# Controlar el acceso a StorageGRID

StorageGRID software

NetApp
July 23, 2026

# Tabla de contenidos


Controlar el acceso a StorageGRID . . . 1
Controlar el acceso a StorageGRID . . . 1
Controla el acceso al Grid Manager . . . 1
Habilitar el inicio de sesión único . . . 1
Cambiar la contraseña de aprovisionamiento . . . 1
${post_edited_translations.segment} . . . 1
Cambia la contraseña de aprovisionamiento de StorageGRID . . . 2
Cambia las contraseñas de la consola de nodo en StorageGRID . . . 3
Accede al asistente . . . 3
Descargar el paquete de recuperación actual . . . 3
Proporciona nuevas contraseñas . . . 4
Finaliza el cambio de contraseña . . . 4
Cambia las contraseñas de acceso SSH para StorageGRID Admin Nodes . . . 5
Accede al asistente . . . 6
Descargar el paquete de recuperación actual . . . 6
Cambiar las claves de acceso SSH . . . 6
Usa la federación de identidades en StorageGRID . . . 7
Configura la federación de identidades para Grid Manager . . . 7
Forzar la sincronización con la fuente de identidad . . . 11
${post_edited_translations.segment} . . . 11
Guía para configurar un servidor OpenLDAP . . . 12
Administra grupos de administración en StorageGRID . . . 12
Crear un grupo de administradores . . . 13
${post_edited_translations.segment} . . . 14
Duplicar un grupo . . . 15
Borrar un grupo . . . 15
Permisos del grupo Admin en StorageGRID . . . 15
${post_edited_translations.segment} . . . 16
Acceso a raíz . . . 16
${post_edited_translations.segment} . . . 16
ILM . . . 16
${post_edited_translations.segment} . . . 16
Gestiona alertas . . . 17
Consulta de métricas . . . 17
Búsqueda de metadatos de objetos . . . 18
Otra configuración de grid . . . 18
${post_edited_translations.segment} . . . 18
${post_edited_translations.segment} . . . 18
Administra usuarios en StorageGRID . . . 18
${post_edited_translations.segment} . . . 18
${post_edited_translations.segment} . . . 19
Importar usuarios federados . . . 20
Duplicar un usuario . . . 21

Eliminar un usuario . . . 21
Utiliza el inicio de sesión único (SSO) . . . 21
Conoce StorageGRID SSO . . . 21
Requisitos y consideraciones para StorageGRID SSO . . . 23
Comprueba que los usuarios federados puedan iniciar sesión en StorageGRID . . . 25
Configura el inicio de sesión único en StorageGRID . . . 26
Crea confianzas de terceros en AD FS para StorageGRID . . . 33
Crea aplicaciones empresariales en Entra ID para StorageGRID . . . 38
Crea conexiones de proveedores de servicios en PingFederate para StorageGRID . . . 40
Desactiva el inicio de sesión único en StorageGRID . . . 44
Deshabilita temporalmente y vuelve a habilitar SSO para un nodo de administración StorageGRID . . . 45

# Controlar el acceso a StorageGRID

## Controlar el acceso a StorageGRID

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

### Controla el acceso al Grid Manager

Tú determinas quién puede acceder a Grid Manager y a la API de gestión de la red importando grupos y usuarios desde un servicio de federación de identidades o configurando grupos y usuarios locales.

Usar "federación de identidades" hace que configurar "grupos" y "${post_edited_translations.segment}" sea más rápido, y permite que los usuarios inicien sesión en StorageGRID con sus credenciales habituales. Puedes configurar la federación de identidades si usas Active Directory, OpenLDAP u Oracle Directory Server.

> Ponte en contacto con el soporte técnico si deseas utilizar otro servicio LDAP v3.

Determinas qué tareas puede realizar cada usuario asignando diferentes "permisos" a cada grupo. Por ejemplo, es posible que quieras que los usuarios de un grupo puedan gestionar las reglas de ILM y que los usuarios de otro grupo realicen tareas de mantenimiento. Un usuario debe pertenecer al menos a un grupo para acceder al sistema.

Opcionalmente, puedes configurar un grupo para que sea de solo lectura. Los usuarios de un grupo de solo lectura solo pueden ver la configuración y las funciones. No pueden realizar ningún cambio ni llevar a cabo ninguna operación en el Grid Manager o en la Grid Management API.

### Habilitar el inicio de sesión único

El sistema StorageGRID admite el inicio de sesión único (SSO) mediante el estándar Security Assertion Markup Language 2.0 (SAML 2.0). Después de que "${post_edited_translations.segment}", todos los usuarios deben autenticarse mediante un proveedor de identidad externo antes de poder acceder al Grid Manager, al Tenant Manager, a la API de Grid Management o a la API de Tenant Management. Los usuarios locales no pueden iniciar sesión en StorageGRID.

### Cambiar la contraseña de aprovisionamiento

La frase de contraseña de aprovisionamiento es necesaria para muchos procedimientos de instalación y mantenimiento, y para descargar el paquete de recuperación de StorageGRID. La frase de contraseña también es necesaria para descargar copias de seguridad de la información de topología del grid y las claves de cifrado para el sistema StorageGRID. Puedes "cambiar la contraseña" según sea necesario.

### ${post_edited_translations.segment}

Cada nodo de tu grid tiene una contraseña de consola de nodo, que necesitas para iniciar sesión en el nodo como "admin" usando SSH, o como usuario raíz en una conexión de consola de VM/física. Si lo necesitas, puedes "cambiar la contraseña de la consola del nodo" para cada nodo.

# Cambia la contraseña de aprovisionamiento de StorageGRID

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

**Antes de empezar**

- Has iniciado sesión en Grid Manager mediante un "navegador web compatible".
- ${post_edited_translations.segment}
- Tienes la contraseña de aprovisionamiento actual.

**Acerca de esta tarea**

La frase de contraseña de aprovisionamiento es necesaria para muchos procedimientos de instalación y mantenimiento, y para "descargar el paquete de recuperación". La frase de contraseña de aprovisionamiento no aparece en el archivo `Passwords.txt`. Asegúrate de documentar la frase de contraseña de aprovisionamiento y de guardarla en un lugar seguro.

**Pasos**

1. Selecciona **Configuración** > **Control de acceso** > **Contraseñas de grid**.
2. ${post_edited_translations.segment}
3. Introduce tu contraseña de aprovisionamiento actual.
4. Introduce la nueva frase de contraseña. La frase de contraseña debe contener al menos 8 y no más de 32 caracteres. Las frases de contraseña distinguen mayúsculas de minúsculas.

   Guarda la frase de contraseña de aprovisionamiento en un lugar seguro. Es necesaria para los procedimientos de instalación, ampliación y mantenimiento.

5. ${post_edited_translations.segment}

   ${post_edited_translations.segment}

6. Selecciona **Paquete de recuperación**.
7. Introduce la nueva frase de contraseña de aprovisionamiento para descargar el nuevo paquete de recuperación.

   Tras cambiar la contraseña de aprovisionamiento, debes descargar inmediatamente un nuevo paquete de recuperación. El archivo del paquete de recuperación te permite restaurar el sistema en caso de que se produzca un fallo.

# Cambia las contraseñas de la consola de nodo en StorageGRID

Cada nodo de tu grid tiene una contraseña de consola de nodo, que usas para iniciar sesión en el nodo. Por defecto, cada nodo tiene una contraseña única. Puedes cambiar cada contraseña por una nueva contraseña única, o puedes cambiar la contraseña de todos los nodos para usar una contraseña global. Las contraseñas se almacenan en el paquete de recuperación.

**Antes de empezar**

- Has iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tienes el "Permiso de mantenimiento o acceso de usuario raíz".
- Tienes la contraseña de aprovisionamiento actual.

**Acerca de esta tarea**

Usas una contraseña de la consola del nodo para iniciar sesión en un nodo como "admin" usando SSH, o como usuario raíz en una conexión de consola de una máquina virtual o física. Puedes cambiar las contraseñas de la consola del nodo usando una de estas opciones:

- Aplicar automáticamente contraseñas aleatorias a cada nodo
- Especifica y aplica una contraseña global a todos los nodos
- Especifica y aplica una contraseña única a uno o varios nodos

Las contraseñas se almacenan en un archivo actualizado `Passwords.txt` que se encuentra en el paquete de recuperación. Las contraseñas aparecen en la columna Password del archivo.

> El "Contraseñas de acceso SSH" de las claves SSH utilizadas para la comunicación entre nodos es independiente de las contraseñas de la consola de los nodos. Este procedimiento no cambia las contraseñas de acceso SSH.

## Accede al asistente

**Pasos**

1. Selecciona **Configuración** > **Control de acceso** > **Contraseñas de grid**.
2. En **Cambiar contraseñas de la consola del nodo**, selecciona **Realizar un cambio**.

## Descargar el paquete de recuperación actual

Antes de cambiar las contraseñas de la consola de los nodos, descarga el paquete de recuperación actual. Puedes utilizar las contraseñas de este archivo si el proceso de cambio de contraseña falla en algún nodo.

**Pasos**

1. Introduce la frase de contraseña de aprovisionamiento de tu grid.
2. Selecciona **Descargar paquete de recuperación**.
3. Copia el archivo del paquete de recuperación (`.zip` en dos ubicaciones seguras y distintas.

El archivo del paquete de recuperación debe protegerse porque contiene claves de cifrado y contraseñas que pueden usarse para obtener datos del sistema StorageGRID.

4. Selecciona **Continuar**.

## Proporciona nuevas contraseñas

1. Selecciona el método de cambio de contraseña que quieras utilizar.
   - **Automático**: StorageGRID asigna automáticamente una nueva contraseña aleatoria de consola a todos los nodos.
   - **Personalizado**: Tú proporcionas las contraseñas de la consola.

**Automático**

1. Selecciona **Continuar**.

**Personalizado**

1. Selecciona una de las siguientes:
   - **Contraseña global de la consola**: aplica la misma contraseña de la consola a todos los nodos.
   - **Contraseñas únicas de consola**: Establece una contraseña diferente en uno o varios nodos.
2. Si has seleccionado **Contraseña global de la consola**, introduce la contraseña que quieras usar para todos los nodos.
3. Si has seleccionado **Contraseñas únicas de consola**, introduce una contraseña única para uno o más nodos.
4. Selecciona **Continuar**.

## Finaliza el cambio de contraseña

1. Cuando aparezca el cuadro de diálogo de confirmación, selecciona **Sí** si estás listo para que StorageGRID comience a cambiar las contraseñas de la consola de los nodos.

   No puedes cancelar este proceso después de que comienza.

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

2. Cuando el nuevo paquete de recuperación esté listo, selecciona **Descargar nuevo paquete de recuperación** y guarda el paquete de recuperación.
3. Abre el archivo `.zip`.
4. Comprueba que puedes acceder a los contenidos, incluido el archivo `Passwords.txt`, que contiene las nuevas contraseñas de la consola de nodo.
5. Copia el nuevo archivo del paquete de recuperación (`.zip` en dos ubicaciones seguras y distintas.

   No sobrescribas el paquete de recuperación anterior.

   Debes proteger el archivo de recuperación, porque contiene claves de cifrado y contraseñas que pueden usarse para obtener datos del sistema StorageGRID.

6. Marca la casilla de verificación para indicar que has descargado el nuevo paquete de recuperación y has verificado el contenido.
7. Selecciona **Continuar**.

   StorageGRID actualiza la contraseña de cada nodo.

   Si se produce un error durante el proceso de actualización, la barra de progreso muestra el número de nodos en los que no se pudo cambiar la contraseña. El sistema volverá a intentar automáticamente el proceso en cualquier nodo en el que no se pudo cambiar la contraseña. Si el proceso termina y todavía hay algunos nodos en los que no se cambió la contraseña, aparece el botón **Reintentar**.

8. Si la actualización de la contraseña falló en uno o varios nodos:
   a. Revisa los mensajes de error que aparecen en la tabla.
   b. Resuelve los problemas.
   c. Selecciona **Reintentar**.

   > Al volver a intentarlo, solo se modifican las contraseñas de la consola de los nodos en los que falló el cambio de contraseña en intentos anteriores.

