Utilice la resiliencia frente al ransomware

NetApp Ransomware Resilience

NetApp
March 12, 2026

Tabla de contenidos

Utilice la resiliencia frente al ransomware

Acceda a la NetApp Ransomware Resilience

Para acceder a NetApp Ransomware Resilience, tienes que iniciar sesión a través de la NetApp Console.

Para iniciar sesión en la consola, puede usar sus credenciales del sitio de soporte de NetApp o puede registrarse para iniciar sesión en la nube de NetApp usando su correo electrónico y una contraseña. "Obtenga más información sobre cómo iniciar sesión" .

Rol de consola requerido Para realizar esta tarea, necesita el rol de administrador de la organización, administrador de carpeta o proyecto, administrador de resiliencia ante ransomware o visor de resiliencia ante ransomware. "Obtenga información sobre las funciones de resiliencia ante ransomware para la NetApp Console" .

Pasos

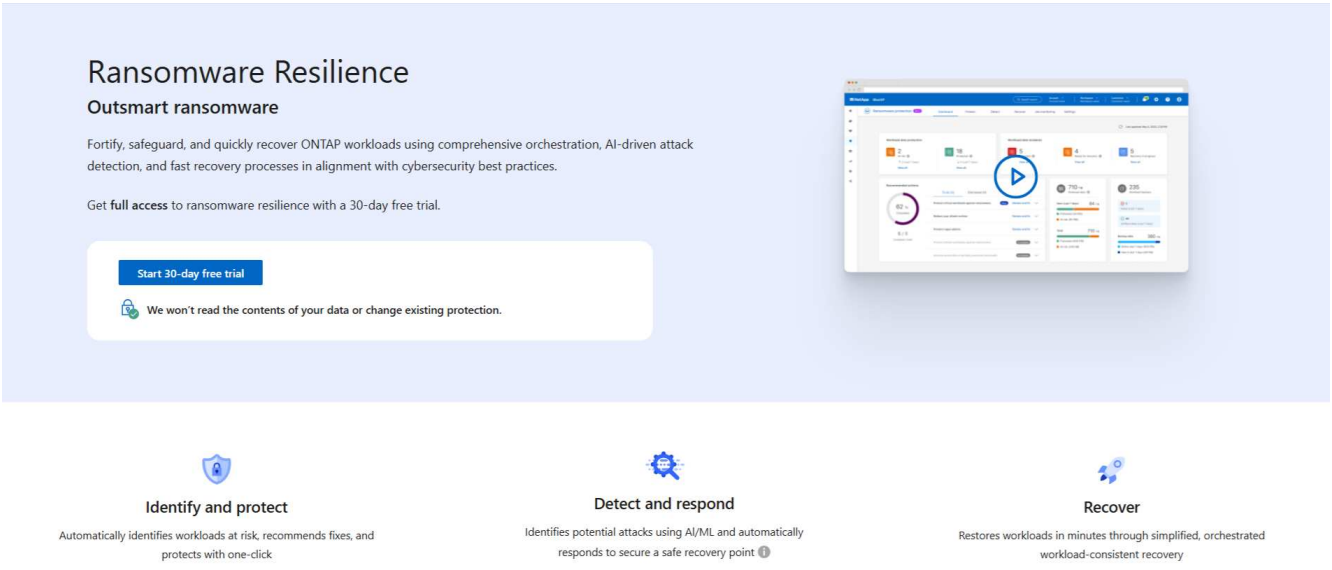
1. Abra un navegador web y vaya a"la consola" .

   Aparece la página de inicio de sesión de la consola.

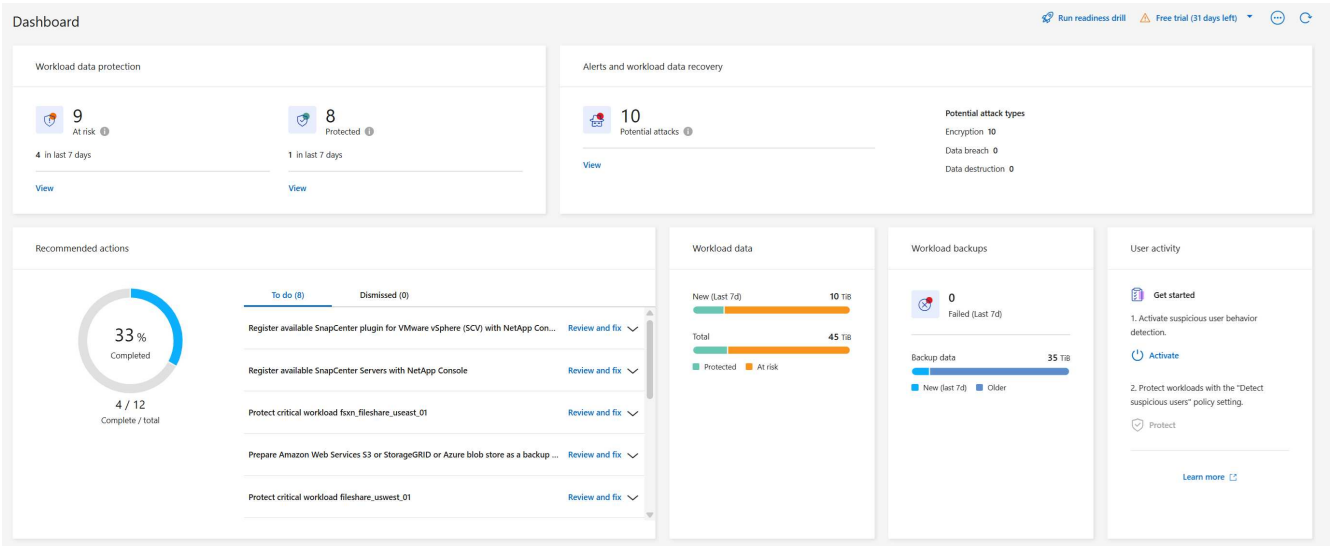
2. Inicie sesión en la consola.
3. Desde la navegación izquierda de la Consola, seleccione **Protección** > **Resiliencia ante ransomware**.

   Si es la primera vez que inicia sesión en este servicio, aparecerá la página de destino.

   Si no tiene un agente de consola o no es el adecuado para este servicio, deberá implementar uno. "Aprenda a configurar un agente de consola" .



   De lo contrario, aparecerá el panel de resiliencia ante ransomware.



4. Si aún no lo ha hecho, seleccione la opción **Descubrir cargas de trabajo**.

   Consulte "Descubrir cargas de trabajo" .

Supervisa la salud de la carga de trabajo en NetApp Ransomware Resilience

El panel NetApp Ransomware Resilience te da información de un vistazo sobre la salud de la protección de tus cargas de trabajo. Puedes determinar rápidamente qué cargas de trabajo están en riesgo o protegidas, identificar las cargas de trabajo afectadas por un incidente o en recuperación, y medir el alcance de la protección viendo cuánto almacenamiento está protegido o en riesgo.

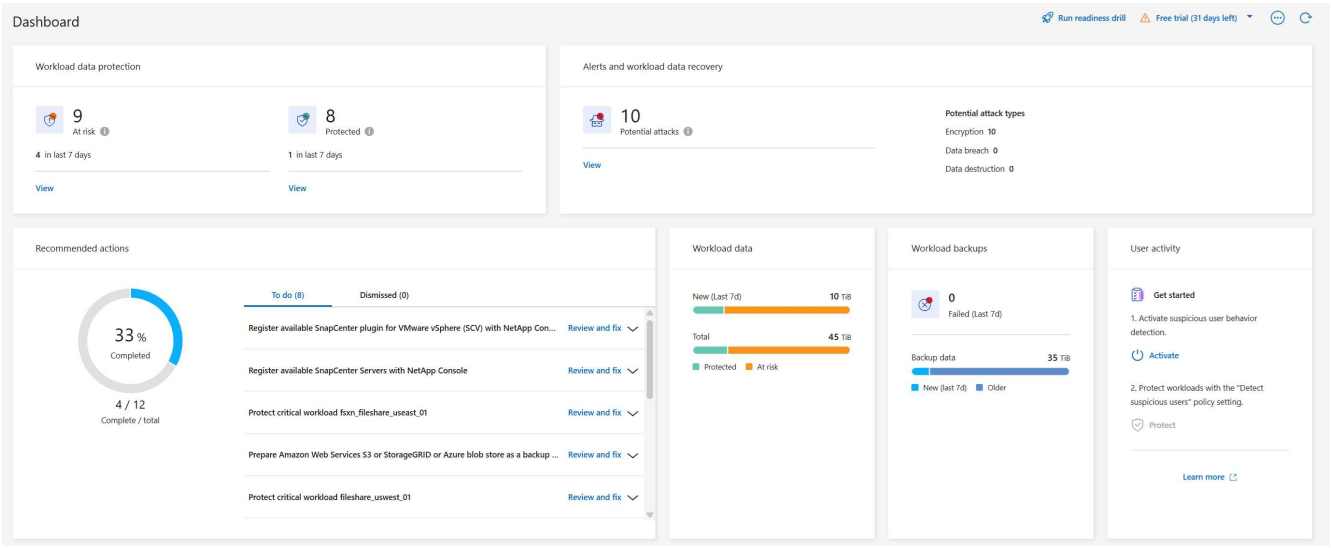
Usa el panel de control para revisar las sugerencias de protección, cambiar la configuración y descargar informes.

Rol de consola requerido Para realizar esta tarea, necesita el rol de administrador de la organización, administrador de carpeta o proyecto, administrador de resiliencia ante ransomware o visor de resiliencia ante ransomware. "Obtenga información sobre las funciones de resiliencia ante ransomware para la NetApp Console" .

Revisa la salud de la carga de trabajo usando el panel de control

Pasos

1. Una vez que la consola descubre sus cargas de trabajo, el panel de resiliencia ante ransomware muestra el estado de protección de datos de la carga de trabajo.



2. Desde el panel de control, puedes hacer las siguientes acciones en cada uno de los paneles:

   - **Protección de datos de carga de trabajo**: seleccione **Ver todo** para ver todas las cargas de trabajo que están en riesgo o protegidas en la página Protección. Las cargas de trabajo están en riesgo cuando los niveles de protección no coinciden con una política de protección. Consulte "Proteger las cargas de trabajo" .

     Seleccione la información sobre herramientas "i" para ver sugerencias sobre estos datos. Para aumentar el límite de carga de trabajo, seleccione **Aumentar el límite de carga de trabajo** dentro de esta nota. Al seleccionar esta opción se le dirigirá a la página de Soporte de la consola, donde podrá crear un ticket de caso.

   - **Alertas y recuperación de datos de carga de trabajo**: seleccione **Ver todo** para ver los incidentes activos que han afectado su carga de trabajo, que están listos para recuperarse después de que se neutralicen los incidentes o que están en recuperación. Consulte "Responder a una alerta detectada" .
     - Un incidente se clasifica en uno de los siguientes estados:
       - Nuevo
       - Despedido
       - Despedir
       - Resuelto
     - Una alerta puede tener uno de los siguientes estados:
       - Nuevo
       - Inactivo
     - Una carga de trabajo puede tener uno de los siguientes estados de restauración:
       - Se necesita restaurar
       - En curso
       - Restaurado
       - Con errores
   - **Acciones recomendadas**: Para aumentar la protección, revise cada recomendación y luego seleccione **Revisar y corregir**.

Consulta "Revisa las sugerencias de protección en el dashboard" o "Proteger las cargas de trabajo".

Ransomware Resilience muestra nuevas recomendaciones desde tu última visita al panel con la etiqueta "Nuevo" durante 24 horas. Las acciones aparecen en orden de prioridad, con la más importante arriba. Revisa, actúa o descarta cada recomendación.

El número total de acciones no incluye las acciones que usted desestimó.

- **Datos de carga de trabajo**: Supervise los cambios en la cobertura de protección durante los últimos 7 días.
- **Copias de seguridad de la carga de trabajo**: supervisa los cambios en las copias de seguridad de la carga de trabajo creadas por Ransomware Resilience que fallaron o se completaron correctamente en los últimos 7 días.

Revisa las recomendaciones de protección en el panel de control

Ransomware Resilience evalúa la protección de sus cargas de trabajo y recomienda acciones para mejorar esa protección.

Puede revisar una recomendación y actuar en consecuencia, lo que cambia el estado de la recomendación a Completada. O, si deseas actuar sobre ello más tarde, puedes descartarlo. Al descartar una acción, la recomendación se mueve a una lista de acciones descartadas, que puedes revisar más tarde.

A continuación se muestra una muestra de las recomendaciones que ofrece Ransomware Resilience.

Recomendación	Descripción	Cómo resolverlo
Agregue una política de protección contra ransomware.	La carga de trabajo actualmente no está protegida.	Asignar una política a la carga de trabajo. Consulte "Proteja las cargas de trabajo contra ataques de ransomware" .
Conéctese a SIEM para generar informes de amenazas.	Envía datos a un sistema de gestión de eventos y seguridad (SIEM) para el análisis y detección de amenazas.	Introduce los detalles del servidor SIEM/XDR para activar la detección de amenazas. Consulta "Conéctate a un SIEM".
Mejorar la postura de seguridad del sistema	NetApp Digital Advisor ha identificado al menos un riesgo de seguridad alto o crítico.	Revise todos los riesgos de seguridad en NetApp Digital Advisor. Referirse a "Documentación de Digital Advisor" .
Hacer una política más fuerte.	Es posible que algunas cargas de trabajo no tengan suficiente protección. Fortalecer la protección de las cargas de trabajo con una política.	Aumente la retención, agregue copias de seguridad, aplique copias de seguridad inmutables, bloquee extensiones de archivos sospechosas, habilite la detección en almacenamiento secundario y más. Consulte "Proteja las cargas de trabajo contra ataques de ransomware" .

Recomendación	Descripción	Cómo resolverlo
Prepare <proveedor de respaldo> como destino de respaldo para realizar una copia de seguridad de los datos de su carga de trabajo.	La carga de trabajo actualmente no tiene ningún destino de respaldo.	Agrega destinos de backup a esta carga de trabajo para protegerla. Consulta "Agregar un destino de respaldo".
Proteja cargas de trabajo de aplicaciones críticas o muy importantes contra ransomware.	La página Proteger muestra cargas de trabajo de aplicaciones críticas o muy importantes (según el nivel de prioridad asignado) que no están protegidas.	Asignar una política a estas cargas de trabajo. Consulte "Proteja las cargas de trabajo contra ataques de ransomware" .
Proteja cargas de trabajo de recursos compartidos de archivos críticos o muy importantes contra ransomware.	La página Protección muestra cargas de trabajo críticas o muy importantes del tipo recurso compartido de archivos o almacén de datos que no están protegidas.	Asigna una política a cada una de las cargas de trabajo. Consulta "Proteja las cargas de trabajo contra ataques de ransomware". Consulta "Proteja las cargas de trabajo contra ataques de ransomware". Consulta "Proteja las cargas de trabajo contra ataques de ransomware".
Revisar nuevas alertas.	Existen nuevas alertas.	Revise las nuevas alertas. Consulte "Responder a una alerta de ransomware detectada" .

Pasos

1. Desde el panel Acciones recomendadas en Ransomware Resilience, seleccione una recomendación y luego **Revisar y corregir**.
2. Para descartar la acción hasta más tarde, seleccione **Descartar**.

   La recomendación desaparece de la lista de tareas pendientes y aparece en la lista de descartadas.

   Más tarde puedes cambiar un elemento descartado a un elemento por hacer. Cuando marcas un elemento como completado o cambias un elemento descartado a una acción por hacer, el Total de acciones aumenta en 1.

3. Para revisar información sobre cómo actuar según las recomendaciones, seleccione el ícono **información**.

Exportar datos de protección a archivos CSV

Puede exportar datos y descargar archivos CSV que muestran detalles de protección, alertas y recuperación.

Puedes descargar archivos CSV desde cualquiera de las opciones del menú principal:

- **Protección**: Contiene el estado y los detalles de todas las cargas de trabajo, incluida la cantidad total de cargas de trabajo que Ransomware Resilience marca como protegidas o en riesgo.
- **Alertas**: Incluye el estado y los detalles de todas las alertas, incluido el número total de alertas e instantáneas automatizadas.
- **Recuperación**: incluye el estado y los detalles de todas las cargas de trabajo que necesitan restaurarse, incluida la cantidad total de cargas de trabajo que Ransomware Resilience marca como "Restauración

necesaria", "En progreso", "Restauración fallida" y "Restaurada exitosamente".

La descarga de un archivo CSV de una página incluye solo los datos de esa página.

Los archivos CSV incluyen datos de todas las cargas de trabajo en todos los sistemas de consola.

Pasos

1. Desde el panel de Resiliencia contra Ransomware, seleccione **Actualizar** Opción en la parte superior derecha para actualizar los datos que aparecerán en los archivos.
2. Debe realizar una de las siguientes acciones:
   - Desde la página, seleccione **Descargar** opción.
   - En el menú Resiliencia ante ransomware, seleccione **Informes**.
3. Si seleccionó la opción **Informes**, seleccione uno de los archivos nombrados preconfigurados y luego seleccione **Descargar (CSV)** o **Descargar (JSON)**.

Acceder a la documentación técnica

Puede acceder a la documentación técnica de Ransomware Resilience desde"docs.netapp.com" o desde dentro de Ransomware Resilience.

Pasos

1. Desde el panel de Resiliencia contra ransomware, seleccione la opción vertical *Acciones* opción.
2. Seleccione una de estas opciones:
   - **Novedades** para ver información sobre las características de la versión actual o anterior en las Notas de la versión.
   - **Documentación** para ver la página de inicio de la documentación de Ransomware Resilience y esta documentación.

Protégete y detecta

Revisa el estado de la protección en NetApp Ransomware Resilience

El panel de protección de NetApp Ransomware Resilience te da una visión general del estado de protección y la preparación de tus cargas de trabajo. Usa el panel de protección para ver qué está protegido, qué necesita protección y cuál es el alcance de la protección.

Una vez que entiendas el alcance de tu protección actual, "puedes crear y aplicar estrategias de protección contra ransomware a tus cargas de trabajo".

Ver la protección en una carga de trabajo

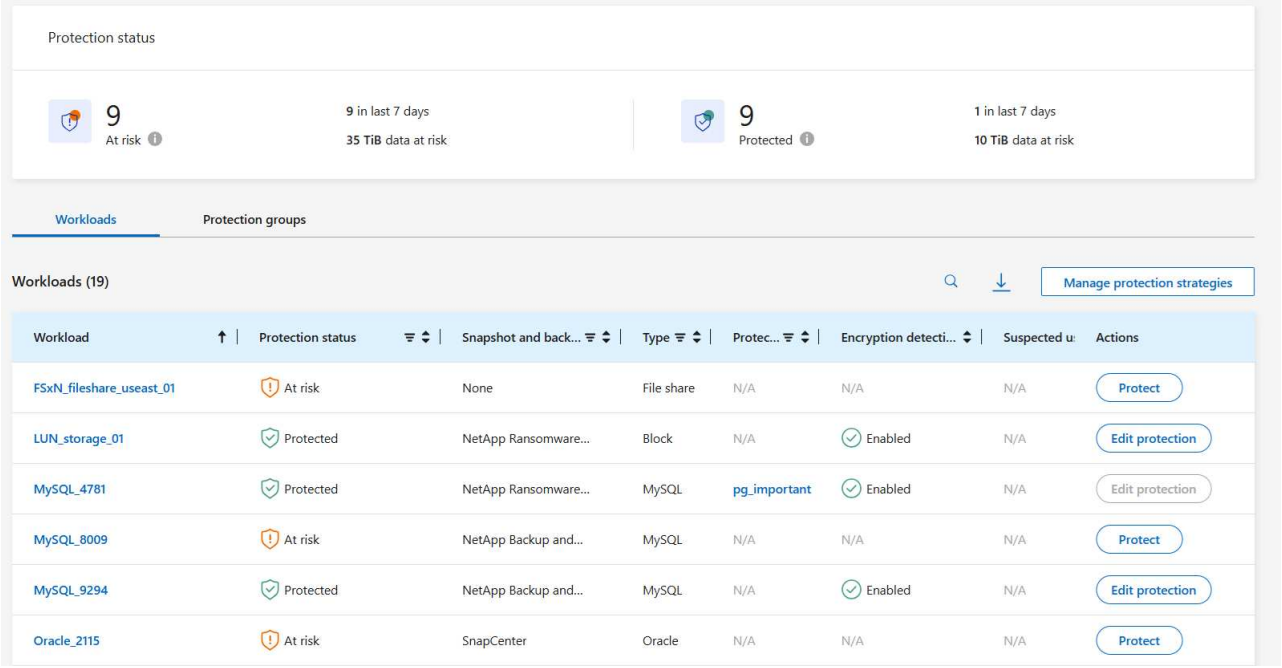
Uno de los primeros pasos para proteger las cargas de trabajo es ver las cargas de trabajo actuales y su estado de protección. Puedes ver los siguientes tipos de cargas de trabajo:

- Cargas de trabajo de aplicaciones

- Bloquear cargas de trabajo
- Cargas de trabajo de uso compartido de archivos
- Cargas de trabajo de máquinas virtuales

Pasos

1. Desde la navegación izquierda de la consola, seleccione **Protección** > **Resiliencia ante ransomware**.
2. Debe realizar una de las siguientes acciones:
   - Desde el panel Data Protection en el dashboard, selecciona **View all**.
   - Desde el menú, seleccione **Protección**.



3. Desde esta página, puede ver y cambiar los detalles de protección para la carga de trabajo.

Consulta "Agregar una estrategia de protección contra ransomware" para aprender sobre el uso de Ransomware Resilience cuando ya hay una política de protección con Backup and Recovery.

Entiende el panel de control de protección

El panel de protección en Ransomware Resilience muestra información detallada sobre las cargas de trabajo (por ejemplo, nombre y tipo de carga de trabajo, agente de Console, sistema y máquina virtual de almacenamiento), además de información sobre el estado de la protección. Usa el panel de protección para revisar y gestionar la preparación frente al ransomware de las cargas de trabajo. Las siguientes columnas son especialmente útiles para entender tu postura de protección:

Estado de protección: Una carga de trabajo puede mostrar uno de los siguientes estados de protección para indicar si una política se aplica o no:

- **Protegido**: Se aplica una política. ARP (o ARP/AI según la versión de ONTAP) está habilitado en todos los volúmenes relacionados con la carga de trabajo.
- **En riesgo**: No se aplica ninguna política. Si una carga de trabajo no tiene habilitada una política de detección primaria, está "en riesgo" incluso si tiene habilitadas una política de instantáneas y de respaldo.

- **En progreso**: Se está aplicando una política pero aún no está completa.
- **Error**: Se aplica una política pero no funciona.

Estado de detección:

+ Ransomware Resilience proporciona información sobre el alcance de las políticas de detección de ransomware que has configurado en tus cargas de trabajo. Revisa el alcance de la detección con los siguientes campos.

- **Estado de detección de cifrado**
- **Estado de detección de comportamiento sospechoso de usuario**
- **Bloquea extensiones de archivo sospechosas**

Snapshot, replicación y backup policies: Esta columna muestra el producto o servicio que está gestionando la política. Si no hay política, el campo muestra N/A.

Importancia

Ransomware Resilience asigna una importancia o prioridad a cada carga de trabajo durante el descubrimiento basándose en un análisis de cada carga de trabajo. La importancia de la carga de trabajo está determinada por las siguientes frecuencias de instantáneas:

- **Crítico**: Se toma más de una copia de instantánea por hora (programa de protección altamente agresivo)
- **Importante**: Las copias instantáneas se crean con una frecuencia menor a cada hora, pero mayor a la de cada día.
- **Estándar**: Se toman copias instantáneas más de una vez al día

Exposición de privacidad: selecciona esta opción para "escanea información de identificación personal con NetApp Data Classification".

Destino de replicación: si has configurado la replicación de instantáneas, se muestran los nombres de las máquinas virtuales de almacenamiento y sistemas de destino. Si no hay replicación, este campo muestra "N/A".

Destino de la copia de seguridad: si has configurado una estrategia de protección contra ransomware con copias de seguridad, el nombre del sistema de destino de la copia de seguridad aparece aquí.

Próximos pasos

- "Proteja las cargas de trabajo con estrategias de protección contra ransomware"
- "Gestiona grupos de protección"
- "Escanear en busca de datos de identificación personal"

Agrega un destino de backup en NetApp Ransomware Resilience

Cuando NetApp Ransomware Resilience descubre cargas de trabajo, si las copias de seguridad están configuradas, Ransomware Resilience reconoce los destinos de copia de seguridad. Si planeas usar copias de seguridad como parte de tu "estrategia de protección contra el ransomware" pero no has configurado destinos de copia de seguridad en la carga de trabajo, debes añadir un destino de copia de seguridad en

Puedes elegir uno de los siguientes destinos de backup:

- StorageGRID en NetApp
- Servicios web de Amazon (AWS)
- Plataforma de Google Cloud
- Microsoft Azure

Los destinos de backup no están disponibles para cargas de trabajo en Amazon FSx for NetApp ONTAP y Azure NetApp Files. Realiza operaciones de backup usando soluciones de backup nativas: FSx for ONTAP backup service o Azure NetApp Files backups.

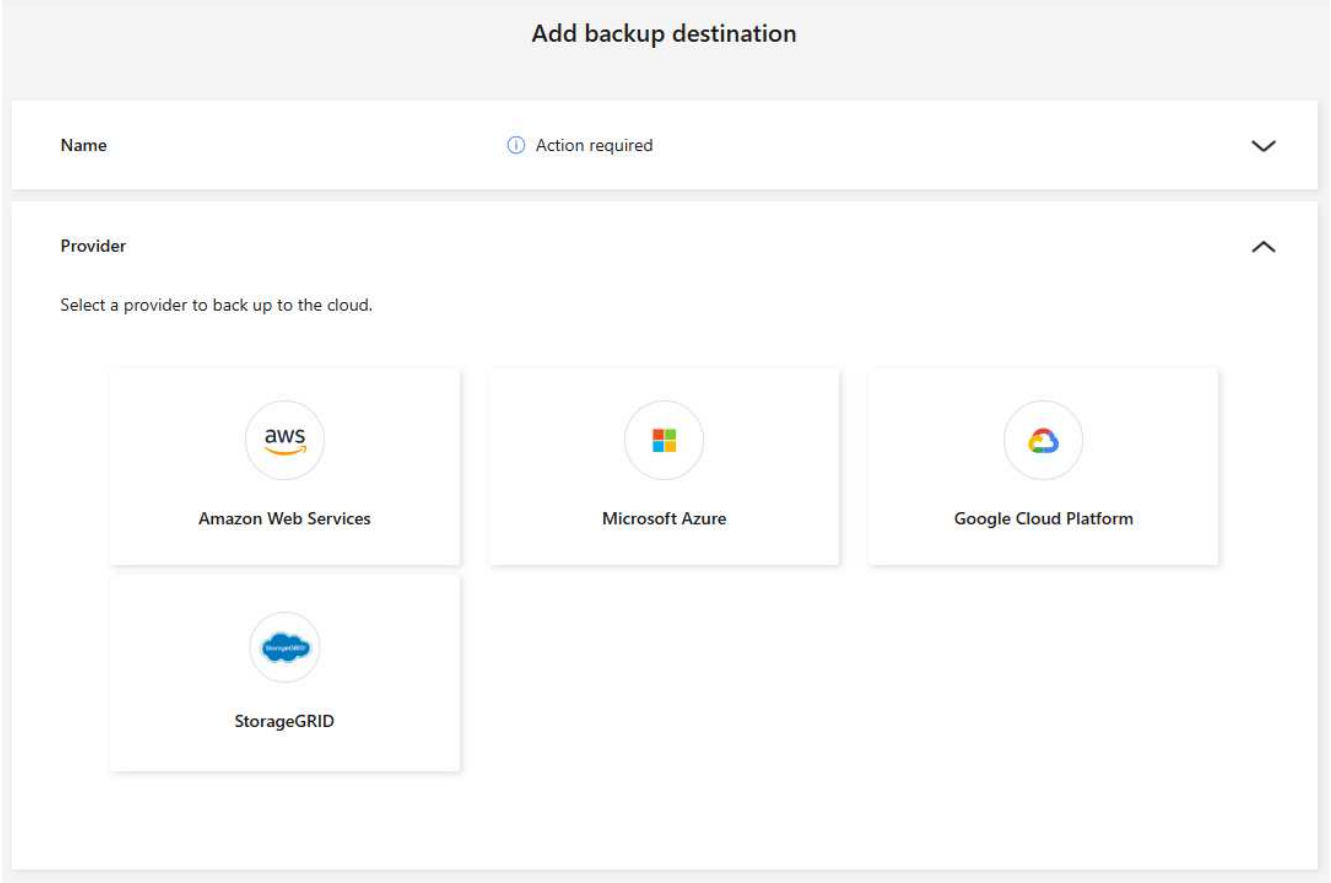
Rol de consola requerido Para realizar esta tarea, necesita el rol de administrador de organización, administrador de carpeta o proyecto, o administrador de resiliencia ante ransomware. "Obtenga información sobre las funciones de resiliencia ante ransomware para la NetApp Console" .

Agregue StorageGRID como destino de respaldo

Para configurar NetApp StorageGRID como destino de respaldo, ingrese la siguiente información.

Pasos

1. En Ransomware Resilience, seleccione **Configuración**.
2. En el mosaico **Destinos de backup**, selecciona **Ver**.
3. Seleccione **Agregar**.
4. Introduzca un nombre para el destino de la copia de seguridad.

