Roles de acceso a la NetApp Console

NetApp Console setup and administration

NetApp
January 13, 2026

Tabla de contenidos

Roles de acceso a la NetApp Console

Obtenga más información sobre los roles de acceso a la NetApp Console

La gestión de identidad y acceso (IAM) en la NetApp Console proporciona roles predefinidos que puede asignar a los miembros de su organización en diferentes niveles de su jerarquía de recursos. Antes de asignar estos roles, debe comprender los permisos que incluye cada rol. Los roles se dividen en las siguientes categorías: plataforma, aplicación y servicio de datos.

Roles de la plataforma

Los roles de plataforma otorgan permisos de administración de la NetApp Console , incluida la asignación de roles y la gestión de usuarios. La consola tiene varios roles de plataforma.

Rol de la plataforma	Responsabilidades
"Administrador de la organización"	Permite a un usuario acceso sin restricciones a todos los proyectos y carpetas dentro de una organización, agregar miembros a cualquier proyecto o carpeta, así como realizar cualquier tarea y utilizar cualquier servicio de datos que no tenga un rol explícito asociado. Los usuarios con este rol administran su organización creando carpetas y proyectos, asignando roles, agregando usuarios y administrando sistemas si tienen las credenciales adecuadas. Este es el único rol de acceso que puede crear agentes de consola.
"Administrador de carpetas o proyectos"	Permite a un usuario acceso sin restricciones a los proyectos y carpetas asignados. Pueden agregar miembros a las carpetas o proyectos que administran, así como realizar cualquier tarea y utilizar cualquier servicio de datos o aplicación en los recursos dentro de la carpeta o el proyecto que están asignados. Los administradores de carpetas o proyectos no pueden crear agentes de consola.
"Administración de la federación"	Permite a un usuario crear y administrar federaciones con la consola, lo que habilita el inicio de sesión único (SSO).
"Visor de la Federación"	Permite que un usuario vea las federaciones existentes con la consola. No se pueden crear ni administrar federaciones.
"Administración de asociaciones"	Permite a un usuario crear y gestionar asociaciones.
"Visor de asociaciones"	Permite a un usuario ver las asociaciones existentes. No se pueden crear ni gestionar asociaciones.
"Superadministrador"	Proporciona al usuario un subconjunto de roles de administrador. Esta función está diseñada para organizaciones más pequeñas que quizás no necesiten distribuir las responsabilidades de la consola entre varios usuarios.
"Súper espectador"	Proporciona al usuario un subconjunto de roles de espectador. Esta función está diseñada para organizaciones más pequeñas que quizás no necesiten distribuir las responsabilidades de la consola entre varios usuarios.

Roles de aplicación

La siguiente es una lista de roles en la categoría de aplicación. Cada rol otorga permisos específicos dentro de su alcance designado. Los usuarios que no tengan el rol de plataforma o aplicación requerido no pueden acceder a la aplicación respectiva.

Rol de la aplicación	Responsabilidades
"Administrador de Google Cloud NetApp Volumes"	Los usuarios con el rol de Google Cloud NetApp Volumes pueden descubrir y administrar Google Cloud NetApp Volumes.
"Visor de Google Cloud NetApp Volumes"	Los usuarios con el rol de usuario de Google Cloud NetApp Volumes pueden ver Google Cloud NetApp Volumes.
"Administrador de Keystone"	Los usuarios con el rol de administrador de Keystone pueden crear solicitudes de servicio. Permite a los usuarios supervisar y ver el uso, los recursos y los detalles de administración dentro del inquilino de Keystone al que están accediendo.
"Visor de Keystone"	Los usuarios con el rol de visualizador de Keystone NO PUEDEN crear solicitudes de servicio. Permite a los usuarios monitorear y visualizar el consumo, los activos y la información administrativa dentro del inquilino de Keystone al que están accediendo.
Rol de configuración del mediador de ONTAP	Las cuentas de servicio con la función de configuración de Mediador de ONTAP pueden crear solicitudes de servicio. Esta función es necesaria en una cuenta de servicio para configurar una instancia de la"Mediador de la nube de ONTAP" .
"Analista de soporte de operaciones"	Proporciona acceso a alertas y herramientas de monitoreo y la capacidad de ingresar y administrar casos de soporte.
"Administrador de almacenamiento"	Administrar las funciones de gobernanza y salud del almacenamiento, descubrir recursos de almacenamiento, así como modificar y eliminar sistemas existentes.
"Visor de almacenamiento"	Visualizar el estado del almacenamiento y las funciones de gobernanza, así como también los recursos de almacenamiento descubiertos previamente. No se pueden descubrir, modificar ni eliminar sistemas de almacenamiento existentes.
"Especialista en salud del sistema"	Administrar funciones de almacenamiento, salud y gobernanza, todos los permisos del administrador de almacenamiento, excepto no poder modificar ni eliminar sistemas existentes.

