Gestione el acceso al sistema

StorageGRID

NetApp
April 10, 2024

Tabla de contenidos

Gestione el acceso al sistema

Usar la federación de identidades

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

Configurar la federación de identidades para el Administrador de inquilinos

Puede configurar la federación de identidades para el administrador de inquilinos si desea que los grupos de inquilinos y los usuarios se gestionen en otro sistema como Active Directory, Azure Active Directory (Azure AD), OpenLDAP u Oracle Directory Server.

Lo que necesitará

- Ha iniciado sesión en el administrador de inquilinos mediante un navegador web compatible.
- Tiene permisos de acceso específicos.
- Se utiliza Active Directory, Azure AD, OpenLDAP u Oracle Directory Server como proveedor de identidades.

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

- Si planea utilizar OpenLDAP, debe configurar el servidor OpenLDAP. Consulte Instrucciones para configurar el servidor OpenLDAP.
- Si planea utilizar la seguridad de la capa de transporte (TLS) para las comunicaciones con el servidor LDAP, el proveedor de identidades debe usar TLS 1.2 o 1.3. Consulte Cifrados compatibles para conexiones TLS salientes.

Acerca de esta tarea

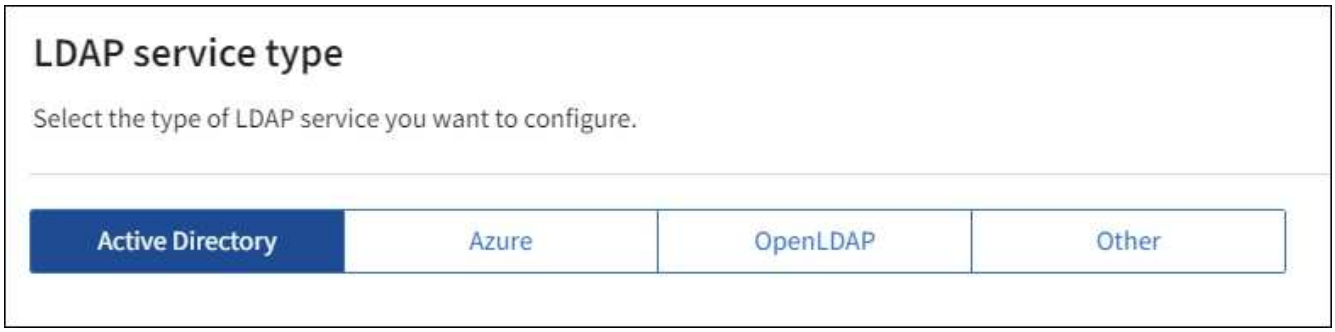
Si puede configurar un servicio de federación de identidades para su inquilino depende de cómo se haya configurado su cuenta de inquilino. Es posible que el inquilino comparta el servicio de federación de identidades configurado para Grid Manager. Si ve este mensaje al acceder a la página Federación de identidades, no podrá configurar un origen de identidad federado independiente para este arrendatario.

> This tenant account uses the LDAP server that is configured for the Grid Manager. Contact the grid administrator for information or to change this setting.

Introducir configuración

Pasos

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



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

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

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

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

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

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

     - `sAMAccountName` o. `uid`

- `objectGUID`, `entryUUID`, o. `nsuniqueid`
- `cn`
- `memberOf` o. `isMemberOf`
- **Active Directory**: `objectSid`, `primaryGroupID`, `userAccountControl`, y. `userPrincipalName`
- **Azure**: `accountEnabled` y.. `userPrincipalName`

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

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

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

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

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

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

  Introduzca uno de estos patrones:

  - **Patrón UserPrincipalName (Active Directory y Azure)**: `[USERNAME]@`*`example`*`.com`
  - **Patrón de nombre de inicio de sesión de nivel inferior (Active Directory y Azure)**: *`example`*`\[USERNAME]`
  - **Patrón de nombre completo**: `CN=[USERNAME],CN=Users,DC=`*`example`*`,DC=com`

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

6. En la sección Seguridad de la capa de transporte (TLS), seleccione una configuración de seguridad.
   - **Use STARTTLS**: Utilice STARTTLS para asegurar las comunicaciones con el servidor LDAP. Esta es la opción recomendada para Active Directory, OpenLDAP u otros, pero esta opción no es compatible con Azure.
   - **Use LDAPS**: La opción LDAPS (LDAP sobre SSL) utiliza TLS para establecer una conexión con el servidor LDAP. Debe seleccionar esta opción para Azure.
   - **No utilice TLS**: El tráfico de red entre el sistema StorageGRID y el servidor LDAP no estará protegido. Esta opción no es compatible con Azure.

> El uso de la opción **no usar TLS** no es compatible si el servidor de Active Directory aplica la firma LDAP. Debe usar STARTTLS o LDAPS.

7. Si seleccionó STARTTLS o LDAPS, elija el certificado utilizado para proteger la conexión.
    - **Utilizar certificado CA del sistema operativo**: Utilice el certificado predeterminado de CA de red instalado en el sistema operativo para asegurar las conexiones.
    - **Utilizar certificado de CA personalizado**: Utilice un certificado de seguridad personalizado.