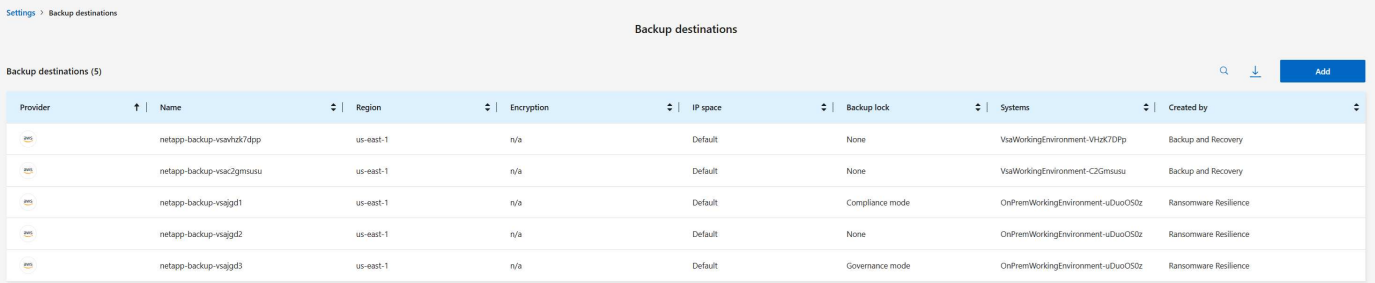


5. Seleccione * StorageGRID*.
6. Selecciona la flecha hacia abajo junto a cada ajuste para revisar los campos obligatorios:
   - **Configuración del proveedor**:
     - Elige **Crear un nuevo bucket** o **Traer tu propio bucket**.
     - Indica el **dominio completo (FQDN)** y el **puerto** del nodo Gateway.
     - Proporciona las credenciales de StorageGRID: **Clave de acceso** y **Clave secreta**.
   - **Redes**: Elija el espacio IP.
     - El espacio IP es el clúster donde residen los volúmenes que desea respaldar. Los LIF entre clústeres para este espacio IP deben tener acceso a Internet saliente.
   - **Backup Lock**

     Elige si quieres configurar el bloqueo de backup. Con el bloqueo de backup, las copias están protegidas para que no se modifiquen ni eliminen y se analizan en busca de amenazas de ransomware. No puedes modificar esta configuración después de configurar el destino del backup. **Si no quieres el bloqueo de backup, selecciona** None**.** Selecciona **Governance mode** para permitir que los usuarios con permisos específicos sobrescriban o eliminen archivos de backup protegidos durante el periodo de retención. **Selecciona** Compliance mode** para evitar que los usuarios sobrescriban o eliminen archivos de backup protegidos durante el periodo de retención.
7. Seleccione **Agregar**.

Resultado

El nuevo destino de copia de seguridad se agrega a la lista de destinos de copia de seguridad.



Agregue Amazon Web Services como destino de respaldo

Para configurar AWS como destino de respaldo, ingrese la siguiente información.

Para obtener más información sobre cómo administrar tu almacenamiento de AWS en la consola, consulta "Administra tus buckets de Amazon S3".

Pasos

1. En Ransomware Resilience, seleccione **Configuración**.
2. En el mosaico **Destinos de backup**, selecciona **Ver**.
3. Seleccione **Agregar**.
4. Seleccione **Amazon Web Services**.
5. Seleccione la flecha hacia abajo junto a cada configuración e ingrese o seleccione valores:
   - **Configuración del proveedor**:
     - Cree un nuevo depósito, seleccione un depósito existente si ya existe uno en la consola o traiga su propio depósito que almacenará las copias de seguridad.
     - Cuenta de AWS, región, clave de acceso y clave secreta para las credenciales de AWS

       "Si desea traer su propio depósito, consulte Agregar depósitos S3" .
   - **Cifrado**: si está creando un nuevo depósito S3, ingrese la información de la clave de cifrado que le proporcionó el proveedor. Si eligió un depósito existente, la información de cifrado ya está disponible.

     Los datos en el bucket se cifran con claves administradas por AWS de forma predeterminada. Puede seguir utilizando claves administradas por AWS o puede administrar el cifrado de sus datos utilizando sus propias claves.
   - **Redes**: elija el espacio IP y si utilizará un punto final privado.
     - El espacio IP es el clúster donde residen los volúmenes que desea respaldar. Los LIF entre clústeres para este espacio IP deben tener acceso a Internet saliente.
     - Opcionalmente, elija si utilizará un punto final privado de AWS (PrivateLink) que configuró previamente.

       Si desea utilizar AWS PrivateLink, consulte "AWS PrivateLink para Amazon S3" .
   - **Bloqueo de copia de seguridad**: elija si desea que Ransomware Resilience proteja las copias de seguridad para que no se modifiquen ni eliminen. Esta opción utiliza la tecnología NetApp DataLock. Cada copia de seguridad se bloqueará durante el período de retención, o durante un mínimo de 30 días, más un período de reserva de hasta 14 días.

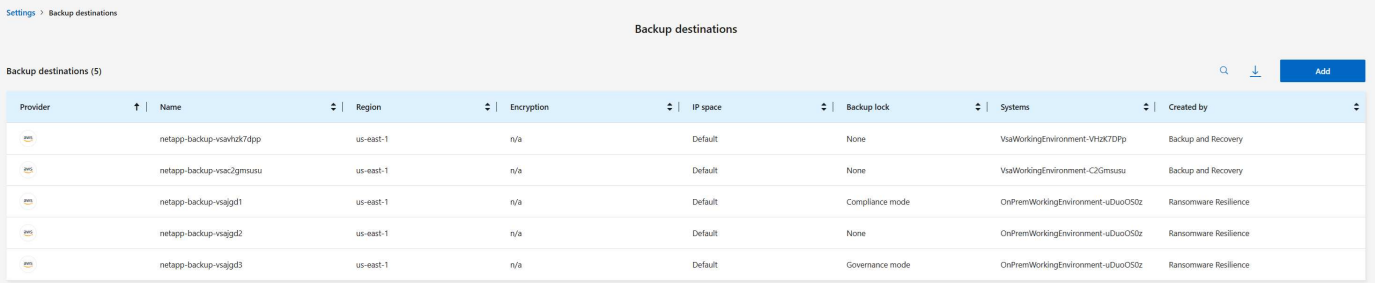
Si configuras ahora la opción de bloqueo de la copia de seguridad, no podrás cambiar la configuración después de que se haya configurado el destino de la copia de seguridad.

- **Modo de gobernanza**: usuarios específicos (con permiso s3:BypassGovernanceRetention) pueden sobrescribir o eliminar archivos protegidos durante el período de retención.
- **Modo de cumplimiento**: los usuarios no pueden sobrescribir ni eliminar archivos de respaldo protegidos durante el período de retención.

6. Seleccione **Agregar**.

Resultado

El nuevo destino de copia de seguridad se agrega a la lista de destinos de copia de seguridad.



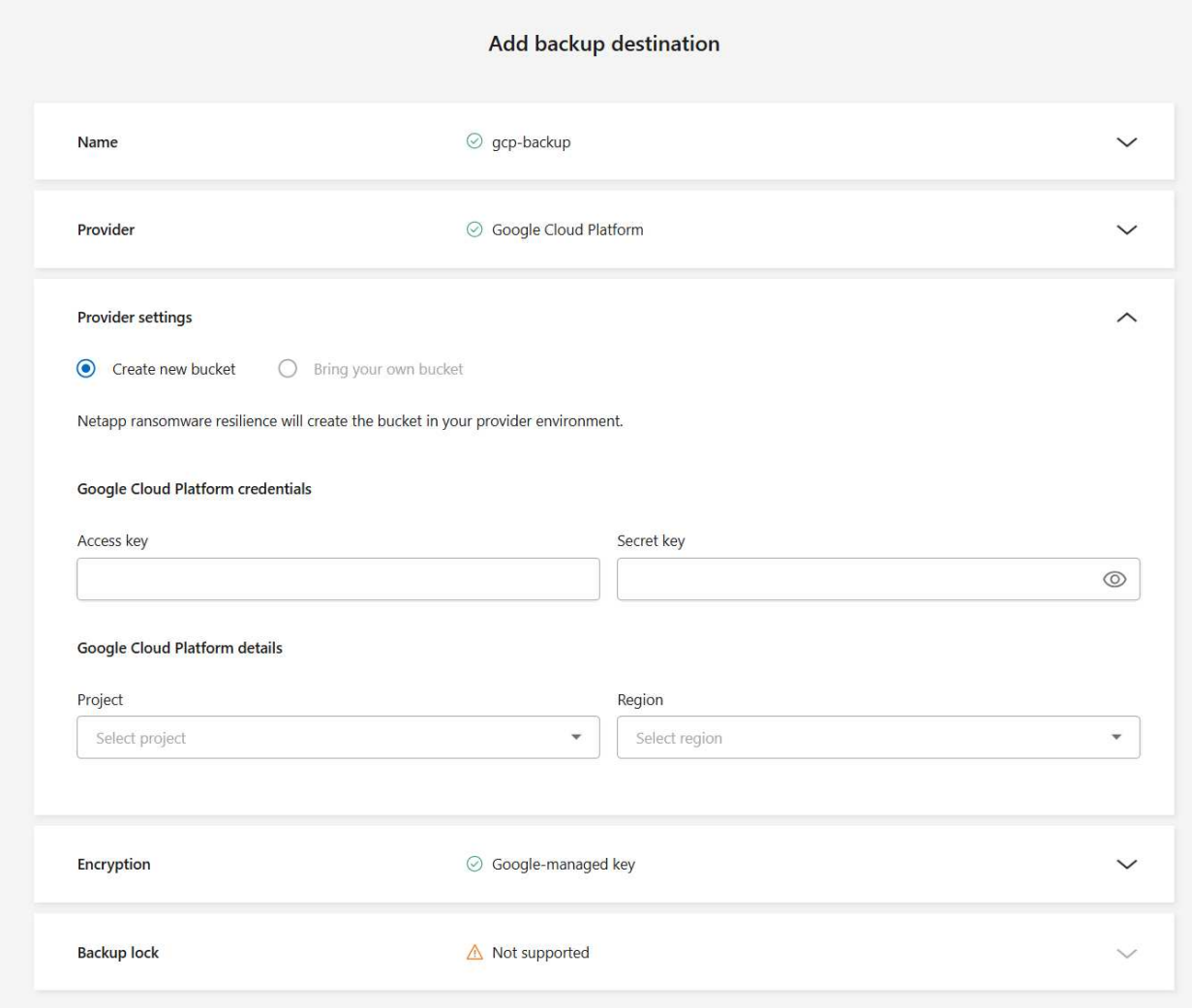
Agregar Google Cloud Platform como destino de respaldo

Para configurar Google Cloud Platform (GCP) como destino de respaldo, ingrese la siguiente información.

Para obtener más información sobre cómo gestionar tu almacenamiento de GCP en la consola, consulta "Opciones de instalación del agente de consola en Google Cloud".

Pasos

1. En Ransomware Resilience, seleccione **Configuración**.
2. En el mosaico **Destinos de backup**, selecciona **Ver**.
3. Seleccione **Agregar**.
4. Introduzca un nombre para el destino de la copia de seguridad.
5. Seleccione **Google Cloud Platform**.
6. Seleccione la flecha hacia abajo junto a cada configuración e ingrese o seleccione valores:
   - **Configuración del proveedor**:
     - Elige **Crear un nuevo bucket** o **Traer tu propio bucket**.
     - Proporciona las credenciales de Google Cloud Platform: **Access key** y **Secret key**.
     - Selecciona tu **Project** y la **Region** en la que existe.



- **Cifrado**: si está creando un nuevo depósito, ingrese la información de la clave de cifrado que le proporcionó el proveedor. Si eligió un depósito existente, la información de cifrado ya está disponible.

  Por defecto, los datos del bucket se cifran con claves gestionadas por Google. Puedes continuar con la configuración predeterminada seleccionando **Google-managed keys** o usar **Customer-managed keys**.

7. Seleccione **Agregar**.

Resultado

El nuevo destino de copia de seguridad se agrega a la lista de destinos de copia de seguridad.

Agregar Microsoft Azure como destino de respaldo

Para configurar Azure como destino de copia de seguridad, ingrese la siguiente información.

Para obtener detalles sobre cómo administrar sus credenciales de Azure y suscripciones de Marketplace en la consola, consulte "Administrar sus credenciales de Azure y suscripciones al Marketplace" .

Pasos

1. En Ransomware Resilience, seleccione **Configuración**.
2. En el mosaico **Destinos de backup**, selecciona **Ver**.

3. Seleccione **Agregar**.
4. Seleccione **Azure**.
5. Seleccione la flecha hacia abajo junto a cada configuración e ingrese o seleccione valores:
   - **Configuración del proveedor**:
     - Cree una nueva cuenta de almacenamiento, seleccione una existente si ya existe una en la Consola o traiga su propia cuenta de almacenamiento que almacenará las copias de seguridad.
     - Proporciona el Application (client) ID, el Client secret y el Directory (tenant) ID. Selecciona **Authenticate**.
     - Selecciona la suscripción de Azure, la región y el grupo de recursos para tu suscripción de Azure.

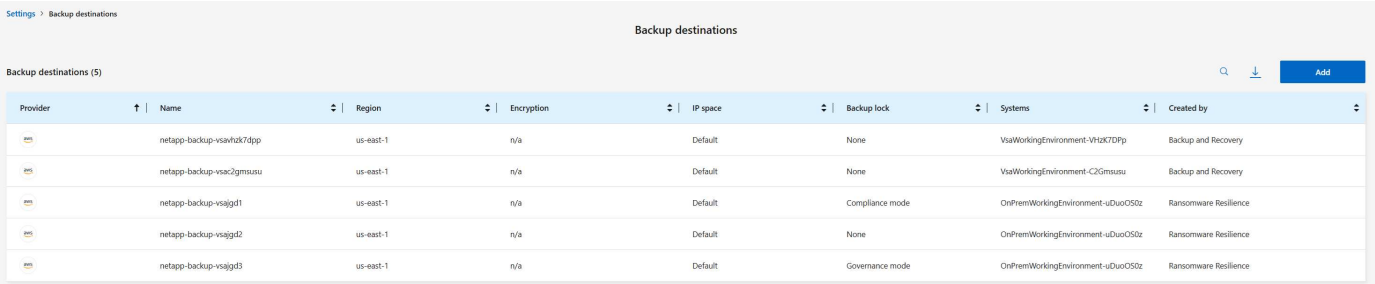
       "Si desea traer su propia cuenta de almacenamiento, consulte Agregar cuentas de almacenamiento de blobs de Azure" .
   - **Cifrado**: por defecto, los datos se cifran con una clave gestionada por Microsoft. Selecciona **Microsoft-managed key** para mantener esta opción; o elige **Customer managed key** para usar tus propias claves para el cifrado.
   - **Redes**: elija el espacio IP y si utilizará un punto final privado.
     - El espacio IP es el clúster donde residen los volúmenes que desea respaldar. Los LIF entre clústeres para este espacio IP deben tener acceso a Internet saliente.
     - Opcionalmente, elija si utilizará un punto de conexión privado de Azure que configuró previamente.

       Si desea utilizar Azure PrivateLink, consulte "Enlace privado de Azure" .
   - **Backup Lock**

     Elige si quieres configurar el bloqueo de backup. Con el bloqueo de backup, las copias están protegidas para que no se modifiquen ni eliminen y se analizan en busca de amenazas de ransomware. No puedes modificar esta configuración después de configurar el destino del backup. **Si no quieres el bloqueo de backup, selecciona** None**.** Selecciona **Governance mode** para permitir que los usuarios con permisos específicos sobrescriban o eliminen archivos de backup protegidos durante el periodo de retención. **Selecciona** Compliance mode** para evitar que los usuarios sobrescriban o eliminen archivos de backup protegidos durante el periodo de retención.
6. Seleccione **Agregar**.

Resultado

El nuevo destino de copia de seguridad se agrega a la lista de destinos de copia de seguridad.



Proteja las cargas de trabajo con las estrategias de protección NetApp Ransomware Resilience

Las estrategias de protección contra el ransomware son una característica clave de NetApp Ransomware Resilience: apoyan la detección, protección y replicación. Las estrategias de protección son una pieza esencial de tu postura de ciberseguridad.

Rol de consola requerido Para realizar esta tarea, necesita el rol de administrador de organización, administrador de carpeta o proyecto, o administrador de resiliencia ante ransomware. "Obtenga información sobre las funciones de resiliencia ante ransomware para la NetApp Console" .

Comprender las estrategias de protección contra ransomware

Las estrategias de protección contra ransomware abarcan *detección*, *protección* y *replicación*.

- **Políticas de detección** identifican amenazas de ransomware
- **Las políticas de protección** incluyen políticas de instantáneas y de copia de seguridad. Se requieren políticas de detección y captura de instantáneas en una estrategia de protección. Las políticas de respaldo son opcionales.

  Si utiliza otros productos de NetApp para proteger su carga de trabajo, Ransomware Resilience los detecta y ofrece la opción de:

  - utilizar una política de detección de ransomware y continuar utilizando las políticas de instantáneas y copias de seguridad creadas por otras herramientas de NetApp , o
  - Utilice Ransomware Resilience para gestionar la detección, las instantáneas y las copias de seguridad.
- **Las políticas de replicación** le permiten replicar instantáneas de Ransomware Resilience a un sitio secundario. Los programas de replicación se pueden configurar con frecuencias horarias, diarias, semanales o mensuales.

  Actualmente, solo puedes replicar instantáneas en el almacenamiento ONTAP local.

Si estás configurando estrategias de protección para Amazon FSxN para ONTAP y Azure NetApp Files, consulta "las limitaciones de cada servicio".

Para mejorar la gestión y la protección de tu parque de datos, puedes crear "cargas de trabajo de grupo" para proteger colectivamente los volúmenes bajo una misma estrategia.

Políticas de protección con otros servicios administrados por NetApp

Además de Ransomware Resilience, puedes usar NetApp Backup and Recovery para gestionar la protección de archivos compartidos y archivos compartidos de VM.

La información de protección de los servicios de Backup & Recovery aparece en Ransomware Resilience. Puedes añadir políticas de detección a estos servicios con Ransomware Resilience. Añadir una política de protección con Ransomware Resilience reemplaza las políticas de protección existentes.

Si una política de detección de ransomware está siendo administrada por Autonomous Ransomware Protection (ARP o ARP/AI, según la versión de ONTAP) y FPolicy en ONTAP, esas cargas de trabajo están protegidas y continuarán siendo administradas por ARP y FPolicy.

Los destinos de backup no están disponibles para cargas de trabajo en Amazon FSx for NetApp ONTAP o Azure NetApp Files. Realiza operaciones de backup usando el servicio de backup de FSx for ONTAP. Configuras las políticas de backup para cargas de trabajo en FSx for ONTAP en AWS, no en Ransomware Resilience. Las políticas de backup aparecen en Ransomware Resilience y permanecen sin cambios desde AWS.

Políticas de protección para cargas de trabajo no protegidas por aplicaciones de NetApp

Si tu carga de trabajo no está gestionada por Backup and Recovery o Ransomware Resilience, es posible que tenga instantáneas tomadas como parte de ONTAP u otros productos. Si la protección de ONTAP FPolicy está implementada, puedes cambiar la protección de FPolicy usando ONTAP.

Políticas de detección predefinidas

Puede elegir una de las siguientes políticas predefinidas de resiliencia ante ransomware, que están alineadas con la importancia de la carga de trabajo.

La política **Extensión de usuario de cifrado** es la única política predefinida que admite la detección de comportamiento sospechoso de usuarios.

+ La **política de replicación crítica** es la única política predefinida que admite la replicación de instantáneas en ONTAP.

Nivel de política	Snapshot	Frecuencia	Retención (días)	Número de copias de instantáneas	Número máximo de copias de instantáneas
Política de carga de trabajo crítica	Cada cuarto de hora	Cada 15 minutos	3	288	309
	Diario	Cada 1 día	14	14	309
	Semanalmente	Cada 1 semana	35	5	309
	Mensual	Cada 30 días	60	2	309
Política de carga de trabajo importante	Cada cuarto de hora	Cada 30 minutos	3	144	165
	Diario	Cada 1 día	14	14	165
	Semanalmente	Cada 1 semana	35	5	165
	Mensual	Cada 30 días	60	2	165

Nivel de política	Snapshot	Frecuencia	Retención (días)	Número de copias de instantáneas	Número máximo de copias de instantáneas
Política de carga de trabajo estándar	Cada cuarto de hora	Cada 30 min	3	72	93
	Diario	Cada 1 día	14	14	93
	Semanalmente	Cada 1 semana	35	5	93
	Mensual	Cada 30 días	60	2	93
Extensión de usuario de cifrado	Cada cuarto de hora	Cada 30 min	3	72	93
	Diario	Cada 1 día	14	14	93
	Semanalmente	Cada 1 semana	35	5	93
	Mensual	Cada 30 días	60	2	93
Política de replicación crítica	Cada cuarto de hora	Cada 15 minutos	3	288	309
	Diario	Cada 1 día	14	14	309
	Semanalmente	Cada 1 semana	35	5	309
	Mensual	Cada 30 días	60	2	309

Agregar una estrategia de protección contra ransomware

Hay tres enfoques para agregar una estrategia de protección contra ransomware:

- **Cree una estrategia de protección contra ransomware si no tiene políticas de instantáneas o copias de seguridad.**

  La estrategia de protección contra ransomware incluye:

  - Política de instantáneas
  - Política de detección de ransomware
  - Política de respaldo
- **Sustituye las políticas de instantáneas o copias de seguridad existentes de Backup and Recovery protection por estrategias de protección gestionadas por Ransomware Resilience.**

  La estrategia de protección contra ransomware incluye:

- Política de instantáneas
- Política de detección de ransomware
- Política de respaldo

- **Cree una política de detección para cargas de trabajo con políticas de backup e instantáneas existentes administradas en otros productos o servicios de NetApp .**

  La política de detección no cambia las políticas administradas en otros productos.

  La política de detección habilita la protección autónoma contra ransomware y la protección FPolicy si ya están activadas en otros servicios. Obtenga más información sobre"Protección autónoma contra ransomware" ,"Copia de seguridad y recuperación" , y"Política de ONTAP" .

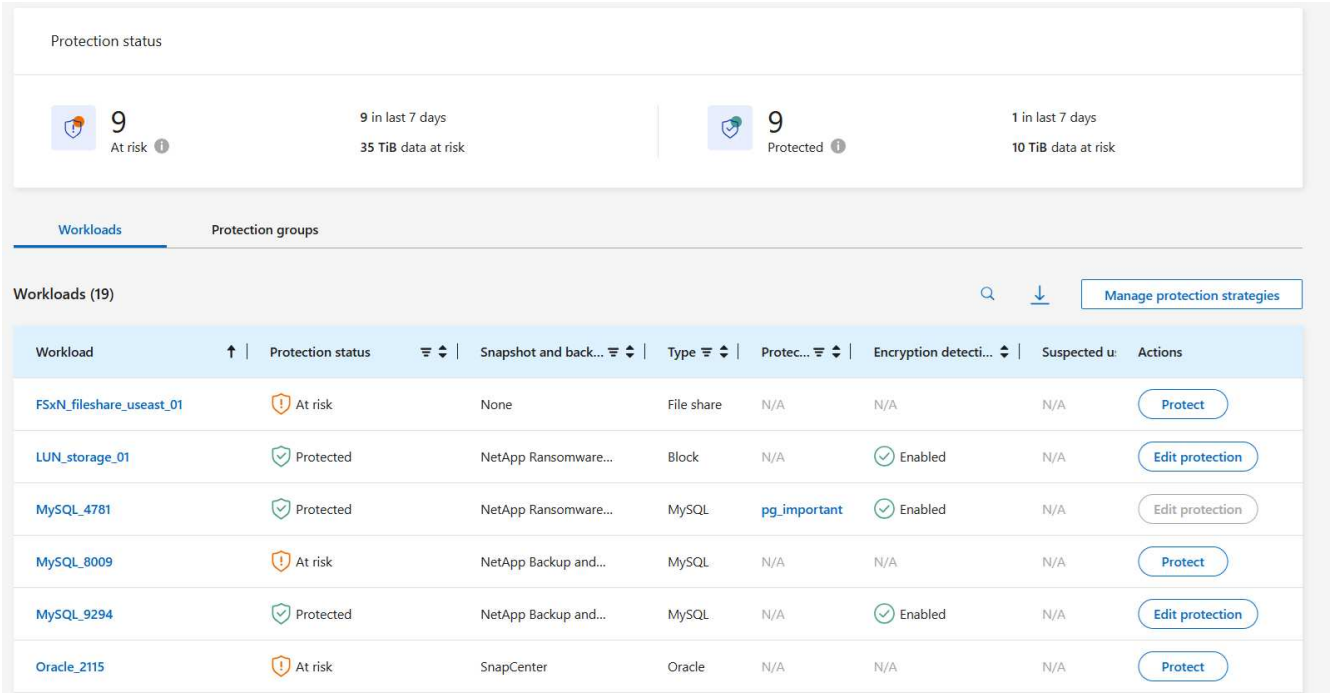
Cree una estrategia de protección contra ransomware (si no tiene políticas de instantáneas o copias de seguridad)

Si no existen políticas de instantáneas o de respaldo en la carga de trabajo, puede crear una estrategia de protección contra ransomware, que puede incluir las siguientes políticas que cree en Ransomware Resilience:

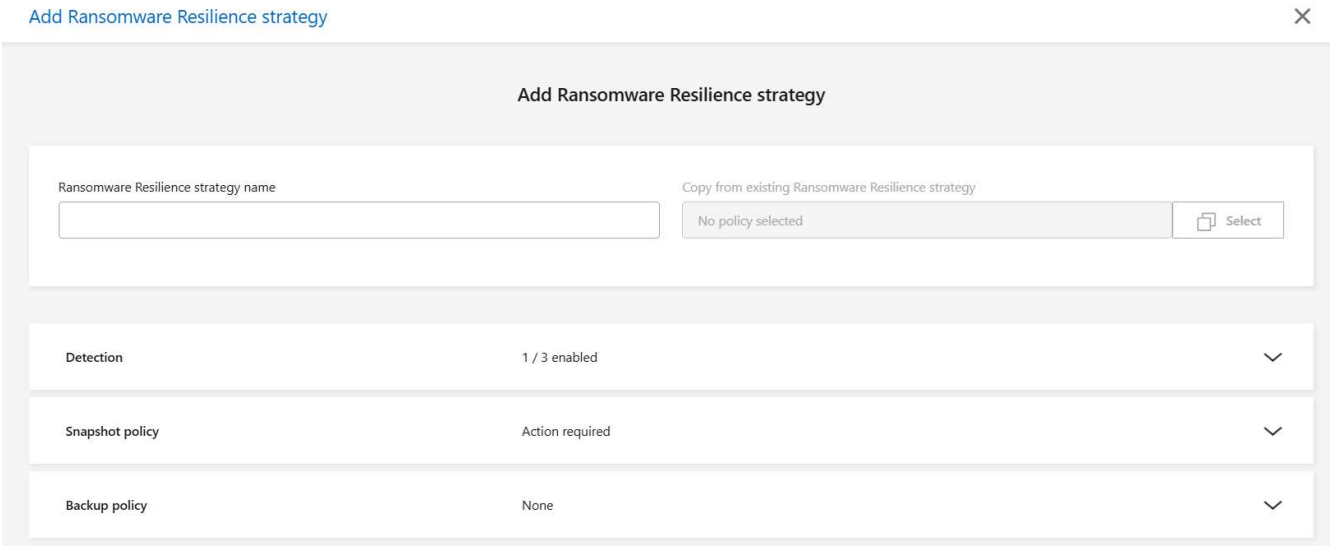
- Política de instantáneas
- Política de respaldo
- Política de detección de ransomware
- Replicación secundaria a ONTAP

Pasos para crear una estrategia de protección contra ransomware

1. En el menú Resiliencia ante ransomware, seleccione **Protección**.



2. Desde la página Protección, seleccione una carga de trabajo y luego **Proteger**.
3. Desde la página de estrategias de protección contra ransomware, seleccione **Agregar**.



4. Ingrese un nuevo nombre de estrategia o ingrese un nombre existente para copiarlo. Si ingresa un nombre existente, elija cuál desea copiar y seleccione **Copiar**.

> Si elige copiar y modificar una estrategia existente, Ransomware Resilience agrega "_copy" al nombre original. Debes cambiar el nombre y al menos una configuración para que sea único.

5. Para cada elemento, seleccione la **flecha hacia abajo**.

   - **Política de detección**:
     - **Política**: Elija una de las políticas de detección prediseñadas.
     - **Detección primaria**: habilite Ransomware Resilience para detectar posibles ataques de ransomware.
     - **Detección de comportamiento sospechoso del usuario**: habilite la detección del comportamiento del usuario para transmitir eventos de actividad del usuario a Ransomware Resilience y detectar eventos sospechosos, como violaciones de datos.
     - **Bloquear extensiones de archivos**: habilite Ransomware Resilience para bloquear extensiones de archivos sospechosas conocidas. Ransomware Resilience toma copias instantáneas automáticas cuando la detección primaria está habilitada.

       Si desea cambiar las extensiones de archivos bloqueadas, edítelas en el Administrador del sistema.

   - **Política de instantáneas**:
     - **Nombre base de la política de instantánea**: seleccione una política o seleccione **Crear** e ingrese un nombre para la política de instantánea.
     - **Bloqueo de instantáneas**: habilite esta opción para bloquear las copias de instantáneas en el almacenamiento principal de modo que no se puedan modificar ni eliminar durante un período de tiempo determinado, incluso si un ataque de ransomware logra llegar al destino de almacenamiento de respaldo. Esto también se llama *almacenamiento inmutable*. Esto permite un tiempo de restauración más rápido.

       Cuando se bloquea una instantánea, el tiempo de expiración del volumen se establece en el tiempo de expiración de la copia de la instantánea.

El bloqueo de copias instantáneas está disponible con ONTAP 9.12.1 y versiones posteriores. Para obtener más información sobre SnapLock, consulte "SnapLock en ONTAP" .

- **Programaciones de instantáneas**: elija las opciones de programación, la cantidad de copias de instantáneas que desea conservar y seleccione para habilitar la programación.
  - **Política de replicación**:
- **Nombre base de la política de replicación**: ingrese un nombre nuevo o elija uno existente. El nombre base es el prefijo que se añade a todas las instantáneas.
- **Programaciones de replicación**: alterne las frecuencias que desea habilitar (por hora, por día, por semana o por mes) y configure el valor de retención (la cantidad de instantáneas replicadas que se conservarán) para cada programación que habilite.
  - **Política de respaldo**:
- **Nombre base de la política de respaldo**: ingrese un nombre nuevo o elija uno existente.
- **Programaciones de respaldo**: elija las opciones de programación para el almacenamiento secundario y habilite la programación.

> Para activar el bloqueo de backup en el almacenamiento secundario, configura tus destinos de backup usando la opción **Settings**. Para más detalles, consulta "Configurar ajustes".