9. Cuando la barra de progreso indique que ya no quedan actualizaciones, selecciona **Finalizar**.
10. Una vez que se hayan cambiado las contraseñas de la consola de todos los nodos, elimina el el primer paquete de recuperación que descargaste.

# Cambia las contraseñas de acceso SSH para StorageGRID Admin Nodes

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

Utiliza una clave SSH para iniciar sesión en un nodo como `admin` o como usuario raíz en una máquina virtual o mediante una conexión a la consola física.

**Antes de empezar**

- Has iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tienes el "Permiso de mantenimiento o acceso de usuario raíz".
- Tienes la contraseña de aprovisionamiento actual.

**Acerca de esta tarea**

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

Existen contraseñas de acceso SSH independientes para las claves SSH que se utilizan para la comunicación entre nodos. Este procedimiento no las modifica.

## Accede al asistente

**Pasos**

1. Selecciona **Configuración** > **Control de acceso** > **Contraseñas de grid**.
2. En **Cambiar claves SSH**, selecciona **Realizar un cambio**.

## Descargar el paquete de recuperación actual

Antes de cambiar las claves de acceso SSH, descarga el paquete de recuperación actual. Puedes utilizar las claves de este archivo si el proceso de cambio de claves falla en algún nodo.

**Pasos**

1. Introduce la frase de contraseña de aprovisionamiento de tu grid.
2. Selecciona **Descargar paquete de recuperación**.
3. Copia el archivo del paquete de recuperación (`.zip` en dos ubicaciones seguras y distintas.

   El archivo del paquete de recuperación debe protegerse porque contiene claves de cifrado y contraseñas que pueden usarse para obtener datos del sistema StorageGRID.

4. Selecciona **Continuar**.
5. Cuando aparezca el cuadro de diálogo de confirmación, selecciona **Sí** si estás listo para empezar a modificar las claves de acceso SSH.

   No puedes cancelar este proceso después de que comienza.

## Cambiar las claves de acceso SSH

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

**Pasos**

1. Espera a que se genere el nuevo paquete de recuperación, lo que puede tardar unos minutos.
2. Cuando el botón «Descargar nuevo paquete de recuperación» esté activo, selecciona **Descargar nuevo paquete de recuperación** y guarda el nuevo archivo del paquete de recuperación (`.zip` en dos ubicaciones seguras y separadas.
3. Cuando finalice la descarga:

   a. Abre el archivo `.zip`.

   b. Confirma que puedes acceder al contenido, incluido el archivo `Passwords.txt`, que contiene las nuevas claves de acceso SSH.

   c. Copia el nuevo archivo del paquete de recuperación (`.zip` en dos ubicaciones seguras y distintas.

      No sobrescribas el paquete de recuperación anterior.

   El archivo del paquete de recuperación debe protegerse porque contiene claves de cifrado y contraseñas que pueden usarse para obtener datos del sistema StorageGRID.

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

   ${post_edited_translations.segment}

   Si se produce un error durante el proceso de actualización, un mensaje en un banner indica el número de nodos en los que no se pudo cambiar la clave. El sistema volverá a intentar automáticamente el proceso en cualquier nodo en el que no se pudo cambiar la clave. Si el proceso termina y algunos nodos siguen sin tener la clave cambiada, aparece el botón **Retry**.

   Si la actualización de la clave falló en uno o varios nodos:

   a. Revisa los mensajes de error que aparecen en la tabla.
   b. Resuelve los problemas.
   c. Selecciona **Reintentar**.

      Al volver a intentarlo, solo se modifican las claves de acceso SSH en los nodos que fallaron durante los intentos anteriores de cambio de clave.

5. Una vez que se hayan cambiado las claves de acceso SSH para todos los nodos, elimina el el primer paquete de recuperación que descargaste.
6. ${post_edited_translations.segment}

# Usa la federación de identidades en StorageGRID

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 que ya conocen.

## Configura la federación de identidades para Grid Manager

Puedes configurar la federación de identidades en Grid Manager si deseas que los grupos de administradores y los usuarios se gestionen en otro sistema, como Active Directory, Microsoft Entra ID, OpenLDAP u Oracle Directory Server.

**Antes de empezar**

- Has iniciado sesión en Grid Manager usando una "navegador web compatible".
- Has "permisos de acceso específicos".
- Estás utilizando Active Directory, Microsoft Entra ID, OpenLDAP u Oracle Directory Server como proveedor de identidades.

  > Si deseas utilizar un servicio LDAP v3 que no figure en la lista, ponte en contacto con soporte técnico.

- Si tienes previsto utilizar OpenLDAP, debes configurar el servidor OpenLDAP. Consulta Guía para configurar un servidor OpenLDAP.
- Si tienes previsto habilitar el inicio de sesión único (SSO), ya revisaste la "Requisitos y consideraciones para el inicio de sesión único".
- Si tienes previsto utilizar Transport Layer Security (TLS) para las comunicaciones con el servidor LDAP, el proveedor de identidad está usando TLS 1.2 o 1.3. Consulta "Algoritmos de cifrado compatibles para las

conexiones TLS salientes".

**Acerca de esta tarea**

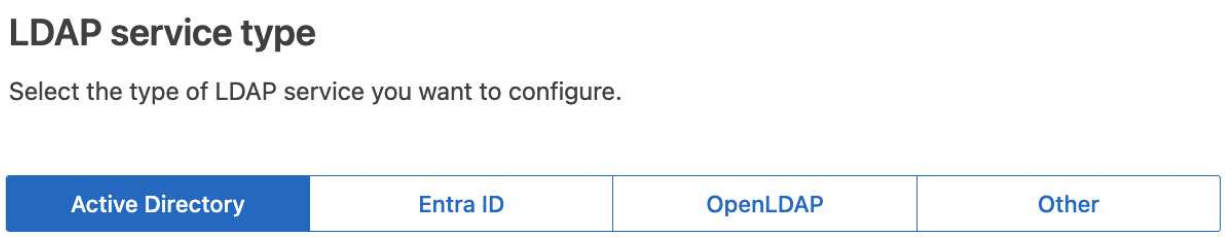
Puedes configurar un origen de identidad para el Grid Manager si quieres importar grupos desde otro sistema como Active Directory, Microsoft Entra ID, OpenLDAP u Oracle Directory Server. Puedes importar los siguientes tipos de grupos:

- Grupos de administradores. Los usuarios que forman parte de los grupos de administradores pueden iniciar sesión en Grid Manager y realizar tareas, en función de los permisos de gestión asignados al grupo.
- Grupos de usuarios de inquilinos para inquilinos que no usan su propia fuente de identidad. Los usuarios de los grupos de inquilinos pueden iniciar sesión en el Tenant Manager y realizar tareas según los permisos asignados al grupo en el Tenant Manager. Consulta "Crear cuenta de inquilino" y "Utiliza una cuenta de inquilino" para obtener más detalles.

**Accede a la configuración**

**Pasos**

1. Selecciona **Configuración** > **Control de acceso** > **Federación de identidades**.
2. Selecciona **Habilitar federación de identidades**.
3. ${post_edited_translations.segment}




${post_edited_translations.segment}

4. Si has seleccionado **Other**, rellena los campos de la sección «Atributos LDAP». De lo contrario, pasa al siguiente paso.
   - **Nombre único de usuario**: El nombre del atributo que contiene el identificador único de un usuario LDAP. Este atributo equivale a `sAMAccountName` para Active Directory y `uid` para OpenLDAP. Si estás configurando Oracle Directory Server, introduce `uid`.
   - **UUID de usuario**: El nombre del atributo que contiene el identificador único permanente de un usuario LDAP. Este atributo es equivalente a `objectGUID` en Active Directory y `entryUUID` en OpenLDAP. Si estás configurando Oracle Directory Server, introduce `nsuniqueid`. El valor de cada usuario para el atributo especificado debe ser un número hexadecimal de 32 dígitos, ya sea en formato de 16 bytes o de cadena, donde se ignoran los guiones.
   - **Nombre único de grupo**: el nombre del atributo que contiene el identificador único de un grupo LDAP. Este atributo es equivalente a `sAMAccountName` para Active Directory y `cn` para OpenLDAP. Si estás configurando Oracle Directory Server, introduce `cn`.
   - **UUID del grupo**: El nombre del atributo que contiene el identificador único permanente de un grupo LDAP. Este atributo es equivalente a `objectGUID` para Active Directory y `entryUUID` para OpenLDAP. Si estás configurando Oracle Directory Server, introduce `nsuniqueid`. El valor de cada grupo para el atributo especificado debe ser un número hexadecimal de 32 dígitos, ya sea en formato

de 16 bytes o de cadena, donde se ignoran los guiones.

5. Para todos los tipos de servicio LDAP, introduce la información necesaria sobre el servidor LDAP y la conexión de red en la sección Configurar el servidor LDAP.
   - **Nombre de host**: el nombre de dominio completo (FQDN) o la dirección IP del servidor LDAP.
   - **Puerto**: El puerto utilizado para conectarse al servidor LDAP.

     > El puerto predeterminado para STARTTLS es 389, y el puerto predeterminado para LDAPS es 636. Sin embargo, puedes usar cualquier puerto siempre que tu firewall esté configurado correctamente.

   - ${post_edited_translations.segment}

     Para Active Directory, también puedes especificar el Down-Level Logon Name o el User Principal Name.

     El usuario especificado debe tener permiso para ver la lista de grupos y usuarios y para acceder a los siguientes atributos:

     - `sAMAccountName` o `uid`
     - `objectGUID`, `entryUUID`, o `nsuniqueid`
     - `cn`
     - `memberOf` o `isMemberOf`
     - **Active Directory**: `objectSid`, `primaryGroupID`, `userAccountControl` y `userPrincipalName`
     - **Entra ID**: `accountEnabled` y `userPrincipalName`
   - **Contraseña**: la contraseña asociada al nombre de usuario.

     > Si cambias la contraseña en el futuro, debes actualizarla en esta página.

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

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

   - **DN de base de usuarios**: La ruta completa del nombre distintivo (DN) de un subárbol LDAP en el que quieres buscar usuarios.

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

   - **Formato de nombre de usuario de enlace** (opcional): el patrón de nombre de usuario predeterminado que StorageGRID debe utilizar si no es posible determinar el patrón automáticamente.

     Se recomienda especificar el **formato de nombre de usuario de enlace** porque puede permitir que los usuarios inicien sesión si StorageGRID no puede enlazarse con la cuenta de servicio.

${post_edited_translations.segment}

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

  Incluye **[USERNAME]** tal y como aparece escrito.

6. En la sección Transport Layer Security (TLS), selecciona una configuración de seguridad.
   - **Usar STARTTLS**: Utiliza STARTTLS para proteger las comunicaciones con el servidor LDAP. Esta es la opción recomendada para Active Directory, OpenLDAP u Other, pero no es compatible con Microsoft Entra ID.
   - **Usar LDAPS**: La opción LDAPS (LDAP sobre SSL) utiliza TLS para establecer una conexión con el servidor LDAP. Debes seleccionar esta opción para Microsoft Entra ID.
   - **No utilices TLS**: El tráfico de red entre el sistema StorageGRID y el servidor LDAP no estará protegido. Esta opción no es compatible con Microsoft Entra ID.

     El uso de la opción **No usar TLS** no se admite si tu servidor de Active Directory exige la firma LDAP. Debes usar STARTTLS o LDAPS.