Roles de servicio de datos

La siguiente es una lista de roles en la categoría de servicio de datos. Cada rol otorga permisos específicos dentro de su alcance designado. Los usuarios que no tengan el rol de servicio de datos requerido o un rol de plataforma no podrán acceder al servicio de datos.

Rol de servicio de datos	Responsabilidades
"Superadministrador de copias de seguridad y recuperación"	Realice cualquier acción en NetApp Backup and Recovery.

Rol de servicio de datos	Responsabilidades
"Administrador de copias de seguridad y recuperación"	Realice copias de seguridad en instantáneas locales, replique en almacenamiento secundario y realice copias de seguridad en almacenamiento de objetos.
"Administrador de restauración de copias de seguridad y recuperación"	Restaurar cargas de trabajo en Copia de seguridad y recuperación.
"Administrador de clones de Backup and Recovery"	Clonar aplicaciones y datos en Copia de seguridad y recuperación.
"Visor de copias de seguridad y recuperación"	Ver información de copia de seguridad y recuperación.
"Administración de recuperación ante desastres"	Realice cualquier acción en el servicio NetApp Disaster Recovery .
"Administrador de conmutación por error de recuperación ante desastres"	Realizar conmutaciones por error y migraciones.
"Administrador de aplicaciones de recuperación ante desastres"	Cree planes de replicación, cámbielos e inicie conmutaciones por error de prueba.
"Visor de recuperación ante desastres"	Ver sólo información.
Visor de clasificación	Permite a los usuarios ver los resultados del análisis de NetApp Data Classification . Los usuarios con este rol pueden ver información de cumplimiento y generar informes para los recursos a los que tienen permiso de acceso. Estos usuarios no pueden habilitar ni deshabilitar el escaneo de volúmenes, depósitos o esquemas de bases de datos. La clasificación no tiene un rol de administrador.
"Administrador de resiliencia frente al ransomware"	Administre acciones en las pestañas Proteger, Alertas, Recuperar, Configuración e Informes de NetApp Ransomware Resilience.
"Visor de resiliencia contra ransomware"	Vea datos de carga de trabajo, vea datos de alerta, descargue datos de recuperación y descargue informes en Ransomware Resilience.
"Comportamiento del usuario de Resiliencia ante Ransomware"	Configure, administre y visualice la detección, alertas y monitoreo de comportamiento sospechoso de usuarios en Ransomware Resilience.
"Visor del comportamiento del usuario de Ransomware Resilience"	Vea alertas e información sobre comportamiento sospechoso de usuarios en Ransomware Resilience.
Administrador de SnapCenter	Proporciona la capacidad de realizar copias de seguridad de instantáneas de clústeres ONTAP locales mediante NetApp Backup and Recovery para aplicaciones. Un miembro que tiene este rol puede completar las siguientes acciones: * Completar cualquier acción desde Copia de seguridad y recuperación > Aplicaciones * Administrar todos los sistemas en los proyectos y carpetas para los que tiene permisos * Usar todos los servicios de la NetApp Console SnapCenter no tiene un rol de espectador.

Enlaces relacionados

- "Obtenga más información sobre la gestión de identidad y acceso de la NetApp Console"
- "Comience a utilizar NetApp Console IAM"
- "Administrar los miembros de la NetApp Console y sus permisos"
- "Obtenga más información sobre la API para NetApp Console IAM"

Roles de acceso a la plataforma de la NetApp Console

Asigne roles de plataforma a los usuarios para otorgar permisos para administrar la NetApp Console, asignar roles, agregar usuarios, crear agentes de consola y administrar federaciones.

Ejemplo de roles organizacionales para una gran organización multinacional

XYZ Corporation organiza el acceso al almacenamiento de datos por región (América del Norte, Europa y Asia-Pacífico), proporcionando control regional con supervisión centralizada.

El **administrador de la organización** en la consola de XYZ Corporation crea una organización inicial y carpetas separadas para cada región. El administrador de carpeta o proyecto de cada región organiza los proyectos (con los recursos asociados) dentro de la carpeta de la región.

Los administradores regionales con el rol de **Administrador de carpeta o proyecto** administran activamente sus carpetas agregando recursos y usuarios. Estos administradores regionales también pueden agregar, eliminar o cambiar el nombre de las carpetas y los proyectos que administran. El **administrador de la organización** hereda los permisos para cualquier recurso nuevo, lo que mantiene la visibilidad del uso del almacenamiento en toda la organización.

Dentro de la misma organización, a un usuario se le asigna el rol de **administrador de federación** para administrar la federación de la organización con su IdP corporativo. Este usuario puede agregar o eliminar organizaciones federadas, pero no puede administrar usuarios ni recursos dentro de la organización. El **Administrador de la organización** asigna a un usuario el rol de **Visor de la federación** para verificar el estado de la federación y ver las organizaciones federadas.