6. Seleccione **Agregar**.

Agrega una política de detección a las cargas de trabajo que ya tienen políticas de snapshot y backup gestionadas por Backup and Recovery

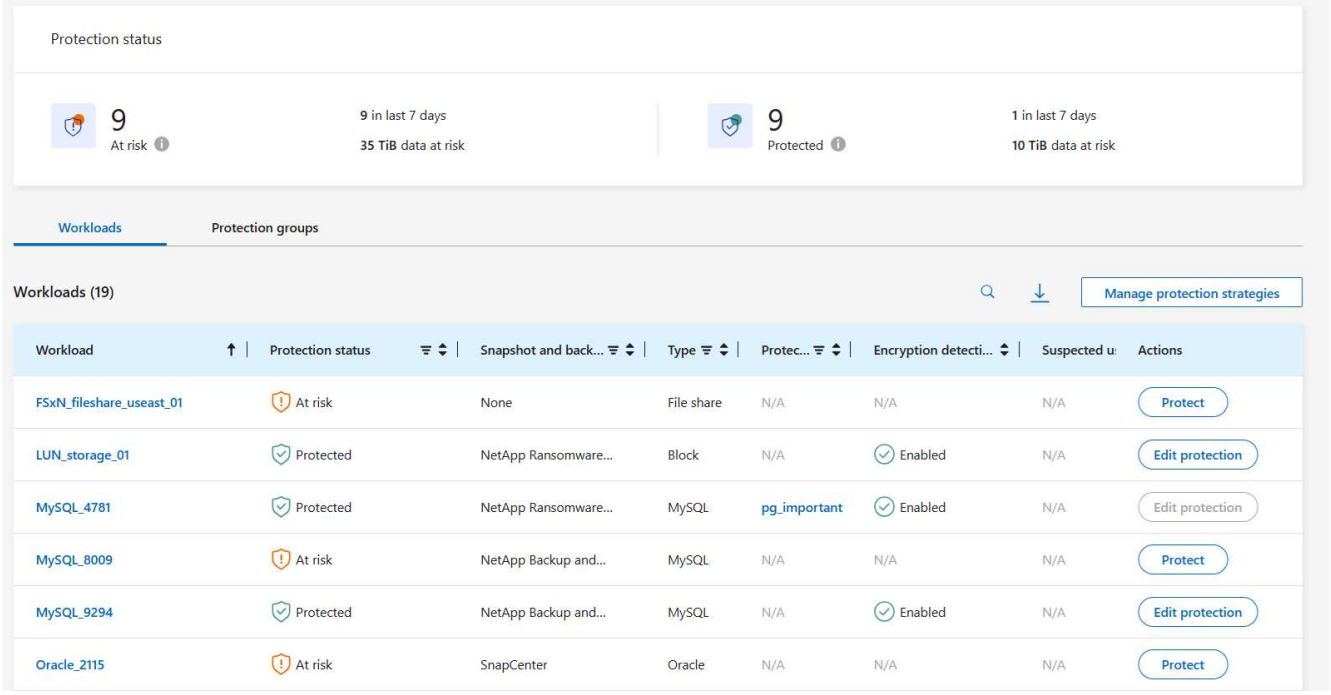
Ransomware Resilience te permite asignar una política de detección o una política de protección a cargas de trabajo con protección de instantáneas y copias de seguridad existente gestionada en otros productos o servicios de NetApp. Backup and Recovery usa políticas que rigen las instantáneas, la replicación a almacenamiento secundario o las copias de seguridad a almacenamiento de objetos.

Agregue una política de detección a las cargas de trabajo con políticas de copia de seguridad o instantáneas existentes

Si ya tienes políticas de instantáneas o copias de seguridad con Backup and Recovery, puedes añadir una política para detectar ataques de ransomware. Para gestionar la protección y la detección con Ransomware Resilience, consulta Protéjase con resiliencia contra ransomware.

Pasos

1. En el menú Resiliencia ante ransomware, seleccione **Protección**.



2. Desde la página Protección, seleccione una carga de trabajo y luego seleccione **Proteger**.
3. Ransomware Resilience detecta si hay políticas activas de Backup and Recovery.
4. Para dejar tu Backup and Recovery existente en su lugar y solo aplicar una política de *detección*, deja la casilla **Replace existing policies** sin marcar.
5. Selecciona la configuración de detección que quieras:
   - **Detección de cifrado**
   - **Detección de comportamiento sospechoso de usuario**
   - **Bloquea extensiones de archivo sospechosas**
6. Seleccione **Siguiente**.
7. Si seleccionaste **Detección de comportamiento sospechoso del usuario** como configuración de detección, selecciona el User activity agent o "o crea uno".

   El agente de actividad del usuario aloja los nuevos recopiladores de datos. Ransomware Resilience crea automáticamente el recopilador de datos para transmitir eventos de actividad del usuario a Ransomware Resilience para detectar un comportamiento anómalo del usuario.

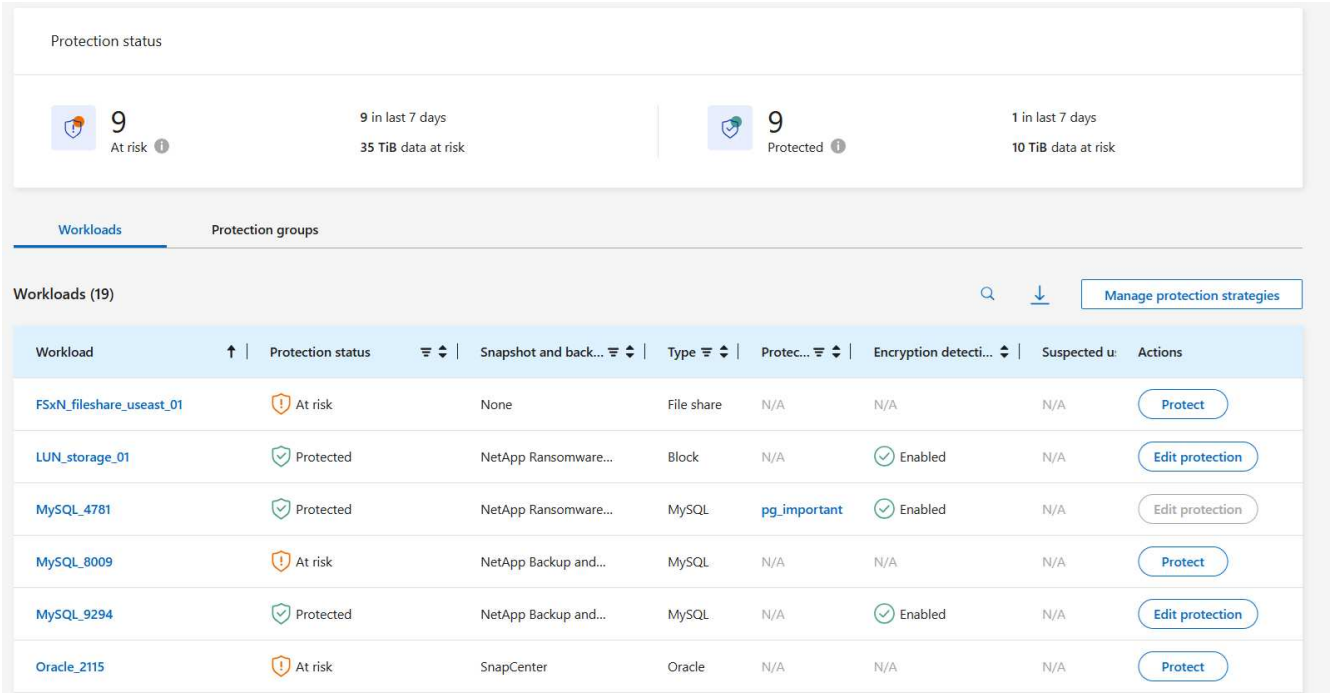
8. Seleccione **Siguiente**.
9. Revise sus opciones Seleccione **Crear** para activar la detección.
10. En la página Protección, revise el **Estado de detección** para confirmar que la detección esté Activa.

Reemplace las políticas de copia de seguridad o instantáneas existentes con una estrategia de protección contra ransomware

Puede reemplazar sus políticas de copia de seguridad o instantáneas existentes con una estrategia de protección contra ransomware. Este enfoque elimina la protección administrada externamente y configura la detección y protección en Ransomware Resilience.

Pasos

1. En el menú Resiliencia ante ransomware, seleccione **Protección**.



2. Desde la página Protección, seleccione una carga de trabajo y luego seleccione **Proteger**.
3. Ransomware Resilience detecta si existen políticas activas de Backup and Recovery. Para reemplazar las políticas existentes, selecciona la casilla **Replace existing policies**. Cuando seleccionas la casilla, Ransomware Resilience reemplaza la lista de políticas de detección por políticas de detección.
4. Elija una política de protección. Si no existe ninguna política de protección, seleccione **Agregar** para crear una nueva política. Para obtener información sobre cómo crear una política, consulteCrear una política de protección . Seleccione **Siguiente**.
5. Si su estrategia incluye replicación, seleccione el **Sistema de destino** y la **VM de almacenamiento de destino**. Seleccione **Siguiente**.
6. Seleccione un destino de copia de seguridad o cree uno nuevo. Seleccione **Siguiente**.
   a. Si su estrategia de protección incluye la detección del comportamiento del usuario, seleccione un agente de actividad del usuario en su entorno para alojar los nuevos recopiladores de datos. Ransomware Resilience crea automáticamente el recopilador de datos para transmitir eventos de actividad del usuario a Ransomware Resilience para detectar un comportamiento anómalo del usuario.
7. Revise la nueva estrategia de protección y luego seleccione **Proteger** para aplicarla.
8. En la página Protección, revise el **Estado de detección** para confirmar que la detección esté Activa.

Asignar una política diferente

Puede reemplazar la política existente por una diferente.

Pasos

1. En el menú Resiliencia ante ransomware, seleccione **Protección**.
2. Desde la página Protección, en la fila de carga de trabajo, seleccione **Editar protección**.
3. Si la carga de trabajo tiene una política de Backup and Recovery existente que quieres mantener, desmarca **Replace existing policies**. Para reemplazar las políticas existentes, marca **Replace existing policies**.

4. En la página Políticas, seleccione la flecha hacia abajo de la política que desea asignar para revisar los detalles.
5. Seleccione la política que desea asignar.
6. Seleccione **Proteger** para completar el cambio.

Gestionar estrategias de protección contra ransomware

Puedes eliminar una estrategia de ransomware.

Ver cargas de trabajo protegidas por una estrategia de protección contra ransomware

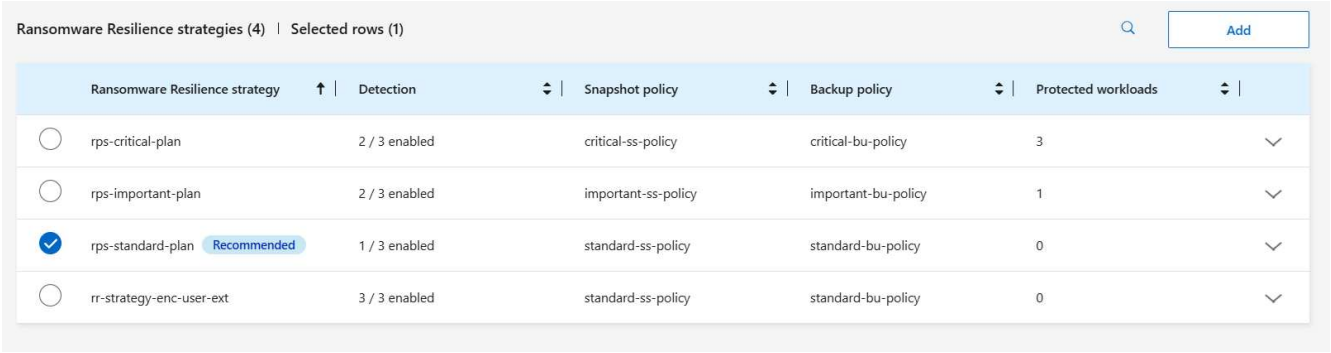
Antes de eliminar una estrategia de protección contra ransomware, es posible que desee ver qué cargas de trabajo están protegidas por esa estrategia.

Puede ver las cargas de trabajo desde la lista de estrategias o cuando está editando una estrategia específica.

Pasos para visualizar estrategias

1. En el menú Resiliencia ante ransomware, seleccione **Protección**.
2. Desde la página Protección, seleccione **Administrar estrategias de protección**.

   La página de estrategias de protección contra ransomware muestra una lista de estrategias.



3. En la página Estrategias de protección contra ransomware, en la columna Cargas de trabajo protegidas, seleccione la flecha hacia abajo al final de la fila.

Eliminar una estrategia de protección contra ransomware

Puede eliminar una estrategia de protección que actualmente no esté asociada con ninguna carga de trabajo.

Pasos

1. En el menú Resiliencia ante ransomware, seleccione **Protección**.
2. Desde la página Protección, seleccione **Administrar estrategias de protección**.
3. En la página Administrar estrategias, seleccione *Acciones* Opción para la estrategia que desea eliminar.
4. En el menú Acciones, seleccione **Eliminar política**.

Configura la detección de la actividad de los usuarios

Conoce la detección de la actividad de los usuarios en NetApp Ransomware Resilience

Con la detección de la actividad de los usuarios, NetApp Ransomware Resilience te permite abordar eventos de ransomware a nivel de usuario, deteniendo eventos como filtraciones de datos y eliminaciones a gran escala.

NetApp Ransomware Resilience ofrece una detección de violación de datos impulsada por IA al monitorear la actividad sospechosa de los usuarios. Los aumentos bruscos en la actividad de lectura y los patrones de acceso a la actividad de lectura se usan para determinar la intención maliciosa. Una vez detectado, Ransomware Resilience genera automáticamente alertas en la NetApp Console, por correo electrónico y en cualquier ecosistema de seguridad configurado (por ejemplo, SIEM).

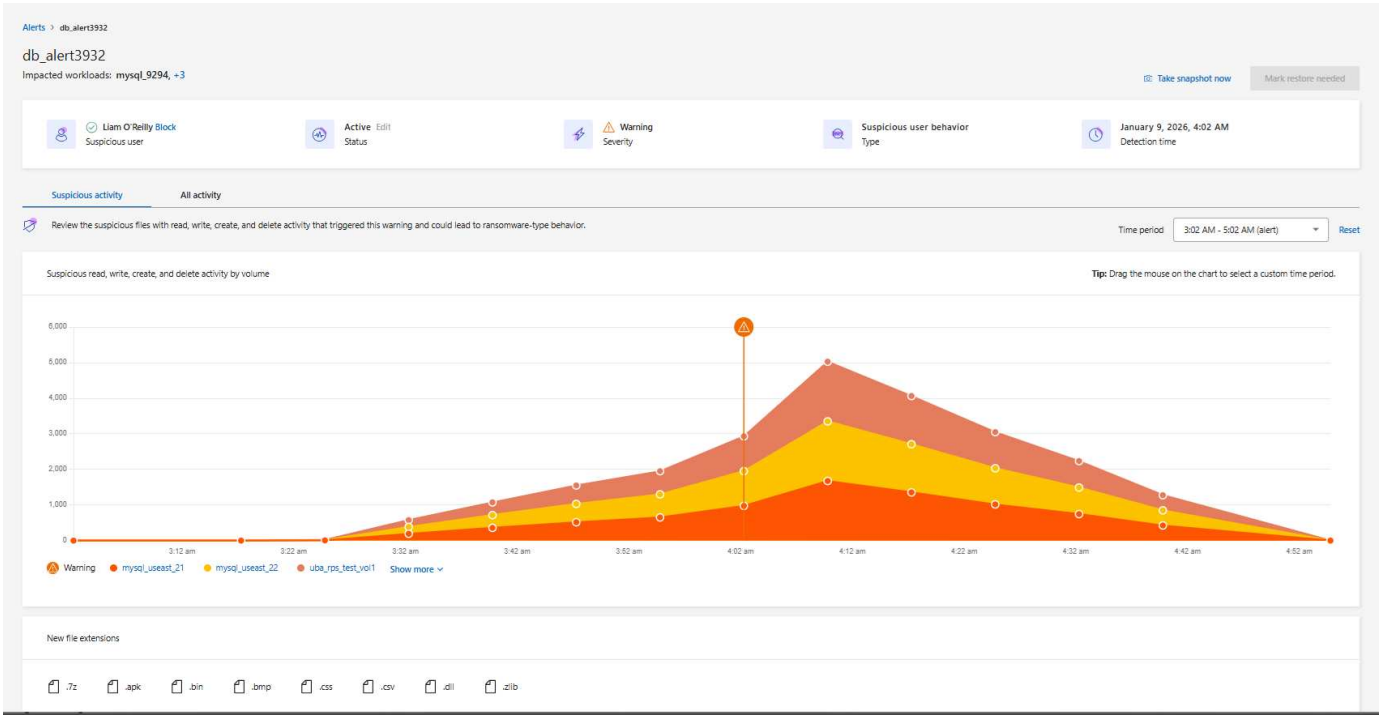
Con la detección y alerta de comportamientos sospechosos de los usuarios, Ransomware Resilience te avisa de los intentos de violación y destrucción de datos y de los patrones que parecen sospechosos. En cada alerta, Ransomware Resilience identifica a un usuario que puedes bloquear.

Ransomware Resilience detecta actividad sospechosa del usuario analizando los eventos de actividad del usuario generados por FPolicy en ONTAP. Para recopilar datos de actividad del usuario, debe implementar uno o más agentes de actividad del usuario. El agente es un servidor Linux o una máquina virtual con conectividad a los dispositivos de su inquilino.

La detección de actividad del usuario no está soportada actualmente para cargas de trabajo SAN. Puedes usar la detección de actividad del usuario con cargas de trabajo NAS en Amazon FSxN para ONTAP, Cloud Volumes ONTAP y ONTAP.

Análisis forense de actividad sospechosa de usuarios

Ransomware Resilience ofrece análisis forenses de los comportamientos de los usuarios: listas y gráficos que muestran cuándo ocurrió actividad sospechosa y cuándo se enviaron notificaciones. Estos detallan la frecuencia de la actividad sospechosa en archivos, directorios, volúmenes y cargas de trabajo a lo largo del tiempo para ayudar a trazar los eventos. También puedes observar la aparición de nuevas extensiones de archivo.



.

Puedes comparar la actividad sospechosa con una vista de toda la actividad. En la vista de toda la actividad, puedes observar eventos de lectura, escritura, cambio de nombre, movimiento, creación y eliminación, además de eventos de cambio de acceso y acceso denegado.

.

Componentes

Hay tres componentes clave en la detección de actividad de comportamiento sospechoso del usuario en Ransomware Resilience.

- El **agente de actividad del usuario** es un entorno ejecutable para los recopiladores de datos. Debes configurar el agente de actividad del usuario.
- El **recolector de datos** comparte los eventos de actividad del usuario con Ransomware Resilience. El recolector de datos se crea automáticamente cuando tú "activa una estrategia de protección contra ransomware con detección de actividad sospechosa de usuarios".
- El **conector de directorio de usuarios** permite el mapeo entre nombres de usuario e identificaciones de usuario, creando mayor claridad al responder a comportamientos sospechosos de los usuarios. Debes configurar el conector de directorio de usuarios.

Ransomware Resilience y Data Infrastructure Insights

La detección de comportamientos sospechosos de usuarios de Ransomware Resilience es una integración con Data Infrastructure Insights (DII) Workload Security y utiliza "Puntos finales DII". No necesitas ninguna configuración de DII para activar la detección de comportamientos de usuarios en Ransomware Resilience. Para activar la detección de comportamientos de usuarios, "crea el agente y los recopiladores necesarios y activa la estrategia de protección contra ransomware adecuada".

Si ya estás usando NetApp Data Infrastructure Insights (DII) Workload Security, se recomienda que uses los mismos agentes de Workload Security para Ransomware Resilience. No necesitas implementar agentes de Workload Security independientes para Ransomware Resilience, pero usar los mismos agentes de Workload Security requiere una relación de emparejamiento entre la organización de la consola de Ransomware Resilience y el tenant de DII Storage Workload Security. Contacta a tu representante de cuenta para habilitar este emparejamiento.

Próximos pasos

- "Requisitos para la detección de la actividad de comportamiento del usuario"
- "Configura los agentes y detectores de actividad del comportamiento del usuario"

Requisitos de detección de actividad de usuario para NetApp Ransomware Resilience

NetApp Ransomware Resilience user behavior detection te permite responder a eventos de ransomware a nivel de usuario. Debes crear un conjunto de agentes para habilitar la detección de comportamiento del usuario. Antes de habilitar la detección, debes asegurarte de cumplir con los requisitos de sistema operativo, servidor y red descritos para que Ransomware Resilience pueda detectar e informar eventos correctamente.

Soporte del proveedor de la nube

Los datos de actividad sospechosa del usuario pueden almacenarse en AWS y Azure en las siguientes regiones:

Proveedor de nube	Región
AWS	• Asia Pacífico (Sídney) (ap-southeast-2) • Europa (Frankfurt) (eu-central-1) • Este de EE. UU. (Norte de Virginia) (us-east-1)
Azur	Este de EE. UU.

Requisitos del sistema operativo

La detección de comportamiento sospechoso del usuario es compatible con los siguientes sistemas operativos:

Sistema operativo	Versiones compatibles
AlmaLinux	9.4 (64 bits) a 9.5 (64 bits) y 10 (64 bits), incluido SELinux
CentOS	CentOS Stream 9 (64 bits)
Debian	11 (64 bits), 12 (64 bits), incluido SELinux
OpenSUSE Leap	15.3 (64 bits) a 15.6 (64 bits)
Oracle Linux	8.10 (64 bits) y 9.1 (64 bits) a 9.6 (64 bits), incluido SELinux
Sombrero rojo	8.10 (64 bits), 9.1 (64 bits) a 9.6 (64 bits) y 10 (64 bits), incluido SELinux
Rocoso	Rocky 9.4 (64 bits) a 9.6 (64 bits), incluido SELinux
SUSE Enterprise Linux	15 SP4 (64 bits) a 15 SP6 (64 bits), incluido SELinux
Ubuntu	20.04 LTS (64 bits), 22.04 LTS (64 bits) y 24.04 LTS (64 bits)

La máquina que utilice para el agente de actividad del usuario no debe estar ejecutando otro software de nivel de aplicación. Se recomienda un servidor dedicado.

El `unzip` Se requiere comando para la instalación. El `sudo su -` El comando es necesario para la instalación, la ejecución de scripts y la desinstalación.

Requisitos del servidor

El servidor debe cumplir los siguientes requisitos mínimos:

- **CPU**: 4 núcleos
- **RAM**: 16 GB de RAM
- **Espacio en disco**: 36 GB de espacio libre en disco

Recomendaciones del servidor

- Asigne espacio de disco adicional para permitir la creación del sistema de archivos. Asegúrese de que haya al menos 35 GB de espacio libre en el sistema de archivos. + Si `/opt` es una carpeta montada desde un almacenamiento NAS, los usuarios locales deben tener acceso a esta carpeta. La creación del agente de actividad del usuario puede fallar si los usuarios locales no tienen los permisos necesarios.
- Se recomienda que instales el agente de actividad del usuario en un sistema independiente de tu entorno de Ransomware Resilience. Si los instalas en la misma máquina, deberías dejar entre 50 y 55 GB de espacio en disco. Para Linux, asigna entre 25 y 30 GB de espacio a `/opt/netapp` y 25 GB a `var/log/netapp`.
- Se recomienda sincronizar la hora tanto en el sistema ONTAP como en la máquina del agente de actividad del usuario mediante el Protocolo de tiempo de red (NTP) o el Protocolo simple de tiempo de red (SNTP).

Reglas de acceso a la red en la nube

Revise las reglas de acceso a la red en la nube para su geografía relevante (Asia Pacífico, Europa o Estados Unidos).

Durante la instalación inicial, reemplaza el `<site_name>` con un permiso comodín (`*`). Después de que el agente esté activado y completamente operativo, puedes reemplazar el permiso por el nombre del sitio. Contacta a tu representante de NetApp para el nombre del sitio.

El agente de actividad del usuario utiliza la tecnología NetApp Data Infrastructure Insights, por eso se usan los endpoints de `cloudinsights`. Para más información, consulta

Implementaciones de agentes de actividad de usuario basadas en APAC

Protocolo	Puerto	Fuente	Destino	Descripción
HTTPS (TCP)	443	Agente de actividad del usuario	• <site_name>.cs01-ap-1.cloudinsights.netapp.com • <site_name>.c01-ap-1.cloudinsights.netapp.com • <site_name>.c02-ap-1.cloudinsights.netapp.com • gentlogin.cs01-ap-1.cloudinsights.netapp.com	Acceso a la resiliencia frente al ransomware

Implementaciones de agentes de actividad de usuarios con sede en Europa

Protocolo	Puerto	Fuente	Destino	Descripción
HTTPS (TCP)	443	Agente de actividad del usuario	• <site_name>.cs01-eu-1.cloudinsights.netapp.com • <site_name>.c01-eu-1.cloudinsights.netapp.com • <site_name>.c02-eu-1.cloudinsights.netapp.com • agentlogin.cs01-eu-1.cloudinsights.netapp.com	Acceso a la resiliencia frente al ransomware

Despliegues de agentes de actividad de usuarios en EE. UU.

Protocolo	Puerto	Fuente	Destino	Descripción
HTTPS (TCP)	443	Agente de actividad del usuario	• <site_name>.cs01.cloudinsights.netapp.com • <site_name>.c01.cloudinsights.netapp.com • <site_name>.c02.cloudinsights.netapp.com • agentlogin.cs01.cloudinsights.netapp.com	Acceso a la resiliencia frente al ransomware

Reglas dentro de la red

Protocolo	Puerto	Fuente	Destino	Descripción
TCP	389(LDAP) 636 (LDAP/start-tls)	Agente de actividad del usuario	URL del servidor LDAP	Conectarse a LDAP

Protocolo	Puerto	Fuente	Destino	Descripción
HTTPS (TCP)	443	Agente de actividad del usuario	Dirección IP de administración del clúster o SVM (según la configuración del recopilador SVM)	Comunicación API con ONTAP
TCP	35000 - 55000	Direcciones IP de LIF de datos SVM	Agente de actividad del usuario	Comunicación de ONTAP al agente de actividad del usuario para eventos de Fpolicy. Estos puertos deben estar abiertos hacia el agente de actividad del usuario para que ONTAP pueda enviarle eventos, incluido cualquier firewall en el propio agente de actividad del usuario (si está presente). + **NOTA:** No es necesario reservar **todos** estos puertos, pero los puertos que reserve para esto deben estar dentro de este rango. Se recomienda comenzar reservando 100 puertos y aumentarlos si es necesario.

Protocolo	Puerto	Fuente	Destino	Descripción
TCP	35000-55000	IP de gestión de clúster	Agente de actividad del usuario	Comunicación desde la IP de administración del clúster ONTAP al agente de actividad del usuario para **eventos EMS**. Estos puertos deben estar abiertos hacia el agente de actividad del usuario para que ONTAP pueda enviarle eventos EMS, incluido cualquier firewall en el propio agente de actividad del usuario. + **NOTA:** No es necesario reservar **todos** estos puertos, pero los puertos que reserve para esto deben estar dentro de este rango. Se recomienda comenzar reservando 100 puertos y aumentarlos si es necesario.
SSH	22	Agente de actividad del usuario	Gestión de clústeres	Necesario para el bloqueo de usuarios CIFS/SMB.

Siguiente paso

- "Configura los agentes y colectores de actividad de los usuarios"

Configura agentes y recopiladores para la detección de actividad de usuarios en NetApp Ransomware Resilience

La detección de actividad del usuario de NetApp Ransomware Resilience te ayuda a prevenir eventos de ransomware a nivel de usuario. Para habilitar la detección de comportamiento sospechoso del usuario en Ransomware Resilience, debes instalar al menos un agente de actividad del usuario, que crea un entorno de recopilación de datos para monitorear el comportamiento del usuario en busca de patrones aberrantes que se parezcan a eventos de ransomware.

Un agente de actividad de usuario aloja un recopilador de datos y un conector de directorio de usuario, que

ambos envían datos a una ubicación SaaS para análisis.

- El **recolector de datos** recopila datos de actividad de usuario de ONTAP. El recolector de datos se crea automáticamente cuando creas una estrategia de protección con detección de comportamiento de usuario.
- El **conector de directorio de usuarios** se conecta a tu directorio para asignar ID de usuario a nombres de usuario. Debes configurar el conector de directorio de usuarios.

El agente de actividad del usuario, el recopilador de datos y el conector del directorio de usuarios se pueden gestionar desde el panel de configuración de Ransomware Resilience.

> Si ya estás usando NetApp Data Infrastructure Insights (DII) Workload Security, se recomienda que uses los mismos agentes de Workload Security para Ransomware Resilience. No necesitas implementar agentes de Workload Security independientes para Ransomware Resilience, pero usar los mismos agentes de Workload Security requiere una relación de emparejamiento entre la organización de la consola de Ransomware Resilience y el tenant de DII Storage Workload Security. Contacta a tu representante de cuenta para habilitar este emparejamiento.

+ Si *no* usas DII, sigue las instrucciones de configuración aquí.

Antes de empezar

- Asegúrate de cumplir los "requisitos del sistema operativo, servidor y red".

Rol requerido de la consola Para activar la detección de actividad sospechosa de usuarios, necesitas el rol **Organization admin role**. Para las configuraciones posteriores de actividad sospechosa de usuarios, necesitas el rol **Ransomware Resilience user behavior admin role**. "Obtenga información sobre las funciones de resiliencia ante ransomware para la NetApp Console".

Asegúrate de que cada función se aplique a nivel de la organización.

Crear un agente de actividad de usuario

Los agentes de actividad de usuario son entornos ejecutables para "recopiladores de datos"; los recopiladores de datos comparten eventos de actividad de usuario con Ransomware Resilience. Debes crear al menos un agente de actividad de usuario para habilitar la detección de actividad de usuario sospechosa.

