



# **Controlando el acceso del administrador a StorageGRID**

StorageGRID 11.5

NetApp  
April 11, 2024

# Tabla de contenidos

- Controlando el acceso del administrador a StorageGRID ..... 1
  - Controlar el acceso mediante firewalls ..... 1
  - Mediante la federación de identidades ..... 2
  - Gestión de los grupos de administración ..... 8
  - Gestión de usuarios locales ..... 17
  - Uso del inicio de sesión único (SSO) para StorageGRID ..... 19
  - Configurar certificados de cliente de administrador ..... 38

# Controlando el acceso del administrador a StorageGRID

Puede controlar el acceso de administrador al sistema StorageGRID abriendo o cerrando puertos de firewall, gestionando grupos de administradores y usuarios, configurando el inicio de sesión único (SSO) y proporcionando certificados de cliente para permitir un acceso externo seguro a las métricas de StorageGRID.

- ["Controlar el acceso mediante firewalls"](#)
- ["Mediante la federación de identidades"](#)
- ["Gestión de los grupos de administración"](#)
- ["Gestión de usuarios locales"](#)
- ["Uso del inicio de sesión único \(SSO\) para StorageGRID"](#)
- ["Configurar certificados de cliente de administrador"](#)

## Controlar el acceso mediante firewalls

Cuando desee controlar el acceso a través de firewalls, puede abrir o cerrar puertos específicos en el firewall externo.

### Control del acceso en el firewall externo

Puede controlar el acceso a las interfaces de usuario y las API de los nodos de administrador de StorageGRID. Para ello, abra y cierre puertos específicos en el firewall externo. Por ejemplo, es posible que desee evitar que los inquilinos puedan conectarse a Grid Manager en el firewall, además de utilizar otros métodos para controlar el acceso al sistema.

Puerto	Descripción	Si el puerto está abierto...
443	Puerto HTTPS predeterminado para nodos de administración	Los exploradores web y los clientes de la API de gestión pueden acceder a Grid Manager, a la API de gestión de grid, al administrador de inquilinos y a la API de gestión de inquilinos.  <b>Nota:</b> el puerto 443 también se utiliza para tráfico interno.
8443	Puerto de Grid Manager restringido en nodos de administración	<ul style="list-style-type: none"><li>• Los exploradores web y los clientes de la API de gestión pueden acceder a Grid Manager y a la API de gestión de grid mediante HTTPS.</li><li>• Los exploradores web y los clientes de API de gestión no pueden acceder al administrador de inquilinos ni a la API de gestión de inquilinos.</li><li>• Se rechazarán las solicitudes de contenido interno.</li></ul>

Puerto	Descripción	Si el puerto está abierto...
9443	Puerto de administrador de inquilinos restringido en los nodos de administrador	<ul style="list-style-type: none"> <li>• Los exploradores web y los clientes de API de gestión pueden acceder al administrador de inquilinos y a la API de gestión de inquilinos mediante HTTPS.</li> <li>• Los exploradores web y los clientes de la API de administración no pueden acceder a Grid Manager ni a la API de gestión de grid.</li> <li>• Se rechazarán las solicitudes de contenido interno.</li> </ul>



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.

### Información relacionada

["Iniciando sesión en Grid Manager"](#)

["Creación de una cuenta de inquilino si StorageGRID no utiliza SSO"](#)

["Resumen: Direcciones IP y puertos para conexiones cliente"](#)

["Administración de redes de clientes que no son de confianza"](#)

["Instalar Ubuntu o Debian"](#)

["Instale VMware"](#)

["Instale Red Hat Enterprise Linux o CentOS"](#)

## Mediante 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.

### Configurando la federación de identidades

Puede configurar la federación de identidades si desea que los grupos de administración y los usuarios se gestionen en otro sistema, como Active Directory, OpenLDAP u Oracle Directory Server.

#### Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener permisos de acceso específicos.
- Si planea habilitar el inicio de sesión único (SSO), debe utilizar Active Directory como el origen de identidad federado y AD FS como proveedor de identidades. Véase «requisitos para el uso de la entrada única».
- Debe utilizar Active Directory, OpenLDAP o Oracle Directory Server como proveedor de identidades.



Si desea utilizar un servicio LDAP v3 que no esté en la lista, debe ponerse en contacto con el soporte técnico.

- Si planea utilizar la seguridad de la capa de transporte (TLS) para las comunicaciones con el servidor LDAP, el proveedor de identidades debe usar TLS 1.2 o 1.3.

### Acerca de esta tarea

Debe configurar un origen de identidad para el Gestor de grid si desea importar los siguientes tipos de grupos federados:

- Grupos administrativos. 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.

### Pasos

1. Seleccione **Configuración > Control de acceso > Federación de identidades**.
2. Seleccione **Activar federación de identidades**.

Aparecen los campos para configurar el servidor LDAP.

3. En la sección Tipo de servicio LDAP, seleccione el tipo de servicio LDAP que desea configurar.

Puede seleccionar **Active Directory**, **OpenLDAP** o **otros**.



Si selecciona **OpenLDAP**, debe configurar el servidor OpenLDAP. Consulte las directrices para configurar un servidor OpenLDAP.



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 .
  - **Nombre único de usuario:** 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 va a configurar Oracle Directory Server, introduzca `uid`.
  - **UUID de usuario:** 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 va a configurar Oracle Directory Server, introduzca `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:** 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 va a configurar Oracle Directory Server, introduzca `cn`.
  - **UUID de grupo:** 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 va a configurar Oracle Directory Server, introduzca `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. En la sección Configure LDAP Server, introduzca la información sobre el servidor LDAP y las conexiones de red necesarias.

- **Hostname:** El nombre de host del servidor 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

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

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

- **Usar STARTTLS (recomendado):** Usar STARTTLS para asegurar las comunicaciones con el servidor LDAP. Esta es la opción recomendada.
- **Use LDAPS:** La opción LDAPS (LDAP sobre SSL) utiliza TLS para establecer una conexión con el servidor LDAP. Esta opción es compatible por motivos de compatibilidad.
- **No utilice TLS:** El tráfico de red entre el sistema StorageGRID y el servidor LDAP no estará protegido.



El uso de la opción **no usar TLS** no es compatible si el servidor de Active Directory aplica la firma LDAP. Debe usar 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 CA predeterminado 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.

8. Opcionalmente, seleccione **probar conexión** para validar la configuración de conexión para el servidor LDAP.

Si la conexión es válida, aparecerá un mensaje de confirmación en la esquina superior derecha de la página.

9. Si la conexión es válida, seleccione **Guardar**.

La siguiente captura de pantalla muestra valores de configuración de ejemplo para un servidor LDAP que utiliza Active Directory.

## LDAP service type

Select the type of LDAP service you want to configure.

Active Directory

OpenLDAP

Other

## Configure LDAP server (All fields are required)

Hostname

my-active-directory.example.com

Port

389

Username

MyDomain\Administrator

Password

••••••••

Group Base DN

DC=storagegrid,DC=example,DC=com

User Base DN

DC=storagegrid,DC=example,DC=com

### Información relacionada

["Cifrados compatibles para conexiones TLS salientes"](#)

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

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

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

### 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.



## Revestimientos memberOf y ref

Se deben habilitar las superposiciones memberof y ref. Para obtener más información, consulte las instrucciones para el mantenimiento de miembros del grupo inverso en la Guía del administrador para OpenLDAP.

## 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 de pertenencia a grupos revertidos en la Guía del administrador para OpenLDAP.

## Información relacionada

["Documentación de OpenLDAP: Guía del administrador de la versión 2.4"](#)

## 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.

### Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener permisos de acceso específicos.
- El origen de identidades debe estar activado.

