



Control del acceso a StorageGRID

StorageGRID software

NetApp

January 14, 2026

Tabla de contenidos

Control del acceso a StorageGRID	1
Control del acceso a StorageGRID	1
Controle el acceso a Grid Manager	1
Active el inicio de sesión único	1
Cambie la clave de acceso de aprovisionamiento	1
Cambie las contraseñas de la consola de los nodos	1
Cambie la clave de acceso del aprovisionamiento	2
Cambie las contraseñas de la consola de los nodos	3
Acceda al asistente	3
Descargue el paquete de recuperación actual	3
Proporcionar nuevas contraseñas	4
Completar el cambio de contraseña	4
Cambiar las contraseñas de acceso SSH para los nodos de administración	5
Acceda al asistente	5
Descargue el paquete de recuperación actual	6
Cambiar las claves de acceso SSH	6
Usar la federación de identidades	7
Configurar la federación de identidades para Grid Manager	7
Forzar la sincronización con el origen de identidades	11
Deshabilitar la federación de identidades	11
Instrucciones para configurar un servidor OpenLDAP	12
Gestione los grupos de administradores	12
Cree un grupo de administración	13
Consulte y edite los grupos de administración	14
Duplicar un grupo	15
Eliminar un grupo	15
Permisos de grupo de administradores	15
Interacción entre permisos y modo de acceso	16
Acceso raíz	16
Cambiar la contraseña raíz del inquilino	16
ILM	16
Mantenimiento	17
Gestionar alertas	17
Consulta de métricas	18
Búsqueda de metadatos de objetos	18
Otra configuración de cuadrícula	18
Administrador de dispositivos de almacenamiento	18
Cuentas de inquilino	18
Gestionar usuarios	18
Cree un usuario local	19
Ver y editar usuarios locales	19
Importar usuarios federados	21
Duplique un usuario	21

Eliminar un usuario	22
Utilizar inicio de sesión único (SSO)	22
Cómo funciona el SSO	22
Requisitos y consideraciones para SSO	24
Confirmar que los usuarios federados pueden iniciar sesión	26
Configurar SSO	27
Crear confianzas de parte de confianza en AD FS	34
Crear aplicaciones empresariales en Entra ID	39
Cree conexiones de proveedores de servicios (SP) en PingFederate	41
Deshabilitar SSO	45
Deshabilitar y volver a habilitar temporalmente el SSO para un nodo de administración	46

Control del acceso a StorageGRID

Control del acceso a StorageGRID

Puede controlar quién puede acceder a StorageGRID y qué tareas pueden realizar los usuarios creando o importando grupos y usuarios, y asignando permisos a cada grupo. De manera opcional, puede habilitar el inicio de sesión único (SSO), crear certificados de cliente y cambiar contraseñas de grid.

Controle el acceso a Grid Manager

Para determinar quién puede acceder a Grid Manager y a la API de gestión de grid, importe grupos y usuarios desde un servicio de federación de identidades o configure grupos locales y usuarios locales.

El uso ["federación de identidades"](#) hace que la configuración ["grupos"](#) ["usuarios"](#) sea más rápida, y permite a los usuarios iniciar sesión en StorageGRID usando credenciales conocidas. Puede configurar la federación de identidades si utiliza Active Directory, OpenLDAP u Oracle Directory Server.



Póngase en contacto con el soporte técnico si desea utilizar otro servicio LDAP v3.

Para determinar qué tareas puede realizar cada usuario, asigne diferentes ["permisos"](#) a cada grupo. Por ejemplo, es posible que desee que los usuarios de un grupo puedan gestionar las reglas de ILM y los usuarios de otro grupo para realizar tareas de mantenimiento. Un usuario debe pertenecer al menos a un grupo para acceder al sistema.

De manera opcional, puede configurar un grupo para que sea de sólo lectura. Los usuarios de un grupo de sólo lectura sólo pueden ver la configuración y las funciones. No pueden realizar cambios ni realizar ninguna operación en Grid Manager o la API de administración de grid.

Active 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). Después de usted ["Configure y habilite SSO"](#) Todos los usuarios deben estar autenticados por un proveedor de identidad externo antes de poder acceder al Administrador de Grid, al Administrador de Inquilinos, a la API de Administración de Grid o a la API de Administración de Inquilinos. Los usuarios locales no pueden iniciar sesión en StorageGRID.

Cambie la clave de acceso de aprovisionamiento

La frase de contraseña de aprovisionamiento es necesaria para muchos procedimientos de instalación y mantenimiento, y para descargar el paquete de recuperación de StorageGRID . La frase de contraseña también es necesaria para descargar copias de seguridad de la información de topología de la red y de las claves de cifrado para el sistema StorageGRID . Puede ["cambie la contraseña"](#) según sea necesario.

Cambie las contraseñas de la consola de los nodos

Cada nodo de su red tiene una contraseña de consola de nodo, que necesita para iniciar sesión en el nodo como "admin" mediante SSH, o como usuario root en una conexión de consola física/VM. Según sea necesario, puede ["cambie la contraseña de la consola del nodo"](#) para cada nodo.

Cambie la clave de acceso del aprovisionamiento

Utilice este procedimiento para cambiar la frase de contraseña de aprovisionamiento de StorageGRID . La frase de contraseña es necesaria para los procedimientos de recuperación, expansión y mantenimiento. La frase de contraseña también es necesaria para descargar copias de seguridad del paquete de recuperación que incluyen la información de topología de la red, las contraseñas de la consola del nodo de la red y las claves de cifrado para el sistema StorageGRID .

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante una ["navegador web compatible"](#).
- Tiene permisos de acceso raíz o de mantenimiento.
- Tiene la clave de acceso de aprovisionamiento actual.

Acerca de esta tarea

La frase de contraseña de aprovisionamiento es necesaria para muchos procedimientos de instalación y mantenimiento, y para ["descargando el paquete de recuperación"](#) . La frase de contraseña de aprovisionamiento no aparece en la `Passwords.txt` archivo. Asegúrese de documentar la contraseña de aprovisionamiento y guardarla en un lugar seguro.

Pasos

1. Seleccione **Configuración > Control de acceso> Contraseñas de red**.
2. En **Cambiar contraseña de aprovisionamiento**, selecciona **Hacer un cambio**
3. Introduzca la clave de acceso de aprovisionamiento actual.
4. Introduzca la nueva frase de contraseña. La frase de contraseña debe contener al menos 8 caracteres y no más de 32. Las passphrasas distinguen entre mayúsculas y minúsculas.



Guarde la contraseña de aprovisionamiento en una ubicación segura. Es necesario para los procedimientos de instalación, expansión y mantenimiento.

5. Vuelva a introducir la nueva contraseña y seleccione **Guardar**.

El sistema muestra un banner verde de éxito cuando se completa el cambio de la clave de acceso de aprovisionamiento.



Provisioning passphrase successfully changed. Go to the [Recovery Package](#) to download a new Recovery Package.

6. Seleccione **paquete de recuperación**.
7. Ingrese la nueva contraseña de aprovisionamiento para descargar el nuevo paquete de recuperación.



Después de cambiar la contraseña de aprovisionamiento, debe descargar inmediatamente un nuevo paquete de recuperación. El archivo del paquete de recuperación le permite restaurar el sistema si ocurre una falla.

Cambie las contraseñas de la consola de los nodos

Cada nodo de su red tiene una contraseña de consola de nodo, que usted utiliza para iniciar sesión en el nodo. De forma predeterminada, cada nodo tiene una contraseña única. Puede cambiar cada contraseña por una nueva contraseña única o puede cambiar la contraseña de cada nodo para utilizar una contraseña global. Las contraseñas se almacenan en el paquete de recuperación.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante una ["navegador web compatible"](#).
- Usted tiene el ["Permiso de mantenimiento o acceso raíz"](#).
- Tiene la clave de acceso de aprovisionamiento actual.

Acerca de esta tarea

Utilice una contraseña de consola de nodo para iniciar sesión en un nodo como "admin" mediante SSH, o como usuario root en una conexión de consola física/VM. Puede cambiar las contraseñas de la consola del nodo utilizando una de estas opciones:

- Aplicar automáticamente contraseñas aleatorias a cada nodo
- Especifique y aplique una contraseña global a todos los nodos
- Especificar y aplicar una contraseña única a uno o más nodos

Las contraseñas se almacenan de forma actualizada. `Passwords.txt` archivo en el paquete de recuperación. Las contraseñas se enumeran en la columna Contraseña del archivo.



El ["Contraseñas de acceso SSH"](#) Las claves SSH utilizadas para la comunicación entre nodos son independientes de las contraseñas de la consola del nodo. Este procedimiento no cambia las contraseñas de acceso SSH.

Acceda al asistente

Pasos

1. Seleccione **Configuración > Control de acceso > Contraseñas de red**.
2. En **Cambiar contraseñas de consola de nodo**, selecciona **Hacer un cambio**.

Descargue el paquete de recuperación actual

Antes de cambiar las contraseñas de la consola del nodo, descargue el paquete de recuperación actual. Puede utilizar las contraseñas de este archivo si el proceso de cambio de contraseña falla para algún nodo.

Pasos

1. Introduzca la clave de acceso de aprovisionamiento para el grid.
2. Seleccione **Descargar paquete de recuperación**.
3. Copiar el archivo del paquete de recuperación(`.zip`) a dos lugares seguros, protegidos y separados.



El archivo del paquete de recuperación debe estar protegido porque contiene claves de cifrado y contraseñas que se pueden utilizar para obtener datos del sistema StorageGRID .

4. Seleccione **continuar**.

Proporcionar nuevas contraseñas

1. Seleccione el método de cambio de contraseña que desea utilizar.
 - **Automático:** StorageGRID asigna automáticamente una nueva contraseña de consola aleatoria a todos los nodos.
 - **Personalizado:** proporcionas contraseñas de consola.

