Gestionar grupos de inquilinos

StorageGRID software

NetApp
February 12, 2026

Tabla de contenidos

Gestionar grupos de inquilinos

Cree grupos para un inquilino de S3

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

Antes de empezar

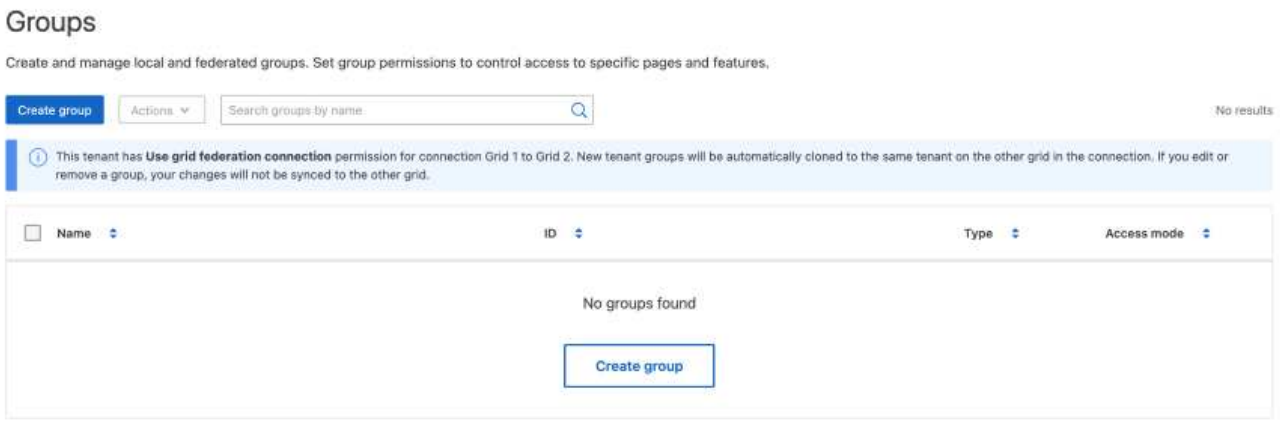
- Ha iniciado sesión en el gestor de inquilinos mediante un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene el "Permiso de acceso raíz".
- Si tiene pensado importar un grupo federado, tiene "federación de identidades configurada", y el grupo federado ya existe en el origen de identidad configurado.
- Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de grid**, ha revisado el flujo de trabajo y las consideraciones de "clonación de usuarios y grupos de inquilinos", y ha iniciado sesión en la cuadrícula de origen del inquilino.

Acceda al asistente Crear grupo

Como primer paso, acceda al asistente de creación de grupos.

Pasos

1. Seleccione **Administración de acceso** > **Grupos**.
2. Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de grid**, confirme que aparece un banner azul, indicando que los nuevos grupos creados en esta cuadrícula se clonarán en el mismo inquilino en la otra cuadrícula de la conexión. Si este banner no aparece, puede que haya iniciado sesión en la cuadrícula de destino del inquilino.



3. Seleccione **Crear grupo**.

Elija un tipo de grupo

Puede crear un grupo local o importar un grupo federado.

Pasos

1. 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.

2. 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.

     > Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de grid**, se producirá un error de clonación si el mismo **nombre único** ya existe para el inquilino en la cuadrícula de destino.

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

Administrar permisos de grupo

Los permisos de grupo controlan las tareas que los usuarios pueden realizar en el gestor de inquilinos y en la API de gestión de inquilinos.

Pasos

1. Para **Modo de acceso**, seleccione una de las siguientes opciones:
   - **Read-write** (por defecto): Los usuarios pueden iniciar sesión en Tenant Manager y administrar la configuración del inquilino.
   - **Sólo lectura**: Los usuarios sólo pueden ver los ajustes y las funciones. No pueden hacer ningún cambio ni realizar ninguna operación en el administrador de inquilinos o la API de gestión de inquilinos. Los usuarios locales de solo lectura pueden cambiar sus propias contraseñas.

