Documentación de NetApp Ransomware Resilience

NetApp Ransomware Resilience

NetApp
December 09, 2025

Tabla de contenidos

Documentación de NetApp Ransomware Resilience

Notas de la versión

Novedades en NetApp Ransomware Resilience

Descubra las novedades en NetApp Ransomware Resilience.

08 de diciembre de 2025

El bloqueo de extensiones está habilitado a nivel de carga de trabajo

Cuando habilita el bloqueo de extensiones, ahora se habilita en el nivel de carga de trabajo en lugar de en el nivel de máquina virtual de almacenamiento.

Editar el estado de alerta de comportamiento del usuario

Ransomware Resilience ahora le permite editar el estado de las alertas de comportamiento del usuario. Puede descartar y resolver alertas manualmente.

Para obtener más información, consulte "Administrar alertas en Ransomware Resilience".

Compatibilidad con múltiples agentes de consola

Ransomware Resilience ahora admite el uso de múltiples agentes de consola para administrar los mismos sistemas.

Para obtener más información sobre los agentes de consola, consulte"Crear un agente de consola" .

10 de noviembre de 2025

Esta versión incluye mejoras generales.

6 de octubre de 2025

La BlueXP ransomware protection ahora es NetApp Ransomware Resilience

El servicio de BlueXP ransomware protection ha pasado a llamarse NetApp Ransomware Resilience.

BlueXP ahora es NetApp Console

La NetApp Console proporciona una gestión centralizada de servicios de almacenamiento y datos en entornos locales y en la nube a nivel empresarial, brindando información en tiempo real, flujos de trabajo más rápidos y una administración simplificada.

Para obtener más detalles sobre lo que ha cambiado, consulte la "Notas de la versión de la NetApp Console" .

Detección de violaciones de datos

Ransomware Resilience incluye un nuevo mecanismo de detección que se puede activar en unos pocos pasos para detectar lecturas anómalas del usuario como un indicador temprano de violación de datos. La resiliencia ante ransomware recopila y analiza eventos de lectura del usuario mediante la creación de una línea de base histórica, que es un perfil del comportamiento normal esperado a partir de datos pasados. Cuando la actividad de un nuevo usuario se desvía significativamente de esta norma establecida (por ejemplo,

un aumento inesperado de lectura combinado con patrones de lectura sospechosos), se genera una alerta. Ransomware Resilience incluye un modelo de IA para detectar patrones de lectura sospechosos.

A diferencia de la detección de cifrado por ARP en la capa de almacenamiento, la detección de la anomalía en el comportamiento del usuario se realiza en el servicio Ransomware Resilience SaaS mediante la recopilación de eventos FPolicy.

> Debes utilizar el nuevo"Administrador del comportamiento del usuario de Ransomware Resilience y visor del comportamiento del usuario de Ransomware Resilience" Roles para acceder a configuraciones de detección de comportamiento sospechoso de usuarios.

Para obtener más información, consulte"Habilitar la detección de actividad sospechosa de usuarios" y"Ver comportamiento anómalo del usuario" .

Detecciones adicionales de actividad sospechosa del usuario

Además de la detección de violaciones de datos, Ransomware Resilience también detecta los siguientes tipos de alertas según la actividad sospechosa del usuario observada:

- **Destrucción de datos - ataque potencial** - Se crea una alerta con la gravedad del ataque potencial cuando la cantidad de eliminaciones de archivos excede la norma histórica.
- **Comportamiento sospechoso del usuario - posible ataque**: se crea una alerta con la gravedad del posible ataque cuando se observan operaciones de lectura, cambio de nombre y eliminación en una secuencia similar a un ataque de ransomware.
- **Comportamiento sospechoso del usuario - Advertencia** - Se crea una alerta con la gravedad de advertencia cuando el número total de actividades de archivo (lectura, eliminación, cambio de nombre, etc.) excede la norma histórica.

Nuevos roles de usuario para la detección de violaciones de datos

Para administrar las alertas de actividad sospechosa de los usuarios, Ransomware Resilience ha introducido dos nuevos roles para que los administradores de la organización de la consola otorguen acceso a la detección de actividad sospechosa de los usuarios: administrador de comportamiento de usuarios de Ransomware Resilience y visor de comportamiento de usuarios de Ransomware Resilience.

Debe ser un administrador de comportamiento de usuario para configurar las opciones de comportamiento de usuario sospechoso. El rol de administrador de Ransomware Resilience no es compatible con la configuración de ajustes de comportamiento de usuarios sospechosos.

Para obtener más información, consulte "Acceso basado en roles de NetApp Ransomware Resilience" .

12 de agosto de 2025

Esta versión incluye mejoras generales.

15 de julio de 2025

Soporte de carga de trabajo SAN

Esta versión incluye soporte para cargas de trabajo SAN en la BlueXP ransomware protection. Ahora puede proteger cargas de trabajo SAN además de cargas de trabajo NFS y CIFS.

Para obtener más información, consulte "Requisitos previos para la BlueXP ransomware protection" .

Protección mejorada de la carga de trabajo

Esta versión mejora el proceso de configuración para cargas de trabajo con políticas de instantáneas y respaldo de otras herramientas de NetApp , como SnapCenter o BlueXP backup and recovery. En versiones anteriores, la BlueXP ransomware protection descubría las políticas de otras herramientas y solo le permitía cambiar la política de detección. Con esta versión, ahora puede reemplazar las políticas de instantáneas y copias de seguridad con las políticas de BlueXP ransomware protection o continuar usando las políticas de otras herramientas.

Para más detalles, consulte"Proteger las cargas de trabajo" .

Notificaciones por correo electrónico

Si la BlueXP ransomware protection detecta un posible ataque, aparece una notificación en Notificaciones de BlueXP y se envía un correo electrónico a la dirección de correo electrónico que usted configuró.

El correo electrónico incluye información sobre la gravedad, la carga de trabajo afectada y un enlace a la alerta en la pestaña **Alertas** de BlueXP ransomware protection .

Si configuró un sistema de gestión de eventos y seguridad (SIEM) en la BlueXP ransomware protection, el servicio envía detalles de alerta a su sistema SIEM.

Para más detalles, consulte"Gestionar alertas de ransomware detectadas" .

9 de junio de 2025

Actualizaciones de la página de destino

Esta versión incluye actualizaciones a la página de inicio de BlueXP ransomware protection que facilitan el inicio de la prueba gratuita y el descubrimiento.

Actualizaciones de simulacros de preparación

Anteriormente, se podía ejecutar un simulacro de preparación ante ransomware simulando un ataque en una nueva carga de trabajo de muestra. Con esta función, puede 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 y programe estos simulacros con tanta frecuencia como sea necesario.

Con esta versión, puede usar un nuevo botón en el Panel de BlueXP ransomware protection para ejecutar un simulacro de preparación para ransomware en una carga de trabajo de prueba, lo que le facilita simular ataques de ransomware, investigar su impacto y recuperar cargas de trabajo de manera eficiente, todo dentro de un entorno controlado.

Ahora puede ejecutar simulacros de preparación en cargas de trabajo CIFS (SMB) además de en cargas de trabajo NFS.

Para más detalles, consulte "Realizar un simulacro de preparación para un ataque de ransomware" .

Habilitar actualizaciones de BlueXP classification

Antes de utilizar la BlueXP classification dentro del servicio de BlueXP ransomware protection , debe habilitar la BlueXP classification para escanear sus datos. La clasificación de datos le ayuda a encontrar información de identificación personal (PII), lo que puede aumentar los riesgos de seguridad.

Puede implementar la BlueXP classification en una carga de trabajo de uso compartido de archivos desde la

BlueXP ransomware protection. En la columna **Exposición de privacidad**, seleccione la opción **Identificar exposición**. Si ha habilitado el servicio de clasificación, esta acción identifica la exposición. De lo contrario, con esta versión, un cuadro de diálogo presenta la opción de implementar la BlueXP classification. Seleccione **Implementar** para ir a la página de inicio del servicio de BlueXP classification , donde puede implementar ese servicio. O

Para más detalles, consulte "Implementar la BlueXP classification en la nube" y para utilizar el servicio dentro de la BlueXP ransomware protection, consulte "Escanee en busca de información de identificación personal con la BlueXP classification" .

13 de mayo de 2025

Informes de entornos de trabajo no compatibles con la BlueXP ransomware protection

Durante el flujo de trabajo de descubrimiento, la BlueXP ransomware protection informa más detalles cuando pasa el cursor sobre Cargas de trabajo compatibles o No compatibles. Esto le ayudará a comprender por qué el servicio de BlueXP ransomware protection no detecta algunas de sus cargas de trabajo.

Hay muchas razones por las cuales el servicio no admite un entorno de trabajo, por ejemplo, la versión de ONTAP en su entorno de trabajo podría ser inferior a la versión requerida. Cuando pasa el cursor sobre un entorno de trabajo no compatible, aparece una información sobre herramientas que muestra el motivo.

Puede ver los entornos de trabajo no compatibles durante el descubrimiento inicial, donde también puede descargar los resultados. También puede ver los resultados del descubrimiento desde la opción **Descubrimiento de carga de trabajo** en la página Configuración.

Para más detalles, consulte "Descubra las cargas de trabajo en la BlueXP ransomware protection" .

29 de abril de 2025

Compatibilidad con Amazon FSx for NetApp ONTAP

Esta versión es compatible con Amazon FSx for NetApp ONTAP. Esta función le ayuda a proteger sus cargas de trabajo de FSx para ONTAP con la BlueXP ransomware protection.

FSx for ONTAP es un servicio totalmente administrado que proporciona la potencia del almacenamiento NetApp ONTAP en la nube. Proporciona las mismas características, rendimiento y capacidades administrativas que utiliza en sus instalaciones con la agilidad y escalabilidad de un servicio nativo de AWS.

Se realizaron los siguientes cambios en el flujo de trabajo de BlueXP ransomware protection :

- Discovery incluye cargas de trabajo en FSx para entornos de trabajo de ONTAP 9.15.
- La pestaña Protección muestra las cargas de trabajo en FSx para entornos ONTAP . En este entorno, debe realizar operaciones de respaldo utilizando el servicio de respaldo FSx para ONTAP . Puede restaurar estas cargas de trabajo utilizando instantáneas de BlueXP ransomware protection .

Las políticas de respaldo para una carga de trabajo que se ejecuta en FSx para ONTAP no se pueden configurar en BlueXP. Cualquier política de respaldo existente establecida en Amazon FSx for NetApp ONTAP permanecerá sin cambios.

- Los incidentes de alerta muestran el nuevo entorno de trabajo de FSx para ONTAP .

Para más detalles, consulte "Obtenga más información sobre la BlueXP ransomware protection y los entornos de trabajo" .

Para obtener información sobre las opciones admitidas, consulte la "Limitaciones de la BlueXP ransomware protection" .

Se necesita el rol de acceso a BlueXP

Ahora necesita uno de los siguientes roles de acceso para ver, descubrir o administrar la BlueXP ransomware protection: administrador de la organización, administrador de carpeta o proyecto, administrador de protección contra ransomware o visor de protección contra ransomware.

"Obtenga información sobre los roles de acceso de BlueXP para todos los servicios" .

14 de abril de 2025

Informes de simulacros de preparación

Con esta versión, puedes revisar los informes de simulacros de preparación para ataques de ransomware. Un simulacro de preparación le permite simular un ataque de ransomware en una carga de trabajo de muestra recién creada. Luego, investigue el ataque simulado y recupere la carga de trabajo de muestra. Esta función le ayuda a saber que está preparado en caso de un ataque de ransomware real al probar los procesos de notificación de alerta, respuesta y recuperación.

Para más detalles, consulte "Realizar un simulacro de preparación para un ataque de ransomware" .

Nuevos roles y permisos de control de acceso basados en roles

Anteriormente, podía asignar roles y permisos a los usuarios en función de sus responsabilidades, lo que le ayudaba a administrar el acceso de los usuarios a la BlueXP ransomware protection. Con esta versión, hay dos nuevos roles específicos para la BlueXP ransomware protection con permisos actualizados. Los nuevos roles son:

- Administrador de protección contra ransomware
- Visor de protección contra ransomware

Para obtener detalles sobre los permisos, consulte "Acceso basado en roles a las funciones de BlueXP ransomware protection" .

Mejoras en los pagos

Esta versión incluye varias mejoras en el proceso de pago.

Para más detalles, consulte "Configurar opciones de licencia y pago" .

10 de marzo de 2025

Simular un ataque y responder

Con esta versión, simule un ataque de ransomware para probar su respuesta a una alerta de ransomware. Esta función le ayuda a saber que está preparado en caso de un ataque de ransomware real al probar los procesos de notificación de alerta, respuesta y recuperación.

Para más detalles, consulte "Realizar un simulacro de preparación para un ataque de ransomware" .

Mejoras en el proceso de descubrimiento

Esta versión incluye mejoras en los procesos de descubrimiento y redescubrimiento selectivo:

- Con esta versión, puede descubrir cargas de trabajo recién creadas que se agregaron a los entornos de trabajo seleccionados previamente.
- También puedes seleccionar *nuevos* entornos de trabajo en esta versión. Esta función le ayuda a proteger las nuevas cargas de trabajo que se agregan a su entorno.
- Puede realizar estos procesos de descubrimiento durante el proceso de descubrimiento inicialmente o dentro de la opción Configuración.

Para más detalles, consulte "Descubra cargas de trabajo recién creadas para entornos de trabajo previamente seleccionados" y "Configurar funciones con la opción Configuración" .

Alertas generadas cuando se detecta un cifrado alto

Con esta versión, puede ver alertas cuando se detecta un cifrado alto en sus cargas de trabajo incluso sin grandes cambios en la extensión de archivo. Esta función, que utiliza la inteligencia artificial de ONTAP Autonomous Ransomware Protection (ARP), lo ayuda a identificar cargas de trabajo que corren riesgo de sufrir ataques de ransomware. Utilice esta función y descargue la lista completa de archivos afectados con o sin cambios de extensión.

Para más detalles, consulte "Responder a una alerta de ransomware detectada" .

16 de diciembre de 2024

Detecte comportamientos anómalos de los usuarios mediante Data Infrastructure Insights Storage Workload Security

Con esta versión, puede utilizar Data Infrastructure Insights Storage Workload Security para detectar comportamientos anómalos de los usuarios en sus cargas de trabajo de almacenamiento. Esta función le ayuda a identificar posibles amenazas a la seguridad y a bloquear usuarios potencialmente maliciosos para proteger sus datos.

Para más detalles, consulte "Responder a una alerta de ransomware detectada" .

Antes de usar Data Infrastructure Insights Storage Workload Security para detectar un comportamiento anómalo del usuario, debe configurar la opción mediante la opción **Configuración** de BlueXP ransomware protection .

Referirse a "Configurar los ajustes de BlueXP ransomware protection" .

Seleccione cargas de trabajo para descubrir y proteger

Con esta versión, ahora puedes hacer lo siguiente:

- Dentro de cada Conector, seleccione los entornos de trabajo donde desea descubrir cargas de trabajo. Esta función puede resultarle beneficiosa si desea proteger cargas de trabajo específicas en su entorno y no otras.
- Durante el descubrimiento de carga de trabajo, puede habilitar el descubrimiento automático de cargas de trabajo por conector. Esta función le permite seleccionar las cargas de trabajo que desea proteger.
- Descubra cargas de trabajo recién creadas para entornos de trabajo previamente seleccionados.

Referirse a "Descubra las cargas de trabajo" .

7 de noviembre de 2024

Habilitar la clasificación de datos y el escaneo de información de identificación personal (PII)

Con esta versión, puede habilitar la BlueXP classification, un componente central de la familia BlueXP , para escanear y clasificar datos en sus cargas de trabajo de uso compartido de archivos. La clasificación de datos le ayuda a identificar si sus datos incluyen información personal o privada, lo que puede aumentar los riesgos de seguridad. Este proceso también afecta la importancia de la carga de trabajo y le ayuda a garantizar que está protegiendo las cargas de trabajo con el nivel de protección adecuado.

El escaneo de datos PII en la BlueXP ransomware protection generalmente está disponible para los clientes que implementaron la BlueXP classification. La BlueXP classification está disponible como parte de la plataforma BlueXP sin costo adicional y puede implementarse localmente o en la nube del cliente.

Referirse a "Configurar los ajustes de BlueXP ransomware protection" .

Para iniciar el escaneo, en la página Protección, haga clic en **Identificar exposición** en la columna Exposición de privacidad.

"Escanee en busca de datos confidenciales de identificación personal con la BlueXP classification" .

Integración de SIEM con Microsoft Sentinel

Ahora puede enviar datos a su sistema de gestión de eventos y seguridad (SIEM) para el análisis y detección de amenazas mediante Microsoft Sentinel. Anteriormente, podía seleccionar AWS Security Hub o Splunk Cloud como su SIEM.

"Obtenga más información sobre cómo configurar los ajustes de BlueXP ransomware protection" .

Prueba gratuita ahora 30 días

Con este lanzamiento, las nuevas implementaciones de BlueXP ransomware protection ahora tienen 30 días de prueba gratuita. Anteriormente, la BlueXP ransomware protection ofrecía una prueba gratuita de 90 días. Si ya está en la prueba gratuita de 90 días, esa oferta continúa durante los 90 días.

Restaurar la carga de trabajo de la aplicación a nivel de archivo para Podman

Antes de restaurar una carga de trabajo de la aplicación a nivel de archivo, ahora puede ver una lista de archivos que podrían haber sido afectados por un ataque e identificar aquellos que desea restaurar. Anteriormente, si los conectores BlueXP de una organización (anteriormente una cuenta) usaban Podman, esta función estaba deshabilitada. Ahora está habilitado para Podman. Puede dejar que la BlueXP ransomware protection elija los archivos a restaurar, puede cargar un archivo CSV que enumere todos los archivos afectados por una alerta o puede identificar manualmente qué archivos desea restaurar.

"Obtenga más información sobre cómo recuperarse de un ataque de ransomware" .

30 de septiembre de 2024

Agrupación personalizada de cargas de trabajo de recursos compartidos de archivos

Con esta versión, ahora puede agrupar recursos compartidos de archivos en grupos para facilitar la protección de su patrimonio de datos. El servicio puede proteger todos los volúmenes de un grupo al mismo tiempo.

Anteriormente, era necesario proteger cada volumen por separado.

"Obtenga más información sobre la agrupación de cargas de trabajo de recursos compartidos de archivos en las estrategias de protección contra ransomware." .

2 de septiembre de 2024

Evaluación de riesgos de seguridad de Digital Advisor

La BlueXP ransomware protection ahora recopila información sobre riesgos de seguridad altos y críticos relacionados con un clúster desde NetApp Digital Advisor. Si se encuentra algún riesgo, la BlueXP ransomware protection proporciona una recomendación en el panel **Acciones recomendadas** del Panel de control: "Solucionar una vulnerabilidad de seguridad conocida en el clúster <nombre>". Según la recomendación en el Panel de Control, al hacer clic en **Revisar y corregir** se sugiere revisar Digital Advisor y un artículo de Vulnerabilidad y Exposición Común (CVE) para resolver el riesgo de seguridad. Si existen múltiples riesgos de seguridad, revise la información en Digital Advisor.

Referirse a "Documentación de Digital Advisor" .

Realizar copias de seguridad en Google Cloud Platform

Con esta versión, puedes establecer un destino de respaldo en un depósito de Google Cloud Platform. Anteriormente, solo podía agregar destinos de respaldo a NetApp StorageGRID, Amazon Web Services y Microsoft Azure.

"Obtenga más información sobre cómo configurar los ajustes de BlueXP ransomware protection" .

Compatibilidad con Google Cloud Platform

El servicio ahora es compatible con Cloud Volumes ONTAP para Google Cloud Platform para la protección del almacenamiento. Anteriormente, el servicio solo admitía Cloud Volumes ONTAP para Amazon Web Services y Microsoft Azure junto con NAS local.

"Obtenga información sobre la BlueXP ransomware protection y las fuentes de datos compatibles, los destinos de copia de seguridad y los entornos de trabajo." .

Control de acceso basado en roles

Ahora puede limitar el acceso a actividades específicas con el control de acceso basado en roles (RBAC). La BlueXP ransomware protection utiliza dos roles de BlueXP: administrador de cuenta de BlueXP y administrador sin cuenta (visor).

Para obtener detalles sobre las acciones que puede realizar cada rol, consulte "Privilegios de control de acceso basados en roles" .

5 de agosto de 2024

Detección de amenazas con Splunk Cloud

Puede enviar datos automáticamente a su sistema de gestión de eventos y seguridad (SIEM) para analizar y detectar amenazas. Con versiones anteriores, solo podía seleccionar AWS Security Hub como su SIEM. Con esta versión, puede seleccionar AWS Security Hub o Splunk Cloud como su SIEM.

"Obtenga más información sobre cómo configurar los ajustes de BlueXP ransomware protection" .

1 de julio de 2024

Traiga su propia licencia (BYOL)

Con esta versión, puede utilizar una licencia BYOL, que es un archivo de licencia de NetApp (NLF) que obtiene de su representante de ventas de NetApp .

"Obtenga más información sobre la configuración de licencias" .

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

Antes de restaurar una carga de trabajo de la aplicación a nivel de archivo, ahora puede ver una lista de archivos que podrían haber sido afectados por un ataque e identificar aquellos que desea restaurar. Puede dejar que la BlueXP ransomware protection elija los archivos a restaurar, puede cargar un archivo CSV que enumere todos los archivos afectados por una alerta o puede identificar manualmente qué archivos desea restaurar.

Con esta versión, si todos los conectores BlueXP de una cuenta no usan Podman, se habilita la función de restauración de un solo archivo. De lo contrario, se deshabilitará para esa cuenta.

"Obtenga más información sobre cómo recuperarse de un ataque de ransomware" .

Descargar una lista de archivos afectados

Antes de restaurar una carga de trabajo de la aplicación a nivel de archivo, ahora puede acceder a la página Alertas para descargar una lista de archivos afectados en un archivo CSV y luego usar la página Recuperación para cargar el archivo CSV.

"Obtenga más información sobre cómo descargar archivos afectados antes de restaurar una aplicación" .

Eliminar plan de protección

Con esta versión, ahora puedes eliminar una estrategia de protección contra ransomware.

"Obtenga más información sobre la protección de las cargas de trabajo y la gestión de estrategias de protección contra ransomware." .

10 de junio de 2024

Bloqueo de copia de instantáneas en el almacenamiento principal

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.

"Obtenga más información sobre cómo proteger las cargas de trabajo y habilitar el bloqueo de copias de seguridad en una estrategia de protección contra ransomware." .

Compatibilidad con Cloud Volumes ONTAP para Microsoft Azure

Esta versión es compatible con Cloud Volumes ONTAP para Microsoft Azure como sistema además de Cloud Volumes ONTAP para AWS y ONTAP NAS local.

"Inicio rápido de Cloud Volumes ONTAP en Azure"

"Obtenga más información sobre la BlueXP ransomware protection" .

Microsoft Azure agregado como destino de respaldo

Ahora puede agregar Microsoft Azure como destino de respaldo junto con AWS y NetApp StorageGRID.

"Obtenga más información sobre cómo configurar los ajustes de protección" .

14 de mayo de 2024

Actualizaciones de licencias

Puedes registrarte para una prueba gratuita de 90 días. Pronto podrás comprar una suscripción de pago por uso con Amazon Web Services Marketplace o traer tu propia licencia de NetApp .

"Obtenga más información sobre la configuración de licencias" .

Protocolo CIFS

El servicio ahora admite ONTAP local y Cloud Volumes ONTAP en sistemas AWS mediante protocolos NFS y CIFS. La versión anterior solo admitía el protocolo NFS.

Detalles de la carga de trabajo

Esta versión ahora proporciona más detalles en la información de la carga de trabajo de Protección y otras páginas para una mejor evaluación de la protección de la carga de trabajo. Desde los detalles de la carga de trabajo, puede revisar la política asignada actualmente y revisar los destinos de respaldo configurados.

"Obtenga más información sobre cómo ver los detalles de la carga de trabajo en las páginas de Protección" .

Protección y recuperación consistentes con las aplicaciones y las máquinas virtuales

Ahora puede realizar una protección consistente con las aplicaciones con el software NetApp SnapCenter y una protección consistente con las máquinas virtuales con el SnapCenter Plug-in for VMware vSphere, logrando un estado inactivo y consistente para evitar una posible pérdida de datos más adelante si se necesita recuperación. Si se requiere recuperación, puede restaurar la aplicación o la máquina virtual a cualquiera de los estados disponibles anteriormente.

"Obtenga más información sobre la protección de las cargas de trabajo" .

Estrategias de protección contra ransomware

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 este servicio:

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

"Obtenga más información sobre la protección de las cargas de trabajo" .

Detección de amenazas

Ahora es posible habilitar la detección de amenazas mediante un sistema de gestión de eventos y seguridad (SIEM) de terceros. El Panel de Control ahora muestra una nueva recomendación para "Habilitar detección de amenazas", que se puede configurar en la página de Configuración.

"Obtenga más información sobre cómo configurar las opciones de Configuración" .

Descartar alertas de falsos positivos

Desde la pestaña Alertas, ahora puede descartar falsos positivos o decidir recuperar sus datos de inmediato.

"Obtenga más información sobre cómo responder a una alerta de ransomware" .

Estado de detección

Aparecen nuevos estados de detección en la página Protección que muestran el estado de la detección de ransomware aplicada a la carga de trabajo.

"Obtenga más información sobre cómo proteger cargas de trabajo y visualizar estados de protección" .

Descargar archivos CSV

Puede descargar archivos CSV* desde las páginas Protección, Alertas y Recuperación.

"Obtenga más información sobre cómo descargar archivos CSV desde el Panel de control y otras páginas" .

Enlace de documentación

El enlace Ver documentación ahora está incluido en la interfaz de usuario. Puede acceder a esta documentación desde el Panel de control vertical **Acciones***  **opción. Seleccione *Novedades** para ver los detalles en las Notas de la versión o **Documentación** para ver la página de inicio de la documentación de BlueXP ransomware protection .

BlueXP backup and recovery

Ya no es necesario que el servicio de BlueXP backup and recovery esté habilitado en el sistema. Ver "prerrequisitos" . El servicio de BlueXP ransomware protection ayuda a configurar un destino de copia de seguridad a través de la opción Configuración. Ver "Configurar ajustes" .

Opción de configuración

Ahora puede configurar destinos de respaldo en la configuración de BlueXP ransomware protection .

"Obtenga más información sobre cómo configurar las opciones de Configuración" .

5 de marzo de 2024

Gestión de políticas de protección

Además de utilizar políticas predefinidas, ahora puedes crear políticas. "Obtenga más información sobre la gestión de políticas" .

Inmutabilidad en el almacenamiento secundario (DataLock)

Ahora puede hacer que la copia de seguridad sea inmutable en el almacenamiento secundario utilizando la tecnología NetApp DataLock en el almacén de objetos. "Obtenga más información sobre la creación de políticas de protección" .

Copia de seguridad automática en NetApp StorageGRID

Además de usar AWS, ahora puedes elegir StorageGRID como tu destino de respaldo. "Obtenga más información sobre cómo configurar destinos de respaldo" .

Funciones adicionales para investigar posibles ataques

Ahora puede ver más detalles forenses para investigar el posible ataque detectado. "Obtenga más información sobre cómo responder a una alerta de ransomware detectada" .

Proceso de recuperación

Se mejoró el proceso de recuperación. Ahora, puede recuperar volumen por volumen o todos los volúmenes para una carga de trabajo. "Obtenga más información sobre cómo recuperarse de un ataque de ransomware (después de que se hayan neutralizado los incidentes)" .

"Obtenga más información sobre la BlueXP ransomware protection" .

6 de octubre de 2023

El servicio de BlueXP ransomware protection es una solución SaaS para proteger datos, detectar posibles ataques y recuperar datos de un ataque de ransomware.

Para la versión preliminar, el servicio protege cargas de trabajo basadas en aplicaciones de Oracle, almacenes de datos de VM y recursos compartidos de archivos en almacenamiento NAS local, así como Cloud Volumes ONTAP en AWS (usando el protocolo NFS) en organizaciones BlueXP de forma individual y realiza copias de seguridad de los datos en el almacenamiento en la nube de Amazon Web Services.