### Pasos

1. Seleccione **Configuración > Control de acceso > Federación de identidades**.

Aparece la página Federación de identidades. El botón **Sincronizar** se encuentra en la parte inferior de la página.

#### Synchronize

---

StorageGRID periodically synchronizes federated groups and users from the configured LDAP server. Clicking the button below will immediately start the synchronization process against the saved LDAP server.

Synchronize

2. Haga clic en **Sincronizar**.

Un mensaje de confirmación indica que la sincronización se ha iniciado correctamente. 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.

## Desactivar la federación de identidades

Puede deshabilitar temporalmente o de forma permanente la federación de identidades para grupos y usuarios. Cuando la federación de identidades está deshabilitada, no existe comunicación entre StorageGRID y el origen de identidades. Sin embargo, cualquier configuración que haya configurado se conservará, lo que le permitirá volver a habilitar fácilmente la federación de identidades en el futuro.

### Lo que necesitará

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

### 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 realizará la sincronización entre el sistema StorageGRID y el origen de identidad, y no se realizarán alertas ni alarmas para las cuentas que no se hayan sincronizado.
- La casilla de verificación **Activar Federación de identidades** está desactivada si el inicio de sesión único (SSO) está establecido en **activado** o **modo Sandbox**. El estado de SSO de la página Single Sign-On debe ser **Desactivado** antes de poder deshabilitar la federación de identidades.

### Pasos

1. Seleccione **Configuración > Control de acceso > Federación de identidades**.
2. Desactive la casilla de verificación **Activar Federación de identidades**.
3. Haga clic en **Guardar**.

### Información relacionada

["Desactivar el inicio de sesión único"](#)

## Gestión de los grupos de administración

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.

### Creando grupos de administradores

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.

### Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.

- Debe tener permisos de acceso específicos.
- Si planea importar un grupo federado, debe haber configurado la federación de identidades y el grupo federado debe existir ya en el origen de identidades configurado.

## Pasos

1. Seleccione **Configuración > Control de acceso > grupos de administración**.

Se mostrará la página Admin Groups, donde se enumeran los grupos de administración existentes.

### Admin Groups

Add and manage local and federated user groups, allowing member users to sign in to the Grid Manager. Set group permissions to control access to specific pages and features.

<input type="button" value="+ Add"/> <input type="button" value="Clone"/> <input type="button" value="Edit"/> <input type="button" value="Remove"/>				
	Name	ID	Group Type	Access Mode
<input checked="" type="radio"/>	Flintstone	264083d0-23b5-3046-9bd4-88b7097731ab	Federated	Read-write
<input type="radio"/>	Simpson	cc8ad11f-68d0-f84a-af29-e7a6fcdc63a2	Federated	Read-only
<input type="radio"/>	ILM (read-only group)	88446141-9599-4543-b183-9c227ce7767a	Local	Read-only
<input type="radio"/>	API Developers	974b2faa-f9a1-4cfc-b364-914cdba2905f	Local	Read-write
<input type="radio"/>	ILM Admins (read-write)	a528c0c2-2417-4559-86ed-f0d2e31da820	Local	Read-write
<input type="radio"/>	Maintenance Users	7e3400ec-de8c-45a7-8bb8-e1496b362a8d	Local	Read-write

Group Type:  Show  rows per page

2. Seleccione **Agregar**.

Aparece el cuadro de diálogo Agregar grupo.

## Add Group

Create a new local group or import a group from the external identity source.

Group Type  Local  Federated

Display Name

Unique Name

Access Mode  Read-write  Read-only

### Management Permissions

Root Access

Acknowledge Alarms

Other Grid Configuration

Change Tenant Root Password

Metrics Query

Object Metadata Lookup

Manage Alerts

Grid Topology Page Configuration

Tenant Accounts

Maintenance

ILM

Storage Appliance Administrator

Cancel

Save

3. En Tipo de grupo, seleccione **local** si desea crear un grupo que sólo se utilizará dentro de StorageGRID, o seleccione **federado** si desea importar un grupo desde el origen de identidades.
4. Si ha seleccionado **local**, introduzca un nombre para mostrar para el grupo. El nombre para mostrar es el nombre que aparece en el Gestor de cuadrícula. Por ejemplo, «usuarios de mantenimiento» o «Administradores de ILM».
5. Introduzca un nombre único para el grupo.
  - **Local**: Introduzca el nombre único que desee. Por ejemplo, «Administradores de ILM».
  - **Federado**: Introduzca el nombre del grupo exactamente como aparece en el origen de identidad configurado.
6. 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 en la API de gestión 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.

7. Seleccione uno o más permisos de gestión.

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

8. Seleccione **Guardar**.

Se creará el nuevo grupo. Si se trata de un grupo local, ahora puede agregar uno o más usuarios. Si se trata de un grupo federado, el origen de identidades gestiona los usuarios que pertenecen al grupo.

### Información relacionada

["Gestión de usuarios locales"](#)

## 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 que pertenezcan a ese grupo no podrán iniciar sesión en Grid Manager.

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
- Consulte la consola
- Puede ver las páginas Nodes
- Supervise la topología de grid
- Ver las alertas actuales y resueltas
- Ver alarmas actuales e históricas (sistema heredado)
- Cambiar su propia contraseña (sólo usuarios locales)
- Vea cierta información en las páginas Configuración y Mantenimiento

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.

### 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.

## Reconocer alarmas (sistema heredado)

Este permiso proporciona acceso para reconocer y responder a alarmas (sistema heredado). Todos los usuarios que han iniciado sesión pueden ver las alarmas actuales e históricas.

Si desea que un usuario supervise la topología de la cuadrícula y reconozca únicamente las alarmas, debe asignar este permiso.

## Configuración de la página de topología de la cuadrícula

Este permiso permite acceder a las siguientes opciones de menú:

- Fichas de configuración disponibles en las páginas de **Soporte > Herramientas > Topología de cuadrícula**.
- **Restablecer recuentos de eventos** enlace en la ficha **nodos > Eventos**.

## Otra configuración de cuadrícula

Este permiso proporciona acceso a opciones de configuración de cuadrícula adicionales.



Para ver estas opciones adicionales, los usuarios también deben tener el permiso Configuración de página de topología de cuadrícula.

- **Alarmas** (sistema heredado):
  - Alarmas globales
  - Configuración de correo electrónico heredado
- **ILM:**
  - Pools de almacenamiento
  - Grados de almacenamiento
- **Configuración > Configuración de red**
  - Coste del enlace
- **Configuración > Configuración del sistema:**
  - Opciones de visualización
  - Opciones de cuadrícula
  - Opciones de almacenamiento
- **Configuración > Supervisión:**
  - Eventos
- **Soporte:**
  - AutoSupport

## Cuentas de inquilino

Este permiso permite acceder a la página **arrendatarios > Cuentas de inquilino**.



La versión 1 de la API de gestión de grid (que se ha obsoleto) utiliza este permiso para gestionar las políticas de grupos de inquilinos, restablecer las contraseñas de administrador de Swift y gestionar las claves de acceso de S3 de usuario raíz.

### Cambiar la contraseña raíz del inquilino

Este permiso proporciona acceso a la opción **Cambiar contraseña raíz** de la página Cuentas de arrendatarios, lo que le permite controlar quién puede cambiar la contraseña del usuario raíz local del arrendatario. Los usuarios que no tienen este permiso no pueden ver la opción **Cambiar contraseña raíz**.



Debe asignar el permiso Cuentas de inquilino al grupo para poder asignar este permiso.