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

2. Seleccione uno o más permisos para este grupo.

   Consulte "Permisos de gestión de inquilinos".

3. Seleccione **continuar**.

Establezca la política de grupo S3

La política de grupo determina qué permisos de acceso S3 tendrán los usuarios.

Pasos

1. Seleccione la política que desea usar para este grupo.

Política de grupo	Descripción
Sin acceso S3	Predeterminado. Los usuarios de este grupo no tienen acceso a los recursos de S3, a menos que el acceso se conceda con una política de bloque. 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 solo lectura a los recursos de 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 total	Los usuarios de este grupo tienen acceso completo a recursos de 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.
Mitigación del ransomware	Esta política de ejemplo se aplica a todos los depósitos de este inquilino. Los usuarios de este grupo pueden realizar acciones comunes, pero no pueden suprimir de forma permanente objetos de los bloques que tienen activado el control de versiones de objetos. Los usuarios del administrador de inquilinos que tienen el permiso **Administrar todos los cubos** pueden anular esta política de grupo. Limite el permiso Gestionar todos los buckets a usuarios de confianza y use la autenticación multifactor (MFA) cuando esté disponible.
Personalizado	A los usuarios del grupo se les conceden los permisos que especifique en el cuadro de texto.

2. 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.

   Para obtener información detallada sobre las políticas de grupo, incluida la sintaxis de idioma y los ejemplos, consulte "Ejemplo de políticas de grupo".

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

Añadir usuarios (sólo grupos locales)

Puede guardar el grupo sin agregar usuarios o, opcionalmente, puede agregar cualquier usuario local que ya exista.

> Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de grid**, los usuarios que seleccione al crear un grupo local en la cuadrícula de origen no se incluyen cuando el grupo se clona en la cuadrícula de destino. Por este motivo, no seleccione usuarios al crear el grupo. En su lugar, seleccione el grupo cuando cree los usuarios.

Pasos

1. Opcionalmente, seleccione uno o varios usuarios locales para este grupo.
2. Seleccione **Crear grupo** y **Finalizar**.

   El grupo creado aparece en la lista de grupos.

   Si su cuenta de inquilino tiene el permiso **Use grid federation connection** y usted está en la cuadrícula de origen del inquilino, el nuevo grupo se clona en la cuadrícula de destino del inquilino. **Success** aparece como **Cloning status** en la sección Overview de la página de detalles del grupo.

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.

Permiso	Descripción	Detalles
Acceso raíz	Proporciona acceso completo al administrador de inquilinos y a la API de gestión de inquilinos.	
Gestione sus propias credenciales 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**.

Permiso	Descripción	Detalles
Ver todos los cubos	Permite a los usuarios ver todos los depósitos y sus configuraciones.	Los usuarios que no tienen el permiso Ver todos los cubos o Gestionar todos los cubos no ven la opción de menú **Buckets**. Este permiso es reemplazado por el permiso Administrar todos los depósitos. No afecta las políticas de grupo o bucket S3 utilizadas por los clientes S3 o la consola S3.
Gestionar todos los cucharones	Permite a los usuarios utilizar el Administrador de inquilinos y la API de administración de inquilinos para crear y eliminar depósitos S3 y administrar las configuraciones de todos los depósitos S3 en la cuenta de inquilino, independientemente de las políticas de grupo o depósito S3.	Los usuarios que no tienen el permiso Ver todos los cubos o Gestionar todos los cubos no ven la opción de menú **Buckets**. Este permiso reemplaza al permiso Ver todos los depósitos. No afecta las políticas de grupo o bucket S3 utilizadas por los clientes S3 o la consola S3.
Gestionar puntos finales	Permite a los usuarios utilizar el Gestor de inquilinos o la API de gestión de inquilinos para crear o editar puntos finales de servicio de plataforma, que se utilizan como destino para los servicios de plataforma de StorageGRID.	Los usuarios que no tienen este permiso no ven la opción de menú **Platform services endpoints**.
Utilice la pestaña Consola de S3	Cuando se combina con el permiso Ver todos los cubos o Gestionar todos los cubos, permite a los usuarios ver y gestionar objetos desde la pestaña Consola de S3 en la página de detalles de un bloque.	

