



# **Administrar claves de acceso S3**

StorageGRID software

NetApp

December 03, 2025

# Tabla de contenidos

- Administrar claves de acceso S3 ..... 1
  - Administrar claves de acceso S3 ..... 1
  - Crea tus propias claves de acceso S3 ..... 1
  - Ver sus claves de acceso S3 ..... 2
  - Eliminar sus propias claves de acceso S3 ..... 3
  - Crear las claves de acceso S3 de otro usuario ..... 4
  - Ver las claves de acceso S3 de otro usuario ..... 5
  - Eliminar las claves de acceso S3 de otro usuario ..... 6

# Administrar claves de acceso S3

## Administrar claves de acceso S3

Cada usuario de una cuenta de inquilino S3 debe tener una clave de acceso para almacenar y recuperar objetos en el sistema StorageGRID . Una clave de acceso consta de un ID de clave de acceso y una clave de acceso secreta.

Las claves de acceso S3 se pueden gestionar de la siguiente manera:

- Los usuarios que tienen el permiso **Administrar sus propias credenciales S3** pueden crear o eliminar sus propias claves de acceso S3.
- Los usuarios que tienen permiso de **acceso root** pueden administrar las claves de acceso para la cuenta raíz S3 y todos los demás usuarios. Las claves de acceso raíz brindan acceso completo a todos los depósitos y objetos para el inquilino, a menos que una política de depósito los deshabilite explícitamente.

StorageGRID admite la autenticación Signature Version 2 y Signature Version 4. No se permite el acceso entre cuentas a menos que lo habilite explícitamente una política de bucket.

## Crea tus propias claves de acceso S3

Si está utilizando un inquilino S3 y tiene el permiso adecuado, puede crear sus propias claves de acceso S3. Debe tener una clave de acceso para acceder a sus depósitos y objetos.

### Antes de empezar

- Ha iniciado sesión en el Administrador de inquilinos mediante un ["navegador web compatible"](#) .
- Pertenece a un grupo de usuarios que tiene la ["Administre sus propias credenciales S3 o permiso de acceso root"](#) .

### Acerca de esta tarea

Puede crear una o más claves de acceso S3 que le permitan crear y administrar depósitos para su cuenta de inquilino. Después de crear una nueva clave de acceso, actualice la aplicación con su nueva ID de clave de acceso y su clave de acceso secreta. Por seguridad, no cree más claves de las que necesita y elimine las claves que no esté utilizando. Si solo tiene una clave y está a punto de caducar, cree una nueva clave antes de que caduque la anterior y luego elimínela.

Cada clave puede tener un tiempo de expiración específico o no tener expiración. Siga estas pautas para el tiempo de vencimiento:

- Establezca un tiempo de vencimiento para sus claves para limitar su acceso a un período de tiempo determinado. Establecer un tiempo de vencimiento corto puede ayudar a reducir el riesgo si su ID de clave de acceso y su clave de acceso secreta se exponen accidentalmente. Las claves caducadas se eliminan automáticamente.
- Si el riesgo de seguridad en su entorno es bajo y no necesita crear nuevas claves periódicamente, no es necesario establecer un tiempo de vencimiento para sus claves. Si más adelante decide crear nuevas claves, elimine las claves antiguas manualmente.



Se puede acceder a los depósitos y objetos S3 que pertenecen a su cuenta mediante el ID de clave de acceso y la clave de acceso secreta que se muestran para su cuenta en el Administrador de inquilinos. Por este motivo, proteja las claves de acceso como lo haría con una contraseña. Rote las claves de acceso periódicamente, elimine las claves no utilizadas de su cuenta y nunca las comparta con otros usuarios.

## Pasos

1. Seleccione **ALMACENAMIENTO (S3) > Mis claves de acceso**.

Aparece la página Mis claves de acceso y enumera todas las claves de acceso existentes.

2. Seleccione **Crear clave**.

3. Debe realizar una de las siguientes acciones:

- Seleccione **No establecer un tiempo de expiración** para crear una clave que no caduque. (Por defecto)
- Seleccione **Establecer una hora de vencimiento** y configure la fecha y hora de vencimiento.



La fecha de vencimiento puede ser de un máximo de cinco años a partir de la fecha actual. El tiempo de expiración puede ser de un mínimo de un minuto a partir de la hora actual.

4. Seleccione **Crear clave de acceso**.

Aparece el cuadro de diálogo Descargar clave de acceso, que incluye el ID de su clave de acceso y su clave de acceso secreta.

5. Copie el ID de la clave de acceso y la clave de acceso secreta a una ubicación segura, o seleccione **Descargar .csv** para guardar un archivo de hoja de cálculo que contenga el ID de la clave de acceso y la clave de acceso secreta.



No cierre este cuadro de diálogo hasta que haya copiado o descargado esta información. No es posible copiar ni descargar claves una vez cerrado el cuadro de diálogo.

6. Seleccione **Finalizar**.

La nueva clave aparece en la página Mis claves de acceso.

7. Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de red**, utilice opcionalmente la API de administración de inquilinos para clonar manualmente las claves de acceso S3 del inquilino en la red de origen al inquilino en la red de destino. Ver ["Clonar claves de acceso S3 usando la API"](#).

## Ver sus claves de acceso S3

Si está utilizando un inquilino S3 y tiene la ["permiso apropiado"](#), puede ver una lista de sus claves de acceso S3. Puede ordenar la lista por tiempo de expiración, para poder determinar qué claves expirarán pronto. Según sea necesario, puede ["crear nuevas claves"](#) o ["borrar teclas"](#) que ya no estas usando.



Se puede acceder a los depósitos y objetos S3 que pertenecen a su cuenta mediante el ID de clave de acceso y la clave de acceso secreta que se muestran para su cuenta en el Administrador de inquilinos. Por este motivo, proteja las claves de acceso como lo haría con una contraseña. Rote las claves de acceso periódicamente, elimine las claves no utilizadas de su cuenta y nunca las comparta con otros usuarios.

#### Antes de empezar

- Ha iniciado sesión en el Administrador de inquilinos mediante un ["navegador web compatible"](#).
- Pertenece a un grupo de usuarios que tiene la opción Administrar sus propias credenciales de S3 ["permiso"](#).

#### Pasos

1. Seleccione **ALMACENAMIENTO (S3) > Mis claves de acceso**.
2. Desde la página Mis claves de acceso, ordene las claves de acceso existentes por **Tiempo de vencimiento** o **ID de clave de acceso**.
3. Según sea necesario, cree nuevas claves o elimine aquellas que ya no utilice.

Si crea nuevas claves antes de que caduquen las claves existentes, puede comenzar a usar las nuevas claves sin perder temporalmente el acceso a los objetos de la cuenta.

Las claves caducadas se eliminan automáticamente.

## Eliminar sus propias claves de acceso S3

Si está utilizando un inquilino S3 y tiene el permiso adecuado, puede eliminar sus propias claves de acceso S3. Una vez que se elimina una clave de acceso, ya no se puede usar para acceder a los objetos y depósitos en la cuenta del inquilino.

#### Antes de empezar

- Ha iniciado sesión en el Administrador de inquilinos mediante un ["navegador web compatible"](#).
- Tú tienes el ["Administrar sus propios permisos de credenciales S3"](#).



Se puede acceder a los depósitos y objetos S3 que pertenecen a su cuenta mediante el ID de clave de acceso y la clave de acceso secreta que se muestran para su cuenta en el Administrador de inquilinos. Por este motivo, proteja las claves de acceso como lo haría con una contraseña. Rote las claves de acceso periódicamente, elimine las claves no utilizadas de su cuenta y nunca las comparta con otros usuarios.

#### Pasos

1. Seleccione **ALMACENAMIENTO (S3) > Mis claves de acceso**.
2. Desde la página Mis teclas de acceso, seleccione la casilla de verificación de cada tecla de acceso que desee eliminar.
3. Seleccione **Tecla Eliminar**.
4. Desde el cuadro de diálogo de confirmación, seleccione **Eliminar tecla**.

Aparece un mensaje de confirmación en la esquina superior derecha de la página.

# Crear las claves de acceso S3 de otro usuario

Si utiliza un inquilino S3 y tiene el permiso adecuado, puede crear claves de acceso S3 para otros usuarios, como aplicaciones que necesitan acceso a depósitos y objetos.

## Antes de empezar

- Ha iniciado sesión en el Administrador de inquilinos mediante un ["navegador web compatible"](#).
- Pertenece a un grupo de usuarios que tiene la ["Permiso de acceso root"](#).

## Acerca de esta tarea

Puede crear una o más claves de acceso S3 para otros usuarios para que puedan crear y administrar depósitos para su cuenta de inquilino. Después de crear una nueva clave de acceso, actualice la aplicación con la nueva ID de clave de acceso y la clave de acceso secreta. Por seguridad, no cree más claves de las que necesita el usuario y elimine las claves que no se estén utilizando. Si solo tiene una clave y está a punto de caducar, cree una nueva clave antes de que caduque la anterior y luego elimínela.

Cada clave puede tener un tiempo de expiración específico o no tener expiración. Siga estas pautas para el tiempo de vencimiento:

- Establezca un tiempo de expiración para las claves para limitar el acceso del usuario a un período de tiempo determinado. Establecer un tiempo de vencimiento corto puede ayudar a reducir el riesgo si el ID de la clave de acceso y la clave de acceso secreta se exponen accidentalmente. Las claves caducadas se eliminan automáticamente.
- Si el riesgo de seguridad en su entorno es bajo y no necesita crear nuevas claves periódicamente, no es necesario establecer un tiempo de vencimiento para las claves. Si más adelante decide crear nuevas claves, elimine las claves antiguas manualmente.



Se puede acceder a los depósitos y objetos S3 que pertenecen a un usuario mediante el ID de clave de acceso y la clave de acceso secreta que se muestran para ese usuario en el Administrador de inquilinos. Por este motivo, proteja las claves de acceso como lo haría con una contraseña. Rote las claves de acceso periódicamente, elimine las claves no utilizadas de la cuenta y nunca las comparta con otros usuarios.