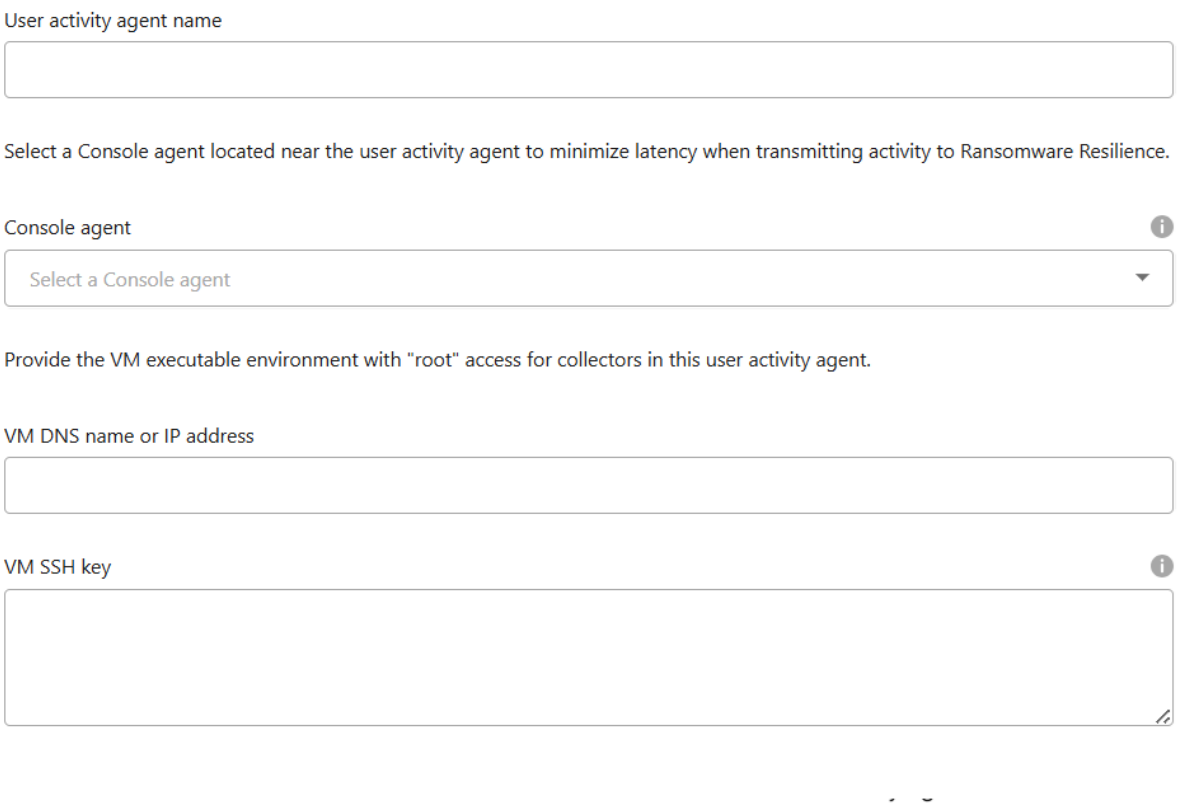
Pasos

1. Si es la primera vez que crea un agente de actividad de usuario, vaya al **Panel de control**. En el mosaico **Actividad del usuario**, seleccione **Activar**.

   Si está agregando un agente de actividad de usuario adicional, vaya a **Configuración**, ubique el mosaico **Actividad de usuario** y luego seleccione **Administrar**. En la pantalla Actividad del usuario, seleccione la pestaña **Agentes de actividad del usuario** y luego **Agregar**.

2. Seleccione un **Proveedor de nube** y luego una **Región**. Seleccione **Siguiente**.
3. Proporcione los detalles del agente de actividad del usuario:
   - **Nombre del agente de actividad del usuario**
   - **Agente de consola**: el agente de consola debe estar en la misma red que el agente de actividad del usuario y tener conectividad SSH a la dirección IP del agente de actividad del usuario.
   - **Nombre DNS o dirección IP de la máquina virtual**
   - **VM SSH Key** - Ingresa la clave SSH usando este formato:

```
-----BEGIN OPENSSH PRIVATE KEY-----
private-key-contents
-----END OPENSSH PRIVATE KEY-----
```



4. Seleccione **Siguiente**.
5. Revise su configuración. Seleccione **Activar** para completar la adición del agente de actividad del usuario.
6. Confirma que el agente de actividad de usuario se creó correctamente. En el mosaico de actividad de usuario, una implementación exitosa se muestra como **Running**.

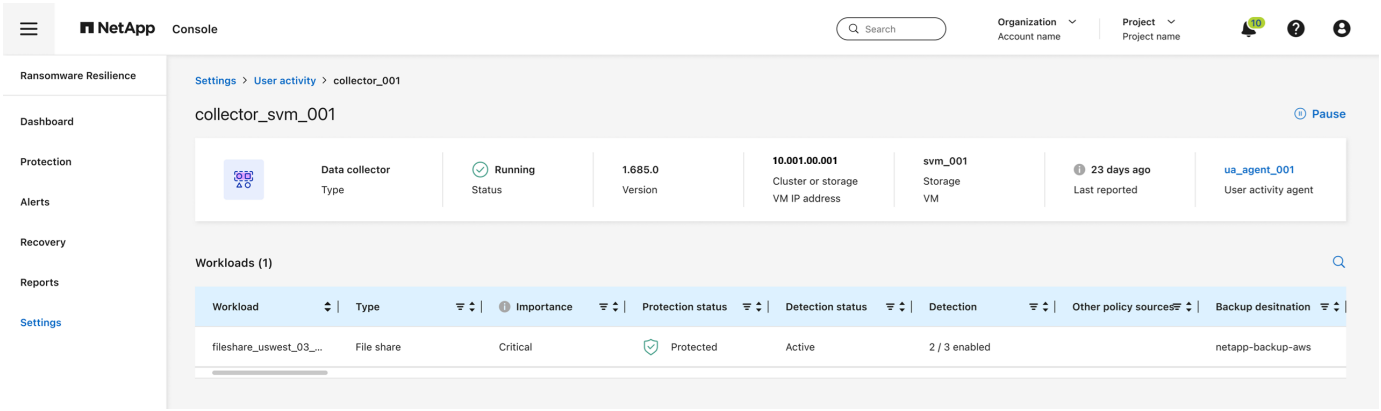
Resultado

Después de que el agente de actividad de usuario se cree correctamente, vuelve al menú **Settings** y luego selecciona **Manage** en el mosaico de User activity. Selecciona la pestaña **User activity agents** y luego selecciona el agente de actividad de usuario para ver detalles sobre él, incluidos los recopiladores de datos y los conectores del directorio de usuarios.

Agregar un recopilador de datos

Los recopiladores de datos se crean automáticamente cuando habilitas una estrategia de protección contra ransomware con detección de actividad sospechosa de usuarios. Para más información, consulta "añadir una política de detección".

Puede ver los detalles del recopilador de datos. Desde Configuración, seleccione **Administrar** en el mosaico Actividad del usuario. Seleccione la pestaña **Recopilador de datos** y luego seleccione el recopilador de datos para ver sus detalles o pausarlo.



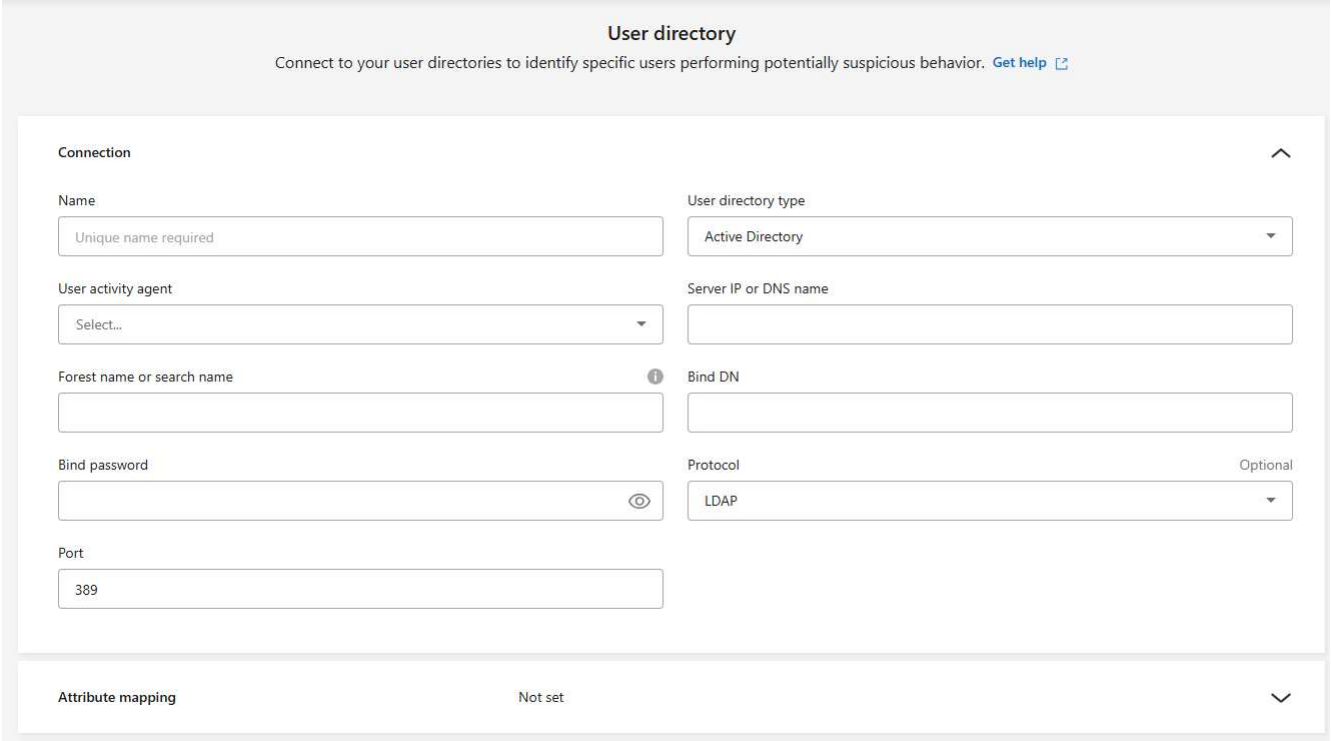
Crear un conector de directorio de usuarios

Para asignar ID de usuario a nombres de usuario, debe crear un conector de directorio de usuarios.

Pasos

1. En Ransomware Resilience, vaya a **Configuración**.
2. En el mosaico Actividad del usuario, seleccione **Administrar**.
3. Seleccione la pestaña **Conectores de directorio de usuario** y luego **Agregar**.
4. Configurar la conexión. Introduzca la información requerida para cada campo.

Campo	Descripción
Nombre	Introduzca un nombre único para el conector del directorio de usuarios
Tipo de directorio de usuario	El tipo de directorio
Dirección IP del servidor o nombre de dominio	La dirección IP o el nombre de dominio completo (FQDN) del servidor que aloja la conexión
Nombre del bosque o nombre de búsqueda	Puede especificar el nivel de bosque de la estructura del directorio como el nombre de dominio directo (por ejemplo `unit.company.com`) o un conjunto de nombres distinguidos relativos (por ejemplo: `DC=unit,DC=company,DC=com`). También puedes introducir un `OU` para filtrar por una unidad organizativa o una `CN` para limitar a un usuario específico (por ejemplo: `CN=user,OU=engineering,DC=unit,DC=company,DC=com`).
VINCULO DN	El DN BIND es una cuenta de usuario autorizada para buscar en el directorio, como por ejemplo usuario@dominio.com. El usuario requiere el permiso de Sólo lectura del dominio.
Contraseña BIND	La contraseña para el usuario proporcionada en BIND DN
Protocolo	El campo de protocolo es opcional. Puede utilizar LDAP, LDAPS o LDAP sobre StartTLS.
Puerto	Introduzca el número de puerto elegido



Proporcione los detalles de mapeo de atributos:

- **Nombre para mostrar**
- **SID** (si estás usando LDAP)
- **Nombre de usuario**
- **ID de Unix** (si estás usando NFS)
- Si selecciona **Incluir atributos opcionales**, también puede agregar una dirección de correo electrónico, número de teléfono, rol, estado, país, departamento, foto, DN de gerente o grupos. Seleccione **Avanzado** para agregar una consulta de búsqueda opcional.

5. Seleccione **Agregar**.
6. Regrese a la pestaña de conectores del directorio de usuarios para verificar el estado de su conector de directorio de usuarios. Si se crea correctamente, el estado del conector del directorio de usuario se muestra como **En ejecución**.

Eliminar un conector de directorio de usuarios

Pasos

1. En Ransomware Resilience, vaya a **Configuración**.
2. Localice el mosaico Actividad del usuario y seleccione **Administrar**.
3. Seleccione la pestaña **Conector de directorio de usuarios**.
4. Identifique el conector del directorio de usuario que desea eliminar. En el menú de acciones al final de la línea, seleccione los tres puntos … luego **Eliminar**.
5. En el cuadro de diálogo emergente, selecciona **Borrar** para confirmar.

Excluir usuarios de alertas

Si hay ciertos usuarios de confianza cuyo comportamiento podría activar alertas de comportamiento del usuario, puedes excluirlos de las alertas.

Pasos

1. En Ransomware Resilience, seleccione **Configuración**.
2. En el panel de control de Configuración, localiza la tarjeta de actividad de usuario y selecciona **Manage**.
3. Selecciona la pestaña **Usuarios excluidos**.
4. Para revisar usuarios individuales en la interfaz de usuario, elige **Seleccionar manualmente**. Para cargar una lista de usuarios excluidos, selecciona **Cargar**.

    a. Si seleccionaste **Seleccionar manualmente**, marca la casilla junto a los nombres de los usuarios específicos que quieres excluir.

    b. Si seleccionas **Upload**, descarga el archivo CSV o JSON que incluye la lista de todos los usuarios. Selecciona **Download** para acceder a la lista.

    En tu equipo local, revisa el archivo. Elimina los nombres de todos los usuarios para los que quieres mantener la detección. Cuando la lista incluya solo los nombres de los usuarios que quieres excluir de la detección, guárdala.

    En Ransomware Resilience, selecciona **Subir**. Localiza y sube el archivo.

5. Selecciona **Add** para terminar de añadir los usuarios a la lista de exclusión.
6. En la pestaña **Usuarios excluidos**, los nombres de los usuarios eliminados de las alertas de detección de comportamiento de usuario ahora se muestran en el panel.

También puedes excluir a un usuario directamente de una alerta. Para más información, consulta "Responde a las alertas de ransomware".

Eliminar usuarios de la lista de usuarios excluidos

Puedes agregar un usuario de nuevo a la detección después.

Pasos

1. En el panel de control de Configuración, localiza la tarjeta de actividad de usuario y selecciona **Manage**.
2. Selecciona la pestaña **Usuarios excluidos**.
3. Seleccione **Agregar**.
4. Para excluir usuarios individuales de la interfaz de usuario, elige **Seleccionar manualmente**.
5. Localiza el nombre del usuario que quieres eliminar de la selección de usuarios excluidos. Selecciona el menú de acciones (…) en la fila con el nombre del usuario y luego **Remove**.
6. En el cuadro de diálogo, selecciona **Eliminar** para confirmar que quieres eliminar a los usuarios seleccionados.

Responder a alertas de actividad sospechosa del usuario

Después de configurar la detección de actividad sospechosa de usuarios, puedes monitorear los eventos en la página de alertas. Para más información, consulta "Detecta actividad maliciosa y comportamiento sospechoso de los usuarios".

Administra los grupos de protección en NetApp Ransomware Resilience

NetApp Ransomware Resilience ofrece grupos de protección para facilitar la gestión de tu patrimonio de datos. Los grupos de protección son agrupaciones lógicas de cargas de trabajo. Ransomware Resilience puede proteger todos los volúmenes de un grupo de protección al mismo tiempo con una sola estrategia de protección, así no tienes que aplicar una estrategia a cada carga de trabajo.

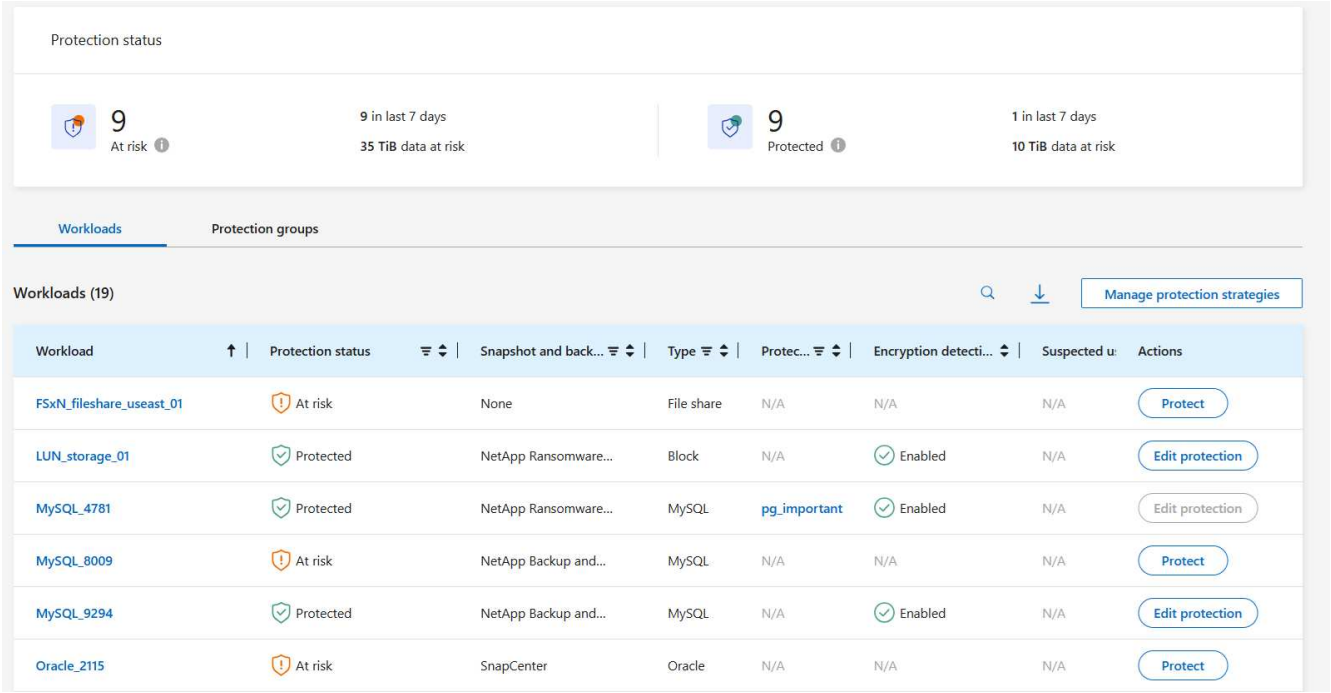
Rol de consola requerido Para realizar esta tarea, necesita el rol de administrador de organización, administrador de carpeta o proyecto, o administrador de resiliencia ante ransomware. "Obtenga información sobre las funciones de resiliencia ante ransomware para la NetApp Console" .

Crear un grupo de protección

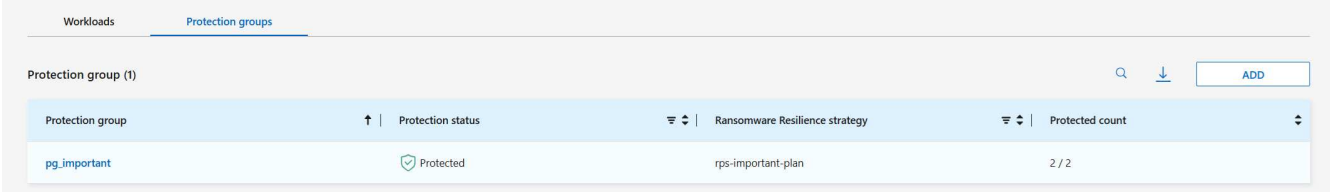
Puedes crear grupos independientemente de su estado de protección (es decir, grupos no protegidos y grupos protegidos). Cuando añades una política de protección a un grupo de protección, la nueva política de protección reemplaza cualquier política existente, incluidas las políticas gestionadas por NetApp Backup and Recovery.

Pasos

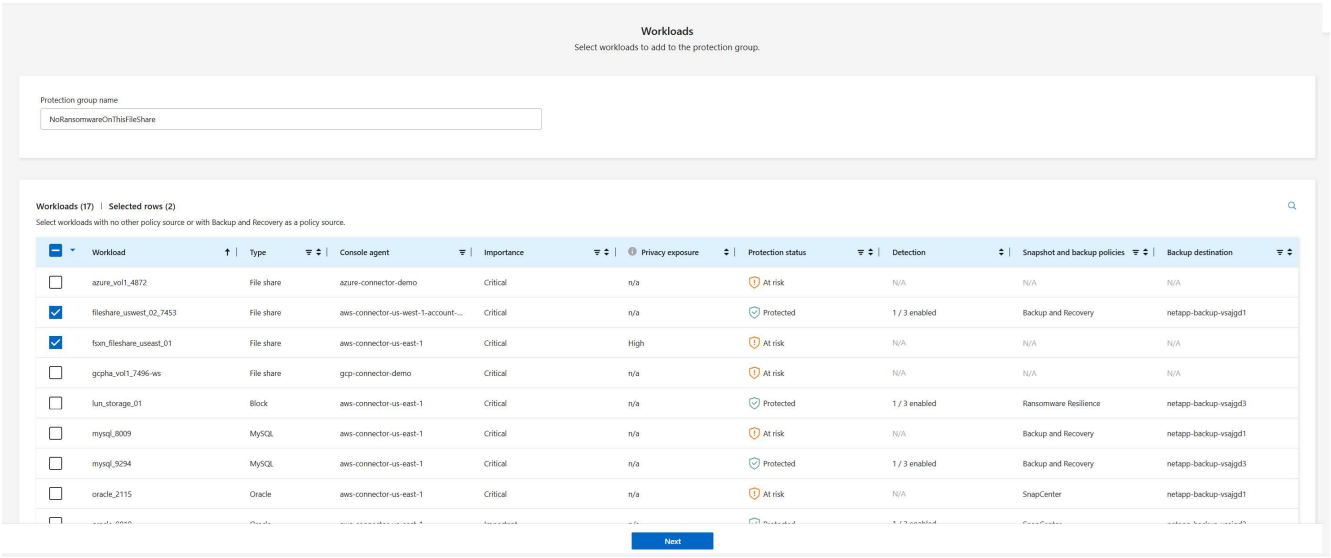
1. En el menú Resiliencia ante ransomware, seleccione **Protección**.



2. Desde el panel Protección, selecciona la pestaña **Protection groups**.



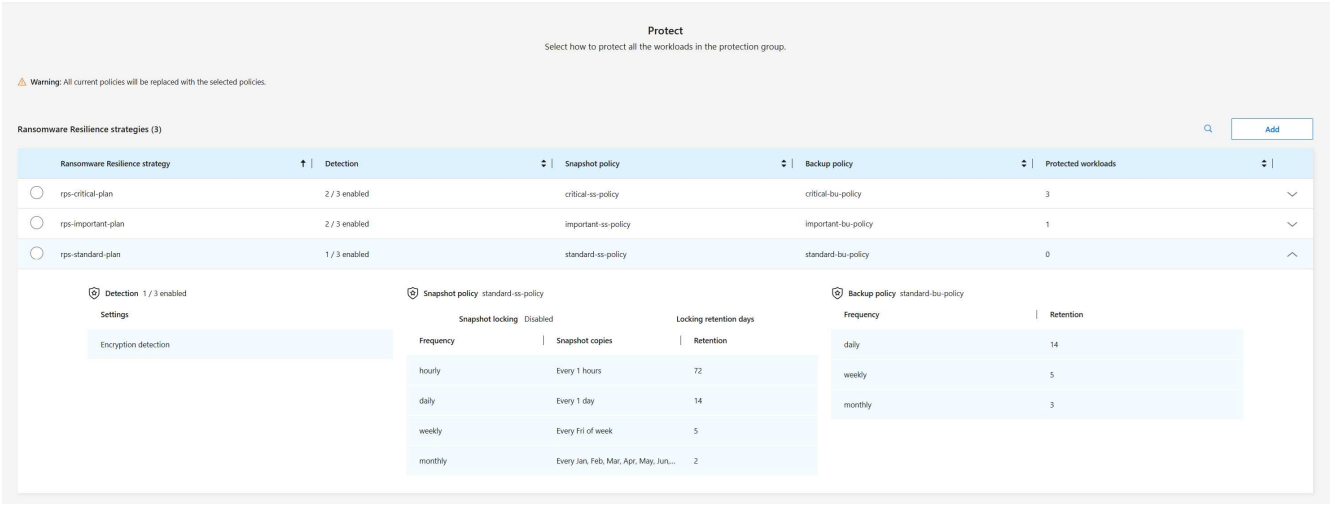
3. Seleccione **Agregar**.



4. Introduzca un nombre para el grupo de protección.
5. Seleccione las cargas de trabajo que desea agregar al grupo.

   Para ver más detalles sobre las cargas de trabajo, desplácese hacia la derecha.

6. Seleccione **Siguiente**.



7. Selecciona una estrategia de protección para el grupo.
8. Si la estrategia de protección incluye replicación, revise la configuración de replicación.
   a. Para replicar todas las instantáneas en el mismo destino, marque **Usar el mismo destino para cada carga de trabajo**. Seleccione un **Sistema de destino** y una **VM de almacenamiento de destino** para las cargas de trabajo en la sección Agente de consola. + Para utilizar destinos diferentes, desmarque esa casilla. Revise cada carga de trabajo bajo cada agente de consola y asigne un **Sistema de destino** y una **VM de almacenamiento de destino** para cada carga de trabajo. Seleccione **Siguiente**.
9. Para configurar una política de respaldo, elija una y luego seleccione **Siguiente**.
10. Si su política de detección incluye la detección del comportamiento del usuario, seleccione el recopilador de datos que desea utilizar y luego **Siguiente**.
11. Revise las selecciones para el grupo de protección.

12. Para finalizar el grupo de protección, selecciona **Add**.

> Al revisar el panel de protección en Ransomware Resilience, puedes ordenar las cargas de trabajo por grupo de protección.

Editar la protección del grupo

Puede cambiar la política de detección en un grupo existente.

Pasos

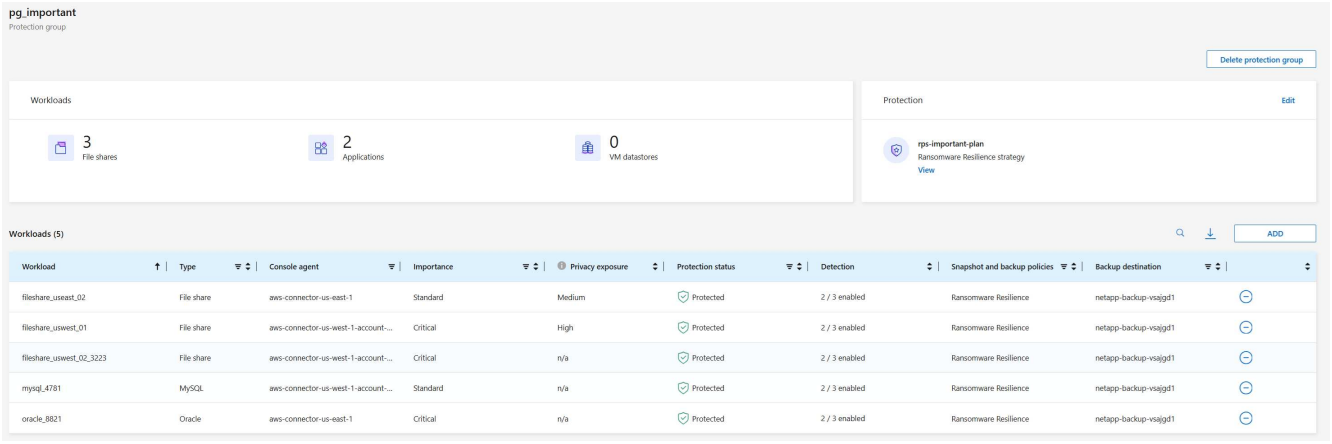
1. En el menú Resiliencia ante ransomware, seleccione **Protección**.
2. Desde la página Protección, seleccione la pestaña **Grupos de protección** y luego seleccione el grupo cuya política desea modificar.
3. Desde la página de descripción general del grupo de protección, seleccione **Editar protección**.
4. Selecciona una política de protección existente para aplicarla o selecciona **Add** para crear una nueva política de protección. Para más información sobre cómo añadir una política de protección, consulta "Crear una política de protección". Luego selecciona **Save**.
5. En la descripción general del destino de copia de seguridad, seleccione un destino de copia de seguridad existente o **Agregar un nuevo destino de copia de seguridad**.
6. Seleccione **Siguiente** para revisar sus cambios.

Eliminar cargas de trabajo de un grupo de protección

Es posible que más adelante necesites eliminar cargas de trabajo de un grupo de protección existente.

Pasos

1. En el menú Resiliencia ante ransomware, seleccione **Protección**.
2. Desde la página Protección, seleccione la pestaña **Grupos de protección**.
3. Seleccione el grupo del cual desea eliminar una o más cargas de trabajo.



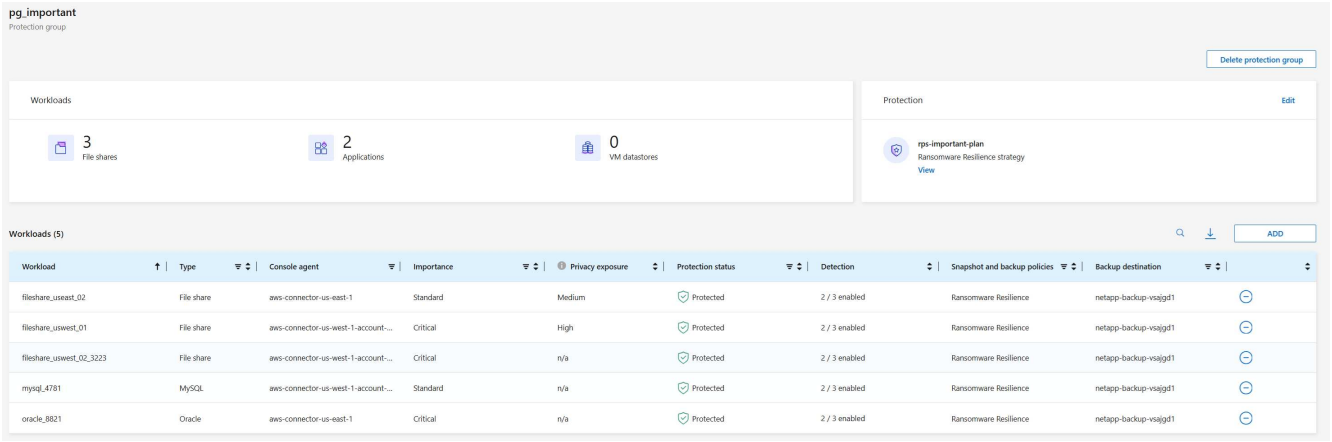
4. En la página del grupo de protección, selecciona la carga de trabajo que quieres quitar del grupo y selecciona la opción **Actions** ⋯.
5. En el menú Acciones, seleccione **Eliminar carga de trabajo**.
6. Confirme que desea eliminar la carga de trabajo y seleccione **Eliminar**.