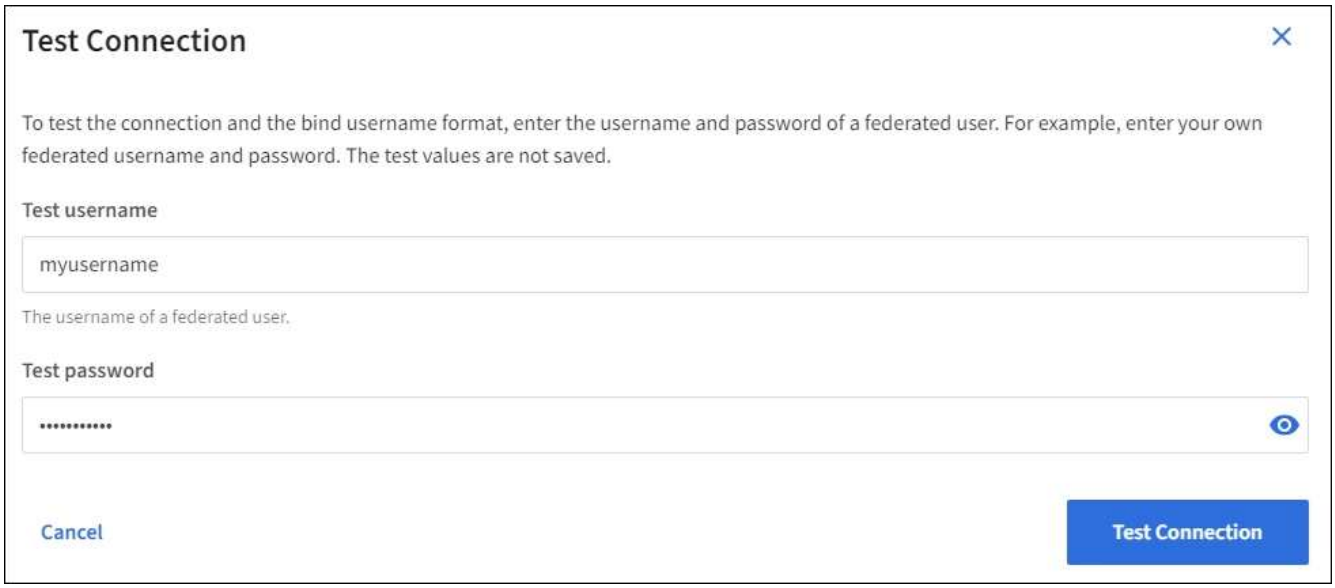
      Si selecciona esta opción, copie y pegue el certificado de seguridad personalizado en el cuadro de texto del certificado de CA.

Pruebe la conexión y guarde la configuración

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

1. Seleccione **probar conexión**.
2. Si no se proporciona un formato de nombre de usuario de enlace:
    - Aparecerá el mensaje «"probar conexión correcta"» si los ajustes de conexión son válidos. Seleccione **Guardar** para guardar la configuración.
    - Aparece el mensaje «"no se ha podido establecer la conexión de prueba"» si los ajustes de conexión no son válidos. Seleccione **Cerrar**. Luego, resuelva cualquier problema y vuelva a probar la conexión.
3. Si proporcionó un formato de nombre de usuario de enlace, introduzca el nombre de usuario y la contraseña de un usuario federado válido.

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



    - Aparecerá el mensaje «"probar conexión correcta"» si los ajustes de conexión son válidos. Seleccione **Guardar** para guardar la configuración.
    - Aparecerá un mensaje de error si las opciones de conexión, el formato de nombre de usuario de enlace o el nombre de usuario y la contraseña de prueba no son válidos. Resuelva los problemas y vuelva a probar la conexión.

Forzar la sincronización con el origen de identidades

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

Pasos

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

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

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

Deshabilitar la federación de identidades

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

Acerca de esta tarea

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

- Los usuarios federados no podrán iniciar sesión.
- Los usuarios federados que hayan iniciado sesión en ese momento, retendrán el acceso al sistema StorageGRID hasta que caduque la sesión, pero no podrán iniciar sesión después de que caduque la sesión.
- No se realizará la sincronización entre el sistema StorageGRID y el origen de identidad, y no se realizarán alertas ni alarmas para las cuentas que no se hayan sincronizado.
- La casilla de verificación **Activar federación de identidades** está desactivada si el inicio de sesión único (SSO) está establecido en **activado** o **modo Sandbox**. El estado de SSO de la página Single Sign-On debe ser **Desactivado** antes de poder deshabilitar la federación de identidades. Consulte Desactive el inicio de sesión único.

Pasos

1. Vaya a la página federación de identidades.
2. Desactive la casilla de verificación **Activar federación de identidades**.

Instrucciones para configurar el servidor OpenLDAP

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

> Para los orígenes de identidad que no son ActiveDirectory ni Azure, StorageGRID no bloqueará automáticamente el acceso S3 a los usuarios que estén deshabilitados externamente. Para bloquear el acceso a S3, elimine cualquier clave S3 del usuario y quite el usuario de todos los grupos.

Revestimientos memberOf y reft

Se deben habilitar las superposiciones memberof y reft. Para obtener más información, consulte las instrucciones para el mantenimiento de miembros del grupo inverso enhttp://www.openldap.org/doc/admin24/index.html["Documentación de OpenLDAP: Guía del administrador de la versión 2.4"^].

Indización

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

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

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

Consulte la información sobre el mantenimiento de pertenencia a grupos inversa en lahttp://www.openldap.org/doc/admin24/index.html["Documentación de OpenLDAP: Guía del administrador de la versión 2.4"^].

Gestionar grupos

Cree grupos para un inquilino de S3

Es posible gestionar permisos para grupos de usuarios S3 importando grupos federados o creando grupos locales.

Lo que necesitará

- Debe iniciar sesión en el administrador de inquilinos mediante un navegador web compatible.
- Debe pertenecer a un grupo de usuarios que tenga el permiso acceso raíz. Consulte Permisos de gestión de inquilinos.
- Si planea importar un grupo federado, ha configurado la federación de identidades y el grupo federado ya existe en el origen de identidades configurado.

Para obtener más información sobre S3, consulte Use S3.

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO** > **grupos**.

2. Seleccione **Crear grupo**.
3. Seleccione la ficha **Grupo local** para crear un grupo local o seleccione la ficha **Grupo federado** para importar un grupo desde el origen de identidad configurado previamente.

   Si se ha habilitado el inicio de sesión único (SSO) para el sistema StorageGRID, los usuarios que pertenecen a grupos locales no podrán iniciar sesión en el Gestor de inquilinos, aunque puedan utilizar las aplicaciones cliente para gestionar los recursos del inquilino, en función de los permisos de grupo.

