Gestionar el acceso y la seguridad de los usuarios

NetApp Console setup and administration

NetApp
February 11, 2026

Tabla de contenidos

Gestionar el acceso y la seguridad de los usuarios

Obtenga más información sobre el control de acceso basado en roles (RBAC) de la NetApp Console

Administre el acceso de los usuarios a la NetApp Console con control de acceso basado en roles (RBAC), asignando roles predefinidos a nivel de organización, carpeta o proyecto. Cada rol otorga permisos específicos que definen qué acciones pueden realizar los usuarios dentro de su ámbito asignado.

NetApp diseña roles de consola con privilegios mínimos, por lo que cada rol incluye solo los permisos necesarios para sus tareas. Este enfoque mejora la seguridad al limitar el acceso a lo que cada miembro necesita.

Después de organizar los recursos en carpetas y proyectos, asigne a los miembros de la organización uno o más roles para carpetas o proyectos específicos, que les permitan realizar solo sus responsabilidades.

Por ejemplo, puede asignar a un miembro el rol de administrador de resiliencia ante ransomware para un nivel de proyecto específico, lo que le permitirá realizar operaciones de resiliencia ante ransomware para recursos dentro de ese proyecto, sin otorgarle un acceso más amplio a toda la organización. A este mismo usuario se le puede otorgar el rol para varios proyectos dentro de su organización.

Puede asignar a los usuarios múltiples roles para el mismo ámbito o para ámbitos diferentes, según sus responsabilidades. Por ejemplo, una organización más pequeña puede tener el mismo usuario que administre las tareas de Resiliencia ante Ransomware y Copia de Seguridad y Recuperación a nivel de la organización, mientras que una organización más grande puede tener diferentes usuarios asignados a cada rol a nivel de proyecto.

Tipos de miembros de la organización de la consola

Hay tres tipos de miembros en una organización de la NetApp Console : * *Cuentas de usuario*: Usuarios individuales que inician sesión en la NetApp Console para administrar recursos. Los usuarios deben registrarse en la NetApp Console antes de poder agregarlos a una organización. * *Cuentas de servicio*: Cuentas no humanas utilizadas por aplicaciones o servicios para interactuar con la NetApp Console a través de API. Puede agregar cuentas de servicio directamente a su organización de la consola. * *Grupos federados*: Grupos sincronizados desde su proveedor de identidad (IdP) que le permiten administrar el acceso de múltiples usuarios de forma colectiva. Cada usuario dentro de un grupo federado debe haberse registrado en la NetApp Console y haber sido agregado a su organización con un rol de acceso antes de poder acceder a los recursos otorgados al grupo.

"Aprenda cómo agregar miembros a su organización."

Roles predefinidos en la NetApp Console

La NetApp Console incluye roles predefinidos que puedes asignar a los miembros de la organización. Cada rol incluye permisos que especifican qué acciones puede realizar un miembro dentro de su ámbito asignado (organización, carpeta o proyecto).

Los roles de la NetApp Console utilizan principios de privilegios mínimos que garantizan que los miembros solo tengan los permisos necesarios para sus tareas y categorizan los roles según el tipo de acceso que

brindan:

- Roles de la plataforma: proporcionar permisos de administración de la consola
- Funciones de servicios de datos: proporcione permisos para administrar servicios de datos específicos, como Resiliencia ante ransomware y Copia de seguridad y recuperación
- Roles de la aplicación: Proporcionan permisos para administrar el almacenamiento, así como para auditar eventos y alertas de la consola.

Puede asignar múltiples roles a un miembro según sus responsabilidades. Por ejemplo, puede asignar a un miembro el rol de administrador de resiliencia contra ransomware y el rol de administrador de copia de seguridad y recuperación para un proyecto específico.

"Obtenga información sobre los roles predefinidos disponibles en NetApp Console".

Administrar el acceso de los miembros en la NetApp Console

Administrar el acceso de los miembros en su organización de la consola. Asignar roles para establecer permisos. Eliminar miembros cuando se van.

Roles de acceso requeridos

Superadministrador, administrador de la organización o administrador de carpeta o proyecto (para carpetas y proyectos que administra). Enlace:reference-iam-predefined-roles.html[Obtenga información sobre los roles de acceso].

Puede asignar roles de acceso por proyecto o carpeta. Por ejemplo, asigne un rol a un usuario para dos proyectos específicos o asigne el rol a nivel de carpeta para darle a un usuario el rol de administrador de Ransomware Resilience para todos los proyectos en una carpeta.

