Gestión de grupos

StorageGRID

NetApp
October 03, 2025

This PDF was generated from https://docs.netapp.com/es-es/storagegrid-115/tenant/creating-groups-for-s3-tenant.html on October 03, 2025. Always check docs.netapp.com for the latest.

Tabla de contenidos

Gestión de grupos

Se asignan permisos a grupos de usuarios para controlar qué tareas pueden realizar los usuarios de inquilinos. Puede importar grupos federados desde un origen de identidades, como Active Directory u OpenLDAP, o bien crear grupos locales.

> Si se habilitó el inicio de sesión único (SSO) para el sistema StorageGRID, los usuarios locales no podrán iniciar sesión en el Gestor de inquilinos, aunque puedan acceder a los recursos de S3 y Swift, según los permisos de 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. 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"

Creación de 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 con un explorador 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. 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.

Información relacionada

"Permisos de gestión de inquilinos"

"Use S3"

Creación de grupos para un inquilino 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 con un explorador 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"

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 con un explorador compatible.
- Debe pertenecer a un grupo de usuarios que tenga el permiso acceso raíz.

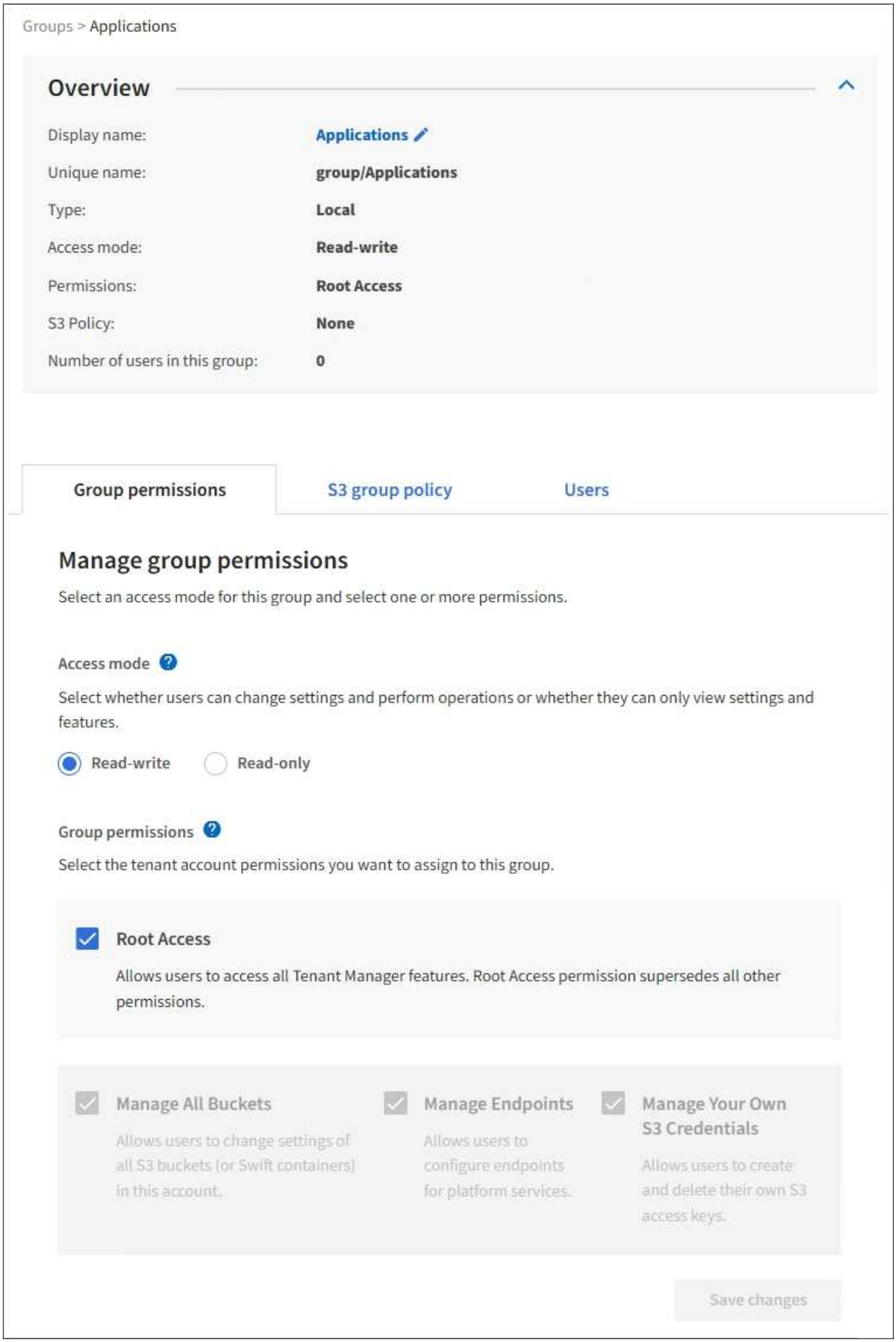
Pasos

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.
Root Access
Allows users to access all Tenant Manager features. Root Access permission supersedes all other permissions.
Manage All Buckets
Allows users to change settings of all S3 buckets (or Swift containers) in this account.
Manage Endpoints
Allows users to configure endpoints for platform services.
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

"Creación de grupos para un inquilino de S3"

"Creación de grupos para un inquilino Swift"

Agregar usuarios a un grupo local

Puede agregar usuarios a un grupo local según sea necesario.

Lo que necesitará

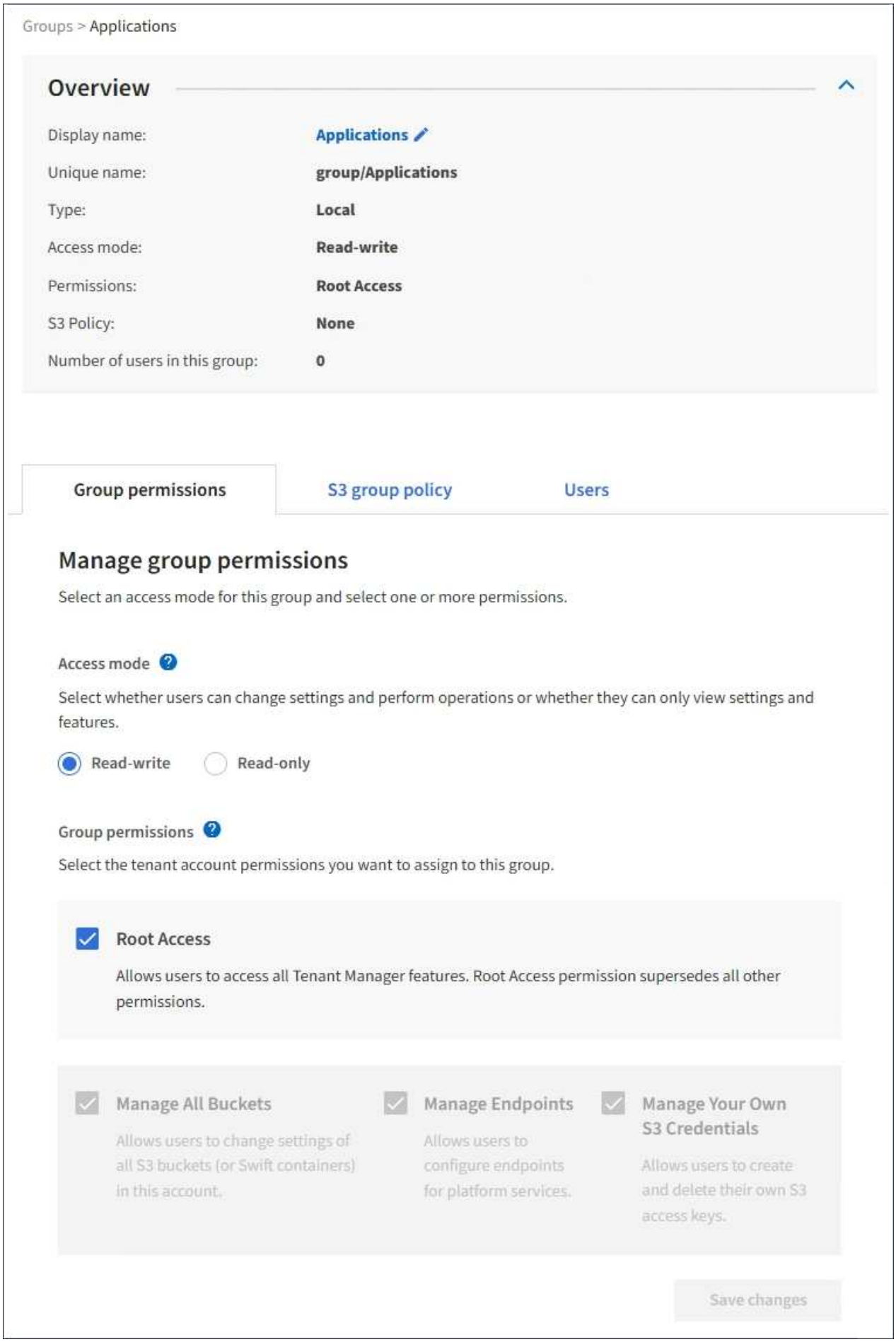
- Debe iniciar sesión en el Administrador de inquilinos con un explorador compatible.
- Debe pertenecer a un grupo de usuarios que tenga el permiso acceso raíz.