Eliminar un grupo de protección

Cuando eliminas un grupo de protección, Ransomware Resilience elimina el grupo y la estrategia de protección de las cargas de trabajo. No elimina las cargas de trabajo individuales.

Pasos

1. En el menú Resiliencia ante ransomware, seleccione **Protección**.
2. Desde la página Protección, seleccione la pestaña **Grupos de protección**.
3. Seleccione el grupo del cual desea eliminar una o más cargas de trabajo.



4. Desde la página del grupo de protección seleccionado, en la parte superior derecha, seleccione **Eliminar grupo de protección**.
5. Confirme que desea eliminar el grupo y seleccione **Eliminar**.

Buscar información personal identificable en NetApp Ransomware Resilience

Dentro de NetApp Ransomware Resilience, puedes usar NetApp Data Classification para escanear y clasificar los datos en una carga de trabajo de archivos compartidos. Clasificar los datos te ayuda a determinar si el conjunto de datos incluye información de identificación personal (PII), lo que puede aumentar los riesgos de seguridad.

"Clasificación de datos"Utiliza el procesamiento del lenguaje natural impulsado por IA para el análisis y la categorización de datos contextuales, proporcionando información útil sobre sus datos para abordar los requisitos de cumplimiento, detectar vulnerabilidades de seguridad, optimizar costos y acelerar la migración.

La clasificación de datos es un componente central de la NetApp Console. No necesitas una licencia para usar Data Classification. Dependiendo de tu configuración, configurar Data Classification puede generar costes, que no son cobrados por Ransomware Resilience. Para más información, consulta "Aprenda sobre la clasificación de datos".

Este proceso puede afectar la importancia de la carga de trabajo para ayudar a garantizar que tenga la protección adecuada.

Rol de consola requerido Para realizar esta tarea, necesita el rol de administrador de organización, administrador de carpeta o proyecto, o administrador de resiliencia ante ransomware. "Obtenga información sobre las funciones de resiliencia ante ransomware para la NetApp Console" .

Identificar la exposición a la privacidad con la clasificación de datos

Antes de utilizar la clasificación de datos dentro de Ransomware Resilience, necesita"para permitir que la clasificación de datos escanee sus datos" .

Puede implementar la clasificación de datos dentro de la página de Protección de Resiliencia contra ransomware. Siga el procedimiento para identificar la exposición a la privacidad. Cuando selecciona **Identificar exposición**, si aún no ha implementado la Clasificación de datos, un cuadro de diálogo le permitirá habilitarla.

Para obtener más información sobre la clasificación de datos, consulte:

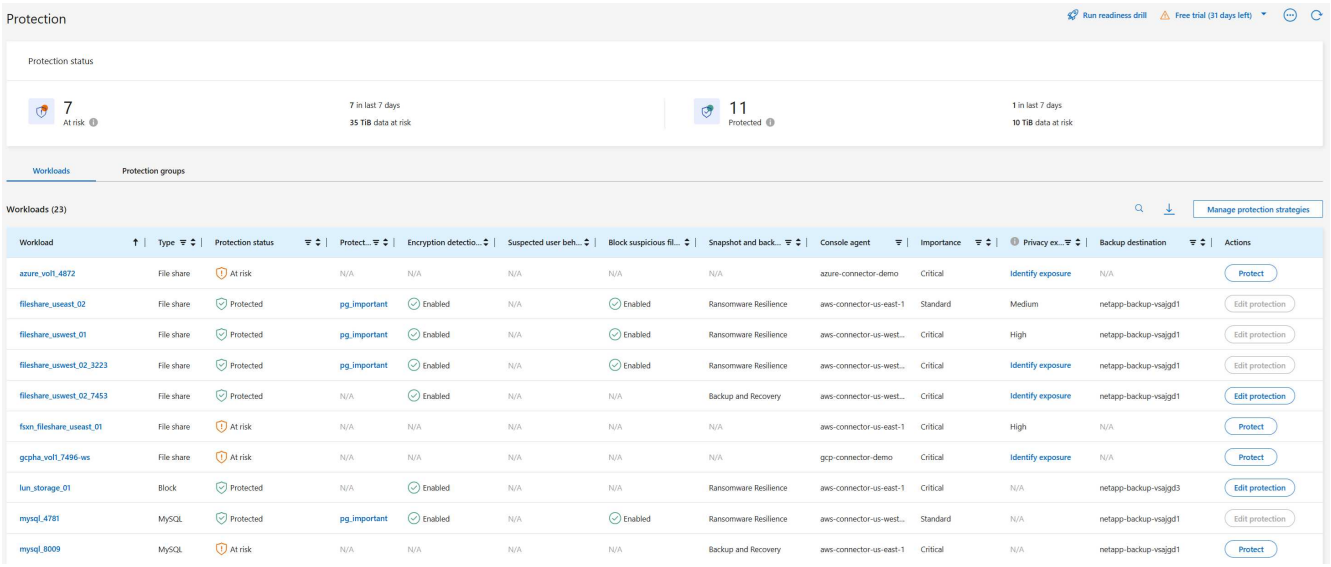
- "Aprenda sobre la clasificación de datos"
- "Categorías de datos privados"
- "Investigue los datos almacenados en su organización"

Antes de empezar

El escaneo de datos PII en Ransomware Resilience está disponible si tiene"Clasificación de datos implementada" . La clasificación de datos está disponible como parte de la consola sin costo adicional y se puede implementar en las instalaciones o en la nube del cliente.

Pasos

1. En el menú Resiliencia ante ransomware, seleccione **Protección**.
2. En la página Protección, busque una carga de trabajo de uso compartido de archivos en la columna Carga de trabajo.



3. Para habilitar la Clasificación de datos para escanear sus datos en busca de información personal identificable, en la columna **Exposición de privacidad**, seleccione **Identificar exposición**.

> Si no ha implementado la Clasificación de datos, al seleccionar **Identificar exposición** se abre un cuadro de diálogo para implementar la Clasificación de datos. Seleccione **Implementar**. Después de haber implementado la Clasificación de datos, puede regresar a la página Protección y luego seleccionar **Identificar exposición**.

Resultado

El escaneo puede tardar varios minutos dependiendo del tamaño y la cantidad de archivos. Durante el escaneo, la página de Protección indica que está identificando archivos y proporciona un recuento de archivos. Una vez finalizado el escaneo, la columna Exposición a la privacidad clasifica el nivel de exposición como Bajo, Medio o Alto.

Revisar la exposición a la privacidad

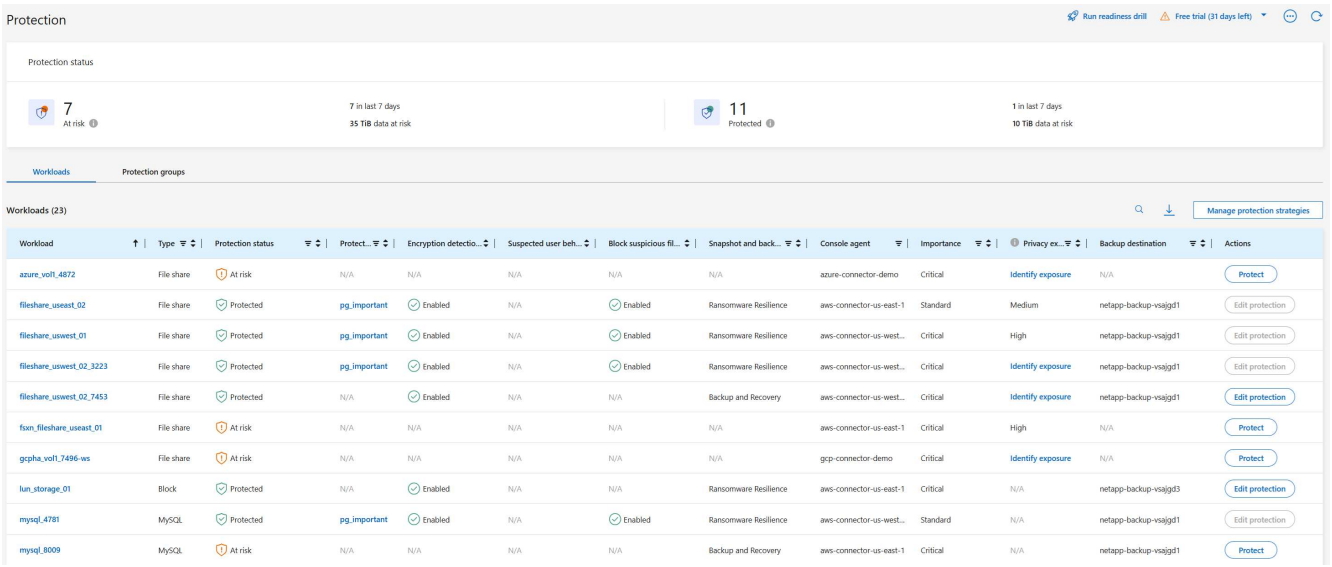
Después de los análisis de clasificación de datos en busca de información personal identificable, evalúe el riesgo.

Los datos PII se clasifican en una de tres designaciones:

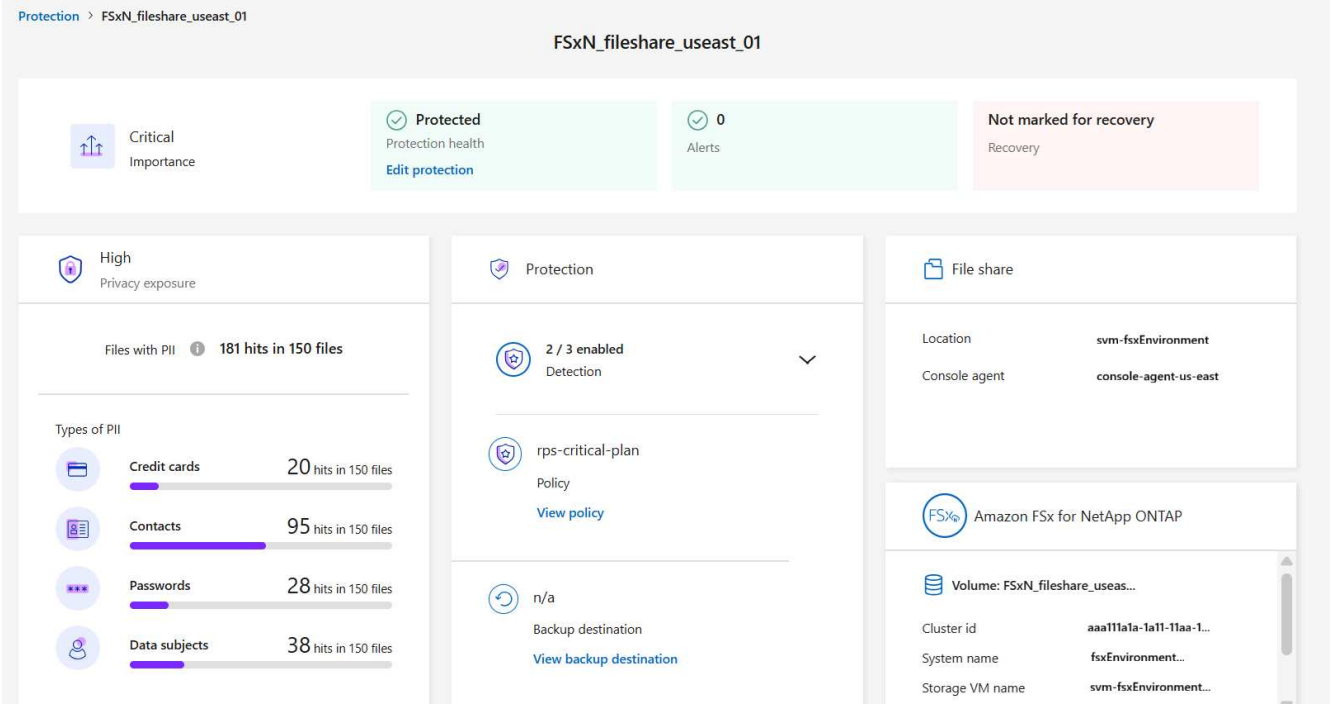
- **Alto**: Más del 70% de los archivos contienen información personal identificable
- **Medio**: Más del 30% y menos del 70% de los archivos contienen información de identificación personal (PII)
- **Bajo**: Más del 0% y menos del 30% de los archivos contienen información personal identificable

Pasos

1. En el menú Resiliencia ante ransomware, seleccione **Protección**.
2. En la página Protección, ubique la carga de trabajo del recurso compartido de archivos en la columna Carga de trabajo que muestra un estado en la columna Exposición de privacidad.



3. Seleccione el enlace de carga de trabajo en la columna Carga de trabajo para ver los detalles de la carga de trabajo.



4. En la página de detalles de la carga de trabajo, observe los detalles en el mosaico de exposición de privacidad.

El impacto de la exposición a la privacidad en la importancia de la carga de trabajo

Los cambios en la exposición a la privacidad pueden afectar la importancia de la carga de trabajo.

Cuando se expone la privacidad:	De esta exposición de privacidad:	A esta exposición de privacidad:	Entonces, la importancia de la carga de trabajo hace esto: .
Disminuye	Alto, Medio o Bajo	Medio, bajo o ninguno	Sigue igual
Aumenta	Ninguno	Bajo	Permanece en Standard
	Bajo	Medio	Cambios de Estándar a Importante
	Bajo o medio	Alto	Cambios de Estándar o Importante a Crítico

Para más información

Para obtener detalles sobre la clasificación de datos, consulte la documentación de clasificación de datos:

- "Aprenda sobre la clasificación de datos"
- "Categorías de datos privados"
- "Investigue los datos almacenados en su organización"

Responder y recuperarse

Administrar alertas en NetApp Ransomware Resilience

Cuando NetApp Ransomware Resilience detecta un posible ataque, muestra una alerta en el panel de control y en el menú de notificaciones. Ransomware Resilience toma inmediatamente una instantánea. Cuando recibas una alerta, revisa el riesgo potencial en la pestaña **Alerts** de Ransomware Resilience para evaluar el impacto en tus datos y prevenir un posible ataque de ransomware.

Si Ransomware Resilience detecta un posible ataque, aparece una notificación en la configuración de notificaciones de la NetApp Console y se envía un correo electrónico a las direcciones configuradas. El correo electrónico incluye información sobre la gravedad, la carga de trabajo afectada y un enlace a la alerta en la pestaña **Alerts** de Ransomware Resilience.

Puede descartar los falsos positivos o decidir recuperar sus datos inmediatamente.

Si descarta la alerta, Ransomware Resilience aprende este comportamiento, lo asocia con operaciones normales y no vuelve a iniciar una alerta al respecto.

Para comenzar a recuperar sus datos, marque la alerta como lista para recuperación para que su administrador de almacenamiento pueda comenzar el proceso de recuperación.

Cada alerta puede incluir múltiples incidentes en diferentes volúmenes y estados. Revisar todos los incidentes.

Cómo se generan las alertas

Ransomware Resilience se basa en pruebas sobre patrones de entropía de datos, tipos de extensión de archivos y cifrado para producir alertas. Las alertas se basan en los siguientes eventos:

- Violación de datos
- Destrucción de datos
- Se crearon o cambiaron extensiones de archivo
- Creación de archivos con comparación de tasas detectadas y esperadas
- Eliminación de archivos con una comparación de las tasas detectadas y esperadas
- Comportamiento sospechoso de usuario
- Cuando el cifrado es alto, sin cambios en la extensión del archivo

Para las alertas de violación de datos, destrucción de datos y comportamiento sospechoso de los usuarios, debes configurar "detección de actividad del usuario".

Tipos y estados de alerta

Las alertas tienen uno de dos estados: **Nueva** o **Inactiva**.

Una alerta se clasifica como uno de los siguientes tipos:

- **Ataque potencial**: Una alerta se clasifica como ataque potencial cuando:

- Autonomous Ransomware Protection detecta una nueva extensión y la ocurrencia se repite más de 20 veces en las últimas 24 horas (comportamiento por defecto).
- Se detectan las brechas de datos.
- Se detecta la destrucción de datos.

- **Advertencia**: Se produce una advertencia basada en los siguientes comportamientos:
  - No se ha identificado antes la detección de una nueva extensión y el mismo comportamiento no se repite suficientes veces como para declararlo como un ataque.
  - Se observa alta entropía.
  - La actividad de lectura, escritura, cambio de nombre o eliminación de archivos se duplicó en comparación con los niveles normales.

Para entornos SAN, las advertencias se basan solo en la alta entropía.

La evidencia se basa en información de Autonomous Ransomware Protection en ONTAP. Para más detalles, consulte "Descripción general de la protección autónoma contra ransomware" .

Estados de alerta

Un incidente de alerta puede tener los siguientes estados:

Estado	Descripción
Nuevo	Todos los incidentes se marcan como "new" cuando se identifican por primera vez.
En revisión	Puedes marcar manualmente un incidente de alerta como "en revisión" mientras lo evalúas.
Descartado	Si sospechas que la actividad no es un ataque de ransomware, puedes cambiar el estado a "descartado". + PRECAUCIÓN: Después de descartar un ataque, no puedes revertir su estado. Si descartas una carga de trabajo, todas las copias instantáneas tomadas automáticamente en respuesta al posible ataque de ransomware se eliminarán permanentemente.
Resuelto	El incidente ha sido solucionado.
Auto Resuelto	Para las alertas de baja prioridad, el incidente se resuelve automáticamente si no se ha tomado ninguna acción sobre él en cinco días.

Ver alertas

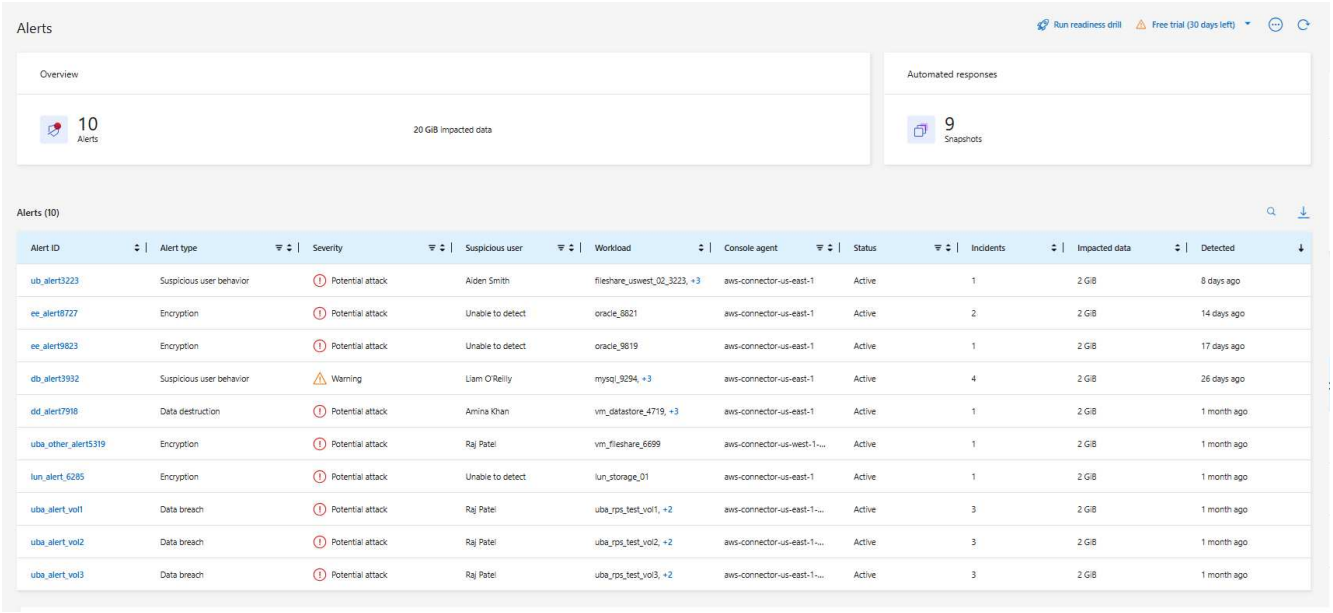
Puedes acceder a las alertas desde el panel de Ransomware Resilience o desde la pestaña **Alertas**.

Rol de consola requerido Para realizar esta tarea, necesita el rol de administrador de la organización, administrador de carpeta o proyecto, administrador de resiliencia ante ransomware o visor de resiliencia ante ransomware. "Obtenga información sobre las funciones de resiliencia ante ransomware para la NetApp Console" .

Pasos

1. En el panel de Ransomware Resilience, revisa el panel de Alertas.
2. Seleccione **Ver todo** en uno de los estados.
3. Seleccione una alerta para revisar todos los incidentes en cada volumen para cada alerta.

4. Para revisar alertas adicionales, seleccione **Alerta** en las rutas de navegación de la parte superior izquierda.
5. Revise las alertas en la página Alertas.



6. Continúe con una de las siguientes opciones:
   - Detectar actividad maliciosa y comportamiento anómalo del usuario .
   - Marcar los incidentes de ransomware como listos para recuperación (después de que se neutralizan los incidentes) .
   - Descartar incidentes que no sean ataques potenciales .

Responder a un correo electrónico de alerta

Cuando Ransomware Resilience detecta un posible ataque, envía una notificación por correo electrónico a los usuarios suscritos según sus preferencias de notificación de suscripción configuradas en la configuración de NetApp Console. El correo electrónico contiene información sobre la alerta, incluyendo la gravedad y los recursos afectados.

Para configurar las notificaciones por correo electrónico en la Console, consulta "Establecer la configuración de notificaciones por correo electrónico".

Rol de consola requerido Para realizar esta tarea, necesita el rol de administrador de la organización, administrador de carpeta o proyecto, administrador de resiliencia ante ransomware o visor de resiliencia ante ransomware. "Obtenga información sobre las funciones de resiliencia ante ransomware para la NetApp Console" .

Pasos

1. Ver el correo electrónico.
2. En el correo electrónico, selecciona **Ver alerta** e inicia sesión en Ransomware Resilience.

   Aparece la página de Alertas.

3. Revise todos los incidentes en cada volumen para cada alerta.

4. Para revisar alertas adicionales, seleccione **Alerta** en las rutas de navegación de la parte superior izquierda.
5. Continúe con una de las siguientes opciones:
    - Detectar actividad maliciosa y comportamiento anómalo del usuario .
    - Marcar los incidentes de ransomware como listos para recuperación (después de que se neutralizan los incidentes) .
    - Descartar incidentes que no sean ataques potenciales .

Detectar actividad maliciosa y comportamiento anómalo del usuario

Al mirar la pestaña Alertas, puede identificar si hay actividad maliciosa o un comportamiento anómalo del usuario.

Debes haber configurado un agente de actividad del usuario y habilitado una política de protección con detección del comportamiento del usuario para ver las alertas a nivel de usuario. La columna **Usuario sospechoso** aparece en el panel de alertas solo cuando la detección del comportamiento del usuario está habilitada. Para habilitar la detección de usuarios sospechosos, consulta "Actividad sospechosa del usuario".

Ver actividad maliciosa

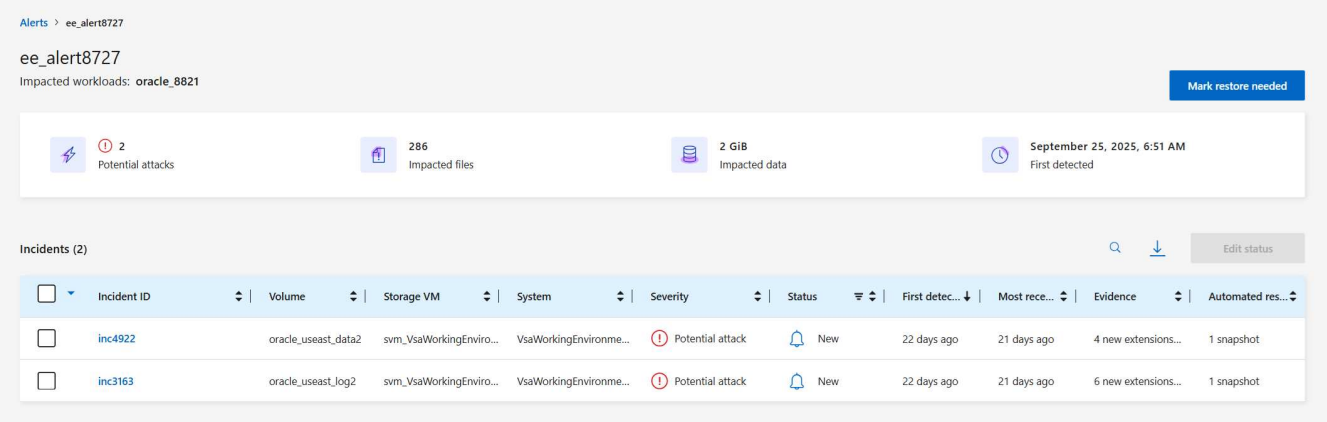
Cuando Autonomous Ransomware Protection activa una alerta en Ransomware Resilience, puedes ver los siguientes detalles:

- Cuándo se activó la alerta
- Cuando se modificó o se denegó el acceso
- Entropía de los datos entrantes
- Tasa esperada de creación de nuevos archivos en comparación con la tasa detectada
- Tasa de eliminación de archivos esperada en comparación con la tasa detectada
- Tasa de cambio de nombre de archivos esperada en comparación con la tasa detectada
- Cargas de trabajo, volúmenes, archivos y directorios afectados

> Estos detalles son visibles para las cargas de trabajo NAS. Para entornos SAN, solo están disponibles los datos de entropía.

Pasos

1. En el menú Resiliencia ante ransomware, seleccione **Alertas**.
2. Seleccione una alerta.
3. Revise los incidentes en la alerta.



4. Seleccione un incidente para revisar los detalles del mismo.

Ver comportamiento anómalo del usuario

Si has configurado la detección de usuarios sospechosos para ver el comportamiento anómalo de los usuarios, puedes ver los datos a nivel de usuario y bloquear usuarios específicos. Para activar la configuración de usuarios sospechosos, consulta "Configura agentes y colectores para la detección de actividad de usuarios".

Pasos

1. En el menú Resiliencia ante ransomware, seleccione **Alertas**.
2. Seleccione una alerta.
3. Revise los incidentes en la alerta.
   a. Para bloquear a un usuario sospechoso en tu entorno, selecciona **Block** junto al nombre del usuario.
   b. Para desactivar las alertas sobre un usuario determinado que es objeto de una alerta que sabes que es falsa, selecciona los tres puntos (...) y luego **Excluir a este usuario de la supervisión**. Revisa el cuadro de diálogo y luego selecciona **Excluir** para confirmar.

Para volver a activar las alertas para un usuario, devuelve la alerta. Selecciona los tres puntos y luego **Incluir a este usuario en la supervisión**. También puedes "Excluir usuarios" de la supervisión.

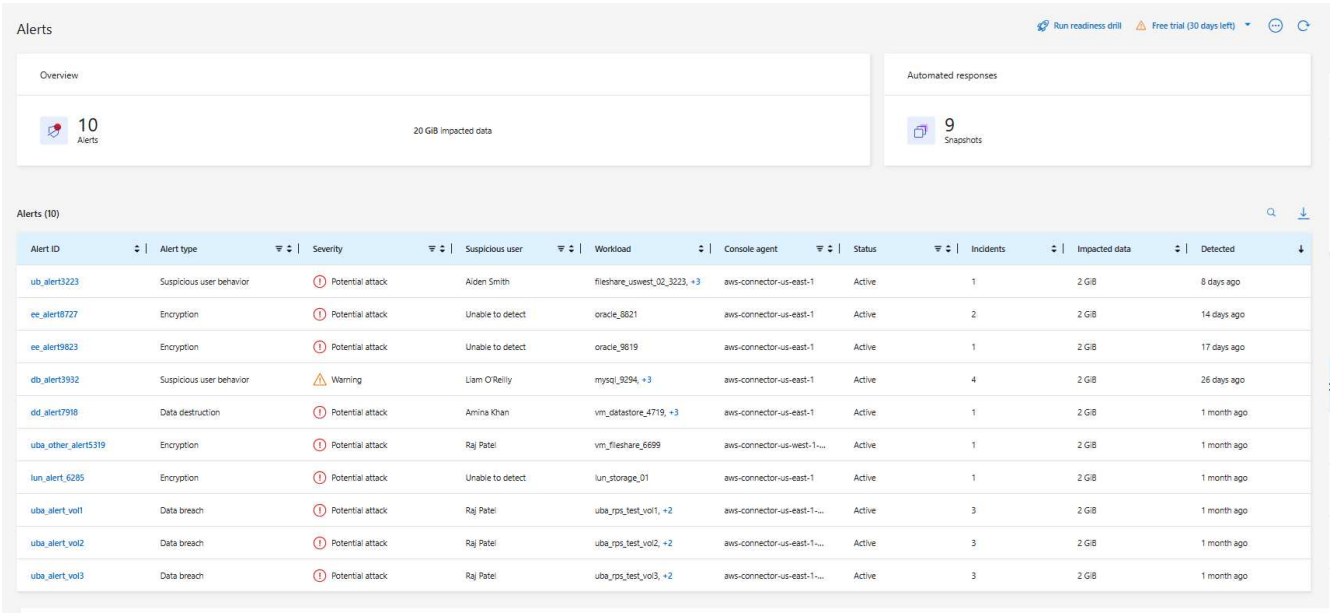
Marcar los incidentes de ransomware como listos para recuperación (después de que se neutralizan los incidentes)

Después de detener el ataque, avisa al administrador de almacenamiento que los datos están listos para que pueda iniciar el proceso de recuperación.