Las siguientes tablas indican las acciones que cada rol de la plataforma de consola puede realizar.

Roles de administración de la organización

Tarea	Administrador de la organización	Administrador de carpetas o proyectos
Crear agentes	Sí	No
Crear, modificar o eliminar sistemas desde la consola (agregar o descubrir sistemas)	Sí	Sí
Crear carpetas y proyectos, incluida la eliminación	Sí	No
Cambiar el nombre de carpetas y proyectos existentes	Sí	Sí
Asignar roles y agregar usuarios	Sí	Sí
Asociar recursos con carpetas y proyectos	Sí	Sí

Tarea	Administrador de la organización	Administrador de carpetas o proyectos
Asociar agentes con carpetas y proyectos	Sí	No
Eliminar agentes de carpetas y proyectos	Sí	No
Administrar agentes (editar certificados, configuraciones, etc.)	Sí	No
Administrar credenciales desde Administración > Credenciales	Sí	Sí
Crear, administrar y visualizar federaciones	Sí	No
Regístrese para recibir soporte y enviar casos a través de la Consola	Sí	Sí
Utilice servicios de datos que no estén asociados a un rol de acceso explícito	Sí	Sí
Ver la página de Auditoría y notificaciones	Sí	Sí

Roles de la federación

Tarea	Administración de la federación	Visor de la Federación
Crear una federación	Sí	No
Verificar un dominio	Sí	No
Agregar un dominio a una federación	Sí	No
Deshabilitar y eliminar federaciones	Sí	No
Federaciones de pruebas	Sí	No
Ver federaciones y sus detalles	Sí	Sí

Roles de asociación

Tarea	Administración de asociaciones	Visor de asociaciones
Puede crear una asociación	Sí	No
Asignar roles a los miembros del socio	Sí	No
Puede agregar miembros a una asociación	Sí	No
Puede ver los detalles de la asociación de la organización	Sí	Sí

Roles de superadministrador y espectador

El rol de **Superadministrador** proporciona acceso completo para administrar las funciones de la consola, el almacenamiento y los servicios de datos. Este rol es adecuado para aquellos que supervisan la administración y la gobernanza. Por el contrario, el rol de **Supervisor** ofrece acceso de solo lectura, ideal para auditores o

partes interesadas que necesitan visibilidad sin realizar cambios.

Las organizaciones deben utilizar el acceso de **superadministrador** con moderación para minimizar los riesgos de seguridad y alinearse con el principio del mínimo privilegio. La mayoría de las organizaciones deberían asignar roles específicos con solo los permisos necesarios para reducir el riesgo y mejorar la auditabilidad.

Ejemplo de roles super

ABC Corporation tiene un pequeño equipo de cinco personas que aprovecha la NetApp Console para los servicios de datos y la gestión del almacenamiento. En lugar de distribuir múltiples roles, asignan el rol de **Superadministrador** a dos miembros senior del equipo que manejan todas las tareas administrativas, incluida la gestión de usuarios y la configuración de recursos. A los tres miembros restantes del equipo se les asigna el rol de **Supervisor**, lo que les permite supervisar el estado del almacenamiento y el servicio de datos sin la posibilidad de modificar las configuraciones.

Role	Roles heredados
Superadministrador	• Administrador de la organización • Administrador de carpetas o proyectos • Administración de la federación • Administración de asociaciones • Administrador de resiliencia frente al ransomware • Administración de recuperación ante desastres • Superadministrador de respaldo • Administrador de almacenamiento • Administrador de Keystone • Administrador de Google Cloud NetApp Volumes

Role	Roles heredados
Súper espectador	• Visor de la organización • Visor de la Federación • Visor de asociaciones • Visor de resiliencia contra ransomware • Visor de recuperación ante desastres • Visor de copias de seguridad • Visor de almacenamiento • Visor de Keystone • Visor de Google Cloud NetApp Volumes

Roles de aplicación

Funciones de Google Cloud NetApp Volumes en la NetApp Console

Puede asignar la siguiente función a los usuarios para brindarles acceso a Google Cloud NetApp Volumes en la NetApp Console.

Google Cloud NetApp Volumes utiliza la siguiente función:

- * Administrador de Google Cloud NetApp Volumes *: descubre y administra Google Cloud NetApp Volumes en la consola.
- *Visor de Google Cloud NetApp Volumes *: Vea los Google Cloud NetApp Volumes en la consola.

Roles de acceso de Keystone en la NetApp Console

Los roles de Keystone brindan acceso a los paneles de Keystone y permiten a los usuarios ver y administrar su suscripción de Keystone . Hay dos roles de Keystone : administrador de Keystone y visor de Keystone . La principal diferencia entre los dos roles son las acciones que pueden realizar en Keystone. El rol de administrador de Keystone es el único rol que puede crear solicitudes de servicio o modificar suscripciones.