### Mantenimiento

Este permiso permite acceder a las siguientes opciones de menú:

- **Configuración > Configuración del sistema:**

- Nombres de dominio\*
- Certificados de servidor\*

- **Configuración > Supervisión:**

- Auditoría\*

- **Configuración > Control de acceso:**

- Contraseñas de grid

- **Mantenimiento > tareas de mantenimiento**

- Retirada
- Expansión
- Recuperación

- **Mantenimiento > Red:**

- Servidores DNS\*
- Red de red\*
- Servidores NTP\*

- **Mantenimiento > sistema:**

- Licencia\*
- Paquete de recuperación
- Actualización de software

- **Soporte > Herramientas:**

- Registros

- Los usuarios que no tienen permiso de mantenimiento pueden ver, pero no editar, las páginas marcadas con un asterisco.

### Consulta de métricas

Este permiso permite acceder a la página **Support > Tools > Metrics**. Este permiso también proporciona

acceso a consultas de métricas Prometheus personalizadas mediante la sección **Metrics** de la API de gestión de grid.

## ILM

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

- **Código de borrado**
- **Reglas**
- **Políticas**
- **Regiones**



El acceso a las opciones de menú **ILM > agrupaciones de almacenamiento** y **ILM > grados de almacenamiento** está controlado por los permisos de configuración de páginas de configuración de cuadrícula y topología de cuadrícula.

## Búsqueda de metadatos de objetos

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

## Administrador de dispositivos de almacenamiento

Este permiso proporciona acceso al System Manager de SANtricity E-Series en dispositivos de almacenamiento a través de Grid Manager.

## 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 funciones 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.

## Desactivación de funciones de la API de Grid Management

Puede utilizar la API de gestión de grid para desactivar por completo determinadas funciones del sistema StorageGRID. Cuando se desactiva una función, no se pueden asignar permisos a nadie para realizar las tareas relacionadas con esa función.

### Acerca de esta tarea

El sistema de funciones desactivadas le permite impedir el acceso a determinadas funciones del sistema StorageGRID. La desactivación de una característica es la única manera de impedir que el usuario raíz o los usuarios que pertenecen a grupos de administrador con el permiso acceso raíz puedan utilizar esa función.

Para comprender cómo puede ser útil esta funcionalidad, considere el siguiente escenario:

*Company A es un proveedor de servicios que arrienda la capacidad de almacenamiento de su sistema StorageGRID mediante la creación de cuentas de inquilino. Para proteger la seguridad de los objetos de sus arrendatarios, la Compañía A desea asegurarse de que sus propios empleados nunca tengan acceso a ninguna cuenta de arrendatario después de que se haya implementado la cuenta.*

*La empresa A puede lograr este objetivo mediante el sistema Desactivar características en la API de gestión de grid. Al desactivar completamente la característica **Cambiar contraseña raíz de inquilino** en el administrador de grid (tanto la interfaz de usuario como la API), la empresa A puede garantizar que ningún*



usuario de administrador (incluido el usuario raíz y los usuarios pertenecientes a grupos con permiso de acceso raíz) puede cambiar la contraseña para el usuario raíz de cualquier cuenta de arrendatario.

### Reactivación de las funciones desactivadas

De forma predeterminada, puede utilizar la API de administración de grid para reactivar una función que se haya desactivado. Sin embargo, si desea evitar que alguna vez se reactiven las funciones desactivadas, puede desactivar la propia función **activateFeatures**.



La función **activateFeatures** no se puede reactivar. Si decide desactivar esta función, tenga en cuenta que perderá permanentemente la capacidad de reactivar otras funciones desactivadas. Para restaurar cualquier funcionalidad perdida, debe ponerse en contacto con el soporte técnico.

Para obtener detalles, consulte las instrucciones para implementar las aplicaciones cliente S3 o Swift.

### Pasos

1. Acceda a la documentación de Swagger para la API de Grid Management.
2. Busque el extremo Desactivar funciones.
3. Para desactivar una función, como **Cambiar contraseña raíz de inquilino**, envíe un cuerpo a la API de este modo:

```
{ "grid": {"changeTenantRootPassword": true} }
```

Cuando se completa la solicitud, se desactiva la función Cambiar contraseña raíz de inquilino. El permiso Cambiar la administración de la contraseña raíz del inquilino ya no aparece en la interfaz de usuario y cualquier solicitud de API que intente cambiar la contraseña raíz de un inquilino fallará con "403 Prohibido".

4. Para reactivar todas las funciones, envíe un cuerpo a la API de este modo:

```
{ "grid": null }
```

Cuando se completa esta solicitud, se reactivan todas las funciones, incluida la función Cambiar contraseña raíz de inquilino. El permiso Cambiar la administración de contraseña raíz de arrendatario ahora aparece en la interfaz de usuario y cualquier solicitud de API que intente cambiar la contraseña raíz de un inquilino se realizará correctamente, suponiendo que el usuario tenga el permiso de administración de acceso raíz o Cambiar contraseña raíz de inquilino.



El ejemplo anterior hace que se reactiven las funciones *all* desactivadas. Si se han desactivado otras funciones que deben permanecer desactivadas, debe especificarlas explícitamente en la solicitud PUT. Por ejemplo, para reactivar la función Cambiar contraseña raíz de inquilino y continuar desactivando la función de confirmación de alarma, envíe esta solicitud DE PUT:

```
{ "grid": { "alarmAcknowledgment": true } }
```

## Información relacionada

["Uso de la API de gestión de grid"](#)

## Modificar un grupo de administración

Es posible modificar un grupo admin para cambiar los permisos asociados con el grupo. Para los grupos de administración locales, también puede actualizar el nombre para mostrar.

### Lo que necesitará

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

### Pasos

1. Seleccione **Configuración > Control de acceso > grupos de administración**.
2. Seleccione el grupo.

Si el sistema incluye más de 20 elementos, puede especificar cuántas filas se muestran en cada página a la vez. A continuación, puede utilizar la función de búsqueda de su navegador para buscar un elemento específico en las filas mostradas actualmente.

3. Haga clic en **Editar**.
4. Opcionalmente, para grupos locales, introduzca el nombre del grupo que aparecerá a los usuarios, por ejemplo, "usuarios de mantenimiento".

No se puede cambiar el nombre único, que es el nombre del grupo interno.

5. Si lo desea, puede cambiar el modo de acceso del grupo.
  - **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 en la API de gestión 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.

6. Opcionalmente, añada o elimine permisos de grupo.

Consulte la información sobre los permisos del grupo de administración.

7. Seleccione **Guardar**.

## Información relacionada

[Permisos de grupo de administradores](#)

## Eliminar un grupo de administrador

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 de administrador del grupo, pero no se eliminan los usuarios de administrador.

### Lo que necesitará

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

### Acerca de esta tarea

Al eliminar un grupo, los usuarios asignados a ese grupo perderán todos los privilegios de acceso al Gestor de cuadrícula, a menos que un grupo diferente les conceda privilegios.

### Pasos

1. Seleccione **Configuración > Control de acceso > grupos de administración**.
2. Seleccione el nombre del grupo.

Si el sistema incluye más de 20 elementos, puede especificar cuántas filas se muestran en cada página a la vez. A continuación, puede utilizar la función de búsqueda de su navegador para buscar un elemento específico en las filas mostradas actualmente.

3. Seleccione **Quitar**.
4. Seleccione **OK**.

## Gestión de usuarios locales

Puede crear usuarios locales y asignarles grupos de administración locales para determinar a qué funciones de Grid Manager pueden acceder estos usuarios.

Grid Manager incluye un usuario local predefinido denominado «'root'». Aunque puede agregar y quitar usuarios locales, no puede quitar el usuario raíz.



Si se ha habilitado el inicio de sesión único (SSO), los usuarios locales no podrán iniciar sesión en StorageGRID.

