Roles de servicios de datos

NetApp Console setup and administration

NetApp
January 13, 2026

Tabla de contenidos

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

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 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
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

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
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:					
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

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
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
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

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
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
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
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

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
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
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
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

Característica y acción	Administrador de resiliencia frente al ransomware	Visor de resiliencia contra ransomware
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
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

Característica y acción	Comportamiento del usuario de Resiliencia ante Ransomware	Visor del comportamiento del usuario de Ransomware Resilience
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
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