7. Si has seleccionado STARTTLS o LDAPS, elige el certificado que se usa para proteger la conexión.
   - ${post_edited_translations.segment}
   - ${post_edited_translations.segment}

     ${post_edited_translations.segment}

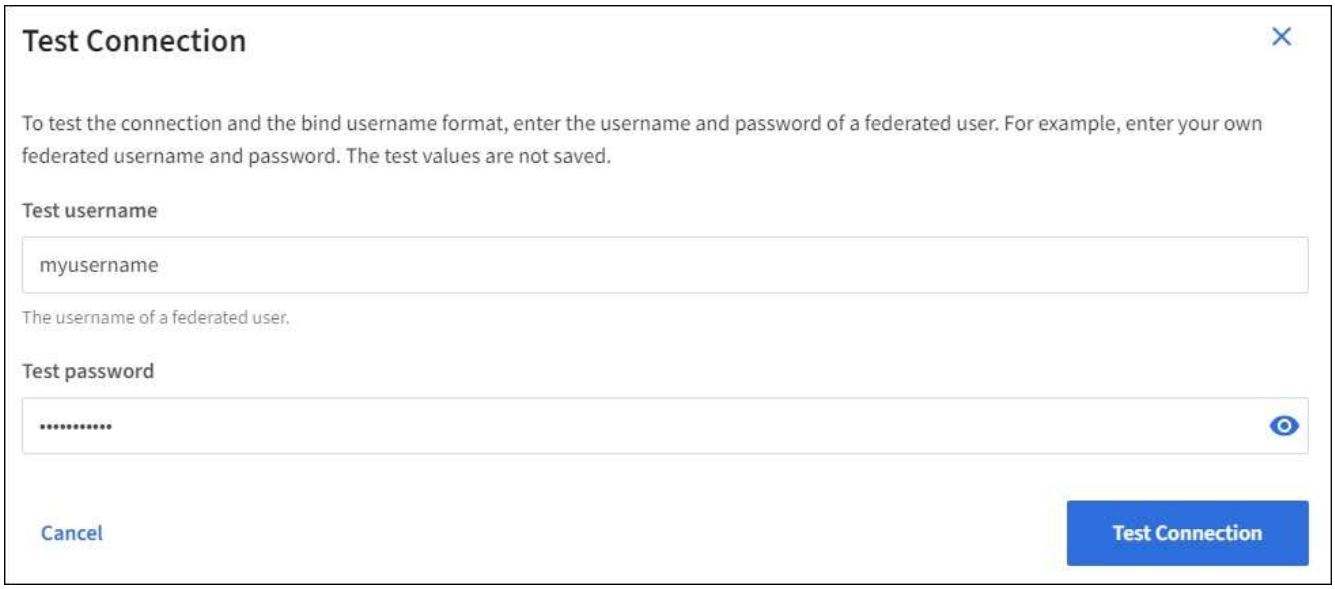
### Comprueba la conexión y guarda la configuración

Una vez introducidos todos los valores, debes comprobar la conexión antes de poder guardar la configuración. StorageGRID verifica los parámetros de conexión del servidor LDAP y el formato del nombre de usuario de enlace, si has especificado alguno.

**Pasos**

1. Selecciona **Probar conexión**.
2. ${post_edited_translations.segment}
   - Si los parámetros de conexión son correctos, aparece el mensaje «Prueba de conexión realizada con éxito». Selecciona **Guardar** para guardar la configuración.
   - Aparecerá el mensaje «No se ha podido establecer una conexión de prueba» si la configuración de la conexión no es válida. Selecciona **Cerrar**. Luego, soluciona cualquier problema y vuelve a probar la conexión.
3. Si has especificado un formato de nombre de usuario de enlace, introduce el nombre de usuario y la contraseña de un usuario federado válido.

   Por ejemplo, introduce tu propio nombre de usuario y contraseña. No incluyas caracteres especiales en el nombre de usuario, como @ o /.




- Si los parámetros de conexión son correctos, aparece el mensaje «Prueba de conexión realizada con éxito». Selecciona **Guardar** para guardar la configuración.
- Aparece un mensaje de error si la configuración de la conexión, el formato del nombre de usuario de enlace o el nombre de usuario y la contraseña de prueba no son válidos. Soluciona cualquier problema y vuelve a probar la conexión.

## Forzar la sincronización con la fuente de identidad

El sistema StorageGRID sincroniza periódicamente los grupos y usuarios federados desde la fuente de identidades. Puedes forzar la sincronización si quieres habilitar o restringir los permisos de los usuarios lo más rápido posible.

**Pasos**

1. Ve a la página de federación de identidades.
2. Selecciona **Sync server** en la parte superior de la página.

   El proceso de sincronización puede tardar un tiempo dependiendo de tu entorno.

   La alerta **Error de sincronización de la federación de identidades** se activa si hay un problema al sincronizar los grupos y usuarios federados desde la fuente de identidades.

## ${post_edited_translations.segment}

Puedes desactivar de forma temporal o permanente la federación de identidades para grupos y usuarios. Cuando la federación de identidades está desactivada, no hay comunicación entre StorageGRID y el origen de identidad. Sin embargo, se conserva cualquier configuración que hayas realizado, lo que te permitirá volver a activar fácilmente la federación de identidades en el futuro.

**Acerca de esta tarea**

Antes de desactivar la federación de identidades, debes tener en cuenta lo siguiente:

- Los usuarios federados no podrán iniciar sesión.
- Los usuarios federados que están conectados actualmente seguirán teniendo acceso al sistema

StorageGRID hasta que su sesión expire, pero no podrán iniciar sesión después de que su sesión expire.

- No se llevará a cabo la sincronización entre el sistema StorageGRID y la fuente de identidades, y no se generarán alertas para las cuentas que no se hayan sincronizado.
- La casilla de selección **Habilitar federación de identidades** aparece desactivada si el estado del inicio de sesión único (SSO) es **Habilitado** o **Modo Sandbox**. El estado del SSO en la página de inicio de sesión único debe estar **Desactivado** antes de que puedas desactivar la federación de identidades. Consulta "Desactivar el inicio de sesión único".

**Pasos**

1. Ve a la página de federación de identidades.
2. Desmarca la casilla **Habilitar federación de identidades**.

## Guía para configurar un servidor OpenLDAP

Si deseas utilizar un servidor OpenLDAP para la federación de identidades, debes configurar determinados parámetros en el servidor OpenLDAP.

> En el caso de las fuentes de identidad que no sean Active Directory o Microsoft Entra ID, StorageGRID no bloqueará automáticamente el acceso a S3 a los usuarios que hayan sido desactivados externamente. Para bloquear el acceso a S3, elimina cualquier clave de S3 del usuario o elimina al usuario de todos los grupos.

**${post_edited_translations.segment}**

Los overlays memberof y refint deben estar habilitados. Para obtener más información, consulta las instrucciones para el mantenimiento de la pertenencia inversa a grupos en "Documentación de OpenLDAP: Guía del administrador versión 2.4".

**Indexación**

Debes configurar los siguientes atributos de 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, asegúrate de que los campos mencionados en la ayuda para Nombre de usuario estén indexados para un rendimiento óptimo.

Consulta la información sobre el mantenimiento inverso de la pertenencia a grupos en la "Documentación de OpenLDAP: Guía del administrador versión 2.4".

# Administra grupos de administración en StorageGRID

Puedes crear grupos de administradores para gestionar los permisos de seguridad de uno o varios usuarios administradores. Los usuarios deben pertenecer a un grupo para que se les conceda acceso al sistema StorageGRID.

**Antes de empezar**

- Has iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tienes "permisos de acceso específicos".
- ${post_edited_translations.segment}

## Crear un grupo de administradores

${post_edited_translations.segment}

### Accede al asistente

**Pasos**

1. ${post_edited_translations.segment}
2. Selecciona **Crear grupo**.

### ${post_edited_translations.segment}

Puedes crear un grupo local o importar un grupo federado.

- ${post_edited_translations.segment}
- Crea un grupo federado para importar usuarios desde la fuente de identidad.

**Grupo local**

**Pasos**

1. ${post_edited_translations.segment}
2. Introduce un nombre para mostrar para el grupo, que podrás modificar más adelante si es necesario. Por ejemplo, «Usuarios de mantenimiento» o «Administradores de ILM».
3. Introduce un nombre único para el grupo, que no podrás actualizar más adelante.
4. Selecciona **Continuar**.

**${post_edited_translations.segment}**

**Pasos**

1. ${post_edited_translations.segment}
2. Introduce el nombre del grupo que deseas importar, exactamente como aparece en la fuente de identidad configurada.
   - ${post_edited_translations.segment}
   - Para OpenLDAP, usa el CN (Common Name).
   - Para otro LDAP, utiliza el nombre único correspondiente para el servidor LDAP.
3. Selecciona **Continuar**.

### ${post_edited_translations.segment}

**Pasos**

1. Para **Modo de acceso**, selecciona si los usuarios del grupo pueden cambiar la configuración y realizar operaciones en el Grid Manager y la Grid Management API o si solo pueden ver la configuración y las

funciones.

- **Lectura/escritura** (por defecto): los usuarios pueden modificar la configuración y realizar las operaciones que les permiten sus permisos de gestión.
- **Solo lectura**: los usuarios solo pueden ver la configuración y las funciones. No pueden realizar ningún cambio ni llevar a cabo ninguna operación en el Grid Manager o la Grid Management API. Los usuarios locales de solo lectura pueden cambiar sus propias contraseñas.

> ${post_edited_translations.segment}

2. Selecciona uno o varios "Permisos del grupo admin".

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

3. Si vas a crear un grupo local, selecciona **Continuar**. Si vas a crear un grupo federado, selecciona **Crear grupo** y **Finalizar**.

**${post_edited_translations.segment}**

**Pasos**

1. ${post_edited_translations.segment}

   Si aún no has creado usuarios locales, puedes guardar el grupo sin añadir usuarios. Puedes añadir este grupo al usuario en la página «Usuarios». Consulta "Gestiona usuarios" para obtener más información.

2. Selecciona **Crear grupo** y **Finalizar**.

## ${post_edited_translations.segment}

${post_edited_translations.segment}

- Para consultar la información básica de todos los grupos, revisa la tabla de la página «Grupos».
- ${post_edited_translations.segment}

| Tarea | Menú de acciones | ${post_edited_translations.segment} |
|---|---|---|
| ${post_edited_translations.segment} | a. Selecciona la casilla para el grupo.<br>b. Selecciona **Acciones** > **Ver detalles del grupo**. | ${post_edited_translations.segment} |
| ${post_edited_translations.segment} | a. Selecciona la casilla para el grupo.<br>b. Selecciona **Acciones** > **Editar nombre del grupo**.<br>c. ${post_edited_translations.segment}<br>d. Selecciona **Guardar cambios**. | a. Selecciona el nombre del grupo para ver los detalles.<br>b. Selecciona el icono de edición .<br>c. ${post_edited_translations.segment}<br>d. Selecciona **Guardar cambios**. |

| Tarea | Menú de acciones | ${post_edited_translations.segment} |
| --- | --- | --- |
| Editar el modo de acceso o los permisos | a. Selecciona la casilla para el grupo.<br>b. Selecciona **Acciones** > **Ver detalles del grupo**.<br>c. Opcionalmente, cambia el modo de acceso del grupo.<br>d. Opcionalmente, selecciona o desmarca "Permisos del grupo admin".<br>e. Selecciona **Guardar cambios**. | a. Selecciona el nombre del grupo para ver los detalles.<br>b. Opcionalmente, cambia el modo de acceso del grupo.<br>c. Opcionalmente, selecciona o desmarca "Permisos del grupo admin".<br>d. Selecciona **Guardar cambios**. |

### Duplicar un grupo

**Pasos**

1. Selecciona la casilla para el grupo.
2. Selecciona **Acciones** > **Duplicar grupo**.
3. Completa el asistente para duplicar grupos.

### Borrar un grupo

Puedes eliminar un grupo de administradores cuando quieras quitar el grupo del sistema y eliminar todos los permisos asociados con el grupo. Al eliminar un grupo de administradores, se eliminan los usuarios del grupo, pero no se eliminan los usuarios.

**Pasos**

1. En la página «Grupos», marca la casilla correspondiente a cada grupo que quieras eliminar.
2. Selecciona **Acciones** > **Eliminar grupo**.
3. Selecciona **Eliminar grupos**.

# Permisos del grupo Admin en StorageGRID

Al crear grupos de usuarios administradores, seleccionas uno o varios permisos para controlar el acceso a funciones específicas de Grid Manager. Luego, puedes asignar a cada usuario a uno o varios de estos grupos de administradores para determinar qué tareas puede realizar ese usuario.