Automático

1. Seleccione **continuar**.

Personalizado

1. Seleccione una de las siguientes opciones:
 - **Contraseña de consola global:** aplica la misma contraseña de consola a todos los nodos.
 - **Contraseñas de consola únicas:** aplique una contraseña diferente en uno o más nodos.
2. Si seleccionó **Contraseña de consola global**, ingrese la contraseña que desea usar para todos los nodos.
3. Si seleccionó **Contraseñas de consola únicas**, ingrese una contraseña única para uno o más nodos.
4. Seleccione **continuar**.

Completar el cambio de contraseña

1. Cuando aparezca el cuadro de diálogo de confirmación, seleccione **Sí** si está listo para que StorageGRID comience a cambiar las contraseñas de la consola del nodo.



No puede cancelar este proceso una vez que se inicia.

StorageGRID genera un nuevo paquete de recuperación que contiene la nueva contraseña.

2. Cuando el nuevo paquete de recuperación esté listo, seleccione **Descargar nuevo paquete de recuperación** y guarde el paquete de recuperación.
3. Abra el `.zip` archivo.
4. Confirme que puede acceder al contenido, incluido `Passwords.txt` el archivo, que contiene las nuevas contraseñas de la consola del nodo.
5. Copiar el nuevo archivo del paquete de recuperación(`.zip`) a dos lugares seguros, protegidos y separados.



No sobrescriba el paquete de recuperación antiguo.

Debe proteger el archivo de recuperación, ya que contiene claves de cifrado y contraseñas que se pueden utilizar para obtener datos del sistema StorageGRID.

6. Seleccione la casilla de verificación para indicar que ha descargado el nuevo paquete de recuperación y verificado el contenido.

7. Seleccione **continuar**.

StorageGRID actualiza la contraseña de cada nodo.

Si hay un error durante el proceso de actualización, la barra de progreso enumera la cantidad de nodos cuyas contraseñas no se pudieron cambiar. El sistema volverá a intentar automáticamente el proceso en cualquier nodo cuya contraseña no se haya podido cambiar. Si el proceso finaliza con algunos nodos que aún no tienen la contraseña cambiada, aparece el botón **Reintentar**.

8. Si la actualización de la contraseña falló para uno o más nodos:

- a. Revise los mensajes de error que aparecen en la tabla.
- b. Resuelva los problemas.
- c. Seleccione **Reintentar**.



Al volver a intentar solo se cambian las contraseñas de la consola de nodos en los nodos que fallaron durante los intentos anteriores de cambio de contraseña.

9. Cuando la barra de progreso indique que no quedan actualizaciones, seleccione **Finalizar**.

10. Después de cambiar las contraseñas de la consola de nodo para todos los nodos, elimine el archivo [primer paquete de recuperación que descargaste](#).

Cambiar las contraseñas de acceso SSH para los nodos de administración

Al cambiar las contraseñas de acceso SSH para los nodos de administración, también se actualizan los conjuntos únicos de claves SSH internas de cada nodo del grid. El nodo de administración principal utiliza estas claves SSH para acceder a los nodos utilizando una autenticación segura y sin contraseña.

Utilice una clave SSH para iniciar sesión en un nodo `admin` como o para el usuario raíz en una máquina virtual o una conexión de consola física.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante una ["navegador web compatible"](#).
- Usted tiene el ["Permiso de mantenimiento o acceso raíz"](#).
- Tiene la clave de acceso de aprovisionamiento actual.

Acerca de esta tarea

Las nuevas contraseñas de acceso para los nodos de administración y las nuevas claves internas para cada nodo se almacenan en el `Passwords.txt` archivo en el paquete de recuperación. Las claves se enumeran en la columna Contraseña de ese archivo.

Hay contraseñas de acceso SSH separadas para las claves SSH que se usan para la comunicación entre nodos. Estos no se modifican con este procedimiento.

Acceda al asistente

Pasos

1. Seleccione **Configuración > Control de acceso > Contraseñas de red**.
2. En **Cambiar claves SSH**, selecciona **Hacer un cambio**.

Descargue el paquete de recuperación actual

Antes de cambiar las claves de acceso SSH, descargue el paquete de recuperación actual. Puede utilizar las claves de este archivo si el proceso de cambio de clave falla para algún nodo.

Pasos

1. Introduzca la clave de acceso de aprovisionamiento para el grid.
2. Seleccione **Descargar paquete de recuperación**.
3. Copiar el archivo del paquete de recuperación(.zip) a dos lugares seguros, protegidos y separados.



El archivo del paquete de recuperación debe estar protegido porque contiene claves de cifrado y contraseñas que se pueden utilizar para obtener datos del sistema StorageGRID .

4. Seleccione **continuar**.
5. Cuando aparezca el cuadro de diálogo de confirmación, seleccione **Sí** si está listo para comenzar a cambiar las claves de acceso SSH.



No puede cancelar este proceso una vez que se inicia.

Cambiar las claves de acceso SSH

Cuando se inicia el proceso de cambio de claves de acceso SSH, se genera un nuevo paquete de recuperación que incluye las nuevas claves. Luego, las claves se actualizan en cada nodo.

Pasos

1. Espere a que se genere el nuevo paquete de recuperación, lo que puede tardar unos minutos.
2. Cuando el botón Descargar nuevo paquete de recuperación esté habilitado, seleccione **Descargar nuevo paquete de recuperación** y guarde el archivo del nuevo paquete de recuperación(.zip) a dos lugares seguros, protegidos y separados.
3. Cuando finalice la descarga:
 - a. Abra el .zip archivo.
 - b. Confirme que puede acceder al contenido, incluido `Passwords.txt` el archivo, que contiene las nuevas claves de acceso SSH.
 - c. Copiar el nuevo archivo del paquete de recuperación(.zip) a dos lugares seguros, protegidos y separados.



No sobrescriba el paquete de recuperación antiguo.

El archivo del paquete de recuperación debe estar protegido porque contiene claves de cifrado y contraseñas que se pueden utilizar para obtener datos del sistema StorageGRID .

4. Espere a que las claves se actualicen en cada nodo, lo que puede tardar unos minutos.

Si se cambian las claves para todos los nodos, aparece un banner verde correcto.

Si se produce un error durante el proceso de actualización, un mensaje de banner muestra el número de nodos que no pudieron cambiar sus claves. El sistema volverá a intentar automáticamente el proceso en cualquier nodo que no haya cambiado su clave. Si el proceso termina con algunos nodos que aún no tienen una clave cambiada, aparece el botón **Reintentar**.

Si la actualización de clave falló para uno o más nodos:

- a. Revise los mensajes de error que aparecen en la tabla.
- b. Resuelva los problemas.
- c. Seleccione **Reintentar**.

El reintento sólo cambia las claves de acceso SSH en los nodos que han fallado durante los intentos de cambio de clave anteriores.

5. Después de cambiar las claves de acceso SSH para todos los nodos, elimine el archivo [primer paquete de recuperación que descargaste](#).
6. Opcionalmente, seleccione **Mantenimiento > Sistema > Paquete de recuperación** para descargar una copia adicional del nuevo paquete de recuperación.

Usar la federación de identidades

El uso de la federación de identidades agiliza la configuración de grupos y usuarios y permite a los usuarios iniciar sesión en StorageGRID utilizando credenciales conocidas.

Configurar la federación de identidades para Grid Manager

Puede configurar la federación de identidad en Grid Manager si desea que los grupos de administradores y los usuarios se administren en otro sistema, como Active Directory, Microsoft Entra ID, OpenLDAP u Oracle Directory Server.

Antes de empezar

- Has iniciado sesión en Grid Manager usando un ["navegador web compatible"](#).
- Tú tienes ["permisos de acceso específicos"](#).
- Está utilizando Active Directory, Microsoft Entra ID, OpenLDAP u Oracle Directory Server como proveedor de identidad.



Si desea utilizar un servicio LDAP v3 que no figura en la lista, comuníquese con el soporte técnico.

- Si planea utilizar OpenLDAP, debe configurar el servidor OpenLDAP. Consulte [Instrucciones para configurar un servidor OpenLDAP](#).
- Si planea habilitar el inicio de sesión único (SSO), ha revisado la ["requisitos y consideraciones para el inicio de sesión único"](#).
- Si planea utilizar la seguridad de la capa de transporte (TLS) para las comunicaciones con el servidor LDAP, el proveedor de identidades usa TLS 1.2 o 1.3. Consulte ["Cifrados compatibles para conexiones TLS salientes"](#).

Acerca de esta tarea

Puede configurar una fuente de identidad para Grid Manager si desea importar grupos de otro sistema, como

Active Directory, Microsoft Entra ID, OpenLDAP u Oracle Directory Server. Puede importar los siguientes tipos de grupos:

- Grupos de administración. Los usuarios de los grupos de administración pueden iniciar sesión en Grid Manager y realizar tareas basándose en los permisos de administración asignados al grupo.
- Grupos de usuarios de inquilinos para inquilinos que no utilizan su propio origen de identidad. Los usuarios de grupos de inquilinos pueden iniciar sesión en el Administrador de inquilinos y realizar tareas, en función de los permisos asignados al grupo en el Administrador de inquilinos. Consulte ["Cree una cuenta de inquilino"](#) y ["Usar una cuenta de inquilino"](#) para obtener más información.

Introduzca la configuración

Pasos

1. Seleccione **Configuración > Control de acceso > Federación de identidades**.
2. Seleccione **Activar federación de identidades**.
3. En la sección Tipo de servicio LDAP, seleccione el tipo de servicio LDAP que desea configurar.

LDAP service type

Select the type of LDAP service you want to configure.

Active Directory	Entra ID	OpenLDAP	Other
------------------	----------	----------	-------

Seleccione **otros** para configurar valores para un servidor LDAP que utilice Oracle Directory Server.