4. Introduzca el nombre del grupo.
   - **Grupo local**: Introduzca tanto un nombre para mostrar como un nombre exclusivo. Puede editar el nombre para mostrar más adelante.
   - **Grupo federado**: Introduzca el nombre único. Para Active Directory, el nombre único es el nombre asociado con `sAMAccountName` atributo. Para OpenLDAP, el nombre único es el nombre asociado con `uid` atributo.
5. Seleccione **continuar**.
6. Seleccione un modo de acceso. Si un usuario pertenece a varios grupos y cualquier grupo está establecido en sólo lectura, el usuario tendrá acceso de sólo lectura a todos los ajustes y características seleccionados.
   - **Read-write** (valor predeterminado): Los usuarios pueden iniciar sesión en el Administrador de inquilinos y administrar la configuración de arrendatario.
   - **Sólo lectura**: Los usuarios sólo pueden ver los ajustes y las funciones. No pueden realizar cambios ni realizar ninguna operación en el Administrador de inquilinos ni en la API de gestión de inquilinos. Los usuarios locales de solo lectura pueden cambiar sus propias contraseñas.
7. Seleccione los permisos de grupo para este grupo.

   Consulte la información sobre los permisos de administración de inquilinos.

8. Seleccione **continuar**.
9. Seleccione una política de grupo para determinar qué permisos de acceso S3 tendrán los miembros de este grupo.

- **Sin acceso S3**: Predeterminado. Los usuarios de este grupo no tienen acceso a los recursos de S3, a menos que se conceda el acceso mediante una política de bloques. Si selecciona esta opción, de forma predeterminada, solo el usuario raíz tendrá acceso a recursos de S3.
- **Acceso de sólo lectura**: Los usuarios de este grupo tienen acceso de sólo lectura a los recursos S3. Por ejemplo, los usuarios de este grupo pueden enumerar objetos y leer datos de objetos, metadatos y etiquetas. Cuando selecciona esta opción, la cadena JSON para una política de grupo de solo lectura aparece en el cuadro de texto. No puede editar esta cadena.
- **Acceso completo**: Los usuarios de este grupo tienen acceso completo a los recursos S3, incluidos los bloques. Cuando selecciona esta opción, la cadena JSON para una política de grupo de acceso completo aparece en el cuadro de texto. No puede editar esta cadena.
- **Personalizado**: A los usuarios del grupo se les conceden los permisos que especifique en el cuadro de texto. Consulte las instrucciones para implementar una aplicación cliente S3 para obtener información detallada acerca de las políticas de grupo, incluidos la sintaxis del idioma y ejemplos.

10. Si ha seleccionado **personalizado**, introduzca la directiva de grupo. Cada política de grupo tiene un límite de tamaño de 5,120 bytes. Debe introducir una cadena con formato JSON válida.

    En este ejemplo, sólo se permite a los miembros del grupo enumerar y acceder a una carpeta que coincida con su nombre de usuario (prefijo de clave) en el bloque especificado. Tenga en cuenta que los permisos de acceso de otras políticas de grupo y la directiva de bloque deben tenerse en cuenta al determinar la privacidad de estas carpetas.

11. Seleccione el botón que aparece, dependiendo de si está creando un grupo federado o un grupo local:

    - Grupo federado: **Crear grupo**
    - Grupo local: **Continuar**

    Si está creando un grupo local, el paso 4 (Agregar usuarios) aparece después de seleccionar **continuar**.

Este paso no aparece para grupos federados.

12. Seleccione la casilla de verificación de cada usuario que desee agregar al grupo y, a continuación, seleccione **Crear grupo**.

    Opcionalmente, puede guardar el grupo sin agregar usuarios. Puede agregar usuarios al grupo más tarde o seleccionar el grupo cuando agregue nuevos usuarios.

13. Seleccione **Finalizar**.

    El grupo creado aparece en la lista de grupos. Los cambios pueden tardar hasta 15 minutos en surtir efecto debido al almacenamiento en caché.

Cree grupos para un inquilino de Swift

Es posible gestionar los permisos de acceso para una cuenta de inquilino de Swift mediante la importación de grupos federados o la creación de grupos locales. Al menos un grupo debe tener el permiso de administrador de Swift, que se requiere para gestionar los contenedores y los objetos de una cuenta de inquilino de Swift.

Lo que necesitará

- Debe iniciar sesión en el administrador de inquilinos mediante un navegador web compatible.
- Debe pertenecer a un grupo de usuarios que tenga el permiso acceso raíz.
- Si planea importar un grupo federado, ha configurado la federación de identidades y el grupo federado ya existe en el origen de identidades configurado.

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO** > **grupos**.

2. Seleccione **Crear grupo**.
3. Seleccione la ficha **Grupo local** para crear un grupo local o seleccione la ficha **Grupo federado** para

importar un grupo desde el origen de identidad configurado previamente.

Si se ha habilitado el inicio de sesión único (SSO) para el sistema StorageGRID, los usuarios que pertenecen a grupos locales no podrán iniciar sesión en el Gestor de inquilinos, aunque puedan utilizar las aplicaciones cliente para gestionar los recursos del inquilino, en función de los permisos de grupo.

4. Introduzca el nombre del grupo.
   - **Grupo local**: Introduzca tanto un nombre para mostrar como un nombre exclusivo. Puede editar el nombre para mostrar más adelante.
   - **Grupo federado**: Introduzca el nombre único. Para Active Directory, el nombre único es el nombre asociado con `sAMAccountName` atributo. Para OpenLDAP, el nombre único es el nombre asociado con `uid` atributo.
5. Seleccione **continuar**.
6. Seleccione un modo de acceso. Si un usuario pertenece a varios grupos y cualquier grupo está establecido en sólo lectura, el usuario tendrá acceso de sólo lectura a todos los ajustes y características seleccionados.
   - **Read-write** (valor predeterminado): Los usuarios pueden iniciar sesión en el Administrador de inquilinos y administrar la configuración de arrendatario.
   - **Sólo lectura**: Los usuarios sólo pueden ver los ajustes y las funciones. No pueden realizar cambios ni realizar ninguna operación en el Administrador de inquilinos ni en la API de gestión de inquilinos. Los usuarios locales de solo lectura pueden cambiar sus propias contraseñas.
7. Establezca el permiso Grupo.
   - Active la casilla de verificación **acceso raíz** si los usuarios necesitan iniciar sesión en el Administrador de inquilinos o la API de administración de inquilinos. (Predeterminado)
   - Anule la selección de la casilla de verificación **acceso raíz** si los usuarios no necesitan acceso al Administrador de inquilinos o a la API de administración de inquilinos. Por ejemplo, anule la selección de la casilla de verificación de las aplicaciones que no necesitan acceder al arrendatario. A continuación, asigne el permiso **Swift Administrator** para permitir que estos usuarios administren contenedores y objetos.
8. Seleccione **continuar**.
9. Active la casilla de verificación **Swift Administrator** si el usuario necesita poder utilizar la API de REST de Swift.

