



Gestión de claves de acceso de S3

StorageGRID 11.7

NetApp
April 12, 2024

Tabla de contenidos

- Gestión de claves de acceso de S3 1
 - Gestionar claves de acceso S3: Descripción general 1
 - Cree sus propias claves de acceso S3 1
 - Consulte las claves de acceso de S3 2
 - Elimine sus propias claves de acceso de S3 3
 - Cree las claves de acceso S3 de otro usuario 4
 - Ver las claves de acceso S3 de otro usuario 5
 - Elimine las claves de acceso S3 de otro usuario 6

Gestión de claves de acceso de S3

Gestionar claves de acceso S3: Descripción general

Cada usuario de una cuenta de inquilino de 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 de S3** pueden crear o eliminar sus propias claves de acceso de S3.
- Los usuarios que tienen el permiso **root access** pueden administrar las claves de acceso para la cuenta root de S3 y todos los demás usuarios. Las claves de acceso raíz proporcionan acceso completo a todos los bloques y objetos para el inquilino, a menos que se deshabilite explícitamente mediante una política de bloque.

StorageGRID admite la autenticación Signature versión 2 y Signature versión 4. No se permite el acceso de cuenta cruzada a menos que una política de bloque lo habilite explícitamente.

Cree sus propias claves de acceso S3

Si usa un inquilino de S3 y tiene el permiso correspondiente, puede crear sus propias claves de acceso S3. Debe tener una clave de acceso para acceder a los cubos 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 el ["Administre sus propias credenciales de S3 o permiso de acceso raíz"](#).

Acerca de esta tarea

Puede crear una o varias claves de acceso S3 que le permiten crear y gestionar bloques para su cuenta de inquilino. Después de crear una nueva clave de acceso, actualice la aplicación con su nuevo ID de clave de acceso y clave de acceso secreta. Por seguridad, no cree más claves de las que necesita, y elimine las claves que no está utilizando. Si sólo tiene una clave y está a punto de caducar, cree una nueva clave antes de que caduque la antigua y, a continuación, elimine la anterior.

Cada clave puede tener un tiempo de caducidad específico o no puede caducar. Siga estas directrices para el tiempo de caducidad:

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



Puede acceder a los bloques y los objetos de S3 que pertenecen a su cuenta mediante el ID de clave de acceso y la clave de acceso secreta que se muestra para su cuenta en el Administrador de inquilinos. Por este motivo, proteja las claves de acceso como lo haría con una contraseña. Gire las claves de acceso de forma regular, elimine las claves que no utilice de su cuenta y nunca las comparta con otros usuarios.

Pasos

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

Aparecerá la página Mis claves de acceso y mostrará una lista de las claves de acceso existentes.

2. Seleccione **Crear clave**.

3. Debe realizar una de las siguientes acciones:

- Seleccione **no establezca un tiempo de caducidad** para crear una clave que no caducará. (Predeterminado)
- Seleccione **establecer un tiempo de caducidad** y establezca la fecha y la hora de caducidad.



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

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

Aparece el cuadro de diálogo Descargar clave de acceso, en el que se enumeran el ID de clave de acceso y la 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 clave de acceso y la clave de acceso secreta.



No cierre este cuadro de diálogo hasta que haya copiado o descargado esta información. No puede copiar ni descargar claves después de cerrar 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 grid**, utilice opcionalmente la API de administración de inquilinos para clonar manualmente las claves de acceso S3 del inquilino en la cuadrícula de origen al inquilino en la cuadrícula de destino. Consulte "[Clone las claves de acceso S3 mediante la API](#)".

Consulte las claves de acceso de S3

Si usa un inquilino de S3 y tiene el permiso correspondiente, puede ver una lista de sus claves de acceso S3. Puede ordenar la lista por tiempo de caducidad, de modo que puede determinar qué claves caducarán pronto. Según sea necesario, puedes "[crear nuevas claves](#)" o "[teclas de eliminación](#)" que ya no utiliza.



Puede acceder a los bloques y los objetos de S3 que pertenecen a su cuenta mediante el ID de clave de acceso y la clave de acceso secreta que se muestra para su cuenta en el Administrador de inquilinos. Por este motivo, proteja las claves de acceso como lo haría con una contraseña. Gire las claves de acceso de forma regular, elimine las claves que no utilice 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 las credenciales Administrar sus propias credenciales 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 caducidad o ID de clave de acceso**.
3. Según sea necesario, cree nuevas claves o elimine las claves que ya no esté utilizando.

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

Las claves caducadas se eliminan automáticamente.

Elimine sus propias claves de acceso de S3

Si usa un inquilino de S3 y tiene el permiso correspondiente, puede eliminar sus propias claves de acceso S3. Cuando se elimina una clave de acceso, ya no se puede utilizar para acceder a los objetos y los bloques de la cuenta de inquilino.

Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un ["navegador web compatible"](#).
- Tiene el permiso gestionar sus propias credenciales de S3. Consulte ["Permisos de gestión de inquilinos"](#).



Puede acceder a los bloques y los objetos de S3 que pertenecen a su cuenta mediante el ID de clave de acceso y la clave de acceso secreta que se muestra para su cuenta en el Administrador de inquilinos. Por este motivo, proteja las claves de acceso como lo haría con una contraseña. Gire las claves de acceso de forma regular, elimine las claves que no utilice de su cuenta y nunca las comparta con otros usuarios.