4. Si ha seleccionado **otros**, complete los campos de la sección atributos LDAP . De lo contrario, vaya al paso siguiente.
 - **Nombre único de usuario:** el nombre del atributo que contiene el identificador único de un usuario LDAP. Este atributo es equivalente a `sAMAccountName` para Active Directory y `uid` para OpenLDAP. Si está configurando Oracle Directory Server, ingrese `uid` .
 - **UUID de usuario:** el nombre del atributo que contiene el identificador único permanente de un usuario LDAP. Este atributo es equivalente a `objectGUID` para Active Directory y `entryUUID` para OpenLDAP. Si está configurando Oracle Directory Server, ingrese `nsuniqueid` . El valor de cada usuario para el atributo especificado debe ser un número hexadecimal de 32 dígitos en formato de 16 bytes o de cadena, donde se ignoran los guiones.
 - **Nombre único del grupo:** el nombre del atributo que contiene el identificador único de un grupo LDAP. Este atributo es equivalente a `sAMAccountName` para Active Directory y `cn` para OpenLDAP. Si está configurando Oracle Directory Server, ingrese `cn` .
 - **UUID de grupo:** el nombre del atributo que contiene el identificador único permanente de un grupo LDAP. Este atributo es equivalente a `objectGUID` para Active Directory y `entryUUID` para OpenLDAP. Si está configurando Oracle Directory Server, ingrese `nsuniqueid` . El valor de cada grupo para el atributo especificado debe ser un número hexadecimal de 32 dígitos en formato de 16 bytes o de cadena, donde se ignoran los guiones.
5. Para todos los tipos de servicio LDAP, introduzca la información de servidor LDAP y conexión de red necesaria en la sección Configure LDAP Server.

- **Hostname:** El nombre de dominio completo (FQDN) o la dirección IP del servidor LDAP.
- **Puerto:** El puerto utilizado para conectarse al servidor LDAP.



El puerto predeterminado para STARTTLS es 389 y el puerto predeterminado para LDAPS es 636. Sin embargo, puede utilizar cualquier puerto siempre que su firewall esté configurado correctamente.

- **Nombre de usuario:** La ruta completa del nombre completo (DN) para el usuario que se conectará al servidor LDAP.

Para Active Directory, también puede especificar el nombre de inicio de sesión de nivel inferior o el nombre principal del usuario.

El usuario especificado debe tener permiso para enumerar grupos y usuarios y para tener acceso a los siguientes atributos:

- `sAMAccountName` O. `uid`
- `objectGUID`, `entryUUID` O. `nsuniqueid`
- `cn`
- `memberOf` O. `isMemberOf`
- **Active Directory** `objectSid`, `primaryGroupID`, `userAccountControl` Y. `userPrincipalName`
- **ID de entrada:** `accountEnabled` y `userPrincipalName`

- **Contraseña:** La contraseña asociada al nombre de usuario.



Si cambia la contraseña en el futuro, debe actualizarla en esta página.

- **DN base de grupo:** La ruta completa del nombre distinguido (DN) para un subárbol LDAP que desea buscar grupos. En el ejemplo de Active Directory (a continuación), se pueden usar como grupos federados todos los grupos cuyo nombre distintivo sea relativo al DN base (`DC=storagegrid,DC=example,DC=com`).



Los valores de **Nombre único de grupo** deben ser únicos dentro del **DN base de grupo** al que pertenecen.

- **DN base de usuario:** La ruta completa del nombre completo (DN) de un subárbol LDAP que desea buscar usuarios.



Los valores de **Nombre único de usuario** deben ser únicos dentro del **DN base de usuario** al que pertenecen.

- **Formato de nombre de usuario de enlace** (opcional): El patrón de nombre de usuario predeterminado `StorageGRID` debe usarse si el patrón no se puede determinar automáticamente.

Se recomienda proporcionar **Formato de nombre de usuario Bind** porque puede permitir que los usuarios inicien sesión si `StorageGRID` no puede enlazar con la cuenta de servicio.

Introduzca uno de estos patrones:

- **Patrón UserPrincipalName (ID de AD y Entra):** [USERNAME]@example.com
- **Patrón de nombre de inicio de sesión de nivel inferior (ID de AD y Entra):**
example\[USERNAME]
- *** Patrón de nombre distinguido *:** CN=[USERNAME],CN=Users,DC=example,DC=com

Incluya **[USERNAME]** exactamente como está escrito.

6. En la sección Seguridad de la capa de transporte (TLS), seleccione una configuración de seguridad.

- **Usar STARTTLS:** utilice STARTTLS para proteger las comunicaciones con el servidor LDAP. Esta es la opción recomendada para Active Directory, OpenLDAP u otros, pero esta opción no es compatible con Microsoft Entra ID.
- **Usar LDAPS:** La opción LDAPS (LDAP sobre SSL) utiliza TLS para establecer una conexión con el servidor LDAP. Debe seleccionar esta opción para Microsoft Entra ID.
- **No utilizar TLS:** El tráfico de red entre el sistema StorageGRID y el servidor LDAP no estará protegido. Esta opción no es compatible con Microsoft Entra ID.



No se admite el uso de la opción **No usar TLS** si su servidor de Active Directory aplica la firma LDAP. Debe utilizar STARTTLS o LDAPS.

7. Si seleccionó STARTTLS o LDAPS, elija el certificado utilizado para proteger la conexión.

- **Utilizar certificado CA del sistema operativo:** Utilice el certificado predeterminado de CA de red instalado en el sistema operativo para asegurar las conexiones.
- **Utilizar certificado de CA personalizado:** Utilice un certificado de seguridad personalizado.

Si selecciona esta opción, copie y pegue el certificado de seguridad personalizado en el cuadro de texto del certificado de CA.

Pruebe la conexión y guarde la configuración

Después de introducir todos los valores, es necesario probar la conexión para poder guardar la configuración. StorageGRID verifica la configuración de conexión del servidor LDAP y el formato de nombre de usuario de enlace, si proporcionó uno.

Pasos

1. Seleccione **probar conexión**.
2. Si no proporcionó un formato de nombre de usuario vinculado:
 - Si la configuración de conexión es válida, aparecerá un mensaje que indica que la conexión se ha realizado correctamente. Seleccione **Guardar** para guardar la configuración.
 - Si la configuración de conexión no es válida, aparecerá un mensaje que indica que no se ha podido establecer la conexión de prueba. Seleccione **Cerrar**. Luego, resuelva cualquier problema y vuelva a probar la conexión.
3. Si proporcionó un formato de nombre de usuario de enlace, introduzca el nombre de usuario y la contraseña de un usuario federado válido.

Por ejemplo, introduzca su propio nombre de usuario y contraseña. No incluya ningún carácter especial en el nombre de usuario, como @ o /.

Test Connection

To test the connection and the bind username format, enter the username and password of a federated user. For example, enter your own federated username and password. The test values are not saved.

Test username

The username of a federated user.

Test password

Cancel

Test Connection

- Si la configuración de conexión es válida, aparecerá un mensaje que indica que la conexión se ha realizado correctamente. Seleccione **Guardar** para guardar la configuración.
- Aparecerá un mensaje de error si las opciones de conexión, el formato de nombre de usuario de enlace o el nombre de usuario y la contraseña de prueba no son válidos. Resuelva los problemas y vuelva a probar la conexión.

Forzar la sincronización con el origen de identidades

El sistema StorageGRID sincroniza periódicamente grupos federados y usuarios del origen de identidades. Puede forzar el inicio de la sincronización si desea habilitar o restringir los permisos de usuario lo antes posible.

Pasos

1. Vaya a la página federación de identidades.
2. Seleccione **servidor de sincronización** en la parte superior de la página.

El proceso de sincronización puede tardar bastante tiempo en función del entorno.



La alerta **fallo de sincronización de la federación de identidades** se activa si hay un problema al sincronizar grupos federados y usuarios del origen de identidades.

Deshabilitar la federación de identidades

Puede deshabilitar temporal o permanentemente la federación de identidad para grupos y usuarios. Cuando la federación de identidad está deshabilitada, no hay comunicación entre StorageGRID y la fuente de identidad. Sin embargo, cualquier configuración que haya realizado se conservará, lo que le permitirá volver a habilitar fácilmente la federación de identidad en el futuro.

Acerca de esta tarea

Antes de deshabilitar la federación de identidades, debe tener en cuenta lo siguiente:

- Los usuarios federados no podrán iniciar sesión.
- Los usuarios federados que hayan iniciado sesión en ese momento, retendrán el acceso al sistema StorageGRID hasta que caduque la sesión, pero no podrán iniciar sesión después de que caduque la

sesión.

- No se producirá sincronización entre el sistema StorageGRID y la fuente de identidad, y no se generarán alertas para las cuentas que no se hayan sincronizado.
- La casilla de verificación **Habilitar federación de identidad** está deshabilitada si el estado de inicio de sesión único (SSO) es **Habilitado** o **Modo Sandbox**. El estado de SSO en la página de inicio de sesión único debe ser **Deshabilitado** antes de poder deshabilitar la federación de identidad. Ver "[Desactive el inicio de sesión único](#)".

Pasos

1. Vaya a la página federación de identidades.
2. Desmarque la casilla de verificación **Habilitar federación de identidad**.

Instrucciones para configurar un servidor OpenLDAP

Si desea utilizar un servidor OpenLDAP para la federación de identidades, debe configurar ajustes específicos en el servidor OpenLDAP.



Para las fuentes de identidad que no sean Active Directory o Microsoft Entra ID, StorageGRID no bloqueará automáticamente el acceso a S3 a los usuarios que estén deshabilitados externamente. Para bloquear el acceso a S3, elimine todas las claves S3 del usuario o elimine el usuario de todos los grupos.

Revestimientos memberOf y ref

Se deben habilitar las superposiciones memberof y ref. Para obtener más información, consulte las instrucciones para invertir el mantenimiento de los miembros del grupo en la "[Documentación de OpenLDAP: Guía del administrador de la versión 2.4](#)"sección .

Indización

Debe configurar los siguientes atributos OpenLDAP con las palabras clave de índice especificadas:

- `olcDbIndex: objectClass eq`
- `olcDbIndex: uid eq,pres,sub`
- `olcDbIndex: cn eq,pres,sub`
- `olcDbIndex: entryUUID eq`

Además, asegúrese de que los campos mencionados en la ayuda para Nombre de usuario estén indexados para un rendimiento óptimo.