   Los usuarios de Swift deben tener el permiso acceso raíz para acceder al Administrador de inquilinos. Sin embargo, el permiso Root Access no permite que los usuarios se autentiquen en la API DE REST de Swift para crear contenedores y procesar objetos. Los usuarios deben tener el permiso de administrador de Swift para autenticarse en la API DE REST de Swift.

10. Seleccione el botón que aparece, dependiendo de si está creando un grupo federado o un grupo local:
    - Grupo federado: **Crear grupo**
    - Grupo local: **Continuar**

      Si está creando un grupo local, el paso 4 (Agregar usuarios) aparece después de seleccionar **continuar**. Este paso no aparece para grupos federados.

11. Seleccione la casilla de verificación de cada usuario que desee agregar al grupo y, a continuación, seleccione **Crear grupo**.

    Opcionalmente, puede guardar el grupo sin agregar usuarios. Puede agregar usuarios al grupo más tarde

o seleccionar el grupo cuando cree nuevos usuarios.

12. Seleccione **Finalizar**.

    El grupo creado aparece en la lista de grupos. Los cambios pueden tardar hasta 15 minutos en surtir efecto debido al almacenamiento en caché.

Información relacionada

Permisos de gestión de inquilinos

Use Swift

Permisos de gestión de inquilinos

Antes de crear un grupo de arrendatarios, tenga en cuenta qué permisos desea asignar a ese grupo. Los permisos de administración de inquilinos determinan qué tareas pueden realizar los usuarios con el Administrador de inquilinos o la API de gestión de inquilinos. Un usuario puede pertenecer a uno o más grupos. Los permisos son acumulativos si un usuario pertenece a varios grupos.

Para iniciar sesión en el Administrador de arrendatarios o utilizar la API de administración de arrendatarios, los usuarios deben pertenecer a un grupo que tenga al menos un permiso. Todos los usuarios que puedan iniciar sesión pueden realizar las siguientes tareas:

- Vea la consola
- Cambiar su propia contraseña (para usuarios locales)

Para todos los permisos, la configuración del modo de acceso del grupo determina si los usuarios pueden cambiar la configuración y realizar operaciones o si sólo pueden ver la configuración y las características relacionadas.

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

Puede asignar los siguientes permisos a un grupo. Tenga en cuenta que los inquilinos de S3 y los inquilinos de Swift tienen diferentes permisos de grupo. Los cambios pueden tardar hasta 15 minutos en surtir efecto debido al almacenamiento en caché.

Permiso	Descripción
Acceso raíz	Proporciona acceso completo al administrador de inquilinos y a la API de gestión de inquilinos. **Nota:** los usuarios de Swift deben tener permiso acceso raíz para iniciar sesión en la cuenta de arrendatario.
Administrador	Solo para inquilinos Swift. Proporciona acceso completo a los contenedores y objetos de Swift para esta cuenta de inquilino **Nota:** los usuarios de Swift deben tener el permiso de Administrador de Swift para realizar cualquier operación con la API de REST de Swift.

Permiso	Descripción
Gestione sus propias credenciales de S3	Solo inquilinos de S3. Permite a los usuarios crear y eliminar sus propias claves de acceso S3. Los usuarios que no tienen este permiso no ven la opción de menú **STORAGE (S3)** > **My S3 access keys**.
Administrar todos los depósitos	• Inquilinos S3: Permite a los usuarios usar el administrador de inquilinos y la API de gestión de inquilinos para crear y eliminar bloques S3, así como para gestionar la configuración de todos los bloques de S3 de la cuenta del inquilino, independientemente de las políticas de grupo o bloque de S3. Los usuarios que no tienen este permiso no ven la opción de menú **Cuchos**. • Inquilinos Swift: Permite a los usuarios de Swift controlar el nivel de coherencia de los contenedores Swift mediante la API de gestión de inquilinos. **Nota:** sólo puede asignar el permiso Administrar todos los cucharones a grupos Swift desde la API de gestión de inquilinos. No puede asignar este permiso a grupos Swift mediante el administrador de inquilinos.
Gestionar extremos	Solo inquilinos de S3. Permite a los usuarios usar el administrador de inquilinos o la API de gestión de inquilinos crear o editar extremos que se usan como destino de los servicios de plataforma StorageGRID. Los usuarios que no tienen este permiso no ven la opción de menú **terminales de servicios de plataforma**.

Información relacionada

Use S3

Use Swift

Ver y editar detalles del grupo

Al ver los detalles de un grupo, puede cambiar el nombre para mostrar del grupo, los permisos, las directivas y los usuarios que pertenecen al grupo.

Lo que necesitará

- Debe iniciar sesión en el administrador de inquilinos mediante un navegador web compatible.
- Debe pertenecer a un grupo de usuarios que tenga el permiso acceso raíz.

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO** > **grupos**.
2. Seleccione el nombre del grupo cuyos detalles desee ver o editar.

   También puede seleccionar **acciones** > **Ver detalles del grupo**.

   Aparece la página de detalles del grupo. En el siguiente ejemplo, se muestra la página de detalles del grupo S3.