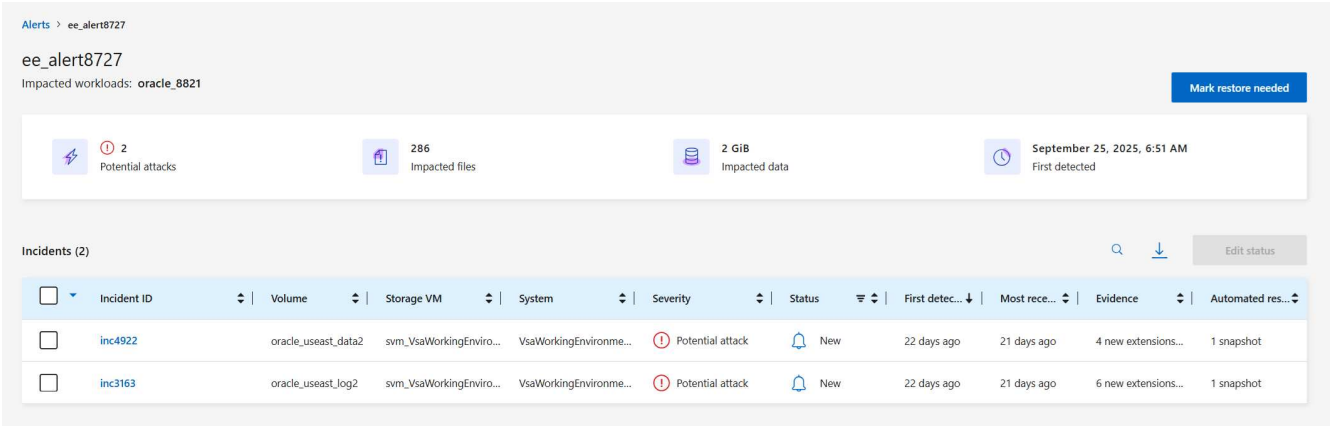
Rol de consola requerido Para realizar esta tarea, necesita el rol de administrador de organización, administrador de carpeta o proyecto, o administrador de resiliencia ante ransomware. "Obtenga información sobre las funciones de resiliencia ante ransomware para la NetApp Console" .

Pasos

1. En el menú Resiliencia ante ransomware, seleccione **Alertas**.



2. En la página Alertas, seleccione la alerta.
3. Revise los incidentes en la alerta.



4. Si determina que los incidentes están listos para recuperación, seleccione **Marcar como necesario para la restauración**.
5. Confirme la acción y seleccione **Marcar como necesaria la restauración**.
6. Para iniciar la recuperación de la carga de trabajo, seleccione **Recuperar** carga de trabajo en el mensaje o seleccione la pestaña **Recuperación**.

Resultado

Una vez que la alerta se marca para restaurar, se mueve de la pestaña Alertas a la pestaña Recuperación.

Descartar incidentes que no sean ataques potenciales

Después de revisar los incidentes, debe determinar si son ataques potenciales. Si no son amenazas reales, pueden descartarse.

Puede descartar los falsos positivos o decidir recuperar sus datos inmediatamente. Si descarta la alerta, Ransomware Resilience aprende este comportamiento y lo asocia con operaciones normales y no vuelve a iniciar una alerta sobre dicho comportamiento.

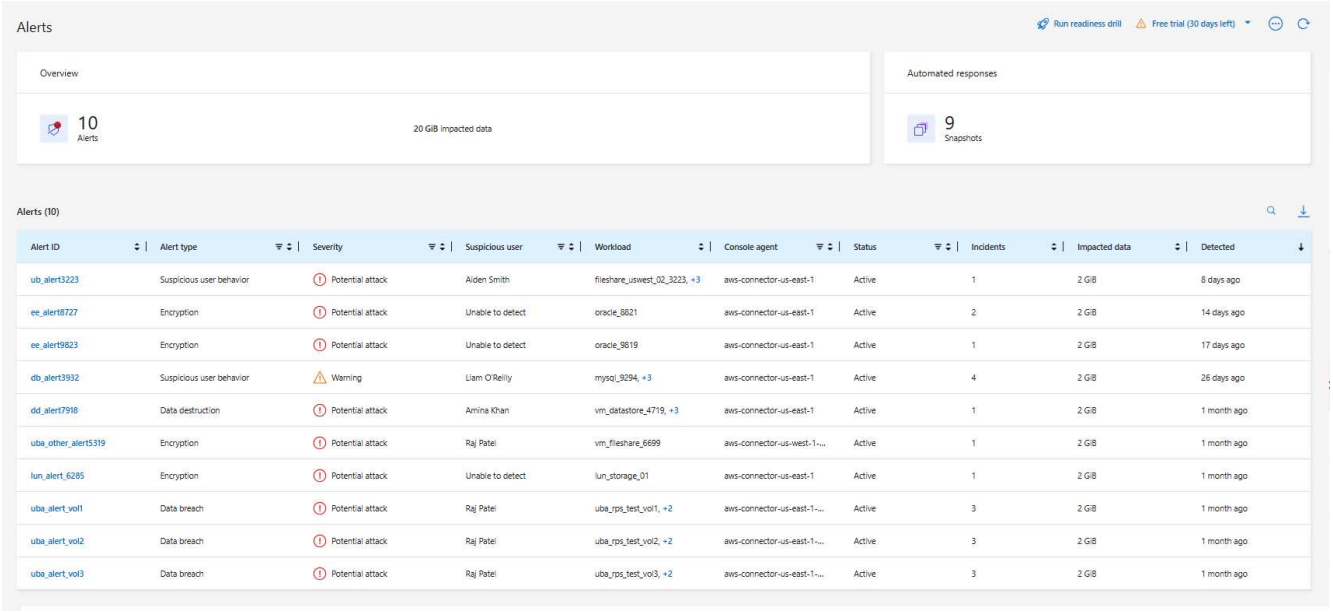
Si descarta una carga de trabajo, todas las copias instantáneas tomadas automáticamente en respuesta a un posible ataque de ransomware se eliminan de forma permanente.

Si descarta una alerta, no podrá cambiar su estado ni deshacer este cambio.

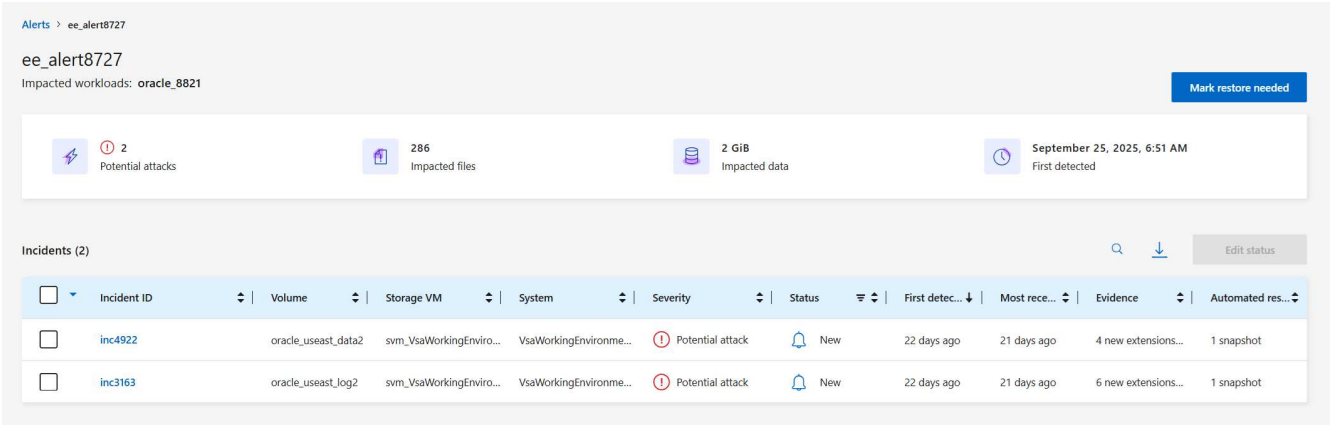
Rol de consola requerido Para realizar esta tarea, necesita el rol de administrador de organización, administrador de carpeta o proyecto, o administrador de resiliencia ante ransomware. "Obtenga información sobre las funciones de resiliencia ante ransomware para la NetApp Console" .

Pasos

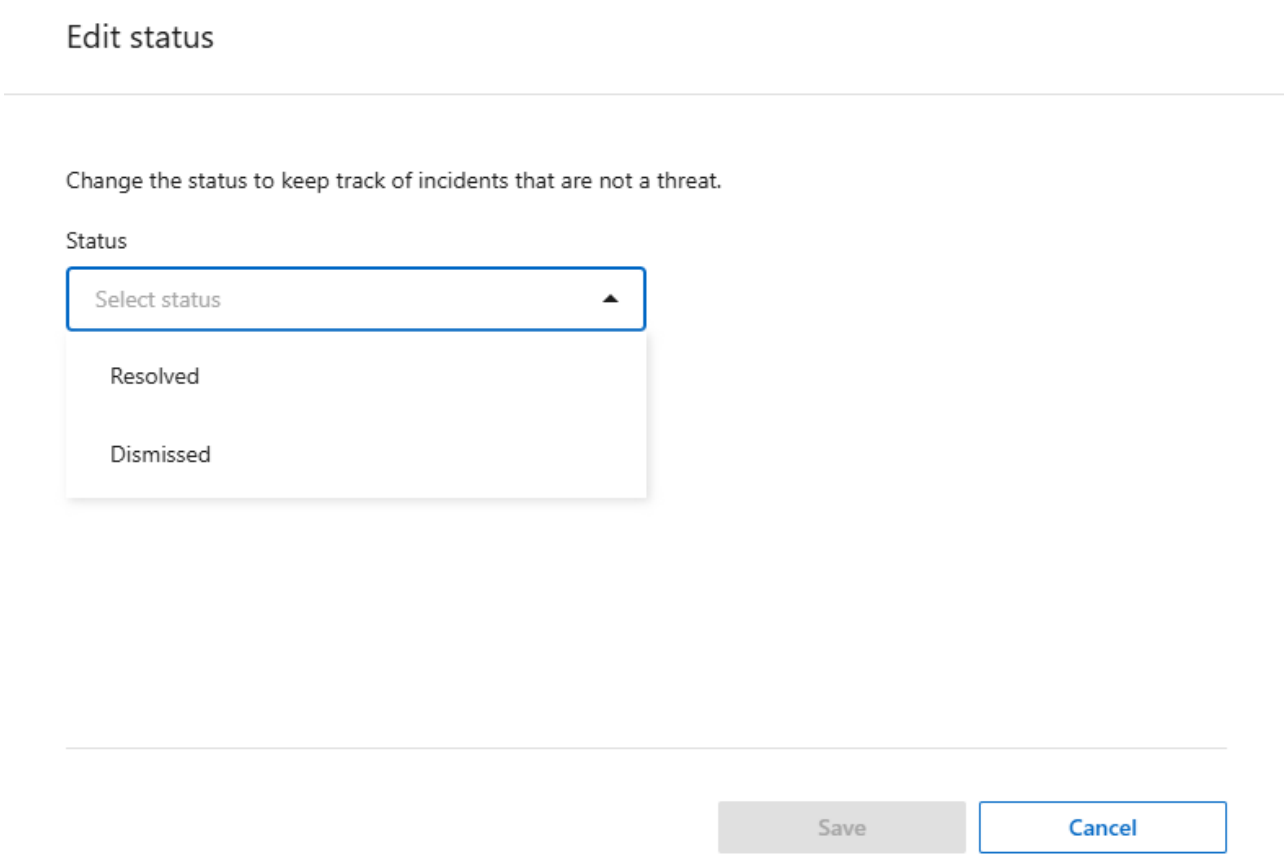
1. En el menú Resiliencia ante ransomware, seleccione **Alertas**.



2. En la página Alertas, seleccione la alerta.



3. Seleccione uno o más incidentes. Alternativamente, seleccione todos los incidentes seleccionando el cuadro ID de incidente en la parte superior izquierda de la tabla.
4. Si determina que el incidente no es una amenaza, deséchelo como un falso positivo:
   - Seleccione el incidente.
   - Seleccione el botón **Editar estado** encima de la tabla.



5. Desde el cuadro Editar estado, elija el estado **Descartado**.

   Aparece información adicional sobre la carga de trabajo y las copias de instantáneas eliminadas.

6. Seleccione **Guardar**.

   El estado del incidente o incidentes cambia a "Descartado".

Ver una lista de archivos afectados

Antes de restaurar una carga de trabajo de la aplicación a nivel de archivo, puede ver una lista de los archivos afectados. Puede acceder a la página de Alertas para descargar una lista de archivos afectados. Luego utilice la página Recuperación para cargar la lista y elegir qué archivos restaurar.

Rol de consola requerido Para realizar esta tarea, necesita el rol de administrador de organización, administrador de carpeta o proyecto, o administrador de resiliencia ante ransomware. "Obtenga información sobre las funciones de resiliencia ante ransomware para la NetApp Console" .

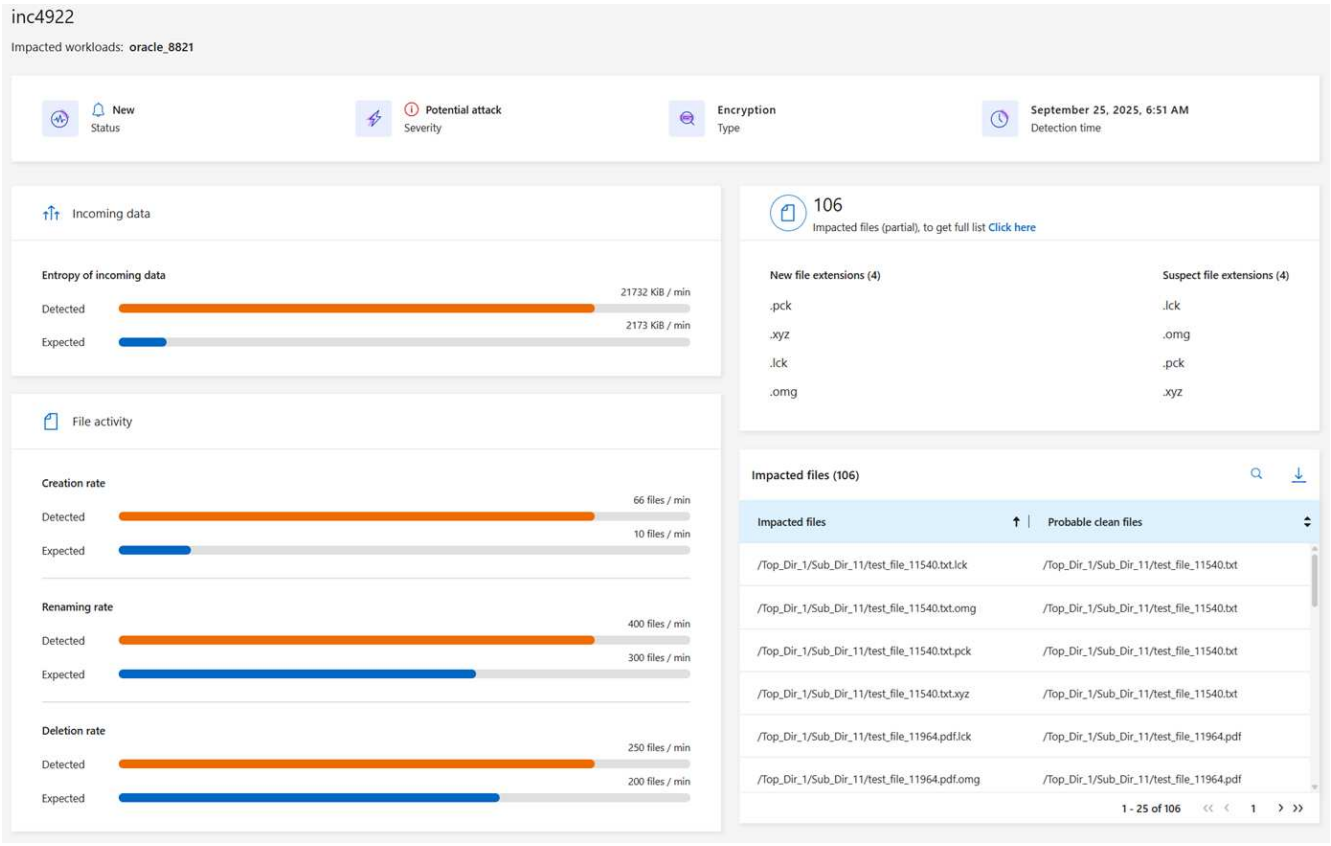
Pasos

Utilice la página Alertas para recuperar la lista de archivos afectados.

Si un volumen tiene varias alertas, es posible que deba descargar la lista CSV de los archivos afectados para cada alerta.

1. En el menú Resiliencia ante ransomware, seleccione **Alertas**.

2. En la página Alertas, ordene los resultados por carga de trabajo para mostrar las alertas de la carga de trabajo de la aplicación que desea restaurar.
3. De la lista de alertas para esa carga de trabajo, seleccione una alerta.
4. Para esa alerta, seleccione un solo incidente.



5. Para ese incidente, seleccione el ícono de descarga para descargar la lista de archivos afectados en formato CSV.

Recupérate de un ataque de ransomware con NetApp Ransomware Resilience

Una vez que las cargas de trabajo se marcan como "Se necesita restauración", NetApp Ransomware Resilience recomienda un punto de recuperación real (RPA) y organiza el flujo de trabajo para una recuperación resistente a fallas.

- Si la aplicación o la máquina virtual está gestionada por NetApp Backup and Recovery o Ransomware Resilience, Ransomware Resilience realiza una restauración coherente con fallos, donde se restaura toda la información que estaba en el volumen en el mismo punto en el tiempo, por ejemplo, si el sistema se bloquea.

  Puede restaurar la carga de trabajo seleccionando todos los volúmenes, volúmenes específicos o archivos específicos.

La recuperación de la carga de trabajo puede afectar las cargas de trabajo en ejecución. Debe coordinar los procesos de recuperación con las partes interesadas adecuadas.

Una carga de trabajo puede tener uno de los siguientes estados de restauración:

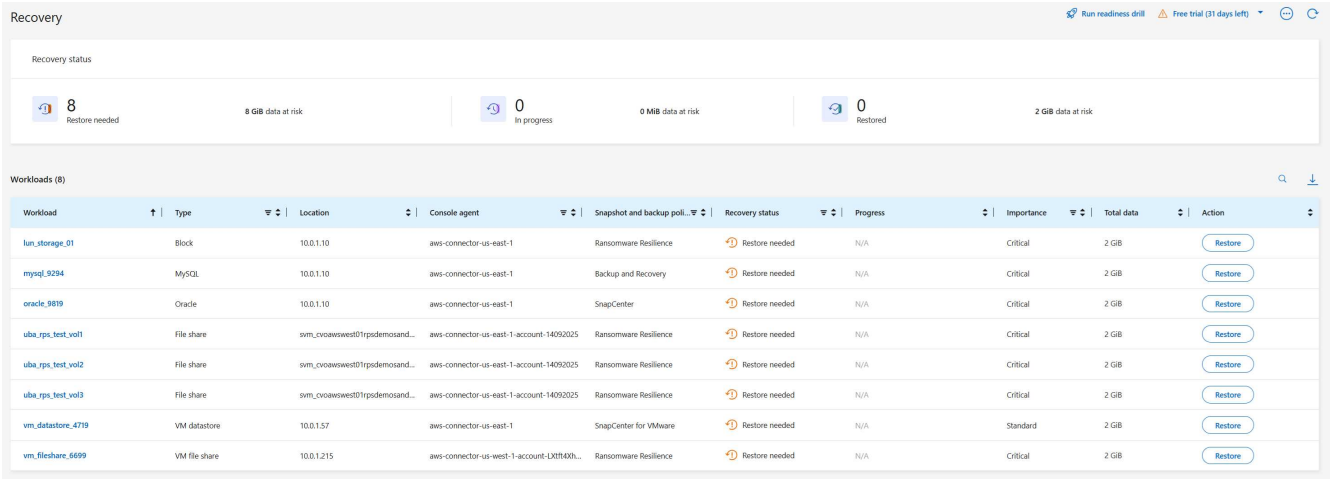
- **Se necesita restaurar**: Es necesario restaurar la carga de trabajo.
- **En progreso**: La operación de restauración está actualmente en curso.
- **Restaurado**: La carga de trabajo ha sido restaurada.
- **Error**: No se pudo completar el proceso de restauración de la carga de trabajo.

Ver las cargas de trabajo que están listas para ser restauradas

Revise las cargas de trabajo que están en el estado de recuperación "Se necesita restauración".

Pasos

1. Debe realizar una de las siguientes acciones:
   - Desde el panel de control, revisa los totales de "Restauración necesaria" en el panel de Alertas y selecciona **Ver todo**.
   - Desde el menú, seleccione **Recuperación**.
2. Revise la información de la carga de trabajo en la página **Recuperación**.



Restaurar una carga de trabajo

Al utilizar Ransomware Resilience, el administrador de almacenamiento puede determinar la mejor manera de restaurar las cargas de trabajo desde el punto de restauración recomendado o el punto de restauración preferido.

Rol de consola requerido Para realizar esta tarea, necesita el rol de administrador de organización, administrador de carpeta o proyecto, o administrador de resiliencia ante ransomware. "Obtenga información sobre las funciones de resiliencia ante ransomware para la NetApp Console" .

El administrador de almacenamiento de seguridad puede recuperar datos en diferentes niveles:

- Recuperar todos los volúmenes
- Recuperar una aplicación a nivel de volumen o de archivo y carpeta.
- Recupere un recurso compartido de archivos a nivel de volumen, directorio o archivo/carpeta.
- Recuperarse de un almacén de datos a nivel de VM.

El proceso varía según el tipo de carga de trabajo.

Pasos

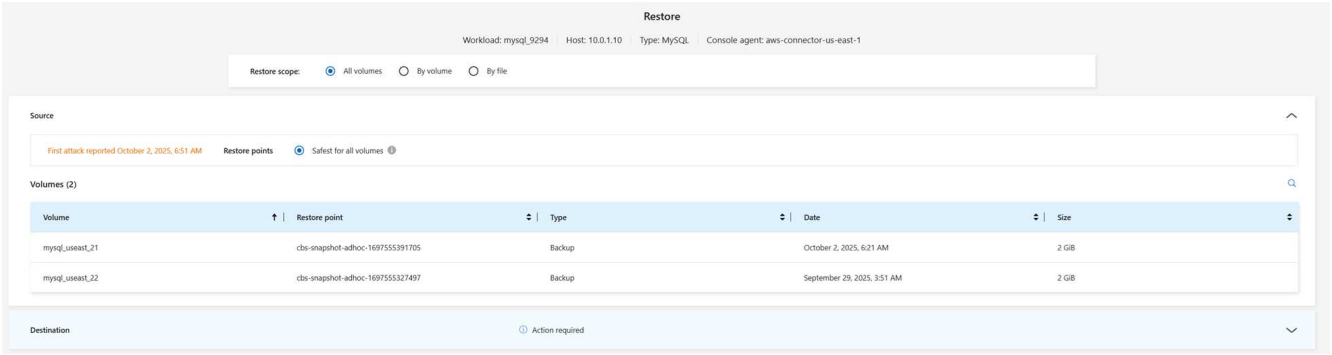
1. En el menú Resiliencia ante ransomware, seleccione **Recuperación**.
2. Revise la información de la carga de trabajo en la página **Recuperación**.
3. Seleccione una carga de trabajo que esté en el estado "Se necesita restaurar".
4. Para restaurar, seleccione **Restaurar**.
5. **Alcance de restauración**: seleccione el tipo de restauración que desea completar:
   - Todos los volúmenes
   - Por volumen
   - Por archivo: puede especificar una carpeta o archivos individuales para restaurar.

   Para las cargas de trabajo SAN, solo se puede restaurar por carga de trabajo.

   Puede seleccionar hasta 100 archivos o una sola carpeta.
6. Continúe con uno de los siguientes procedimientos dependiendo de si eligió aplicación, volumen o archivo.

Restaurar todos los volúmenes

1. En el menú Resiliencia ante ransomware, seleccione **Recuperación**.
2. Seleccione una carga de trabajo que esté en el estado "Se necesita restaurar".
3. Para restaurar, seleccione **Restaurar**.
4. En la página Restaurar, en el ámbito de restauración, seleccione **Todos los volúmenes**.



5. **Fuente**: Seleccione la flecha hacia abajo junto a Fuente para ver los detalles.
   a. Seleccione el punto de restauración que desea utilizar para restaurar los datos.

   Ransomware Resilience identifica el mejor punto de restauración como la última copia de seguridad justo antes del incidente y muestra una indicación de "Más seguro para todos los volúmenes". Esto significa que todos los volúmenes se restaurarán a una copia anterior al primer ataque al primer volumen detectado.
6. **Destino**: Seleccione la flecha hacia abajo junto a Destino para ver los detalles.
   a. Seleccione el sistema.
   b. Seleccione la máquina virtual de almacenamiento.

c. Seleccione el agregado.

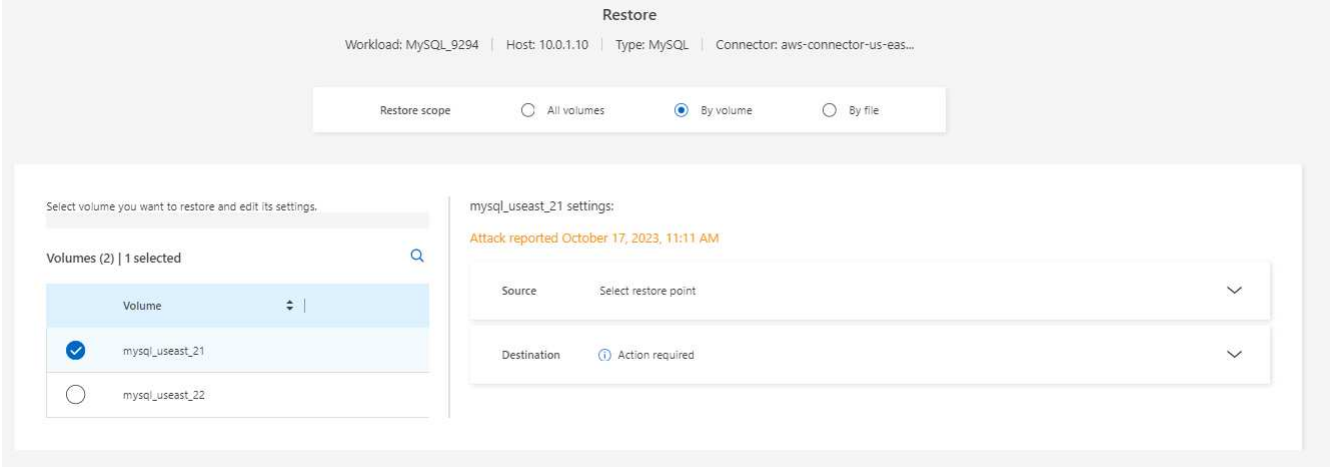
d. Cambie el prefijo de volumen que se agregará a todos los volúmenes nuevos.

> El nuevo nombre del volumen aparece como prefijo + nombre del volumen original + nombre de la copia de seguridad + fecha de la copia de seguridad.

7. Seleccione **Guardar**.
8. Seleccione **Siguiente**.
9. Revise sus selecciones.
10. Seleccione **Restaurar**.
11. Desde el menú superior, seleccione **Recuperación** para revisar la carga de trabajo en la página Recuperación, donde el estado de la operación se mueve a través de los estados.

Restaurar una carga de trabajo de la aplicación a nivel de volumen

1. En el menú Resiliencia ante ransomware, seleccione **Recuperación**.
2. Seleccione una carga de trabajo de aplicación que esté en el estado "Se necesita restaurar".
3. Para restaurar, seleccione **Restaurar**.
4. En la página Restaurar, en el ámbito de restauración, seleccione **Por volumen**.



5. En la lista de volúmenes, seleccione el volumen que desea restaurar.
6. **Fuente**: Seleccione la flecha hacia abajo junto a Fuente para ver los detalles.
   a. Seleccione el punto de restauración que desea utilizar para restaurar los datos.

> Ransomware Resilience identifica el mejor punto de restauración como la última copia de seguridad justo antes del incidente y muestra una indicación de "Recomendado".

7. **Destino**: Seleccione la flecha hacia abajo junto a Destino para ver los detalles.
   a. Seleccione el sistema.
   b. Seleccione la máquina virtual de almacenamiento.
   c. Seleccione el agregado.
   d. Revise el nuevo nombre del volumen.

El nuevo nombre del volumen aparece como el nombre del volumen original + el nombre de la copia de seguridad + la fecha de la copia de seguridad.

8. Seleccione **Guardar**.
9. Seleccione **Siguiente**.
10. Revise sus selecciones.
11. Seleccione **Restaurar**.
12. Desde el menú superior, seleccione **Recuperación** para revisar la carga de trabajo en la página Recuperación, donde el estado de la operación se mueve a través de los estados.

Restaurar una carga de trabajo de la aplicación a nivel de archivo

Antes de restaurar una carga de trabajo de la aplicación a nivel de archivo, puede ver una lista de los archivos afectados. Puede acceder a la página de Alertas para descargar una lista de archivos afectados. Luego utilice la página Recuperación para cargar la lista y elegir qué archivos restaurar.

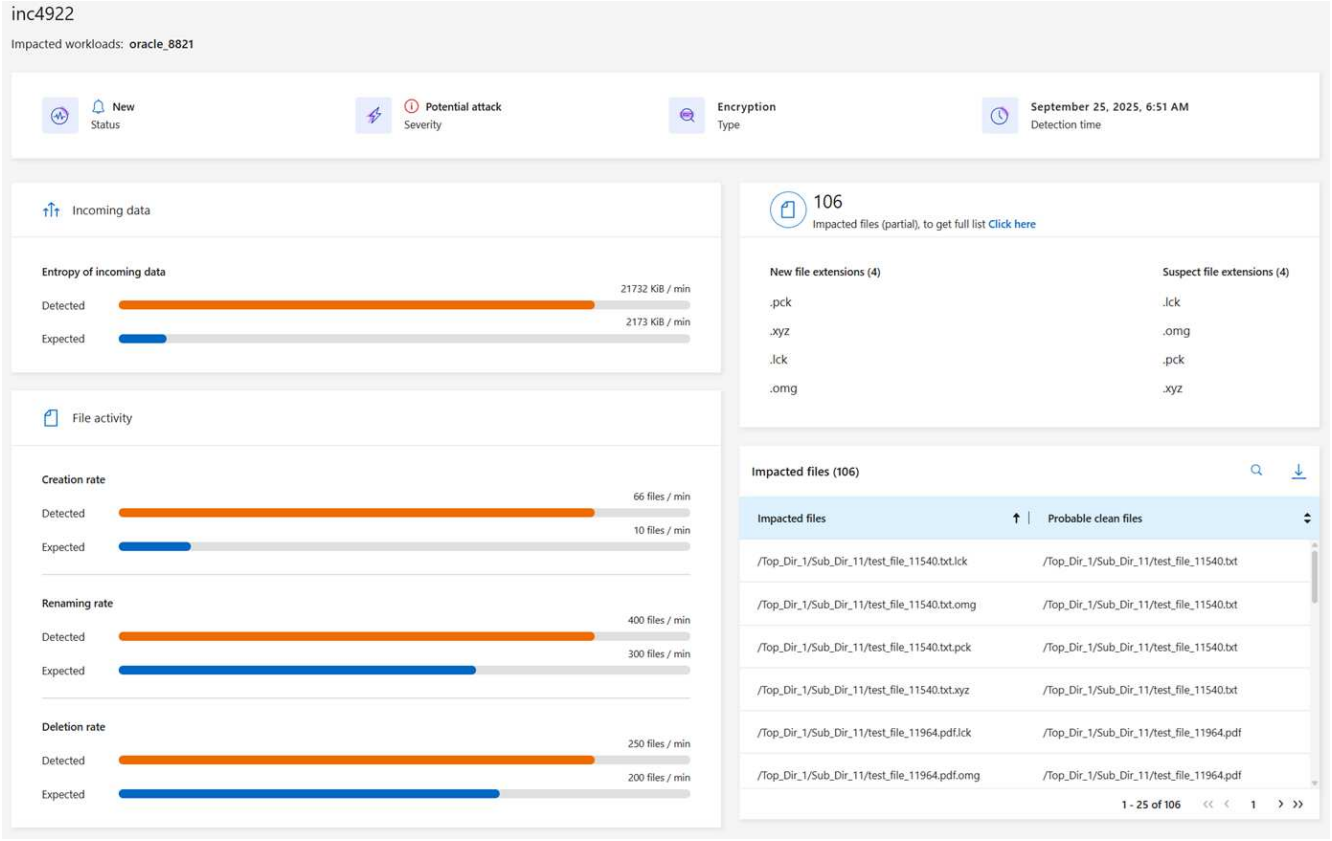
Puede restaurar una carga de trabajo de la aplicación a nivel de archivo en el mismo sistema o en uno diferente.