Consulte la información sobre el mantenimiento inverso de miembros de grupo en la "[Documentación de OpenLDAP: Guía del administrador de la versión 2.4](#)".

Gestione los grupos de administradores

Es posible crear grupos de administración para gestionar los permisos de seguridad de uno o más usuarios de administrador. Los usuarios deben pertenecer a un grupo para tener acceso al sistema StorageGRID.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante una "[navegador web compatible](#)".
- Tienes "[permisos de acceso específicos](#)".
- Si planea importar un grupo federado, ha configurado la federación de identidades y el grupo federado ya existe en el origen de identidades configurado.

Cree un grupo de administración

Los grupos de administración permiten determinar a qué usuarios se puede acceder a qué características y operaciones en Grid Manager y en la API de gestión de grid.

Acceda al asistente

Pasos

1. Seleccione **Configuración > Control de acceso > Grupos de administradores**.
2. Seleccione **Crear grupo**.

Elija un tipo de grupo

Puede crear un grupo local o importar un grupo federado.

- Cree un grupo local si desea asignar permisos a los usuarios locales.
- Cree un grupo federado para importar usuarios desde el origen de identidades.

Grupo local

Pasos

1. Seleccione **Grupo local**.
2. Introduzca un nombre para mostrar para el grupo, que puede actualizar más adelante si es necesario. Por ejemplo, «Usuarios de mantenimiento» o «Administradores de ILM».
3. Introduzca un nombre único para el grupo, que no podrá actualizar más tarde.
4. Seleccione **continuar**.

Grupo federado

Pasos

1. Seleccione **Grupo federado**.
2. Introduzca el nombre del grupo que desea importar, exactamente como aparece en el origen de identidad configurado.
 - Para Active Directory y Microsoft Entra ID, utilice sAMAccountName.
 - Para OpenLDAP, utilice CN (Nombre común).
 - Para otro LDAP, utilice el nombre exclusivo adecuado para el servidor LDAP.
3. Seleccione **continuar**.

Administrar permisos de grupo

Pasos

1. En **modo de acceso**, seleccione si los usuarios del grupo pueden cambiar la configuración y realizar operaciones en Grid Manager y la API de gestión de grid o si sólo pueden ver la configuración y las características.
 - **Read-write** (predeterminado): Los usuarios pueden cambiar la configuración y realizar las operaciones permitidas por sus permisos de administración.
 - **Sólo lectura**: Los usuarios sólo pueden ver los ajustes y las funciones. No pueden realizar cambios ni realizar ninguna operación en Grid Manager o la API de administración de grid. Los usuarios locales de solo lectura pueden cambiar sus propias contraseñas.



Si un usuario pertenece a varios grupos y cualquier grupo está establecido en **sólo lectura**, el usuario tendrá acceso de sólo lectura a todos los ajustes y características seleccionados.

2. Seleccione una o más "[permisos de grupo de administración](#)".

Debe asignar al menos un permiso a cada grupo; de lo contrario, los usuarios que pertenezcan al grupo no podrán iniciar sesión en StorageGRID.

3. Si está creando un grupo local, seleccione **continuar**. Si está creando un grupo federado, seleccione **Crear grupo y Finalizar**.

Añadir usuarios (sólo grupos locales)

Pasos

1. Opcionalmente, seleccione uno o varios usuarios locales para este grupo.

Si todavía no ha creado usuarios locales, puede guardar el grupo sin agregar usuarios. Puede agregar este grupo al usuario en la página usuarios. Consulte "[Gestionar usuarios](#)" para obtener más información.


2. Seleccione **Crear grupo y Finalizar**.

Consulte y edite los grupos de administración

Puede ver los detalles de los grupos existentes, modificar un grupo o duplicar un grupo.

- Para ver información básica de todos los grupos, revise la tabla de la página grupos.
- Para ver todos los detalles de un grupo específico o editar un grupo, utilice el menú **acciones** o la página de detalles.

Tarea	Menú Actions	Detalles
Ver detalles del grupo	a. Seleccione la casilla de verificación para el grupo. b. Seleccione acciones > Ver detalles del grupo .	Seleccione el nombre del grupo en la tabla.

Tarea	Menú Actions	Detalles
Editar nombre para mostrar (sólo grupos locales)	a. Seleccione la casilla de verificación para el grupo. b. Seleccione acciones > Editar nombre de grupo . c. Introduzca el nuevo nombre. d. Seleccione Guardar cambios .	a. Seleccione el nombre del grupo para mostrar los detalles. b. Seleccione el icono de edición  . c. Introduzca el nuevo nombre. d. Seleccione Guardar cambios .
Edite el modo de acceso o los permisos	a. Seleccione la casilla de verificación para el grupo. b. Seleccione acciones > Ver detalles del grupo . c. Si lo desea, cambie el modo de acceso del grupo. d. Si lo desea, seleccione o desactive "permisos de grupo de administración" . e. Seleccione Guardar cambios .	a. Seleccione el nombre del grupo para mostrar los detalles. b. Si lo desea, cambie el modo de acceso del grupo. c. Si lo desea, seleccione o desactive "permisos de grupo de administración" . d. Seleccione Guardar cambios .

Duplicar un grupo

Pasos

1. Seleccione la casilla de verificación para el grupo.
2. Seleccione **acciones > Duplicar grupo**.
3. Complete el asistente para grupos duplicados.

Eliminar un grupo

Es posible eliminar un grupo de administración cuando se desea quitar el grupo del sistema y quitar todos los permisos asociados con el grupo. Al eliminar un grupo de administración, se quitan todos los usuarios del grupo, pero no se eliminan los usuarios.

Pasos

1. En la página Groups, seleccione la casilla de comprobación de cada grupo que desea quitar.
2. Seleccione **acciones > Eliminar grupo**.
3. Seleccione **Eliminar grupos**.

Permisos de grupo de administradores

Al crear grupos de usuarios de administrador, debe seleccionar uno o más permisos para controlar el acceso a funciones específicas de Grid Manager. A continuación, puede asignar cada usuario a uno o varios de estos grupos de administración para determinar qué tareas puede realizar el usuario.

Debe asignar al menos un permiso a cada grupo; de lo contrario, los usuarios pertenecientes a ese grupo no podrán iniciar sesión en Grid Manager o en la API de gestión de grid.

De forma predeterminada, cualquier usuario que pertenezca a un grupo que tenga al menos un permiso puede realizar las siguientes tareas:

- Inicie sesión en Grid Manager
- Vea la consola
- Puede ver las páginas Nodes
- Ver las alertas actuales y resueltas
- Cambiar su propia contraseña (sólo usuarios locales)
- Ver cierta información proporcionada en las páginas de configuración y mantenimiento

Interacción entre permisos y modo de acceso

Para todos los permisos, la configuración del **modo de acceso** del grupo determina si los usuarios pueden cambiar la configuración y realizar operaciones o si sólo pueden ver la configuración y las características relacionadas. Si un usuario pertenece a varios grupos y cualquier grupo está establecido en **sólo lectura**, el usuario tendrá acceso de sólo lectura a todos los ajustes y características seleccionados.

En las siguientes secciones se describen los permisos que se pueden asignar al crear o editar un grupo de administradores. Cualquier funcionalidad que no se haya mencionado explícitamente requiere el permiso **acceso raíz**.

Acceso raíz

Este permiso proporciona acceso a todas las funciones de administración de grid.

Cambiar la contraseña raíz del inquilino

Este permiso proporciona acceso a la opción **Cambiar contraseña raíz** de la página arrendatarios, lo que le permite controlar quién puede cambiar la contraseña del usuario raíz local del arrendatario. Este permiso también se usa para migrar claves S3 cuando se habilita la función de importación de claves S3. Los usuarios que no tienen este permiso no pueden ver la opción **Cambiar contraseña raíz**.



Para conceder acceso a la página arrendatarios, que contiene la opción **Cambiar contraseña root**, también asigne el permiso **Cuentas de arrendatario**.

ILM

Este permiso permite acceder a las siguientes opciones del menú **ILM**:

- Bases de datos
- Normativas
- Etiquetas de políticas
- Pools de almacenamiento
- Grados de almacenamiento
- Regiones

- Búsqueda de metadatos de objetos



Los usuarios deben tener el permiso **Otra configuración de red** para administrar los niveles de almacenamiento.

Mantenimiento

Los usuarios deben tener permiso de mantenimiento para utilizar estas opciones:

- **Configuración > Control de acceso:**
 - Contraseñas de grid
- **Configuración > Red:**
 - Nombres de dominio de punto final S3
- **Mantenimiento > Tareas:**
 - Retirada
 - Expansión
 - Comprobación de existencia de objeto
 - Recuperación
- **Mantenimiento > Sistema:**
 - Paquete de recuperación
 - Actualización de software
- **Soporte > Herramientas:**
 - Registros

Los usuarios que no tienen el permiso de mantenimiento pueden ver, pero no editar, estas páginas:

- **Mantenimiento > Red:**
 - Servidores DNS
 - Red Grid
 - Servidores NTP
- **Mantenimiento > Sistema:**
 - Licencia
- **Configuración > Red:**
 - Nombres de dominio de punto final S3
- **Configuración > Seguridad:**
 - Certificados
- **Configuración > Monitoreo:**
 - Servidor de auditoría y syslog

Gestionar alertas

Este permiso proporciona acceso a opciones para gestionar alertas. Los usuarios deben tener este permiso

para gestionar los silencios, las notificaciones de alerta y las reglas de alerta.

Consulta de métricas

Este permiso proporciona acceso a:

- Página **Soporte > Herramientas > Métricas**
- Consultas personalizadas de métricas de Prometheus utilizando la sección **Metrics** de la API de administración de grid
- Tarjetas del panel de control de Grid Manager que contienen métricas

Búsqueda de metadatos de objetos

Este permiso proporciona acceso a la página **ILM > Búsqueda de metadatos de objetos**.