El servicio de BlueXP ransomware protection proporciona el uso completo de varias tecnologías de NetApp para que su administrador de seguridad de datos o ingeniero de operaciones de seguridad pueda lograr los siguientes objetivos:

- Vea la protección contra ransomware en todas sus cargas de trabajo de un vistazo.
- Obtenga información sobre las recomendaciones de protección contra ransomware
- Mejore la postura de protección según las recomendaciones de BlueXP ransomware protection .
- Asigne políticas de protección contra ransomware para proteger sus principales cargas de trabajo y datos de alto riesgo contra ataques de ransomware.
- Supervise la salud de sus cargas de trabajo contra ataques de ransomware en busca de anomalías en los datos.
- Evalúe rápidamente el impacto de los incidentes de ransomware en su carga de trabajo.
- Recupérese de incidentes de ransomware de forma inteligente restaurando datos y garantizando que no se produzca una reinfección a partir de los datos almacenados.

"Obtenga más información sobre la BlueXP ransomware protection" .

Limitaciones conocidas de NetApp Ransomware Resilience

Las limitaciones conocidas identifican plataformas, dispositivos o funciones que no son compatibles con esta versión del producto o que no interoperan correctamente con él. Revise estas limitaciones cuidadosamente.

Problema con la opción de reinicio del ejercicio de preparación

Si selecciona un volumen ONTAP 9.11.1 para el simulacro de preparación para ataques de ransomware, Ransomware Resilience envía una alerta. Si recupera los datos utilizando la opción "clonar a volumen" y reinicia el taladro, la operación de reinicio falla.

Limitaciones de Amazon FSx for NetApp ONTAP

El sistema Amazon FSx for NetApp ONTAP es compatible con Ransomware Resilience. Las siguientes limitaciones se aplican a este sistema:

- Las políticas de respaldo no son compatibles con Fsx para ONTAP. En este entorno, debe realizar operaciones de respaldo utilizando Amazon FSx para respaldos. Puede restaurar estas cargas de trabajo utilizando Ransomware Resilience.
- Las operaciones de restauración se realizan únicamente desde instantáneas.

Empezar

Obtenga más información sobre la NetApp Ransomware Resilience

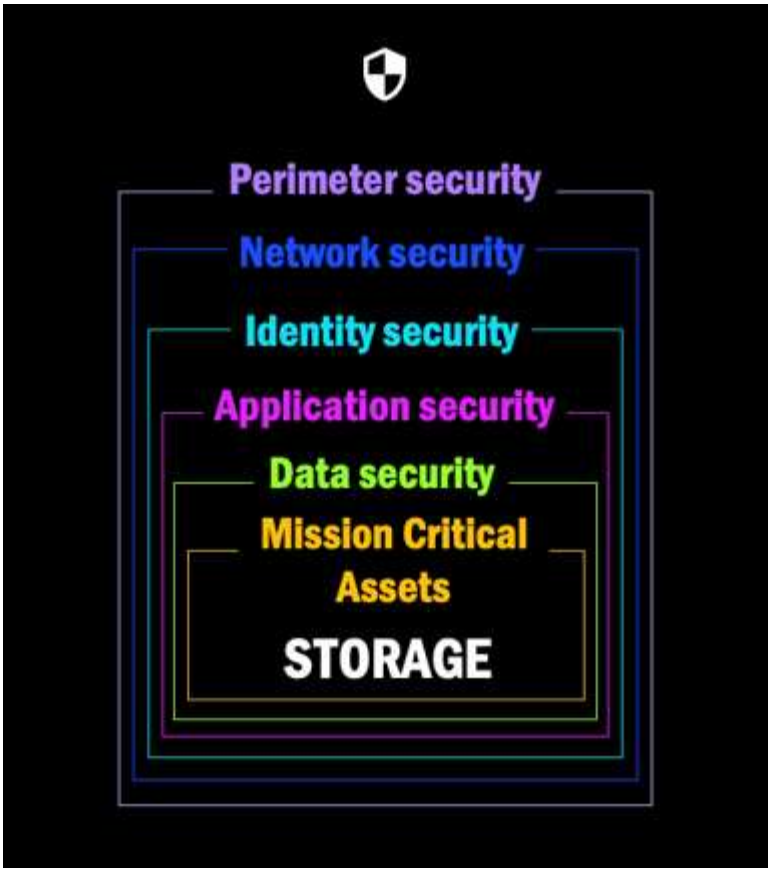
Los ataques de ransomware pueden bloquear el acceso a sus datos y los atacantes pueden pedir un rescate a cambio de la liberación de datos o el descifrado. Según IDC, no es raro que las víctimas de ransomware experimenten múltiples ataques de ransomware. El ataque puede interrumpir el acceso a sus datos durante un período que puede durar desde un día hasta varias semanas.

NetApp Ransomware Resilience protege sus datos de los ataques de ransomware. En Ransomware Resilience, la protección está disponible para cargas de trabajo basadas en aplicaciones de Oracle, almacenes de datos de VM y recursos compartidos de archivos en almacenamiento NAS local (usando los protocolos NFS y CIFS) y almacenamiento SAN (FC, iSCSI y NVMe), así como Cloud Volumes ONTAP para Amazon Web Services, Cloud Volumes ONTAP para Google Cloud, Cloud Volumes ONTAP para Microsoft Azure y Amazon FSx for NetApp ONTAP en la NetApp Console. Puede realizar copias de seguridad de datos en Amazon Web Services, Google Cloud, almacenamiento en la nube de Microsoft Azure y NetApp StorageGRID.

Resiliencia frente al ransomware en la capa de datos

Su postura de seguridad generalmente abarca múltiples capas de defensa para protegerse contra una variedad de amenazas cibernéticas.

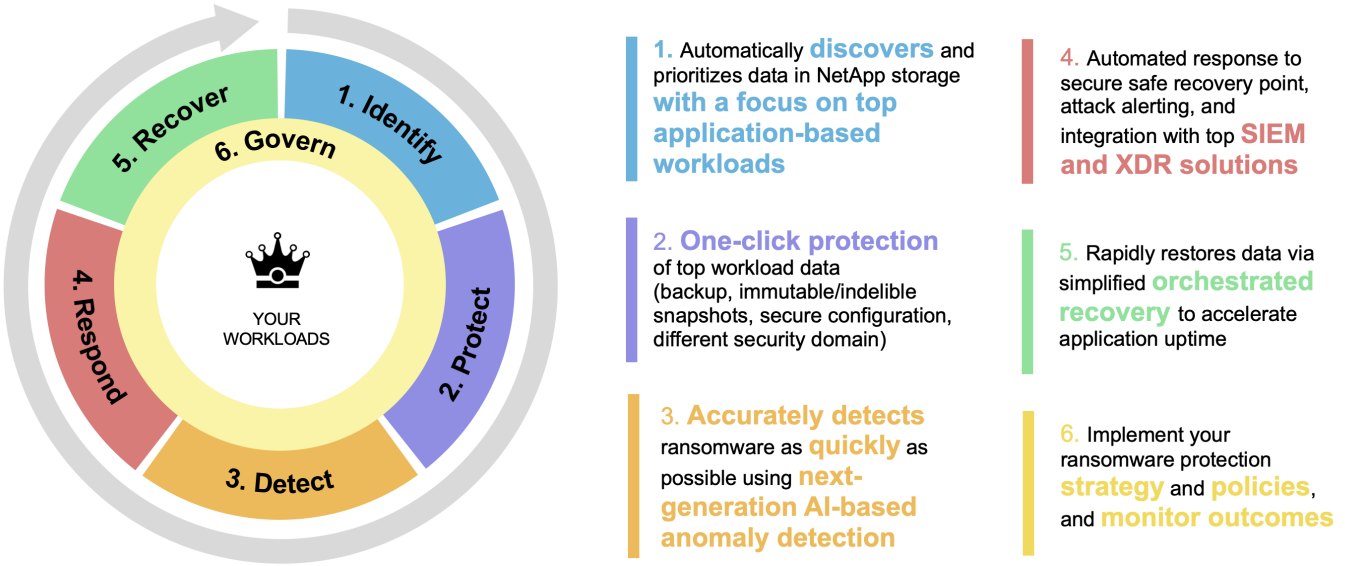
- **Capa más externa**: esta es su primera línea de defensa, que utiliza firewalls, sistemas de detección de intrusiones y redes privadas virtuales para proteger los límites de la red.
- **Seguridad de la red**: esta capa se basa en la base con segmentación de red, monitoreo de tráfico y cifrado.
- **Seguridad de identidad**: utiliza métodos de autenticación, controles de acceso y gestión de identidad para garantizar que solo los usuarios autorizados puedan acceder a recursos confidenciales.
- **Seguridad de la aplicación**: protege las aplicaciones de software mediante prácticas de codificación segura, pruebas de seguridad y autoprotección de aplicaciones en tiempo de ejecución.
- **Seguridad de datos**: protege tus datos con protección de datos, copias de seguridad y estrategias de recuperación. La resiliencia frente al ransomware opera en esta capa.



Qué puedes hacer con Ransomware Resilience

Ransomware Resilience proporciona el uso completo de varias tecnologías de NetApp para que su administrador de almacenamiento, administrador de seguridad de datos o ingeniero de operaciones de seguridad puedan lograr los siguientes objetivos:

- **Identifique** todas las cargas de trabajo basadas en aplicaciones, recursos compartidos de archivos o administradas por VMware en los sistemas NAS locales de NetApp (NFS o CIFS) y SAN (FC, iSCSI y NVMe) en la NetApp Console, los proyectos y los agentes de la consola. Ransomware Resilience clasifica la prioridad de los datos y le brinda recomendaciones para mejorar la resiliencia contra el ransomware.
- **Proteja** sus cargas de trabajo habilitando copias de seguridad, copias instantáneas y estrategias de protección contra ransomware en sus datos.
- **Detectar** anomalías que podrían ser ataques de ransomware. Nota al pie: [Si bien es posible que un ataque pase desapercibido, nuestra investigación indica que la tecnología de NetApp ha dado como resultado un alto grado de detección para ciertos ataques de ransomware basados en cifrado de archivos].
- **Responda** a posibles ataques de ransomware iniciando automáticamente una instantánea de NetApp ONTAP a prueba de manipulaciones que está bloqueada para que la copia no se pueda eliminar de manera accidental o maliciosa. Sus datos de respaldo permanecerán inmutables y protegidos de extremo a extremo contra ataques de ransomware en el origen y en el destino.
- **Recupere** sus cargas de trabajo que ayudan a acelerar el tiempo de actividad de la carga de trabajo mediante la orquestación de varias tecnologías de NetApp . Puede elegir recuperar volúmenes específicos. Ransomware Resilience ofrece recomendaciones sobre las mejores opciones.
- **Gobernar**: Implemente su estrategia de protección contra ransomware y monitoree los resultados.



Beneficios de utilizar Ransomware Resilience

La resiliencia frente al ransomware ofrece los siguientes beneficios:

- Descubre cargas de trabajo y sus programaciones de instantáneas y copias de seguridad existentes, y clasifica su importancia relativa.
- Evalúa su postura de protección contra ransomware y la muestra en un panel fácil de entender.
- Proporciona recomendaciones sobre los próximos pasos basados en el descubrimiento y el análisis de la postura de protección.
- Aplica recomendaciones de protección de datos impulsadas por IA/ML con acceso con un solo clic.
- Protege datos en cargas de trabajo basadas en aplicaciones, como Oracle, almacenes de datos de VMware y recursos compartidos de archivos.
- Detecta ataques de ransomware a datos en tiempo real en el almacenamiento primario utilizando tecnología de IA.
- Inicia acciones automatizadas en respuesta a posibles ataques detectados creando copias instantáneas e iniciando alertas sobre actividad anormal.
- Aplica una recuperación curada para cumplir con las políticas de RPO. Ransomware Resilience orquesta la recuperación de incidentes de ransomware mediante el uso de varios servicios de recuperación de NetApp , incluidos NetApp Backup and Recovery (anteriormente Cloud Backup) y SnapCenter.
- Utiliza el control de acceso basado en roles (RBAC) para gobernar el acceso a funciones y operaciones.

Costo

NetApp no le cobra por utilizar la versión de prueba de Ransomware Resilience.

> Con el lanzamiento de octubre de 2024, las nuevas implementaciones de Ransomware Resilience ofrecen una prueba gratuita de 30 días. Anteriormente, Ransomware Resilience ofrecía una prueba gratuita de 90 días. Si ya se ha inscrito en la prueba gratuita de 90 días, dicha prueba será válida durante los 90 días.

Si tiene Backup and Recovery y Ransomware Resilience, cualquier dato común protegido por ambos

productos se factura únicamente por Ransomware Resilience.

Después de comprar una licencia o suscripción PayGo, cualquier carga de trabajo que tenga una política de detección de ransomware (Protección autónoma contra ransomware) habilitada (descubierta o configurada por Ransomware Resilience) y al menos una política de instantánea o respaldo, Ransomware Resilience la clasifica como "Protegida" y cuenta para la capacidad comprada o la suscripción PayGo. Si se descubre una carga de trabajo sin una política de detección, incluso si tiene políticas de respaldo o instantáneas, se clasifica como “En riesgo” y *no* cuenta para la capacidad comprada.

Las cargas de trabajo protegidas se contabilizan para la capacidad adquirida o la suscripción una vez finalizado el período de prueba de 90 días. Ransomware Resilience se cobra por GB de datos asociados con cargas de trabajo protegidas antes de aplicar eficiencias.

Licencias

Con Ransomware Resilience, puede utilizar diferentes planes de licencia, incluida una prueba gratuita, una suscripción de pago por uso o traer su propia licencia.

La resiliencia contra ransomware requiere una licencia de NetApp ONTAP One.

La licencia Ransomware Resilience no incluye productos NetApp adicionales. Ransomware Resilience puede utilizar Backup and Recovery incluso si no tiene una licencia para ello.

Para detectar un comportamiento anómalo del usuario, Ransomware Resilience utiliza NetApp Autonomous Ransomware Protection, un modelo de aprendizaje automático (ML) dentro de ONTAP que detecta la actividad de archivos maliciosos. Este modelo está incluido en la licencia Ransomware Resilience.

Para obtener más información, consulte "Configurar licencias" .

NetApp Console

Se puede acceder a Ransomware Resilience a través de la NetApp Console.

La NetApp Console proporciona una gestión centralizada de los servicios de datos y almacenamiento de NetApp en entornos locales y en la nube a nivel empresarial. La consola es necesaria para acceder y utilizar los servicios de datos de NetApp . Como interfaz de administración, le permite administrar muchos recursos de almacenamiento desde una sola interfaz. Los administradores de la consola pueden controlar el acceso al almacenamiento y los servicios para todos los sistemas dentro de la empresa.

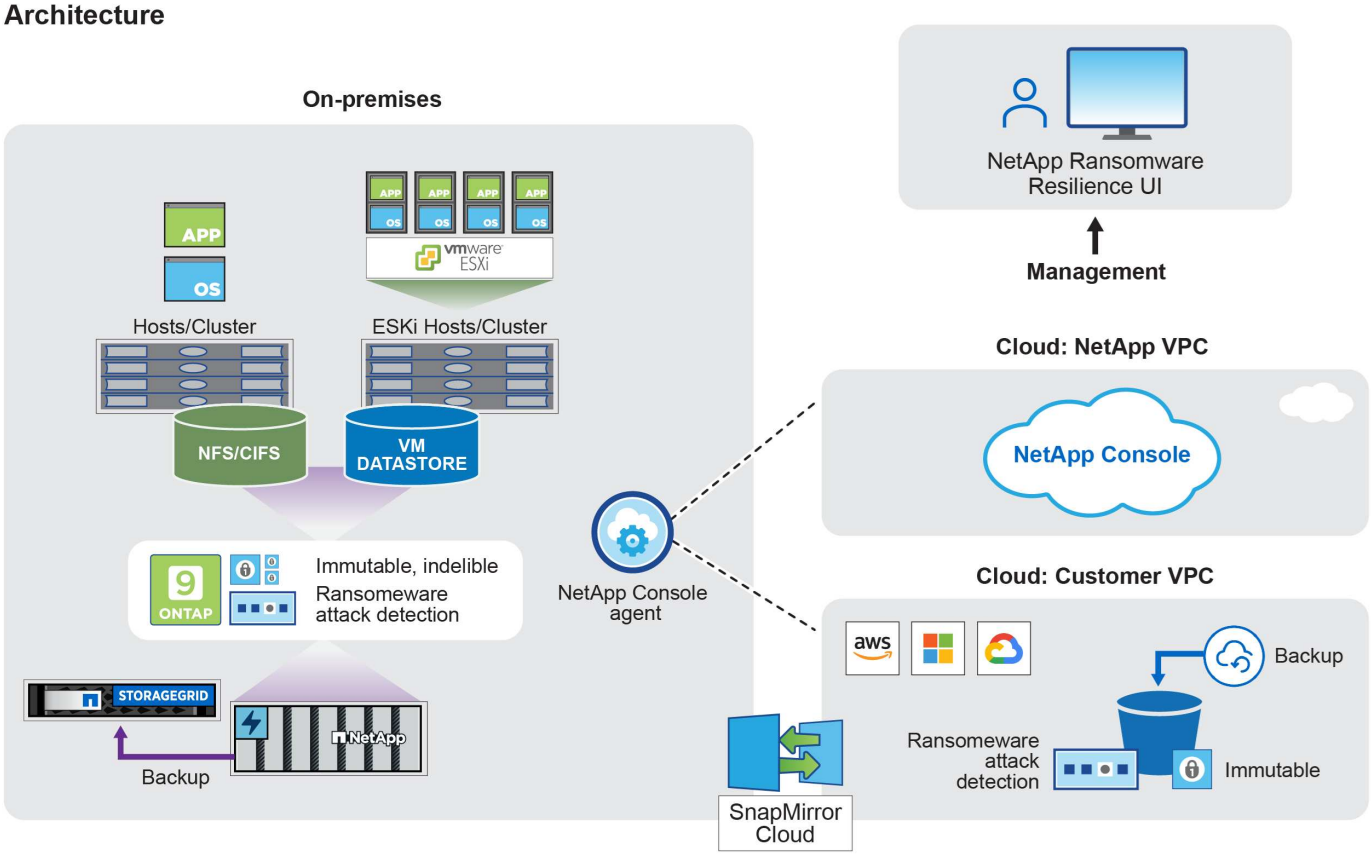
No necesita una licencia o suscripción para comenzar a usar NetApp Console y solo incurre en cargos cuando necesita implementar agentes de Console en su nube para garantizar la conectividad con sus sistemas de almacenamiento o servicios de datos de NetApp . Sin embargo, algunos servicios de datos de NetApp accesibles desde la consola requieren licencia o suscripción.

Obtenga más información sobre el"NetApp Console" .

Cómo funciona la resiliencia frente al ransomware

Ransomware Resilience utiliza NetApp Backup and Recovery para descubrir y establecer políticas de instantáneas y copias de seguridad para cargas de trabajo de uso compartido de archivos, y SnapCenter o SnapCenter for VMware para descubrir y establecer políticas de instantáneas y copias de seguridad para cargas de trabajo de aplicaciones y máquinas virtuales. Además, Ransomware Resilience utiliza Backup and Recovery y SnapCenter / SnapCenter for VMware para realizar una recuperación consistente con los archivos y la carga de trabajo.

Architecture



Característica	Descripción
IDENTIFICAR	• Encuentra todos los datos locales NAS (protocolos NFS y CIFS), SAN (FC, iSCSI y NVMe) y Cloud Volumes ONTAP del cliente conectados a la consola. • Identifica datos de clientes de las API de servicio ONTAP y SnapCenter y los asocia con cargas de trabajo. Obtenga más información sobre "ONTAP" y "Software SnapCenter" . • Descubre el nivel de protección actual de cada volumen de las copias de instantáneas de NetApp y las políticas de respaldo, así como también cualquier capacidad de detección integrada. Luego, Ransomware Resilience asocia esta postura de protección con las cargas de trabajo mediante el uso de Backup and Recovery, servicios ONTAP y tecnologías de NetApp como Autonomous Ransomware Protection (ARP o ARP/AI según su versión de ONTAP), FPolicy, políticas de backup y políticas de snapshots. Obtenga más información sobre "Protección autónoma contra ransomware" , "NetApp Backup and Recovery" , y "Política de ONTAP" . • Asigna una prioridad comercial a cada carga de trabajo en función de los niveles de protección descubiertos automáticamente y recomienda políticas de protección para las cargas de trabajo en función de su prioridad comercial. La prioridad de la carga de trabajo se basa en las frecuencias de instantáneas ya aplicadas a cada volumen asociado con la carga de trabajo.
PROTEGER	• Supervisa activamente las cargas de trabajo y orquesta el uso de las API de Backup and Recovery, SnapCenter y ONTAP mediante la aplicación de políticas a cada una de las cargas de trabajo identificadas.

Característica	Descripción
DETECTAR	• Detecta ataques potenciales con un modelo de aprendizaje automático (ML) integrado que detecta actividad y cifrado potencialmente anómalos. • Proporciona detección de doble capa que comienza con la detección de posibles ataques de ransomware en el almacenamiento principal y responde a actividades anormales tomando copias instantáneas automatizadas adicionales para crear los puntos de restauración de datos más cercanos. Ransomware Resilience proporciona la capacidad de profundizar para identificar ataques potenciales con mayor precisión sin afectar el rendimiento de las cargas de trabajo principales. • Determina los archivos sospechosos específicos y los asigna a las cargas de trabajo asociadas, utilizando ONTAP, Autonomous Ransomware Protection (ARP o ARP/AI según su versión de ONTAP) y tecnologías FPolicy.
RESPONDER	• Muestra datos relevantes, como la actividad del archivo, la actividad del usuario y la entropía, para ayudarlo a completar revisiones forenses sobre el ataque. • Inicia copias instantáneas rápidas mediante el uso de tecnologías y productos de NetApp , como ONTAP, Autonomous Ransomware Protection (ARP o ARP/AI según su versión de ONTAP) y FPolicy.
RECUPERAR	• Determina la mejor instantánea o copia de seguridad y recomienda el mejor punto de recuperación real (RPA) mediante el uso de Backup and Recovery, ONTAP, Autonomous Ransomware Protection (ARP o ARP/AI según su versión de ONTAP) y tecnologías y servicios de FPolicy. • Orquesta la recuperación de cargas de trabajo, incluidas máquinas virtuales, recursos compartidos de archivos, almacenamiento en bloque y bases de datos con consistencia de aplicaciones.
GOBERNAR	• Asigna las estrategias de protección contra ransomware • Le ayuda a monitorear los resultados.

Destinos de copia de seguridad, sistemas y fuentes de datos de carga de trabajo compatibles

Ransomware Resilience admite los siguientes objetivos de respaldo, sistemas y fuentes de datos:

Destinos de copia de seguridad compatibles

- Servicios web de Amazon (AWS) S3
- Plataforma de Google Cloud
- Blob de Microsoft Azure
- StorageGRID en NetApp

Sistemas compatibles

Ambiente	Protocolo	Versiones compatibles
Amazon FSx for NetApp ONTAP*	NFS, CIFS y SAN	N/A

Ambiente	Protocolo	Versiones compatibles
Cloud Volumes ONTAP para AWS	CIFS y NFS	9.11.1 y posteriores
	SAN (FC, iSCSI y NVMe)	9.17.1 y posteriores
Cloud Volumes ONTAP para Google Cloud Platform	CIFS y NFS	9.11.1 y posteriores
	SAN (FC, iSCSI y NVMe)	9.17.1 y posteriores
Cloud Volumes ONTAP para Microsoft Azure	CIFS y NFS	9.12.1 y posteriores
	SAN (FC, iSCSI y NVMe)	9.17.1 y posteriores
ONTAP (en las instalaciones)	CIFS y NFS	9.11.1 y posteriores
	SAN (FC, iSCSI y NVMe)	9.17.1 y posteriores

* Amazon FSx for NetApp ONTAP utiliza la Protección Autónoma contra el Ransomware (ARP) y no ARP/AI. Para obtener más información sobre la diferencia, consulte"ARP/IA" .

> El uso de ARP/AI en ONTAP requiere ONTAP 9.16 o superior. + ONTAP no proporciona soporte de protección contra ransomware para FabricPool FlexCache, volúmenes FlexGroup , volúmenes de punto de montaje de grupos de consistencia, volúmenes de ruta de montaje, volúmenes sin conexión y volúmenes de protección de datos (DP). Asegúrese de revisar"Configuraciones admitidas y no admitidas en ONTAP" .

Fuentes de datos de carga de trabajo compatibles

Ransomware Resilience protege las siguientes cargas de trabajo basadas en aplicaciones en volúmenes de datos primarios:

- Almacenamiento en bloque
- Bases de datos:
  - Microsoft SQL Server
  - Oráculo
  - PostgreSQL
- Recursos compartidos de archivos de NetApp
- Almacenes de datos de VMware

Si utiliza SnapCenter o SnapCenter para VMware, todas las cargas de trabajo compatibles con esos productos también se identifican en Ransomware Resilience. Ransomware Resilience puede protegerlos y recuperarlos de manera consistente con la carga de trabajo.

Términos que podrían ayudarle con la protección contra ransomware

Podría resultarle beneficioso comprender cierta terminología relacionada con la protección contra ransomware.

- **Protección**: La protección contra ransomware significa garantizar que se realicen instantáneas y copias de seguridad inmutables de forma regular en un dominio de seguridad diferente mediante políticas de protección.
- **Carga de trabajo**: una carga de trabajo en Ransomware Resilience puede incluir bases de datos de

Oracle, almacenes de datos de VMware o recursos compartidos de archivos.

Requisitos previos de NetApp Ransomware Resilience

Comience a usar NetApp Ransomware Resilience verificando la preparación de su entorno operativo, acceso a la red y navegador web.

Para utilizar Ransomware Resilience, asegúrese de cumplir con los requisitos previos.

Sistemas compatibles

Asegúrese de estar utilizando un sistema compatible:

Ambiente	Protocolo	Versiones compatibles
Amazon FSx for NetApp ONTAP*	NFS, CIFS y SAN	N/A
Cloud Volumes ONTAP para AWS	CIFS y NFS	9.11.1 y posteriores
	SAN (FC, iSCSI y NVMe)	9.17.1 y posteriores
Cloud Volumes ONTAP para Google Cloud Platform	CIFS y NFS	9.11.1 y posteriores
	SAN (FC, iSCSI y NVMe)	9.17.1 y posteriores
Cloud Volumes ONTAP para Microsoft Azure	CIFS y NFS	9.12.1 y posteriores
	SAN (FC, iSCSI y NVMe)	9.17.1 y posteriores
ONTAP (en las instalaciones)	CIFS y NFS	9.11.1 y posteriores
	SAN (FC, iSCSI y NVMe)	9.17.1 y posteriores

* Amazon FSx for NetApp ONTAP utiliza la Protección Autónoma contra el Ransomware (ARP) y no ARP/AI. Para obtener más información sobre la diferencia, consulte"ARP/IA" .

Requisitos de la NetApp Console

La configuración de su NetApp Console requiere:

- Una cuenta de usuario de la NetApp Console con privilegios de administrador de la organización para descubrir recursos.
- Una organización y sistema de consola con al menos un agente de consola activo conectado a una"sistema compatible" .
  - Si sus clústeres ONTAP locales o Cloud Volumes ONTAP en AWS o en la nube de Azure no están configurados en la consola, consulte"Aprenda a configurar un agente de consola" y"Requisitos estándar de la consola" .

  Si tiene varios agentes de consola en una sola organización de consola, Ransomware Resilience escaneará los recursos de ONTAP en todos los agentes de consola más allá del que esté seleccionado actualmente en la interfaz de usuario de la consola.

- El agente de consola debe tener la `cloudmanager-ransomware-protection` contenedor en estado activo.

- Al menos un sistema de consola con un clúster ONTAP local de NetApp o Cloud Volumes ONTAP en AWS o Azure. Ransomware Resilience admite protocolos NAS (NFS y SMB) y SAN (iSCSI, FC y NVMe).
  - Ransomware Resilience es compatible con clústeres ONTAP o Cloud Volumes ONTAP con la versión 9.11.1 o superior de ONTAP .

> Para utilizar la resiliencia contra el ransomware en cargas de trabajo SAN, debe estar ejecutando ONTAP 9.17.1 o posterior.