${post_edited_translations.segment}

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

- Inicia sesión en Grid Manager
- Ver el panel de control
- Ver las páginas de Nodes

- Ver alertas actuales y resueltas
- Cambiar su propia contraseña (solo usuarios locales)
- Ver determinada información que aparece en las páginas de Configuración y Mantenimiento

## ${post_edited_translations.segment}

Para todos los permisos, la configuración del **modo de acceso** del grupo determina si los usuarios pueden cambiar los ajustes y realizar operaciones o si solo pueden ver los ajustes y funciones relacionados. Si un usuario pertenece a varios grupos y cualquier grupo está configurado como **solo lectura**, el usuario tendrá acceso de solo lectura a todos los ajustes y funciones seleccionados.

En los apartados siguientes se describen los permisos que puedes asignar al crear o editar un grupo de administradores. Cualquier funcionalidad que no se mencione explícitamente requiere el permiso **Root access**.

## Acceso a raíz

${post_edited_translations.segment}

## ${post_edited_translations.segment}

Este permiso proporciona acceso a la opción **Cambiar contraseña de root** en la página Tenants, lo que te permite controlar quién puede cambiar la contraseña del usuario raíz local del tenant. Este permiso también se utiliza para migrar claves S3 cuando la función de importación de claves S3 está habilitada. Los usuarios que no tengan este permiso no pueden ver la opción **Cambiar contraseña de root**.

Para conceder acceso a la página Tenants, que contiene la opción **Change root password**, asigna también el permiso **Tenant accounts**.

## ILM

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

- ${post_edited_translations.segment}
- Políticas
- Etiquetas de políticas
- Grupos de almacenamiento
- Grados de almacenamiento
- Regiones
- Búsqueda de metadatos de objetos

${post_edited_translations.segment}

## ${post_edited_translations.segment}

Los usuarios deben tener el permiso de Mantenimiento para usar estas opciones:

- ${post_edited_translations.segment}

    - ${post_edited_translations.segment}
- ${post_edited_translations.segment}
    - Nombres de dominio de los endpoints S3
- ${post_edited_translations.segment}
    - Decomisionar
    - Expansión
    - Comprobación de la existencia de un objeto
    - Recuperación
- **Mantenimiento** > **Sistema**:
    - Paquete de recuperación
    - Actualización de software
- **Soporte** > **Herramientas**:
    - Registros

Los usuarios que no tengan el permiso de Maintenance pueden ver, pero no editar, estas páginas:

- ${post_edited_translations.segment}
    - Servidores DNS
    - Red de grid
    - Servidores NTP
- **Mantenimiento** > **Sistema**:
    - Licencia
- ${post_edited_translations.segment}
    - Nombres de dominio de los endpoints S3
- ${post_edited_translations.segment}
    - Certificados
- **Configuración** > **Supervisión**:
    - ${post_edited_translations.segment}

## Gestiona alertas

Este permiso proporciona acceso a las opciones para gestionar alertas. Los usuarios deben tener este permiso para gestionar silencios, notificaciones de alerta y reglas de alerta.

## Consulta de métricas

Este permiso permite acceder a:

- **Soporte** > **Herramientas** > **Métricas** página
- ${post_edited_translations.segment}
- Tarjetas del panel de control de Grid Manager que contienen métricas

### Búsqueda de metadatos de objetos

Este permiso permite acceder a la página **ILM** > **Búsqueda de metadatos de objetos**.

### Otra configuración de grid

${post_edited_translations.segment}

- ${post_edited_translations.segment}
  - Grados de almacenamiento
- **Configuración** > **Sistema**:
- ${post_edited_translations.segment}
  - ${post_edited_translations.segment}

### ${post_edited_translations.segment}

${post_edited_translations.segment}

- Acceso al E-Series SANtricity System Manager en los dispositivos de almacenamiento a través de Grid Manager.
- La posibilidad de realizar tareas de resolución de problemas y mantenimiento en la pestaña Manage drives para los dispositivos que admiten estas operaciones.

### ${post_edited_translations.segment}

Este permiso permite:

- ${post_edited_translations.segment}
- Ver las políticas de clasificación de tráfico existentes
- Ver las tarjetas del panel de Grid Manager que contienen los detalles de los inquilinos

# Administra usuarios en StorageGRID

Puedes ver los usuarios locales y federados. También puedes crear usuarios locales y asignarlos a grupos de administradores locales para determinar a qué funciones de Grid Manager pueden acceder dichos usuarios.

**Antes de empezar**

- Has iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tienes "permisos de acceso específicos".

### ${post_edited_translations.segment}

Puedes crear uno o varios usuarios locales y asignar cada usuario a uno o varios grupos locales. Los permisos del grupo controlan a qué funciones de Grid Manager y de Grid Management API puede acceder el usuario.

Solo puedes crear usuarios locales. Utiliza la fuente de identidades externa para gestionar usuarios y grupos federados.

El Grid Manager incluye un usuario local predefinido, llamado "root". No puedes eliminar el usuario raíz.

${post_edited_translations.segment}

**Accede al asistente**

**Pasos**

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

**${post_edited_translations.segment}**

**Pasos**

1. ${post_edited_translations.segment}
2. Si lo deseas, selecciona **Sí** si este usuario no debe tener acceso a Grid Manager ni a Grid Management API.
3. Selecciona **Continuar**.

**${post_edited_translations.segment}**

**Pasos**

1. Si lo deseas, asigna al usuario a uno o varios grupos para determinar sus permisos.

   Si aún no has creado ningún grupo, puedes guardar el usuario sin seleccionar grupos. Puedes añadir este usuario a un grupo en la página Grupos.

   Si un usuario pertenece a varios grupos, los permisos son acumulativos. Consulta "${post_edited_translations.segment}" para ver los detalles.

2. Selecciona **Crear usuario** y selecciona **Finalizar**.

## ${post_edited_translations.segment}

Puedes consultar los detalles de los usuarios locales y federados existentes. Puedes modificar un usuario local para cambiar su nombre completo, contraseña o pertenencia a grupos. También puedes impedir temporalmente que un usuario acceda a Grid Manager y a la Grid Management API.

Solo puedes editar usuarios locales. Utiliza la fuente de identidades externa para gestionar usuarios federados.

- Para consultar la información básica de todos los usuarios locales y federados, revisa la tabla de la página Usuarios.
- Para ver todos los detalles de un usuario concreto, editar un usuario local o cambiar la contraseña de un usuario local, utiliza el menú **Acciones** o la página de detalles.

  Cualquier cambio se aplica la próxima vez que el usuario cierre sesión y vuelva a iniciar sesión en Grid Manager.

  Los usuarios locales pueden cambiar sus propias contraseñas mediante la opción **Cambiar contraseña** del banner de Grid Manager.

| Tarea | Menú de acciones | ${post_edited_translations.segment} |
|---|---|---|
| Ver los datos del usuario | a. ${post_edited_translations.segment}<br>b. ${post_edited_translations.segment} | Selecciona el nombre del usuario en la tabla. |
| Editar nombre completo (solo usuarios locales) | a. ${post_edited_translations.segment}<br>b. Selecciona **Acciones** > **Editar nombre completo**.<br>c. ${post_edited_translations.segment}<br>d. Selecciona **Guardar cambios**. | a. Selecciona el nombre del usuario para ver los detalles.<br>b. Selecciona el icono de edición .<br>c. ${post_edited_translations.segment}<br>d. Selecciona **Guardar cambios**. |
| ${post_edited_translations.segment} | a. ${post_edited_translations.segment}<br>b. ${post_edited_translations.segment}<br>c. Selecciona la pestaña Acceso.<br>d. Selecciona **Sí** para impedir que el usuario inicie sesión en Grid Manager o en la Grid Management API, o selecciona **No** para permitirle iniciar sesión.<br>e. Selecciona **Guardar cambios**. | a. Selecciona el nombre del usuario para ver los detalles.<br>b. Selecciona la pestaña Acceso.<br>c. Selecciona **Sí** para impedir que el usuario inicie sesión en Grid Manager o en la Grid Management API, o selecciona **No** para permitirle iniciar sesión.<br>d. Selecciona **Guardar cambios**. |
| Cambiar contraseña (solo usuarios locales) | a. ${post_edited_translations.segment}<br>b. ${post_edited_translations.segment}<br>c. Selecciona la pestaña «Contraseña».<br>d. ${post_edited_translations.segment}<br>e. Selecciona **Cambiar contraseña**. | a. Selecciona el nombre del usuario para ver los detalles.<br>b. Selecciona la pestaña «Contraseña».<br>c. ${post_edited_translations.segment}<br>d. Selecciona **Cambiar contraseña**. |
| Cambiar grupos (solo usuarios locales) | a. ${post_edited_translations.segment}<br>b. ${post_edited_translations.segment}<br>c. Selecciona la pestaña Grupos.<br>d. Si lo deseas, selecciona el enlace que aparece junto al nombre de un grupo para ver los detalles del grupo en una nueva pestaña del navegador.<br>e. ${post_edited_translations.segment}<br>f. Selecciona **Guardar cambios**. | a. Selecciona el nombre del usuario para ver los detalles.<br>b. Selecciona la pestaña Grupos.<br>c. Si lo deseas, selecciona el enlace que aparece junto al nombre de un grupo para ver los detalles del grupo en una nueva pestaña del navegador.<br>d. ${post_edited_translations.segment}<br>e. Selecciona **Guardar cambios**. |

## Importar usuarios federados

Puedes importar uno o varios usuarios federados, hasta un máximo de 100 usuarios, directamente en la página de Usuarios.

**Pasos**

1. Selecciona **Configuración** > **Control de acceso** > **Usuarios administradores**.
2. Selecciona **Importar usuarios federados**.
3. Introduce el UUID o el nombre de usuario de uno o varios usuarios federados.

   ${post_edited_translations.segment}

4. ${post_edited_translations.segment}

   Si la importación al campo «Usuarios» falla para uno o varios usuarios, realiza los siguientes pasos:

   a. ${post_edited_translations.segment}
   b. ${post_edited_translations.segment}

   Después de que cierres el cuadro de diálogo **Importar usuarios federados**, la información de los usuarios federados importados correctamente se muestra en la página Usuarios.

### Duplicar un usuario

${post_edited_translations.segment}

**Pasos**

1. ${post_edited_translations.segment}
2. Selecciona **Acciones** > **Duplicar usuario**.
3. ${post_edited_translations.segment}

### Eliminar un usuario

Puedes eliminar un usuario local para borrarlo definitivamente del sistema.

> No puedes eliminar el usuario raíz.

**Pasos**

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}
3. Selecciona **Eliminar usuario**.

# Utiliza el inicio de sesión único (SSO)

### Conoce StorageGRID SSO

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

El sistema StorageGRID admite el inicio de sesión único (SSO) mediante el estándar Security Assertion

Markup Language 2.0 (SAML 2.0).

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

### Inicia sesión cuando el inicio de sesión único está habilitado

Cuando el SSO está activado y te conectas a StorageGRID, se te redirige a la página de SSO de tu organización para validar tus credenciales.

**Pasos**

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

   Aparece la página de Sign in de StorageGRID.

   - Si es la primera vez que accedes a la URL desde este navegador, se te pedirá que introduzcas un ID de cuenta.
   - Si ya has accedido anteriormente al Grid Manager o al Tenant Manager, se te pedirá que selecciones una cuenta reciente o que introduzcas un ID de cuenta.

   > La página de inicio de sesión de StorageGRID no aparece cuando introduces la URL completa de una cuenta de inquilino (es decir, un dominio completo o una dirección IP seguida de `/?accountId=20-digit-account-id`). En su lugar, te redirigen inmediatamente a la página de inicio de sesión único (SSO) de tu organización, donde puedes inicia sesión con tus credenciales de SSO.

2. Indica si deseas acceder al Grid Manager o al Tenant Manager:
   - Para acceder al Grid Manager, deja en blanco el campo **ID de cuenta**, introduce **0** como ID de cuenta o selecciona **Grid Manager** si aparece en la lista de cuentas recientes.
   - Para acceder al Gestor de inquilinos, introduce el ID de cuenta del inquilino de 20 dígitos o selecciona un inquilino por su nombre si aparece en la lista de cuentas recientes.
3. Selecciona **Sign in**

   StorageGRID te redirige a la página de inicio de sesión único (SSO) de tu organización. Por ejemplo:

4. Inicia sesión con tus credenciales de SSO.

   Si tus credenciales de SSO son correctas:

   a. El proveedor de identidad (IdP) proporciona una respuesta de autenticación a StorageGRID.
   b. StorageGRID valida la respuesta de autenticación.
   c. Si la respuesta es válida y perteneces a un grupo federado con permisos de acceso a StorageGRID, has iniciado sesión en Grid Manager o en Tenant Manager, dependiendo de la cuenta que hayas seleccionado.

