



# **Gestionar grupos de inquilinos**

StorageGRID 11.7

NetApp  
April 12, 2024

# Tabla de contenidos

- Gestionar grupos de inquilinos ..... 1
  - Cree grupos para un inquilino de S3 ..... 1
  - Cree grupos para un inquilino de Swift ..... 4
- Permisos de gestión de inquilinos ..... 6
- Gestionar grupos ..... 7

# 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

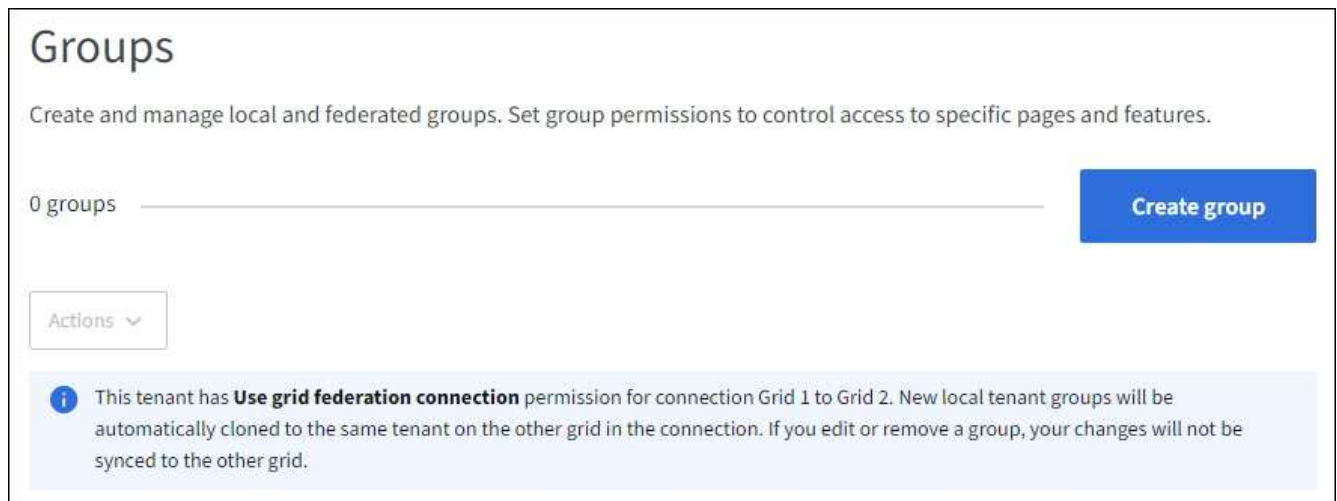
- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene el "Permiso de acceso raíz".
- Si planea importar un grupo federado, tiene "federación de identidades configurada", y el grupo federado ya existe en el origen de identidad configurado.
- Si su cuenta de inquilino tiene el permiso **Use grid federation connection**, ha revisado el flujo de trabajo y las consideraciones para "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 con `sAMAccountName` atributo. Para OpenLDAP, el nombre único es el nombre asociado con `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 arrendatario. 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 <b>Administrar todos los cubos</b> 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.

- 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 del idioma y los ejemplos, consulte ["Ejemplo de políticas de grupo"](#).

- 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.

## 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.



Se eliminó la compatibilidad con aplicaciones cliente de Swift y se quitará en unas versiones futuras.

### 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"](#).
- Si planea importar un grupo federado, tiene ["federación de identidades configurada"](#), y el grupo federado ya existe en el origen de identidad configurado.

## Acceda al asistente Crear grupo

### Pasos

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

1. Seleccione **ADMINISTRACIÓN de ACCESO > grupos**.
2. 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.

- **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.

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 la casilla de verificación **acceso raíz** si los usuarios del grupo necesitan iniciar sesión en el Administrador de inquilinos o en la API de administración de inquilinos.
3. Seleccione **continuar**.

## Configure la política de grupo de Swift

Los usuarios de Swift necesitan permiso de administrador para autenticarse en la API REST DE Swift para crear contenedores e ingerir objetos.

1. Seleccione la casilla de verificación **Swift administrator** si los usuarios del grupo necesitan usar la API REST DE Swift para administrar contenedores y objetos.
2. 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.

