexión SP en PingFederate, importa los metadatos SAML que descargó de StorageGRID para el nodo de administración. El archivo de metadatos contiene muchos de los valores específicos que necesita.



Debe crear una conexión SP para cada nodo de administración en su sistema StorageGRID, de modo que los usuarios puedan iniciar y cerrar sesión de forma segura en cualquier nodo. Utilice estas instrucciones para crear la primera conexión SP. Luego, ve a [Crear conexiones SP adicionales](#) para crear cualquier conexión adicional que necesite.

Elija el tipo de conexión SP

Pasos

1. Vaya a **Aplicaciones > Integración > *Conexiones SP ***.
2. Seleccione **Crear conexión**.
3. Seleccione **No utilizar una plantilla para esta conexión**.
4. Seleccione **Perfiles SSO del navegador** y **SAML 2.0** como protocolo.

Importar metadatos de SP

Pasos

1. En la pestaña Importar metadatos, seleccione **Archivo**.
2. Elija el archivo de metadatos SAML que descargó de la página de inicio de sesión único de StorageGRID para el nodo de administración.
3. Revise el Resumen de metadatos y la información proporcionada en la pestaña Información general.

El ID de entidad del socio y el nombre de la conexión se establecen en el ID de conexión de StorageGRID SP. (por ejemplo, 10.96.105.200-DC1-ADM1-105-200). La URL base es la IP del nodo de administración de StorageGRID.

4. Seleccione **Siguiente**.

Configurar el inicio de sesión único (SSO) del navegador IdP

Pasos

1. Desde la pestaña SSO del navegador, seleccione **Configurar SSO del navegador**.
2. En la pestaña Perfiles SAML, seleccione las opciones * SP-initiated SSO*, * SP-initial SLO*, **IdP-initiated SSO** y **IdP-initiated SLO**.
3. Seleccione **Siguiente**.
4. En la pestaña Duración de la afirmación, no realice cambios.
5. En la pestaña Creación de aserciones, seleccione **Configurar creación de aserciones**.
 - a. En la pestaña Asignación de identidad, seleccione **Estándar**.
 - b. En la pestaña Contrato de atributo, utilice **SAML_SUBJECT** como Contrato de atributo y el formato de nombre no especificado que se importó.
6. Para extender el contrato, seleccione **Eliminar** para quitar el `urn:oid`, que no se utiliza.

Instancia del adaptador de mapas

Pasos

1. En la pestaña Mapeo de origen de autenticación, seleccione **Asignar nueva instancia de adaptador**.
2. En la pestaña Instancia del adaptador, seleccione la [instancia de adaptador](#) que creaste.
3. En la pestaña Método de mapeo, seleccione **Recuperar atributos adicionales de un almacén de datos**.
4. En la pestaña Origen de atributos y búsqueda de usuarios, seleccione **Agregar origen de atributos**.
5. En la pestaña Almacén de datos, proporcione una descripción y seleccione la [almacén de datos](#) que usted agregó.
6. En la pestaña Búsqueda de directorio LDAP:
 - Ingrese el **DN base**, que debe coincidir exactamente con el valor ingresado en StorageGRID para el servidor LDAP.
 - Para el ámbito de búsqueda, seleccione **Subárbol**.
 - Para la clase de objeto raíz, busque y agregue cualquiera de estos atributos: **objectGUID** o **userPrincipalName**.
7. En la pestaña Tipos de codificación de atributos binarios LDAP, seleccione **Base64** para el atributo **objectGUID**.
8. En la pestaña Filtro LDAP, ingrese **sAMAccountName=\${username}**.
9. En la pestaña Cumplimiento de contrato de atributo, seleccione **LDAP (atributo)** en el menú desplegable Fuente y seleccione **objectGUID** o **userPrincipalName** en el menú desplegable Valor.
10. Revise y luego guarde la fuente del atributo.
11. En la pestaña Origen del atributo de guardado fallido, seleccione **Anular la transacción SSO**.
12. Revise el resumen y seleccione **Listo**.
13. Seleccione **Listo**.

Configurar los ajustes del protocolo

Pasos

1. En la pestaña **Conexión SP * > *SSO del navegador > Configuración del protocolo**, seleccione

Configurar configuración del protocolo.

2. En la pestaña URL del servicio de consumidor de aserciones, acepte los valores predeterminados, que se importaron de los metadatos SAML de StorageGRID (**POST** para enlace y `/api/saml-response` para la URL del punto final).
3. En la pestaña URL del servicio SLO, acepte los valores predeterminados, que se importaron de los metadatos SAML de StorageGRID (**REDIRECT** para enlace y `/api/saml-logout` para URL de punto final).
4. En la pestaña Enlaces SAML permitidos, desactive **ARTIFACT** y **SOAP**. Sólo se requieren **POST** y **REDIRECT**.
5. En la pestaña Política de firma, deje seleccionadas las casillas de verificación **Requerir que las solicitudes de autenticación estén firmadas** y **Firmar siempre la afirmación**.
6. En la pestaña Política de cifrado, seleccione **Ninguno**.
7. Revise el resumen y seleccione **Listo** para guardar la configuración del protocolo.
8. Revise el resumen y seleccione **Listo** para guardar la configuración de SSO del navegador.