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

### Creando un usuario local

Si creó grupos de administración locales, puede crear uno o más usuarios locales y asignar cada usuario a uno o más grupos. Los permisos del grupo controlan a qué funciones de Grid Manager puede acceder el usuario.

### Acerca de esta tarea

Solo es posible crear usuarios locales, y solo es posible asignar estos usuarios a grupos de administración locales. Los usuarios federados y los grupos federados se gestionan usando el origen de identidades externo.

### Pasos

1. Seleccione **Configuración > Control de acceso > usuarios de administración**.
2. Haga clic en **Crear**.
3. Introduzca el nombre para mostrar, el nombre exclusivo y la contraseña del usuario.
4. Asigne el usuario a uno o varios grupos que rijan los permisos de acceso.

La lista de nombres de grupo se genera a partir de la tabla grupos.

5. Haga clic en **Guardar**.

### Información relacionada

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

## Modificar una cuenta de usuario local

Puede modificar la cuenta de un usuario administrador local para actualizar el nombre para mostrar del usuario o la pertenencia a grupos. También es posible impedir temporalmente que un usuario acceda al sistema.

### Acerca de esta tarea

Solo puede editar usuarios locales. Los detalles de usuario federado se sincronizan automáticamente con el origen de identidad externo.

### Pasos

1. Seleccione **Configuración > Control de acceso > usuarios de administración**.
2. Seleccione el usuario que desea editar.

Si el sistema incluye más de 20 elementos, puede especificar cuántas filas se muestran en cada página a la vez. A continuación, puede utilizar la función de búsqueda de su navegador para buscar un elemento específico en las filas mostradas actualmente.

3. Haga clic en **Editar**.
4. Si lo desea, puede realizar cambios en el nombre o la pertenencia al grupo.
5. Opcionalmente, para evitar que el usuario acceda temporalmente al sistema, marque **Denegar acceso**.
6. Haga clic en **Guardar**.

La nueva configuración se aplica la próxima vez que el usuario cierre sesión y vuelva a acceder al Gestor de cuadrícula.

## Eliminar una cuenta de usuario local

Puede eliminar cuentas de usuarios locales que ya no requieran acceso a Grid Manager.

### Pasos

1. Seleccione **Configuración > Control de acceso > usuarios de administración**.
2. Seleccione el usuario local que desea eliminar.



No se puede eliminar el usuario local raíz predefinido.

Si el sistema incluye más de 20 elementos, puede especificar cuántas filas se muestran en cada página a la vez. A continuación, puede utilizar la función de búsqueda de su navegador para buscar un elemento específico en las filas mostradas actualmente.

3. Haga clic en **Quitar**.
4. Haga clic en **Aceptar**.

## Cambiar la contraseña de un usuario local

Los usuarios locales pueden cambiar sus propias contraseñas mediante la opción **Cambiar contraseña** del banner de Grid Manager. Además, los usuarios que tienen acceso a la página Admin Users pueden cambiar las contraseñas de otros usuarios locales.

### Acerca de esta tarea

Solo es posible cambiar contraseñas para usuarios locales. Los usuarios federados deben cambiar sus propias contraseñas en el origen de identidades externo.

### Pasos

1. Seleccione **Configuración > Control de acceso > usuarios de administración**.
2. En la página Users, seleccione el usuario.

Si el sistema incluye más de 20 elementos, puede especificar cuántas filas se muestran en cada página a la vez. A continuación, puede utilizar la función de búsqueda de su navegador para buscar un elemento específico en las filas mostradas actualmente.

3. Haga clic en **Cambiar contraseña**.
4. Introduzca y confirme la contraseña y haga clic en **Guardar**.

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

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

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

### Cómo funciona el inicio de sesión único

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

#### Inicio de sesión cuando SSO está habilitado

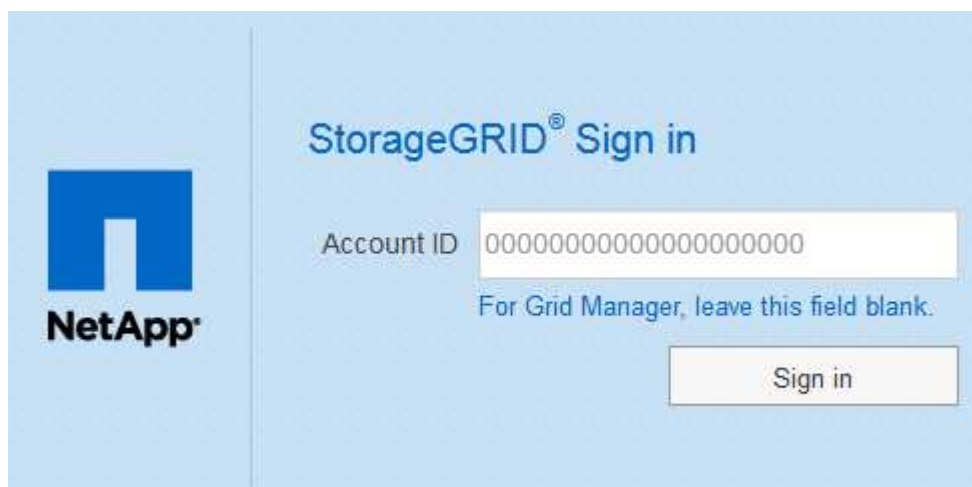
Cuando se habilita SSO y usted inicia sesión en StorageGRID, se le redirigirá a la página SSO de su organización para validar sus credenciales.

#### Pasos

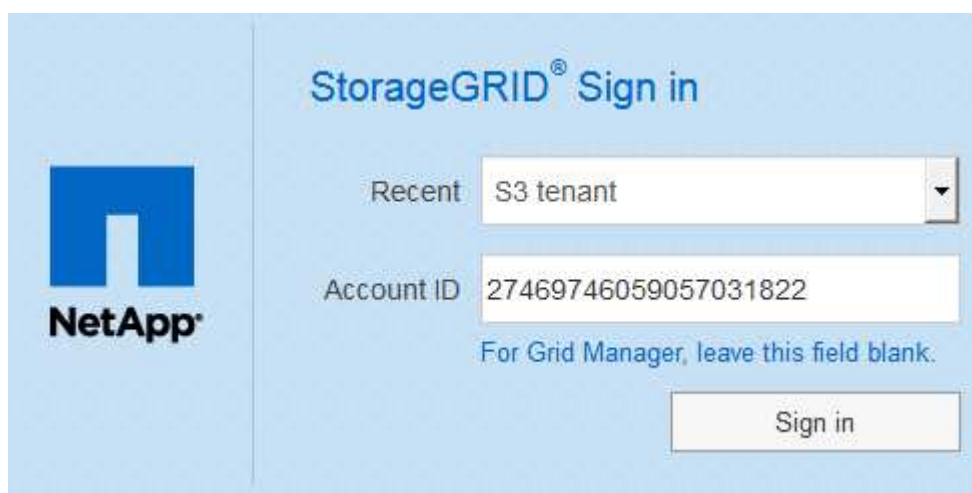
1. Introduzca el nombre de dominio o la dirección IP completos de cualquier nodo de administración de StorageGRID en un navegador web.

Aparece la página Inicio de sesión de StorageGRID.

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



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



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

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

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

## 3. Haga clic en **Iniciar sesión**

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

Sign in with your organizational account



[Sign in](#)

4. inicia sesión con sus credenciales de SSO.