   > Si no se puede acceder a la cuenta de servicio, aún puedes iniciar sesión, siempre y cuando seas un usuario existente que pertenezca a un grupo federado con permisos de acceso a StorageGRID.

5. Si lo deseas, accede a otros nodos de administración o accede al Grid Manager o al Tenant Manager, si

tienes los permisos adecuados.

No es necesario que vuelvas a introducir tus credenciales de SSO.

### Cerrar sesión cuando el SSO está activado

Cuando el SSO está habilitado para StorageGRID, lo que ocurre al cerrar sesión depende de en qué hayas iniciado sesión y desde dónde la cierres.

**Pasos**

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

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

   La tabla resume lo que ocurre al cerrar sesión si estás usando una sola sesión del navegador. Si has iniciado sesión en StorageGRID en varias sesiones del navegador, debes cerrar sesión en todas ellas por separado.

| Si has iniciado sesión en… | Y cierras sesión en… | Se te ha desconectado de… |
|---|---|---|
| Grid Manager en uno o varios nodos de administración | Grid Manager en cualquier nodo de administración | Grid Manager en todos los nodos de administración<br><br>**Nota:** Si utilizas Entra ID para el inicio de sesión único, es posible que tardes unos minutos en cerrar sesión en todos los nodos de administración. |
| Tenant Manager en uno o varios nodos de administración | Tenant Manager en cualquier nodo de administración | Tenant Manager en todos los nodos de administración |
| Tanto Grid Manager como Tenant Manager | Grid Manager | Solo el Grid Manager. También debes cerrar la sesión en el Tenant Manager para cerrar la sesión de inicio de sesión único. |

## Requisitos y consideraciones para StorageGRID SSO

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

### Requisitos del proveedor de identidad

StorageGRID es compatible con los siguientes proveedores de identidad (IdP) de SSO:

- Servicio de federación de Active Directory (AD FS)

- Microsoft Entra ID
- PingFederate

Debes configurar la federación de identidades para tu sistema StorageGRID antes de poder configurar un proveedor de identidades de SSO. El tipo de servicio LDAP que utilices para la federación de identidades controla qué tipo de SSO puedes implementar.

| Tipo de servicio LDAP configurado | Opciones para el proveedor de identidad de SSO |
|---|---|
| Active Directory | • Active Directory<br>• Entra ID<br>• PingFederate |
| Entra ID | Entra ID |

#### Requisitos de AD FS

Puedes utilizar cualquiera de las siguientes versiones de AD FS:

- ${post_edited_translations.segment}
- Windows Server 2019 AD FS
- Windows Server 2016 AD FS

> Windows Server 2016 debería estar usando el "${post_edited_translations.segment}", o una versión superior.

#### Requisitos adicionales

- ${post_edited_translations.segment}
- Microsoft .NET Framework, versión 3.5.1 o superior

#### ${post_edited_translations.segment}

Si utilizas Entra ID como tipo de SSO y los usuarios tienen nombres principales de usuario que no usan sAMAccountName como prefijo, pueden ocurrir problemas de inicio de sesión si StorageGRID pierde la conexión con el servidor LDAP. Para permitir que los usuarios inicien sesión, debes restablecer la conexión con el servidor LDAP.

### ${post_edited_translations.segment}

De forma predeterminada, StorageGRID utiliza un certificado de interfaz de gestión en cada nodo de administración para proteger el acceso a Grid Manager, Tenant Manager, la Grid Management API y la Tenant Management API. Cuando configuras relaciones de confianza con partes de confianza (AD FS), aplicaciones empresariales (Entra ID) o conexiones de proveedor de servicios (PingFederate) para StorageGRID, utilizas el certificado de servidor como certificado de firma para las solicitudes de StorageGRID.

Si aún no has "he configurado un certificado personalizado para la interfaz de gestión", deberías hacerlo ahora. Cuando instalas un certificado de servidor personalizado, este se utiliza para todos los Admin Nodes, y puedes usarlo en todas las relying party trusts de StorageGRID, aplicaciones empresariales o conexiones SP.

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

Puedes acceder al certificado de servidor de un Admin Node iniciando sesión en la línea de comandos del nodo y yendo al directorio `/var/local/mgmt-api`. Un certificado de servidor personalizado se llama `custom-server.crt`. El certificado de servidor predeterminado del nodo se llama `server.crt`.

#### Requisitos de puertos

El inicio de sesión único (SSO) no está disponible en los puertos restringidos de Grid Manager o Tenant Manager. Debes utilizar el puerto HTTPS predeterminado (443) si deseas que los usuarios se autentiquen mediante el inicio de sesión único. Consulta "Controla el acceso en el cortafuegos externo".

## Comprueba que los usuarios federados puedan iniciar sesión en StorageGRID

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

#### Antes de empezar

- Has iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tienes "permisos de acceso específicos".
- Ya has configurado la federación de identidades.

#### Pasos

1. Si ya existen cuentas de inquilinos, comprueba que ninguno de los inquilinos esté usando su propia fuente de identidad.

   Cuando habilitas el SSO, el origen de identidad configurado en el Tenant Manager se sustituye por el origen de identidad configurado en el Grid Manager. Los usuarios que pertenecen al origen de identidad del inquilino ya no podrán iniciar sesión a menos que tengan una cuenta en el origen de identidad del Grid Manager.

   a. Inicia sesión en Tenant Manager con cada cuenta de inquilino.
   b. Selecciona **Gestión de acceso** > **Federación de identidades**.
   c. Comprueba que la casilla **Habilitar federación de identidades** no esté marcada.
   d. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}
   a. En Grid Manager, selecciona **Configuración** > **Control de acceso** > **Grupos de administradores**.
   b. Asegúrate de que se haya importado al menos un grupo federado desde la fuente de identidades de Active Directory y de que se le haya asignado el permiso de acceso Root.
   c. ${post_edited_translations.segment}
   d. ${post_edited_translations.segment}

3. Si ya existen cuentas de inquilinos, confirma que un usuario federado con permiso de acceso de usuario raíz pueda iniciar sesión:
   a. ${post_edited_translations.segment}
   b. ${post_edited_translations.segment}
   c. En la pestaña «Introducir datos», selecciona **Continuar**.
   d. Si la casilla **Usar fuente de identidad propia** está marcada, desmárcala y selecciona **Guardar**.

      ${post_edited_translations.segment}

   e. ${post_edited_translations.segment}
   f. ${post_edited_translations.segment}
   g. ${post_edited_translations.segment}
   h. ${post_edited_translations.segment}
   i. Confirma que puedes volver a iniciar sesión en el inquilino como usuario del grupo federado.

**Información relacionada**

- "Requisitos y aspectos a tener en cuenta para el inicio de sesión único"
- "${post_edited_translations.segment}"
- "Utiliza una cuenta de inquilino"

## Configura el inicio de sesión único en StorageGRID

Puedes seguir el asistente Configurar SSO y entrar en el modo sandbox para configurar y probar el inicio de sesión único (SSO) antes de habilitarlo para todos los usuarios de StorageGRID. Después de habilitar el SSO, puedes volver al modo sandbox cuando lo necesites para cambiar o volver a probar la configuración.

**Antes de empezar**

- Has iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tienes el "Permiso de acceso raíz".
- Has configurado la federación de identidades para tu sistema StorageGRID.
- ${post_edited_translations.segment}

| Tipo de servicio LDAP configurado | Opciones para el proveedor de identidad de SSO |
|---|---|
| Servicio de federación de Active Directory (AD FS) | • Active Directory<br>• Entra ID<br>• PingFederate |
| Entra ID | Entra ID |

**Acerca de esta tarea**

Cuando el SSO está habilitado y un usuario intenta iniciar sesión en un nodo de administración, StorageGRID envía una solicitud de autenticación al proveedor de identidad del SSO. A su vez, el proveedor de identidad

del SSO envía una respuesta de autenticación a StorageGRID, indicando si la solicitud de autenticación fue exitosa. Para solicitudes exitosas:

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

Para que StorageGRID (el proveedor de servicios) y el proveedor de identidad SSO puedan comunicarse de forma segura sobre las solicitudes de autenticación de los usuarios, deberás realizar estas tareas:

1. Configura los ajustes en StorageGRID.
2. Utiliza el software del proveedor de identidad de SSO para crear una confianza de parte confiable (AD FS), una aplicación empresarial (Entra ID) o un proveedor de servicios (PingFederate) para cada Admin Node.
3. Vuelve a StorageGRID para activar el inicio de sesión único.

El modo sandbox facilita realizar esta configuración iterativa y probar todos los ajustes antes de habilitar SSO. Cuando usas el modo sandbox, los usuarios no pueden iniciar sesión mediante SSO.

### Accede al asistente

**Pasos**

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

   > Si el botón «Configurar ajustes de SSO» aparece desactivado, comprueba que hayas configurado el proveedor de identidad como fuente de identidad federada. Consulta "Requisitos y aspectos a tener en cuenta para el inicio de sesión único".

2. Selecciona **Configurar ajustes de SSO**. Aparece la página «Proporcionar datos del proveedor de identidad».

### Facilita los datos del proveedor de identidad

**Pasos**

1. Selecciona el **tipo de SSO** en la lista desplegable.
2. Si has seleccionado Active Directory como tipo de SSO, introduce el **nombre del servicio de federación** del proveedor de identidad, tal y como aparece en el Servicio de federación de Active Directory (AD FS).

   > Para localizar el nombre del servicio de federación, ve al Administrador de servidores de Windows Server. Selecciona **Herramientas** > **Administración de AD FS**. En el menú Acción, selecciona **Editar propiedades del servicio de federación**. El nombre del servicio de federación aparece en el segundo campo.

3. Especifica qué certificado TLS se utilizará para proteger la conexión cuando el proveedor de identidad envíe la información de configuración de inicio de sesión único en respuesta a las solicitudes de StorageGRID.
   - **Utilizar el certificado de CA del sistema operativo**: Utiliza el certificado de CA predeterminado instalado en el sistema operativo para proteger la conexión.
   - **Utilizar un certificado de CA personalizado**: Utiliza un certificado de CA personalizado para proteger la conexión.

Si seleccionas esta opción, copia el texto del certificado personalizado y pégalo en el cuadro de texto **Certificado de la CA**.

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

> Si cambias el certificado de la CA, "Reinicia el servicio mgmt-api en los nodos de administración" y prueba que el inicio de sesión único en Grid Manager funciona correctamente.

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

**Proporciona el identificador de la parte que confía**

1. Rellena los campos de la página Proporcionar el identificador de la parte que confía según el tipo de SSO que seleccionaste.

**Active Directory**

a. Especifica el **identificador de la parte de confianza** para StorageGRID. Este valor controla el nombre que usas para cada relación de confianza con una parte de confianza en AD FS.

   - Por ejemplo, si tu grid solo tiene un Admin Node y no tienes previsto añadir más Admin Nodes en el futuro, introduce `SG` o `StorageGRID`.
   - Si tu grid incluye más de un Admin Node, incluye la cadena `[HOSTNAME]` en el identificador. Por ejemplo, `SG-[HOSTNAME]`. Incluir esta cadena da como resultado una tabla que muestra el identificador de la relying party para cada Admin Node en el grid, basado en el hostname del nodo.

   > Debes crear una relación de confianza de parte confiable para cada Admin Node en tu sistema StorageGRID. Contar con una relación de confianza de parte confiable para cada Admin Node garantiza que los usuarios puedan iniciar sesión y cerrar sesión de forma segura en cualquier Admin Node.

b. Selecciona **Guardar y entrar en modo sandbox**.

**Entra ID**

a. En la sección «Aplicación empresarial», especifica el **nombre de la aplicación empresarial** para StorageGRID. Este valor controla el nombre que usas para cada aplicación empresarial en Entra ID.