Agregue sus carpetas y proyectos antes de asignar acceso a los usuarios. "Aprenda a agregar carpetas y proyectos."

Comprenda cómo se otorga el acceso en la NetApp Console

La NetApp Console utiliza un modelo de control de acceso basado en roles (RBAC) para administrar los permisos de los usuarios. Puede asignar roles predefinidos a los miembros de forma individual o a través de grupos federados. Puede agregar y asignar roles a cuentas de servicio, así como a grupos federados. Cada rol define qué acciones puede realizar un miembro en los recursos asociados.

Tenga en cuenta lo siguiente sobre cómo conceder acceso en la NetApp Console:

- Todos los usuarios deben registrarse primero en la NetApp Console antes de poder obtener acceso a los recursos.
- Debe asignar explícitamente un rol a cada usuario en la Consola antes de que puedan acceder a los recursos, incluso si son miembros de un grupo federado al que se le ha asignado un rol.
- Puede agregar cuentas de servicio directamente desde la consola y asignarles roles.

Uso de la herencia de roles

Cuando se asigna un rol a nivel de organización, carpeta o proyecto en NetApp Console, ese rol es heredado

automáticamente por todos los recursos dentro del alcance seleccionado. Por ejemplo, los roles a nivel de carpeta se aplican a todos los proyectos contenidos, mientras que los roles a nivel de proyecto se aplican a todos los recursos dentro de ese proyecto.

Ver miembros de la organización

Para comprender qué recursos y permisos están disponibles para un miembro, puede ver los roles asignados al miembro en diferentes niveles de la jerarquía de recursos de su organización."Aprenda a usar roles para controlar el acceso a los recursos de la consola."

Pasos

1. Seleccione **Administración > Identidad y acceso**.
2. Seleccione **Miembros**.

   La tabla **Miembros** enumera los miembros de su organización.

3. Desde la página **Miembros**, navegue hasta un miembro en la tabla, seleccione ••• y luego seleccione **Ver detalles**.

Ver los roles asignados a un miembro

Puede verificar qué roles tienen asignados actualmente.

Si tiene el rol de *Administrador de carpeta o de proyecto*, la página muestra todos los miembros de la organización. Sin embargo, solo puede ver y administrar los permisos de miembros para las carpetas y proyectos para los que tiene permisos. "Obtenga más información sobre las acciones que un administrador de carpeta o proyecto puede completar" .

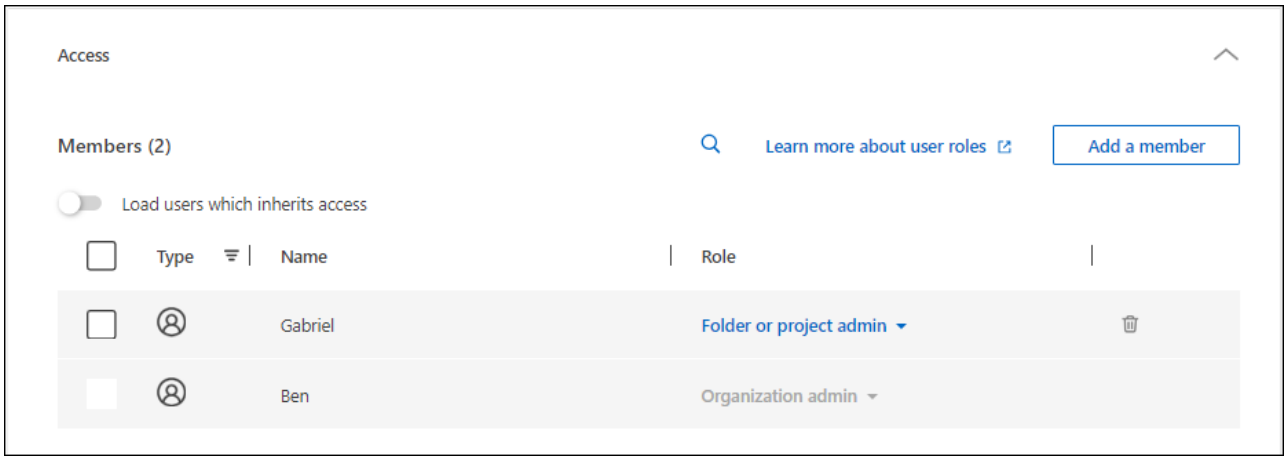
1. Desde la página **Miembros**, navegue hasta un miembro en la tabla, seleccione ••• y luego seleccione **Ver detalles**.
2. En la tabla, expanda la fila correspondiente a la organización, carpeta o proyecto donde desea ver el rol asignado al miembro y seleccione **Ver** en la columna **Rol**.