Pasos

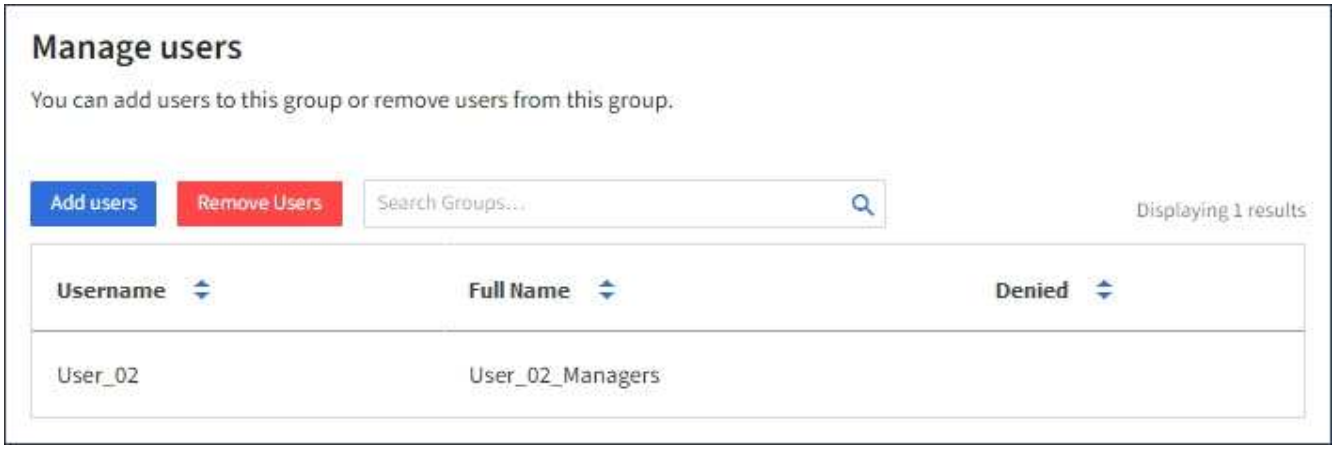
1. Seleccione **ADMINISTRACIÓN de ACCESO** > **grupos**.
2. Seleccione el nombre del grupo local al que desea añadir usuarios.

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

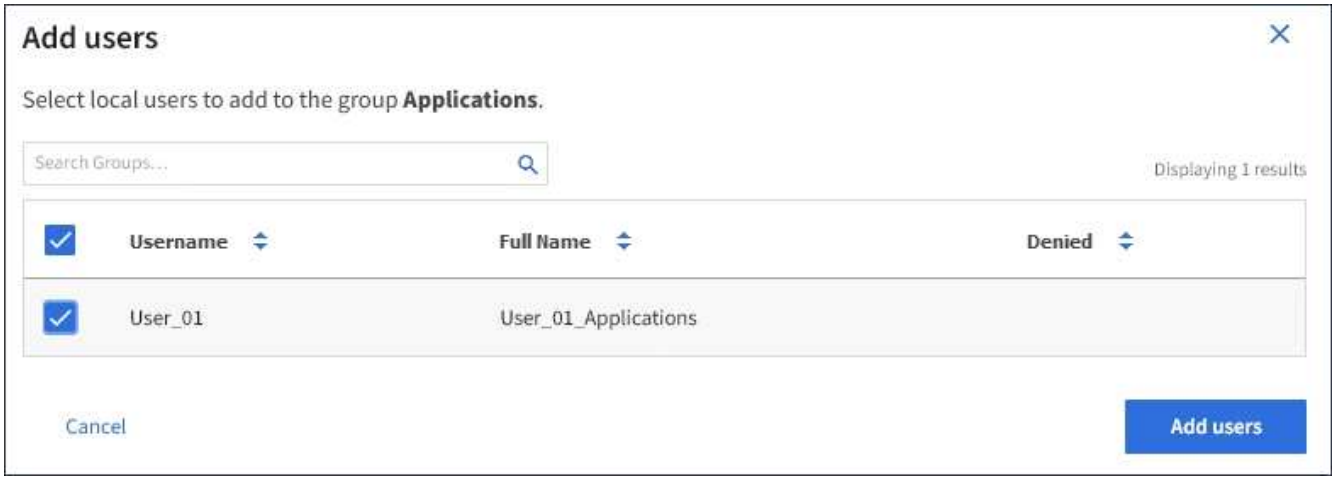
   Aparece la página de detalles del grupo.