Requisitos de ONTAP

- Debe estar ejecutando ONTAP 9.11.1 o posterior con una licencia ONTAP One habilitada en la instancia ONTAP local. Para obtener más información sobre la compatibilidad con ONTAP , consulte"Descripción general de la protección autónoma contra ransomware" .
- Para aplicar configuraciones de protección (como habilitar la protección autónoma contra ransomware), Ransomware Resilience necesita permisos de administrador en el clúster ONTAP . El clúster ONTAP debería haberse incorporado utilizando únicamente las credenciales de usuario administrador del clúster ONTAP .

> Si ha conectado un clúster ONTAP a la consola con credenciales que no son de administrador, [debe actualizar las credenciales en el clúster ONTAP](#update-non-admin-user-permissions-in-an-ontap-system).

Copias de seguridad de datos

- Una cuenta en NetApp StorageGRID, AWS S3, Azure Blob o Google Cloud Platform para destinos de copia de seguridad con los permisos de acceso adecuados configurados.

  Consulte la "Lista de permisos de AWS, Azure o S3" Para más detalles.

- No es necesario habilitar NetApp Backup and Recovery en el sistema.

  Ransomware Resilience ayuda a configurar un destino de respaldo a través de la opción Configuración. Ver "Configurar ajustes" .

Comportamiento sospechoso del usuario

Para que Ransomware Resilience proporcione alertas sobre el comportamiento sospechoso del usuario, debe configurar un agente de actividad del usuario. Para obtener más información, consulte "Configurar la detección de actividad sospechosa de usuarios en NetApp Ransomware Resilience".

Actualizar los permisos de usuarios no administradores en un sistema ONTAP

Si necesita actualizar los permisos de usuarios que no son administradores para un sistema en particular, complete estos pasos.

1. Inicie sesión en la consola y busque el sistema que necesita actualizar sus permisos de usuario de ONTAP .
2. Seleccione el sistema para ver los detalles.
3. Seleccione **Ver información adicional** para mostrar el nombre de usuario.

4. Inicie sesión en la CLI del clúster ONTAP como usuario administrador.
5. Mostrar los roles existentes para ese usuario. Ingresar:

```
security login show -user-or-group-name <username>
```

6. Cambiar el rol del usuario. Ingresar:

```
security login modify -user-or-group-name <username> -application
console|http|ontapi|ssh|telnet -authentication-method password -role
admin
```

7. Vuelva a la NetApp Console para usar la función de resiliencia ante ransomware.

Inicio rápido para la NetApp Ransomware Resilience

Comprenda los pasos de alto nivel que debe seguir para configurar Ransomware Resilience y proteger sus cargas de trabajo.

Siga los enlaces en cada paso para obtener información detallada.

1 Revisar los prerrequisitos

Estas tareas requieren el rol de *Administrador de consola*.

- "Asegúrese de haber instalado un agente de consola"
- "Asegúrese de que su sistema cumpla con los requisitos"
- "Revise los roles de usuario de Ransomware Resilience y asigne permisos a los usuarios que acceden a Ransomware Resilience"
- "Configurar licencias"

2 Comience a utilizar Ransomware Resilience

Estas tareas requieren el rol de *administrador de resiliencia ante ransomware*.

- "Descubra cargas de trabajo en la consola"
- "Ver el estado de protección de la carga de trabajo en el Panel de control"
- "Opcionalmente, realice un simulacro de preparación para un ataque de ransomware."

3 Configurar la protección y detección en Ransomware Resilience

Estas tareas requieren el rol de *administrador de resiliencia ante ransomware*. Para configurar la actividad de comportamiento de usuario sospechoso se requiere el rol adicional *Administrador de comportamiento de usuario de Ransomware Resilience*.

- "Proteger las cargas de trabajo"
  - Opcionalmente,"Mejore la protección configurando la detección de actividad sospechosa del usuario"
- Opcionalmente, configure los destinos de respaldo:
  - "Prepare NetApp StorageGRID, Amazon Web Services, Google Cloud Platform o Microsoft Azure como destino de respaldo" .
  - "Configurar destinos de respaldo"
- "Responder a la detección de posibles ataques de ransomware"
- "Recuperarse de un ataque (después de que se neutralizan los incidentes)"

4 **¿Que sigue?**

Después de configurar la protección en Ransomware Resilience, esto es lo que puede hacer a continuación.

- "Habilitar la clasificación de datos para identificar riesgos de gobernanza y seguridad"
- "Enviar alertas a SIEM"
- "Descargue informes de alerta, protección, simulacro de preparación, recuperación o resumen"

Configurar NetApp Ransomware Resilience

Puede implementar NetApp Ransomware Resilience fácilmente. Antes de comenzar, revise"prerrequisitos" para garantizar que su entorno esté preparado.

Preparar el destino de la copia de seguridad

Prepare uno de los siguientes destinos de respaldo:

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

Después de configurar las opciones en el destino de la copia de seguridad, más tarde lo configurará como destino de copia de seguridad en Ransomware Resilience. Para obtener detalles sobre cómo configurar el destino de la copia de seguridad en Ransomware Resilience, consulte"Configurar destinos de respaldo" .

Prepare StorageGRID para que se convierta en un destino de respaldo

Si desea utilizar StorageGRID como destino de su copia de seguridad, consulte "Documentación de StorageGRID" para obtener detalles sobre StorageGRID.

Prepare AWS para convertirse en un destino de respaldo

- Configurar una cuenta en AWS.
- Configurar "Permisos de AWS" en AWS.

Para obtener detalles sobre cómo administrar su almacenamiento de AWS en la consola, consulte "Administra tus buckets de Amazon S3" .

Prepare Azure para convertirse en un destino de respaldo

- Configurar una cuenta en Azure.
- Configurar "Permisos de Azure" en Azure.

Para obtener detalles sobre cómo administrar su almacenamiento de Azure en la consola, consulte "Administrar sus cuentas de almacenamiento de Azure" .

Configurar la NetApp Console

El siguiente paso es configurar la consola y la resiliencia contra ransomware.

Revisar "Requisitos de consola para el modo estándar" .

Crear un agente de consola

Comuníquese con su representante de ventas de NetApp para probar o utilizar este servicio. Luego, cuando utilice el agente de consola, incluirá las capacidades adecuadas para la resiliencia ante ransomware.

Para crear un agente de consola mediante Ransomware Resilience, comuníquese con el administrador de su organización de consola que tenga permisos para crear agentes de consola y consulte la documentación que describe "Cómo crear un agente de consola" .

> Si tiene varios agentes de consola, los datos del análisis de resiliencia contra ransomware se recopilan en todos los agentes de consola más allá del que se muestra actualmente en la consola. Este servicio descubre todos los proyectos y todos los agentes de consola asociados con esta organización.

Acceda a la NetApp Ransomware Resilience

Inicie sesión en NetApp Ransomware Resilience 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

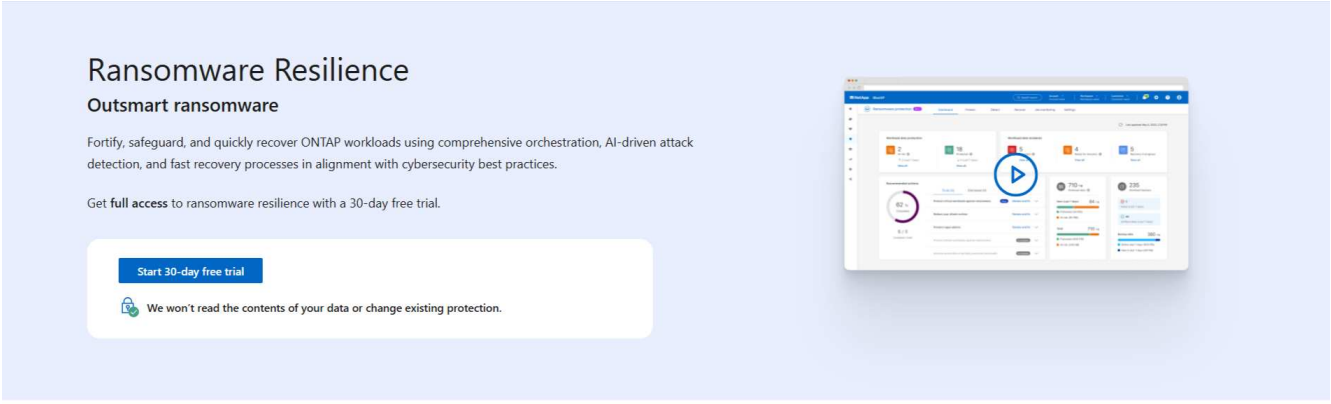
1. Abra un navegador web y vaya a"la consola" .

   Aparece la página de inicio de sesión de la consola.

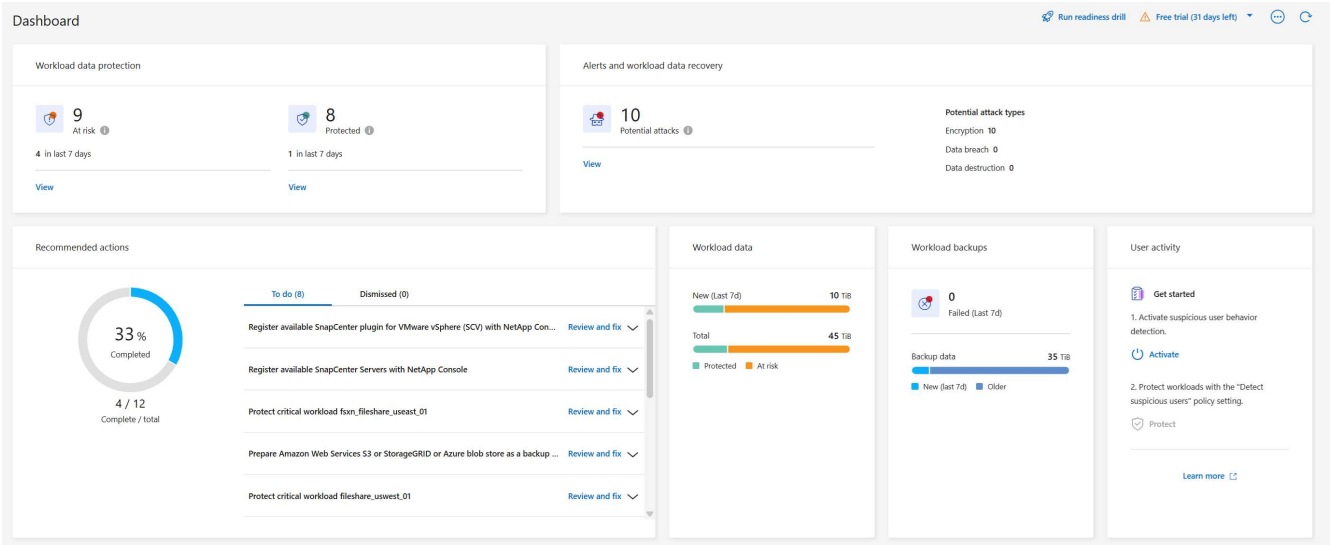
2. Inicie sesión en la consola.
3. Desde la navegación izquierda de la Consola, seleccione **Protección** > **Resiliencia ante ransomware**.

   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" .

Configurar licencias para NetApp Ransomware Resilience

Con NetApp Ransomware Resilience, puede utilizar diferentes planes de licencia.

Para realizar esta tarea, necesita el rol de administrador de organización, carpeta o proyecto. "Obtenga más información sobre los roles de acceso a la consola" .

Tipos de licencia

La resiliencia ante el ransomware está disponible con los siguientes tipos de licencia:

- Prueba gratuita de 30 días
- Compre una suscripción de pago por uso (PAYGO) con Amazon Web Services (AWS) Marketplace, Google Cloud Marketplace o Azure Marketplace
- Traiga su propia licencia (BYOL): un archivo de licencia de NetApp (NLF) que obtiene de su representante de ventas de NetApp . Puede utilizar el número de serie de la licencia para activar el BYOL en la consola.

Después de configurar su BYOL o comprar una suscripción PAYGO, podrá ver la licencia en la sección Licenses and subscriptions de la Consola.

Una vez finalizada la prueba gratuita o vencida la licencia o suscripción, aún puedes:

- Ver cargas de trabajo y el estado de las cargas de trabajo
- Eliminar recursos como políticas
- Ejecute todas las operaciones programadas creadas durante el período de prueba o bajo la licencia

Otras licencias

La licencia Ransomware Resilience no incluye productos NetApp adicionales. Sin embargo, Ransomware Resilience puede integrarse con NetApp Backup and Recovery, incluso si no tiene una licencia separada para Backup and Recovery.

Si tiene Backup and Recovery y Ransomware Resilience, cualquier dato común protegido por ambos productos se facturará únicamente por Ransomware Resilience.

Pruebe Ransomware Resilience con una prueba gratuita de 30 días

Puedes probar Ransomware Resilience con una prueba gratuita de 30 días. Debes ser administrador de la organización de la consola para comenzar la prueba gratuita.

Los límites de capacidad de almacenamiento no se aplican durante la prueba.

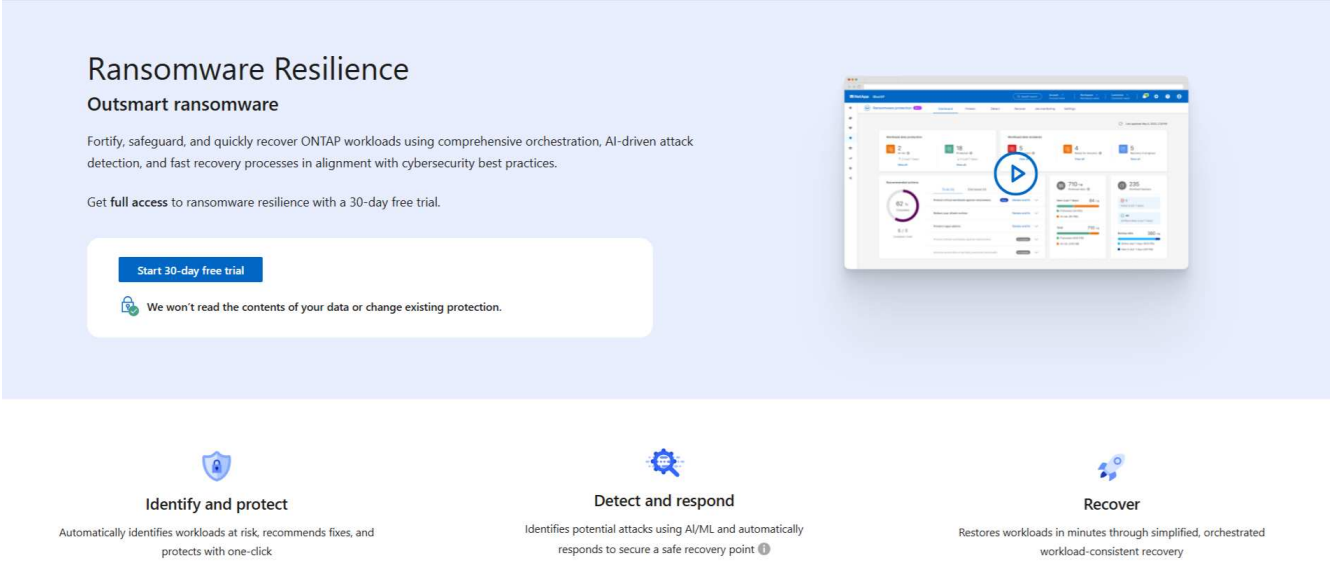
Puede obtener una licencia o suscribirse en cualquier momento y no se le cobrará hasta que finalice la prueba de 30 días. Para continuar después de la prueba de 30 días, deberá comprar una licencia BYOL o una suscripción PAYGO.

Durante la prueba, tendrás acceso a todas las funciones.

Pasos

1. Acceder a la "Consola" .
2. Inicie sesión en la consola.
3. Desde la NetApp Console, seleccione **Protección** > **Resiliencia contra ransomware**.

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



4. Si aún no ha agregado un agente de consola para otros servicios,"añadir uno" .
5. En la página de inicio de Resiliencia contra ransomware, seleccione **Comenzar por descubrir cargas de trabajo** para descubrir sus cargas de trabajo.

   Esta opción solo está disponible si ha instalado correctamente un agente de consola.

6. Para revisar la información de la prueba gratuita, seleccione la opción desplegable en la parte superior derecha.

Una vez finalizada la prueba, obtén una suscripción o licencia

Una vez finalizada la prueba gratuita, puedes suscribirte a través de uno de los Marketplaces o comprar una licencia de NetApp.

Si ya tiene una suscripción PAYGO, la licencia se cambia automáticamente a la suscripción una vez finalizada la prueba gratuita.

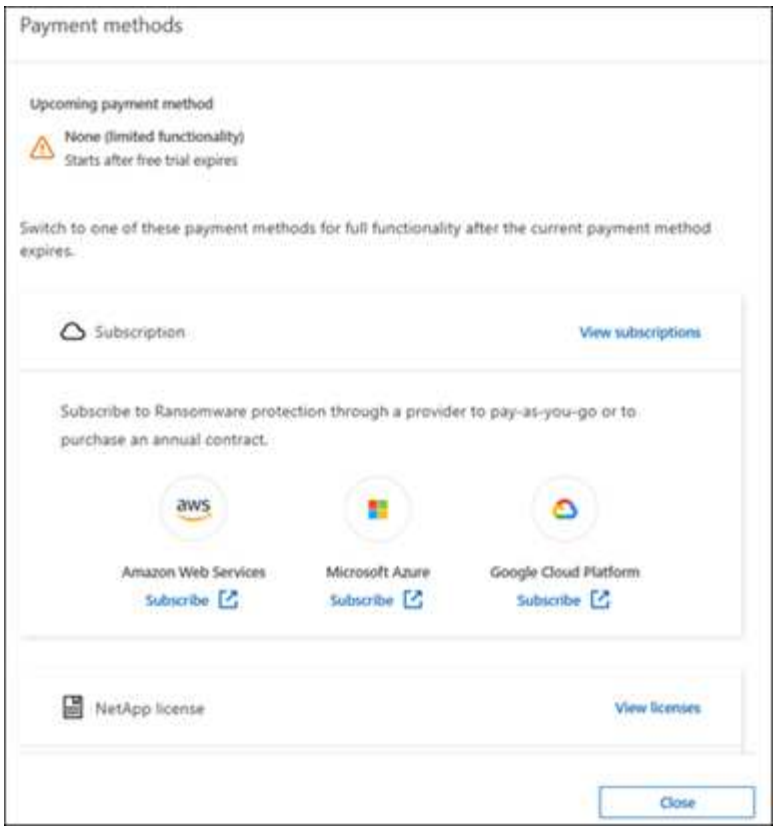
Suscríbete a través de AWS Marketplace Suscríbete a través de Microsoft Azure Marketplace Suscríbete a través de Google Cloud Platform Marketplace Traiga su propia licencia (BYOL)

Suscríbete a través de AWS Marketplace

Este procedimiento proporciona una descripción general de alto nivel sobre cómo suscribirse directamente en AWS Marketplace.

Pasos

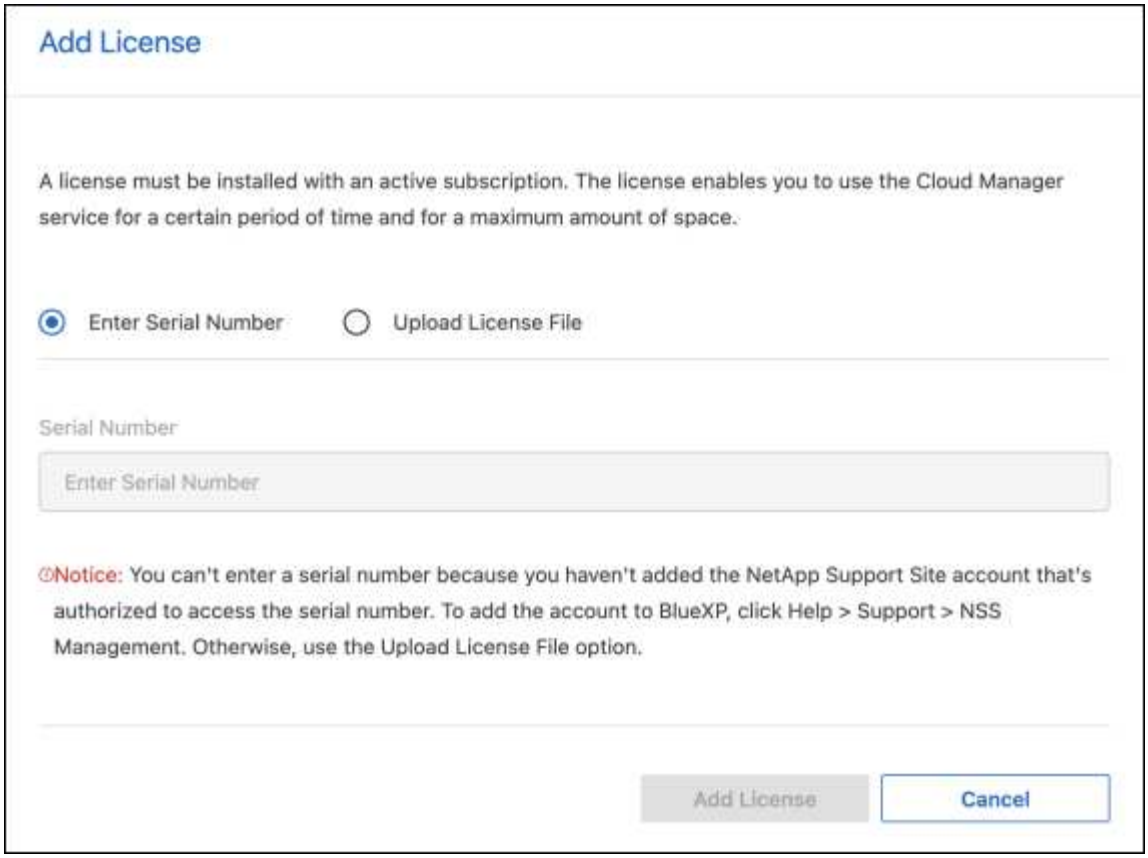
1. En Ransomware Resilience, realice una de las siguientes acciones:
   - Si aparece un mensaje que indica que la prueba gratuita está por vencer, seleccione **Ver métodos de pago**.
   - Si aún no ha comenzado la prueba, seleccione el aviso **Prueba gratuita** en la parte superior derecha y luego **Ver métodos de pago**.



2. En la página de Métodos de pago, seleccione **Suscribirse** a **Amazon Web Services**.
3. En AWS Marketplace, seleccione **Ver opciones de compra**.
4. Utilice AWS Marketplace para suscribirse a * NetApp Intelligent Services* y * Ransomware Resilience *.
5. Cuando regresa a Ransomware Resilience, un mensaje indica que está suscrito.

> Se le envía un correo electrónico que incluye el número de serie de Ransomware Resilience e indica que Ransomware Resilience está suscrito en AWS Marketplace.

6. Regresar a la página de métodos de pago de Ransomware Resilience.
7. Agregue la licencia a la Consola seleccionando **Agregar licencia**.



8. En la página Agregar licencia, seleccione **Ingresar número de serie**, ingrese el número de serie que se incluyó en el correo electrónico que le enviamos y luego seleccione **Agregar licencia**.
9. Para ver los detalles de la licencia, desde la navegación izquierda de la Consola, seleccione **Administración** > * Licenses and subscriptions*.
   - Para ver la información de la suscripción, seleccione **Suscripciones**.
   - Para ver las licencias BYOL, seleccione **Licencias de servicios de datos**.
10. Regresar a Resiliencia frente al ransomware. Desde la navegación izquierda de la Consola, seleccione **Protección** > **Resiliencia ante ransomware**.

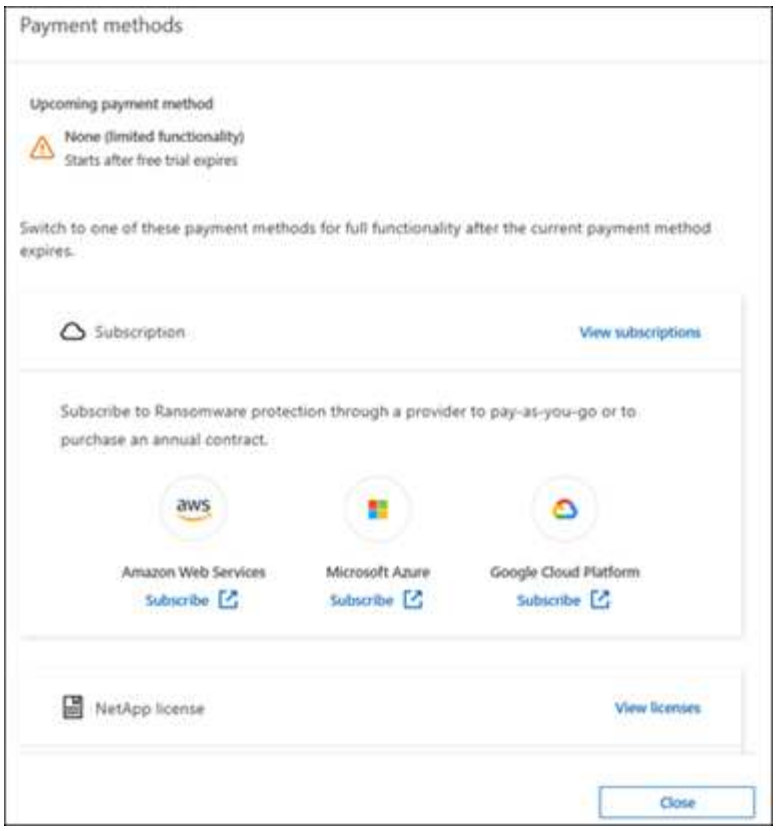
    Un mensaje confirma que se ha agregado una licencia.

Suscríbete a través de Microsoft Azure Marketplace

Este procedimiento proporciona una descripción general de alto nivel sobre cómo suscribirse directamente en Azure Marketplace.

Pasos

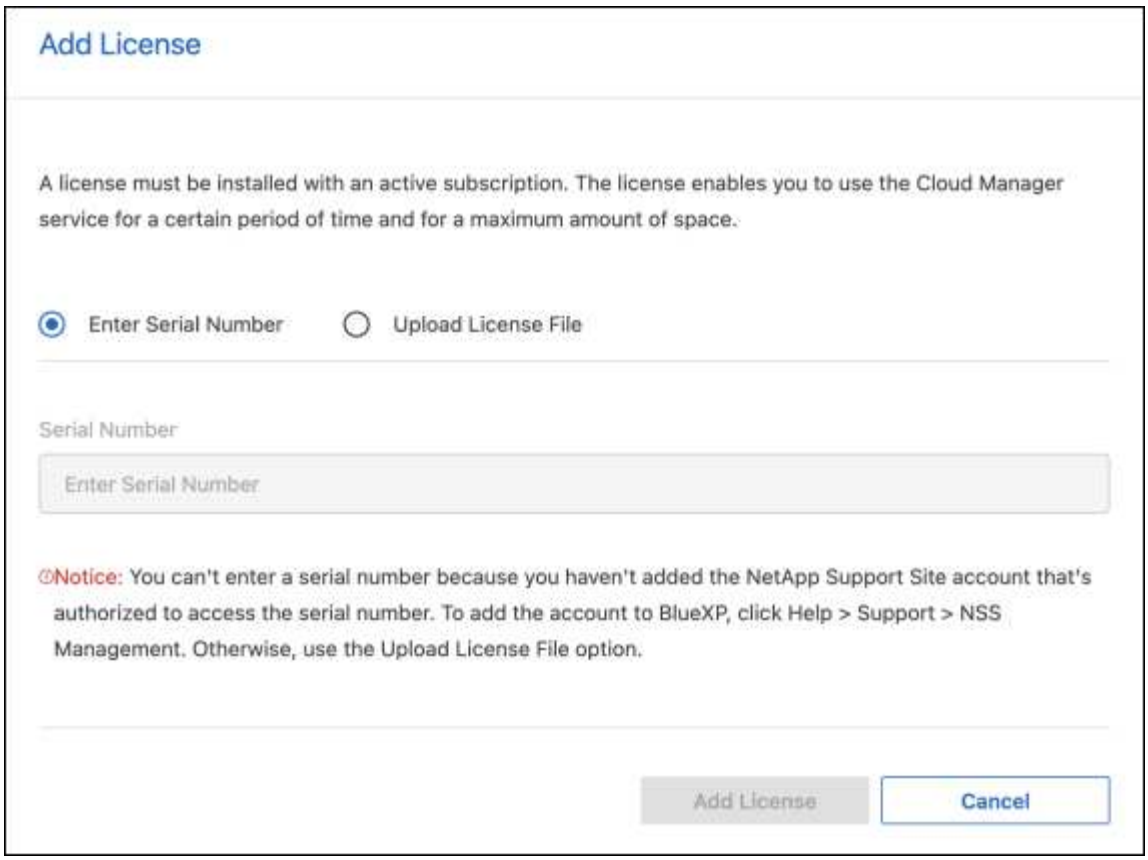
1. En Ransomware Resilience, realice una de las siguientes acciones:
   - Si aparece un mensaje que indica que la prueba gratuita está por vencer, seleccione **Ver métodos de pago**.
   - Si aún no ha comenzado la prueba, seleccione el aviso **Prueba gratuita** en la parte superior derecha y luego **Ver métodos de pago**.