## Pasos

1. Seleccione **GESTIÓN DE ACCESO > Usuarios**.
2. Seleccione el usuario cuyas claves de acceso S3 desea administrar.

Aparece la página de detalles del usuario.

3. Seleccione **Teclas de acceso** y luego seleccione **Crear clave**.
4. Debe realizar una de las siguientes acciones:
  - Seleccione **No establecer un tiempo de expiración** para crear una clave que no expire. (Por defecto)
  - Seleccione **Establecer una hora de vencimiento** y configure la fecha y hora de vencimiento.



La fecha de vencimiento puede ser de un máximo de cinco años a partir de la fecha actual. El tiempo de expiración puede ser de un mínimo de un minuto a partir de la hora actual.

5. Seleccione **Crear clave de acceso**.

Aparece el cuadro de diálogo Descargar clave de acceso, que enumera el ID de la clave de acceso y la clave de acceso secreta.

6. Copie el ID de la clave de acceso y la clave de acceso secreta a una ubicación segura, o seleccione **Descargar .csv** para guardar un archivo de hoja de cálculo que contenga el ID de la clave de acceso y la clave de acceso secreta.



No cierre este cuadro de diálogo hasta que haya copiado o descargado esta información. No es posible copiar ni descargar claves una vez cerrado el cuadro de diálogo.

7. Seleccione **Finalizar**.

La nueva clave aparece en la pestaña Teclas de acceso de la página de detalles del usuario.

8. Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de red**, utilice opcionalmente la API de administración de inquilinos para clonar manualmente las claves de acceso S3 del inquilino en la red de origen al inquilino en la red de destino. Ver "[Clonar claves de acceso S3 usando la API](#)".

## Ver las claves de acceso S3 de otro usuario

Si está utilizando un inquilino S3 y tiene los permisos adecuados, puede ver las claves de acceso S3 de otro usuario. Puede ordenar la lista por tiempo de vencimiento para poder determinar qué claves caducarán pronto. Según sea necesario, puede crear nuevas claves y eliminar claves que ya no se utilizan.

### Antes de empezar

- Ha iniciado sesión en el Administrador de inquilinos mediante un "[navegador web compatible](#)".
- Tú tienes el "[Permiso de acceso root](#)".



Se puede acceder a los depósitos y objetos S3 que pertenecen a un usuario mediante el ID de clave de acceso y la clave de acceso secreta que se muestran para ese usuario en el Administrador de inquilinos. Por este motivo, proteja las claves de acceso como lo haría con una contraseña. Rote las claves de acceso periódicamente, elimine las claves no utilizadas de la cuenta y nunca las comparta con otros usuarios.

### Pasos

1. Seleccione **GESTIÓN DE ACCESO > Usuarios**.
2. Desde la página Usuarios, seleccione el usuario cuyas claves de acceso S3 desea ver.
3. Desde la página de detalles del usuario, seleccione **Teclas de acceso**.
4. Ordene las claves por **Tiempo de expiración** o **ID de clave de acceso**.
5. Según sea necesario, cree nuevas claves y elimine manualmente las claves que ya no se utilizan.

Si crea nuevas claves antes de que caduquen las claves existentes, el usuario puede comenzar a usar las nuevas claves sin perder temporalmente el acceso a los objetos de la cuenta.

Las claves caducadas se eliminan automáticamente.

### Información relacionada

- ["Crear las claves de acceso S3 de otro usuario"](#)
- ["Eliminar las claves de acceso S3 de otro usuario"](#)

## Eliminar las claves de acceso S3 de otro usuario

Si está utilizando un inquilino S3 y tiene los permisos adecuados, puede eliminar las claves de acceso S3 de otro usuario. Una vez que se elimina una clave de acceso, ya no se puede usar para acceder a los objetos y depósitos en la cuenta del inquilino.

### Antes de empezar

- Ha iniciado sesión en el Administrador de inquilinos mediante un ["navegador web compatible"](#).
- Tú tienes el ["Permiso de acceso root"](#).



Se puede acceder a los depósitos y objetos S3 que pertenecen a un usuario mediante el ID de clave de acceso y la clave de acceso secreta que se muestran para ese usuario en el Administrador de inquilinos. Por este motivo, proteja las claves de acceso como lo haría con una contraseña. Rote las claves de acceso periódicamente, elimine las claves no utilizadas de la cuenta y nunca las comparta con otros usuarios.

### Pasos

1. Seleccione **GESTIÓN DE ACCESO > Usuarios**.
2. Desde la página Usuarios, seleccione el usuario cuyas claves de acceso S3 desea administrar.
3. Desde la página de detalles del usuario, seleccione **Teclas de acceso** y luego seleccione la casilla de verificación para cada tecla de acceso que desee eliminar.
4. Seleccione **Acciones > Eliminar clave seleccionada**.
5. Desde el cuadro de diálogo de confirmación, seleccione **Eliminar tecla**.

Aparece un mensaje de confirmación en la esquina superior derecha de la página.



## 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.