### Pasos

1. Opcionalmente, seleccione uno o varios usuarios locales para este grupo.

Si aún no ha creado usuarios locales, puede agregar este grupo al usuario en la página Usuarios. Consulte "[Gestionar usuarios locales](#)".

2. Seleccione **Crear grupo** y **Finalizar**.

El grupo creado aparece en la lista de grupos.

# 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.

Permiso	Descripción
Acceso raíz	Proporciona acceso completo al administrador de inquilinos y a la API de gestión de inquilinos.  <b>Nota:</b> Los usuarios de Swift deben tener permiso de acceso root para iniciar sesión en la cuenta del inquilino.
Administrador	Solo para inquilinos Swift. Proporciona acceso completo a los contenedores y objetos de Swift para esta cuenta de inquilino  <b>Nota:</b> los usuarios de Swift deben tener el permiso de Administrador de Swift para realizar cualquier operación con la API de REST de Swift.
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 <b>STORAGE (S3) &gt; My S3 access keys</b> .



Permiso	Descripción
Gestionar todos los cucharones	<ul style="list-style-type: none"> <li>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.</li> </ul> <p>Los usuarios que no tienen este permiso no ven la opción de menú <b>Buckets</b>.</p> <ul style="list-style-type: none"> <li>Inquilinos Swift: Permite a los usuarios de Swift controlar el nivel de coherencia de los contenedores Swift mediante la API de gestión de inquilinos.</li> </ul> <p><b>Nota:</b> Solo puede asignar el permiso Administrar todos los cubos a grupos Swift desde la API de administración de inquilinos. No puede asignar este permiso a grupos Swift mediante el administrador de inquilinos.</p>
Gestionar puntos finales	<p>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.</p> <p>Los usuarios que no tienen este permiso no ven la opción de menú <b>Platform services endpoints</b>.</p>
Gestionar objetos con S3 Console	<p>Cuando se combina con el permiso Gestionar todos los depósitos, permite a los usuarios acceder a la Consola Experimental S3 desde la página Buckets. Los usuarios que tienen este permiso pero que no tienen el permiso Administrar todos los depósitos pueden navegar directamente a la Consola Experimental S3.</p>

## Gestionar grupos

Puede ver un grupo; editar el nombre, los permisos, las políticas y los usuarios de un grupo; duplicar un grupo; o eliminar un grupo.

### 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"](#).


### 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 **Usar conexión de federación de grid** y está viendo grupos en la cuadrícula de origen del inquilino, un banner azul indica que si edita o elimina un grupo, sus cambios no se sincronizarán con la otra cuadrícula. Consulte ["Clone los usuarios y los grupos de inquilinos"](#).

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. Seleccione **Guardar cambios**.
4. Si desea ver más detalles o realizar modificaciones adicionales, realice una de las siguientes acciones:
  - Seleccione el nombre del grupo.
  - Seleccione la casilla de verificación del grupo y seleccione **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. Consulte "[Cree grupos para un inquilino de S3](#)" y "[Cree grupos para un inquilino de Swift](#)" para obtener más información acerca de lo que se debe introducir.
  - 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**.
    - Si está editando un grupo S3, seleccione opcionalmente una política de grupo S3 diferente o introduzca la cadena JSON de una política personalizada, según corresponda.
    - Si está editando un grupo Swift, opcionalmente seleccione o desactive la casilla de verificación **Swift Administrator**.
7. Para añadir uno o varios usuarios locales existentes al grupo:
  - a. Seleccione la ficha Usuarios.

**Manage users**

You can add users to this group or remove users from this group.

Add users
Remove Users

Displaying 1 results

Username	Full Name	Denied
User_02	User_02_Managers	

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. Consulte "[Cree grupos para un inquilino de S3](#)" o "[Cree grupos para un inquilino de Swift](#)" para obtener más información acerca de lo que se debe introducir.

5. Seleccione **Crear grupo**.

## 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. Seleccione **Acciones > Eliminar grupo** o **Acciones > Eliminar grupos**.

Se muestra un cuadro de diálogo de confirmación.

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

## 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.