Si sus credenciales de SSO son correctas:

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

### Cerrar sesión cuando SSO está habilitado

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

#### Pasos

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

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

Si ha iniciado sesión en...	Y salir de...	Se ha cerrado sesión en...
Grid Manager en uno o varios nodos de administrador	Grid Manager en cualquier nodo de administrador	Grid Manager en todos los nodos de administración
Administrador de inquilinos en uno o varios nodos de administrador	Inquilino Manager en cualquier nodo de administrador	Administrador de inquilinos en todos los nodos de administrador

Si ha iniciado sesión en...	Y salir de...	Se ha cerrado sesión en...
Tanto Grid Manager como Inquilino Manager	Administrador de grid	Sólo Grid Manager. También debe cerrar sesión en el Administrador de inquilinos para cerrar la sesión de SSO.



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

## Requisitos para usar el inicio de sesión único

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



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

## Requisitos del proveedor de identidades

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

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



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

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

## Requisitos de certificado de servidor

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

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





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

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

#### Información relacionada

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

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

## Configuración del inicio de sesión único

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

- ["Confirmación de que los usuarios federados pueden iniciar sesión"](#)
- ["Uso del modo de recinto de seguridad"](#)
- ["Creación de confianzas de parte de confianza en AD FS"](#)
- ["Prueba de fideicomisos de la parte de confianza"](#)
- ["Habilitar el inicio de sesión único"](#)
- ["Desactivar el inicio de sesión único"](#)
- ["Desactive y vuelva a habilitar temporalmente el inicio de sesión único para un nodo de administración"](#)

#### Confirmación de que los usuarios federados pueden iniciar sesión

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

#### Lo que necesitará

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

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

#### Pasos

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

identidad.



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

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

**Edit Tenant Account**

**Tenant Details**

Display Name

**Uses Own Identity Source**

Allow Platform Services

Storage Quota (optional)

Aparece la página Cuentas de arrendatario.

- a. Seleccione la cuenta de arrendatario, haga clic en **Iniciar sesión** e inicie sesión en la cuenta de arrendatario como usuario raíz local.
- b. En el Administrador de arrendatarios, haga clic en **Control de acceso > grupos**.

- c. Asegúrese de que al menos un grupo federado de Grid Manager ha sido asignado el permiso acceso raíz para este arrendatario.
- d. Cierre la sesión.
- e. Confirme que puede volver a iniciar sesión en el inquilino como usuario en el grupo federado.

### Información relacionada

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

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

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

### Uso del modo de recinto de seguridad

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

### Lo que necesitará

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

### Acerca de esta tarea

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

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

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



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

### Pasos

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

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

## Single Sign-on

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

SSO Status    Disabled    Sandbox Mode    Enabled

Save



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

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

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

### 3. En la sección Proveedor de identidades:

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



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

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

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

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

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

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

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

## 5. Haga clic en **Guardar**.

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



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

### Single Sign-on

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

SSO Status    Disabled    Sandbox Mode    Enabled

#### Sandbox mode

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

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

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

### Información relacionada

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

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

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

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

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

#### Lo que necesitará

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



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

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

### Acerca de esta tarea

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

### Pasos

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

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

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

3. En Windows Server Manager, seleccione **Herramientas > Administración de AD FS**.

Aparece la herramienta de administración de AD FS.

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

Aparece la lista de confianzas de parte de confianza.

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

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

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

- a. Busque la parte de confianza que acaba de crear.
- b. Haga clic con el botón derecho del ratón en la confianza y seleccione **Editar política de emisión de reclamaciones**.
- c. Haga clic en **Agregar regla**.

- d. En la página Seleccionar plantilla de regla, seleccione **Enviar atributos LDAP como reclamaciones** en la lista y haga clic en **Siguiente**.
- e. En la página Configurar regla, introduzca un nombre para mostrar para esta regla.  
  
Por ejemplo, **ObjectGUID to Name ID**.
- f. Para el almacén de atributos, seleccione **Active Directory**.
- g. En la columna atributo LDAP de la tabla Mapping, escriba **objectGUID**.
- h. En la columna Tipo de reclamación saliente de la tabla asignación, seleccione **ID de nombre** en la lista desplegable.
- i. Haga clic en **Finalizar** y haga clic en **Aceptar**.

7. Confirme que los metadatos se han importado correctamente.

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

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

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

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

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

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

#### Lo que necesitará

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



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

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

#### Acerca de esta tarea

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

#### Pasos

1. En Windows Server Manager, haga clic en **Herramientas** y, a continuación, seleccione **Administración de AD FS**.



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

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

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

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



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

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

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

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

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

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

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



## Crear una confianza de parte de confianza manualmente

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

### Lo que necesitará

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



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

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

### Acerca de esta tarea

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

### Pasos

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

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

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

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

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

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

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

*Admin\_Node\_Identifier*

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

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

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



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

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

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

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

- a. Agregue el certificado personalizado:

- Si posee el certificado de gestión personalizado cargado en StorageGRID, seleccione ese certificado.

- Si no tiene el certificado personalizado, inicie sesión en el nodo de administrador, vaya al `/var/local/mgmt-api` directorio del nodo Admin y añada el `custom-server.crt` archivo de certificado.

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

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

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

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

### Prueba de fideicomisos de la parte de confianza

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

#### Lo que necesitará

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

#### Pasos

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

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

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

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

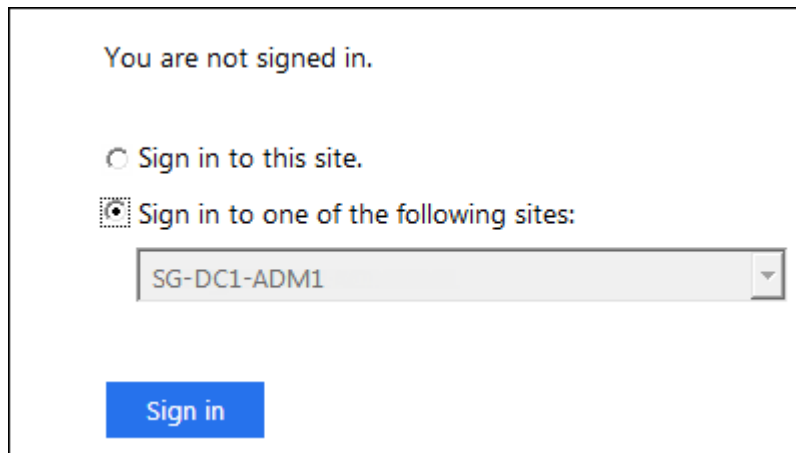
## Sandbox mode

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

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

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

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



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

5. Introduzca el nombre de usuario y la contraseña federados.
  - Si las operaciones de inicio de sesión y cierre de sesión SSO se realizan correctamente, se muestra un mensaje de éxito.

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

- Si la operación de SSO se realiza sin errores, se muestra un mensaje de error. Solucione el problema, borre las cookies del navegador e inténtelo de nuevo.
6. Repita los pasos anteriores para confirmar que puede iniciar sesión en cualquier otro nodo de administrador.

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

## Habilitar el inicio de sesión único

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

### Lo que necesitará

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

### Pasos

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

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

2. Cambie el estado de SSO a **habilitado**.
3. Haga clic en **Guardar**.

Aparecerá un mensaje de advertencia.

### Warning

#### Enable single sign-on

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

Before proceeding, confirm the following:

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

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

Cancel

OK

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

El inicio de sesión único ahora está activado.