2. En la página Métodos de pago, seleccione **Suscribirse** para **Microsoft Azure Marketplace**.
3. En Azure Marketplace, seleccione **Ver opciones de compra**.
4. Utilice Azure Marketplace para suscribirse a * NetApp Intelligent Services* y * Ransomware Resilience *.
5. Cuando regresa a Ransomware Resilience, un mensaje indica que está suscrito.

> Se le envía un correo electrónico que incluye el número de serie de Ransomware Resilience e indica que Ransomware Resilience está suscrito en Azure Marketplace.

6. Regresar a la página de Métodos de pago de Ransomware Resilience.
7. Para agregar la licencia, seleccione **Agregar una licencia**.



8. En la página Agregar licencia, seleccione **Ingresar número de serie** y luego ingrese el número de serie en el correo electrónico que le enviamos. Seleccione **Agregar licencia**.
9. Para ver los detalles de la licencia en Licenses and subscriptions, desde la navegación izquierda de la Consola, seleccione **Gobernanza** > * Licenses and subscriptions*.
   - Para ver la información de la suscripción, seleccione **Suscripciones**.
   - Para ver las licencias BYOL, seleccione **Licencias de servicios de datos**.
10. Regresar a Resiliencia frente al ransomware. Desde la navegación izquierda de la Consola, seleccione **Protección** > **Resiliencia ante ransomware**.

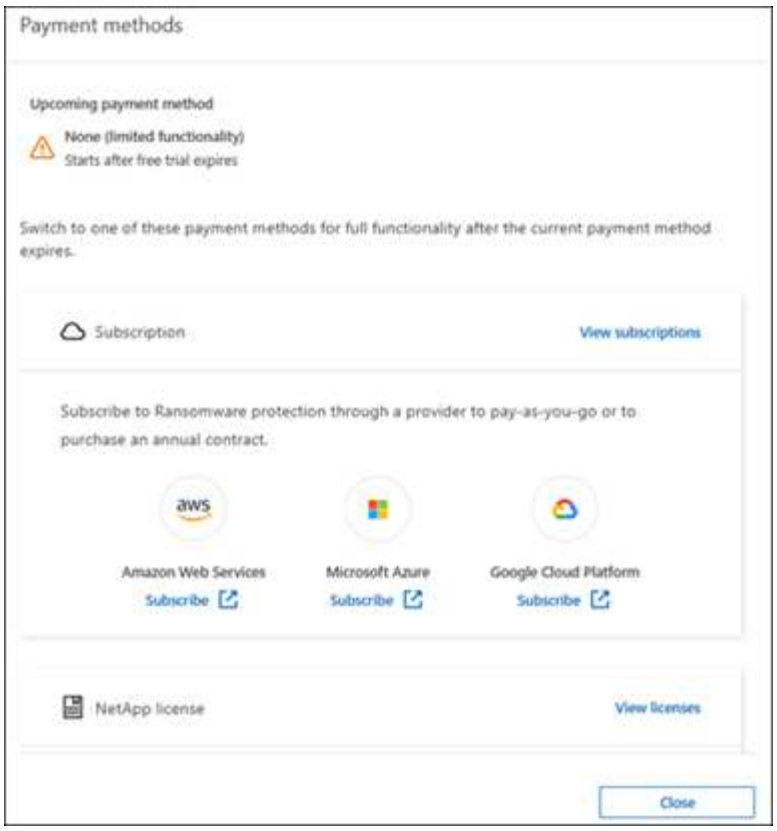
    Aparece un mensaje indicando que se ha añadido una licencia.

Suscríbete a través de Google Cloud Platform Marketplace

Este procedimiento proporciona una descripción general de alto nivel sobre cómo suscribirse directamente en Google Cloud Platform Marketplace.

Pasos

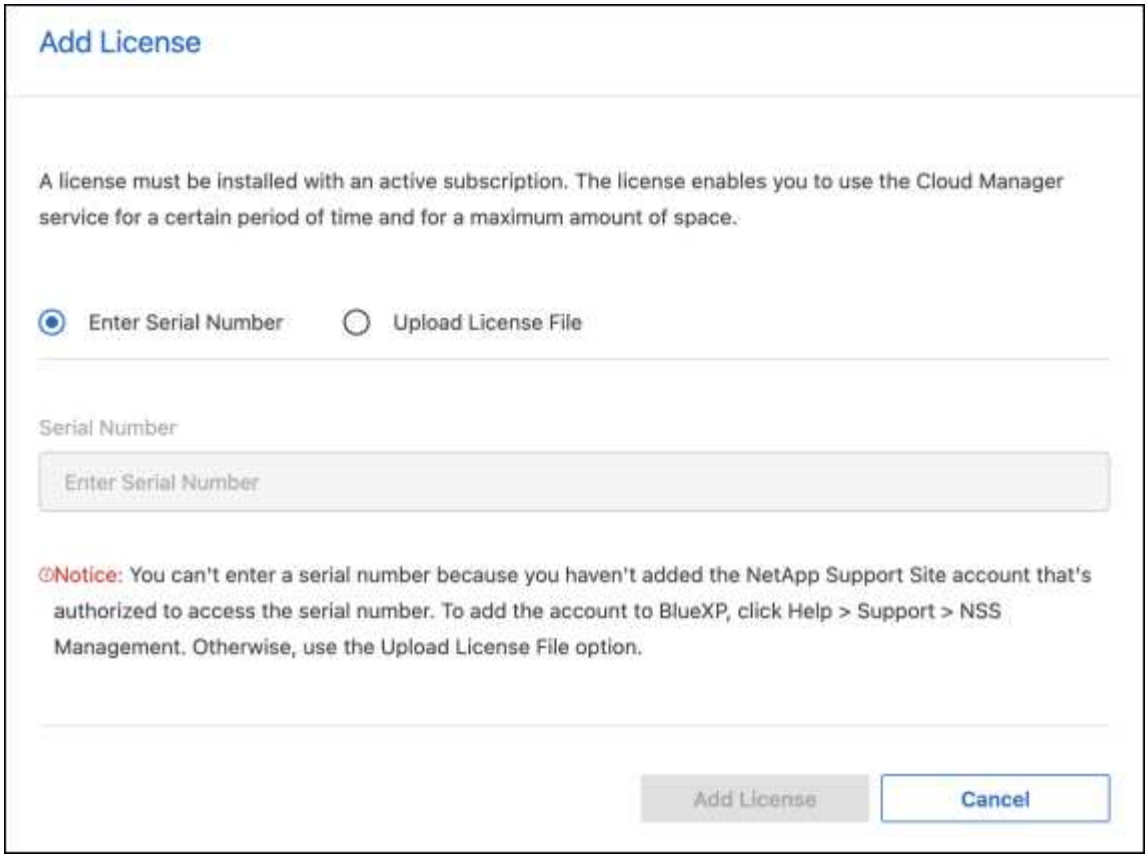
1. En Ransomware Resilience, realice una de las siguientes acciones:
   - Si aparece un mensaje que indica que la prueba gratuita está por vencer, seleccione **Ver métodos de pago**.
   - Si aún no ha comenzado la prueba, seleccione el aviso **Prueba gratuita** en la parte superior derecha y luego **Ver métodos de pago**.



2. En la página Métodos de pago, seleccione **Suscribirse** a Google Cloud Platform Marketplace*.
3. En Google Cloud Platform Marketplace, seleccione **Suscribirse**.
4. Utilice Google Cloud Platform Marketplace para suscribirse a * NetApp Intelligent Services* y * Ransomware Resilience *.
5. Cuando regresa a Ransomware Resilience, un mensaje indica que está suscrito.

> Se le envía un correo electrónico que incluye el número de serie de Ransomware Resilience e indica que Ransomware Resilience está suscrito en Google Cloud Platform Marketplace.

6. Regresar a la página de Métodos de pago de Ransomware Resilience.
7. Para agregar la licencia a la Consola, seleccione **Agregar licencia**.



8. En la página Agregar licencia, seleccione **Ingresar número de serie**. Introduzca el número de serie en el correo electrónico que le enviamos. Seleccione **Agregar licencia**.
9. Para ver los detalles de la licencia, desde la navegación izquierda de la Consola, seleccione **Gobernanza** > * Licenses and subscriptions*.
   - Para ver la información de la suscripción, seleccione **Suscripciones**.
   - Para ver las licencias BYOL, seleccione **Licencias de servicios de datos**.
10. Regresar a Resiliencia frente al ransomware. Desde la navegación izquierda de la Consola, seleccione **Protección** > **Resiliencia ante ransomware**.

    Aparece un mensaje indicando que se ha añadido una licencia.

Traiga su propia licencia (BYOL)

Si desea traer su propia licencia (BYOL), debe comprar la licencia, obtener el archivo de licencia de NetApp (NLF) y luego agregar la licencia a la consola.

Agregue su archivo de licencia a la consola

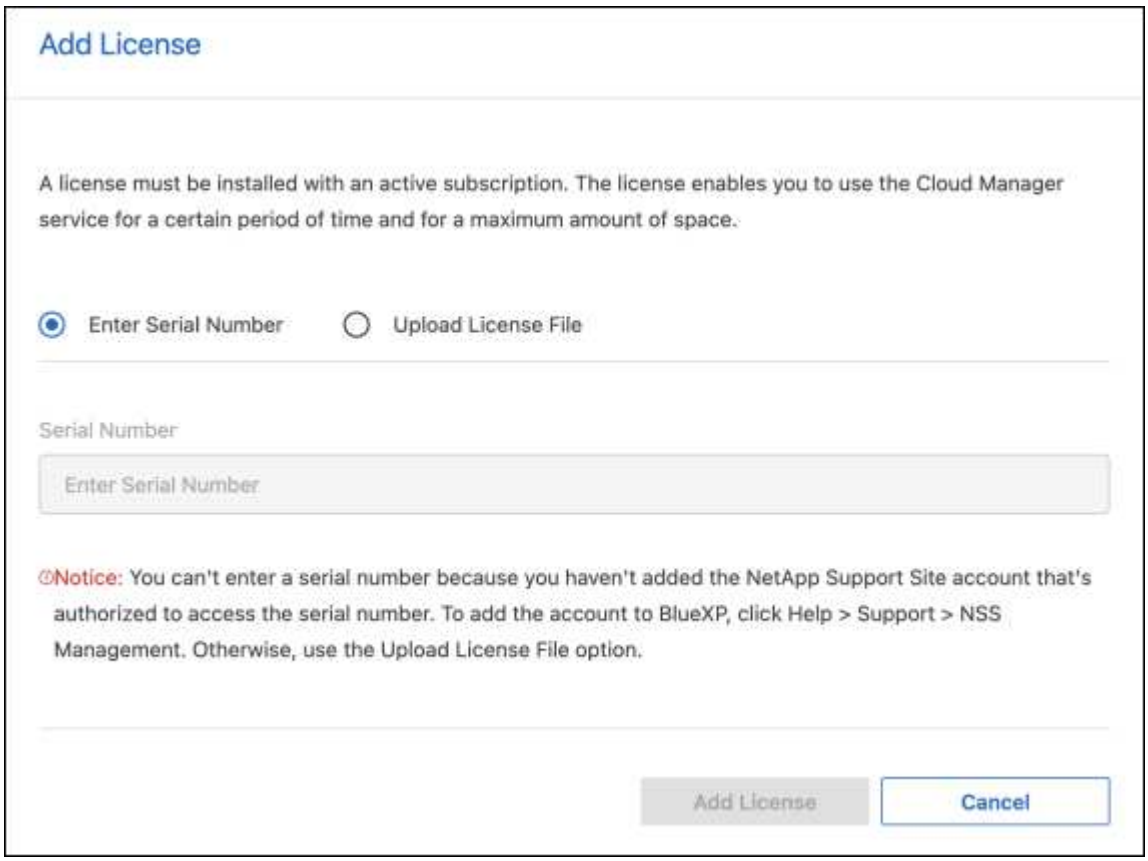
Una vez que haya comprado su licencia de Ransomware Resilience a su representante de ventas de NetApp , active la licencia ingresando el número de serie de Ransomware Resilience y la información de la cuenta del sitio de soporte de NetApp (NSS).

Antes de empezar

Necesita el número de serie de Ransomware Resilience. Localice este número en su orden de venta o comuníquese con el equipo de cuentas para obtener esta información.

Pasos

1. Después de obtener la licencia, regrese a Ransomware Resilience. Seleccione la opción **Ver métodos de pago** en la parte superior derecha. O bien, en el mensaje que indica que la prueba gratuita está por vencer, seleccione **Suscribirse o comprar una licencia**.
2. Seleccione **Agregar licencia** para ir a la página de Licencias y suscripciones de la consola.
3. Desde la pestaña **Licencias de servicios de datos**, seleccione **Agregar licencia**.



4. En la página Agregar licencia, ingrese el número de serie y la información de la cuenta del sitio de soporte de NetApp .
   - Si tiene el número de serie de la licencia de la consola y conoce su cuenta NSS, seleccione la opción **Ingresar número de serie** e ingrese esa información.

     Si su cuenta del sitio de soporte de NetApp no está disponible en la lista desplegable, "Agregue la cuenta NSS a la consola" .

   - Si tiene el archivo de licencia de zvondolr (necesario cuando se instala en un sitio oscuro), seleccione la opción **Cargar archivo de licencia** y siga las instrucciones para adjuntar el archivo.
5. Seleccione **Agregar licencia**.

Resultado

La página Licenses and subscriptions muestra que Ransomware Resilience tiene una licencia.

Actualice su licencia de consola cuando caduque

Si su período de licencia está cerca de la fecha de vencimiento, o si su capacidad de licencia está llegando al límite, se le notificará en la interfaz de usuario de resiliencia ante ransomware. Puede actualizar su licencia de

Ransomware Resilience antes de que expire para que no haya interrupciones en su capacidad de acceder a sus datos escaneados.

Este mensaje también aparece en Licenses and subscriptions y en "Configuración de notificaciones" .

Pasos

1. Puede enviar un correo electrónico al soporte para solicitar una actualización de su licencia.

   Una vez que paga la licencia y la registra en el sitio de soporte de NetApp , la consola actualiza automáticamente la licencia. La página de Licencias de Servicios de Datos reflejará el cambio en 5 a 10 minutos.

2. Si la consola no puede actualizar automáticamente la licencia, deberá cargar manualmente el archivo de licencia.
   a. Puede obtener el archivo de licencia en el sitio de soporte de NetApp .
   b. En la consola, seleccione **Administración** > **Licenses and subscriptions**.
   c. Seleccione la pestaña **Licencias de servicios de datos**, seleccione el ícono **Acciones…** para el número de serie que está actualizando y luego seleccione **Actualizar licencia**.

Finalizar la suscripción PAYGO

Si desea finalizar su suscripción PAYGO, puede hacerlo en cualquier momento.

Pasos

1. En Ransomware Resilience, en la parte superior derecha, seleccione la opción de licencia.
2. Seleccione **Ver métodos de pago**.
3. En los detalles desplegables, desmarque la casilla **Usar después de que expire el método de pago actual**.
4. Seleccione **Guardar**.

Descubra las cargas de trabajo en NetApp Ransomware Resilience

Antes de poder utilizar NetApp Ransomware Resilience, primero debe descubrir datos. Durante el descubrimiento, Ransomware Resilience analiza todos los volúmenes y archivos de los sistemas en todos los agentes de la consola y proyectos dentro de una organización.

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" .

¿Qué descubre Ransomware Resilience? Ransomware Resilience evalúa aplicaciones Oracle, almacenes de datos VMware, recursos compartidos de archivos y almacenamiento en bloques.

Ransomware Resilience no descubre cargas de trabajo con volúmenes que utilizan FlexGroup.

Ransomware Resilience descubre y muestra configuraciones del sistema compatibles y no compatibles en el Panel de control.

Ransomware Resilience verifica su protección de respaldo actual, copias instantáneas y opciones de protección autónoma contra ransomware de NetApp . Luego recomienda formas de mejorar su protección contra ransomware.

¿Cómo puedes descubrir las cargas de trabajo? Puedes hacer lo siguiente:

- Dentro de cada agente de consola, seleccione los sistemas en los que desea descubrir cargas de trabajo. Esta función puede resultarle beneficiosa si desea proteger cargas de trabajo específicas en su entorno y no otras.
- Descubra cargas de trabajo recién creadas para sistemas previamente seleccionados.
- Descubra nuevos sistemas.

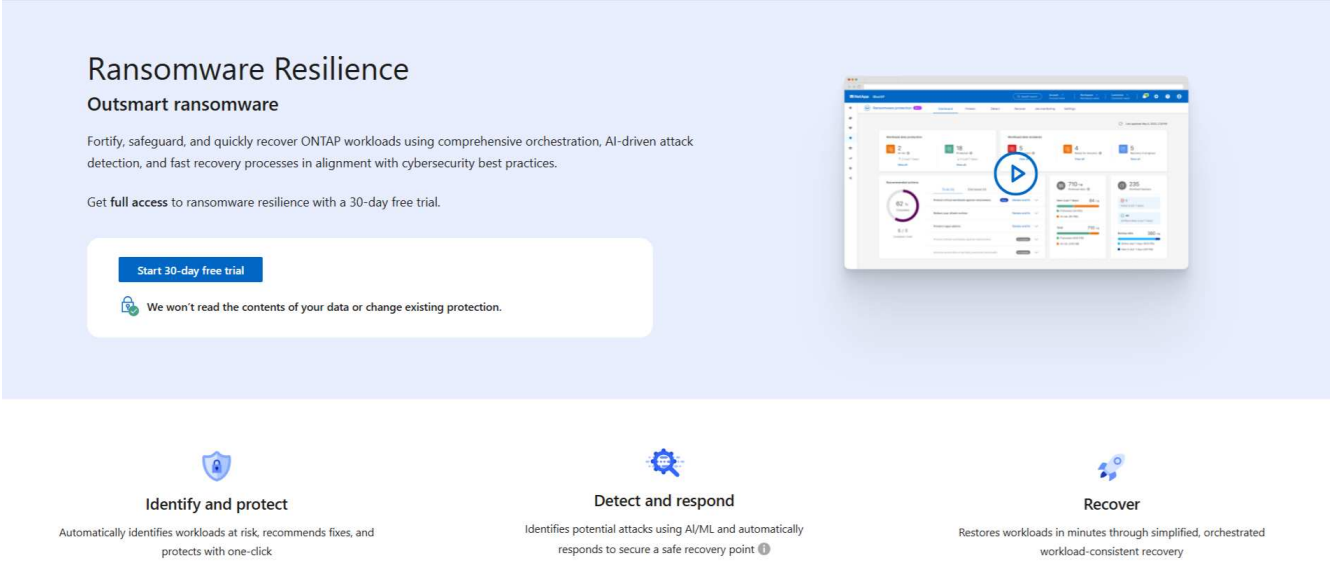
Seleccione cargas de trabajo para descubrir y proteger

Dentro de cada agente de consola, seleccione los sistemas en los que desea descubrir cargas de trabajo.

Pasos

1. Desde la NetApp Console, seleccione **Protección** > **Protección contra ransomware**.

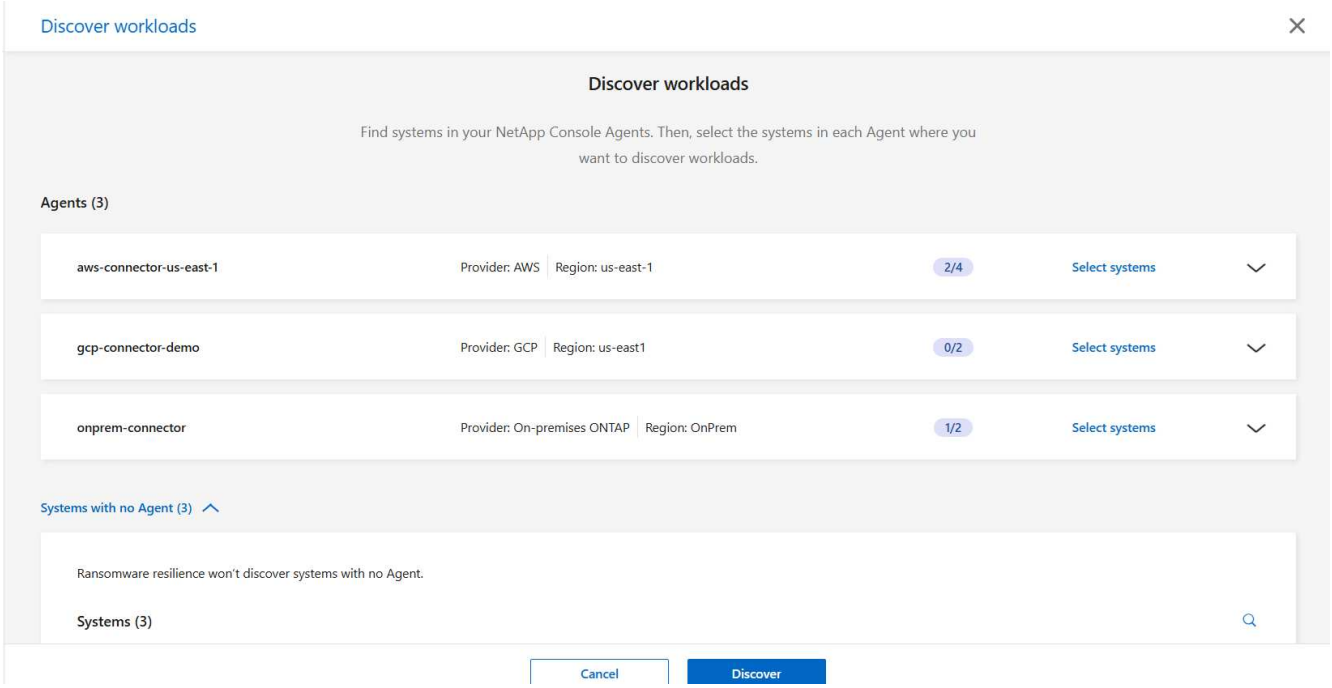
   Si este es su primer inicio de sesión, aparecerá la página de destino.



   Si inició la prueba gratuita, la etiqueta del botón **Iniciar prueba gratuita de 30 días** cambia a **Comenzar descubriendo cargas de trabajo**.

2. Desde la página de destino inicial, seleccione **Comenzar por descubrir cargas de trabajo**.

   Ransomware Resilience encuentra sistemas compatibles y no compatibles. Este proceso puede tardar unos minutos.

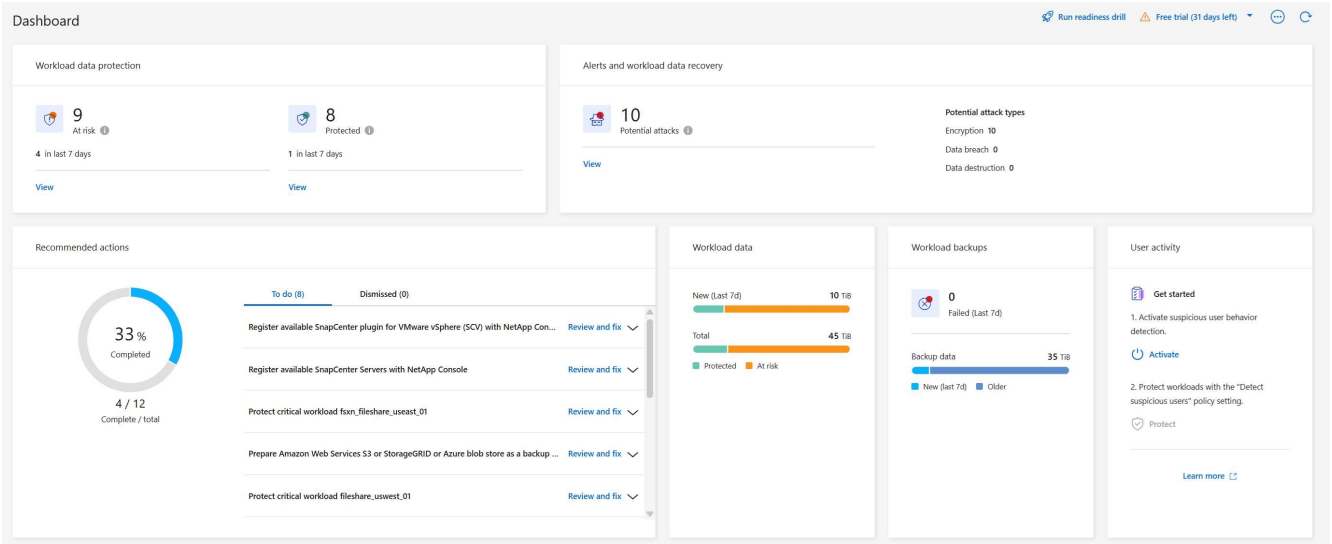


3. Para descubrir cargas de trabajo para un agente de consola específico, seleccione **Seleccionar sistemas** junto al agente de consola donde desea descubrir cargas de trabajo.
4. Seleccione los sistemas en los que desea descubrir cargas de trabajo.
5. Seleccione **Descubrir**.

   Ransomware Resilience descubre datos de carga de trabajo solo para aquellos agentes de consola con sistemas seleccionados. Este proceso puede tardar unos minutos.

6. Para descargar la lista de cargas de trabajo descubiertas, seleccione **Descargar resultados**.
7. Para mostrar el panel de resiliencia ante ransomware, seleccione **Ir al panel**.

   El panel de control muestra el estado de la protección de datos. La cantidad de cargas de trabajo protegidas o en riesgo se actualiza a medida que se descubren nuevas cargas de trabajo.



"Descubra lo que le muestra el Dashboard."

Descubra cargas de trabajo recién creadas para sistemas previamente seleccionados

Si ya ha seleccionado sistemas para el descubrimiento, puede descubrir cargas de trabajo recién creadas para esos entornos desde el Panel de control.

Pasos

1. Para identificar la fecha del último descubrimiento, observe la fecha y la hora junto al ícono **Actualizar** en la parte superior derecha del panel de resiliencia ante ransomware.
2. Desde el Panel de control, seleccione el **ícono Actualizar** para buscar nuevas cargas de trabajo.

Descubra nuevos sistemas

Si ya has descubierto sistemas, podrás encontrar otros nuevos o no seleccionados anteriormente.

Pasos

1. En el menú Resiliencia contra ransomware, seleccione la vertical  …opción en la parte superior derecha. En el menú desplegable, seleccione **Configuración**.
2. En la tarjeta Descubrimiento de carga de trabajo, seleccione **Descubrir cargas de trabajo**.

    Este proceso puede tardar unos minutos y un ícono de carga muestra el progreso.

3. Ransomware Resilience descubre sistemas compatibles y no compatibles. Ransomware Resilience no admite un sistema si su versión de ONTAP es inferior a la versión requerida. Cuando pasa el cursor sobre un sistema no compatible, aparece una información sobre herramientas que muestra el motivo. Seleccione los sistemas en los que desea descubrir cargas de trabajo.
4. Seleccione **Descubrir**.

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.