Pasos para obtener la lista de archivos afectados

Utilice la página Alertas para recuperar la lista de archivos afectados.

Si un volumen tiene varias alertas, deberá descargar la lista CSV de los archivos afectados para cada alerta.

1. En el menú Resiliencia ante ransomware, seleccione **Alertas**.
2. En la página Alertas, ordene los resultados por carga de trabajo para mostrar las alertas de la carga de trabajo de la aplicación que desea restaurar.
3. De la lista de alertas para esa carga de trabajo, seleccione una alerta.
4. Para esa alerta, seleccione un solo incidente.



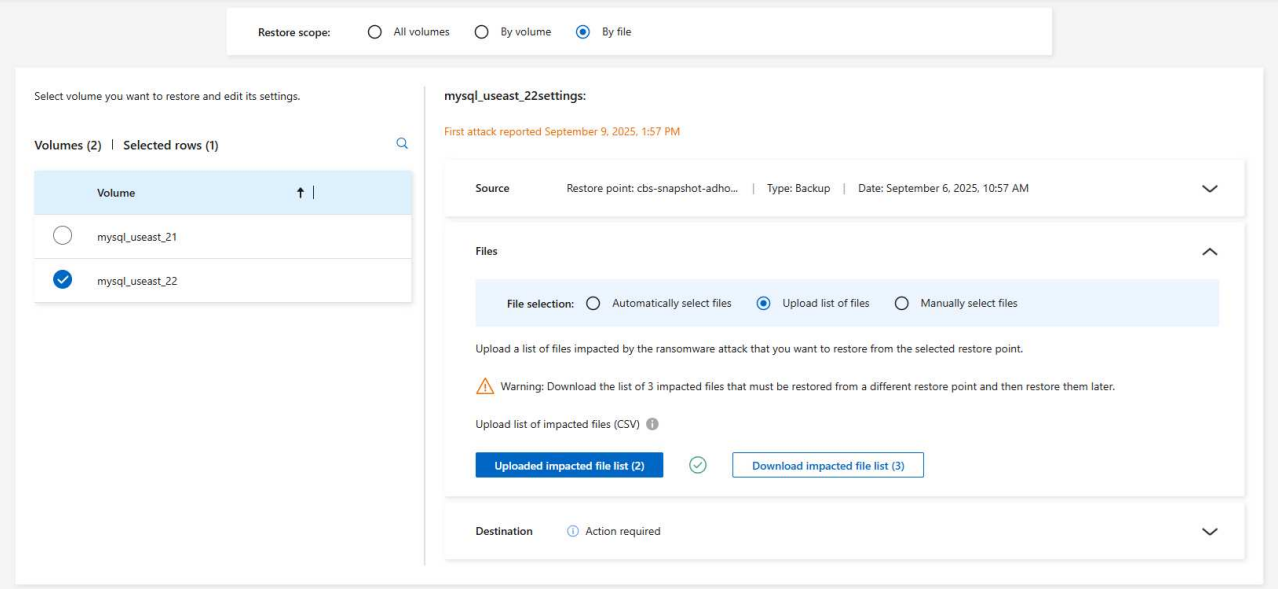
5. Para ver la lista completa de archivos, seleccione **Haga clic aquí** en la parte superior del panel Archivos afectados.
6. Para ese incidente, seleccione el ícono de descarga y descargue la lista de archivos afectados en formato CSV.

Pasos para restaurar esos archivos

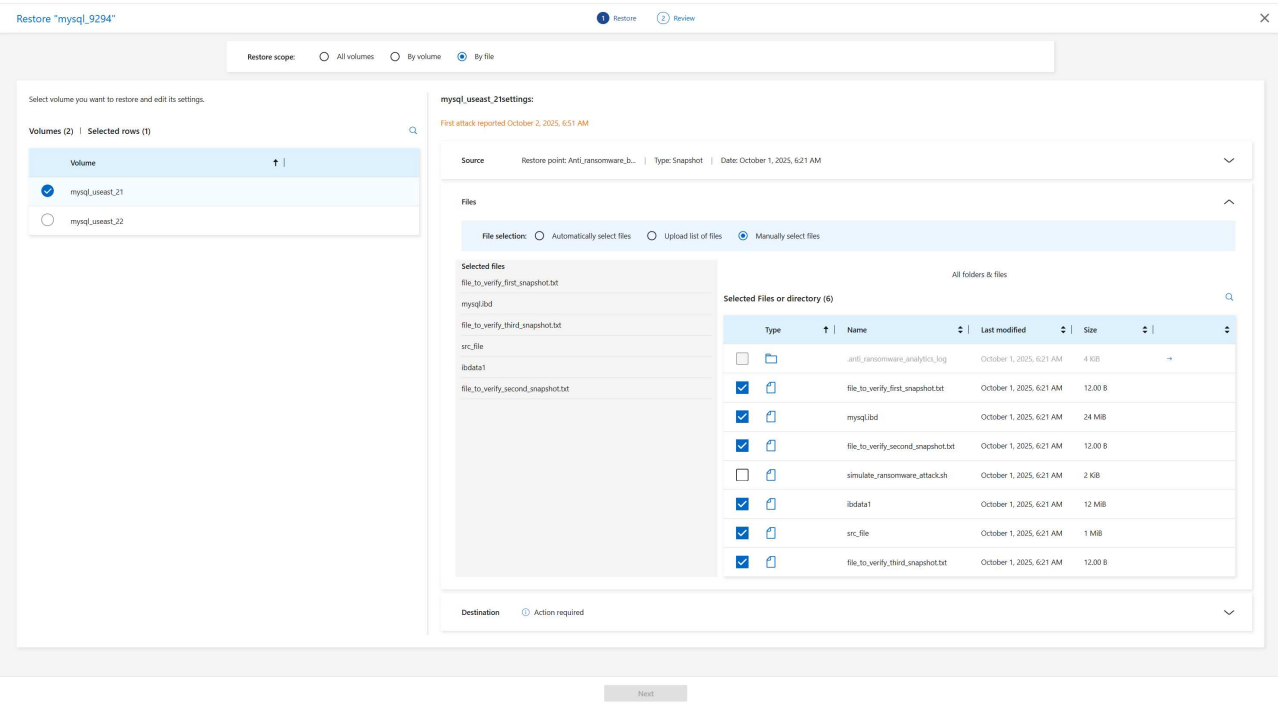
1. En el menú Resiliencia ante ransomware, seleccione **Recuperación**.
2. Seleccione una carga de trabajo de aplicación que esté en el estado "Se necesita restaurar".
3. Para restaurar, seleccione **Restaurar**.
4. En la página Restaurar, en el ámbito de restauración, seleccione **Por archivo**.
5. En la lista de volúmenes, seleccione el volumen que contiene los archivos que desea restaurar.
6. **Punto de restauración**: seleccione la flecha hacia abajo junto a **Punto de restauración** para ver los detalles. Seleccione el punto de restauración que desea utilizar para restaurar los datos.

> La columna Motivo en el panel Puntos de restauración muestra el motivo de la instantánea o copia de seguridad como "Programado" o "Respuesta automatizada al incidente de ransomware".

7. **Archivos**:
   - **Seleccionar archivos automáticamente**: permita que Ransomware Resilience seleccione los archivos que se restaurarán.
   - **Subir lista de archivos**: Sube un archivo CSV que contenga la lista de archivos afectados que obtuviste de la página de Alertas o que tienes. Puede restaurar hasta 10.000 archivos a la vez.



- **Seleccionar archivos manualmente**: seleccione hasta 10 000 archivos o una sola carpeta para restaurar.



> Si no se puede restaurar algún archivo utilizando el punto de restauración seleccionado, aparece un mensaje que indica la cantidad de archivos que no se pueden restaurar y le permite descargar la lista de esos archivos seleccionando **Descargar lista de archivos afectados**.

8. **Destino**: Seleccione la flecha hacia abajo junto a Destino para ver los detalles.
   a. Elija dónde restaurar los datos: la ubicación de origen original o una ubicación alternativa que pueda especificar.

Aunque los archivos o directorios originales se sobrescribirán con los datos restaurados, los nombres de archivos y carpetas originales permanecerán iguales a menos que especifique nombres nuevos.

b. Seleccione el sistema.

c. Seleccione la máquina virtual de almacenamiento.

d. Opcionalmente, introduzca la ruta.

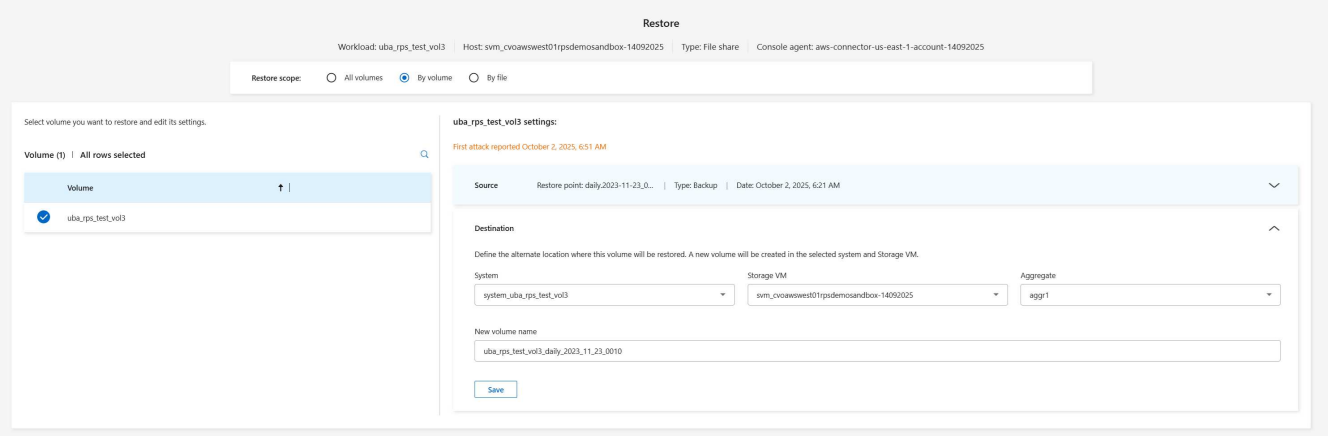
Si no especifica una ruta para la restauración, los archivos se restaurarán a un nuevo volumen en el directorio de nivel superior.

e. Seleccione si desea que los nombres de los archivos o directorios restaurados sean los mismos que los de la ubicación actual o nombres diferentes.

9. Seleccione **Siguiente**.
10. Revise sus selecciones.
11. Seleccione **Restaurar**.
12. Desde el menú superior, seleccione **Recuperación** para revisar la carga de trabajo en la página Recuperación, donde el estado de la operación se mueve a través de los estados.

Restaurar un recurso compartido de archivos o un almacén de datos

1. Después de seleccionar un recurso compartido de archivos o un almacén de datos para restaurar, en la página Restaurar, en el ámbito de restauración, seleccione **Por volumen**.



2. En la lista de volúmenes, seleccione el volumen que desea restaurar.
3. **Fuente**: Seleccione la flecha hacia abajo junto a Fuente para ver los detalles.
   a. Seleccione el punto de restauración que desea utilizar para restaurar los datos.

Ransomware Resilience identifica el mejor punto de restauración como la última copia de seguridad justo antes del incidente y muestra una indicación de "Recomendado".

4. **Destino**: Seleccione la flecha hacia abajo junto a Destino para ver los detalles.
   a. Elija dónde restaurar los datos: la ubicación de origen original o una ubicación alternativa que pueda especificar.

Aunque los archivos o directorios originales se sobrescribirán con los datos restaurados, los nombres de archivos y carpetas originales permanecerán iguales a menos que especifique nombres nuevos.

b. Seleccione el sistema.

c. Seleccione la máquina virtual de almacenamiento.

d. Opcionalmente, introduzca la ruta.

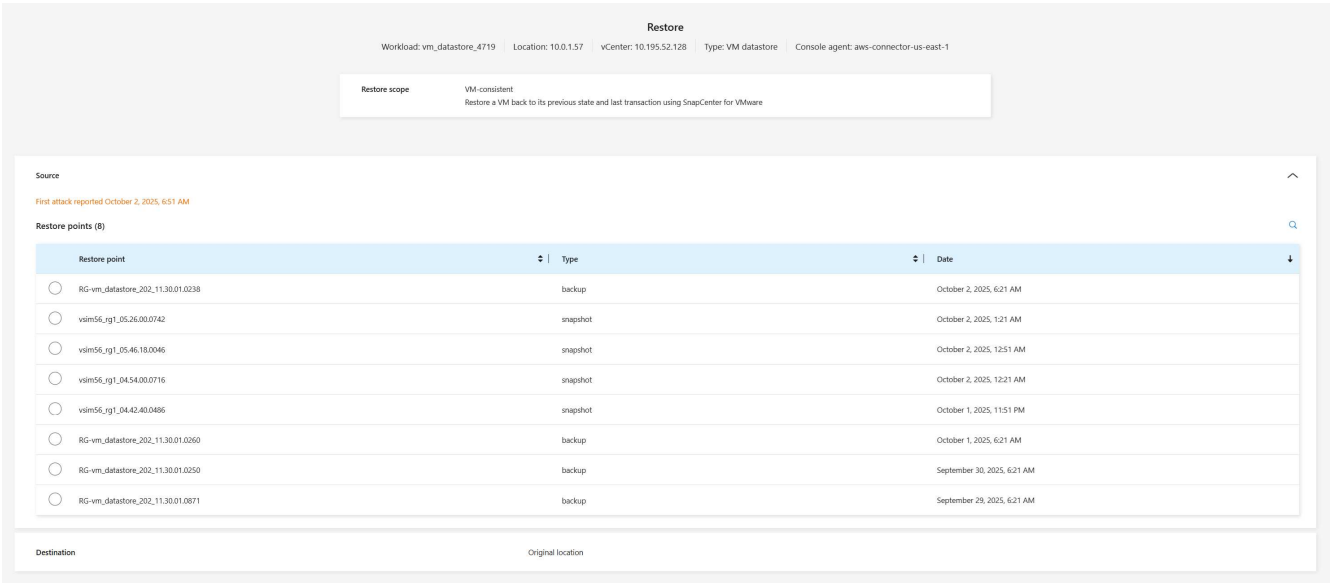
Si no especifica una ruta para la restauración, los archivos se restaurarán a un nuevo volumen en el directorio de nivel superior.

5. Seleccione **Guardar**.
6. Revise sus selecciones.
7. Seleccione **Restaurar**.
8. Desde el menú, seleccione **Recuperación** para revisar la carga de trabajo en la página Recuperación, donde el estado de la operación se mueve a través de los estados.

Restaurar un recurso compartido de archivos de VM en el nivel de VM

En la página Recuperación, después de seleccionar una máquina virtual para restaurar, continúe con estos pasos.

1. **Fuente**: Seleccione la flecha hacia abajo junto a Fuente para ver los detalles.



2. Seleccione el punto de restauración que desea utilizar para restaurar los datos.
3. **Destino**: A la ubicación original.
4. Seleccione **Siguiente**.
5. Revise sus selecciones.
6. Seleccione **Restaurar**.
7. Desde el menú, seleccione **Recuperación** para revisar la carga de trabajo en la página Recuperación, donde el estado de la operación se mueve a través de los estados.

Realice un simulacro de preparación para ataques de ransomware en NetApp Ransomware Resilience

Ejecute un simulacro de preparación para un ataque de ransomware simulando un ataque en una nueva carga de trabajo de muestra. Investigar el ataque simulado y recuperar la carga de trabajo. Utilice esta función para probar las notificaciones de alerta, la respuesta y la recuperación. Ejecute el ejercicio con tanta frecuencia como sea necesario.

Sus datos de carga de trabajo reales no se verán afectados.

Puede ejecutar simulacros de preparación en cargas de trabajo NFS y CIFS (SMB).

Configurar un simulacro de preparación para un ataque de ransomware

Antes de ejecutar una simulación, configure un ejercicio en la página Configuración. Acceda a la página de Configuración desde la opción Acciones en el menú superior.

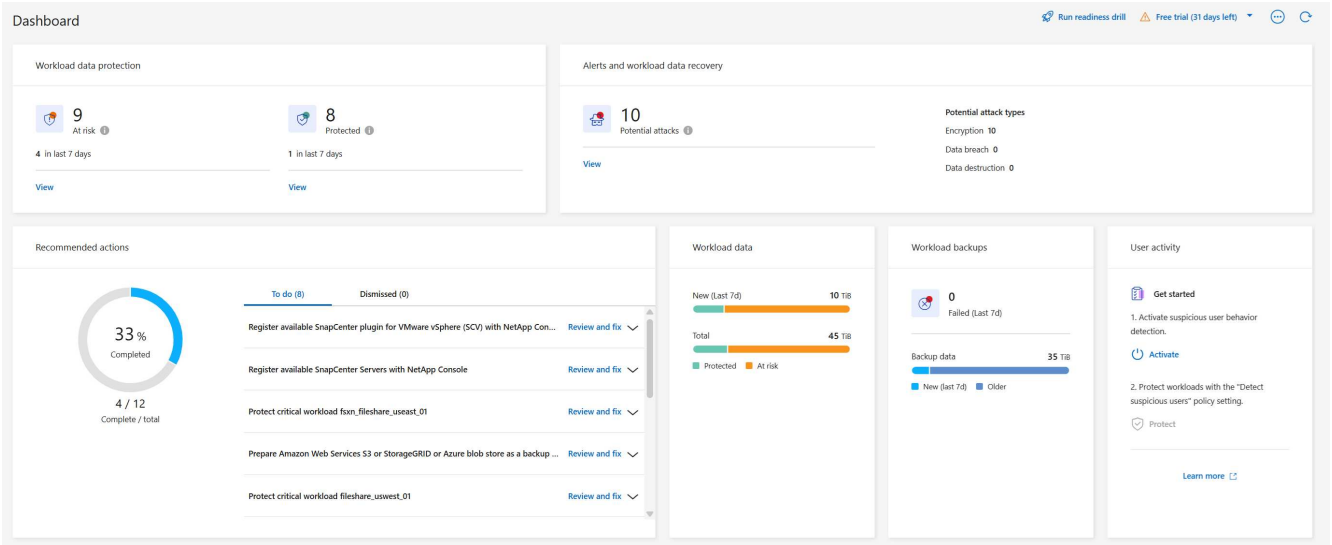
Debe ingresar un nombre de usuario y contraseña para las siguientes situaciones:

- Si se produjeron cambios en el nombre de usuario o la contraseña para la máquina virtual de almacenamiento seleccionada anteriormente
- Si selecciona una máquina virtual de almacenamiento CIFS (SMB) diferente
- Si ingresa un nombre de carga de trabajo de prueba diferente

Rol de consola requerido Para realizar esta tarea, necesita el rol de administrador de organización, administrador de carpeta o proyecto, o administrador de resiliencia ante ransomware. "Obtenga información sobre las funciones de resiliencia ante ransomware para la NetApp Console" .

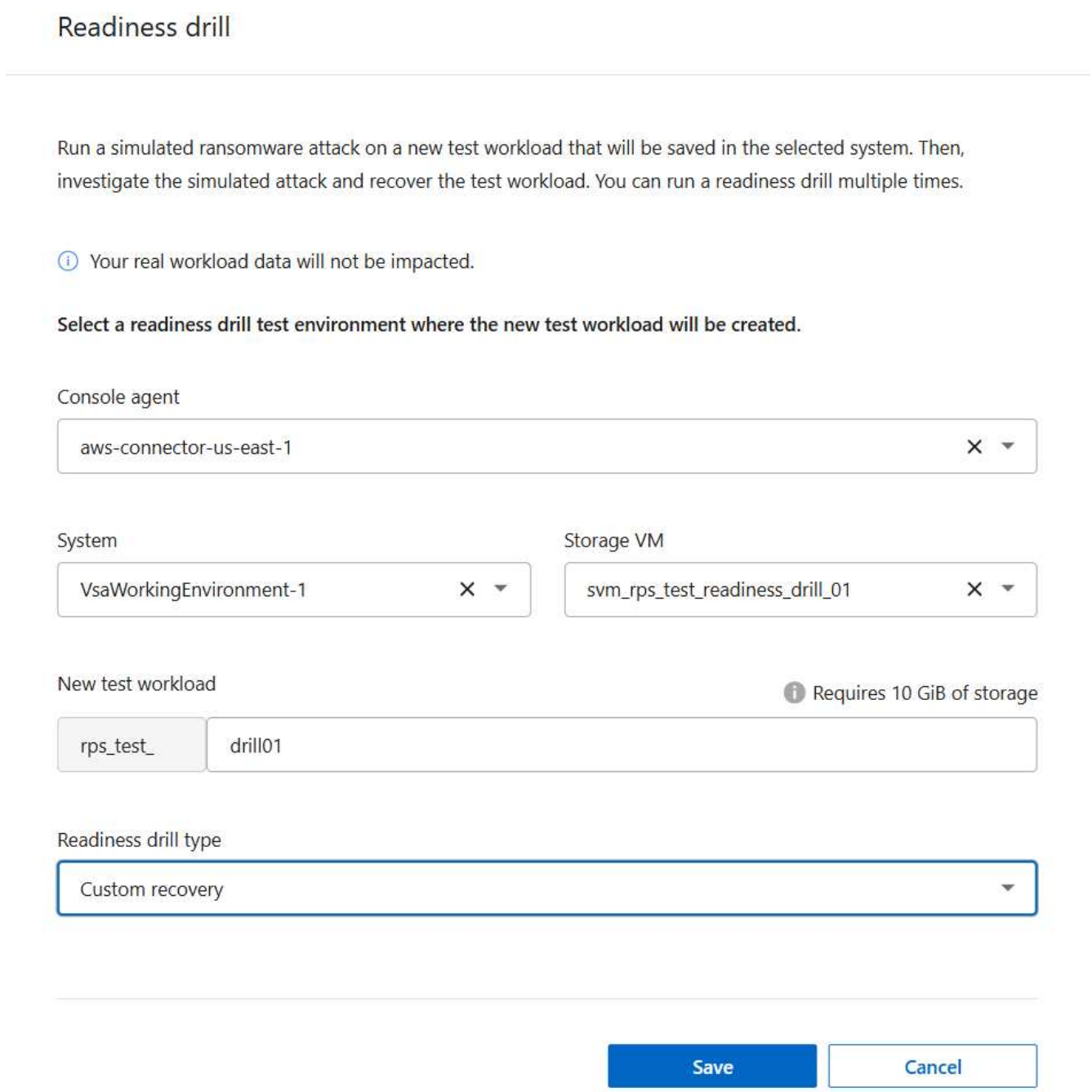
Pasos

1. Desde el menú NetApp Ransomware Resilience , seleccione el botón **Ejecutar simulacro de preparación** en la parte superior derecha.



2. En la tarjeta de simulacro de preparación de la página Configuración, seleccione **Configurar**.

La consola muestra la página Configurar simulacro de preparación.



3. Haga lo siguiente:
   a. Seleccione el agente de consola que desea utilizar para el simulacro de preparación.
   b. Seleccione un sistema de prueba.
   c. Seleccione un SVM de almacenamiento de prueba.
   d. Si seleccionó una máquina virtual de almacenamiento CIFS (SMB), aparecerán los campos **Nombre de usuario** y **Contraseña**. Introduzca el nombre de usuario y la contraseña para la máquina virtual de almacenamiento.
   e. Seleccione el tipo de simulacro de preparación. Para una recuperación manual de una violación de

datos de cifrado, elija **Recuperación personalizada**. Para recuperarse de una actividad de usuario sospechosa, elija **Violación de datos**.

f. Introduzca el nombre de una nueva carga de trabajo de prueba que se creará. No incluya guiones en el nombre.

4. Seleccione **Guardar**.

Puede editar la configuración del simulacro de preparación más tarde utilizando la página Configuración.

Iniciar un simulacro de preparación

Después de configurar el simulacro de preparación, puede iniciarlo.

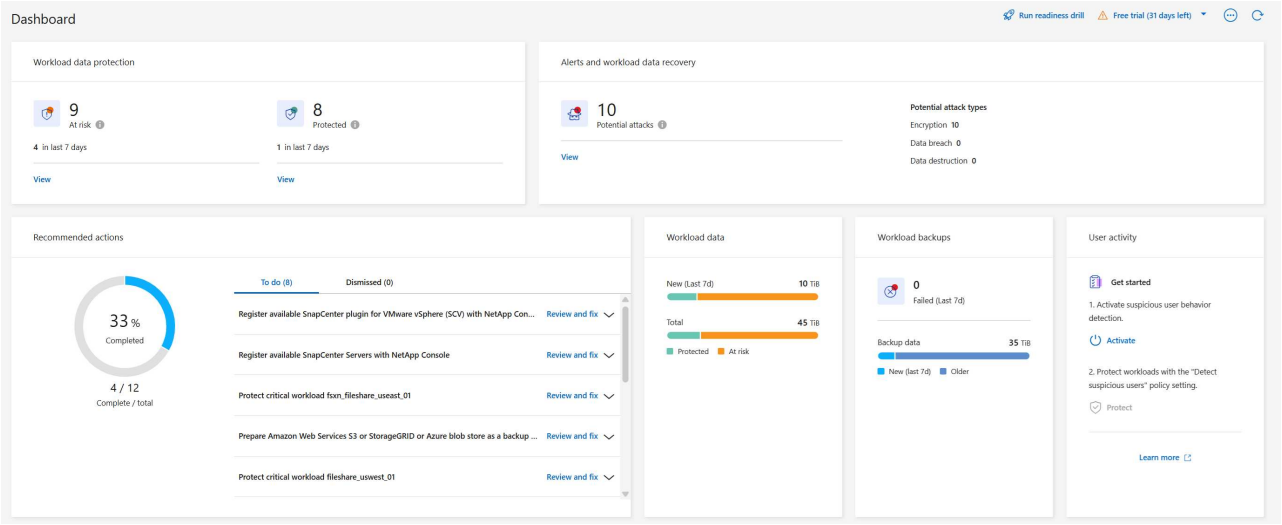
Rol de consola requerido Para realizar esta tarea, necesita el rol de administrador de organización, administrador de carpeta o proyecto, o administrador de resiliencia ante ransomware. "Obtenga información sobre las funciones de resiliencia ante ransomware para la NetApp Console" .

Cuando se inicia el simulacro de preparación, Ransomware Resilience omite el modo de aprendizaje y comienza el simulacro en modo activo. El estado de detección de la carga de trabajo es Activo.

Una carga de trabajo puede tener un estado de **Modo de aprendizaje** de detección de ransomware cuando se asigna recientemente una política de detección y Ransomware Resilience escanea las cargas de trabajo.

Pasos

1. Debe realizar una de las siguientes acciones:
   - Desde el menú Resiliencia ante ransomware, seleccione el botón **Ejecutar simulacro de preparación** en la parte superior derecha.



   - O bien, desde la página Configuración, en la tarjeta de simulacro de preparación, seleccione **Iniciar**.

No es posible editar la configuración del simulacro de preparación mientras el simulacro se está ejecutando. Puedes reiniciar el taladro para detenerlo y modificar la configuración.

Responder a una alerta de simulacro de preparación

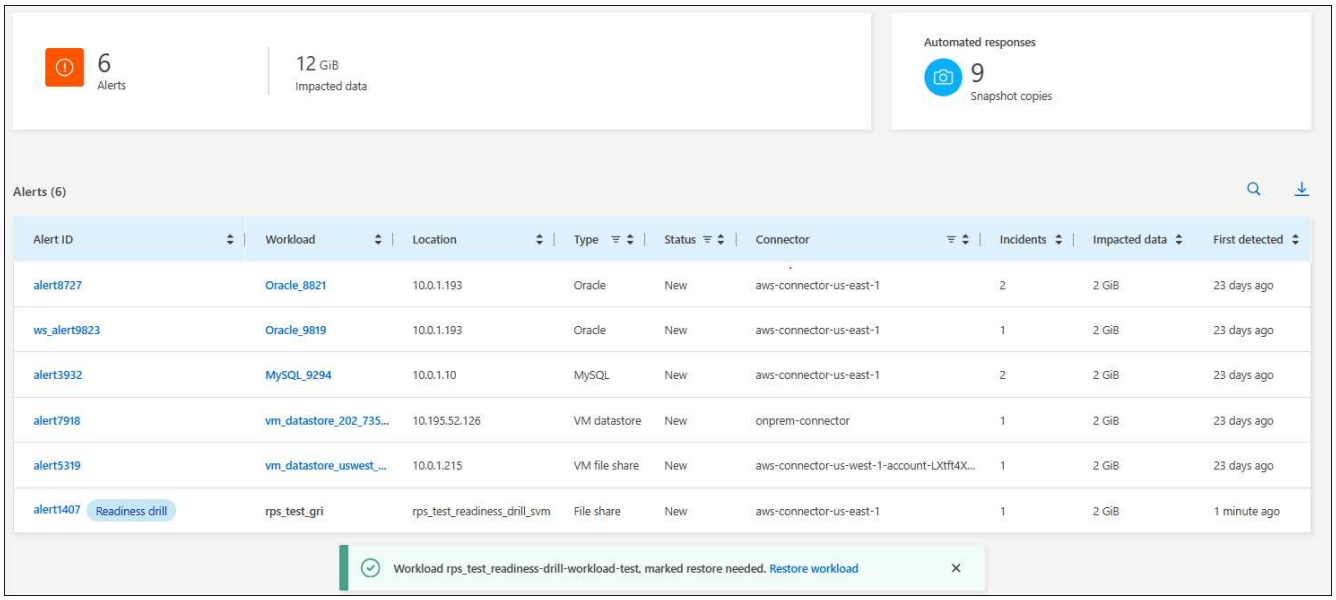
Pon a prueba tu preparación respondiendo a una alerta de simulacro de preparación.