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

## Desactivar el inicio de sesión único

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

### Lo que necesitará

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

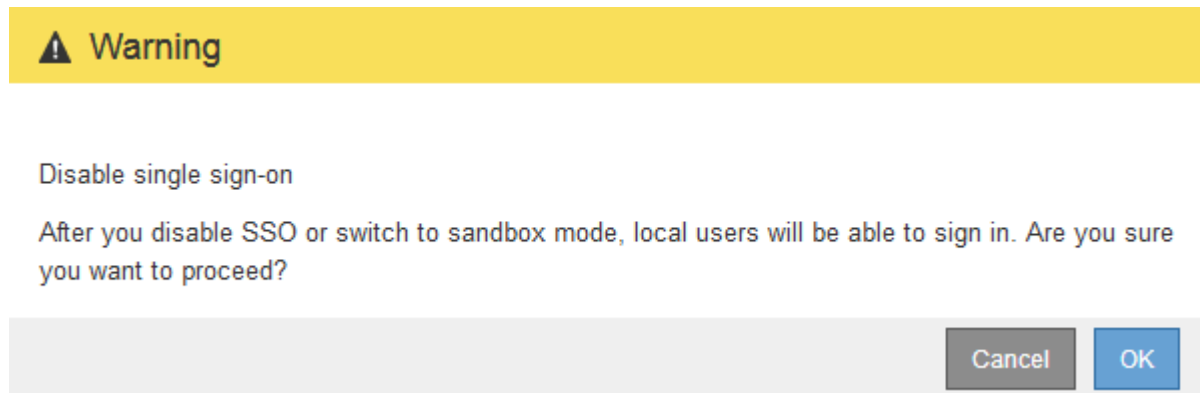
### Pasos

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

Aparece la página Single Sign-On.

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

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



4. Haga clic en **Aceptar**.

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

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

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

### Lo que necesitará

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

## Acerca de esta tarea

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



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

## Pasos

1. Inicie sesión en un nodo de administrador:

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

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

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

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

3. Confirme que desea deshabilitar SSO.

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

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

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

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

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

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

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

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

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

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

Confirme que desea habilitar SSO.

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

◦ Reinicie el nodo de cuadrícula: `reboot`

8. Desde un explorador web, acceda a Grid Manager desde el mismo nodo de administración.
9. Confirme que aparece la página de inicio de sesión de StorageGRID y que debe introducir sus credenciales de SSO para acceder a Grid Manager.

#### Información relacionada

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

## Configurar certificados de cliente de administrador

Puede utilizar certificados de cliente para permitir que clientes externos autorizados accedan a la base de datos Prometheus de StorageGRID. Los certificados de cliente proporcionan una forma segura de utilizar herramientas externas para supervisar StorageGRID.

Si necesita acceder a StorageGRID mediante una herramienta de supervisión externa, debe cargar o generar un certificado de cliente mediante el Gestor de cuadrícula y copiar la información de certificado a la herramienta externa.

### Añadiendo certificados de cliente de administrador

Para agregar un certificado de cliente, puede proporcionar su propio certificado o generar uno mediante el Gestor de cuadrícula.

#### Lo que necesitará

- Debe tener el permiso acceso raíz.
- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe conocer la dirección IP o el nombre de dominio del nodo de administrador.
- Debe haber configurado el certificado de servidor de interfaz de gestión de StorageGRID y tener el bundle de CA correspondiente
- Si desea cargar su propio certificado, la clave pública y la clave privada del certificado deben estar disponibles en el equipo local.

#### Pasos

1. En Grid Manager, seleccione **Configuración > Control de acceso > certificados de cliente**.

Aparece la página certificados de cliente.



## Client Certificates

You can upload or generate one or more client certificates to allow StorageGRID to authenticate external client access.

<a href="#">+ Add</a>	<a href="#">✎ Edit</a>	<a href="#">✕ Remove</a>
Name	Allow Prometheus	Expiration Date
No client certificates configured.		

### 2. Seleccione **Agregar**.

Aparece la página cargar certificado.

### Upload Certificate

Name

Allow Prometheus

---

#### Certificate Details

Upload the public key for the client certificate.

### 3. Escriba un nombre entre 1 y 32 caracteres para el certificado.

### 4. Para acceder a las métricas de Prometheus mediante la herramienta de supervisión externa, active la casilla de verificación **permitir Prometheus**.

### 5. Cargar o generar un certificado:

- a. Para cargar un certificado, vaya [aquí](#).
- b. Para generar un certificado, vaya [aquí](#).

### 6. para cargar un certificado:

- a. Seleccione **cargar certificado de cliente**.
- b. Busque la clave pública del certificado.

Después de cargar la clave pública para el certificado, se rellenan los campos **metadatos de certificado** y **PEM de certificado**.

## Upload Certificate

Name  test-certificate-upload

Allow Prometheus 

### Certificate Details

Upload the public key for the client certificate.

Upload Client Certificate

Generate Client Certificate

Uploaded file name: client (1).crt

Certificate metadata 

```
Subject DN: /C=US/ST=California/L=Sunnyvale/O=Example Co./OU=IT/CN=*.s3.example.com
Serial Number: 0D:0E:FC:16:75:B8:BE:3E:7D:47:4D:05:49:08:F3:7B:E8:4A:71:90
Issuer DN: /C=US/ST=California/L=Sunnyvale/O=Example Co./OU=IT/CN=*.s3.example.com
Issued On: 2020-06-19T22:11:56.000Z
Expires On: 2021-06-19T22:11:56.000Z
SHA-1 Fingerprint: 13:AA:D6:06:2B:90:FE:B7:7B:EB:1A:83:BE:C3:62:39:B7:A6:E7:F0
SHA-256 Fingerprint: 5C:29:06:6B:CF:81:50:B8:4F:A9:56:F7:A7:AB:3C:36:FA:3D:B7:32:A4:C9:74:85:2C:8D:E6:67:37:C3:AC:60
```

Certificate PEM 

```
-----BEGIN CERTIFICATE-----
MIIDmzCCAoOgAwIBAgIUdQ78FnW4vj59R00FSQjze+hKcZAwDQYJKoZIhvcNAQEL
BQAwDELMAkGA1UEBhMCVVMxZzARBgNVBAgMCkNhbnG1mb3JuaWEuXzAQBgNVBAcM
CVN1bm55dmFsZTEUMBIGA1UECgwLRXhhbXBsZSBDbj4xCzAJBgNVBAsMAk1UMRkw
FwYDQDDDBAqLnMzLmV4YW1wbGUuY29tMB4XDTEwMDYxOTIyMTE1oXDTIxMDYx
OTIyMTE1LowdDELMAkGA1UEBhMCVVMxZzARBgNVBAgMCkNhbnG1mb3JuaWEuXzAQBg
NVBAcMCVN1bm55dmFsZTEUMBIGA1UECgwLRXhhbXBsZSBDbj4xCzAJBgNVBAsMAk1UMRkw
FwYDQDDDBAqLnMzLmV4YW1wbGUuY29tMIIIBIjANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEAzVqq2MnjvVotLeStq1Co4coJmsQ2ygRhuwSza0bgMnjf
cWUgHNVPXGuGlzY/Tl37r3Dk5bu2fyGYAeJ6mqbQA6cE3yp0p5Hx7Cm/AWJknFw6
```


Copy certificate to clipboard


Cancel Save

- a. Seleccione **Copiar certificado en el portapapeles** y pegue el certificado en la herramienta de supervisión externa.
  - b. Utilice una herramienta de edición para copiar y pegar la clave privada en su herramienta de supervisión externa.
  - c. Seleccione **Guardar** para guardar el certificado en Grid Manager.
7. para generar un certificado:
- a. Seleccione **generar certificado de cliente**.
  - b. Introduzca el nombre de dominio o la dirección IP del nodo de administración.
  - c. Opcionalmente, introduzca un asunto X.509, también denominado Nombre distintivo (DN), para identificar al administrador que posee el certificado.
  - d. De manera opcional, seleccione el número de días en los que el certificado es válido. El valor predeterminado es 730 días.
  - e. Seleccione **generar**.

Se rellenan los campos **metadatos de certificado**, **PEM de certificado** y **clave privada de certificado**.