   - Por ejemplo, si tu grid solo tiene un Admin Node y no tienes previsto añadir más Admin Nodes en el futuro, introduce `SG` o `StorageGRID`.
   - Si tu grid incluye más de un Admin Node, incluye la cadena `[HOSTNAME]` en el identificador. Por ejemplo, `SG-[HOSTNAME]`. Incluir esta cadena da como resultado una tabla que muestra un nombre de aplicación empresarial para cada Admin Node en tu sistema, basado en el hostname del nodo.

   > Debes crear una aplicación empresarial para cada nodo de administración de tu sistema StorageGRID. Contar con una aplicación empresarial para cada nodo de administración garantiza que los usuarios puedan iniciar sesión y cerrar sesión de forma segura en cualquier nodo de administración.

b. Sigue los pasos en "Crear aplicaciones empresariales en Entra ID" para crear una aplicación empresarial para cada Admin Node que aparece en la tabla.

c. En Entra ID, copia la URL de metadatos de federación de cada aplicación empresarial. Luego, pega esta URL en el campo correspondiente **Federation metadata URL** en StorageGRID.

d. Una vez que hayas copiado y pegado una URL de metadatos de federación para todos los nodos de administración, selecciona **Guardar y entrar en modo sandbox**.

**PingFederate**

a. En la sección SP (Proveedor de servicios), especifica el **SP connection ID** para StorageGRID. Este valor controla el nombre que usas para cada conexión de SP en PingFederate.

   - Por ejemplo, si tu grid solo tiene un Admin Node y no tienes previsto añadir más Admin Nodes en el futuro, introduce `SG` o `StorageGRID`.
   - Si tu grid incluye más de un Admin Node, incluye la cadena `[HOSTNAME]` en el identificador. Por ejemplo, `SG-[HOSTNAME]`. Incluir esta cadena da como resultado una tabla que muestra

el ID de conexión SP de cada Admin Node en tu sistema, según el hostname del nodo.

> Debes crear una conexión SP para cada nodo de administración de tu sistema StorageGRID. Disponer de una conexión SP para cada nodo de administración garantiza que los usuarios puedan iniciar y cerrar sesión de forma segura en cualquier nodo de administración.

b. Indica la URL de los metadatos de la federación para cada Admin Node en el campo **Federation metadata URL**.

   Utiliza el siguiente formato:

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

c. Selecciona **Guardar y entrar en modo sandbox**.

**Configura relaciones de confianza de terceros, aplicaciones empresariales o conexiones SP**

Después de guardar la configuración y entrar en el modo de prueba, puedes completar y probar la configuración para el tipo de SSO que seleccionaste.

StorageGRID puede permanecer en modo «sandbox» todo el tiempo que sea necesario. Sin embargo, solo pueden iniciar sesión los usuarios federados y los usuarios locales.

**Active Directory**

**Pasos**

1. Ve a Servicios de federación de Active Directory (AD FS).
2. Crea una o varias relaciones de confianza con las partes confiables para StorageGRID, usando cada identificador de parte confiable que aparece en la tabla de la página Configurar SSO.

   Debes crear un trust para cada Admin Node que aparece en la tabla.

   Para obtener instrucciones, visita "Crear relaciones de confianza de terceros en AD FS".

**Entra ID**

**Pasos**

1. En la página de inicio de sesión único del Admin Node en el que has iniciado sesión actualmente, selecciona el botón para descargar y guardar los metadatos SAML.
2. Luego, para cualquier otro nodo de administración en tu grid, repite estos pasos:
   a. Inicia sesión en el nodo.
   b. Selecciona **Configuración** > **Control de acceso** > **inicio de sesión único**.
   c. Descarga y guarda los metadatos SAML de ese nodo.
3. Accede al portal de Azure.
4. Sigue los pasos en "Crear aplicaciones empresariales en Entra ID" para cargar el archivo de metadatos SAML de cada Admin Node en su aplicación empresarial de Entra ID correspondiente.

**PingFederate**

**Pasos**

1. En la página de inicio de sesión único del Admin Node en el que has iniciado sesión actualmente, selecciona el botón para descargar y guardar los metadatos SAML.
2. Luego, para cualquier otro nodo de administración en tu grid, repite estos pasos:
   a. Inicia sesión en el nodo.
   b. Selecciona **Configuración** > **Control de acceso** > **inicio de sesión único**.
   c. Descarga y guarda los metadatos SAML de ese nodo.
3. Entra en PingFederate.
4. "Crea una o varias conexiones de proveedor de servicios (SP) para StorageGRID". Utiliza el ID de conexión SP de cada nodo de administración (que aparece en la tabla de la página Configurar SSO) y los metadatos SAML que descargaste para ese nodo de administración.

   Debes crear una conexión SP para cada nodo de administración que aparece en la tabla.

### Configuración de prueba

Antes de aplicar el inicio de sesión único en todo tu sistema StorageGRID, comprueba que el inicio de sesión único y el cierre de sesión único estén correctamente configurados en cada Admin Node.

**Active Directory**

**Pasos**

1. En la página Configurar SSO, busca el enlace en el paso Probar la configuración del asistente.

   La URL se deriva del valor que has introducido en el campo **Federation service name**.

2. Selecciona el enlace o copia y pega la URL en un navegador para acceder a la página de inicio de sesión de tu proveedor de identidad.
3. Para confirmar que puedes utilizar el inicio de sesión único (SSO) para iniciar sesión en StorageGRID, selecciona **Sign in to one of the following sites**, selecciona el identificador de la parte de confianza correspondiente a tu nodo de administración principal y selecciona **Sign in**.
4. Introduce tu nombre de usuario y contraseña federados.
   - Si el inicio de sesión y el cierre de sesión mediante SSO se realizan correctamente, aparece un mensaje de éxito.
   - Si la operación de SSO no se realiza correctamente, aparece un mensaje de error. Soluciona el problema, borra las cookies del navegador e inténtalo de nuevo.
5. Repite estos pasos para comprobar la conexión de inicio de sesión único (SSO) de cada Admin Node en tu grid.

**Entra ID**

**Pasos**

1. Accede a la página de inicio de sesión único en el portal de Azure.
2. Selecciona **Probar esta aplicación**.
3. Introduce las credenciales de un usuario federado.
   - Si el inicio de sesión y el cierre de sesión mediante SSO se realizan correctamente, aparece un mensaje de éxito.
   - Si la operación de SSO no se realiza correctamente, aparece un mensaje de error. Soluciona el problema, borra las cookies del navegador e inténtalo de nuevo.
4. Repite estos pasos para comprobar la conexión de inicio de sesión único (SSO) de cada Admin Node en tu grid.

**PingFederate**

**Pasos**

1. En la página Configurar SSO, selecciona el primer enlace en el mensaje de modo Sandbox.

   Selecciona y comprueba un enlace cada vez.

2. Introduce las credenciales de un usuario federado.
   - Si el inicio de sesión y el cierre de sesión mediante SSO se realizan correctamente, aparece un mensaje de éxito.
   - Si la operación de SSO no se realiza correctamente, aparece un mensaje de error. Soluciona el problema, borra las cookies del navegador e inténtalo de nuevo.
3. Selecciona el siguiente enlace para verificar la conexión de inicio de sesión único para cada Admin Node en tu grid.

   Si aparece el mensaje «Página caducada», selecciona el botón **Atrás** de tu navegador y vuelve a

introducir tus credenciales.

### Habilitar el inicio de sesión único

Cuando hayas comprobado que puedes usar el inicio de sesión único (SSO) para acceder a cada nodo de administración, puedes habilitar el inicio de sesión único para todo tu sistema StorageGRID.

> Cuando el SSO está habilitado, todos los usuarios deben usar el SSO para acceder al Grid Manager, al Tenant Manager, a la Grid Management API y a la Tenant Management API. Los usuarios locales ya no pueden acceder a StorageGRID.

**Pasos**

1. En el paso «Configuración de la prueba» del asistente de configuración de SSO, selecciona **Enable SSO**.
2. Lee el mensaje de advertencia y selecciona **Enable SSO**.

   El inicio de sesión único ya está activado. Aparece la página de inicio de sesión único y ahora incluye los detalles del SSO que acabas de configurar.

3. Para editar la configuración, selecciona **Editar**.
4. Para desactivar el inicio de sesión único, selecciona **Desactivar SSO**.

> Si utilizas el Portal de Azure y accedes a StorageGRID desde el mismo ordenador que usas para acceder a Entra ID, asegúrate de que el usuario del Portal de Azure también sea un usuario autorizado de StorageGRID (un usuario de un grupo federado que se haya importado a StorageGRID) o cierra la sesión del Portal de Azure antes de intentar iniciar sesión en StorageGRID.

## Crea confianzas de terceros en AD FS para StorageGRID

Debes utilizar los Servicios de federación de Active Directory (AD FS) para crear una relación de confianza de parte confiable para cada nodo de administración de tu sistema. Puedes crear relaciones de confianza de parte confiable usando comandos de PowerShell, importando metadatos SAML desde StorageGRID o introduciendo los datos manualmente.

**Antes de empezar**

- ${post_edited_translations.segment}
- Tienes "ha entrado en modo sandbox" en Grid Manager.
- Conoces el nombre de dominio completo (o la dirección IP) y el identificador de la parte de confianza de cada nodo de administración en tu sistema. Puedes encontrar estos valores en la tabla de detalles de los nodos de administración en la página StorageGRID Configure SSO.

  > Debes crear una relación de confianza de parte confiable para cada Admin Node en tu sistema StorageGRID. Contar con una relación de confianza de parte confiable para cada Admin Node garantiza que los usuarios puedan iniciar sesión y cerrar sesión de forma segura en cualquier Admin Node.

- ${post_edited_translations.segment}

- Estás utilizando el complemento de administración de AD FS y perteneces al grupo Administrators.
- ${post_edited_translations.segment}

**Acerca de esta tarea**

Estas instrucciones se aplican a Windows Server 2016 AD FS. Si utilizas una versión diferente de AD FS, notarás ligeras diferencias en el procedimiento. Consulta la documentación de Microsoft AD FS si tienes preguntas.

### Crea una relación de confianza de parte confiable usando Windows PowerShell

Puedes usar Windows PowerShell para crear rápidamente una o más relaciones de confianza con la parte de confianza.

**Pasos**

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

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

   - Para *`Admin_Node_Identifier`*, introduce el identificador de la parte de confianza para el Admin Node, exactamente como aparece en la página de inicio de sesión único. Por ejemplo, `SG-DC1-ADM1`.
   - Para *`Admin_Node_FQDN`*, introduce el nombre de dominio completo para ese mismo nodo de administración. (Si es necesario, puedes usar la dirección IP del nodo en su lugar. Sin embargo, si introduces aquí una dirección IP, ten en cuenta que deberás actualizar o volver a crear esta relación de confianza entre partes si esa dirección IP llega a cambiar.)
3. En el Administrador de servidores de Windows Server, selecciona **Herramientas** > **Administración de AD FS**.

   ${post_edited_translations.segment}

4. Selecciona **AD FS** > **Relying Party Trusts**.

   ${post_edited_translations.segment}

5. Añade una política de control de acceso a la relación de confianza de parte confiable recién creada:
   a. Busca la confianza de la parte confiable que acabas de crear.
   b. Haz clic con el botón derecho del ratón sobre la confianza y selecciona **Editar política de control de acceso**.
   c. Selecciona una política de control de acceso.
   d. ${post_edited_translations.segment}
6. Agrega una directiva de emisión de declaraciones a la nueva relación de confianza de la parte confiable:
   a. Busca la confianza de la parte confiable que acabas de crear.
   b. Haz clic con el botón derecho del ratón sobre la confianza y selecciona **Editar política de emisión de reclamaciones**.
   c. Selecciona **Add rule**.
   d. En la página «Seleccionar plantilla de regla», selecciona **Enviar atributos LDAP como**

**reclamaciones** en la lista y selecciona **Siguiente**.

e. En la página Configurar regla, introduce un nombre para mostrar para esta regla.

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

f. Para el almacén de atributos, selecciona **Active Directory**.

g. En la columna Atributo LDAP de la tabla de asignación, escribe **objectGUID** o selecciona **User-Principal-Name**.

h. En la columna Outgoing Claim Type de la tabla de correspondencias, selecciona **Name ID** en la lista desplegable.

i. Selecciona **Finalizar** y, a continuación, **OK**.