Otra configuración de cuadrícula

Este permiso proporciona acceso a estas opciones de configuración de cuadrícula adicionales:

- **ILM:**
 - Grados de almacenamiento
- **Configuración > Sistema:**
- **Soporte > Otros:**
 - Coste del enlace

Administrador de dispositivos de almacenamiento

Este permiso proporciona:

- Acceso al SANtricity System Manager de E-Series en dispositivos de almacenamiento a través de Grid Manager.
- La capacidad de realizar tareas de solución de problemas y mantenimiento en la pestaña Gestionar unidades para los dispositivos que admiten estas operaciones.

Cuentas de inquilino

Este permiso permite:

- Acceda a la página Tenedores, donde puede crear, editar y eliminar cuentas de arrendatario
- Ver las políticas de clasificación de tráfico existentes
- Ver tarjetas de consola de Grid Manager que contienen detalles de arrendatario

Gestionar usuarios

Es posible ver usuarios locales y federados. También puede crear usuarios locales y asignarles grupos de administración locales para determinar a qué funciones de Grid Manager pueden acceder estos usuarios.

Antes de empezar

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

Cree un usuario local

Es posible crear uno o varios usuarios locales y asignar cada usuario a uno o varios grupos locales. Los permisos del grupo controlan a qué funciones de Grid Manager y la API de gestión de grid puede acceder el usuario.

Solo es posible crear usuarios locales. Utilice el origen de identidades externo para administrar grupos y usuarios federados.

Grid Manager incluye un usuario local predefinido, denominado «root». No puede eliminar el usuario root.



Si el inicio de sesión único (SSO) está activado, los usuarios locales no pueden iniciar sesión en StorageGRID.

Acceda al asistente

Pasos

1. Seleccione **Configuración > Control de acceso > Usuarios administradores**.
2. Seleccione **Crear usuario**.

Introduzca las credenciales de usuario

Pasos

1. Introduzca el nombre completo del usuario, un nombre de usuario único y una contraseña.
2. Opcionalmente, seleccione **Sí** si este usuario no debe tener acceso a Grid Manager o a la API de gestión de grid.
3. Seleccione **continuar**.

Asignar a grupos

Pasos

1. Opcionalmente, asigne el usuario a uno o más grupos para determinar los permisos del usuario.

Si aún no ha creado grupos, puede guardar el usuario sin seleccionar grupos. Puede agregar este usuario a un grupo en la página grupos.

Si un usuario pertenece a varios grupos, los permisos son acumulativos. Consulte ["Gestione los grupos de administradores"](#) para obtener más información.

2. Seleccione **Crear usuario** y seleccione **Finalizar**.

Ver y editar usuarios locales

Es posible ver detalles de los usuarios locales y federados existentes. Es posible modificar un usuario local para cambiar el nombre completo, la contraseña o la pertenencia a grupos del usuario. También puede impedir temporalmente que un usuario acceda a Grid Manager y a la API de gestión de grid.


Solo puede editar usuarios locales. Utilice el origen de identidad externo para administrar usuarios federados.

- Para ver la información básica de todos los usuarios locales y federados, revise la tabla en la página Users.
- Para ver todos los detalles de un usuario específico, editar un usuario local o cambiar la contraseña de un usuario local, utilice el menú **acciones** o la página de detalles.

Las modificaciones se aplican la próxima vez que el usuario cierre sesión y vuelva a acceder al Gestor de cuadrícula.



Los usuarios locales pueden cambiar sus propias contraseñas usando la opción **Cambiar contraseña** en el banner de Grid Manager.

Tarea	Menú Actions	Detalles
Ver los detalles del usuario	a. Seleccione la casilla de control para el usuario. b. Seleccione acciones > Ver detalles del usuario .	Seleccione el nombre del usuario en la tabla.
Editar nombre completo (sólo usuarios locales)	a. Seleccione la casilla de control para el usuario. b. Seleccione acciones > Editar nombre completo . c. Introduzca el nuevo nombre. d. Seleccione Guardar cambios .	a. Seleccione el nombre del usuario para mostrar los detalles. b. Seleccione el icono de edición  . c. Introduzca el nuevo nombre. d. Seleccione Guardar cambios .
Denegar o permitir el acceso a StorageGRID	a. Seleccione la casilla de control para el usuario. b. Seleccione acciones > Ver detalles del usuario . c. Seleccione la pestaña Access. d. Seleccione Sí para evitar que el usuario inicie sesión en Grid Manager o en la API de gestión de grid, o seleccione no para permitir que el usuario inicie sesión. e. Seleccione Guardar cambios .	a. Seleccione el nombre del usuario para mostrar los detalles. b. Seleccione la pestaña Access. c. Seleccione Sí para evitar que el usuario inicie sesión en Grid Manager o en la API de gestión de grid, o seleccione no para permitir que el usuario inicie sesión. d. Seleccione Guardar cambios .
Cambiar contraseña (solo usuarios locales)	a. Seleccione la casilla de control para el usuario. b. Seleccione acciones > Ver detalles del usuario . c. Seleccione la ficha Contraseña. d. Introduzca una contraseña nueva. e. Seleccione Cambiar contraseña .	a. Seleccione el nombre del usuario para mostrar los detalles. b. Seleccione la ficha Contraseña. c. Introduzca una contraseña nueva. d. Seleccione Cambiar contraseña .

Tarea	Menú Actions	Detalles
Cambiar grupos (sólo usuarios locales)	a. Seleccione la casilla de control para el usuario. b. Seleccione acciones > Ver detalles del usuario . c. Seleccione la ficha grupos. d. Opcionalmente, seleccione el vínculo después del nombre de un grupo para ver los detalles del grupo en una nueva pestaña del explorador. e. Seleccione Editar grupos para seleccionar diferentes grupos. f. Seleccione Guardar cambios .	a. Seleccione el nombre del usuario para mostrar los detalles. b. Seleccione la ficha grupos. c. Opcionalmente, seleccione el vínculo después del nombre de un grupo para ver los detalles del grupo en una nueva pestaña del explorador. d. Seleccione Editar grupos para seleccionar diferentes grupos. e. Seleccione Guardar cambios .

Importar usuarios federados

Puede importar uno o más usuarios federados, hasta un máximo de 100 usuarios, directamente a la página Usuarios.

Pasos

1. Seleccione **Configuración > Control de acceso > Usuarios administradores**.
2. Seleccione **Importar usuarios federados**.
3. Introduzca el UUID o nombre de usuario de uno o más usuarios federados.

Para entradas múltiples, agregue cada UUID o nombre de usuario en una nueva línea.

4. Seleccione **Importar**.

Si la importación al campo Usuarios falla para uno o más usuarios, realice los siguientes pasos:

- a. Expande **Usuarios no importados** y selecciona **Copiar usuarios**.
- b. Vuelva a intentar la importación seleccionando **Anterior** y pegando los usuarios copiados en el cuadro de diálogo **Importar usuarios federados**.

Después de cerrar el cuadro de diálogo **Importar usuarios federados**, la información del usuario federado se muestra en la página Usuarios para los usuarios importados correctamente.

Duplique un usuario

Puede duplicar un usuario existente para crear un nuevo usuario con los mismos permisos.

Pasos

1. Seleccione la casilla de control para el usuario.
2. Seleccione **acciones > Duplicar usuario**.
3. Complete el asistente Duplicar usuario.

Eliminar un usuario

Puede eliminar un usuario local para eliminar de forma permanente ese usuario del sistema.



No puede eliminar el usuario root.

Pasos

1. En la página Usuarios, seleccione la casilla de verificación de cada usuario que desee eliminar.
2. Seleccione **acciones** > **Eliminar usuario**.
3. Seleccione **Eliminar usuario**.

Utilizar inicio de sesión único (SSO)

Cómo funciona el SSO

Cuando el inicio de sesión único (SSO) está habilitado, los usuarios pueden acceder a Grid Manager, Tenant Manager, Grid Management API o Tenant Management API solo 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.

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).

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.

Inicie sesión cuando SSO esté 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 solicitará un ID de cuenta.
- 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.



La página de inicio de sesión de StorageGRID no se muestra cuando se introduce la dirección 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 redirigirá inmediatamente a la página de inicio de sesión de SSO de su organización, donde puede [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 el campo **ID de cuenta** en blanco, introduzca **0** como ID de cuenta o seleccione **Gestor de cuadrícula** 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. Seleccione **Iniciar sesión**

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

4. inicia sesión con sus credenciales de SSO.

Si sus credenciales de SSO son correctas:

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



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

5. 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 las credenciales de SSO.

Cierre sesión cuando SSO esté 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

- Localice el enlace **Sign Out** en la esquina superior derecha de la interfaz de usuario.
- Selecciona **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.



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.

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 Nota: Si usa Entra ID para SSO, puede que tome algunos minutos cerrar sesión 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.

Requisitos y consideraciones para SSO

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

Requisitos del proveedor de identidades

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

- Servicio de Federación de Active Directory (AD FS)
- Identificador de Microsoft Entra
- PingFederate

Debe configurar la federación de identidades para el sistema StorageGRID antes de poder configurar un proveedor de identidades SSO. El tipo de servicio LDAP que utiliza para controlar la federación de identidades qué tipo de SSO puede implementar.

Se ha configurado el tipo de servicio LDAP	Opciones para el proveedor de identidades SSO
Active Directory	<ul style="list-style-type: none"> • Active Directory • Identificación de entrada • PingFederate
Identificación de entrada	Identificación de entrada

Requisitos DE AD FS

Puede utilizar cualquiera de las siguientes versiones de AD FS:

- Windows Server 2022 AD FS
- Windows Server 2019 AD FS
- Windows Server 2016 AD FS



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

Requisitos adicionales

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

Consideraciones para Entra ID

Si utiliza Entra ID como tipo de SSO y los usuarios tienen nombres principales de usuario que no utilizan 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 de 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 (Entra ID) 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 ha hecho "[se configuró un certificado personalizado para la interfaz de gestión](#)", debería hacerlo ahora. Cuando instala un certificado de servidor personalizado, se utiliza para todos los nodos de administrador y puede usarlo en todas las confianzas de parte que dependen de StorageGRID, aplicaciones de empresa o conexiones del SP.