Ejemplo de roles de Keystone en la NetApp Console

XYZ Corporation tiene cuatro ingenieros de almacenamiento de diferentes departamentos que visualizan la información de suscripción de Keystone . Aunque todos estos usuarios necesitan supervisar la suscripción de Keystone , solo el líder del equipo puede realizar solicitudes de servicio. A tres de los miembros del equipo se les asigna el rol de *visualizador de Keystone *, mientras que al líder del equipo se le asigna el rol de *administrador de Keystone * para que haya un punto de control sobre las solicitudes de servicio de la empresa.

La siguiente tabla indica las acciones que puede realizar cada rol de Keystone .

Característica y acción	Administrador de Keystone	Visor de Keystone
Ver las siguientes pestañas: Suscripción, Activos, Monitor y Administración	Sí	Sí
*Página de suscripción de Keystone *:		
Ver suscripciones	Sí	Sí
Modificar o renovar suscripciones	Sí	No
*Página de activos de Keystone *:		
Ver activos	Sí	Sí
Administrar activos	Sí	No
*Página de alertas de Keystone *:		
Ver alertas	Sí	Sí
Administrar alertas	Sí	No
Crear alertas para mí mismo	Sí	Sí
* Licenses and subscriptions*:		
Puede ver licencias y suscripciones	Sí	Sí
*Página de informes de Keystone *:		
Descargar informes	Sí	Sí
Administrar informes	Sí	Sí
Crear informes para uno mismo	Sí	Sí
Solicitudes de servicio:		
Crear solicitudes de servicio	Sí	No
Ver solicitudes de servicio creadas por cualquier usuario dentro de la Organización	Sí	Sí

Rol de acceso de analista de soporte operativo para la NetApp Console

Puede asignar el rol de analista de soporte operativo a los usuarios para brindarles acceso a alertas y monitoreo. Los usuarios con este rol también pueden abrir casos de soporte.

Analista de soporte operativo

Tarea	Puede realizar
Administre sus propias credenciales de usuario desde Configuración > Credenciales	Sí
Ver recursos descubiertos	Sí
Regístrese para recibir soporte y enviar casos a través de la Consola	Sí
Ver la página de Auditoría y notificaciones	Sí
Ver, descargar y configurar alertas	Sí

Roles de acceso al almacenamiento para la NetApp Console

Puede asignar los siguientes roles a los usuarios para brindarles acceso a las funciones de administración de almacenamiento en la NetApp Console. Puede asignar a los usuarios un rol administrativo para administrar el almacenamiento o un rol de espectador para monitorear.

Estos roles no están disponibles desde la API de asociación de la NetApp Console .

Los administradores pueden asignar roles de almacenamiento a los usuarios para los siguientes recursos y funciones de almacenamiento:

Recursos de almacenamiento:

- Clústeres ONTAP locales
- StorageGRID
- Serie E

Servicios y características de la consola:

- Asesor digital
- Actualizaciones de software
- Planificación del ciclo de vida
- Sostenibilidad

Ejemplo de roles de almacenamiento en la NetApp Console

XYZ Corporation, una empresa multinacional, tiene un gran equipo de ingenieros de almacenamiento y administradores de almacenamiento. Permiten que este equipo administre los activos de almacenamiento de sus regiones y al mismo tiempo limite el acceso a las tareas principales de la consola, como la administración de usuarios, la creación de agentes y la administración de licencias.

Dentro de un equipo de 12 personas, a dos usuarios se les asigna el rol de **Visor de almacenamiento**, que les permite supervisar los recursos de almacenamiento asociados con los proyectos de consola a los que están asignados. A los nueve restantes se les asigna el rol de **administrador de almacenamiento**, que

incluye la capacidad de administrar actualizaciones de software, acceder a ONTAP System Manager a través de la consola y también descubrir recursos de almacenamiento (agregar sistemas). A una persona del equipo se le asigna el rol de **Especialista en salud del sistema** para que pueda administrar la salud de los recursos de almacenamiento en su región, pero no modificar ni eliminar ningún sistema. Esta persona también puede realizar actualizaciones de software en los recursos de almacenamiento para los proyectos que se le asignan.

La organización tiene dos usuarios adicionales con el rol de **Administrador de la organización** que pueden administrar todos los aspectos de la Consola, incluida la administración de usuarios, la creación de agentes y la administración de licencias, así como varios usuarios con el rol de **Administrador de carpeta o proyecto** que pueden realizar tareas de administración de la Consola para las carpetas y los proyectos a los que están asignados.

La siguiente tabla muestra las acciones que realiza cada rol de almacenamiento.