Gestionar grupos

Gestione los grupos de arrendatarios según sea necesario para ver, editar o duplicar un grupo y mucho más.

Antes de empezar

- Ha iniciado sesión en el gestor de inquilinos mediante un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene el "Permiso de acceso raíz".

Ver o editar grupo

Puede ver y editar la información básica y los detalles de cada grupo.

Pasos

1. Seleccione **Administración de acceso** > **Grupos**.
2. Revise la información proporcionada en la página Grupos, que muestra información básica de todos los grupos locales y federados de esta cuenta de arrendatario.

Si la cuenta de inquilino tiene el permiso **Use grid federation connection** y está viendo grupos en la cuadrícula de origen del inquilino:

- Un mensaje de banner indica que si edita o elimina un grupo, los cambios no se sincronizarán con la otra cuadrícula.
- Según sea necesario, un mensaje de banner indica si los grupos no se clonaron en el inquilino en la cuadrícula de destino. Usted puede volver a intentar un clon de grupo que falló.

3. Si desea cambiar el nombre del grupo:
   a. Seleccione la casilla de verificación para el grupo.
   b. Seleccione **acciones** > **Editar nombre de grupo**.
   c. Introduzca el nuevo nombre.
   d. Selecciona **Guardar cambios.**
4. Si desea ver más detalles o realizar modificaciones adicionales, realice una de las siguientes acciones:
   - Seleccione el nombre del grupo.
   - Selecciona la casilla de verificación del grupo y selecciona **Acciones** > **Ver detalles del grupo**.
5. Revise la sección Visión General, que muestra la siguiente información para cada grupo:
   - Nombre para mostrar
   - Nombre exclusivo
   - Tipo
   - Modo de acceso
   - Permisos
   - S3 Política
   - Número de usuarios en este grupo
   - Campos adicionales si la cuenta de inquilino tiene el permiso **Use grid federation connection** y está viendo el grupo en la cuadrícula de origen del inquilino:
     - Estado de clonación, ya sea **Success** o **Failure**
     - Un banner azul que indica que si edita o elimina este grupo, los cambios no se sincronizarán con la otra cuadrícula.
6. Edite la configuración del grupo según sea necesario. Referirse a"Cree grupos para un inquilino de S3" para obtener detalles sobre qué ingresar.
   a. En la sección Descripción general, cambie el nombre mostrado seleccionando el nombre o el icono de edición .
   b. En la pestaña **Permisos de grupo**, actualice los permisos y seleccione **Guardar cambios**.
   c. En la pestaña **Política de grupo**, realice los cambios y seleccione **Guardar cambios**.

      Opcionalmente, seleccione una política de grupo S3 diferente o ingrese la cadena JSON para una política personalizada según sea necesario.
7. Para añadir uno o varios usuarios locales existentes al grupo:
   a. Seleccione la ficha Usuarios.

b. Selecciona **Añadir usuarios**.
c. Seleccione los usuarios existentes que desea agregar y seleccione **Agregar usuarios**.

   Aparece un mensaje de éxito en la parte superior derecha.

8. Para eliminar usuarios locales del grupo:
   a. Seleccione la ficha Usuarios.
   b. Selecciona **Eliminar usuarios**.
   c. Seleccione los usuarios que desea eliminar y seleccione **Eliminar usuarios**.

      Aparece un mensaje de éxito en la parte superior derecha.