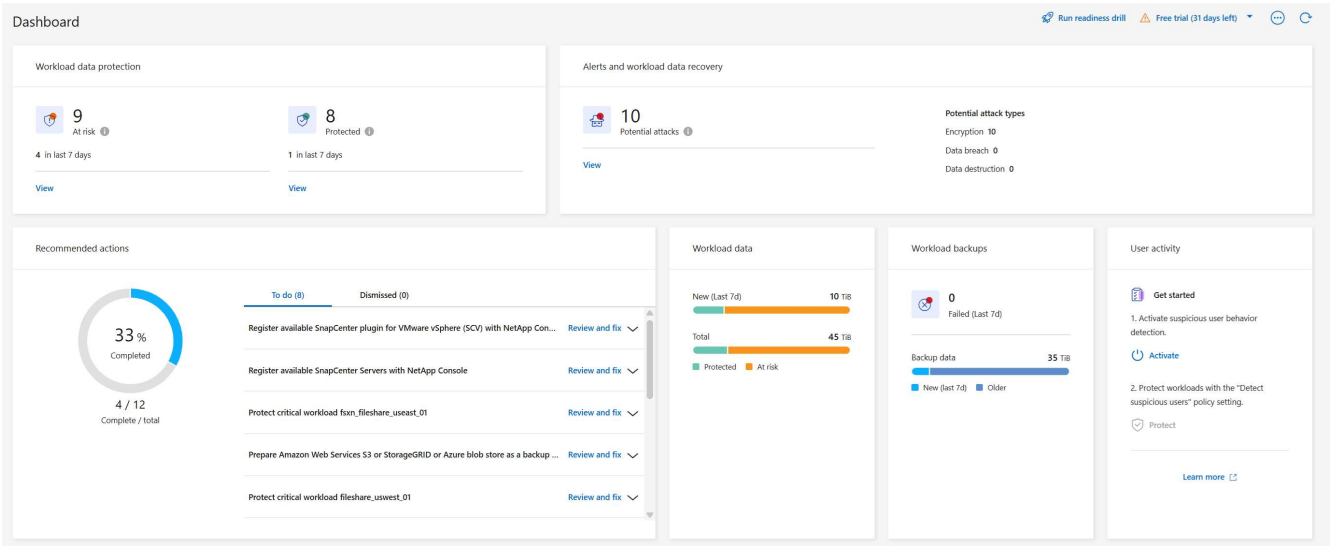
Debe ingresar un nombre de usuario y contraseña para las siguientes situaciones:

- 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" .

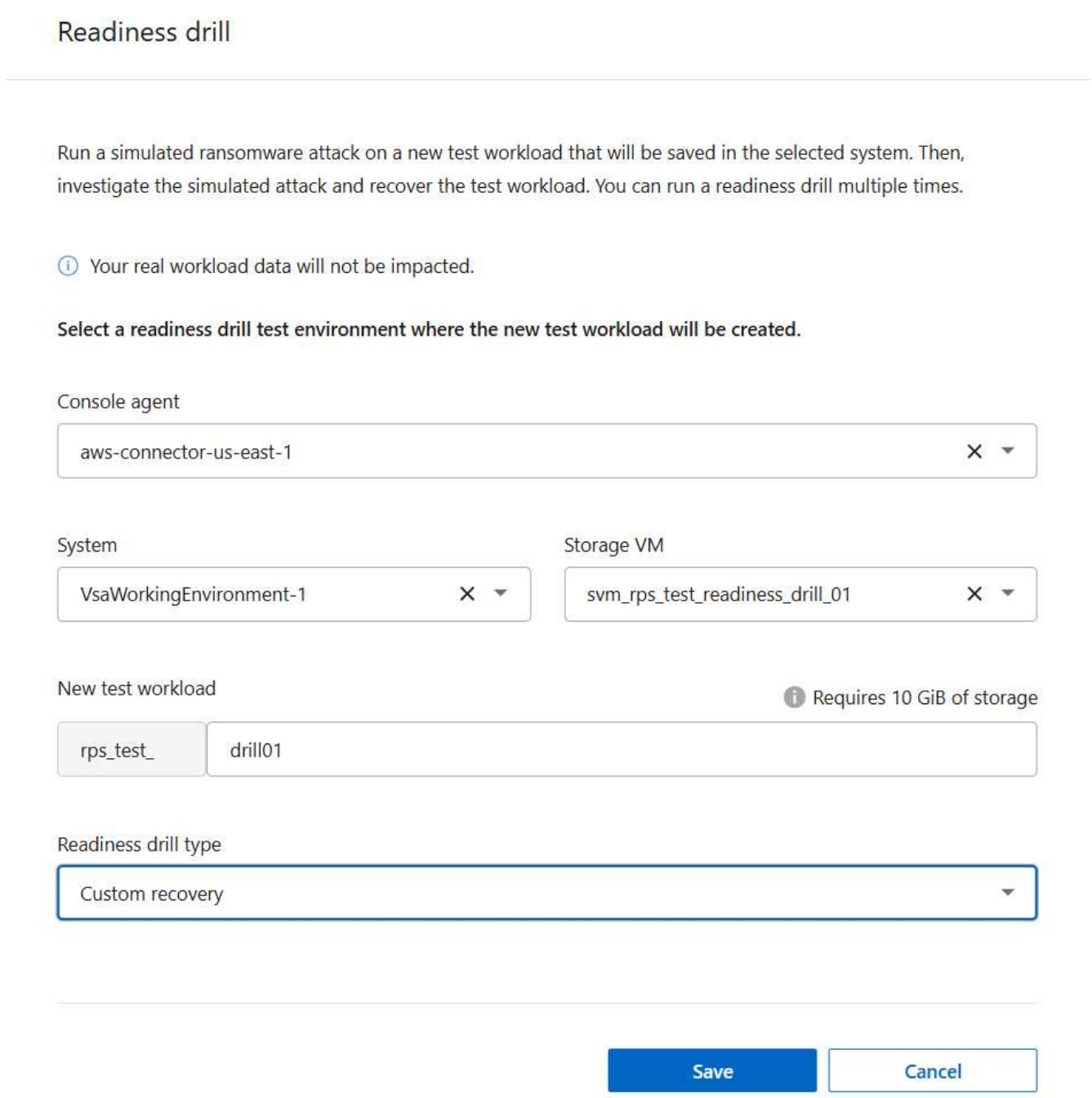
Pasos

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.

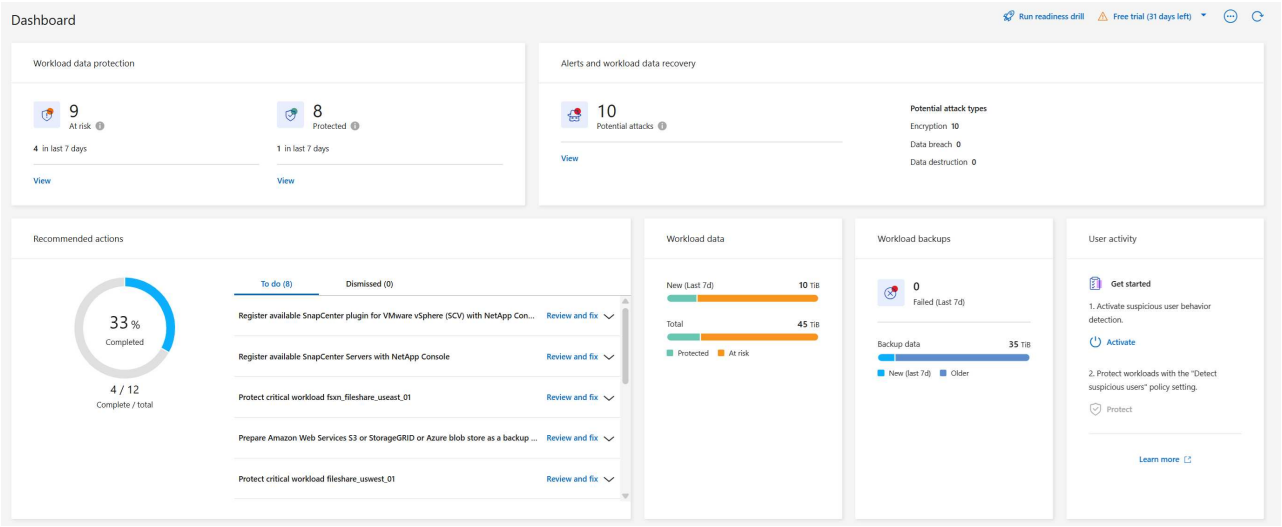
Rol de consola requerido Para realizar esta tarea, necesita el rol de administrador de organización, administrador de carpeta o proyecto, o administrador de resiliencia ante ransomware. "Obtenga información sobre las funciones de resiliencia ante ransomware para la NetApp Console" .

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

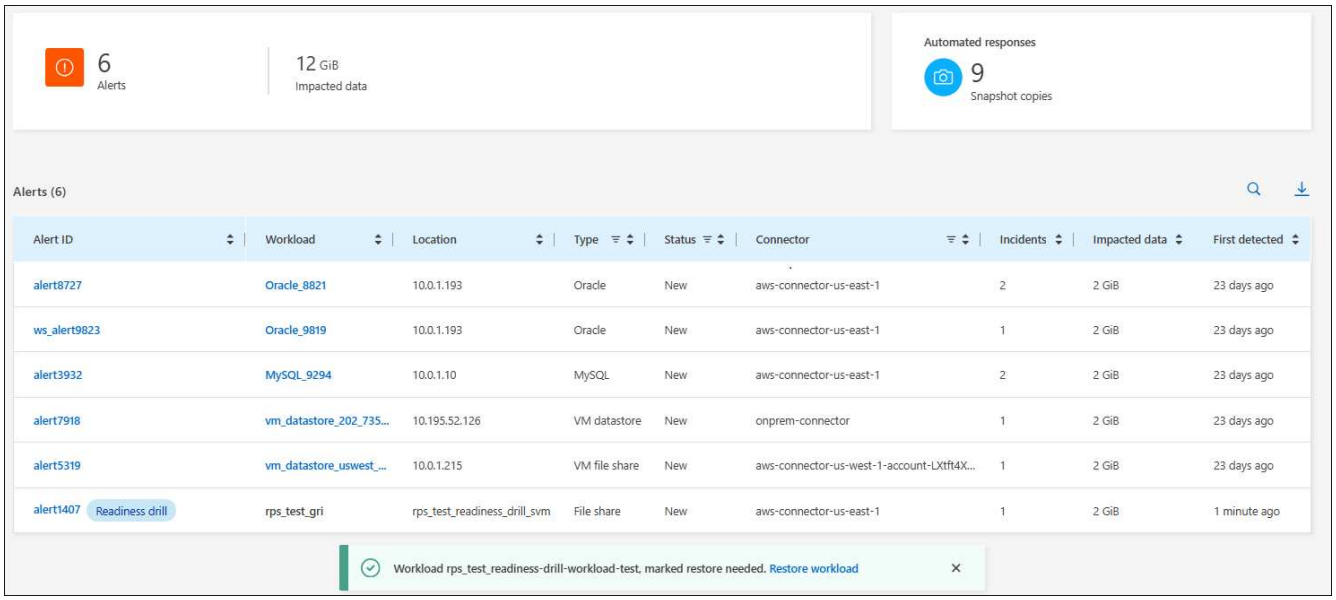
Pon a prueba tu preparación respondiendo a una alerta de simulacro de preparación.

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" .

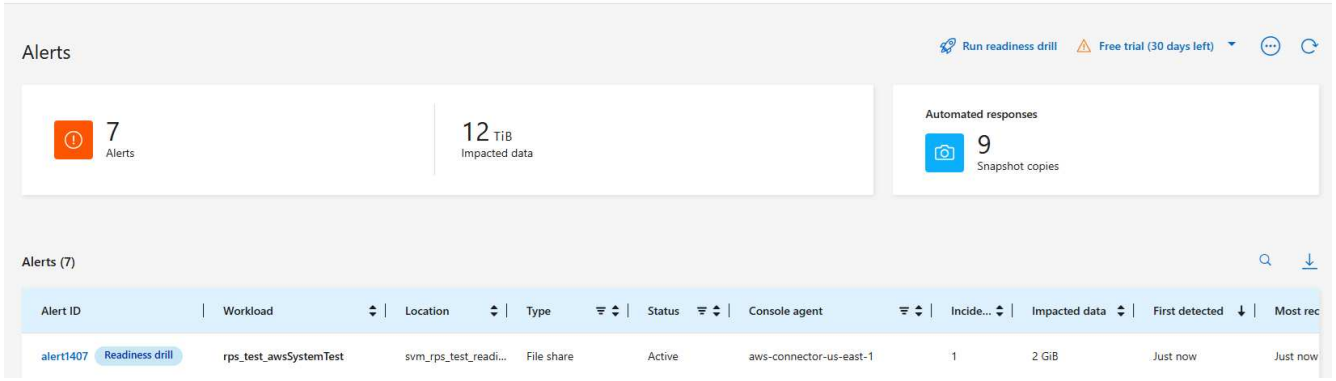
Pasos

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

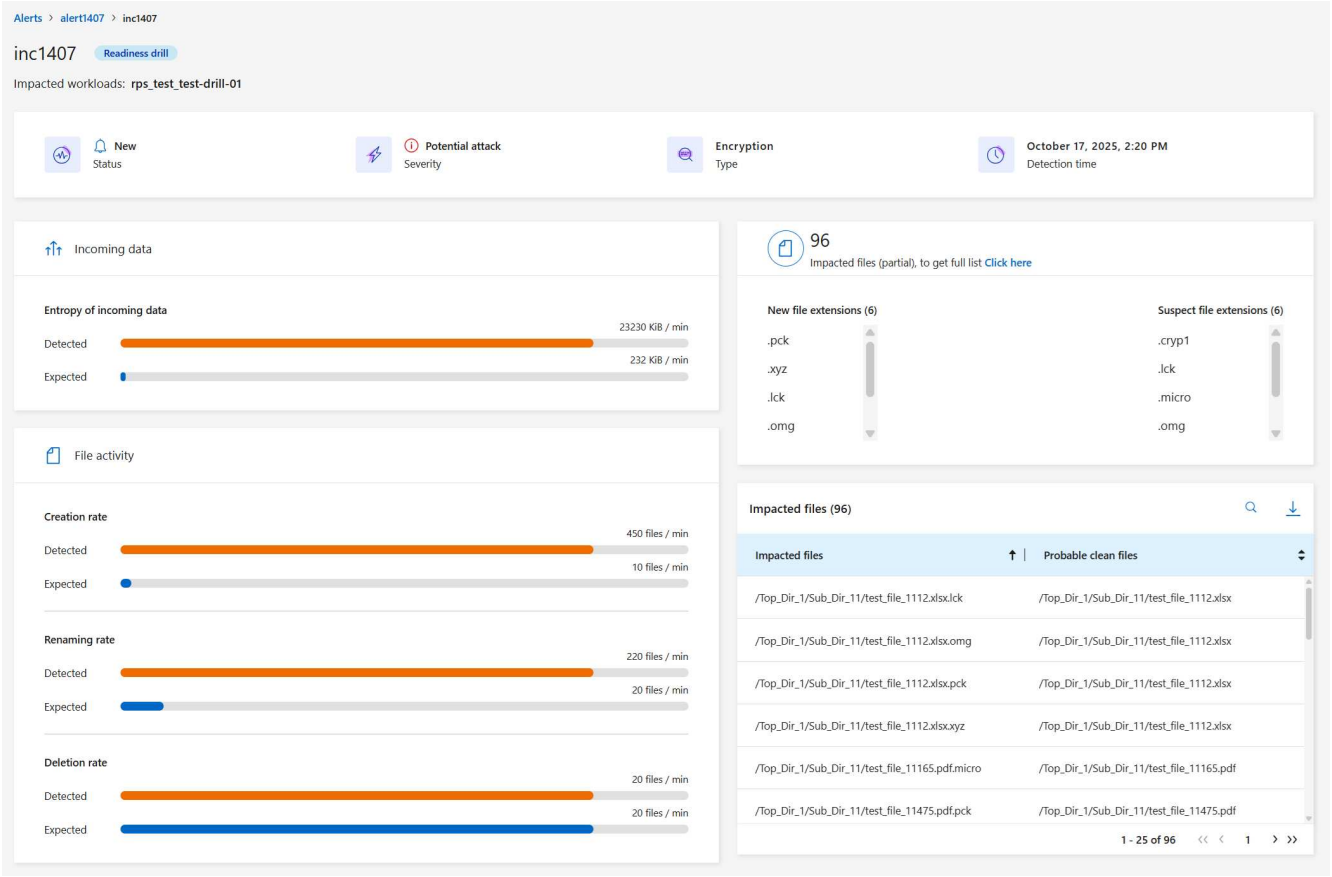
   La consola muestra la página Alertas. En la columna ID de alerta, verá "Simulacro de preparación" junto al ID.



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.

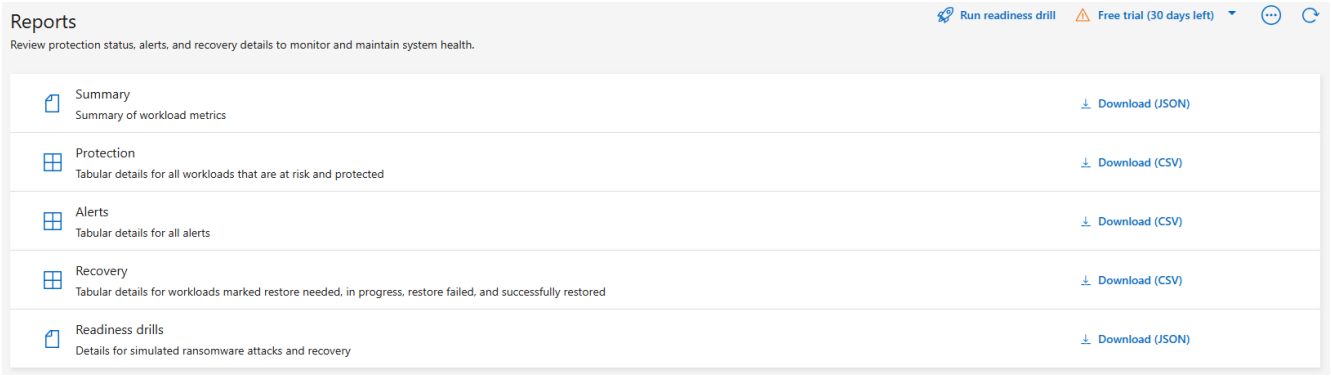
Revisar los informes sobre el simulacro de preparación

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.

Configurar los ajustes de protección en NetApp Ransomware Resilience

Puede configurar destinos de respaldo, enviar datos a un sistema externo de seguridad y gestión de eventos (SIEM), realizar un simulacro de preparación para ataques, configurar el descubrimiento de carga de trabajo o configurar la detección de actividad sospechosa de usuarios accediendo a la opción **Configuración**.

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" .

¿Qué puedes hacer en la página de Configuración? Desde la página de Configuración, puede hacer lo siguiente:

- Simule un ataque de ransomware realizando un simulacro de preparación y responda a una alerta de ransomware simulada. Para obtener más información, consulte "Realizar un simulacro de preparación para un ataque de ransomware" .
- Configurar la detección de carga de trabajo.
- Configurar el informe de actividad de usuarios sospechosos.
- Agregar un destino de respaldo.
- Conecte su sistema de gestión de eventos y seguridad (SIEM) para el análisis y detección de amenazas. Al habilitar la detección de amenazas, se envían automáticamente datos a su SIEM para el análisis de

amenazas.

Acceda directamente a la página de Configuración

Puede acceder fácilmente a la página de Configuración desde la opción Acciones cerca del menú superior.

1. Desde Resiliencia contra el ransomware, seleccione la vertical  …opción en la parte superior derecha.
2. En el menú desplegable, seleccione **Configuración**.

Simular un ataque de ransomware

Realice un simulacro de preparación ante ransomware simulando un ataque de ransomware en una carga de trabajo de muestra recién creada. Luego, investigue el ataque simulado y recupere la carga de trabajo de muestra. Esta función le ayuda a saber que está preparado en caso de un ataque de ransomware real al probar los procesos de notificación de alerta, respuesta y recuperación. Puede ejecutar un simulacro de preparación ante ransomware varias veces.

Para más detalles, consulte"Realizar un simulacro de preparación para un ataque de ransomware" .

Configurar el descubrimiento de carga de trabajo

Puede configurar la detección de cargas de trabajo para descubrir automáticamente nuevas cargas de trabajo en su entorno.

1. En la página Configuración, ubique el mosaico **Descubrimiento de carga de trabajo**.
2. En el mosaico **Descubrimiento de carga de trabajo**, seleccione **Descubrir cargas de trabajo**.

   Esta página muestra agentes de consola con sistemas que no se seleccionaron anteriormente, agentes de consola recientemente disponibles y sistemas recientemente disponibles. Esta página no muestra aquellos sistemas que fueron seleccionados previamente.

3. Seleccione el agente de consola donde desea descubrir cargas de trabajo.
4. Revise la lista de sistemas.
5. Marque los sistemas en los que desea descubrir cargas de trabajo o seleccione la casilla en la parte superior de la tabla para descubrir cargas de trabajo en todos los entornos de cargas de trabajo descubiertos.
6. Haga esto para otros sistemas según sea necesario.
7. Seleccione **Descubrir** para que Ransomware Resilience descubra automáticamente nuevas cargas de trabajo en el agente de consola seleccionado.

Actividad sospechosa del usuario

En la tarjeta de actividad del usuario, puede crear y administrar el agente de actividad del usuario necesario para detectar actividad sospechosa del usuario.

Para obtener más información, consulte "Actividad sospechosa del usuario" .

Agregar un destino de respaldo

Ransomware Resilience puede identificar cargas de trabajo que aún no tienen copias de seguridad y también cargas de trabajo que aún no tienen destinos de copia de seguridad asignados.

Para proteger esas cargas de trabajo, debe agregar un destino de respaldo. Puede elegir uno de los siguientes destinos de copia de seguridad:

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

> Los destinos de respaldo no están disponibles para cargas de trabajo en Amazon FSx for NetApp ONTAP. Realice operaciones de respaldo utilizando el servicio de respaldo FSx para ONTAP .

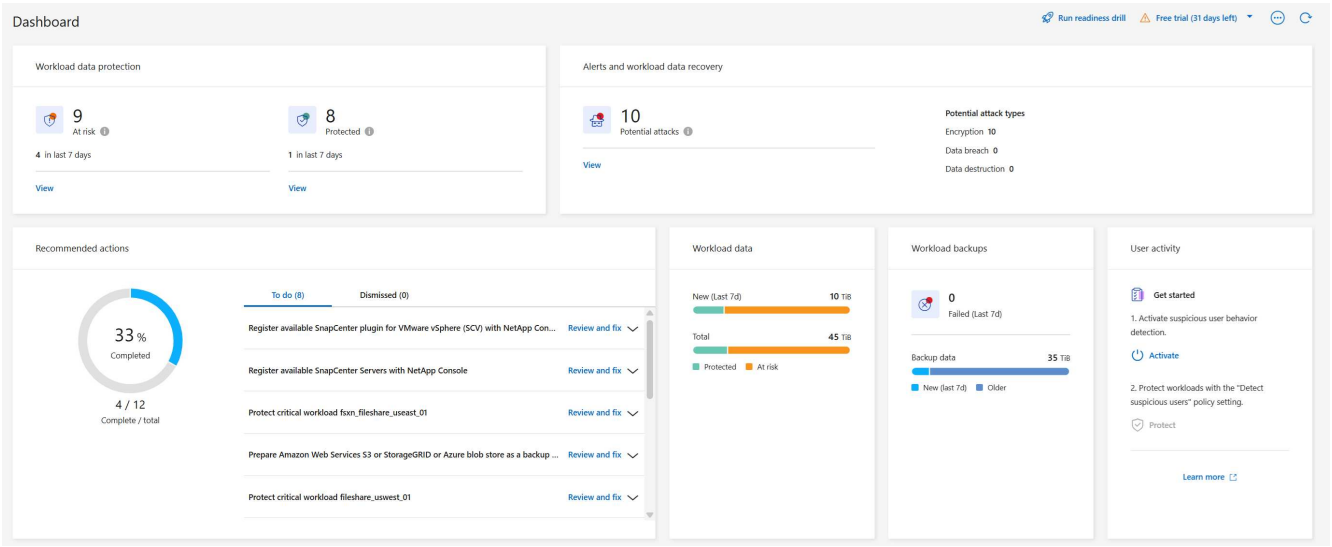
Puede agregar un destino de respaldo según una acción recomendada desde el Panel de Control o accediendo a la opción Configuración en el menú.

Acceda a las opciones de Destino de la copia de seguridad desde las acciones recomendadas del Panel de control

El panel de control ofrece muchas recomendaciones. Una recomendación podría ser configurar un destino de respaldo.

Pasos

1. En el panel de Resiliencia ante Ransomware, revise el panel Acciones recomendadas.



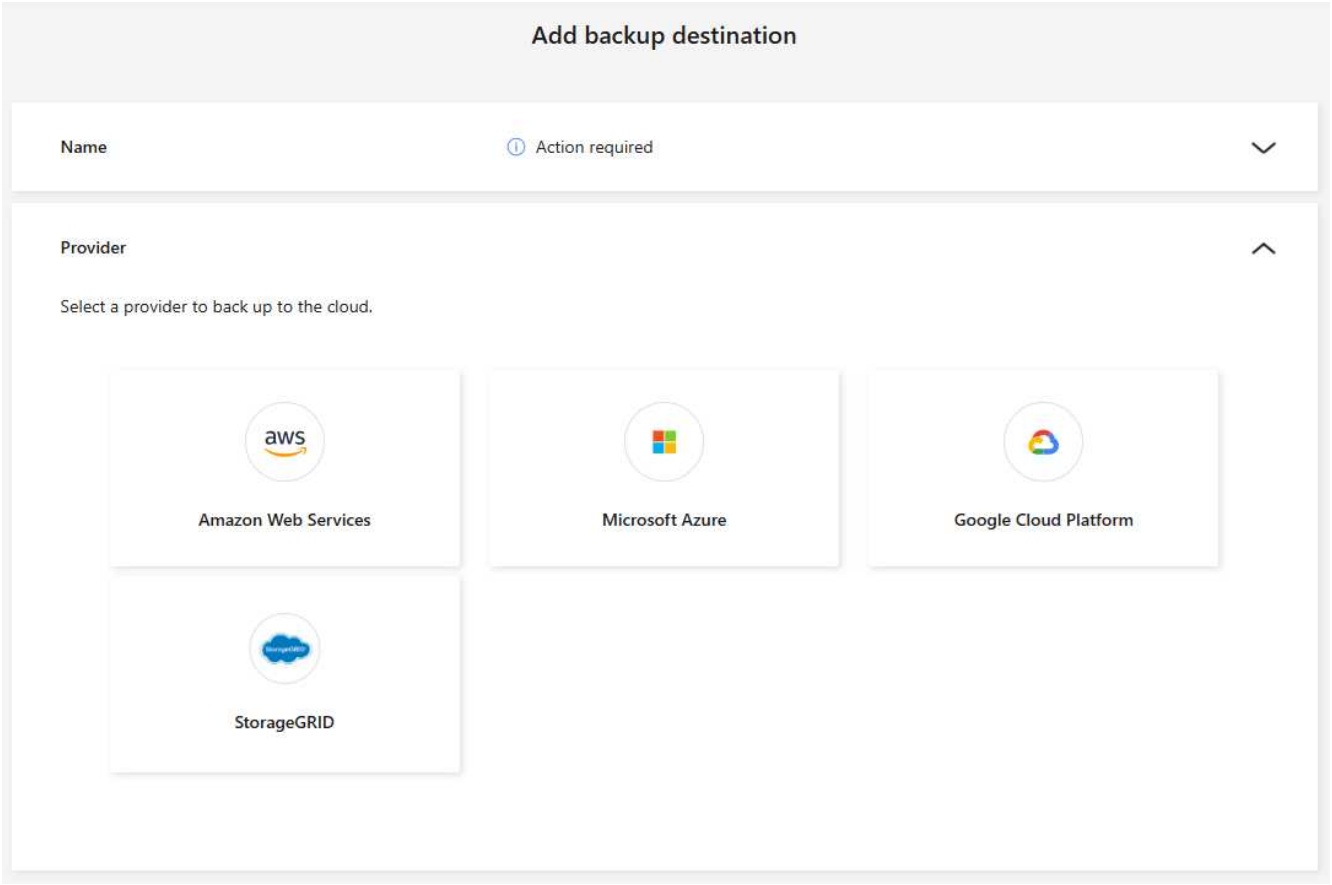
2. Desde el Panel de control, seleccione **Revisar y corregir** para la recomendación de "Preparar <proveedor de respaldo> como destino de respaldo".
3. Continúe con las instrucciones según el proveedor de respaldo.