Groups > Applications

Overview

Display name:	**Applications**
Unique name:	**group/Applications**
Type:	**Local**
Access mode:	**Read-write**
Permissions:	**Root Access**
S3 Policy:	**None**
Number of users in this group:	**0**

Group permissions | S3 group policy | Users

Manage group permissions

Select an access mode for this group and select one or more permissions.

Access mode

Select whether users can change settings and perform operations or whether they can only view settings and features.

(●) Read-write ( ) Read-only

Group permissions

Select the tenant account permissions you want to assign to this group.

[x] **Root Access**

Allows users to access all Tenant Manager features. Root Access permission supersedes all other permissions.

[x] **Manage All Buckets**

Allows users to change settings of all S3 buckets (or Swift containers) in this account.

[x] **Manage Endpoints**

Allows users to configure endpoints for platform services.

[x] **Manage Your Own S3 Credentials**

Allows users to create and delete their own S3 access keys.

Save changes

3. Realice cambios en la configuración del grupo según sea necesario.

> Para asegurarse de que se guardan los cambios, seleccione **Guardar cambios** después de realizar cambios en cada sección. Cuando se guarden los cambios, aparecerá un mensaje de confirmación en la esquina superior derecha de la página.

   a. De forma opcional, seleccione el nombre para mostrar o el icono de edición para actualizar el nombre para mostrar.

      No se puede cambiar el nombre exclusivo de un grupo. No se puede editar el nombre para mostrar de un grupo federado.

   b. Si lo desea, actualice los permisos.

   c. Para la política de grupo, realice los cambios adecuados para su inquilino S3 o Swift.

      - Si va a editar un grupo para un inquilino de S3, seleccione de forma opcional una política de grupo S3 diferente. Si selecciona una política de S3 personalizada, actualice la cadena JSON según sea necesario.
      - Si está editando un grupo para un inquilino Swift, también puede activar o desactivar la casilla de verificación **Swift Administrator**.

        Para obtener más información sobre el permiso de administrador de Swift, consulte las instrucciones para crear grupos para un inquilino Swift.

   d. Opcionalmente, agregue o elimine usuarios.

4. Confirme que ha seleccionado **Guardar cambios** para cada sección que haya cambiado.

   Los cambios pueden tardar hasta 15 minutos en surtir efecto debido al almacenamiento en caché.

Información relacionada

Cree grupos para el inquilino de S3

Cree grupos para el inquilino Swift

Agregar usuarios a un grupo local

Puede agregar usuarios a un grupo local según sea necesario.

Lo que necesitará

- Debe iniciar sesión en el administrador de inquilinos mediante un navegador web compatible.
- Debe pertenecer a un grupo de usuarios que tenga el permiso acceso raíz.

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO** > **grupos**.
2. Seleccione el nombre del grupo local al que desea añadir usuarios.

   También puede seleccionar **acciones** > **Ver detalles del grupo**.

   Aparece la página de detalles del grupo.

Groups > Applications

Overview

Display name:	**Applications**
Unique name:	**group/Applications**
Type:	**Local**
Access mode:	**Read-write**
Permissions:	**Root Access**
S3 Policy:	**None**
Number of users in this group:	**0**

Group permissions | S3 group policy | Users

Manage group permissions

Select an access mode for this group and select one or more permissions.

Access mode

Select whether users can change settings and perform operations or whether they can only view settings and features.

(●) Read-write ( ) Read-only

Group permissions

Select the tenant account permissions you want to assign to this group.

[x] **Root Access**

Allows users to access all Tenant Manager features. Root Access permission supersedes all other permissions.

[x] **Manage All Buckets**

Allows users to change settings of all S3 buckets (or Swift containers) in this account.

[x] **Manage Endpoints**

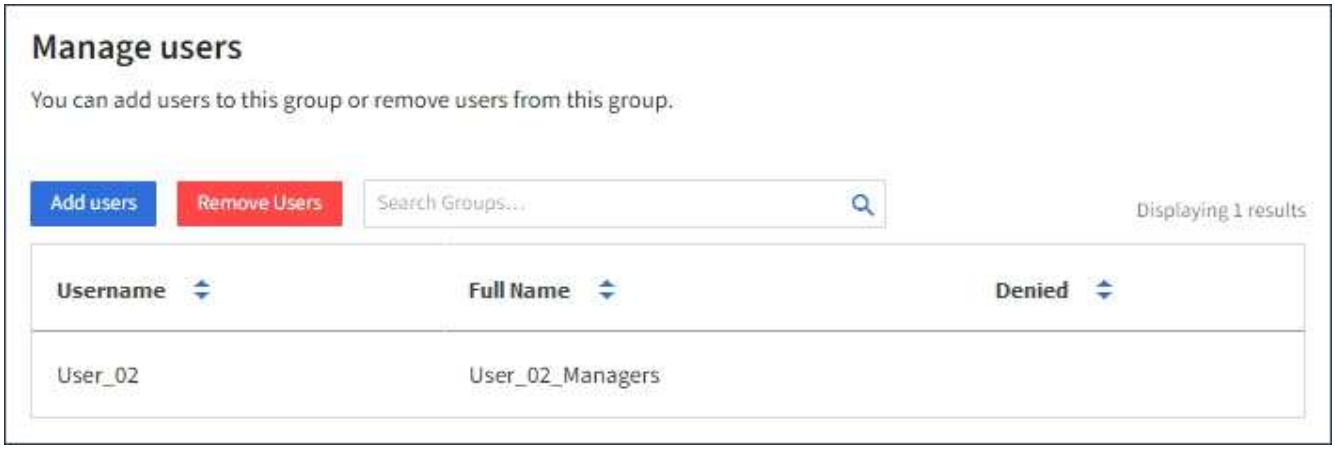
Allows users to configure endpoints for platform services.