9. Confirma que has seleccionado **Guardar cambios** para cada sección que cambiaste.

Grupo duplicado

Puede duplicar un grupo existente para crear nuevos grupos más rápidamente.

> Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de grid** y duplica un grupo de la cuadrícula de origen del inquilino, el grupo duplicado se clonará en la cuadrícula de destino del inquilino.

Pasos

1. Seleccione **Administración de acceso** > **Grupos**.
2. Seleccione la casilla de control del grupo que desea duplicar.
3. Seleccione **acciones** > **Duplicar grupo**.
4. Ver"Cree grupos para un inquilino de S3" para obtener detalles sobre qué ingresar.
5. Seleccione **Crear grupo**.

Vuelva a intentar clonar el grupo

Para volver a intentar un clon que generó errores:

1. Seleccione cada grupo que indique *(Error de clonación)* debajo del nombre del grupo.
2. Selecciona **Acciones** > **Clonar grupos**.
3. Vea el estado de la operación de clonación desde la página de detalles de cada grupo que está clonando.

Para obtener más información, consulte "Clone los usuarios y los grupos de inquilinos".

Elimine uno o más grupos

Puede eliminar uno o varios grupos. Cualquier usuario que pertenezca únicamente a un grupo que se haya eliminado ya no podrá iniciar sesión en el gestor de inquilinos ni utilizar la cuenta de inquilino.

> Si tu cuenta de inquilino tiene el permiso **Usar conexión de federación de grid** y eliminas un grupo, StorageGRID no eliminará el grupo correspondiente en la otra cuadrícula. Si necesita mantener esta información sincronizada, debe eliminar el mismo grupo de ambas cuadrículas.

Pasos

1. Seleccione **Administración de acceso** > **Grupos**.
2. Seleccione la casilla de verificación para cada grupo que desee eliminar.
3. Selecciona **Acciones** > **Eliminar grupo** o **Acciones** > **Eliminar grupos**.

   Se muestra un cuadro de diálogo de confirmación.

4. Selecciona **Borrar grupo** o **Eliminar grupos**.

Configurar AssumeRole

Antes de empezar

Debe ser administrador para configurar AssumeRole.

Acerca de esta tarea

Para configurar AssumeRole, cree el grupo objetivo que se asumirá, si el grupo aún no existe. Edite la política S3 del grupo para especificar las acciones permitidas para asumir este grupo. Edite la política de confianza S3 del grupo para especificar los usuarios de confianza autorizados para asumir el grupo con la API AssumeRole.

Credenciales de seguridad temporales creadas asumiendo que este grupo es válido por un tiempo limitado. La sesión dura entre 15 minutos y 12 horas, y la sesión predeterminada es de 1 hora. Cuando se elimina al usuario de la política de confianza S3 del grupo, el usuario ya no podrá asumir este grupo.

Pasos

1. Seleccione **Administración de acceso** > **Grupos**.
2. Haga clic en el nombre del grupo.
3. Seleccione la pestaña **Política de confianza S3**.
4. Agregue su política de confianza S3, incluida una lista de usuarios que pueden realizar AssumeRole.
5. Seleccione **Guardar cambios**.
6. Seleccione la pestaña **Política de grupo S3**.
7. Edite la política S3 para especificar solo las acciones S3 requeridas para los usuarios de confianza agregados en la política de confianza S3 de este grupo.
8. Seleccione **Guardar cambios**.

Ejemplo de una política de confianza de AssumeRole S3

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Principal": {
                "AWS": [
                    "urn:sgws:identity::1234567890:user/user1",
                    "arn:aws:iam::1234567890:user/user2"
                ]
            }
        }
    ]
}
```

Una vez completada la configuración, los usuarios enumerados en la política de confianza de S3 pueden ejecutar AssumeRole y recibir credenciales. Los permisos finales están determinados por la política de grupo, la política de depósito y la política de sesión. Para más información, consulte "Utilizar políticas de acceso" .

Información de copyright

Información de la marca comercial