7. Comprueba que los metadatos se hayan importado correctamente.

   a. Haz clic con el botón derecho del ratón sobre la confianza de la parte dependiente para abrir sus propiedades.

   b. Comprueba que los campos de las pestañas **Puntos finales**, **Identificadores** y **Firma** estén rellenados.

      ${post_edited_translations.segment}

8. Repite estos pasos para configurar una relación de confianza de parte confiable para todos los nodos de administración en tu sistema StorageGRID.

9. Cuando hayas terminado, vuelve a StorageGRID y "${post_edited_translations.segment}" para confirmar que están configurados correctamente.

### Crea una relación de confianza con una parte confiable importando metadatos de federación

Puedes importar los valores de cada relación de confianza de la parte que confía accediendo a los metadatos SAML de cada Admin Node.

**Pasos**

1. En el Administrador de servidores de Windows Server, selecciona **Herramientas** y, a continuación, selecciona **Administración de AD FS**.

2. En Acciones, selecciona **Add Relying Party Trust**.

3. En la página de bienvenida, elige **Claims aware** y selecciona **Start**.

4. ${post_edited_translations.segment}

5. En **Dirección de metadatos de la federación (nombre de host o URL)**, escribe la ubicación de los metadatos SAML de este nodo de administración:

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

   Para *`Admin_Node_FQDN`*, introduce el nombre de dominio completo para ese mismo nodo de administración. (Si es necesario, puedes usar la dirección IP del nodo en su lugar. Sin embargo, si introduces aquí una dirección IP, ten en cuenta que deberás actualizar o volver a crear esta relación de confianza entre partes si esa dirección IP llega a cambiar.)

6. ${post_edited_translations.segment}

Al introducir el nombre para mostrar, utiliza el identificador de la parte de confianza del nodo de administración, exactamente como aparece en la página de inicio de sesión único de Grid Manager. Por ejemplo, `SG-DC1-ADM1`.

7. Agrega una regla de reclamación:
   a. Haz clic con el botón derecho del ratón sobre la confianza y selecciona **Editar política de emisión de reclamaciones**.
   b. Selecciona **Add rule**:
   c. En la página «Seleccionar plantilla de regla», selecciona **Enviar atributos LDAP como reclamaciones** en la lista y selecciona **Siguiente**.
   d. En la página Configurar regla, introduce un nombre para mostrar para esta regla.

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

   e. Para el almacén de atributos, selecciona **Active Directory**.
   f. En la columna Atributo LDAP de la tabla de asignación, escribe **objectGUID** o selecciona **User-Principal-Name**.
   g. En la columna Outgoing Claim Type de la tabla de correspondencias, selecciona **Name ID** en la lista desplegable.
   h. Selecciona **Finalizar** y, a continuación, **OK**.
8. Comprueba que los metadatos se hayan importado correctamente.
   a. Haz clic con el botón derecho del ratón sobre la confianza de la parte dependiente para abrir sus propiedades.
   b. Comprueba que los campos de las pestañas **Puntos finales**, **Identificadores** y **Firma** estén rellenados.

      ${post_edited_translations.segment}

9. Repite estos pasos para configurar una relación de confianza de parte confiable para todos los nodos de administración en tu sistema StorageGRID.
10. Cuando hayas terminado, vuelve a StorageGRID y "${post_edited_translations.segment}" para comprobar que están configurados correctamente.

### Crear una relación de confianza de parte confiable manualmente

${post_edited_translations.segment}

**Pasos**

1. En el Administrador de servidores de Windows Server, selecciona **Herramientas** y, a continuación, selecciona **Administración de AD FS**.
2. En Acciones, selecciona **Add Relying Party Trust**.
3. En la página de bienvenida, elige **Claims aware** y selecciona **Start**.
4. Selecciona **Introducir manualmente los datos de la parte confiable** y selecciona **Siguiente**.
5. Completa el asistente de confianza de la parte que confía:

   a. ${post_edited_translations.segment}

Para garantizar la coherencia, utiliza el identificador de la parte de confianza del nodo de administración exactamente como aparece en la página de inicio de sesión único de Grid Manager. Por ejemplo, `SG-DC1-ADM1`.

b. ${post_edited_translations.segment}

c. En la página «Configurar URL», selecciona la casilla **Habilitar compatibilidad con el protocolo WebSSO de SAML 2.0**.

d. Escribe la URL del punto final del servicio SAML para el nodo de administración:

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

Para *`Admin_Node_FQDN`*, introduce el nombre de dominio completo para el Admin Node. (Si es necesario, puedes usar la dirección IP del nodo en su lugar. Sin embargo, si introduces una dirección IP aquí, ten en cuenta que deberás actualizar o volver a crear esta relying party trust si esa dirección IP cambia en algún momento.)

e. En la página Configurar identificadores, especifica el Relying Party Identifier para el mismo Admin Node:

*`Admin_Node_Identifier`*

Para *`Admin_Node_Identifier`*, introduce el identificador de la parte de confianza para el Admin Node, exactamente como aparece en la página de inicio de sesión único. Por ejemplo, `SG-DC1-ADM1`.

f. ${post_edited_translations.segment}

Aparece el cuadro de diálogo «Edit Claim Issuance Policy».

> Si no aparece el cuadro de diálogo, haz clic con el botón derecho sobre la relación de confianza y selecciona **Editar política de emisión de reclamaciones**.

6. ${post_edited_translations.segment}

a. En la página «Seleccionar plantilla de regla», selecciona **Enviar atributos LDAP como reclamaciones** en la lista y selecciona **Siguiente**.

b. En la página Configurar regla, introduce un nombre para mostrar para esta regla.

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

c. Para el almacén de atributos, selecciona **Active Directory**.

d. En la columna Atributo LDAP de la tabla de asignación, escribe **objectGUID** o selecciona **User-Principal-Name**.

e. En la columna Outgoing Claim Type de la tabla de correspondencias, selecciona **Name ID** en la lista desplegable.

f. Selecciona **Finalizar** y, a continuación, **OK**.

7. Haz clic con el botón derecho del ratón sobre la confianza de la parte dependiente para abrir sus propiedades.

8. En la pestaña **Puntos finales**, configura el punto final para el cierre de sesión único (SLO):

a. Selecciona **Add SAML**.

b. ${post_edited_translations.segment}

c. Selecciona **Binding** > **Redirect**.

d. En el campo **URL de confianza**, introduce la URL utilizada para el cierre de sesión único (SLO) desde este Admin Node:

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

Para *Admin_Node_FQDN*, introduce el nombre de dominio completo del nodo de administración. (si es necesario, puedes usar la dirección IP del nodo en su lugar. Sin embargo, si introduces una dirección IP aquí, ten en cuenta que deberás actualizar o volver a crear esta relación de confianza entre partes si esa dirección IP cambia en algún momento).

a. Selecciona **Aceptar**.

9. En la pestaña **Firma**, especifica el certificado de firma para esta relación de confianza de parte confiable:

a. Agrega el certificado personalizado:

- Si dispones del certificado de gestión personalizado que has subido a StorageGRID, selecciona ese certificado.
- Si no tienes el certificado personalizado, inicia sesión en el Admin Node, ve al directorio `/var/local/mgmt-api` del Admin Node y añade el archivo de certificado `custom-server.crt`.

> No se recomienda utilizar el certificado predeterminado del nodo de administración (`server.crt`). Si el nodo de administración falla, el certificado predeterminado se volverá a generar al recuperar el nodo, y será necesario actualizar la confianza de la parte que confía.

b. Selecciona **Aplicar** y selecciona **Aceptar**.

Se guardan y se cierran las propiedades de la parte que confía.

10. Repite estos pasos para configurar una relación de confianza de parte confiable para todos los nodos de administración en tu sistema StorageGRID.
11. Cuando hayas terminado, vuelve a StorageGRID y "${post_edited_translations.segment}" para comprobar que están configurados correctamente.

## Crea aplicaciones empresariales en Entra ID para StorageGRID

Utiliza Entra ID para crear una aplicación empresarial para cada Admin Node en tu sistema.

**Antes de empezar**

- ${post_edited_translations.segment}
- Tienes "ha entrado en modo sandbox" en Grid Manager.
- Tienes el **nombre de la aplicación empresarial** para cada nodo de administración de tu sistema. Puedes copiar estos valores de la tabla de detalles del nodo de administración en la página Configurar SSO.

Debes crear una aplicación empresarial para cada nodo de administración de tu sistema StorageGRID. Contar con una aplicación empresarial para cada nodo de administración garantiza que los usuarios puedan iniciar sesión y cerrar sesión de forma segura en cualquier nodo de administración.

- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- Tienes uno de los siguientes roles en la cuenta de Entra ID: Global Administrator, Cloud Application Administrator, Application Administrator o propietario del service principal.

### Accede a Entra ID

**Pasos**

1. Inicia sesión en el "${post_edited_translations.segment}".
2. Accede a "Entra ID".
3. Selecciona "Aplicaciones empresariales".

### ${post_edited_translations.segment}

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

**Pasos**

1. ${post_edited_translations.segment}
   a. ${post_edited_translations.segment}
   b. Selecciona **Crear tu propia aplicación**.
   c. ${post_edited_translations.segment}
   d. Deja seleccionado el botón de opción **Integrar cualquier otra aplicación que no encuentres en la galería (fuera de la galería)**.
   e. Selecciona **Crear**.
   f. Selecciona el enlace **Empezar** en el recuadro **2. Configura el inicio de sesión único**, o selecciona el enlace **Inicio de sesión único** en el margen izquierdo.
   g. Selecciona la casilla **SAML**.
   h. ${post_edited_translations.segment}
   i. Ve a la página «Configurar SSO» y pega la URL en el campo **URL de metadatos de federación** que corresponde al **Enterprise application name** que usaste.
2. Una vez que hayas pegado la URL de metadatos de la federación para cada nodo de administración y hayas realizado todos los demás cambios necesarios en la configuración de SSO, selecciona **Guardar** en la página Configure SSO.

### ${post_edited_translations.segment}

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

**Pasos**

1. ${post_edited_translations.segment}
   a. Inicia sesión en StorageGRID desde el nodo de administración.
   b. Selecciona **Configuración** > **Control de acceso** > **inicio de sesión único**.
   c. Pulsa el botón para descargar los metadatos SAML de ese nodo de administración.
   d. Guarda el archivo, que luego subirás a Entra ID.

#### Sube los metadatos SAML a cada aplicación empresarial

${post_edited_translations.segment}

**Pasos**

1. Vuelve al Portal de Azure.
2. Repite estos pasos para cada aplicación empresarial:

   > Es posible que tengas que actualizar la página de aplicaciones de Enterprise para ver en la lista las aplicaciones que añadiste anteriormente.

   a. Ve a la página Propiedades de la aplicación empresarial.
   b. Establece **Asignación obligatoria** en **No** (a menos que quieras configurar las asignaciones por separado).
   c. Accede a la página de inicio de sesión único.
   d. Completa la configuración de SAML.
   e. Pulsa el botón **Cargar archivo de metadatos** y selecciona el archivo de metadatos SAML que descargaste para el Admin Node correspondiente.
   f. Una vez que se cargue el archivo, selecciona **Guardar** y luego selecciona **X** para cerrar el panel. Regresarás a la página Configurar el inicio de sesión único con SAML.
3. "Prueba cada aplicación".

## Crea conexiones de proveedores de servicios en PingFederate para StorageGRID

Utilizas PingFederate para crear una conexión de proveedor de servicios (SP) para cada nodo de administración en tu sistema. Para agilizar el proceso, importarás los metadatos SAML desde StorageGRID.

**Antes de empezar**

- Has configurado el inicio de sesión único para StorageGRID y seleccionaste **Ping Federate** como tipo de SSO.
- Tienes "ha entrado en modo sandbox" en Grid Manager.
- Dispones del **ID de conexión SP** de cada nodo de administración de tu sistema. Puedes encontrar estos valores en la tabla de detalles de los nodos de administración en la página Configurar SSO.
- Has descargado los **metadatos SAML** de cada nodo de administración en tu sistema.
- Tienes experiencia creando conexiones de SP en PingFederate Server.
- Tienes el "${post_edited_translations.segment}" para PingFederate Server. La documentación de PingFederate ofrece instrucciones detalladas paso a paso y explicaciones.