[x] **Manage Your Own S3 Credentials**

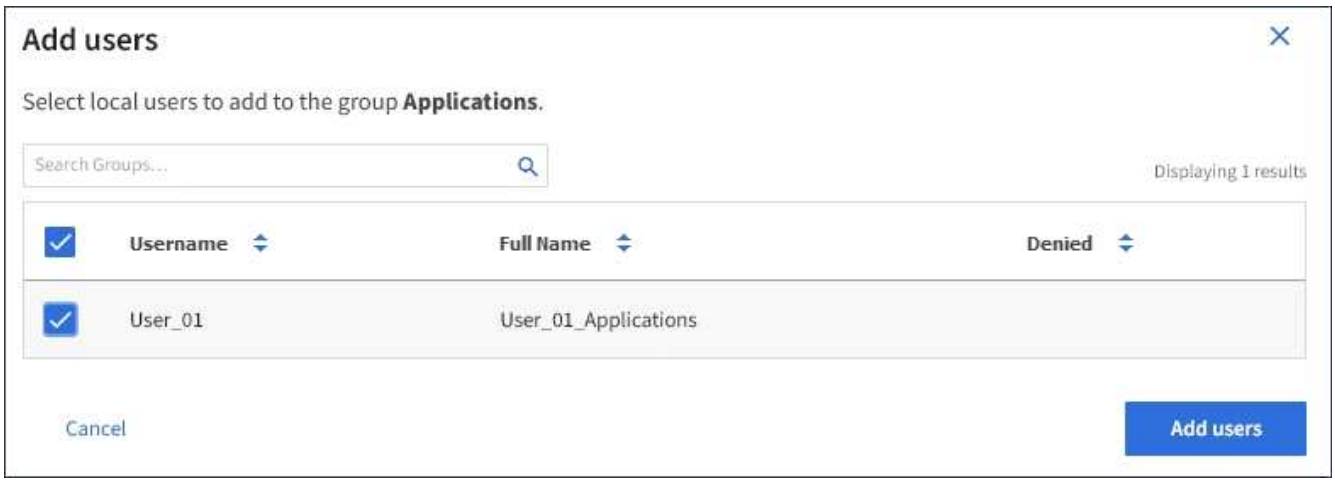
Allows users to create and delete their own S3 access keys.

Save changes

3. Seleccione **usuarios** y, a continuación, seleccione **Agregar usuarios**.



4. Seleccione los usuarios que desea agregar al grupo y, a continuación, seleccione **Agregar usuarios**.



Aparecerá un mensaje de confirmación en la esquina superior derecha de la página. Los cambios pueden tardar hasta 15 minutos en surtir efecto debido al almacenamiento en caché.

Editar el nombre del grupo

Puede editar el nombre para mostrar de un grupo. No se puede editar el nombre único de un grupo.

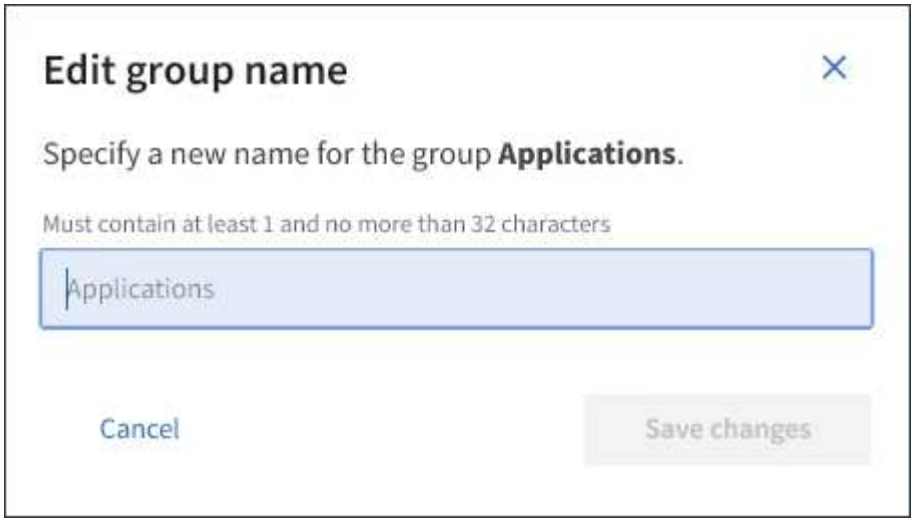
Lo que necesitará

- Debe iniciar sesión en el administrador de inquilinos mediante un navegador web compatible.
- Debe pertenecer a un grupo de usuarios que tenga el permiso acceso raíz. Consulte Permisos de gestión de inquilinos.

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO** > **grupos**.
2. Seleccione la casilla de verificación del grupo cuyo nombre para mostrar desee editar.
3. Seleccione **acciones** > **Editar nombre de grupo**.

   Aparece el cuadro de diálogo Editar nombre del grupo.



4. Si está editando un grupo local, actualice el nombre para mostrar según sea necesario.

   No se puede cambiar el nombre exclusivo de un grupo. No se puede editar el nombre para mostrar de un grupo federado.

5. Seleccione **Guardar cambios**.

   Aparecerá un mensaje de confirmación en la esquina superior derecha de la página. Los cambios pueden tardar hasta 15 minutos en surtir efecto debido al almacenamiento en caché.

Grupo duplicado

Puede crear nuevos grupos más rápidamente duplicando un grupo existente.

Lo que necesitará

- Debe iniciar sesión en el administrador de inquilinos mediante un navegador web compatible.
- Debe pertenecer a un grupo de usuarios que tenga el permiso acceso raíz. Consulte Permisos de gestión de inquilinos.

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO** > **grupos**.
2. Seleccione la casilla de verificación del grupo que desea duplicar.
3. Seleccione **Duplicar grupo**. Para obtener más información sobre cómo crear un grupo, consulte las instrucciones para crear grupos Un inquilino de S3 o para Un inquilino de Swift.
4. Seleccione la ficha **Grupo local** para crear un grupo local o seleccione la ficha **Grupo federado** para importar un grupo desde el origen de identidad configurado previamente.

   Si se ha activado el inicio de sesión único (SSO) para el sistema StorageGRID, los usuarios que pertenecen a grupos locales no podrán iniciar sesión en el Gestor de inquilinos, aunque puedan usar las aplicaciones cliente para gestionar los recursos del inquilino, basado en permisos de grupo.