Configurar credenciales

Pasos

1. Desde la pestaña Conexión SP , seleccione **Credenciales**.
2. Desde la pestaña Credenciales, seleccione **Configurar credenciales**.
3. Seleccione el [certificado de firma](#) usted creó o importó.
4. Seleccione **Siguiente** para ir a **Administrar configuración de verificación de firma**.
 - a. En la pestaña Modelo de confianza, seleccione **Sin ancla**.
 - b. En la pestaña Certificado de verificación de firma, revise la información del certificado de firma, que se importó de los metadatos SAML de StorageGRID .
5. Revise las pantallas de resumen y seleccione **Guardar** para guardar la conexión SP .

Crear conexiones SP adicionales

Puede copiar la primera conexión SP para crear las conexiones SP que necesita para cada nodo de administración en su red. Carga nuevos metadatos para cada copia.



Las conexiones SP para diferentes nodos de administración utilizan configuraciones idénticas, con la excepción del ID de entidad del socio, la URL base, el ID de conexión, el nombre de la conexión, la verificación de firma y la URL de respuesta de SLO.

Pasos

1. Seleccione **Acción** > **Copiar** para crear una copia de la conexión SP inicial para cada nodo de administración adicional.
2. Ingrese el ID de conexión y el nombre de conexión para la copia y seleccione **Guardar**.
3. Seleccione el archivo de metadatos correspondiente al Nodo de Administración:
 - a. Seleccione **Acción** > **Actualizar con metadatos**.
 - b. Seleccione **Elegir archivo** y cargue los metadatos.
 - c. Seleccione **Siguiente**.

- d. Seleccione **Guardar**.
4. Resuelva el error debido al atributo no utilizado:
 - a. Seleccione la nueva conexión.
 - b. Seleccione **Configurar SSO del navegador > Configurar creación de afirmaciones > Contrato de atributos**.
 - c. Eliminar la entrada para **urn:oid**.
 - d. Seleccione **Guardar**.

Deshabilitar el inicio de sesión único

Puede desactivar el inicio de sesión único (SSO) si ya no desea utilizar esta funcionalidad. Debe deshabilitar el inicio de sesión único antes de poder deshabilitar la federación de identidad.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes ["permisos de acceso específicos"](#).

Pasos

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

Aparece la página de inicio de sesión único.

2. Seleccione la opción **Deshabilitado**.
3. Seleccione **Guardar**.

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

4. Seleccione **Aceptar**.

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

Deshabilitar temporalmente y volver a habilitar el inicio de sesión único para un nodo de administración

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

Antes de empezar

- Tienes ["permisos de acceso específicos"](#).
- Tú tienes el `Passwords.txt` archivo.
- Conoces la contraseña del usuario root 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 su sistema StorageGRID , debe usar el shell de comandos del nodo para volver a habilitar SSO en el nodo de administración tan pronto como cierre la sesión.



Deshabilitar SSO para un nodo de administración no afecta la configuración de SSO de ningún otro nodo de administración en la red. La casilla de verificación **Habilitar SSO** en la página de Inicio de sesión único en el Administrador de Grid permanece seleccionada y todas las configuraciones de SSO existentes se mantienen a menos que las actualice.

Pasos

1. Inicie sesión en un nodo de administración:

- Introduzca el siguiente comando: `ssh admin@Admin_Node_IP`
- Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
- Introduzca el siguiente comando para cambiar a root: `su -`
- Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

Cuando inicia sesión como root, el mensaje cambia de \$ a # .

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

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

3. Confirme que desea deshabilitar SSO.

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

4. Desde un navegador web, acceda al Administrador de cuadrícula en el mismo nodo de administración.

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

5. Sign in con el nombre de usuario root y la contraseña del usuario root local.

6. Si deshabilitó SSO temporalmente porque necesitaba corregir la configuración de SSO:

- Seleccione **CONFIGURACIÓN > Control de acceso > Inicio de sesión único**.
- Cambie la configuración de SSO incorrecta o desactualizada.
- Seleccione **Guardar**.

Al seleccionar **Guardar** en la página de inicio de sesión único, se vuelve a habilitar automáticamente el SSO para toda la red.

7. Si deshabilitó el SSO temporalmente porque necesitaba acceder al Administrador de Grid por algún otro motivo:

- Realice cualquier tarea o tareas que necesite realizar.
- Seleccione **Cerrar sesión** y cierre el Administrador de cuadrícula.
- Vuelva a habilitar SSO en el nodo de administración. 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 administración.

Confirme que desea habilitar SSO.

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

° Reiniciar el nodo de la red: `reboot`

8. Desde un navegador web, acceda al Administrador de cuadrícula desde el mismo nodo de administración.
9. Confirme que aparezca la página de Sign in de StorageGRID y que debe ingresar sus credenciales de SSO para acceder al Administrador de Grid.

Información de copyright

Copyright © 2025 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.