No se recomienda utilizar el certificado de servidor predeterminado de un nodo de administración en la confianza de una parte que confía, la aplicación de empresa o la conexión de SP. 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, la aplicación de empresa o la conexión del SP con el nuevo certificado.

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

Requisitos de puertos

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. Consulte "[Controle el acceso a un firewall externo](#)".

Confirmar 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.

Antes de empezar

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

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 **Administración de acceso > Federación de identidades**.
 - c. Confirme que la casilla de verificación **Habilitar federación de identidad** no está seleccionada.
 - d. Si lo es, confirme que los grupos federados que puedan estar en uso para esta cuenta de inquilino ya no son necesarios, desactive la casilla de verificación y seleccione **Guardar**.
2. Confirme que un usuario federado puede acceder a Grid Manager:
 - a. Desde 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. Desde el Administrador de red, seleccione **Inquilinos**.
 - b. Seleccione la cuenta de arrendatario y seleccione **acciones > Editar**.
 - c. En la ficha introducir 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 inquilino.

 - e. Seleccione la cuenta de arrendatario, seleccione **Iniciar sesión** e inicie sesión en la cuenta de arrendatario como usuario raíz local.
 - f. Desde el Administrador de inquilinos, seleccione **Administración de acceso > Grupos**.
 - g. Asegúrese de que al menos un grupo federado de Grid Manager ha sido asignado el permiso de

acceso raíz para este arrendatario.

h. Cierre la sesión.

i. 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"](#)
- ["Gestione los grupos de administradores"](#)
- ["Usar una cuenta de inquilino"](#)

Configurar SSO

Puede seguir el asistente de configuración de SSO e ingresar al 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 cuando sea necesario para cambiar o volver a probar la configuración.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante una ["navegador web compatible"](#).
- Usted tiene el ["Permiso de acceso raíz"](#).
- Configuró la federación de identidades para el sistema StorageGRID.
- Para la federación de identidad **tipo de servicio LDAP**, seleccionó Active Directory o Entra ID, según el proveedor de identidad SSO que planea utilizar.

Se ha configurado el tipo de servicio LDAP	Opciones para el proveedor de identidades SSO
Servicio de Federación de Active Directory (AD FS)	<ul style="list-style-type: none">• Active Directory• Identificación de entrada• PingFederate
Identificación de entrada	Identificación de entrada

Acerca de esta tarea

Cuando se habilita el inicio de sesión único y un usuario intenta iniciar sesión en un nodo de administración, StorageGRID envía una solicitud de autenticación al proveedor de identidades de SSO. A su vez, el proveedor de identidades SSO envía una respuesta de autenticación a StorageGRID para indicar si la solicitud de autenticación se ha realizado correctamente. Para solicitudes correctas:

- La respuesta de Active Directory o PingFederate incluye un identificador único universal (UUID) para el usuario.
- La respuesta de Entra ID 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, deberá completar estas tareas:

1. Configurar ajustes en StorageGRID.
2. Utilice el software del proveedor de identidad SSO para crear una relación de confianza entre usuarios

(AD FS), una aplicación empresarial (Entra ID) o un proveedor de servicios (PingFederate) para cada nodo de administración.

3. Regrese 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.

Acceda al asistente

Pasos

1. Seleccione **Configuración > Control de acceso > Inicio de sesión único**. Aparece la página de inicio de sesión único.



Si el botón Configurar ajustes de SSO está deshabilitado, confirme que haya configurado el proveedor de identidad como fuente de identidad federada. Consulte ["Requisitos y consideraciones para el inicio de sesión único"](#).

2. Seleccione **Configurar ajustes de SSO**. Aparece la página Proporcionar detalles del proveedor de identidad.

Proporcionar detalles del proveedor de identidad

Pasos

1. Seleccione **Tipo SSO** en la lista desplegable.
2. Si seleccionó Active Directory como tipo de SSO, 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 buscar el nombre del servicio de federación, vaya al Administrador de Windows Server. 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.

3. Especifique qué certificado TLS se utilizará para proteger la conexión cuando el proveedor de identidades envíe información de configuración de SSO en respuesta a las 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 esta configuración, copie el texto del certificado personalizado y péguelo en el cuadro de texto **Certificado CA**.

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



Si cambia el certificado de CA, inmediatamente ["Reinicie el servicio mgmt-api en los nodos de administración"](#) y prueba un SSO correcto en Grid Manager.

4. Seleccione **Continuar**. Aparece la página Proporcionar identificador de parte confiable.

Proporcionar identificador de parte confiable

1. Complete los campos en la página Proporcionar identificador de parte confiable según el tipo de SSO que haya seleccionado.

Active Directory

- a. Especifique el **Identificador de la 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 el grid solo tiene un nodo de administración y no prevé agregar más nodos de administración en el futuro, introduzca `SG` o `StorageGRID`.
 - Si su cuadrícula incluye más de un nodo de administración, incluya la cadena `[HOSTNAME]` en el identificador. Por ejemplo, `SG-[HOSTNAME]`. Al incluir esta cadena, se genera una tabla que muestra el identificador de la parte confiada para cada nodo de administración en la cuadrícula, según el nombre de host del nodo.



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.

- b. Seleccione **Guardar e ingresar al modo sandbox**.

Identificación de entrada

- a. 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 Entra ID.
 - Por ejemplo, si el grid solo tiene un nodo de administración y no prevé agregar más nodos de administración en el futuro, introduzca `SG` o `StorageGRID`.
 - Si su cuadrícula incluye más de un nodo de administración, incluya la cadena `[HOSTNAME]` en el identificador. Por ejemplo, `SG-[HOSTNAME]`. Al incluir esta cadena, se 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 administrador en el sistema StorageGRID. Disponer de una aplicación empresarial para cada nodo de administración garantiza que los usuarios puedan iniciar sesión de forma segura en cualquier nodo de administración.

- b. Siga los pasos en "[Crear aplicaciones empresariales en Entra ID](#)" para crear una aplicación empresarial para cada nodo de administración enumerado en la tabla.
- c. Desde Entra ID, 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.
- d. Después de haber copiado y pegado una URL de metadatos de federación para todos los nodos de administración, seleccione **Guardar e ingresar al modo sandbox**.

PingFederate

- a. En la sección Proveedor de servicios (SP), especifique **ID de conexión SP** para StorageGRID. Este valor controla el nombre que utiliza para cada conexión SP en PingFederate.
 - Por ejemplo, si el grid solo tiene un nodo de administración y no prevé agregar más nodos de administración en el futuro, introduzca `SG` o `StorageGRID`.
 - Si su cuadrícula incluye más de un nodo de administración, incluya la cadena `[HOSTNAME]`

en el identificador. Por ejemplo, SG-[HOSTNAME] . Al incluir esta cadena, se 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 de SP para cada nodo de administrador en el sistema StorageGRID. Tener una conexión de SP para cada nodo de administrador garantiza que los usuarios puedan iniciar sesión de forma segura en cualquier nodo de administrador.

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

Utilice el siguiente formato:

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

- c. Seleccione **Guardar e ingresar al modo sandbox**.

Configurar las confianzas de partes de confianza, las aplicaciones de la empresa o las conexiones de SP

Después de guardar la configuración e ingresar al modo sandbox, puede completar y probar la configuración para el tipo de SSO que seleccionó.

StorageGRID puede permanecer en modo sandbox tanto tiempo como sea necesario. Sin embargo, sólo los usuarios federados y los usuarios locales pueden iniciar sesión.

Active Directory

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 Configurar SSO.

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

Para obtener instrucciones, vaya a ["Crear confianzas de parte de confianza en AD FS"](#).

Identificación de entrada

Pasos

1. En la página Single Sign-On del nodo de administrador al que ha iniciado sesión actualmente, seleccione el botón para descargar y guardar los metadatos SAML.
2. A continuación, para cualquier otro nodo de administrador en el grid, repita estos pasos:
 - a. Inicie sesión en el nodo.
 - b. Seleccione **Configuración > Control de acceso > Inicio de sesión único**.
 - c. Descargue y guarde los metadatos de SAML de ese nodo.
3. Vaya al portal de Azure.
4. Siga los pasos en ["Crear aplicaciones empresariales en Entra ID"](#) para cargar el archivo de metadatos SAML para cada nodo de administración en su aplicación empresarial Entra ID correspondiente.

PingFederate

Pasos

1. En la página Single Sign-On del nodo de administrador al que ha iniciado sesión actualmente, seleccione el botón para descargar y guardar los metadatos SAML.
2. A continuación, para cualquier otro nodo de administrador en el grid, repita estos pasos:
 - a. Inicie sesión en el nodo.
 - b. Seleccione **Configuración > Control de acceso > Inicio de sesión único**.
 - c. Descargue y guarde los metadatos de SAML de ese nodo.
3. Vaya a PingFederate.
4. ["Cree una o varias 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 Configurar SSO) y los metadatos SAML que descargó para ese nodo de administración.

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

Configuración de prueba

Antes de implementar el uso del inicio de sesión único para todo el sistema StorageGRID , confirme que el inicio de sesión único y el cierre de sesión único estén configurados correctamente para cada nodo de administración.

Active Directory

Pasos

1. Desde la página Configurar SSO, busque el enlace en el paso de configuración de prueba del asistente.

La dirección URL se deriva del valor introducido en el campo **Nombre de servicio de Federación**.

2. Seleccione el enlace, o copie y pegue la URL en un navegador para acceder a la página de inicio de sesión del proveedor de identidades.
3. 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 seleccione **Iniciar sesión**.
4. 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.
 - 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.
5. Repita estos pasos para verificar la conexión SSO para cada nodo de administrador en el grid.