5. Introduzca el nombre del grupo.
   - **Grupo local**: Introduzca tanto un nombre para mostrar como un nombre exclusivo. Puede editar el nombre para mostrar más adelante.

- **Grupo federado**: Introduzca el nombre único. Para Active Directory, el nombre único es el nombre asociado con `sAMAccountName` atributo. Para OpenLDAP, el nombre único es el nombre asociado con `uid` atributo.

6. Seleccione **continuar**.
7. Según sea necesario, modifique los permisos para este grupo.
8. Seleccione **continuar**.
9. Según sea necesario, si va a duplicar un grupo para un inquilino S3, seleccione opcionalmente una directiva diferente de los botones de opción * Agregar directiva S3*. Si seleccionó una política personalizada, actualice la cadena JSON como sea necesario.
10. Seleccione **Crear grupo**.

Eliminar grupo

Puede eliminar un grupo del sistema. Cualquier usuario que sólo pertenezca a ese grupo ya no podrá iniciar sesión en el Administrador de inquilinos ni utilizar la cuenta de arrendatario.

Lo que necesitará

- Debe iniciar sesión en el administrador de inquilinos mediante un navegador web compatible.
- Debe pertenecer a un grupo de usuarios que tenga el permiso acceso raíz. Consulte Permisos de gestión de inquilinos.

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO** > **grupos**.

2. Seleccione las casillas de verificación de los grupos que desea eliminar.
3. Seleccione **acciones** > **Eliminar grupo**.

   Aparecerá un mensaje de confirmación.

4. Seleccione **Eliminar grupo** para confirmar que desea eliminar los grupos indicados en el mensaje de confirmación.

   Aparecerá un mensaje de confirmación en la esquina superior derecha de la página. Los cambios pueden tardar hasta 15 minutos en surtir efecto debido al almacenamiento en caché.

Gestionar usuarios locales

Puede crear usuarios locales y asignarles grupos locales para determinar las funciones a las que pueden acceder estos usuarios. El Administrador de arrendatarios incluye un usuario local predefinido denominado «'root'». Aunque puede agregar y quitar usuarios locales, no puede quitar el usuario raíz.

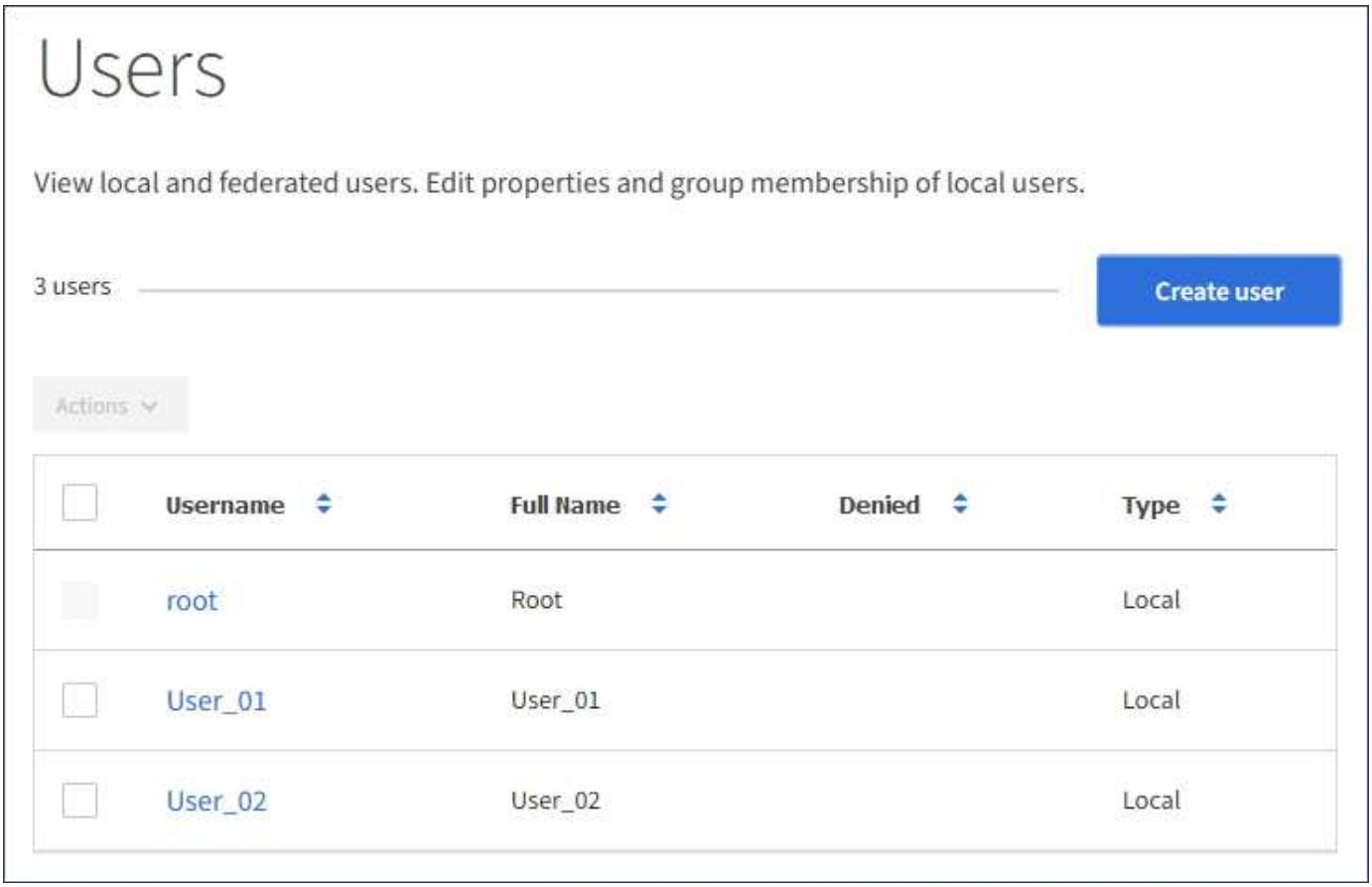
Lo que necesitará

- Debe iniciar sesión en el administrador de inquilinos mediante un navegador web compatible.
- Debe pertenecer a un grupo de usuarios de lectura y escritura que tenga el permiso acceso raíz. Consulte Permisos de gestión de inquilinos.