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.
Root Access
Allows users to access all Tenant Manager features. Root Access permission supersedes all other permissions.
Manage All Buckets
Allows users to change settings of all S3 buckets (or Swift containers) in this account.
Manage Endpoints
Allows users to configure endpoints for platform services.
Manage Your Own S3 Credentials
Allows users to create and delete their own S3 access keys.
Save changes

3. Seleccione **gestionar 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.

Edición de un nombre de grupo

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

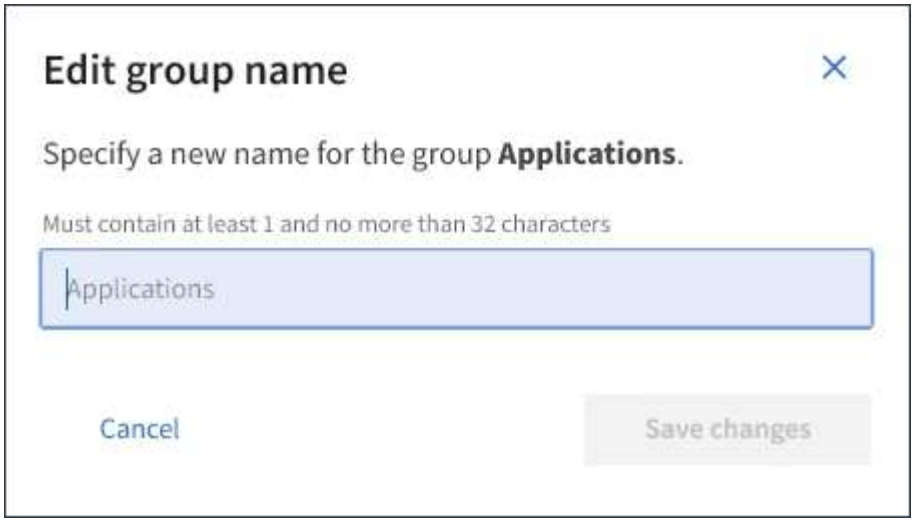
Lo que necesitará

- Debe iniciar sesión en el Administrador de inquilinos con un explorador compatible.
- Debe pertenecer a un grupo de usuarios que tenga el permiso acceso raíz.

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.

Información relacionada

"Permisos de gestión de inquilinos"

Duplicación de un grupo

Puede crear nuevos grupos más rápidamente duplicando un grupo existente.

Lo que necesitará

- Debe iniciar sesión en el Administrador de inquilinos con un explorador compatible.
- Debe pertenecer a un grupo de usuarios que tenga el permiso acceso raíz.

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO** > **grupos**.
2. Seleccione la casilla de verificación del grupo que desea duplicar.
3. Seleccione **Duplicar grupo**. Para obtener detalles adicionales sobre cómo crear un grupo, consulte las instrucciones para crear grupos para un inquilino S3 o para un inquilino 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 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.

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**.

Información relacionada

"Creación de grupos para un inquilino de S3"

"Creación de grupos para un inquilino Swift"

"Permisos de gestión de inquilinos"

Eliminar un 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 con un explorador compatible.
- Debe pertenecer a un grupo de usuarios que tenga el permiso acceso raíz.

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.

Información relacionada

"Permisos de gestión de inquilinos"

Información de copyright

Copyright © 2025 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

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

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

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

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

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

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

Información de la marca comercial

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