Característica y acción	Administrador de almacenamiento	Especialista en salud del sistema	Visor de almacenamiento
Gestión de almacenamiento:			
Descubrir nuevos recursos (crear sistemas)	Sí	Sí	No
Ver sistemas descubiertos	Sí	Sí	No
Eliminar sistemas de la consola	Sí	No	No
Modificar sistemas	Sí	No	No
Crear agentes	No	No	No
Asesor digital			
Ver todas las páginas y funciones	Sí	Sí	Sí
* Licenses and subscriptions*			
Ver todas las páginas y funciones	No	No	No
Actualizaciones de software			
Ver página de destino y recomendaciones	Sí	Sí	Sí
Revise las posibles recomendaciones de versiones y los beneficios clave	Sí	Sí	Sí
Ver detalles de actualización de un clúster	Sí	Sí	Sí
Ejecute comprobaciones previas a la actualización y descargue el plan de actualización	Sí	Sí	Sí
Instalar actualizaciones de software	Sí	Sí	No
Planificación del ciclo de vida			

Característica y acción	Administrador de almacenamiento	Especialista en salud del sistema	Visor de almacenamiento
Revisar el estado de la planificación de la capacidad	Sí	Sí	Sí
Elija la siguiente acción (mejor práctica, nivel)	Sí	No	No
Almacene datos fríos en la nube y libere espacio	Sí	Sí	No
Configurar recordatorios	Sí	Sí	Sí
Sostenibilidad			
Ver el panel de control y las recomendaciones	Sí	Sí	Sí
Descargar datos del informe	Sí	Sí	Sí
Editar el porcentaje de mitigación de carbono	Sí	Sí	No
Recomendaciones de corrección	Sí	Sí	No
Aplazar recomendaciones	Sí	Sí	No
Acceso de administrador del sistema			
Puede ingresar credenciales	Sí	Sí	No
Cartas credenciales			
Credenciales de usuario	Sí	Sí	No

Roles de servicios de datos

Funciones de NetApp Backup and Recovery en la NetApp Console

Puede asignar los siguientes roles a los usuarios para brindarles acceso a NetApp Backup and Recovery dentro de la consola. Los roles de respaldo y recuperación le brindan la flexibilidad de asignar a los usuarios un rol específico para las tareas que necesitan realizar dentro de su organización. La forma de asignar roles depende de su propio negocio y de sus prácticas de gestión de almacenamiento.

El servicio utiliza los siguientes roles que son específicos de NetApp Backup and Recovery.

- **Superadministrador de Backup and Recovery**: realiza cualquier acción en NetApp Backup and Recovery.
- **Administrador de copias de seguridad y recuperación**: realice copias de seguridad en instantáneas locales, replique en almacenamiento secundario y realice copias de seguridad en acciones de

almacenamiento de objetos en NetApp Backup and Recovery.

- **Administrador de restauración de copias de seguridad y recuperación**: restaure cargas de trabajo mediante NetApp Backup and Recovery.
- **Administrador de clones de respaldo y recuperación**: clona aplicaciones y datos usando NetApp Backup and Recovery.
- **Visor de copias de seguridad y recuperación**: ve información en NetApp Backup and Recovery, pero no realiza ninguna acción.

Para obtener detalles sobre todos los roles de acceso a la NetApp Console , consulte "La documentación de configuración y administración de la consola" .

Roles utilizados para acciones comunes

La siguiente tabla indica las acciones que cada rol de NetApp Backup and Recovery puede realizar para todas las cargas de trabajo.

Característica y acción	Superadministrador de copias de seguridad y recuperación	Administrador de copias de seguridad y recuperación	Administrador de restauración de copias de seguridad y recuperación	Administrador de clones de Backup and Recovery	Visor de copias de seguridad y recuperación
Agregar, editar o eliminar hosts	Sí	No	No	No	No
Instalar complementos	Sí	No	No	No	No
Agregar credenciales (host, instancia, vCenter)	Sí	No	No	No	No
Ver el panel y todas las pestañas	Sí	Sí	Sí	Sí	Sí
Comience una prueba gratuita	Sí	No	No	No	No
Iniciar el descubrimiento de cargas de trabajo	No	Sí	Sí	Sí	No
Ver información de la licencia	Sí	Sí	Sí	Sí	Sí
Activar licencia	Sí	No	No	No	No
Ver anfitriones	Sí	Sí	Sí	Sí	Sí
Horarios:					
Activar horarios	Sí	Sí	Sí	Sí	No

Característica y acción	Superadministrador de copias de seguridad y recuperación	Administrador de copias de seguridad y recuperación	Administrador de restauración de copias de seguridad y recuperación	Administrador de clones de Backup and Recovery	Visor de copias de seguridad y recuperación
Suspender horarios	Sí	Sí	Sí	Sí	No
Políticas y protección:					
Ver planes de protección	Sí	Sí	Sí	Sí	Sí
Crear, modificar o eliminar planes de protección	Sí	Sí	No	No	No
Restaurar cargas de trabajo	Sí	No	Sí	No	No
Crear, dividir o eliminar clones	Sí	No	No	Sí	No
Crear, modificar o eliminar una política	Sí	Sí	No	No	No
Informes:					
Ver informes	Sí	Sí	Sí	Sí	Sí
Crear informes	Sí	Sí	Sí	Sí	No
Eliminar informes	Sí	No	No	No	No
Importar desde SnapCenter y administrar el host:					
Ver datos importados de SnapCenter	Sí	Sí	Sí	Sí	Sí
Importar datos desde SnapCenter	Sí	Sí	No	No	No
Administrar (migrar) host	Sí	Sí	No	No	No
Configurar ajustes:					
Configurar el directorio de registro	Sí	Sí	Sí	No	No
Asociar o eliminar credenciales de instancia	Sí	Sí	Sí	No	No
Cubos:					