> Si se habilitó el inicio de sesión único (SSO) para el sistema StorageGRID, los usuarios locales no podrán iniciar sesión en el administrador de inquilinos o la API de gestión de inquilinos, aunque puedan usar las aplicaciones cliente S3 o Swift para acceder a los recursos del inquilino, en función de los permisos de grupo.

Acceder a la página usuarios

Seleccione **ADMINISTRACIÓN de ACCESO** > **usuarios**.



Crear usuarios locales

Es posible crear usuarios locales y asignarles a uno o varios grupos locales para controlar sus permisos de acceso.

Los usuarios de S3 que no pertenecen a ningún grupo no tienen permisos de gestión ni políticas de grupo S3 aplicadas. Es posible que estos usuarios tengan acceso a bloques de S3 otorgado a través de una política de bloques.

Los usuarios de Swift que no pertenecen a ningún grupo no tienen permisos de gestión ni acceso al contenedor de Swift.

Pasos

1. Seleccione **Crear usuario**.
2. Complete los siguientes campos.
   - **Nombre completo**: El nombre completo de este usuario, por ejemplo, el nombre y apellido de una persona o el nombre de una aplicación.
   - **Nombre de usuario**: El nombre que este usuario utilizará para iniciar sesión. Los nombres de usuario deben ser únicos y no se pueden cambiar.
   - **Contraseña**: Contraseña que se utiliza cuando el usuario inicia sesión.
   - **Confirmar contraseña**: Escriba la misma contraseña que escribió en el campo Contraseña.
   - **Denegar acceso**: Si selecciona **Sí**, este usuario no puede iniciar sesión en la cuenta de arrendatario, aunque el usuario pueda seguir perteneciendo a uno o más grupos.

     Por ejemplo, puede utilizar esta función para suspender temporalmente la capacidad de un usuario

para iniciar sesión.

3. Seleccione **continuar**.
4. Asigne el usuario a uno o más grupos locales.

   Los usuarios que no pertenecen a ningún grupo no tendrán permisos de administración. Los permisos son acumulativos. Los usuarios tendrán todos los permisos para todos los grupos a los que pertenezcan.

5. Seleccione **Crear usuario**.

   Los cambios pueden tardar hasta 15 minutos en surtir efecto debido al almacenamiento en caché.

Edite los detalles del usuario

Al editar los detalles de un usuario, puede cambiar el nombre completo y la contraseña del usuario, agregar el usuario a grupos diferentes e impedir que el usuario acceda al arrendatario.

Pasos

1. En la lista usuarios, seleccione el nombre del usuario cuyos detalles desee ver o editar.

   Como alternativa, puede seleccionar la casilla de verificación para el usuario y, a continuación, seleccionar **acciones** > **Ver detalles del usuario**.

2. Realice los cambios necesarios en la configuración del usuario.
   a. Cambie el nombre completo del usuario según sea necesario seleccionando el nombre completo o el icono de edición En la sección Descripción general.

      No puede cambiar el nombre de usuario.

   b. En la ficha **Contraseña**, cambie la contraseña del usuario según sea necesario.
   c. En la ficha **Access**, permita que el usuario inicie sesión (seleccione **no**) o impida que el usuario inicie sesión (seleccione **Sí**) según sea necesario.
   d. En la ficha **grupos**, agregue el usuario a grupos o elimine el usuario de los grupos según sea necesario.
   e. Según sea necesario para cada sección, seleccione **Guardar cambios**.

      Los cambios pueden tardar hasta 15 minutos en surtir efecto debido al almacenamiento en caché.

Duplique los usuarios locales

Puede duplicar un usuario local para crear un usuario nuevo más rápidamente.

Pasos

1. En la lista usuarios, seleccione el usuario que desea duplicar.
2. Seleccione **Duplicar usuario**.
3. Modifique los campos siguientes para el nuevo usuario.
   - **Nombre completo**: El nombre completo de este usuario, por ejemplo, el nombre y apellido de una persona o el nombre de una aplicación.
   - **Nombre de usuario**: El nombre que este usuario utilizará para iniciar sesión. Los nombres de usuario

deben ser únicos y no se pueden cambiar.

- **Contraseña**: Contraseña que se utiliza cuando el usuario inicia sesión.
- **Confirmar contraseña**: Escriba la misma contraseña que escribió en el campo Contraseña.
- **Denegar acceso**: Si selecciona **Sí**, este usuario no puede iniciar sesión en la cuenta de arrendatario, aunque el usuario pueda seguir perteneciendo a uno o más grupos.

  Por ejemplo, puede utilizar esta función para suspender temporalmente la capacidad de un usuario para iniciar sesión.

4. Seleccione **continuar**.
5. Seleccione uno o más grupos locales.

   Los usuarios que no pertenecen a ningún grupo no tendrán permisos de administración. Los permisos son acumulativos. Los usuarios tendrán todos los permisos para todos los grupos a los que pertenezcan.

6. Seleccione **Crear usuario**.

   Los cambios pueden tardar hasta 15 minutos en surtir efecto debido al almacenamiento en caché.

Eliminar usuarios locales

Es posible eliminar de forma permanente usuarios locales que ya no necesiten acceder a la cuenta de inquilino de StorageGRID.

Con el Administrador de inquilinos, puede eliminar usuarios locales, pero no usuarios federados. Debe utilizar el origen de identidad federado para eliminar usuarios federados.

Pasos

1. En la lista usuarios, seleccione la casilla de verificación del usuario local que desea eliminar.
2. Seleccione **acciones** > **Eliminar usuario**.
3. En el cuadro de diálogo de confirmación, seleccione **Eliminar usuario** para confirmar que desea eliminar al usuario del sistema.

   Los cambios pueden tardar hasta 15 minutos en surtir efecto debido al almacenamiento en caché.