Identificación de entrada

Pasos

1. Vaya a la página Single Sign-On del portal de Azure.
2. Seleccione **probar esta aplicación**.
3. Introduzca las credenciales de un usuario federado.
 - Si las operaciones de inicio de sesión y cierre de sesión SSO se realizan correctamente, se muestra un mensaje de éxito.
 - 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.
4. Repita estos pasos para verificar la conexión SSO para cada nodo de administrador en el grid.

PingFederate

Pasos

1. Desde la página Configurar SSO, seleccione el primer enlace en el mensaje del modo Sandbox.

Seleccione y pruebe un enlace cada vez.

2. Introduzca las credenciales de un usuario federado.
 - Si las operaciones de inicio de sesión y cierre de sesión SSO se realizan correctamente, se muestra un mensaje de éxito.
 - 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.
3. Seleccione el siguiente enlace para verificar la conexión de SSO para cada nodo de administrador de la cuadrícula.

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

Active el inicio de sesión único

Una vez que haya confirmado que puede usar SSO para iniciar sesión en cada nodo de administración, puede habilitar SSO en todo el sistema StorageGRID.



Cuando SSO está habilitado, todos los usuarios deben utilizar SSO para acceder a Grid Manager, al arrendatario Manager, a la API de gestión de grid y a la API de gestión de inquilinos. Los usuarios locales ya no pueden acceder a StorageGRID.

Pasos

1. Desde el paso de configuración de prueba del asistente de configuración de SSO, seleccione **Habilitar SSO**.
2. Revise el mensaje de advertencia y seleccione **Habilitar SSO**.

El inicio de sesión único ahora está habilitado. Aparece la página de inicio de sesión único y ahora incluye los detalles del SSO que acaba de configurar.

3. Para editar la configuración, seleccione **Editar**.
4. Para deshabilitar el inicio de sesión único, seleccione **Deshabilitar SSO**.



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

Crear 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.

Antes de empezar

- Ha configurado el inicio de sesión único para StorageGRID y ha seleccionado **AD FS** como tipo SSO.
- Tienes "[entró en modo sandbox](#)" en el Administrador de cuadrícula.
- 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 Configurar SSO de StorageGRID .



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.
- Si crea la confianza de la parte de confianza manualmente, tiene el certificado personalizado que se cargó

para la interfaz de gestión de StorageGRID, o sabe cómo iniciar sesión en un nodo de administrador 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. Consulte la documentación de Microsoft AD FS si tiene alguna pregunta.

Cree una confianza de parte de confianza mediante Windows PowerShell

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

Pasos

1. En el menú de inicio de Windows, seleccione con el botón derecho 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_Identifier*, introduzca el identificador de parte de confianza para el nodo de administración, tal y como aparece en la página Conexión Única. Por ejemplo, SG-DC1-ADM1.
- Para *Admin_Node_FQDN*, introduzca 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. Seleccione **aplicar** y seleccione **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. Seleccione **Agregar regla**.
- d. En la página Seleccionar plantilla de regla, seleccione **Enviar atributos LDAP como reclamaciones** en la lista y seleccione **Siguiente**.
- e. En la página Configurar regla, introduzca un nombre para mostrar para esta regla.

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

- f. Para el almacén de atributos, seleccione **Active Directory**.
 - g. En la columna Atributo LDAP de la tabla de asignación, escriba **objectGUID** o seleccione **User-Principal-Name**.
 - h. En la columna Tipo de reclamación saliente de la tabla asignación, seleccione **ID de nombre** en la lista desplegable.
 - i. Seleccione **Finalizar** y seleccione **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 los metadatos, confirme que la dirección de metadatos de federación es correcta o 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, regrese a StorageGRID y "[Probar todos los fideicomisos de partes confiantes](#)" para confirmar que están configurados correctamente.

Cree una confianza de parte de confianza importando 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.

Pasos

1. En Windows Server Manager, seleccione **Herramientas** y, a continuación, seleccione **Administración de AD FS**.
2. En acciones, seleccione **Agregar confianza de parte de confianza**.
3. En la página de bienvenida, elija **Claims aware** y seleccione **Start**.
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*, introduzca 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. Seleccione **Agregar regla**:
- c. En la página Seleccionar plantilla de regla, seleccione **Enviar atributos LDAP como reclamaciones** en la lista y seleccione **Siguiente**.
- d. En la página Configurar regla, introduzca un nombre para mostrar para esta regla.

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

- e. Para el almacén de atributos, seleccione **Active Directory**.
- f. En la columna Atributo LDAP de la tabla de asignación, escriba **objectGUID** o seleccione **User-Principal-Name**.
- g. En la columna Tipo de reclamación saliente de la tabla asignación, seleccione **ID de nombre** en la lista desplegable.
- h. Seleccione **Finalizar** y seleccione **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 los metadatos, confirme que la dirección de metadatos de federación es correcta o 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, regrese a StorageGRID y "[Probar todos los fideicomisos de partes confiantes](#)" para confirmar que están configurados correctamente.

Cree 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.

Pasos

1. En Windows Server Manager, seleccione **Herramientas** y, a continuación, seleccione **Administración de AD FS**.
2. En acciones, seleccione **Agregar confianza de parte de confianza**.
3. En la página de bienvenida, elija **Claims aware** y seleccione **Start**.
4. Seleccione **introducir datos sobre la parte que confía manualmente** y seleccione **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, seleccione la casilla de verificación **Habilitar soporte para 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*, introduzca 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*, introduzca el identificador de parte de confianza para el nodo de administración, tal y como aparece en la página Conexión Única. 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, seleccione **Agregar regla**:
 - a. En la página Seleccionar plantilla de regla, seleccione **Enviar atributos LDAP como reclamaciones** en la lista y seleccione **Siguiente**.
 - b. En la página Configurar regla, introduzca un nombre para mostrar para esta regla.

Por ejemplo, **ObjectGUID to Name ID** o **UPN to Name ID**.
 - c. Para el almacén de atributos, seleccione **Active Directory**.
 - d. En la columna Atributo LDAP de la tabla de asignación, escriba **objectGUID** o seleccione **User-Principal-Name**.
 - e. En la columna Tipo de reclamación saliente de la tabla asignación, seleccione **ID de nombre** en la lista desplegable.
 - f. Seleccione **Finalizar** y seleccione **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. Seleccione **Añadir 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`, introduzca 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. Seleccione **OK**.

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 administración, vaya al `/var/local/mgmt-api` directorio del nodo de administración y agregue el `custom-server.crt` archivo de certificado.



(`server.crt` No se recomienda utilizar el certificado por defecto del nodo de administración). 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. Seleccione **aplicar** y seleccione **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, regrese a StorageGRID y "[Probar todos los fideicomisos de partes confiantes](#)" para confirmar que están configurados correctamente.

Crear aplicaciones empresariales en Entra ID

Utilice Entra ID 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 **Entra ID** como tipo de SSO.
- Tienes "[entró en modo sandbox](#)" en el Administrador de cuadrícula.
- 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 Configurar SSO.



Debe crear una aplicación empresarial para cada nodo administrador en el sistema StorageGRID. Disponer de una aplicación empresarial para cada nodo de administración garantiza que los usuarios puedan iniciar sesión de forma segura en cualquier nodo de administración.

- Tienes experiencia en la creación de aplicaciones empresariales en Entra ID.

- Tienes una cuenta Entra ID con una suscripción activa.
- Tiene uno de los siguientes roles en la cuenta de Entra ID: Administrador global, Administrador de aplicaciones en la nube, Administrador de aplicaciones o propietario de la entidad de servicio.

Acceso Entra ID

Pasos

1. Inicie sesión en el ["Portal de Azure"](#).
2. Navegar a ["Identificación de entrada"](#).
3. Seleccione ["Aplicaciones de negocio"](#).

Creación de aplicaciones empresariales y guardado de la configuración de SSO de StorageGRID

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

Pasos

1. Repita los siguientes pasos para cada nodo de administrador.
 - a. En el panel de aplicaciones de Entra ID Enterprise, seleccione **Nueva aplicación**.
 - b. Seleccione **Crear su 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 Configurar SSO.
 - d. Deje seleccionada la opción **integrar cualquier otra aplicación que no encuentre en la galería (no galería)**.
 - e. Seleccione **Crear**.
 - f. Seleccione el enlace **Get Started** en **2. Configure el cuadro de inicio de sesión único** en o seleccione el enlace **Single Sign-On** en el margen izquierdo.
 - g. Seleccione la casilla **SAML**.
 - h. Copie la URL * metadatos de Federación de aplicaciones*, que puede encontrar en **Paso 3 Certificado de firma SAML**.
 - i. Vaya a la página Configurar SSO 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 Configurar SSO.

Descargue los metadatos de SAML para cada nodo de administración

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

Pasos

1. Repita estos pasos para cada nodo de administración.
 - a. Inicie sesión en StorageGRID desde el nodo de administrador.

- b. Seleccione **Configuración > Control de acceso > Inicio de sesión único**.
- c. Seleccione el botón para descargar los metadatos de SAML de ese nodo de administración.
- d. Guarde el archivo que cargará en Entra ID.

Cargue metadatos de SAML en cada aplicación empresarial

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

Pasos

1. Vuelva al portal de Azure.
2. Repita estos pasos con cada aplicación de empresa:



Es posible que deba actualizar la página aplicaciones de empresa para ver las aplicaciones que ha agregado anteriormente en la lista.

- a. Vaya a la página Propiedades de la aplicación de empresa.
 - b. Establezca **asignación requerida** en **no** (a menos que desee configurar las asignaciones por separado).
 - c. Vaya a la página Single Sign-On.
 - d. Complete la configuración de SAML.
 - e. Seleccione el botón **Upload metadata file** y seleccione el archivo de metadatos SAML que descargó para el nodo de administración correspondiente.
 - f. Después de cargar el archivo, seleccione **Guardar** y, a continuación, seleccione **X** para cerrar el panel. Volverá a la página Set up Single Sign-On with SAML.
3. ["Pruebe cada aplicación"](#) .