Rol de consola requerido Para realizar esta tarea, necesita el rol de administrador de organización, administrador de carpeta o proyecto, o administrador de resiliencia ante ransomware. "Obtenga información sobre las funciones de resiliencia ante ransomware para la NetApp Console" .

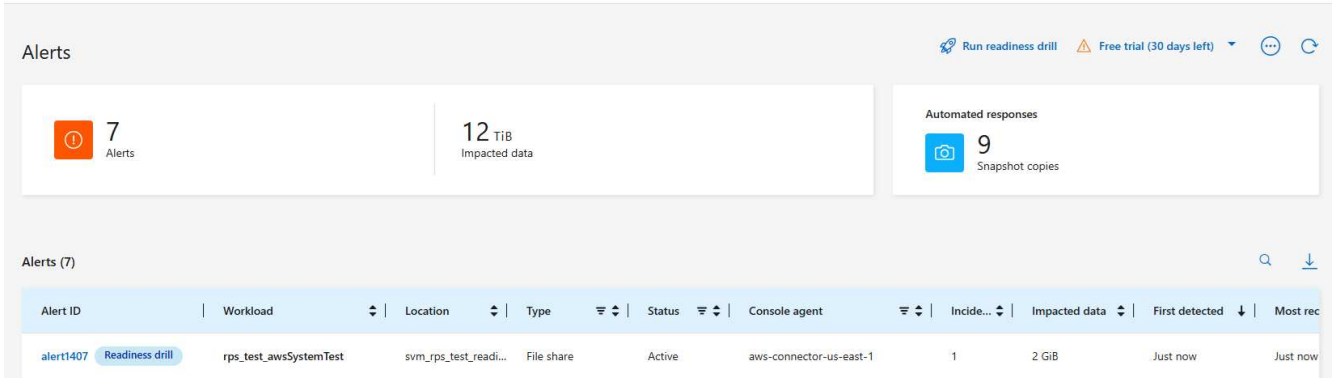
Pasos

1. En el menú Resiliencia ante ransomware, seleccione **Alertas**.

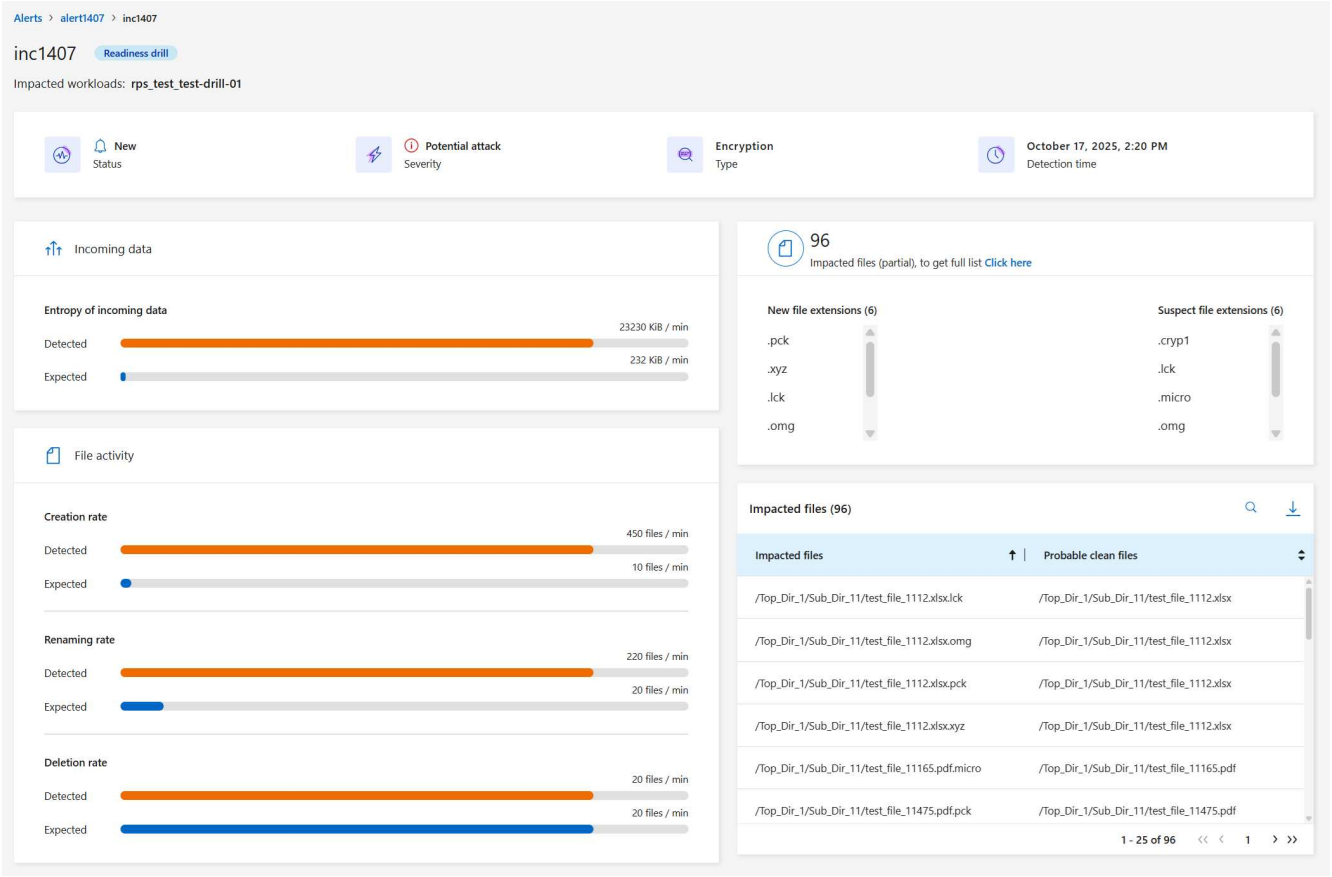
   La consola muestra la página Alertas. En la columna ID de alerta, verá "Simulacro de preparación" junto al ID.



2. Seleccione la alerta con la indicación "Simulacro de preparación". En la página de detalles de Alertas aparece una lista de alertas de incidentes.



3. Revisar los incidentes de alerta.
4. Seleccione un incidente de alerta.



Aquí hay algunas cosas que debes tener en cuenta:

- Observe la gravedad del ataque potencial.

  Si la gravedad indica que se sospecha que un usuario ha realizado una actividad maliciosa, revise el nombre del usuario. También puedes"bloquear al usuario."

- Observe la actividad del archivo y los procesos sospechosos:
  - Observe los datos detectados entrantes en comparación con los datos esperados.
  - Observe la tasa de creación de archivos que se detecta en comparación con la tasa esperada.
  - Observe la tasa de cambio de nombre de archivo que se detecta en comparación con la tasa esperada.
  - Observe la tasa de eliminación en comparación con la tasa esperada.
- Mire la lista de archivos afectados. Mira las extensiones que podrían estar causando el ataque.
- Determine el impacto y la amplitud del ataque revisando la cantidad de archivos y directorios afectados.

Restaurar la carga de trabajo de prueba

Después de revisar la alerta del simulacro de preparación, restaure la carga de trabajo de prueba si es necesario.

Rol de consola requerido Para realizar esta tarea, necesita el rol de administrador de organización, administrador de carpeta o proyecto, o administrador de resiliencia ante ransomware. "Obtenga información sobre las funciones de resiliencia ante ransomware para la NetApp Console" .

Pasos

1. Regresar a la página de detalles de alerta.
2. Si se debe restaurar la carga de trabajo de prueba, haga lo siguiente:
   - Seleccione **Marcar como necesario restaurar**.
   - Revise la confirmación y seleccione **Marcar como necesaria la restauración** en el cuadro de confirmación.
     - En el menú Resiliencia ante ransomware, seleccione **Recuperación**.
     - Seleccione la carga de trabajo de prueba marcada con "Simulacro de preparación" que desea restaurar.
     - Seleccione **Restaurar**.
     - En la página Restaurar, proporcione información para la restauración:
   - Seleccione la copia de la instantánea de origen.
   - Seleccione el volumen de destino.
3. En la página de revisión de restauración, seleccione **Restaurar**.

   La consola muestra el estado de la restauración del simulacro de preparación como "En progreso" en la página Recuperación.

   Una vez completada la restauración, la consola cambia el estado de la carga de trabajo a **Restaurada**.

4. Revise la carga de trabajo restaurada.

Para obtener detalles sobre el proceso de restauración, consulte"Recuperarse de un ataque de ransomware (después de neutralizar los incidentes)" .

Cambiar el estado de las alertas después del simulacro de preparación

Después de revisar la alerta del simulacro de preparación y restaurar la carga de trabajo, cambie el estado de la alerta si es necesario.

Se requiere el rol de consola Administrador de organización, administrador de carpeta o proyecto, o administrador de resiliencia ante ransomware. "Obtenga información sobre los roles de acceso a la consola para todos los servicios" .

Pasos

1. Regresar a la página de detalles de alerta.
2. Seleccione la alerta nuevamente.
3. Indique el estado seleccionando **Editar estado** y cambie el estado a uno de los siguientes:
   - Descartado: si sospecha que la actividad no es un ataque de ransomware, cambie el estado a Descartado.

Después de descartar un ataque, no puedes revertirlo. Si descarta una carga de trabajo, todas las copias instantáneas tomadas automáticamente en respuesta al posible ataque de ransomware se eliminarán de forma permanente. Si descarta la alerta, el simulacro de preparación se considerará completado.

   - Resuelto: El incidente ha sido mitigado.

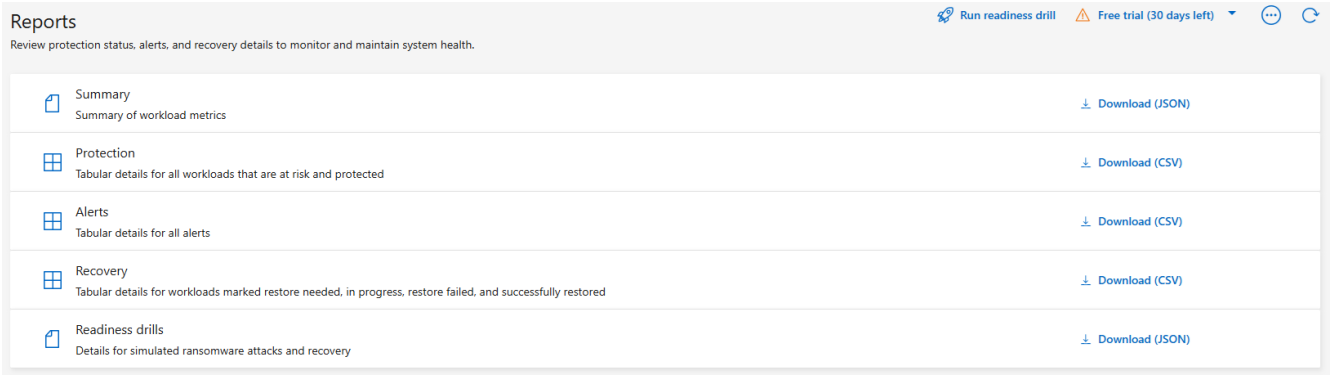
Revisar los informes sobre el simulacro de preparación

Una vez finalizado el simulacro de preparación, es posible que desees revisar y guardar un informe sobre el simulacro.

Rol de consola requerido Para realizar esta tarea, necesita el rol de administrador de la organización, administrador de carpeta o proyecto, administrador de resiliencia ante ransomware o visor de resiliencia ante ransomware. "Obtenga información sobre las funciones de resiliencia ante ransomware para la NetApp Console" .

Pasos

1. En el menú Resiliencia ante ransomware, seleccione **Informes**.



2. Seleccione **Simulacros de preparación** y **Descargar** para descargar el informe del simulacro de preparación.

Conecta NetApp Ransomware Resilience a un SIEM para el análisis y detección de amenazas

Un sistema de gestión de información y eventos de seguridad (SIEM) centraliza los datos de registros y eventos para proporcionar información sobre eventos de seguridad y cumplimiento. NetApp Ransomware Resilience admite enviar datos automáticamente a tu SIEM para agilizar el análisis y la detección de amenazas.

Ransomware Resilience es compatible con los siguientes SIEMs:

- AWS Security Hub
- Microsoft Sentinel
- Splunk Cloud

Antes de habilitar SIEM en Ransomware Resilience, debe configurar su sistema SIEM.

NetApp Ransomware Resilience también es compatible con "libros de jugadas de orquestación, automatización y respuesta (SOAR) de seguridad".

Datos de eventos enviados a un SIEM

Ransomware Resilience puede enviar los siguientes datos de eventos a su sistema SIEM:

- **contexto**:
  - **os**: Esta es una constante con el valor de ONTAP.
  - **os_version**: La versión de ONTAP que se ejecuta en el sistema.
  - **connector_id**: El ID del agente de consola que administra el sistema.
  - **cluster_id**: El ID de clúster informado por ONTAP para el sistema.
  - **svm_name**: El nombre de la SVM donde se encontró la alerta.
  - **volume_name**: el nombre del volumen en el que se encuentra la alerta.
  - **volume_id**: El ID del volumen informado por ONTAP para el sistema.
- **incidente**:
  - **incident_id**: El ID del incidente generado por Ransomware Resilience para el volumen atacado en Ransomware Resilience.
  - **alert_id**: El ID generado por Ransomware Resilience para la carga de trabajo.
  - **gravedad**: Uno de los siguientes niveles de alerta: "CRÍTICO", "ALTO", "MEDIO", "BAJO".
  - **descripción**: Detalles sobre la alerta detectada, por ejemplo, "Se detectó un posible ataque de ransomware en la carga de trabajo arp_learning_mode_test_2630".

Configurar AWS Security Hub para la detección de amenazas

Antes de habilitar AWS Security Hub en Ransomware Resilience, tienes que hacer los siguientes pasos de alto nivel en AWS Security Hub:

- Configurar permisos en AWS Security Hub.
- Configure la clave de acceso de autenticación y la clave secreta en AWS Security Hub. (Estos pasos no se proporcionan aquí.)

Pasos para configurar permisos en AWS Security Hub

1. Vaya a la **consola AWS IAM**.
2. Seleccione **Políticas**.
3. Cree una política utilizando el siguiente código en formato JSON:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "NetAppSecurityHubFindings",
      "Effect": "Allow",
      "Action": [
        "securityhub:BatchImportFindings",
        "securityhub:BatchUpdateFindings"
      ],
      "Resource": [
        "arn:aws:securityhub:*:*:product/*/default",
        "arn:aws:securityhub:*:*:hub/default"
      ]
    }
  ]
}
```

Configurar Microsoft Sentinel para la detección de amenazas

Antes de activar Microsoft Sentinel en Ransomware Resilience, tienes que hacer los siguientes pasos a grandes rasgos en Microsoft Sentinel:

- **Prerrequisitos**
  - Habilitar Microsoft Sentinel.
  - Crear un rol personalizado en Microsoft Sentinel.
- **Registro**
  - Registre Ransomware Resilience para recibir eventos de Microsoft Sentinel.
  - Crear un secreto para el registro.
- **Permisos**: Asigna permisos a la aplicación.
- **Autenticación**: Ingrese las credenciales de autenticación para la aplicación.

Pasos para habilitar Microsoft Sentinel

1. Vaya a Microsoft Sentinel.
2. Cree un **espacio de trabajo de Log Analytics**.
3. Habilite Microsoft Sentinel para utilizar el espacio de trabajo de Log Analytics que acaba de crear.

Pasos para crear un rol personalizado en Microsoft Sentinel

1. Vaya a Microsoft Sentinel.
2. Seleccione **Suscripción** > **Control de acceso (IAM)**.
3. Introduzca un nombre de rol personalizado. Utilice el nombre **Ransomware Resilience Sentinel Configurator**.
4. Copie el siguiente JSON y péguelo en la pestaña **JSON**.

```
{
  "roleName": "Ransomware Resilience Sentinel Configurator",
  "description": "",
  "assignableScopes":["/subscriptions/{subscription_id}"],
  "permissions": [

  ]
}
```

5. Revise y guarde su configuración.

Pasos para registrar Ransomware Resilience para recibir eventos de Microsoft Sentinel

1. Vaya a Microsoft Sentinel.
2. Seleccione **ID de entrada** > **Aplicaciones** > **Registros de aplicaciones**.
3. Para el **Nombre para mostrar** de la aplicación, ingrese "**Ransomware Resilience**".
4. En el campo **Tipo de cuenta compatible**, seleccione **Solo cuentas en este directorio organizacional**.
5. Seleccione un **Índice predeterminado** donde se enviarán los eventos.
6. Seleccione **Revisar**.
7. Seleccione **Registrarse** para guardar su configuración.

   Después del registro, el centro de administración de Microsoft Entra muestra el panel Descripción general de la aplicación.

Pasos para crear un secreto para el registro

1. Vaya a Microsoft Sentinel.
2. Seleccione **Certificados y secretos** > **Secretos de cliente** > **Nuevo secreto de cliente**.
3. Agregue una descripción para el secreto de su aplicación.
4. Seleccione una **Expiración** para el secreto o especifique un período de vida personalizado.

   La vida útil del secreto de un cliente está limitada a dos años (24 meses) o menos. Microsoft recomienda que establezca un valor de expiración inferior a 12 meses.

5. Seleccione **Agregar** para crear su secreto.
6. Registre el secreto que se utilizará en el paso de Autenticación. El secreto nunca volverá a mostrarse después de salir de esta página.

Pasos para asignar permisos a la aplicación

1. Vaya a Microsoft Sentinel.
2. Seleccione **Suscripción** > **Control de acceso (IAM)**.
3. Seleccione **Agregar** > **Agregar asignación de rol**.
4. Para el campo **Roles de administrador privilegiado**, seleccione **Configurador de Ransomware Resilience Sentinel**.

Éste es el rol personalizado que creaste anteriormente.

5. Seleccione **Siguiente**.
6. En el campo **Asignar acceso a**, seleccione **Usuario, grupo o entidad de servicio**.
7. Seleccione **Seleccionar miembros**. Luego, seleccione **Ransomware Resilience Sentinel Configurator**.
8. Seleccione **Siguiente**.
9. En el campo **Qué puede hacer el usuario**, seleccione **Permitir al usuario asignar todos los roles excepto los roles de administrador privilegiado Propietario, UAA, RBAC (recomendado)**.
10. Seleccione **Siguiente**.
11. Seleccione **Revisar y asignar** para asignar los permisos.

Pasos para ingresar credenciales de autenticación para la aplicación

1. Vaya a Microsoft Sentinel.
2. Introduzca las credenciales:
   a. Ingrese el ID del inquilino, el ID de la aplicación del cliente y el secreto de la aplicación del cliente.
   b. Selecciona **Autenticar**.

   Una vez que la autenticación es exitosa, aparece un mensaje de "Autenticado".
3. Ingrese los detalles del espacio de trabajo de Log Analytics para la aplicación.
   a. Seleccione el ID de suscripción, el grupo de recursos y el espacio de trabajo de Log Analytics.

Configurar Splunk Cloud para la detección de amenazas

Antes de habilitar Splunk Cloud en Ransomware Resilience, deberá realizar los siguientes pasos de alto nivel en Splunk Cloud:

- Habilite un recopilador de eventos HTTP en Splunk Cloud para recibir datos de eventos a través de HTTP o HTTPS desde la consola.
- Cree un token de recopilador de eventos en Splunk Cloud.

Pasos para habilitar un recopilador de eventos HTTP en Splunk

1. Vaya a Splunk Cloud.
2. Seleccione **Configuración** > **Entradas de datos**.
3. Seleccione **Recopilador de eventos HTTP** > **Configuración global**.
4. En el interruptor Todos los tokens, seleccione **Habilitado**.
5. Para que el Recopilador de eventos escuche y se comunique a través de HTTPS en lugar de HTTP, seleccione **Habilitar SSL**.
6. Introduzca un puerto en **Número de puerto HTTP** para el recopilador de eventos HTTP.

Pasos para crear un token de recopilador de eventos en Splunk

1. Vaya a Splunk Cloud.
2. Seleccione **Configuración** > **Agregar datos**.
3. Seleccione **Monitor** > **Recopilador de eventos HTTP**.

4. Ingrese un nombre para el token y seleccione **Siguiente**.
5. Seleccione un **Índice predeterminado** donde se enviarán los eventos y luego seleccione **Revisar**.
6. Confirme que todas las configuraciones del punto final sean correctas y luego seleccione **Enviar**.
7. Copie el token y péguelo en otro documento para tenerlo listo para el paso de autenticación.

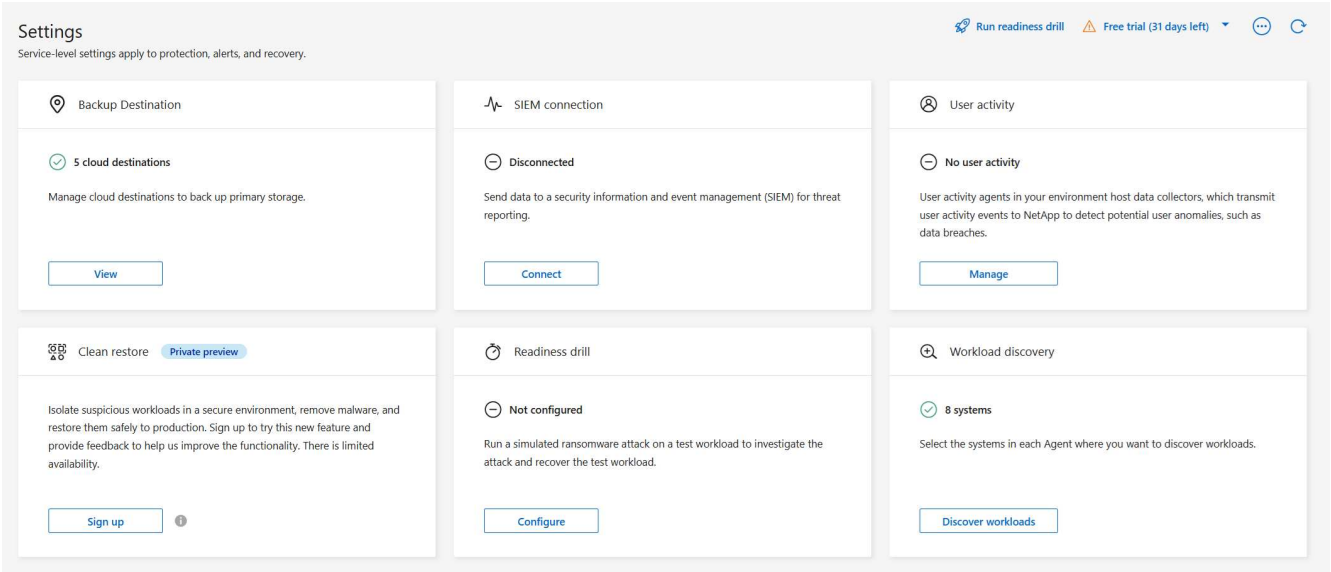
Conecte SIEM en la resiliencia contra el ransomware

Al habilitar SIEM se envían datos de Ransomware Resilience a su servidor SIEM para análisis e informes de amenazas.

Pasos

1. Desde el menú Consola, seleccione **Protección** > **Resiliencia ante ransomware**.
2. En el menú Resiliencia contra ransomware, seleccione la vertical …opción en la parte superior derecha.
3. Seleccione **Configuración**.

   Aparece la página de Configuración.



4. En la página Configuración, seleccione **Conectar** en el mosaico de conexión SIEM.

5. Elija uno de los sistemas SIEM.
6. Ingrese el token y los detalles de autenticación que configuró en AWS Security Hub o Splunk Cloud.

   La información que ingrese dependerá del SIEM que haya seleccionado.

7. Seleccione **Habilitar**.

   La página de Configuración muestra "Conectado".

Próximos pasos

- "Integra un playbook SOAR"

Integra un playbook SOAR para NetApp Ransomware Resilience

NetApp Ransomware Resilience ofrece playbooks de orquestación, automatización y respuesta de seguridad (SOAR) que te permiten automatizar tareas como la respuesta ante amenazas.

Los playbooks de Ransomware Resilience ofrecen las siguientes capacidades:

- Crear una instantánea de un volumen
- Enriquece una dirección IP con información sobre amenazas
- Enriquecer la información de almacenamiento para un agente y un sistema determinados
- Desconecta un volumen para responder a incidentes
- Probar conectividad
- Revisa el estado de un trabajo de enriquecimiento

Playbooks

Ransomware Resilience ofrece guías para Microsoft Sentinel y Splunk. Revisa las páginas respectivas de

GitHub para detalles sobre la configuración.

- "Microsoft Sentinel"
- "Splunk"

Para Splunk Cloud, debes estar usando la versión 7.0, 7.1, 7.2, 8.0 o 8.4 de la plataforma. Para más información, mira "Splunkbase".

Más información

- "Conecta NetApp Ransomware Resilience a un SIEM para el análisis y detección de amenazas"

Descargar informes de NetApp Ransomware Resilience

NetApp Ransomware Resilience proporciona informes en formatos CSV y JSON que muestran detalles de volúmenes admitidos y no admitidos, simulacros de preparación para ataques, protección, alertas y recuperación. Con los informes, puedes guardar y revisar informes sin conexión sobre simulacros, postura de protección, alertas y eventos de recuperación.

Antes de descargar los archivos, actualice el panel para capturar los datos más recientes en sus informes.

Rol de consola requerido Para realizar esta tarea, necesita el rol de administrador de la organización, administrador de carpeta o proyecto, administrador de resiliencia ante ransomware o visor de resiliencia ante ransomware. "Obtenga información sobre las funciones de resiliencia ante ransomware para la NetApp Console" .

¿Qué datos puedes descargar? Puedes descargar archivos desde cualquiera de las opciones del menú principal:

- **Resumen**: Incluye listas de cargas de trabajo admitidas y no admitidas, acciones recomendadas para mejorar su postura de resiliencia cibernética e información capturada en el panel de resiliencia ante ransomware.
- **Protección**: Incluye el estado y los detalles de todas las cargas de trabajo, incluido el número total de cargas protegidas y en riesgo.
- **Alertas**: Incluye el estado y los detalles de todas las alertas, incluido el número total de alertas e instantáneas automatizadas.
- **Recuperación**: incluye el estado y los detalles de todas las cargas de trabajo que necesitan restaurarse, incluido el número total de cargas de trabajo marcadas como "Restauración necesaria", "En progreso", "Restauración fallida" y "Restaurada exitosamente".
- **Informes**: Puedes exportar datos de cualquiera de las páginas y descargar los archivos.

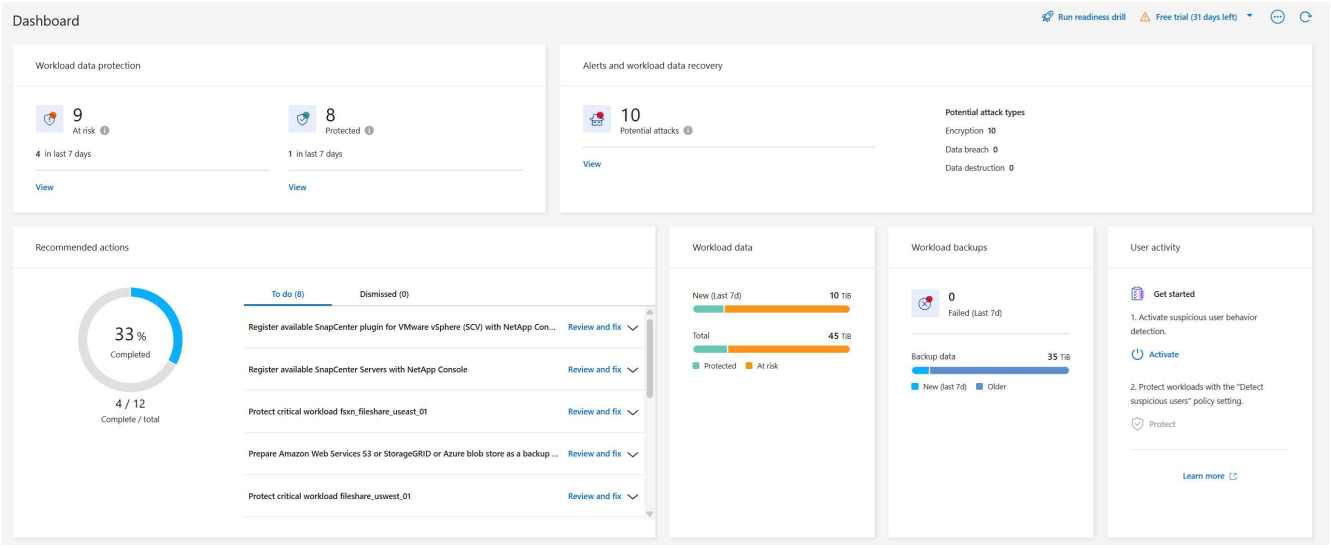
  Puede descargar informes de simulacros de preparación únicamente desde la página **Informes**.

Si descarga archivos CSV o JSON desde la página Protección, Alertas o Recuperación, los datos muestran solo los datos de esa página.

Los archivos CSV o JSON incluyen datos de todas las cargas de trabajo en todos los sistemas de consola.

Pasos

1. Desde la navegación izquierda de la Consola, seleccione **Protección** > **Resiliencia ante ransomware**.



2. Desde el cuadro de mandos u otra página, selecciona la opción **Refrescar** en la parte superior derecha para actualizar los datos que aparecerán en los informes.
3. Debe realizar una de las siguientes acciones:
   - Desde la página, seleccione *Descargar* opción.
   - En el menú NetApp Ransomware Resilience , seleccione **Informes**.
4. Si seleccionó la opción **Informes**, seleccione uno de los nombres de archivo preconfigurados y seleccione **Descargar**.