Característica y acción	Superadministrador de copias de seguridad y recuperación	Administrador de copias de seguridad y recuperación	Administrador de restauración de copias de seguridad y recuperación	Administrador de clones de Backup and Recovery	Visor de copias de seguridad y recuperación
Ver depósitos	Sí	Sí	Sí	Sí	Sí
Crear, editar o eliminar un depósito	Sí	Sí	No	No	No

Roles utilizados para acciones específicas de la carga de trabajo

La siguiente tabla indica las acciones que cada rol de NetApp Backup and Recovery puede realizar para cargas de trabajo específicas.

Cargas de trabajo de Kubernetes

Esta tabla indica las acciones que cada rol de NetApp Backup and Recovery puede realizar para acciones específicas de las cargas de trabajo de Kubernetes.

Característica y acción	Superadministrador de copias de seguridad y recuperación	Administrador de copias de seguridad y recuperación	Administrador de restauración de copias de seguridad y recuperación	Visor de copias de seguridad y recuperación
Ver clústeres, espacios de nombres, clases de almacenamiento y recursos de API	Sí	Sí	Sí	Sí
Agregar nuevos clústeres de Kubernetes	Sí	Sí	No	No
Actualizar las configuraciones del clúster	Sí	No	No	No
Eliminar clústeres de la administración	Sí	No	No	No
Ver aplicaciones	Sí	Sí	Sí	Sí
Crear y definir nuevas aplicaciones	Sí	Sí	No	No
Actualizar las configuraciones de la aplicación	Sí	Sí	No	No
Eliminar aplicaciones de la administración	Sí	Sí	No	No

Característica y acción	Superadministrador de copias de seguridad y recuperación	Administrador de copias de seguridad y recuperación	Administrador de restauración de copias de seguridad y recuperación	Visor de copias de seguridad y recuperación
Ver los recursos protegidos y el estado de la copia de seguridad	Sí	Sí	Sí	Sí
Cree copias de seguridad y proteja aplicaciones con políticas	Sí	Sí	No	No
Desproteger aplicaciones y eliminar copias de seguridad	Sí	Sí	No	No
Ver puntos de recuperación y resultados del visor de recursos	Sí	Sí	Sí	Sí
Restaurar aplicaciones desde puntos de recuperación	Sí	No	Sí	No
Ver las políticas de respaldo de Kubernetes	Sí	Sí	Sí	Sí
Crear políticas de respaldo de Kubernetes	Sí	Sí	Sí	No
Actualizar las políticas de respaldo	Sí	Sí	Sí	No
Eliminar políticas de copia de seguridad	Sí	Sí	Sí	No
Ver ganchos de ejecución y fuentes de ganchos	Sí	Sí	Sí	Sí
Crear ganchos de ejecución y fuentes de gancho	Sí	Sí	Sí	No
Actualizar los ganchos de ejecución y las fuentes de los ganchos	Sí	Sí	Sí	No
Eliminar ganchos de ejecución y fuentes de ganchos	Sí	Sí	Sí	No
Ver plantillas de gancho de ejecución	Sí	Sí	Sí	Sí

Característica y acción	Superadministrador de copias de seguridad y recuperación	Administrador de copias de seguridad y recuperación	Administrador de restauración de copias de seguridad y recuperación	Visor de copias de seguridad y recuperación
Crear plantillas de gancho de ejecución	Sí	Sí	Sí	No
Actualizar plantillas de gancho de ejecución	Sí	Sí	Sí	No
Eliminar plantillas de gancho de ejecución	Sí	Sí	Sí	No
Ver el resumen de la carga de trabajo y los paneles de análisis	Sí	Sí	Sí	Sí
Ver depósitos y destinos de almacenamiento de StorageGRID	Sí	Sí	Sí	Sí

Funciones de NetApp Disaster Recovery en la NetApp Console

Puede asignar los siguientes roles a los usuarios para brindarles acceso a NetApp Disaster Recovery dentro de la consola. Los roles de recuperación ante desastres le brindan la flexibilidad de asignar a los usuarios un rol específico para las tareas que necesitan realizar dentro de su organización. La forma de asignar roles depende de su propio negocio y de sus prácticas de gestión de almacenamiento.