Ver miembros asociados a una carpeta o proyecto

Puede ver los miembros que tienen acceso a una carpeta o proyecto específico.

Pasos

1. Seleccione **Administración > Identidad y acceso**.
2. Seleccione **Organización**.
3. Desde la página **Organización**, navegue hasta un proyecto o carpeta en la tabla, seleccione ••• y luego seleccione **Editar carpeta** o **Editar proyecto**.
   - Seleccione **Acceso** para ver los miembros que tienen acceso a la carpeta o al proyecto.



Asignar o modificar el acceso de los miembros

Una vez que un usuario se registra en NetApp Console, puede agregarlo a su organización y asignarle un rol para brindarle acceso a los recursos. "Aprenda cómo agregar miembros a su organización."

Puede ajustar el acceso de un miembro agregando o eliminando roles según sea necesario.

Agregar un rol de acceso a un miembro

Normalmente, se asigna un rol al agregar un miembro a su organización, pero puede actualizarlo en cualquier momento eliminando o agregando roles.

Puede asignar a un usuario un rol de acceso para su organización, carpeta o proyecto.

Los miembros pueden tener múltiples roles dentro del mismo proyecto y en diferentes proyectos. Por ejemplo, las organizaciones más pequeñas pueden asignar todos los roles de acceso disponibles al mismo usuario, mientras que las organizaciones más grandes pueden hacer que los usuarios realicen tareas más especializadas. Como alternativa, también puede asignar a un usuario el rol de administrador de Resiliencia contra ransomware a nivel de la organización. En ese ejemplo, el usuario podría realizar tareas de resiliencia frente a ransomware en todos los proyectos dentro de su organización.

Su estrategia de roles de acceso debe estar alineada con la forma en que ha organizado sus recursos de NetApp .

Pasos

1. Seleccione **Administración > Identidad y acceso**.
2. Seleccione **Miembros**.
3. Seleccione una de las pestañas de miembros: **Usuarios**, **Cuentas de servicio** o **Grupos federados**.
4. Seleccione el menú de acciones ••• junto al miembro al que desea asignar un rol y seleccione **Agregar un rol**.
5. Para agregar un rol, complete los pasos en el cuadro de diálogo:
   - **Seleccione una organización, carpeta o proyecto**: elija el nivel de su jerarquía de recursos para el cual el miembro debe tener permisos.

     Si selecciona la organización o una carpeta, el miembro tendrá permisos sobre todo lo que resida dentro de la organización o carpeta.

- **Seleccionar una categoría**: Elija una categoría de rol. "Obtenga más información sobre los roles de acceso" .
- Seleccionar un **Rol**: elija un rol que proporcione al miembro permisos para los recursos asociados con la organización, carpeta o proyecto que seleccionó.
- **Agregar rol**: si desea proporcionar acceso a carpetas o proyectos adicionales dentro de su organización, seleccione **Agregar rol**, especifique otra carpeta, proyecto o categoría de rol y luego seleccione una categoría de rol y un rol correspondiente.

6. Seleccione **Agregar nuevos roles**.

Cambiar el rol asignado a un miembro

Cambiar los roles de un miembro para actualizar su acceso.

Los usuarios deben tener al menos un rol asignado. No se pueden eliminar todos los roles de un usuario. Si necesita eliminar todos los roles, debe eliminar el usuario de su organización.

Pasos

1. Seleccione **Administración > Identidad y acceso**.
2. Seleccione **Miembros**.
3. Seleccione una de las pestañas de miembros: **Usuarios**, **Cuentas de servicio** o **Grupos federados**.
4. Desde la página **Miembros**, navegue hasta un miembro en la tabla, seleccione ••• y luego seleccione **Ver detalles**.
5. En la tabla, expanda la fila correspondiente a la organización, carpeta o proyecto donde desea cambiar el rol asignado al miembro y seleccione **Ver** en la columna **Rol** para ver los roles asignados a este miembro.
6. Puede cambiar un rol existente de un miembro o eliminar un rol.
   a. Para cambiar el rol de un miembro, seleccione **Cambiar** junto al rol que desea cambiar. Sólo puedes cambiar un rol a un rol dentro de la misma categoría de rol. Por ejemplo, puede cambiar de un rol de servicio de datos a otro. Confirmar el cambio.
   b. Para desasignar el rol de un miembro, seleccione 🗑 junto al rol para eliminar el rol respectivo del miembro.. Se le pedirá que confirme la eliminación.