Agregue StorageGRID como destino de respaldo

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

Pasos

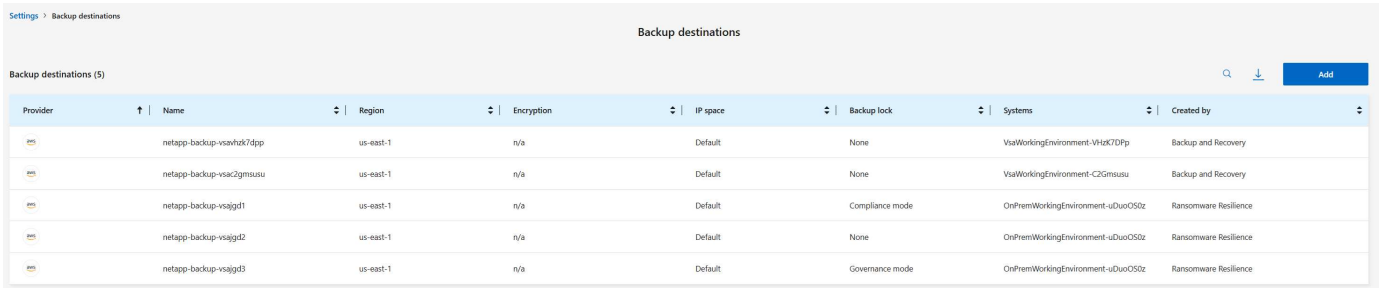
1. En la página **Configuración > Destinos de copia de seguridad**, seleccione **Agregar**.
2. Introduzca un nombre para el destino de la copia de seguridad.



3. Seleccione * StorageGRID*.
4. Seleccione la flecha hacia abajo junto a cada configuración e ingrese o seleccione valores:
   - **Configuración del proveedor**:
     - Crea un nuevo depósito o trae tu propio depósito que almacenará las copias de seguridad.
     - Nombre de dominio completo, puerto, clave de acceso de StorageGRID y credenciales de clave secreta del nodo de puerta de enlace de StorageGRID .
   - **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.
5. Seleccione **Agregar**.

Resultado

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



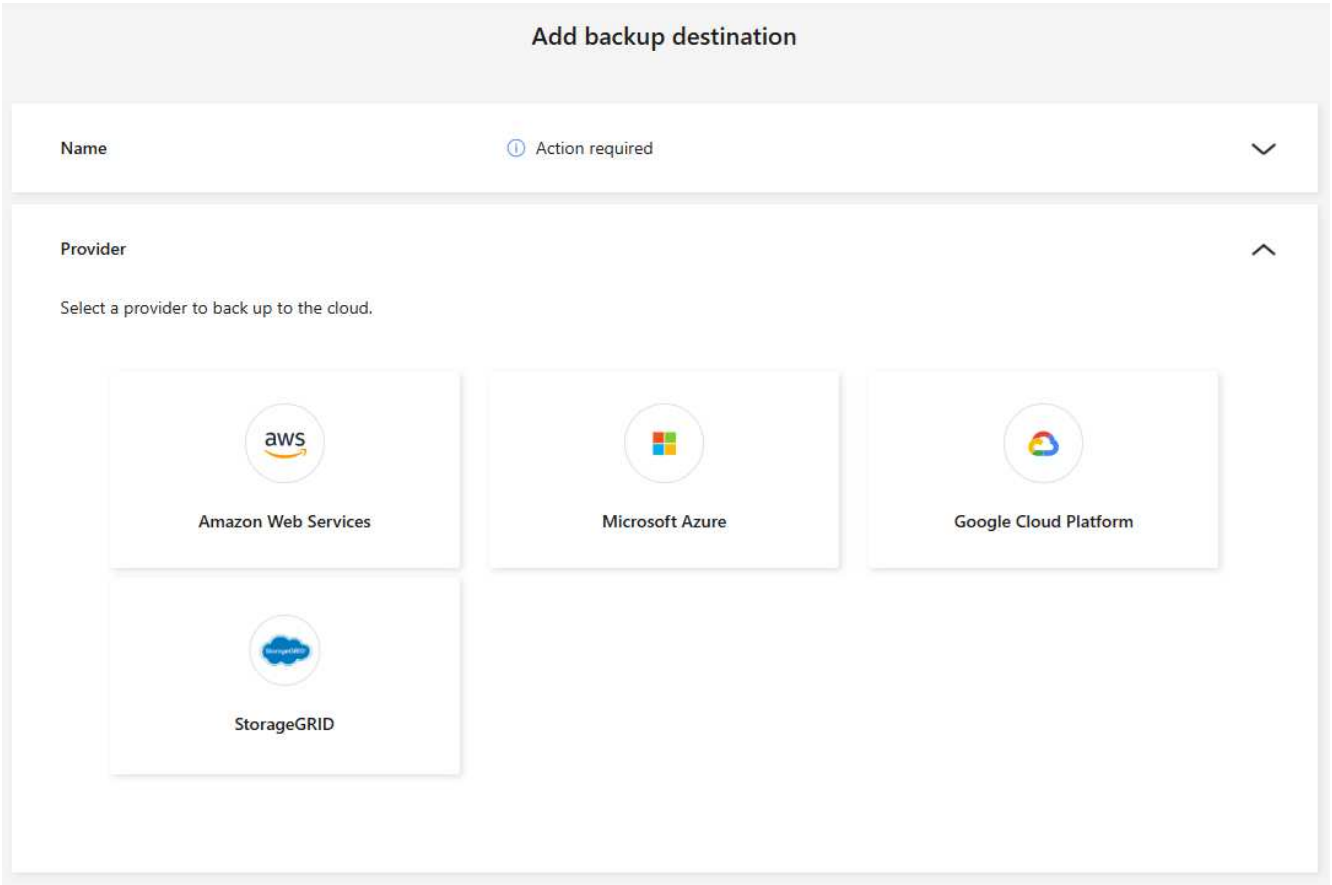
Agregue Amazon Web Services como destino de respaldo

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

Para obtener detalles sobre cómo administrar su almacenamiento de AWS en la consola, consulte "Administra tus buckets de Amazon S3" .

Pasos

1. En la página **Configuración > Destinos de copia de seguridad**, seleccione **Agregar**.
2. Introduzca un nombre para el destino de la copia de seguridad.



3. Seleccione **Amazon Web Services**.
4. 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.

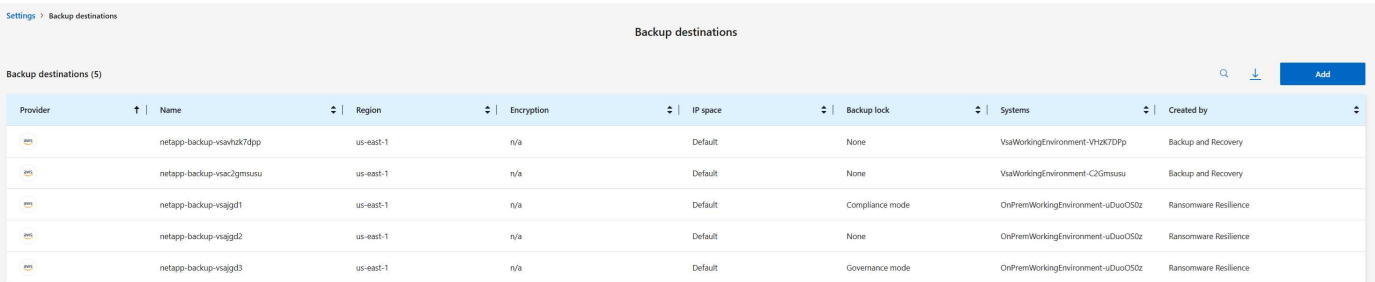
  Si configura el ajuste de bloqueo de respaldo ahora, no podrá cambiar el ajuste más tarde una vez configurado el destino de respaldo.

  - **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.

5. Seleccione **Agregar**.

Resultado

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



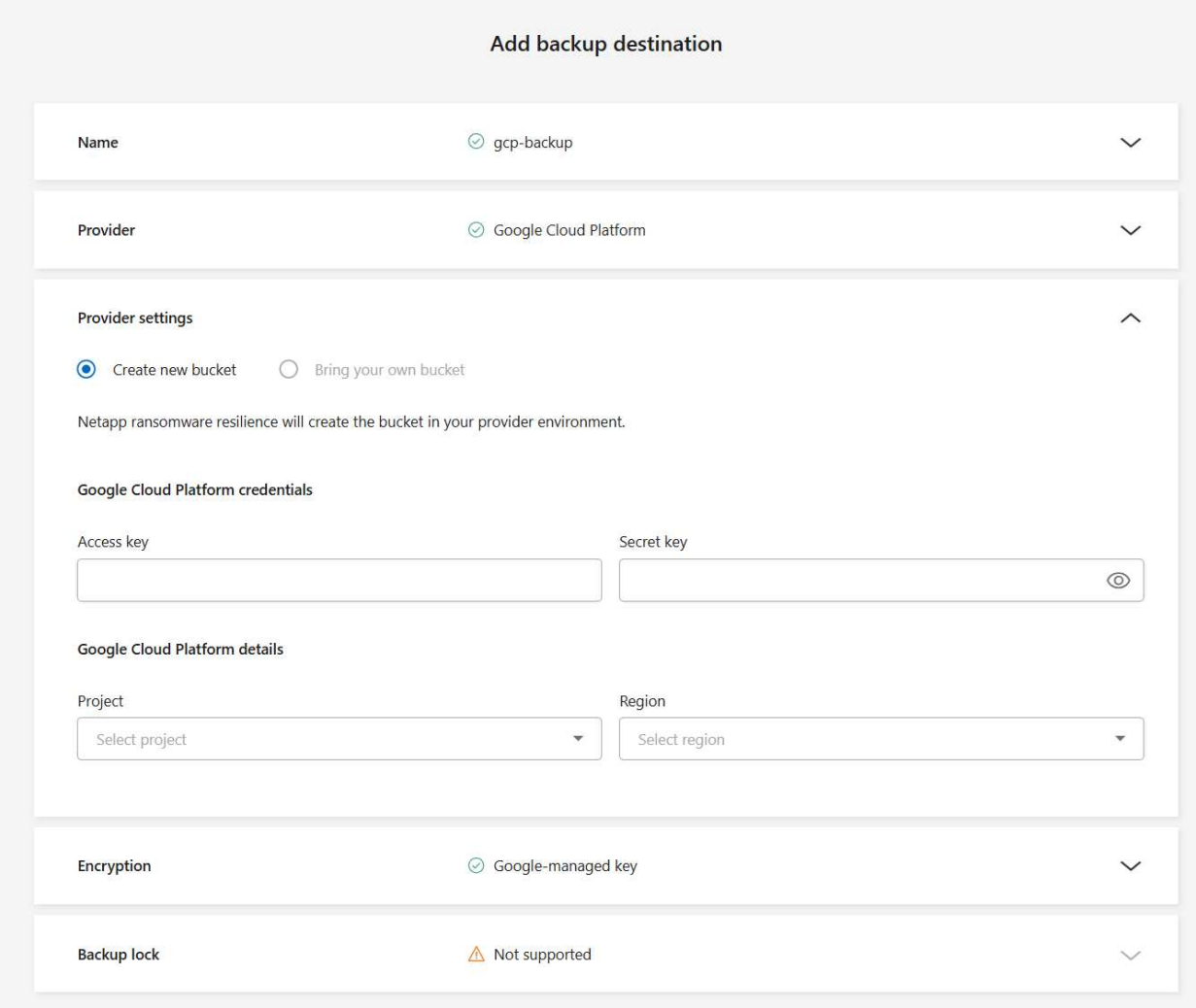
Agregar Google Cloud Platform como destino de respaldo

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

Para obtener detalles sobre cómo administrar su almacenamiento de GCP en la consola, consulte "Opciones de instalación del agente de consola en Google Cloud" .

Pasos

1. En la página **Configuración > Destinos de copia de seguridad**, seleccione **Agregar**.
2. Introduzca un nombre para el destino de la copia de seguridad.
3. Seleccione **Google Cloud Platform**.
4. Seleccione la flecha hacia abajo junto a cada configuración e ingrese o seleccione valores:
   - **Configuración del proveedor**:
     - Crear un nuevo depósito. Introduzca la clave de acceso y la clave secreta.
     - Ingrese o seleccione su proyecto y región de Google Cloud Platform.



   - **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.

     Los datos del depósito se cifran con claves administradas por Google de forma predeterminada. Puedes seguir utilizando las claves administradas por Google.

   - **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.
     - De manera opcional, elija si utilizará un punto final privado de GCP (PrivateLink) que configuró

previamente.

5. Seleccione **Agregar**.

Resultado

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

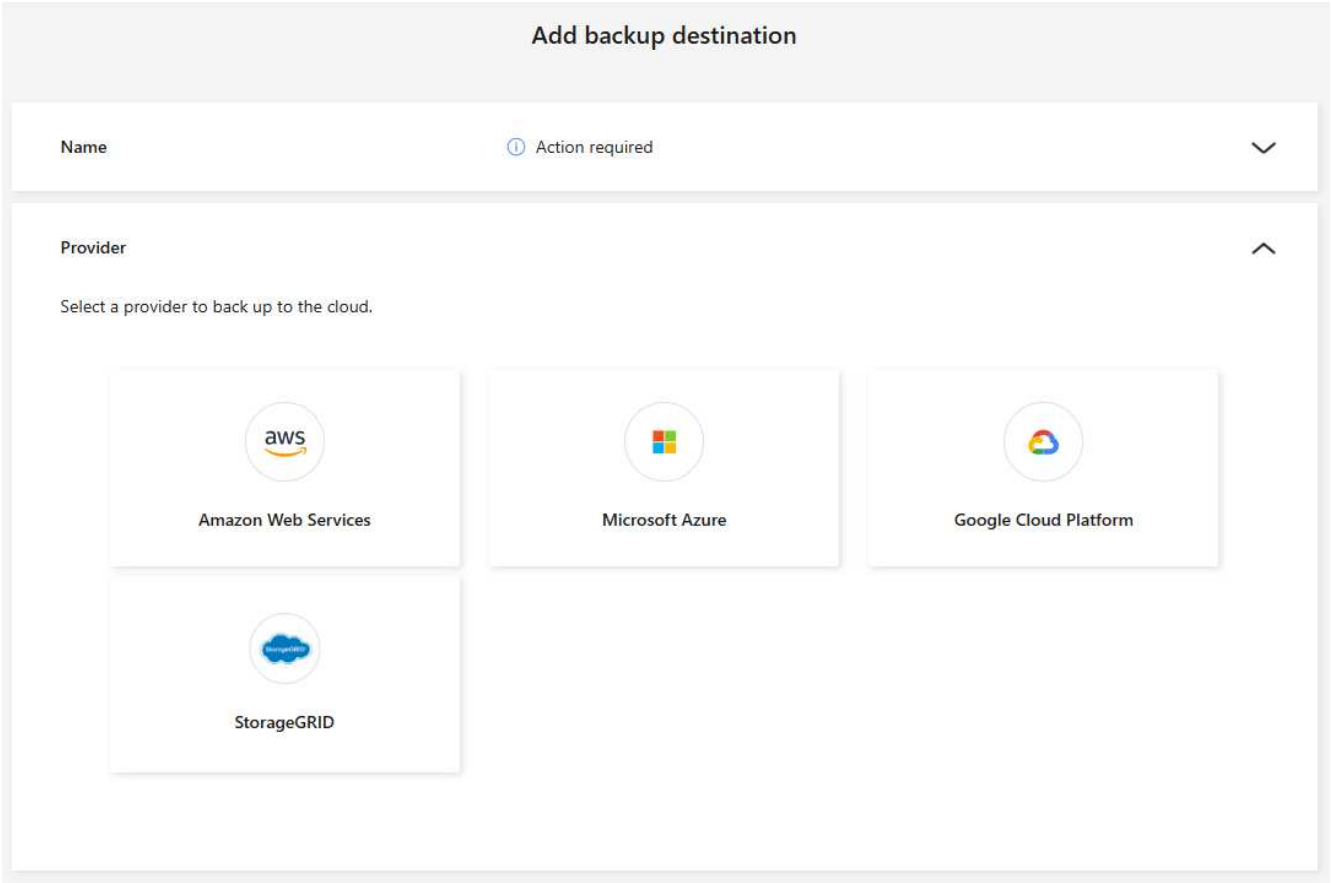
Agregar Microsoft Azure como destino de respaldo

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 la página **Configuración > Destinos de copia de seguridad**, seleccione **Agregar**.
2. Introduzca un nombre para el destino de la copia de seguridad.



3. Seleccione **Azure**.
4. 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.
     - Suscripción, región y grupo de recursos de Azure para credenciales de Azure

       "Si desea traer su propia cuenta de almacenamiento, consulte Agregar cuentas de

almacenamiento de blobs de Azure" .

- **Cifrado**: Si está creando una nueva cuenta de almacenamiento, ingrese la información de la clave de cifrado que le proporcionó el proveedor. Si eligió una cuenta existente, la información de cifrado ya está disponible.

  Los datos de la cuenta están cifrados con claves administradas por Microsoft de forma predeterminada. Puede seguir utilizando claves administradas por Microsoft o puede administrar el cifrado de sus datos utilizando sus propias claves.

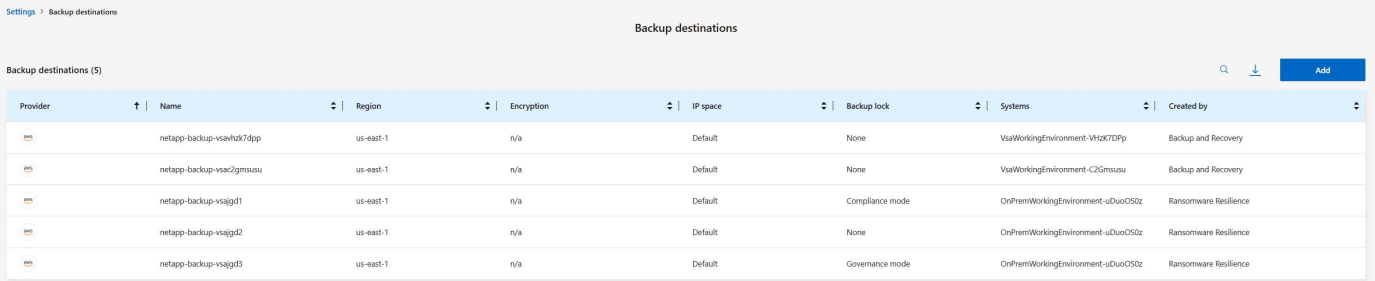
- **Redes**: elija el espacio IP y si utilizará un punto final privado.
  - El espacio IP es el clúster donde residen los volúmenes que desea respaldar. Los LIF entre clústeres para este espacio IP deben tener acceso a Internet saliente.
  - Opcionalmente, elija si utilizará un punto de conexión privado de Azure que configuró previamente.

    Si desea utilizar Azure PrivateLink, consulte "Enlace privado de Azure" .

5. Seleccione **Agregar**.

Resultado

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



Conectarse a un sistema de gestión de eventos y seguridad (SIEM) para el análisis y detección de amenazas

Puede enviar datos automáticamente a su sistema de gestión de eventos y seguridad (SIEM) para analizar y detectar amenazas. Puede seleccionar AWS Security Hub, Microsoft Sentinel o Splunk Cloud como su SIEM.

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

Acerca de los 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, deberá realizar 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 habilitar Microsoft Sentinel en Ransomware Resilience, deberá realizar los siguientes pasos de alto nivel 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. Haga clic en **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.

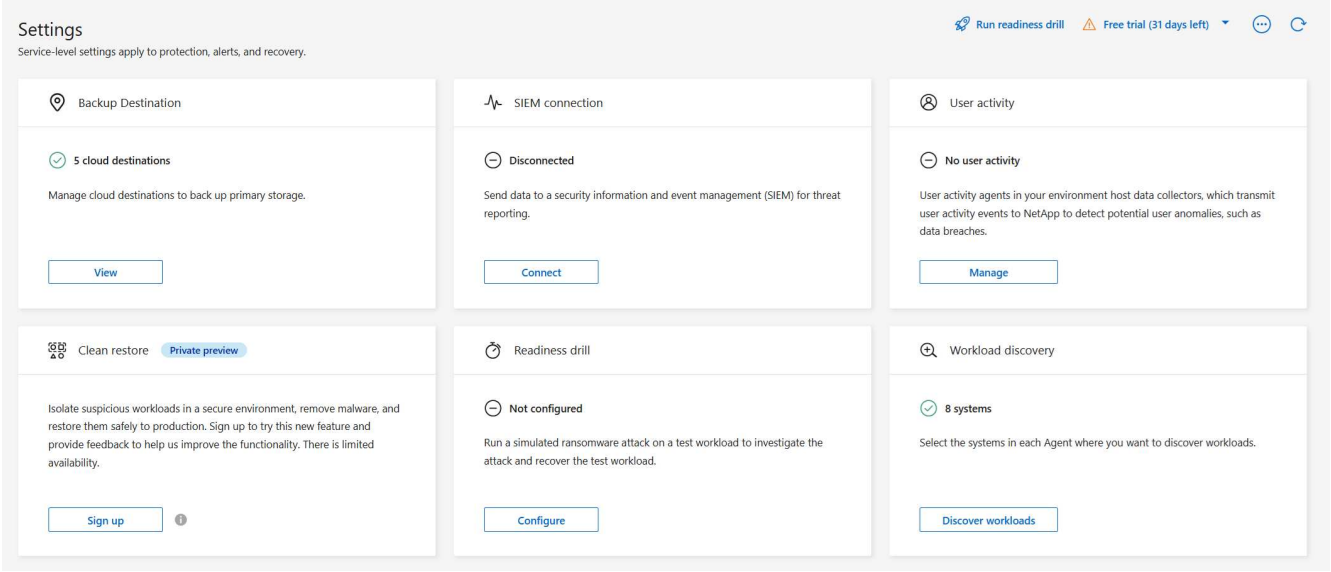
Conecte SIEM en la resiliencia contra el ransomware

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

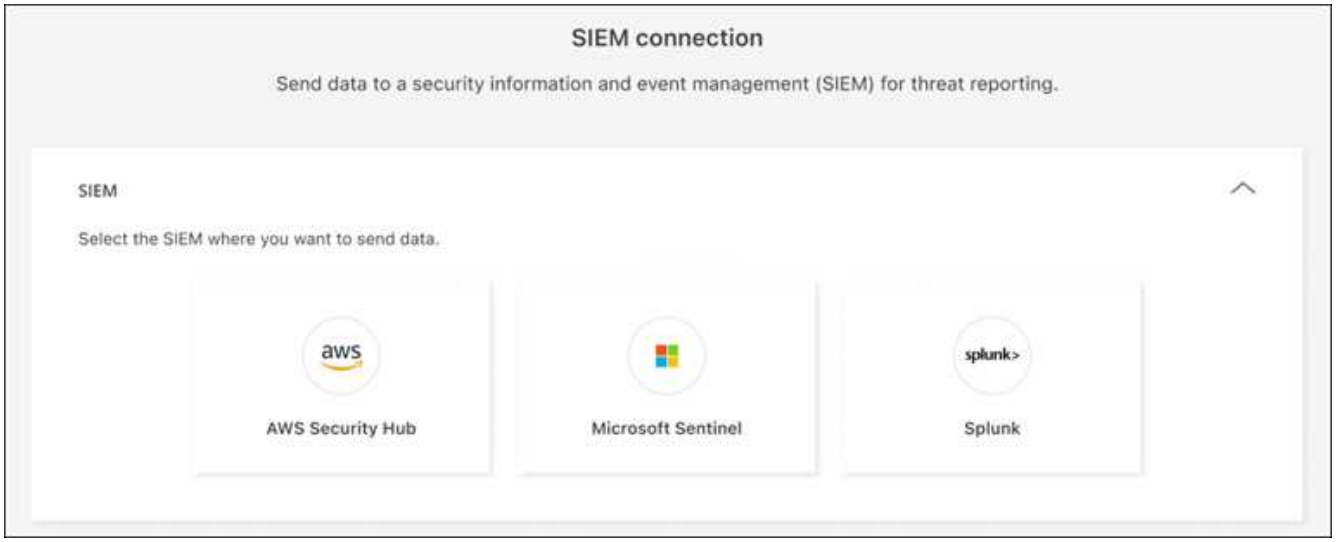
Pasos

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".

Configurar la detección de actividad sospechosa de usuarios en NetApp Ransomware Resilience

Ransomware Resilience admite la detección de comportamiento sospechoso de los usuarios en las políticas de detección, lo que le permite abordar incidentes de ransomware a nivel de usuario.

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.

Agentes y coleccionistas

Se debe instalar al menos un agente de actividad del usuario para activar la detección de actividad de usuario sospechosa en Ransomware Resilience. Cuando activa la función de actividad de usuario sospechosa desde el panel de resiliencia contra ransomware, debe proporcionar la información del host del agente.

Un agente puede alojar varios recopiladores de datos. Los recopiladores de datos envían datos a una ubicación SaaS para su análisis. Hay dos tipos de coleccionistas:

- El **recopilador de datos** recopila datos de actividad del usuario de ONTAP.
- El **conector de directorio de usuarios** se conecta a su directorio para asignar ID de usuarios a nombres de usuario.

Los recopiladores se configuran en la configuración de Resiliencia ante ransomware.

Habilitar la detección de actividad sospechosa de usuarios

Rol de consola requerido Para activar la detección de actividad de usuarios sospechosos, necesita el rol de administrador de la organización. Para configuraciones posteriores de actividad de usuarios sospechosa, necesita el rol de administrador de comportamiento de usuario de Ransomware Resilience. "Obtenga información sobre las funciones de resiliencia ante ransomware para la NetApp Console".

Agregar un agente de actividad del usuario

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

Requisitos

Para instalar un agente de actividad del usuario, necesita un host o una máquina virtual que cumpla con los siguientes requisitos de servidor y sistema operativo compatibles.

Requisitos del sistema operativo

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

Sistema operativo	Versiones compatibles
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)

Requisitos del servidor

El servidor debe cumplir los siguientes requisitos mínimos:

- **CPU**: 4 núcleos
- **RAM**: 16 GB de RAM
- **Espacio en disco**: 35 GB de espacio libre en disco

Soporte del proveedor de la nube

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

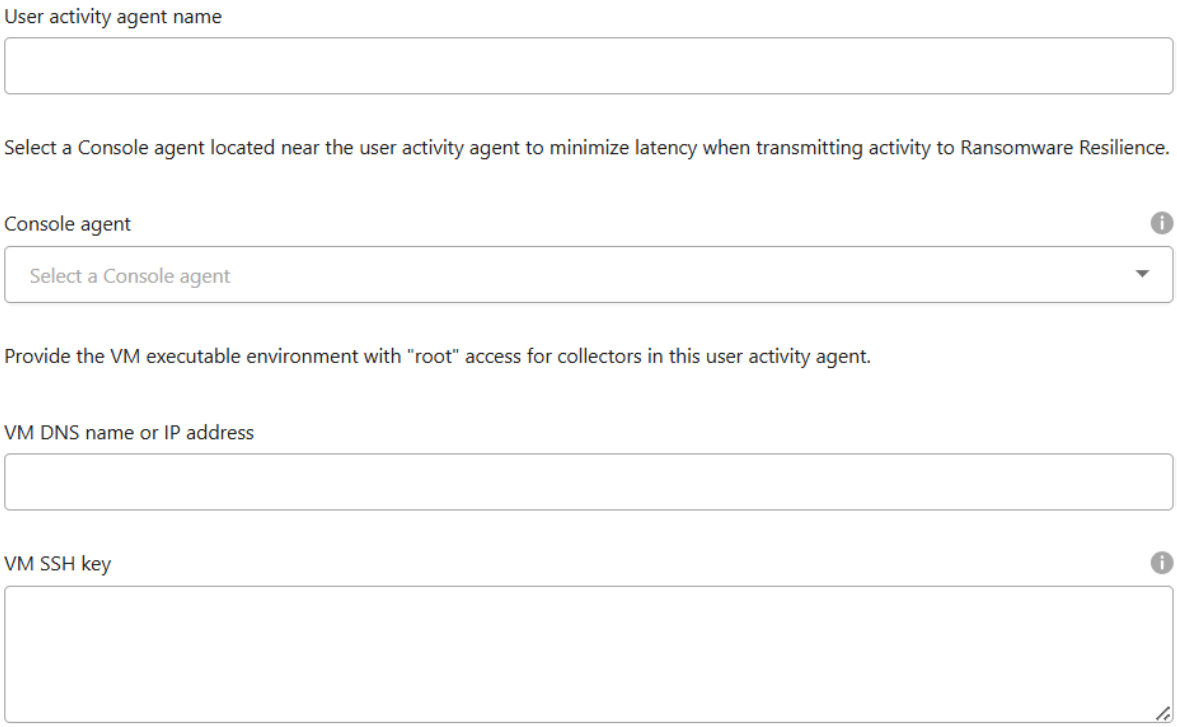
Proveedor de nube	Región
AWS	• Asia Pacífico (Sídney) (ap-southeast-2) • Europa (Frankfurt) (eu-central-1) • Este de EE. UU. (Norte de Virginia) (us-east-1)
Azur	Este de EE. UU.