La recuperación ante desastres utiliza los siguientes roles:

- **Administrador de recuperación ante desastres**: Realizar cualquier acción.
- **Administrador de conmutación por error de recuperación ante desastres**: realiza conmutaciones por error y migraciones.
- **Administrador de aplicaciones de recuperación ante desastres**: crear planes de replicación. Modificar los planes de replicación. Iniciar pruebas de conmutación por error.
- **Visor de recuperación ante desastres**: Ver solo información.

La siguiente tabla indica las acciones que puede realizar cada rol.

Característica y acción	Administración de recuperación ante desastres	Administrador de conmutación por error de recuperación ante desastres	Administrador de aplicaciones de recuperación ante desastres	Visor de recuperación ante desastres
Ver el panel y todas las pestañas	Sí	Sí	Sí	Sí
Comience una prueba gratuita	Sí	No	No	No

Característica y acción	Administración de recuperación ante desastres	Administrador de conmutación por error de recuperación ante desastres	Administrador de aplicaciones de recuperación ante desastres	Visor de recuperación ante desastres
Iniciar el descubrimiento de cargas de trabajo	Sí	No	No	No
Ver información de la licencia	Sí	Sí	Sí	Sí
Activar licencia	Sí	No	Sí	No
En la pestaña Sitios:				
Ver sitios	Sí	Sí	Sí	Sí
Agregar, modificar o eliminar sitios	Sí	No	No	No
En la pestaña Planes de replicación:				
Ver planes de replicación	Sí	Sí	Sí	Sí
Ver detalles del plan de replicación	Sí	Sí	Sí	Sí
Crear o modificar planes de replicación	Sí	Sí	Sí	No
Crear informes	Sí	No	No	No
Ver instantáneas	Sí	Sí	Sí	Sí
Realizar pruebas de conmutación por error	Sí	Sí	Sí	No
Realizar conmutaciones por error	Sí	Sí	No	No
Realizar conmutaciones por recuperación	Sí	Sí	No	No
Realizar migraciones	Sí	Sí	No	No
En la pestaña Grupos de recursos:				
Ver grupos de recursos	Sí	Sí	Sí	Sí
Crear, modificar o eliminar grupos de recursos	Sí	No	Sí	No
En la pestaña Supervisión de trabajos:				
Ver trabajos	Sí	No	Sí	Sí

Característica y acción	Administración de recuperación ante desastres	Administrador de conmutación por error de recuperación ante desastres	Administrador de aplicaciones de recuperación ante desastres	Visor de recuperación ante desastres
Cancelar trabajos	Sí	Sí	Sí	No

Roles de acceso de resiliencia contra ransomware para la NetApp Console

Los roles de resiliencia contra ransomware brindan a los usuarios acceso a NetApp Ransomware Resilience. Ransomware Resilience admite las siguientes funciones:

Roles de base

- Administrador de resiliencia contra ransomware: configure los ajustes de resiliencia contra ransomware; investigue y responda a las alertas de cifrado
- Visor de resiliencia contra ransomware: vea incidentes de cifrado, informes y configuraciones de detección

Roles de actividad de comportamiento del usuario"Detección de actividad sospechosa de usuarios" Las alertas proporcionan visibilidad de datos tales como eventos de actividad de archivos; estas alertas incluyen nombres de archivos y acciones de archivos (como leer, escribir, eliminar, cambiar nombre) realizadas por el usuario. Para limitar la visibilidad de estos datos, solo los usuarios con estos roles pueden administrar o ver estas alertas.

- Administrador de comportamiento del usuario de Ransomware Resilience: active la detección de actividad sospechosa de usuarios, investigue y responda a las alertas de actividad sospechosa de usuarios
- Visor de comportamiento del usuario de Ransomware Resilience: vea alertas de actividad sospechosa del usuario

> Los roles de comportamiento del usuario no son roles independientes; están diseñados para agregarse a los roles de administrador o espectador de Ransomware Resilience. Para obtener más información, consulte Roles de comportamiento del usuario.

Consulte las siguientes tablas para obtener descripciones detalladas de cada función.

Roles de base

La siguiente tabla describe las acciones disponibles para los roles de administrador y espectador de Ransomware Resilience.