Cree conexiones de proveedores de servicios (SP) en PingFederate

Puede utilizar PingFederate para crear una conexión de proveedor de servicios (SP) para cada nodo de administración del sistema. Para acelerar el proceso, importe los metadatos SAML de StorageGRID.

Antes de empezar

- Ha configurado el inicio de sesión único para StorageGRID y ha seleccionado **Ping federate** como tipo de SSO.
- Tienes ["entró en modo sandbox"](#) en el Administrador de cuadrícula.
- 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 Configurar SSO.
- Ha descargado los **metadatos SAML** de cada nodo de administración del sistema.
- Tiene experiencia en la creación de conexiones SP en PingFederate Server.
- Tiene el ["Guía de referencia del administrador"](#) servidor FOR PingFederate. La documentación de PingFederate proporciona instrucciones detalladas paso a paso y explicaciones.
- 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 un proveedor SSO para StorageGRID. Si está utilizando otra versión de PingFederate, puede que necesite adaptar estas instrucciones. Consulte la documentación de PingFederate Server para obtener instrucciones detalladas para su publicación.

Complete los requisitos previos en PingFederate

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

Crear almacén de datos

Si aún no lo ha hecho, cree un almacén de datos para conectar PingFederate al servidor LDAP de AD FS. Use los valores que utilizó en ["configurando la federación de identidades"](#)StorageGRID.

- **Tipo:** Directorio (LDAP)
- **Tipo LDAP:** Active Directory
- **Nombre del atributo binario:** Introduzca **objectGUID** en la ficha atributos binarios LDAP exactamente como se muestra.

Crear validador de credenciales de contraseña

Si todavía no lo ha hecho, cree un validador de credencial de contraseña.

- **Tipo:** Validador de credenciales de nombre de usuario de LDAP
- **Almacén de datos:** Seleccione el almacén de datos que creó.
- **Search base:** Introduzca la información de LDAP (por ejemplo, DC=saml,DC=sgws).
- **Filtro de búsqueda:** SAMAccountName=\${username}
- **Ámbito:** Subárbol

Crear instancia de adaptador IDP[[instancia de adaptador]]

Si todavía no lo ha hecho, cree una instancia de adaptador de IDP.

Pasos

1. Vaya a **autenticación > integración > Adaptadores IDP**.
2. Seleccione **Crear nueva instancia**.
3. En la ficha Tipo, seleccione **adaptador IDP de formulario HTML**.
4. En la ficha adaptador IDP, seleccione **Agregar una nueva fila a 'Validadores de credenciales'**.
5. Seleccione el [validador de credenciales de contraseña](#) que creaste.
6. En la ficha atributos del adaptador, seleccione el atributo **nombre de usuario** para **seudónimo**.
7. Seleccione **Guardar**.

Crear o importar un certificado de firma[[certificado de firma]]

Si todavía 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.

Cree una conexión SP en PingFederate

Cuando crea una conexión del SP en PingFederate, importe los metadatos SAML que ha descargado de StorageGRID para el nodo de administración. El archivo de metadatos contiene muchos de los valores específicos necesarios.



Debe crear una conexión de SP para cada nodo de administrador en su sistema de StorageGRID, de modo que los usuarios puedan iniciar sesión desde y hacia cualquier nodo de forma segura. Utilice estas instrucciones para crear la primera conexión del SP. A continuación, vaya a [Cree conexiones adicionales del SP](#) para crear las conexiones adicionales que necesite.

Elija el tipo de conexión del SP

Pasos

1. Vaya a **aplicaciones > integración > conexiones SP**.
2. Seleccione **Crear conexión**.
3. Seleccione **no utilice una plantilla para esta conexión**.
4. Seleccione **Examinador SSO Profiles y SAML 2.0** como protocolo.

Importe los metadatos de SP

Pasos

1. En la ficha Importar metadatos, seleccione **Archivo**.
2. Elija el archivo de metadatos SAML que descargó de la página Configurar SSO 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 partner y el nombre de 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 administrador de StorageGRID.

4. Seleccione **Siguiente**.

Configure el SSO del explorador IDP

Pasos

1. En la ficha SSO del explorador, seleccione **Configurar SSO del explorador**.
2. En la ficha Perfiles de SAML, seleccione las opciones **SSO iniciado por el SP**, **SLO inicial de SP**, **SSO iniciado por IDP** y **SLO iniciado por IDP**.
3. Seleccione **Siguiente**.
4. En la ficha ciclo de vida de las aserción, no realice cambios.
5. En la ficha creación de aserción, seleccione **Configurar creación de aserción**.
 - a. En la ficha asignación de identidades, seleccione **Estándar**.
 - b. En la ficha Contrato de atributo, utilice el formato **SAML_SUBJECT** como atributo Contract y el formato de nombre no especificado que se importó.
6. Para Extender el contrato, seleccione **Eliminar** para eliminar el `urn:oid`, que no se utiliza.

Asigne la instancia del adaptador

Pasos

1. En la ficha asignación de origen de autenticación, seleccione **asignar nueva instancia de adaptador**.
2. En el separador Instancia de Adaptador, seleccione el **instancia del adaptador** que ha creado.
3. En la ficha método de asignación, seleccione **recuperar atributos adicionales de un almacén de datos**.
4. En la ficha origen del atributo y Búsqueda del usuario, seleccione **Agregar origen del atributo**.
5. En la pestaña Almacén de datos, proporcione una descripción y seleccione la que **almacén de datos** ha agregado.
6. En la ficha Búsqueda de directorios LDAP:
 - Introduzca el **DN base**, que debe coincidir exactamente con el valor especificado en StorageGRID para el servidor LDAP.
 - Para el ámbito de búsqueda, seleccione **Subtree**.
 - Para la clase de objeto raíz, busque y agregue cualquiera de estos atributos: **ObjectGUID** o **userPrincipalName**.
7. En la ficha tipos de codificación de atributos binarios LDAP , seleccione **Base64** para el atributo **objectGUID** .
8. En la ficha filtro LDAP, introduzca **sAMAccountName=\${username}**.
9. En la pestaña Cumplimiento de contrato de atributo, seleccione **LDAP (atributo)** en la lista desplegable Origen y seleccione **objectGUID** o **userPrincipalName** en la lista desplegable Valor.
10. Revise y, a continuación, guarde el origen del atributo.
11. En la ficha origen del atributo Failsave, seleccione **Anular la transacción SSO**.
12. Revise el resumen y seleccione **hecho**.
13. Seleccione **Listo**.

Configure los ajustes de protocolo

Pasos

1. En la ficha **Conexión SP > SSO del navegador > Configuración de protocolo**, seleccione **Configurar ajustes de protocolo**.
2. En la pestaña URL de servicio al consumidor de aserción, acepte los valores predeterminados, que se importaron desde los metadatos de SAML de StorageGRID (**POST** para enlace y `/api/saml-response` para URL de punto final).
3. En la pestaña URL del servicio de SLO, acepte los valores predeterminados, que se importaron desde los metadatos de SAML de StorageGRID (**REDIRECT** para enlace y `/api/saml-logout` para URL de punto final).
4. En la pestaña Enlaces SAML permitidos, desactive **ARTEFACTO** y **SOAP**. Sólo se requieren **POST** y **REDIRECT**.
5. En la pestaña Política de firma, deje las casillas de verificación **Requerir que se firmen las solicitudes AUTHN** y **Siempre firmar afirmación** seleccionadas.
6. En la ficha Directiva de cifrado, seleccione **Ninguno**.
7. Revise el resumen y seleccione **hecho** para guardar la configuración del protocolo.
8. Revise el resumen y seleccione **hecho** para guardar la configuración de SSO del explorador.

Configurar credenciales

Pasos

1. En la ficha Conexión SP, seleccione **credenciales**.
2. En la ficha credenciales, seleccione **Configurar credenciales**.
3. Seleccione el [certificado de firma](#) usted creó o importó.
4. Seleccione **Siguiente** para ir a **gestionar ajustes de verificación de firma**.
 - a. En la ficha Modelo de confianza, seleccione **sin anclar**.
 - b. En la pestaña Certificado de verificación de firma, revise la información de certificación 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.

Cree conexiones adicionales del SP

Puede copiar la primera conexión de SP para crear las conexiones de SP que necesita para cada nodo de administrador de su grid. Se cargan metadatos nuevos para cada copia.



Las conexiones SP para diferentes nodos de administración utilizan valores idénticos, a excepción del ID de entidad del partner, la URL base, el ID de conexión, el nombre de conexión, la verificación de firma, Y 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. Introduzca el ID de conexión y el nombre de conexión para la copia y seleccione **Guardar**.
3. Elija el archivo de metadatos que corresponde 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 explorador > Configurar creación de aserción > Contrato de atributo**.
 - c. Elimine la entrada para **urn:oid**.
 - d. Seleccione **Guardar**.

Deshabilitar SSO

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.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante una ["navegador web compatible"](#).

- Tienes "permisos de acceso específicos".

Pasos

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

Aparece la página Single Sign-On.

2. Seleccione **Deshabilitar SSO**.
3. Seleccione **Sí**.

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

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.

Deshabilitar y volver a habilitar temporalmente el SSO 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.

Antes de empezar

- Tienes "permisos de acceso específicos".
- Tiene el `Passwords.txt` archivo.
- Conoce 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 **Enable SSO** en la página Single Sign-On en Grid Manager permanece seleccionada y se mantienen todas las configuraciones de SSO existentes a menos que las actualice.

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 el `Passwords.txt` archivo.
 - c. Introduzca el siguiente comando para cambiar a raíz: `su -`
 - d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

Al iniciar sesión como root, la petición de datos cambia de \$ a #.

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. Seleccione **Guardar**.

Al seleccionar **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. Seleccione **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 de copyright

Copyright © 2026 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 INTERRUPTIÓN 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.