## Upload Certificate

Name  test-certificate-generate

Allow Prometheus 

### Certificate Details

Upload the public key for the client certificate.

Upload Client Certificate

Generate Client Certificate

Certificate metadata 

```
Subject DN: /CN=test.com
Serial Number: 08:F8:FB:76:B2:13:E4:DF:54:83:3D:35:56:0F:2A:03:53:B0:E2:0
A
Issuer DN: /CN=test.com
Issued On: 2020-11-20T22:44:46.000Z
Expires On: 2022-11-20T22:44:46.000Z
SHA-1 Fingerprint: 6E:DB:8C:F8:3E:20:88:E4:C6:42:52:5F:32:7E:E7:93:66:89:F3:3
D
SHA-256 Fingerprint: 73:D3:51:83:ED:D3:89:AD:7B:89:4C:AF:AE:34:76:B6:42:FE:0D:
EF:78:C0:A4:66:C2:EB:65:64:C3:D4:7A:B0
```

Certificate PEM 


```
-----BEGIN CERTIFICATE-----
MIICyzCCAbOgAwIBAgIUUCFj7dxITSN9Ugs01Vm8qA1Ow4gowDQYJKoZIhvcNAQEL
BQAwEwERMA8GA1UEAwIgdGVudC5jb20wHhcNMjA1MTIwMjI0NDQ2WWhcMTIw
MjI0NDQ2WjATMREwDwYDVQQDDAh0ZXN0LmNvbTCCASAwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAR02dS9mx2jFrGuBb22Mjcidf/tTcKxLtB9m+4vIwt1gvrR
XgHZ31B9YIqn/Vo729R2mNKKyBwkyQTkGCO2Ixvv0STBLEIWFb8sTgcIcMyt1V1F
OseBWy402xxjnR3/X+AX+6s2WZIsVe+3CDjGu4ie0V/uVQxx4yA1T9SoKnjBmOa
LCVjL6iVnkUGB8GbkYUPeOaoMjsL6TN1QsoFv9VEB0xBKCP4D7FDbaIy2f9Ng8rS
FEOQoLN=NxCasLO4D7j2qFqOVUpFJ3M0ohlx0n5pQ78Z5KEYwV=DKg6v52P8UBM
1o6GeuoFaW+dbpLZKp09N1V=FlghXe9AxxN8s+kCAwEAAAMXMBUwEwYDVR0RBAAw
```

Copy certificate to clipboard

Certificate private key 

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEAR20H2bHaM+sa4Fv2kyNyJ1/+1NwzEu0Eab7i8jC2KNC/BFe
AdneUH1ghCf9Wjvb1HaY0oxIHCTJBOQYI5kjG+/RjMEb4h29sKxOBwiczK2VWUU7
OwF2jPg7bPGoOrf9f4Bf7xN1ZkixV75IICMa7iJaRX+5VDPHjIDVP1KggelMGYSos
JWMvqJWeRQYFI2uTJQ946qgyOwvpm2VDOgW/1UQHTEEoKngPfeUNtojL2/02DmtJ8
Q8Cg=202xoxJrMe7gFuNmoWo5hS8kUncw6iHXHSfmlDvxnkp9jBWMqDm/nY/xQEwW
jw266h9pb51ukt2k703VW0WGCfD7GDPE2yyQIDAQABoIBAQCfEUfY4pE0Hqcv
2uEL6De4yXMTwg/3Gn+W8mvdgQB4xWEGQrk1kEUG+HTYrFJen6XX0vACDYAC/
Hh1Q67xDVpwrjdpuK0ctr1W8ervsEmpBx99MqH9Y2UGx6Yub3UBJaqfDvja4Nvaon
MxaYJRFBLvAR7f2z2xXVY3b0zRPA+rnoYCs1Lct5Y0K73e0G8naTmwIdm2YM6EE
```

Copy private key to clipboard

 You will not be able to view the certificate private key after you close this dialog. To save the keys for future reference, copy and paste the values to another location.

Cancel

Save

- Seleccione **Copiar certificado en el portapapeles** y pegue el certificado en la herramienta de supervisión externa.
- Seleccione **Copiar clave privada en el portapapeles** y pegue la clave en su herramienta de monitorización externa.

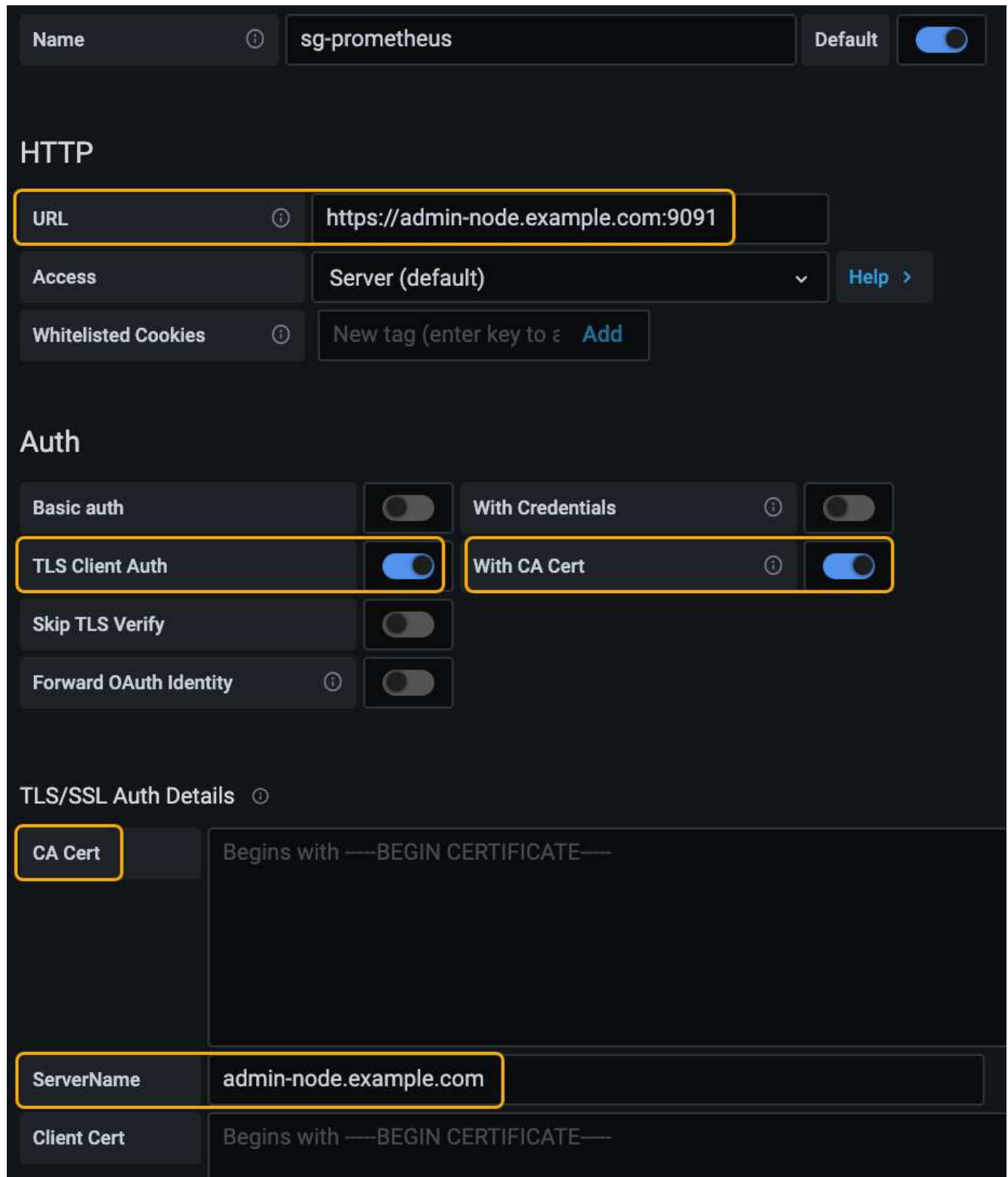


No podrá ver la clave privada después de cerrar el cuadro de diálogo. Copie la llave en una ubicación segura.

- Seleccione **Guardar** para guardar el certificado en Grid Manager.

8. Configure los siguientes ajustes en su herramienta de supervisión externa, como Grafana.

En la siguiente captura de pantalla se muestra un ejemplo de Grafana:



a. **Nombre:** Escriba un nombre para la conexión.

StorageGRID no requiere esta información, pero se debe proporcionar un nombre para probar la conexión.

- b. **URL:** Introduzca el nombre de dominio o la dirección IP del nodo de administración. Especifique HTTPS y el puerto 9091.

Por ejemplo: `https://admin-node.example.com:9091`

- c. Activar **autorización de cliente TLS y con CA Cert**.
- d. Copie y pegue el certificado de servidor de interfaz de administración o el paquete de CA en **CA Cert** en Detalles de autenticación TLS/SSL.
- e. **ServerName:** Introduzca el nombre de dominio del nodo Admin.

Servername debe coincidir con el nombre de dominio tal y como aparece en el certificado de servidor de la interfaz de gestión.

- f. Guarde y pruebe el certificado y la clave privada que copió desde StorageGRID o un archivo local.

Ahora puede acceder a la métrica Prometheus desde StorageGRID con su herramienta de supervisión externa.

Para obtener información acerca de las métricas, consulte las instrucciones para supervisar y solucionar problemas de StorageGRID.

## Información relacionada

["Usar certificados de seguridad StorageGRID"](#)

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

["Solución de problemas de monitor"](#)

## Editar certificados de cliente de administrador

Un certificado se puede editar para cambiar su nombre, habilitar o deshabilitar el acceso a Prometheus, o cargar un nuevo certificado cuando el actual haya caducado.

### Lo que necesitará

- Debe tener el permiso acceso raíz.
- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe conocer la dirección IP o el nombre de dominio del nodo de administrador.
- Si desea cargar un nuevo certificado y una clave privada, deben estar disponibles en el equipo local.

### Pasos

1. Seleccione **Configuración > Control de acceso > certificados de cliente**.

Aparece la página certificados de cliente. Se muestra una lista de los certificados existentes.

Las fechas de vencimiento del certificado se muestran en la tabla. Si un certificado caducará pronto o ya ha caducado, aparecerá un mensaje en la tabla y se activará una alerta.

	Name	Allow Prometheus	Expiration Date
<input type="radio"/>	test-certificate-upload	✓	2021-06-19 16:11:56 MDT
<input checked="" type="radio"/>	test-certificate-generate	✓	2022-08-20 09:42:00 MDT

Displaying 2 certificates.

2. Seleccione el botón de opción situado a la izquierda del certificado que desea editar.
3. Seleccione **Editar**.

Se muestra el cuadro de diálogo Editar certificado.

### Edit Certificate test-certificate-generate

Name

Allow Prometheus

---

#### Certificate Details

Upload the public key for the client certificate.

Upload Client Certificate
Generate Client Certificate

Certificate metadata

**Subject DN:** /CN=test.com  
**Serial Number:** 0C:11:87:6C:1E:FD:13:16:F3:F2:06:D9:DA:6D:BC:CE:2A:A9:C3:53  
**Issuer DN:** /CN=test.com  
**Issued On:** 2020-11-23T15:53:33.000Z  
**Expires On:** 2022-11-23T15:53:33.000Z  
**SHA-1 Fingerprint:** AE:E6:70:A7:D3:C3:39:7A:09:F9:62:9B:81:8A:87:CD:43:16:89:A7  
**SHA-256 Fingerprint:** 63:07:BF:FF:08:1E:84:F1:D4:67:C6:16:B0:35:26:00:C6:A3:13:11:7E:5E:90:EC:7A:7B:EF:23:14:55:3D:56

Certificate PEM