Característica y acción	Administrador de resiliencia frente al ransomware	Visor de resiliencia contra ransomware
Ver el panel y todas las pestañas	Sí	Sí
En el panel, actualice el estado de la recomendación	Sí	No
Comience una prueba gratuita	Sí	No

Característica y acción	Administrador de resiliencia frente al ransomware	Visor de resiliencia contra ransomware
Iniciar el descubrimiento de cargas de trabajo	Sí	No
Iniciar el redescubrimiento de cargas de trabajo	Sí	No
En la pestaña Proteger:		
Agregar, modificar o eliminar planes de protección para políticas de *cifrado*	Sí	No
Proteger las cargas de trabajo	Sí	No
Identifique la exposición a datos confidenciales con la clasificación de datos	Sí	No
Enumere los planes de protección y los detalles	Sí	Sí
Lista de grupos de protección	Sí	Sí
Ver detalles del grupo de protección	Sí	Sí
Crear, editar o eliminar grupos de protección	Sí	No
Descargar datos	Sí	Sí
En la pestaña Alertas:		
Ver alertas de cifrado y detalles de alertas	Sí	Sí
Editar el estado del incidente de cifrado	Sí	No
Marcar alerta de cifrado para recuperación	Sí	No
Ver detalles del incidente de cifrado	Sí	Sí
Descartar o resolver incidentes de cifrado	Sí	No
Obtenga la lista completa de archivos afectados en el evento de cifrado	Sí	No
Descargar datos de alertas de eventos de cifrado	Sí	Sí
Bloquear usuario (con configuración del agente de Workload Security)	Sí	No
En la pestaña Recuperar:		
Descargar archivos afectados por el evento de cifrado	Sí	No

Característica y acción	Administrador de resiliencia frente al ransomware	Visor de resiliencia contra ransomware
Restaurar la carga de trabajo a partir de un evento de cifrado	Sí	No
Descargar datos de recuperación del evento de cifrado	Sí	Sí
Descargar informes de eventos de cifrado	Sí	Sí
En la pestaña Configuración:		
Agregar o modificar destinos de copia de seguridad	Sí	No
Lista de destinos de copia de seguridad	Sí	Sí
Ver objetivos SIEM conectados	Sí	Sí
Agregar o modificar objetivos SIEM	Sí	No
Configurar el simulacro de preparación	Sí	No
Iniciar, reiniciar o editar el simulacro de preparación	Sí	No
Revisar el estado del simulacro de preparación	Sí	Sí
Actualizar la configuración de descubrimiento	Sí	No
Ver configuración de descubrimiento	Sí	Sí
En la pestaña Informes:		
Descargar informes	Sí	Sí

Roles de comportamiento del usuario

Para configurar los ajustes de comportamiento de usuario sospechoso y responder a las alertas, un usuario debe tener el rol de administrador de comportamiento de usuario de Ransomware Resilience. Para ver únicamente alertas de comportamiento sospechoso del usuario, el usuario debe tener el rol de visualizador de comportamiento del usuario de Ransomware Resilience.

Los roles de comportamiento del usuario deben otorgarse a los usuarios con privilegios de administrador o espectador de Ransomware Resilience existentes que necesitan acceso a"Configuración y alertas de actividad de usuario sospechosa" . Un usuario con el rol de administrador de Ransomware Resilience, por ejemplo, debería recibir el rol de administrador de comportamiento de usuario de Ransomware Resilience para configurar agentes de actividad de usuario y bloquear o desbloquear usuarios. El rol de administrador de comportamiento del usuario de Ransomware Resilience no debe otorgarse a un visor de Ransomware Resilience.

Para activar la detección de actividad de usuarios sospechosos, debe tener el rol de administrador de la organización de la consola.

La siguiente tabla describe las acciones disponibles para los roles de administrador y espectador del comportamiento del usuario de Ransomware Resilience.

Característica y acción	Comportamiento del usuario de Resiliencia ante Ransomware	Visor del comportamiento del usuario de Ransomware Resilience
En la pestaña Configuración:		
Crear, modificar o eliminar un agente de actividad del usuario	Sí	No
Crear o eliminar el conector del directorio de usuarios	Sí	No
Pausar o reanudar el recopilador de datos	Sí	No
Realizar un simulacro de preparación ante una violación de datos	Sí	No
En la pestaña Proteger:		
Agregar, modificar o eliminar planes de protección para políticas de *comportamiento sospechoso de usuarios*	Sí	No
En la pestaña Alertas:		
Ver alertas de actividad del usuario y detalles de las alertas	Sí	Sí
Editar el estado del incidente de actividad del usuario	Sí	No
Marcar la alerta de actividad del usuario para recuperación	Sí	No
Ver detalles de incidentes de actividad del usuario	Sí	Sí
Descartar o resolver incidentes de actividad del usuario	Sí	No
Obtenga una lista completa de archivos afectados por usuarios sospechosos	Sí	Sí
Descargar datos de alertas de eventos de actividad del usuario	Sí	Sí
Bloquear o desbloquear usuario	Sí	No
En la pestaña Recuperar:		
Descargar archivos afectados por el evento de actividad del usuario	Sí	No

Característica y acción	Comportamiento del usuario de Resiliencia ante Ransomware	Visor del comportamiento del usuario de Ransomware Resilience
Restaurar la carga de trabajo a partir del evento de actividad del usuario	Sí	No
Descargar datos de recuperación del evento de actividad del usuario	Sí	Sí
Descargar informes de eventos de actividad del usuario	Sí	Sí