- Tienes el "Permiso de administrador" para PingFederate Server.

**Acerca de esta tarea**

Estas instrucciones resumen cómo configurar PingFederate Server versión 10.3 como proveedor de SSO para StorageGRID. Si estás usando otra versión de PingFederate, puede que necesites adaptar estas instrucciones. Consulta la documentación de PingFederate Server para obtener instrucciones detalladas para tu versión.

## Completa los requisitos previos en PingFederate

Antes de poder crear las conexiones SP que utilizarás para StorageGRID, debes completar las tareas previas en PingFederate. Utilizarás la información de estos requisitos previos cuando configures las conexiones SP.

#### ${post_edited_translations.segment}

Si aún no lo has hecho, crea un almacén de datos para conectar PingFederate al servidor LDAP de AD FS. Utiliza los valores que usaste al "${post_edited_translations.segment}" en StorageGRID.

- ${post_edited_translations.segment}
- **Tipo de LDAP**: Active Directory
- **Nombre del atributo binario**: Introduce **objectGUID** en la pestaña de atributos binarios de LDAP exactamente como se muestra.

#### ${post_edited_translations.segment}

Si aún no lo has hecho, crea un validador de credenciales de contraseña.

- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- **Filtro de búsqueda**: sAMAccountName=${username}
- ${post_edited_translations.segment}

#### ${post_edited_translations.segment}

${post_edited_translations.segment}

**Pasos**

1. Ve a **Autenticación** > **Integración** > **Adaptadores de IdP**.
2. Selecciona **Crear nueva instancia**.
3. En la pestaña Tipo, selecciona **HTML Form IdP Adapter**.
4. En la pestaña «Adaptador IdP», selecciona **Add a new row to 'Credential Validators'**.
5. Selecciona el ${post_edited_translations.segment} que creaste.
6. En la pestaña «Atributos del adaptador», selecciona el atributo **username** para **Pseudonym**.
7. Selecciona **Guardar**.

#### Crear o importar un certificado de firma

Si aún no lo has hecho, crea o importa el certificado de firma.

**Pasos**

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}

### Crea una conexión de SP en PingFederate

Al crear una conexión SP en PingFederate, debes importar los metadatos SAML que descargaste de StorageGRID para el nodo de administración. El archivo de metadatos contiene muchos de los valores específicos que necesitas.

> Debes crear una conexión de SP para cada nodo de administración en tu sistema StorageGRID, de modo que los usuarios puedan iniciar y cerrar sesión de forma segura en cualquier nodo. Usa estas instrucciones para crear la primera conexión de SP. Luego, ve a Crear conexiones SP adicionales para crear las conexiones adicionales que necesites.

#### ${post_edited_translations.segment}

**Pasos**

1. Ve a **Aplicaciones** > **Integración** > **Conexiones SP**.
2. Selecciona **Crear conexión**.
3. ${post_edited_translations.segment}
4. Selecciona **Perfiles de SSO del navegador** y **SAML 2.0** como el protocolo.

#### Importar metadatos de SP

**Pasos**

1. En la pestaña «Importar metadatos», selecciona **File**.
2. Selecciona el archivo de metadatos SAML que descargaste desde la página Configurar SSO para el nodo de administración.
3. Revisa el resumen de metadatos y la información que aparece en la pestaña General Info.

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

4. Selecciona **Siguiente**.

#### Configura el inicio de sesión único (SSO) del IdP en el navegador

**Pasos**

1. En la pestaña SSO del navegador, selecciona **Configurar SSO del navegador**.
2. En la pestaña «Perfiles SAML», selecciona las opciones **SSO iniciado por el SP**, **SLO iniciado por el SP**, **SSO iniciado por el IdP** y **SLO iniciado por el IdP**.
3. Selecciona **Siguiente**.
4. En la pestaña «Duración de la afirmación», no hagas ningún cambio.
5. En la pestaña «Creación de aserciones», selecciona **Configurar la creación de aserciones**.
   a. En la pestaña Asignación de identidad, selecciona **Estándar**.

b. En la pestaña «Contrato de atributos», usa **SAML_SUBJECT** como contrato de atributos y el formato de nombre no especificado que se importó.

6. Para "Extend the Contract", selecciona **Eliminar** para quitar el `urn:oid`, que no se usa.

#### Instancia del adaptador de mapas

**Pasos**

1. ${post_edited_translations.segment}
2. En la pestaña Adapter instance, selecciona el instancia del adaptador que creaste.
3. En la pestaña «Método de asignación», selecciona **Recuperar atributos adicionales de un almacén de datos**.
4. En la pestaña «Fuente de atributos y búsqueda de usuarios», selecciona **Add Attribute Source**.
5. En la pestaña Data Store, proporciona una descripción y selecciona el almacén de datos que añadiste.
6. En la pestaña «Búsqueda en el directorio LDAP»:
   - ${post_edited_translations.segment}
   - Para el Search Scope, selecciona **Subtree**.
   - En la clase de objeto raíz, busca y añade cualquiera de estos atributos: **objectGUID** o **userPrincipalName**.
7. En la pestaña «Tipos de codificación de atributos binarios LDAP», selecciona **Base64** para el atributo **objectGUID**.
8. En la pestaña «Filtro LDAP», introduce **sAMAccountName=${username}**.
9. En la pestaña «Cumplimiento del contrato de atributos», selecciona **LDAP (atributo)** en el menú desplegable «Origen» y selecciona **objectGUID** o **userPrincipalName** en el menú desplegable «Valor».
10. ${post_edited_translations.segment}
11. En la pestaña «Failsave Attribute Source», selecciona **Abort the SSO Transaction**.
12. ${post_edited_translations.segment}
13. Selecciona **Hecho**.

#### Configura los ajustes del protocolo

**Pasos**

1. ${post_edited_translations.segment}
2. En la pestaña «URL del servicio de consumidor de aserciones», acepta los valores predeterminados, que se importaron de los metadatos SAML de StorageGRID (**POST** para Binding y `/api/saml-response` para Endpoint URL).
3. En la pestaña «URL de servicio SLO», acepta los valores predeterminados, que se importaron de los metadatos SAML de StorageGRID (**REDIRECT** para Binding y `/api/saml-logout` para Endpoint URL.
4. En la pestaña «Enlaces SAML permitidos», desmarca **ARTIFACT** y **SOAP**. Solo son obligatorios **POST** y **REDIRECT**.
5. ${post_edited_translations.segment}
6. ${post_edited_translations.segment}
7. Revisa el resumen y selecciona **Hecho** para guardar la configuración del protocolo.
8. Revisa el resumen y selecciona **Hecho** para guardar la configuración de SSO del navegador.

#### Configura credenciales

**Pasos**

1. ${post_edited_translations.segment}
2. En la pestaña «Credenciales», selecciona **Configurar credenciales**.
3. Selecciona el ${post_edited_translations.segment} que creaste o importaste.
4. ${post_edited_translations.segment}
   a. En la pestaña Trust Model, selecciona **Unanchored**.
   b. En la pestaña «Certificado de verificación de firma», revisa la información del certificado de firma, que se importó desde los metadatos SAML de StorageGRID.
5. Revisa las pantallas de resumen y selecciona **Guardar** para guardar la conexión SP.

#### Crear conexiones SP adicionales

Puedes copiar la primera conexión SP para crear las conexiones SP que necesites para cada Admin Node en tu grid. Subes nuevos metadatos para cada copia.

> Las conexiones SP para los distintos nodos de administración utilizan una configuración idéntica, salvo en lo que respecta al Partner's Entity ID, la Base URL, el Connection ID, el Connection Name, la verificación de la firma y la SLO Response URL.

**Pasos**

1. Selecciona **Acción** > **Copiar** para crear una copia de la conexión SP inicial para cada Admin Node adicional.
2. ${post_edited_translations.segment}
3. Selecciona el archivo de metadatos correspondiente al nodo de administración:
   a. Selecciona **Action** > **Actualizar con metadatos**.
   b. Selecciona **Elegir archivo** y sube los metadatos.
   c. Selecciona **Siguiente**.
   d. Selecciona **Guardar**.
4. Soluciona el error provocado por el atributo no utilizado:
   a. Selecciona la nueva conexión.
   b. Selecciona **Configurar SSO del navegador > Configurar la creación de aserciones > Contrato de atributos**.
   c. ${post_edited_translations.segment}
   d. Selecciona **Guardar**.

## Desactiva el inicio de sesión único en StorageGRID

Puedes desactivar el inicio de sesión único (SSO) si ya no quieres usar esta funcionalidad. Debes desactivar el inicio de sesión único antes de poder desactivar la federación de identidades.

#### Antes de empezar

- Has iniciado sesión en Grid Manager mediante un "navegador web compatible".

- Tienes "permisos de acceso específicos".

**Pasos**

1. Selecciona **Configuración** > **Control de acceso** > **inicio de sesión único**.

   Aparece la página de inicio de sesión único.

2. Selecciona **Desactivar SSO**.
3. Selecciona **Sí**.

   Aparece un mensaje de aviso en el que se indica que los usuarios locales ahora podrán iniciar sesión.

La próxima vez que inicies sesión en StorageGRID, aparece la página de Sign in de StorageGRID y debes introducir el nombre de usuario y la contraseña de un usuario local o federado de StorageGRID.

## Deshabilita temporalmente y vuelve a habilitar SSO para un nodo de administración StorageGRID

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

**Antes de empezar**

- Tienes "permisos de acceso específicos".
- Tienes el archivo `Passwords.txt`.
- Conoces la contraseña del usuario raíz local.

**Acerca de esta tarea**

Después de deshabilitar el SSO para un nodo de administración, puedes iniciar sesión en el Grid Manager como el usuario raíz local. Para proteger tu sistema StorageGRID, debes usar el shell de comandos del nodo para volver a habilitar el SSO en el nodo de administración tan pronto como cierres sesión.

> Desactivar el SSO en un nodo de administración no afecta la configuración del SSO de los demás nodos de administración en la grid. La casilla **Habilitar SSO** en la página de inicio de sesión único en el Grid Manager permanece seleccionada y todos los ajustes de SSO existentes se mantienen a menos que los actualices.

**Pasos**

1. Inicia sesión en un nodo de administración:
   a. Introduce el siguiente comando: `ssh admin@Admin_Node_IP`
   b. Introduce la contraseña que figura en el archivo `Passwords.txt`.
   c. Introduce el siguiente comando para pasar a ser usuario root: `su -`
   d. Introduce la contraseña que figura en el archivo `Passwords.txt`.

      Cuando inicias sesión como root, el indicador cambia de `$` a `#`.

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

   Un mensaje indica que el comando solo se aplica a este Admin Node.

3. ${post_edited_translations.segment}

   Aparece un mensaje que indica que el inicio de sesión único está desactivado en el nodo.

4. Desde un navegador web, accede al Grid Manager en el mismo nodo de administración.

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

5. ${post_edited_translations.segment}
6. Si has desactivado temporalmente el SSO porque tenías que corregir la configuración del SSO:
   a. Selecciona **Configuración** > **Control de acceso** > **inicio de sesión único**.
   b. ${post_edited_translations.segment}
   c. Selecciona **Guardar**.

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

7. Si has desactivado temporalmente el SSO porque necesitabas acceder al Grid Manager por cualquier otro motivo:
   a. ${post_edited_translations.segment}
   b. Selecciona **Cerrar sesión** y cierra el Grid Manager.
   c. Vuelve a activar el SSO en el nodo de administración. Puedes seguir cualquiera de los siguientes pasos:

      - Ejecuta el siguiente comando: `enable-saml`

        Un mensaje indica que el comando solo se aplica a este Admin Node.

      Confirma que deseas activar el inicio de sesión único.

   Aparece un mensaje que indica que el inicio de sesión único está activado en el nodo.

      ◦ Reinicia el nodo de grid: `reboot`

8. ${post_edited_translations.segment}
9. Comprueba que aparece la página de Sign in de StorageGRID y que debes introducir tus credenciales de SSO para acceder a Grid Manager.