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**
   - **Clave SSH de VM**



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

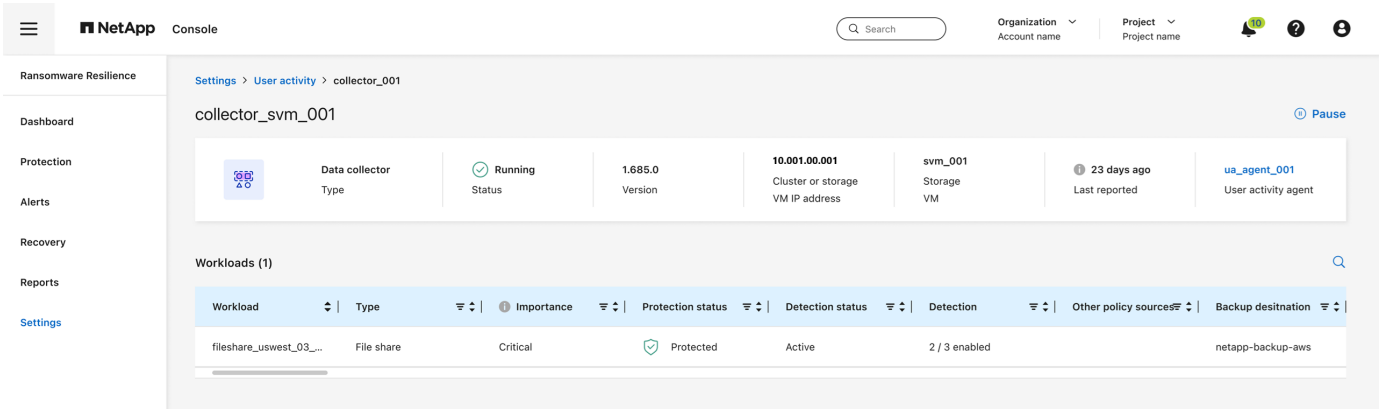
Resultado

Una vez creado exitosamente el agente de actividad del usuario, regrese al menú **Configuración** y seleccione **Administrar** en el mosaico Actividad del usuario. Seleccione la pestaña **Agente de actividad del usuario** y luego seleccione el agente de actividad del usuario para ver detalles al respecto, 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 habilita una estrategia de protección contra ransomware con detección de actividad de usuario sospechosa. Para obtener más información, consulte 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.



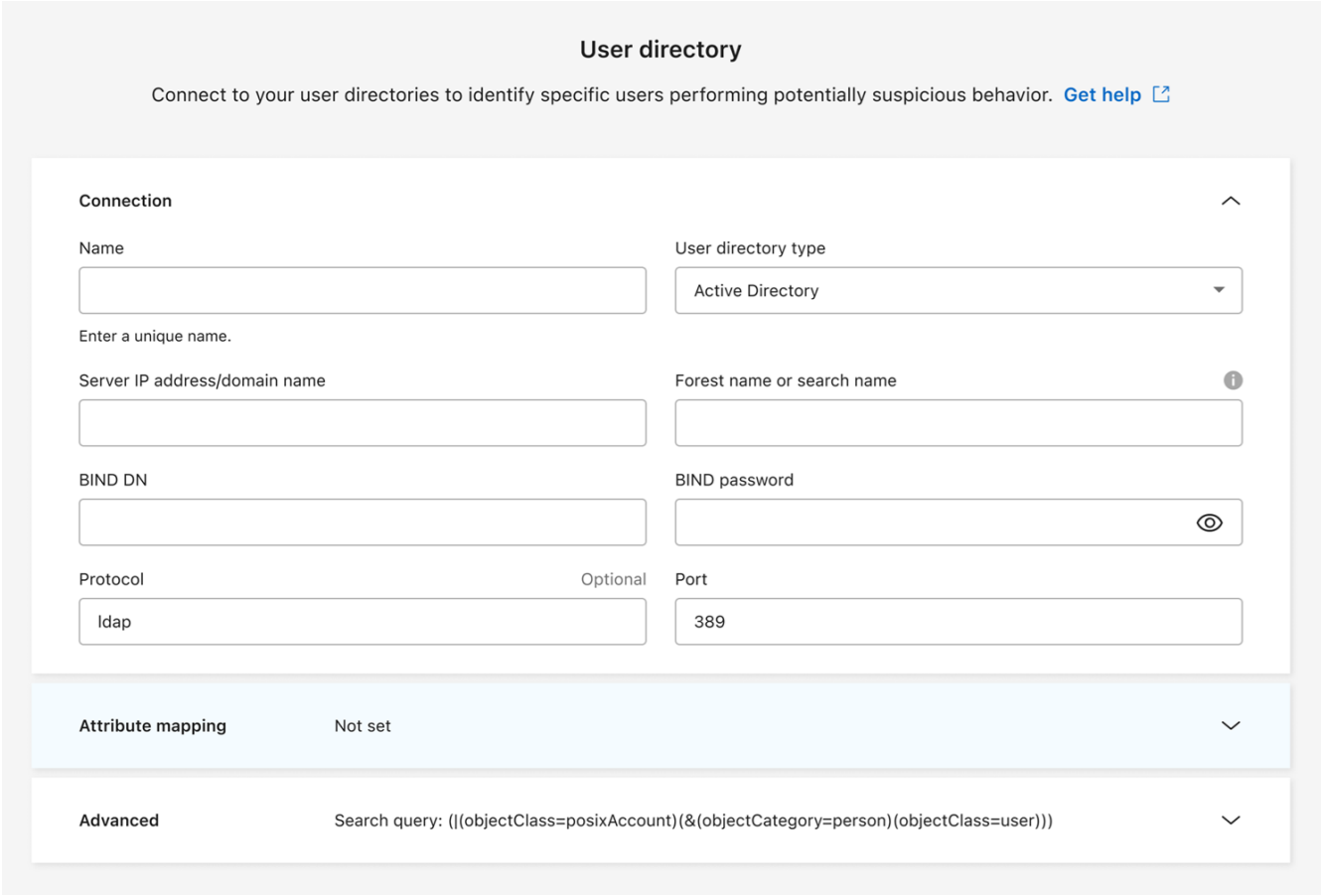
Agregar un conector de directorio de usuarios

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

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, seleccione **Eliminar** para confirmar sus acciones.

Responder a alertas de actividad sospechosa del usuario

Después de configurar la detección de actividad de usuarios sospechosas, puede monitorear eventos en la página de alertas. Para obtener más información, consulte "Detectar actividad maliciosa y comportamiento anómalo del usuario" .

Utilice la resiliencia frente al ransomware

Supervise el estado de la carga de trabajo mediante el panel de resiliencia contra ransomware de NetAPp

El panel de NetApp Ransomware Resilience proporciona información general sobre el estado de protección de sus cargas de trabajo. Puede determinar rápidamente las cargas de trabajo que están en riesgo o protegidas, identificar las cargas de trabajo afectadas por un incidente o en recuperación y medir el alcance de la protección observando cuánto almacenamiento está protegido o en riesgo.

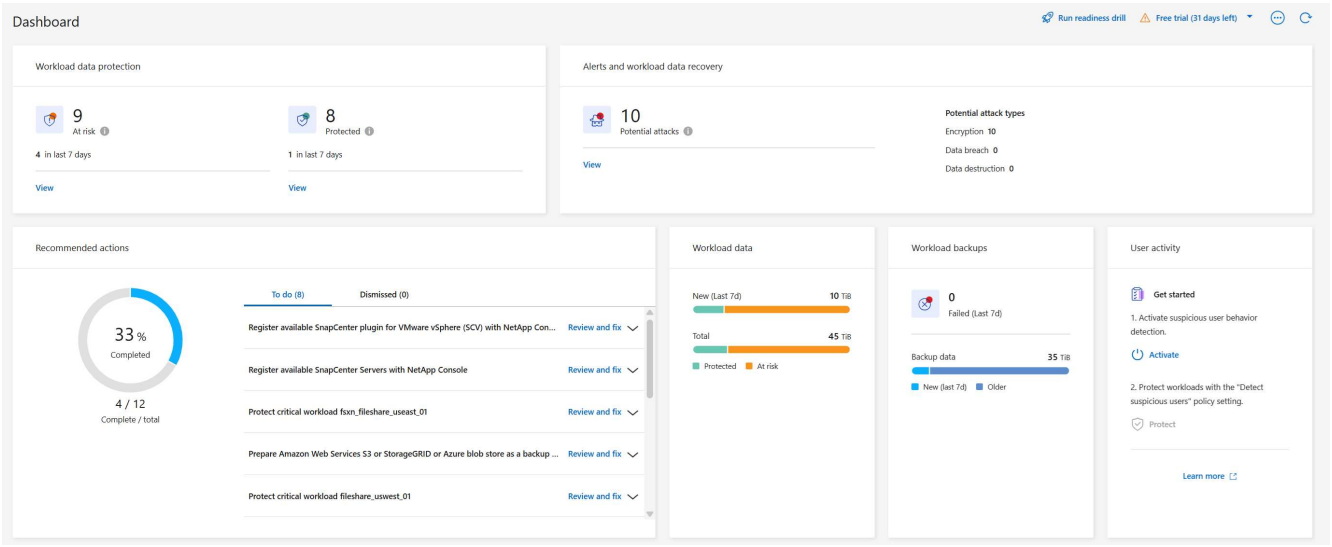
Utilice el Panel de control para revisar sugerencias de protección, cambiar configuraciones, descargar informes y ver documentación.

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" .

Revisar el estado de la carga de trabajo mediante 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 Dashboard, puedes realizar 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**.

  Ver "Revisar las sugerencias de protección en el Panel de Control" o "Proteger las cargas de trabajo" .

  Ransomware Resilience muestra nuevas recomendaciones desde su última visita al Panel de Control con la etiqueta "Nuevo" durante 24 horas. Las acciones aparecen en orden de prioridad, con las más importantes en la parte superior. Revise, actúe o descarte 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.

Revisar 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.	Ingrese los detalles del servidor SIEM/XDR para habilitar la detección de amenazas. Consulte "Configurar los ajustes de protección" .
Habilite la protección consistente con la carga de trabajo para aplicaciones o VMware.	Estas cargas de trabajo no son administradas por el software SnapCenter ni por el SnapCenter Plug-in for VMware vSphere.	Para que SnapCenter los administre, habilite la protección consistente con la carga de trabajo. Consulte "Proteja la carga de trabajo contra ataques de ransomware" .
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" .
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.	Agregue destinos de respaldo a esta carga de trabajo para protegerla. Consulte "Configurar los ajustes de protección" .
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.	Asignar una política a cada una de las cargas de trabajo. Consulte "Proteja las cargas de trabajo contra ataques de ransomware" .

Recomendación	Descripción	Cómo resolverlo
Registre el complemento SnapCenter disponible para VMware vSphere (SCV) con la consola	Una carga de trabajo de VM no está protegida.	Asigne protección consistente con VM a la carga de trabajo de VM habilitando el complemento SnapCenter para VMware vSphere. Consulte "Proteja las cargas de trabajo contra ataques de ransomware" .
Registrar el servidor SnapCenter disponible con la consola	Una aplicación no está protegida.	Asigne protección consistente con la aplicación a la carga de trabajo habilitando SnapCenter Server. Consulte "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".

Descargar 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.

Proteger las cargas de trabajo

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

Puede proteger las cargas de trabajo contra ataques de ransomware habilitando una protección consistente con la carga de trabajo o creando estrategias de protección contra ransomware en NetApp Ransomware Resilience.

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 políticas tanto de *detección* como de *protección*.

- **Políticas de detección** detectan 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.

Para una mejor gestión y protección de su patrimonio de datos, puede crear"recursos compartidos de archivos grupales" proteger colectivamente los volúmenes bajo una sola estrategia.

Políticas de protección con otros servicios administrados por NetApp

Más allá de Ransomware Resilience, se pueden utilizar los siguientes servicios para gestionar la protección:

- NetApp Backup and Recovery para recursos compartidos de archivos y recursos compartidos de archivos de máquinas virtuales
- SnapCenter para VMware para almacenes de datos de máquinas virtuales
- SnapCenter para Oracle

La información de protección de estos servicios aparece en Ransomware Resilience. Puede agregar políticas de detección a estos servicios con Ransomware Resilience. Agregar 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 respaldo no están disponibles para cargas de trabajo en Amazon FSx for NetApp ONTAP. Realice operaciones de respaldo utilizando el servicio de respaldo FSx para ONTAP . Las políticas de respaldo se establecen para cargas de trabajo en FSx para ONTAP en AWS, no en Ransomware Resilience. Las políticas de respaldo aparecen en Ransomware Resilience y permanecen sin cambios desde AWS.

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

Si su carga de trabajo no está administrada por Backup and Recovery, Ransomware Resilience, SnapCenter o el SnapCenter Plug-in for VMware vSphere, es posible que tenga instantáneas tomadas como parte de ONTAP u otros productos. Si la protección FPolicy de ONTAP está activada, puede cambiarla usando ONTAP.

Ver la protección contra ransomware en una carga de trabajo

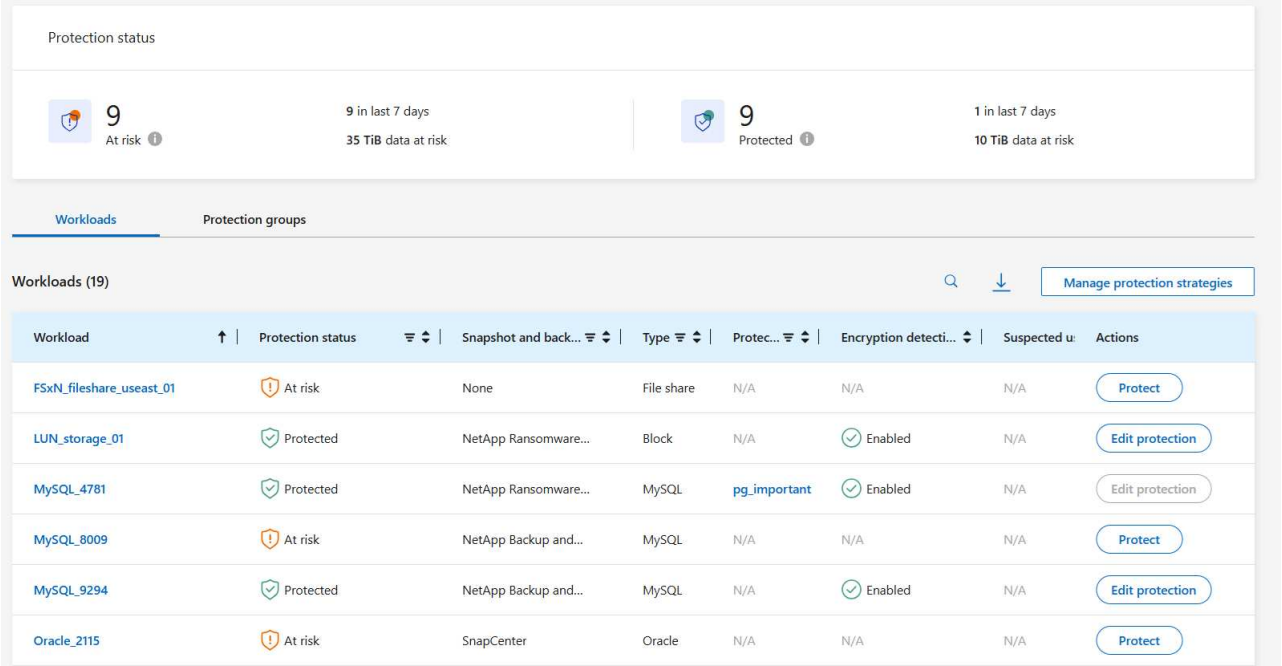
Uno de los primeros pasos para proteger las cargas de trabajo es ver las cargas de trabajo actuales y su estado de protección. Puedes ver los siguientes tipos de cargas de trabajo:

- 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 de Protección de datos en el Tablero, seleccione **Ver todo**.
- Desde el menú, seleccione **Protección**.



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

> Ver"Agregar una estrategia de protección contra ransomware" para aprender sobre el uso de Ransomware Resilience cuando existe una política de protección con SnapCenter o Backup and Recovery.

Comprender la página de Protección

La página Protección muestra la siguiente información sobre la protección de la carga de trabajo:

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: Una carga de trabajo puede tener uno de los siguientes estados de detección de ransomware:

- **Aprendizaje**: Recientemente se asignó una política de detección de ransomware a la carga de trabajo y Ransomware Resilience está escaneando las cargas de trabajo.
- **Activo**: Se asigna una política de protección contra detección de ransomware.
- **No establecido**: No se asigna una política de protección contra detección de ransomware.

- **Error**: Se asignó una política de detección de ransomware, pero Ransomware Resilience encontró un error.

> Cuando la protección está habilitada en Ransomware Resilience, la detección de alertas y los informes comienzan después de que el estado de la política de detección de ransomware cambia del modo de aprendizaje al modo activo.

Política de detección: aparece el nombre de la política de detección de ransomware, si se ha asignado una. Si no se ha asignado la política de detección, aparece "N/A".

Políticas de instantáneas y copias de seguridad: esta columna muestra las políticas de instantáneas y copias de seguridad aplicadas a la carga de trabajo y al producto o servicio que administra esas políticas.

- Administrado por SnapCenter
- Administrado por el SnapCenter Plug-in for VMware vSphere
- Administrado por Backup and Recovery
- Nombre de la política de protección contra ransomware que rige las instantáneas y las copias de seguridad
- Ninguno

Importancia de la carga de trabajo

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 toman más de 1 copia instantánea por hora (programa de protección altamente agresivo)
- **Importante**: Se toman copias instantáneas menos de 1 por hora pero más de 1 por día
- **Estándar**: Se toman más de 1 copia instantánea por día

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.

Nivel de política	Snapshot	Frecuencia	Retención (días)	# de copias de instantáneas	Número máximo total 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
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

Habilite la protección consistente con aplicaciones o máquinas virtuales con SnapCenter

Habilitar la protección consistente con la aplicación o la máquina virtual le ayuda a proteger sus cargas de trabajo de aplicaciones o máquinas virtuales de manera consistente, logrando un estado inactivo y consistente para evitar una posible pérdida de datos más adelante si se necesita recuperación.

Este proceso inicia el registro del servidor de software SnapCenter para aplicaciones o del SnapCenter Plug-in

for VMware vSphere para máquinas virtuales que utilizan Copia de seguridad y recuperación.

Después de habilitar la protección consistente con la carga de trabajo, puede administrar las estrategias de protección en Ransomware Resilience. La estrategia de protección incluye las políticas de instantáneas y copias de seguridad administradas en otro lugar junto con una política de detección de ransomware administrada en Ransomware Resilience.

Para obtener más información sobre cómo registrar SnapCenter o el SnapCenter Plug-in for VMware vSphere mediante Backup and Recovery, consulte la siguiente información:

- "Registrar el software del servidor SnapCenter"
- "Registrar el SnapCenter Plug-in for VMware vSphere"

Pasos

1. Desde el menú Resiliencia ante ransomware, seleccione **Panel de control**.
2. Desde el panel Recomendaciones, busque una de las siguientes recomendaciones y seleccione **Revisar y corregir**:
   - Registre el servidor SnapCenter disponible con la NetApp Console
   - Registre el SnapCenter Plug-in for VMware vSphere (SCV) con la NetApp Console
3. Siga la información para registrar SnapCenter o el SnapCenter Plug-in for VMware vSphere mediante Copia de seguridad y recuperación.
4. Regresar a Resiliencia frente al ransomware.
5. Desde Ransomware Resilience, navegue hasta el Panel de control e inicie el proceso de descubrimiento nuevamente.
6. Desde Ransomware Resilience, seleccione **Protección** para ver la página de Protección.
7. Revise los detalles en la columna de políticas de instantáneas y copias de seguridad en la página Protección para ver que las políticas se administran en otra parte.

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
- **Reemplace las políticas de instantáneas o copias de seguridad existentes de SnapCenter o la protección de Backup and Recovery con estrategias de protección administradas 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" .

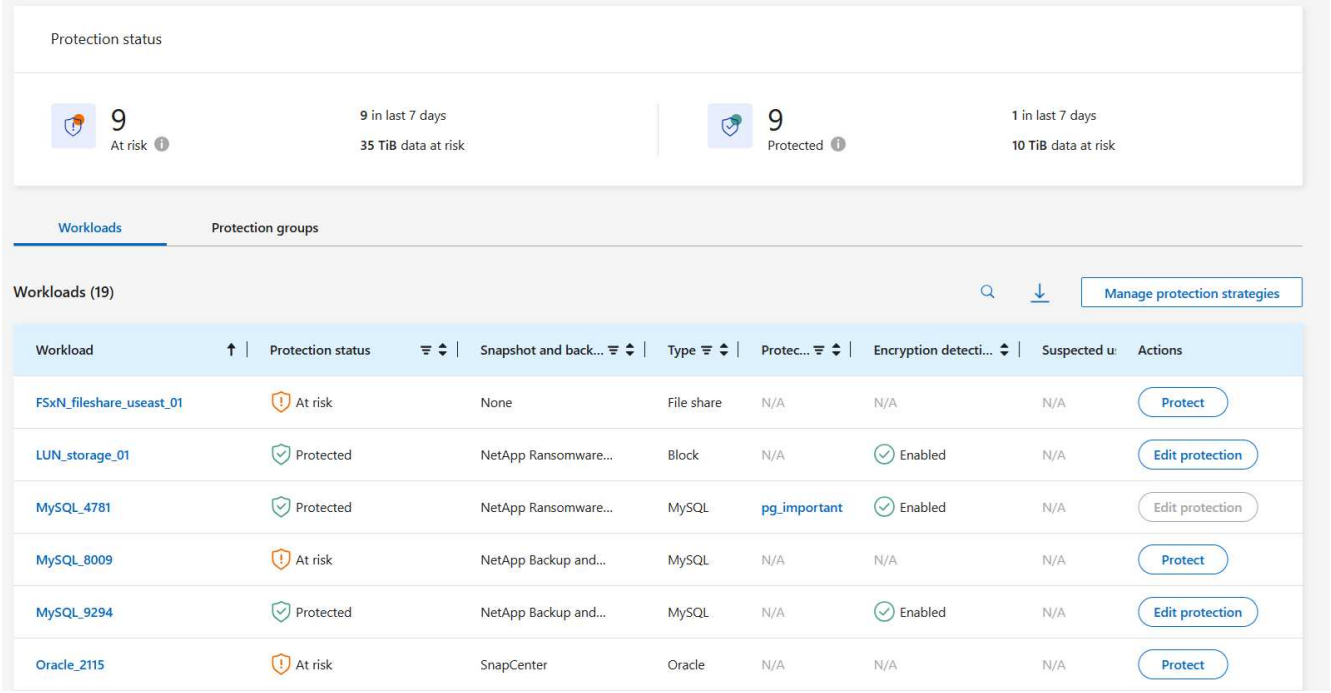
Cree una estrategia de protección contra ransomware (si no tiene políticas de instantáneas o copias de seguridad)

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:

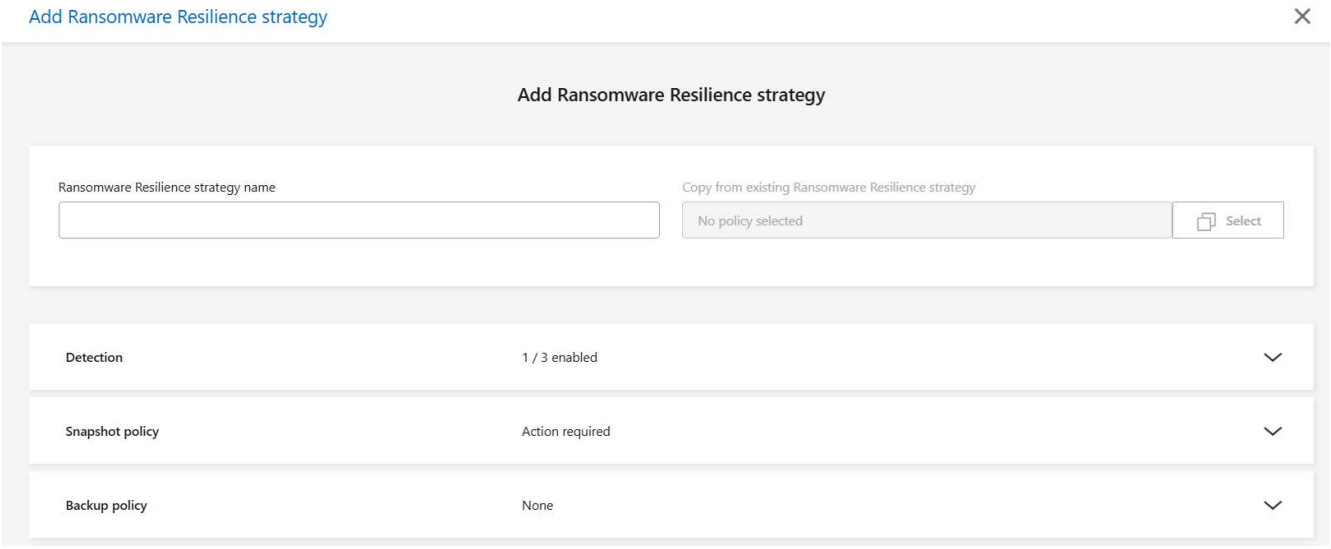
- Política de instantáneas
- Política de respaldo
- Política de detección de ransomware

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 la detección de ransomware para que Ransomware Resilience detecte 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 archivo**: habilite esta opción para que Ransomware Resilience bloquee las 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 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 habilitar el bloqueo de copias de seguridad en el almacenamiento secundario, configure los destinos de copia de seguridad utilizando la opción **Configuración**. Para obtener más información, consulte "Configurar ajustes" .