Eliminar un miembro de su organización

Eliminar a un miembro si abandona tu organización.

Cuando se elimina un miembro, el sistema revoca sus permisos de consola, pero conserva sus cuentas de consola y del sitio de soporte de NetApp .

Miembros federados

- Los usuarios federados pierden automáticamente el acceso a la NetApp Console cuando se los elimina de su IdP. Pero aún así debes eliminarlos de tu organización de consola para mantener tu lista de miembros actualizada.
- Si elimina un usuario de un grupo federado en su IdP, perderá el acceso a la consola asociado con ese grupo. Sin embargo, aún conservan cualquier acceso asociado con un rol explícito asignado a ellos en la Consola.

Pasos

1. Seleccione **Administración > Identidad y acceso**.
2. Seleccione **Miembros**.
3. Seleccione una de las pestañas de miembros: **Usuarios**, **Cuentas de servicio** o **Grupos federados**.
4. Desde la página **Miembros**, navegue hasta un miembro en la tabla, seleccione ••• luego seleccione **Eliminar usuario**.
5. Confirme que desea eliminar al miembro de su organización.

Seguridad del usuario

Proteja el acceso de los usuarios a su organización de NetApp Console administrando la configuración de seguridad de los miembros. Puede restablecer las contraseñas de usuario, administrar la autenticación multifactor (MFA) y recrear las credenciales de la cuenta de servicio.

Roles de acceso requeridos

Superadministrador, administrador de la organización o administrador de carpeta o proyecto (para carpetas y proyectos que administra). Enlace:reference-iam-predefined-roles.html[Obtenga información sobre los roles de acceso].

Restablecer contraseñas de usuario (solo usuarios locales)

Los administradores de la organización no pueden restablecer las contraseñas de los usuarios locales. Sin embargo, pueden indicar a los usuarios que restablezcan sus propias contraseñas.

Indique a un usuario que restablezca su contraseña desde la página de inicio de sesión de la consola seleccionando **¿Olvidó su contraseña?**.

Esta opción no está disponible para los usuarios de una organización federada.

Administrar la autenticación multifactor (MFA) de un usuario

Si un usuario pierde el acceso a su dispositivo MFA, puede eliminar o deshabilitar su configuración MFA.

La autenticación multifactor solo está disponible para usuarios locales. Los usuarios federados no pueden habilitar MFA.

Los usuarios deben configurar MFA nuevamente cuando inicien sesión después de la eliminación. Si el usuario pierde temporalmente el acceso a su dispositivo MFA, puede usar su código de recuperación guardado para iniciar sesión.

Si no tienen su código de recuperación, deshabilite temporalmente MFA para permitir el inicio de sesión. Cuando deshabilita MFA para un usuario, esta se deshabilita solo durante ocho horas y luego se vuelve a habilitar automáticamente. Al usuario se le permite un inicio de sesión durante ese tiempo sin MFA. Después de las ocho horas, el usuario deberá utilizar MFA para iniciar sesión.

Para administrar la autenticación multifactor de un usuario, debe tener una dirección de correo electrónico en el mismo dominio que el usuario afectado.

Pasos

1. Seleccione **Administración > Identidad y acceso**.
2. Seleccione **Miembros**.

   La tabla **Miembros** enumera los miembros de su organización.

3. Desde la página **Miembros**, navegue hasta un miembro en la tabla, seleccione ••• y luego seleccione **Administrar autenticación multifactor**.
4. Elija si desea eliminar o deshabilitar la configuración MFA del usuario.

Recrear las credenciales para una cuenta de servicio

Puede crear nuevas credenciales para un servicio si las pierde o necesita actualizarlas.

Al crear nuevas credenciales se eliminan las antiguas. No puedes utilizar las credenciales antiguas.

Pasos

1. Seleccione **Administración > Identidad y acceso**.
2. Seleccione **Miembros**.
3. En la tabla **Miembros**, navegue hasta una cuenta de servicio, seleccione ••• y luego seleccione **Recrear secretos**.
4. Seleccione **Recrear**.
5. Descargue o copie el ID del cliente y el secreto del cliente.

   La consola muestra el secreto del cliente solo una vez. Asegúrese de copiarlo o descargarlo y almacenarlo de forma segura.