Pasos

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

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

Cree las claves de acceso S3 de otro usuario

Si usa un inquilino de S3 y tiene el permiso apropiado, puede crear claves de acceso S3 para otros usuarios, como las aplicaciones que necesitan acceso a bloques 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 el "Permiso de acceso raíz".

Acerca de esta tarea

Puede crear una o varias claves de acceso de S3 para otros usuarios, de modo que puedan crear y gestionar bloques para su cuenta de inquilino. Después de crear una nueva clave de acceso, actualice la aplicación con el nuevo 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 están utilizando. Si sólo tiene una clave y está a punto de caducar, cree una nueva clave antes de que caduque la antigua y, a continuación, elimine la anterior.

Cada clave puede tener un tiempo de caducidad específico o no puede caducar. Siga estas directrices para el tiempo de caducidad:

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



Es posible acceder a los bloques y los objetos de S3 que pertenecen a un usuario mediante el ID de clave de acceso y la clave de acceso secreta mostrada para ese usuario en el Administrador de inquilinos. Por este motivo, proteja las claves de acceso como lo haría con una contraseña. Gire las claves de acceso de forma regular, elimine las claves que no utilice de la cuenta y nunca las comparta con otros usuarios.

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO > usuarios**.
2. Seleccione el usuario cuyas claves de acceso de S3 desee gestionar.

Aparece la página de detalles del usuario.

3. Seleccione **teclas de acceso** y, a continuación, seleccione **tecla de creación**.
4. Debe realizar una de las siguientes acciones:
 - Seleccione **No establecer un tiempo de caducidad** para crear una clave que no caduque. (Predeterminado)
 - Seleccione **establecer un tiempo de caducidad** y establezca la fecha y la hora de caducidad.



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

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

Se muestra el cuadro de diálogo Descargar clave de acceso, en el que se enumeran el ID de 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 clave de acceso y la clave de acceso secreta.



No cierre este cuadro de diálogo hasta que haya copiado o descargado esta información. No puede copiar ni descargar claves después de cerrar el cuadro de diálogo.

7. Seleccione **Finalizar**.

La nueva clave aparece en la ficha teclas de acceso de la página de detalles del usuario.

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

Ver las claves de acceso S3 de otro usuario

Si usa un inquilino de S3 y tiene los permisos adecuados, puede ver las claves de acceso S3 de otro usuario. Puede ordenar la lista por tiempo de caducidad para que pueda determinar qué claves caducarán pronto. Según sea necesario, puede crear nuevas claves y eliminar claves que ya no estén en uso.

Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un "[navegador web compatible](#)".
- Tiene el permiso acceso raíz.



Es posible acceder a los bloques y los objetos de S3 que pertenecen a un usuario mediante el ID de clave de acceso y la clave de acceso secreta mostrada para ese usuario en el Administrador de inquilinos. Por este motivo, proteja las claves de acceso como lo haría con una contraseña. Gire las claves de acceso de forma regular, elimine las claves que no utilice de la cuenta y nunca las comparta con otros usuarios.

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO > usuarios**.
2. En la página Usuarios, seleccione el usuario cuyas S3 claves de acceso desea ver.
3. En la página Detalles del usuario, selecciona **Teclas de acceso**.
4. Ordene las teclas por **tiempo de caducidad** o **ID de clave de acceso**.
5. Según sea necesario, cree nuevas claves y elimine manualmente las que ya no estén en uso.

Si crea claves nuevas antes de que caduquen las claves existentes, el usuario podrá empezar a utilizar las nuevas claves sin perder temporalmente el acceso a los objetos de la cuenta.

Las claves caducadas se eliminan automáticamente.

Información relacionada

["Cree las claves de acceso S3 de otro usuario"](#)

["Elimine las claves de acceso S3 de otro usuario"](#)

Elimine las claves de acceso S3 de otro usuario

Si usa un inquilino de S3 y tiene los permisos adecuados, puede eliminar las claves de acceso S3 de otro usuario. Cuando se elimina una clave de acceso, ya no se puede utilizar para acceder a los objetos y los bloques de la cuenta de inquilino.

Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un ["navegador web compatible"](#).
- Tiene el permiso acceso raíz. Consulte ["Permisos de gestión de inquilinos"](#).



Es posible acceder a los bloques y los objetos de S3 que pertenecen a un usuario mediante el ID de clave de acceso y la clave de acceso secreta mostrada para ese usuario en el Administrador de inquilinos. Por este motivo, proteja las claves de acceso como lo haría con una contraseña. Gire las claves de acceso de forma regular, elimine las claves que no utilice de la cuenta y nunca las comparta con otros usuarios.

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO > usuarios**.
2. En la página Usuarios, seleccione el usuario cuyas S3 claves de acceso desea administrar.
3. En la página Detalles del usuario, selecciona **Teclas de acceso** y luego selecciona la casilla de verificación para cada clave de acceso que quieras eliminar.
4. Seleccione **acciones > Borrar clave seleccionada**.
5. En el cuadro de diálogo de confirmación, seleccione **Tecla Eliminar**.

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

Información de copyright

Copyright © 2024 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 INTERRUPTIÓN 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.