```
-----BEGIN CERTIFICATE-----
MIICyzCCAbOgAwIBAgIUDBGHbB79Exbz8gbZ2m28ziqpw1MwDQYJKoZIhvcNAQEL
BQAwEzERMA8GA1UEAwIdGVzdC5jb20wHhcNMjAxMTIzMTU1MzE1LjE1LjE1LjE1
MTU1MzE1LjE1MREwDwYDVQQDDAh0ZXN0LmNvbVtCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBBAKdGEeneCDFsLjvLnX9ow6oPrdU7m2EN6SS6xdVI155sCH+
hkwO5a2Mym7EhbNrfwOt2nMjQkcaKIrK8OAmutRgG6N1N12FIW0qYQuzFQ0QddLq
n7ymFw6w8a9zYSu7Lp84Yn0/LSDPk+h3Jio7Mrt2X70It52DRwFmbLNvEvYEtTS
h+FbNh885AIRO2eLxvC0IRij1bySe76wK+Wmc97HdxRSgyxIWk6BD47XC+d0rv55
wvtjc/41qc5xsE6Xm7s2yJg4VARx10y8Icwa9fz00+xPwIdC0NwXkpWJXeBnCoXx
YqQxbWzjz+iVLJqLTMxU8zTIT30zUgN00M82GJUCAwEAAaMKMBUwEwYDVR0RBAAw

```

Copy certificate to clipboard

Cancel Save

4. Realice los cambios que desee en el certificado.
5. Seleccione **Guardar** para guardar el certificado en Grid Manager.
6. Si cargó un nuevo certificado:
  - a. Seleccione **Copiar certificado en el portapapeles** para pegar el certificado en la herramienta de supervisión externa.
  - b. Utilice una herramienta de edición para copiar y pegar la nueva clave privada en su herramienta de supervisión externa.

c. Guarde y pruebe el certificado y la clave privada en la herramienta de supervisión externa.

7. Si generó un nuevo certificado:

a. Seleccione **Copiar certificado en el portapapeles** para pegar el certificado en la herramienta de supervisión externa.

b. Seleccione **Copiar clave privada en el portapapeles** para pegar el certificado en la herramienta de supervisión externa.



No podrá ver ni copiar la clave privada después de cerrar el cuadro de diálogo. Copie la llave en una ubicación segura.

c. Guarde y pruebe el certificado y la clave privada en la herramienta de supervisión externa.

## Quitar certificados de cliente de administrador

Si ya no necesita un certificado, es posible eliminarlo.

### Lo que necesitará

- Debe tener el permiso acceso raíz.
- Debe iniciar sesión en Grid Manager mediante un explorador compatible.

### Pasos

1. Seleccione **Configuración > Control de acceso > certificados de cliente**.

Aparece la página certificados de cliente. Se muestra una lista de los certificados existentes.

	Name	Allow Prometheus	Expiration Date
<input type="radio"/>	test-certificate-upload	✓	2021-06-19 16:11:56 MDT
<input checked="" type="radio"/>	test-certificate-generate	✓	2022-08-20 09:42:00 MDT

Displaying 2 certificates.

2. Seleccione el botón de opción situado a la izquierda del certificado que desea eliminar.

3. Seleccione **Quitar**.

Se muestra un cuadro de diálogo de confirmación.

**Warning**

Delete certificate

Are you sure you want to delete the certificate "test-certificate-generate"?

Cancel OK

4. Seleccione **OK**.

El certificado se eliminará.



## Información de copyright

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

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

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

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

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

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

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

## Información de la marca comercial

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