6. Seleccione **Agregar**.

Agregue una política de detección a las cargas de trabajo con políticas de instantáneas y copias de seguridad existentes administradas por SnapCenter o Backup and Recovery

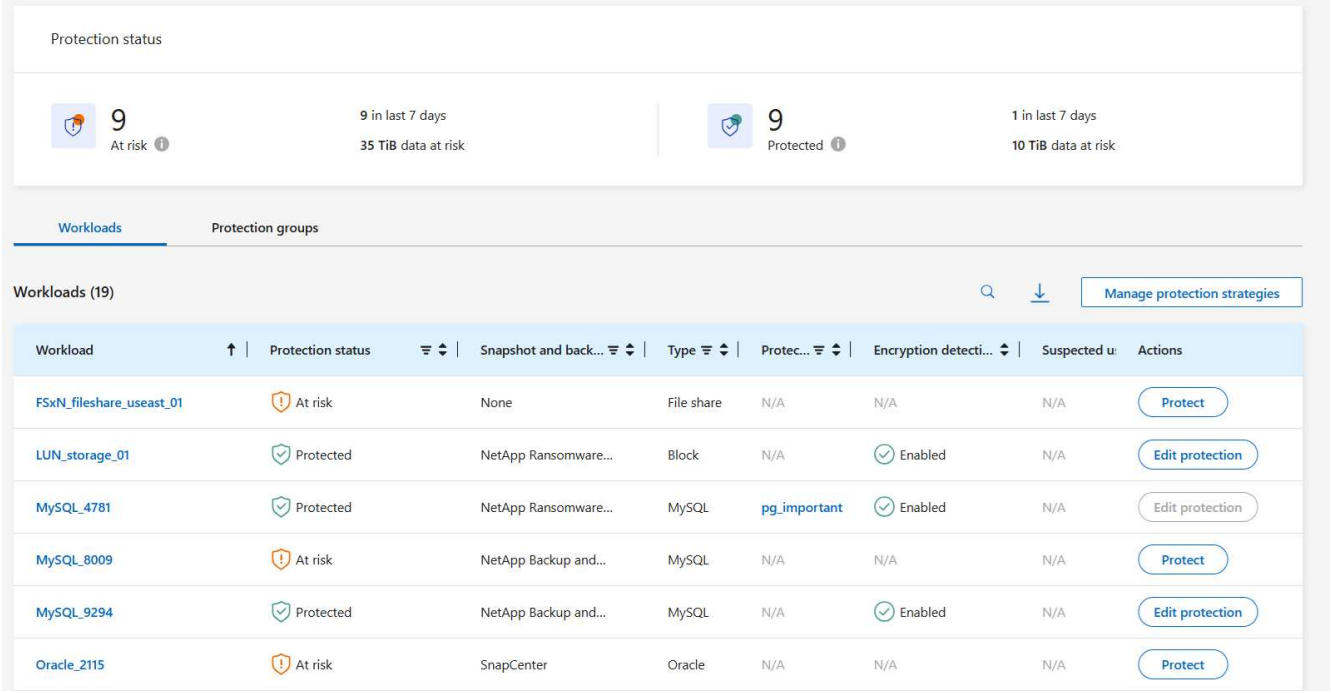
Ransomware Resilience le permite asignar una política de detección o una política de protección a cargas de trabajo con protección de instantáneas y copias de seguridad existentes administradas en otros productos o servicios de NetApp . Otros servicios, como Backup and Recovery y SnapCenter, utilizan políticas que rigen las instantáneas, la replicación en almacenamiento secundario o las copias de seguridad en almacenamiento de objetos.

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

Si tiene políticas de instantáneas o de respaldo existentes con Backup and Recovery o SnapCenter, puede agregar una política para detectar ataques de ransomware. Para administrar la protección y detección con Ransomware Resilience, consulteProtéjase 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 existen políticas activas de SnapCenter o de Backup and Recovery.
4. Para dejar sus políticas de Backup and Recovery o SnapCenter existentes en su lugar y solo aplicar una política de *detección*, deje la casilla **Reemplazar políticas existentes** sin marcar.
5. Para ver detalles de las políticas de SnapCenter , seleccione la **flecha hacia abajo**.
6. Seleccione la configuración de detección que desee: **Detección de cifrado Detección de comportamiento sospechoso del usuario Bloquear extensiones de archivos sospechosas**
7. Seleccione **Siguiente**.
8. Si seleccionó **Detección de comportamiento sospechoso del usuario** como configuración de detección, seleccione el agente de actividad del usuario 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.

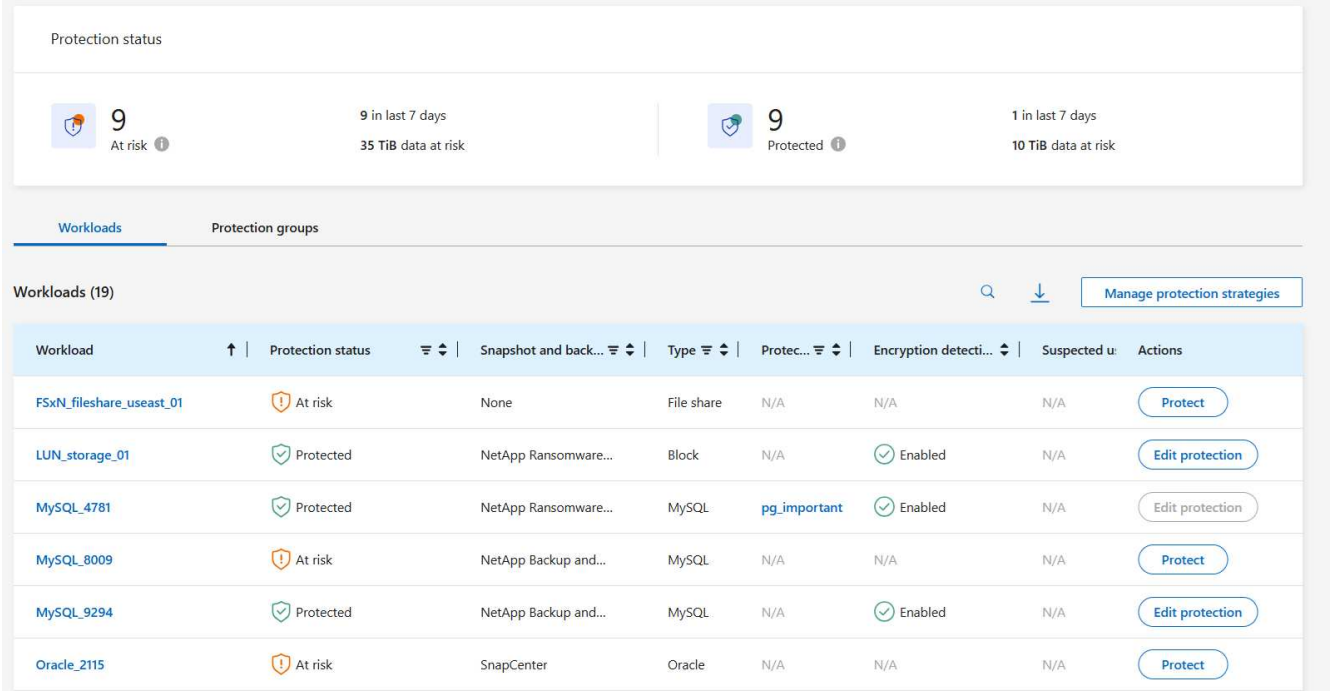
9. Seleccione **Siguiente**.
10. Revise sus opciones Seleccione **Crear** para activar la detección.
11. En la página Protección, revise el **Estado de detección** para confirmar que la detección esté Activa.

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 o de SnapCenter . Para reemplazar las políticas de Backup and Recovery o SnapCenter existentes, seleccione la casilla **Reemplazar políticas existentes**. Al seleccionar la casilla, Ransomware Resilience reemplaza la lista de políticas de detección con 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. 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.
6. Revise la nueva estrategia de protección y luego seleccione **Proteger** para aplicarla.
7. 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 o de SnapCenter existente que desea mantener, desmarque **Reemplazar políticas existentes**. Para reemplazar las políticas existentes, marque **Reemplazar políticas existentes**.
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.

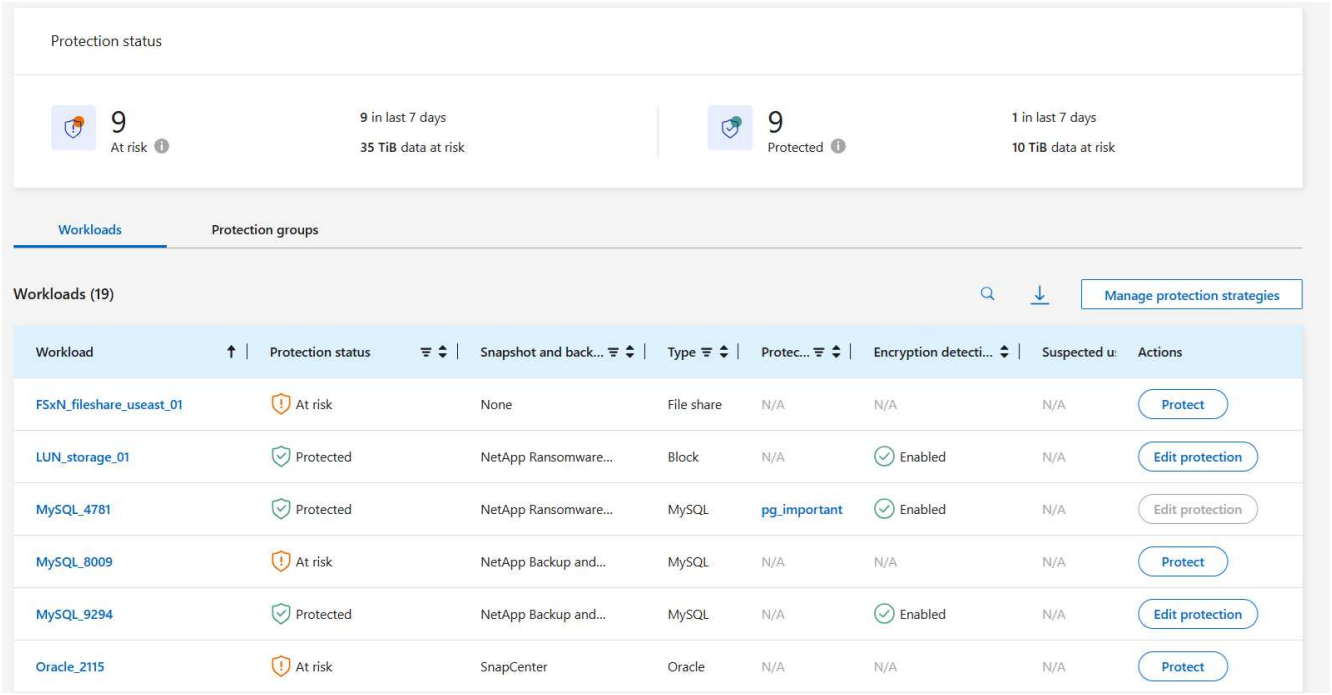
Crear un grupo de protección

Agrupar recursos compartidos de archivos en un grupo de protección facilita la protección de su patrimonio de datos. Ransomware Resilience puede proteger todos los volúmenes de un grupo al mismo tiempo en lugar de proteger cada volumen por separado.

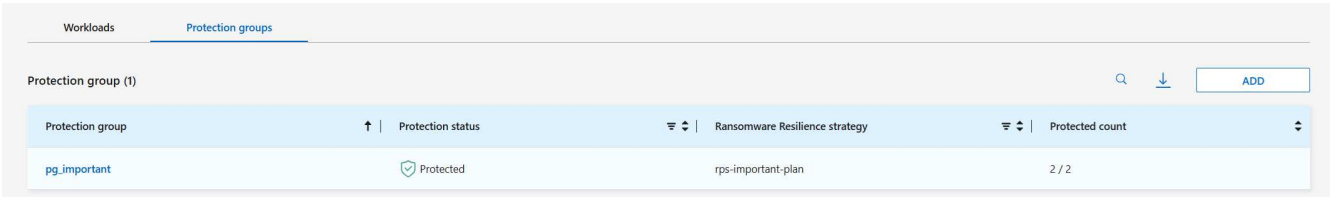
Puede crear grupos independientemente de su estado de protección (es decir, grupos no protegidos y grupos que están protegidos). Cuando agrega una política de protección a un grupo de protección, la nueva política de protección reemplaza cualquier política existente, incluidas las políticas administradas por SnapCenter y NetApp Backup and Recovery.

Pasos

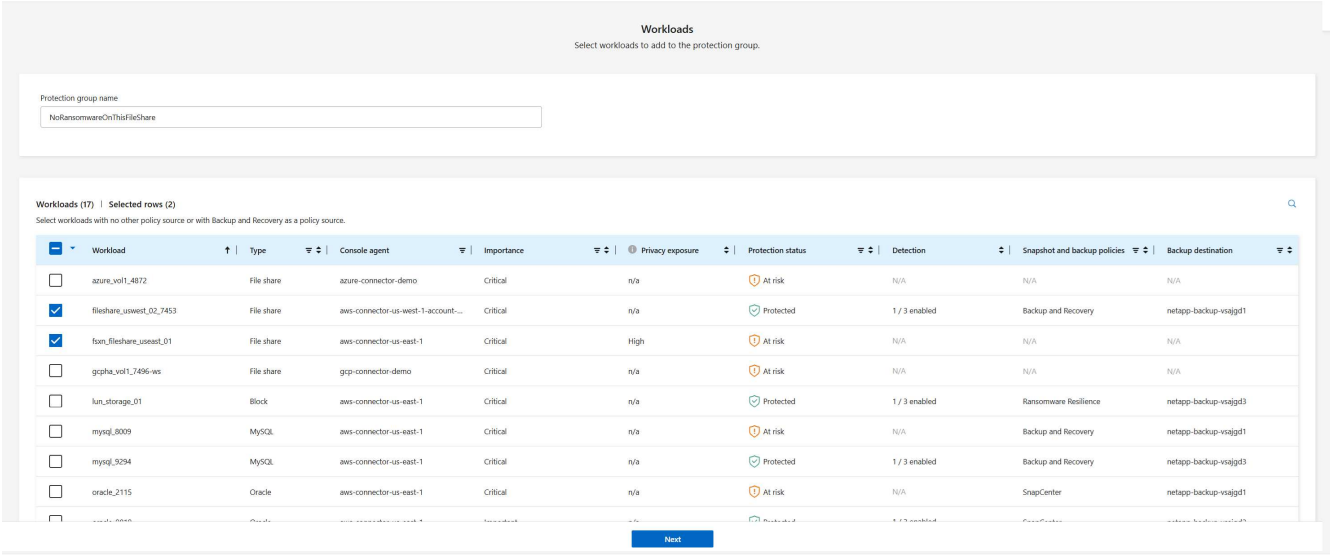
1. En el menú Resiliencia ante ransomware, seleccione **Protección**.



2. Desde la página Protección, seleccione la pestaña **Grupos de protección**.



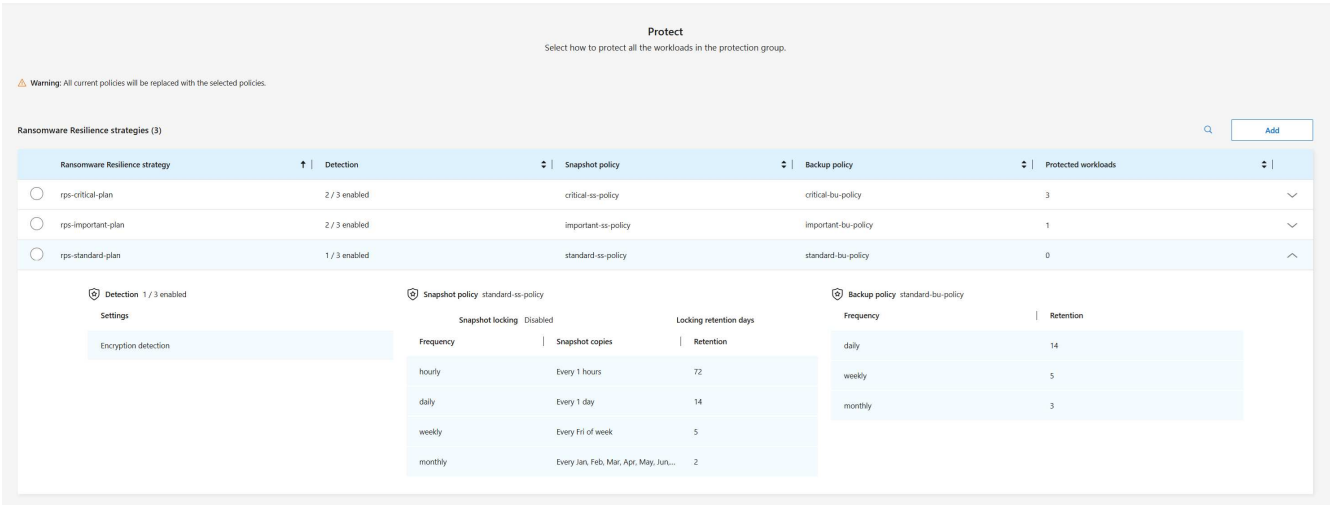
3. Seleccione **Agregar**.



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. Seleccione la política que regirá la protección para este grupo. Para confirmar, seleccione **Siguiente**.
   a. Si necesita configurar una política de respaldo, elija una y luego seleccione **Siguiente**.
   b. Si su política de detección incluye la detección del comportamiento del usuario, seleccione el recopilador de datos que desea utilizar y luego **Siguiente**.
8. Revise las selecciones para el grupo de protección.
9. Para finalizar la creación del grupo de protección, seleccione **Agregar**.

Editar la protección del grupo

Puede cambiar la política de detección en un grupo existente.

Pasos

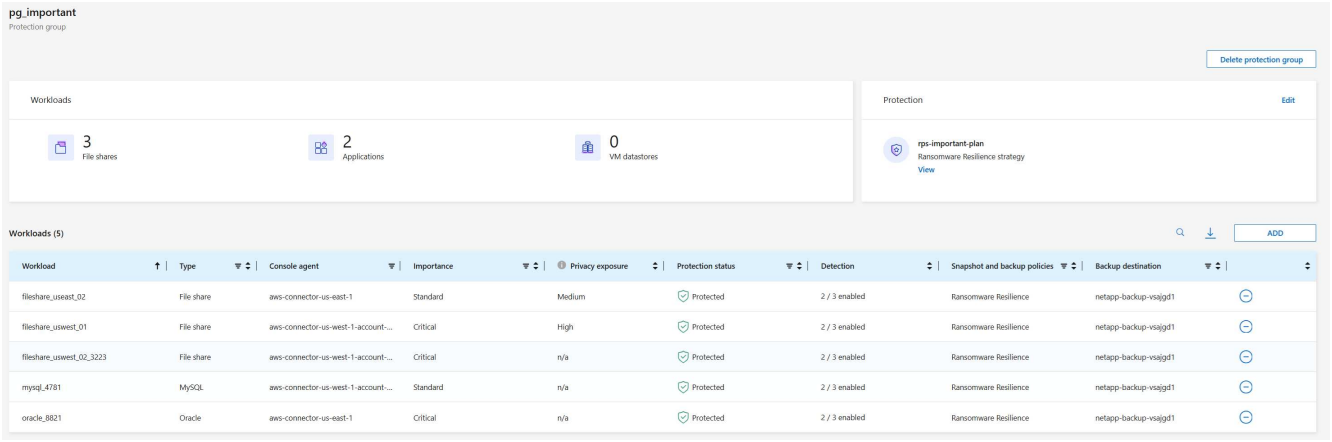
1. En el menú Resiliencia ante ransomware, seleccione **Protección**.
2. Desde la página Protección, seleccione la pestaña **Grupos de protección** y luego seleccione el grupo cuya política desea modificar.
3. Desde la página de descripción general del grupo de protección, seleccione **Editar protección**.
4. Seleccione una política de protección existente para aplicar o seleccione **Agregar** para crear una nueva política de protección. Para obtener más información sobre cómo agregar una política de protección, consulteCrear una política de protección . Luego seleccione **Guardar**.
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

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



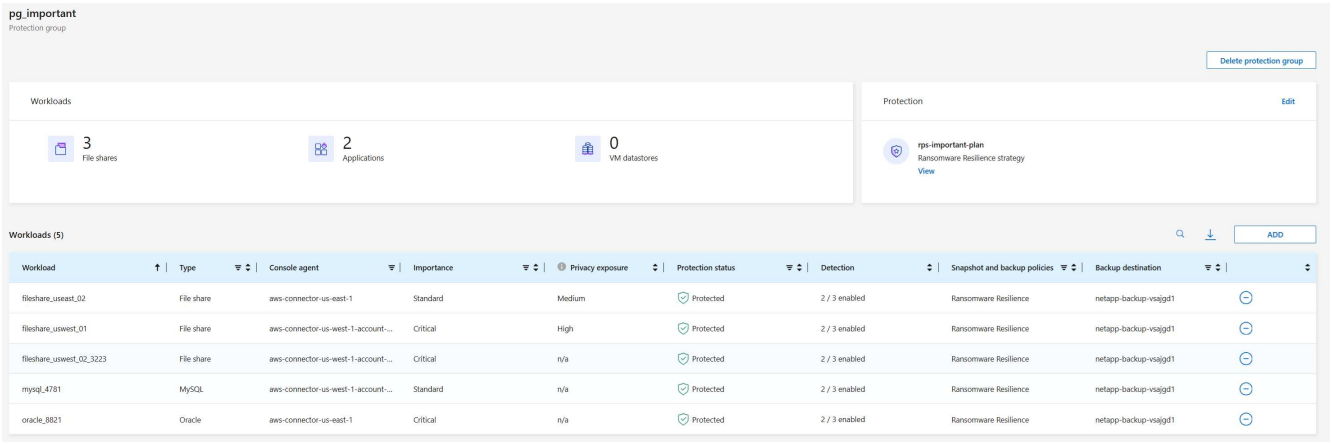
4. Desde la página del grupo de protección seleccionado, seleccione la carga de trabajo que desea eliminar del grupo y seleccione *Acciones* ••• opción.
5. En el menú Acciones, seleccione **Eliminar carga de trabajo**.
6. Confirme que desea eliminar la carga de trabajo y seleccione **Eliminar**.

Eliminar el grupo de protección

Al eliminar el grupo de protección, se elimina el grupo y su protección, pero no se eliminan 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**.

Gestionar estrategias de protección contra ransomware

Puedes eliminar una estrategia de ransomware.

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

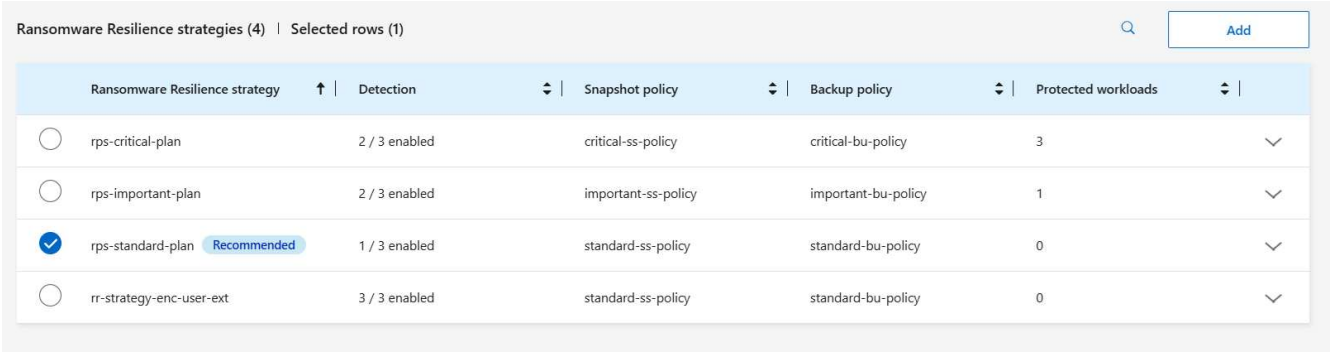
Antes de eliminar una estrategia de protección contra ransomware, es posible que desee ver qué cargas de trabajo están protegidas por esa estrategia.

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**.

Busque información de identificación personal con la NetApp Data Classification en Ransomware Resilience

Dentro de NetApp Ransomware Resilience, puede utilizar NetApp Data Classification para escanear y clasificar los datos en una carga de trabajo de uso compartido de archivos. La clasificación de datos le ayuda a determinar si el conjunto de datos incluye información de identificación personal (PII), lo que puede aumentar los riesgos de seguridad. La clasificación de datos es un componente central de la NetApp Console y está disponible sin costo adicional.

"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.

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:

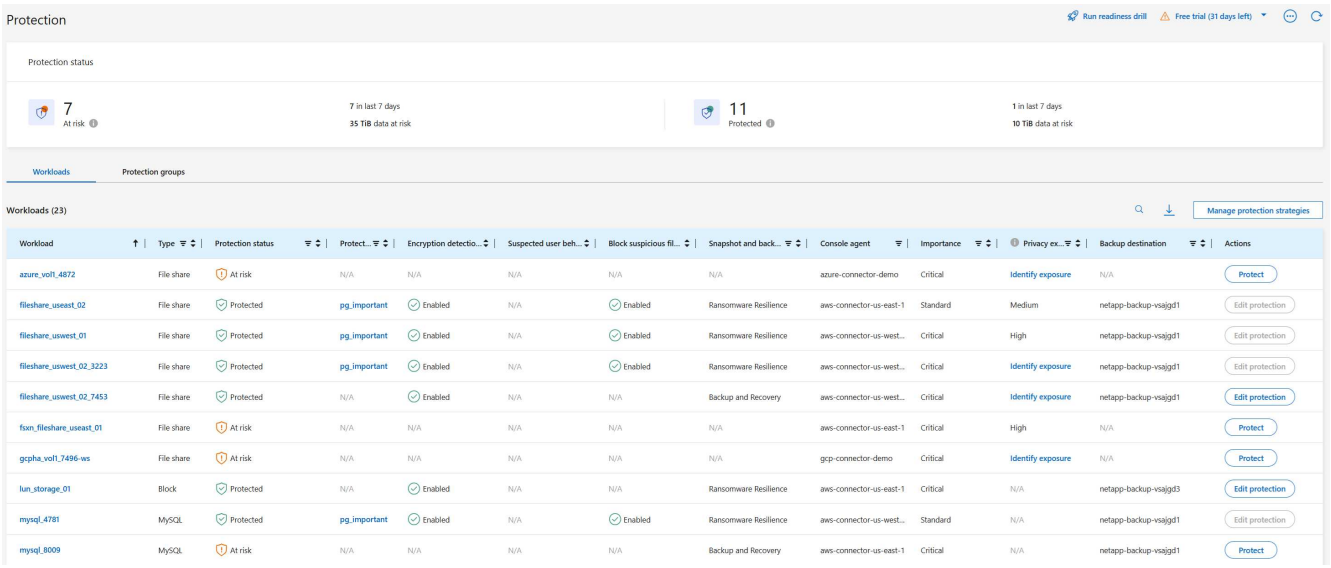
- "Aprenda sobre la clasificación de datos"
- "Categorías de datos privados"
- "Investigue los datos almacenados en su organización"

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

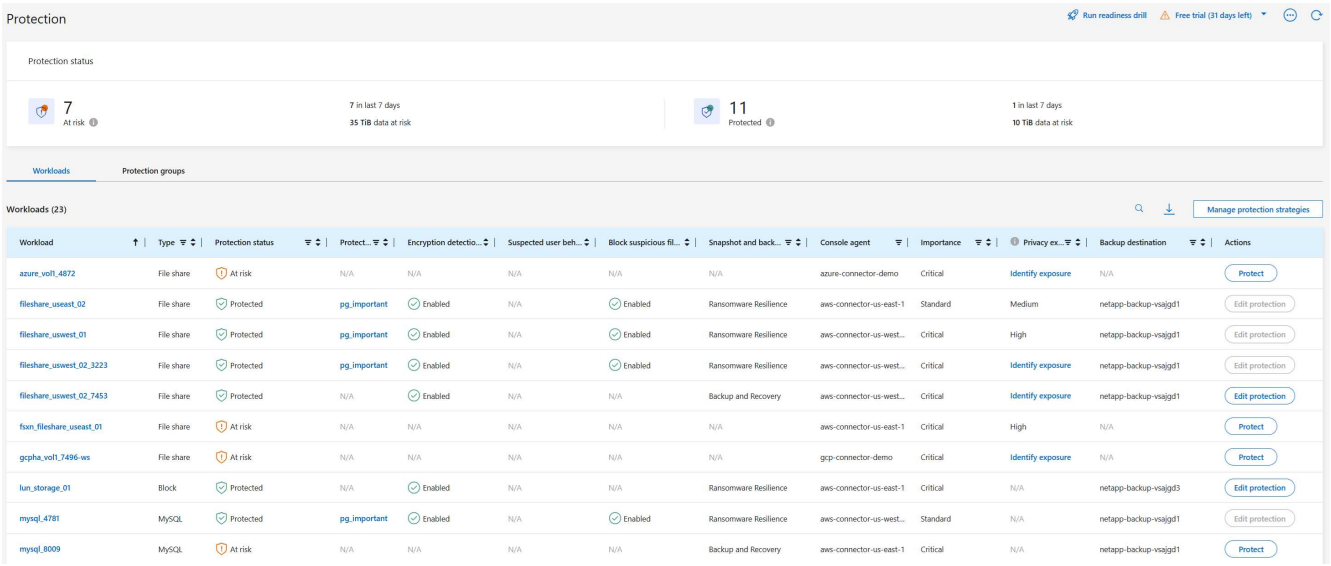
Después de los análisis de clasificación de datos en busca de información personal identificable, evalúe el riesgo.

Los datos PII se clasifican en una de tres designaciones:

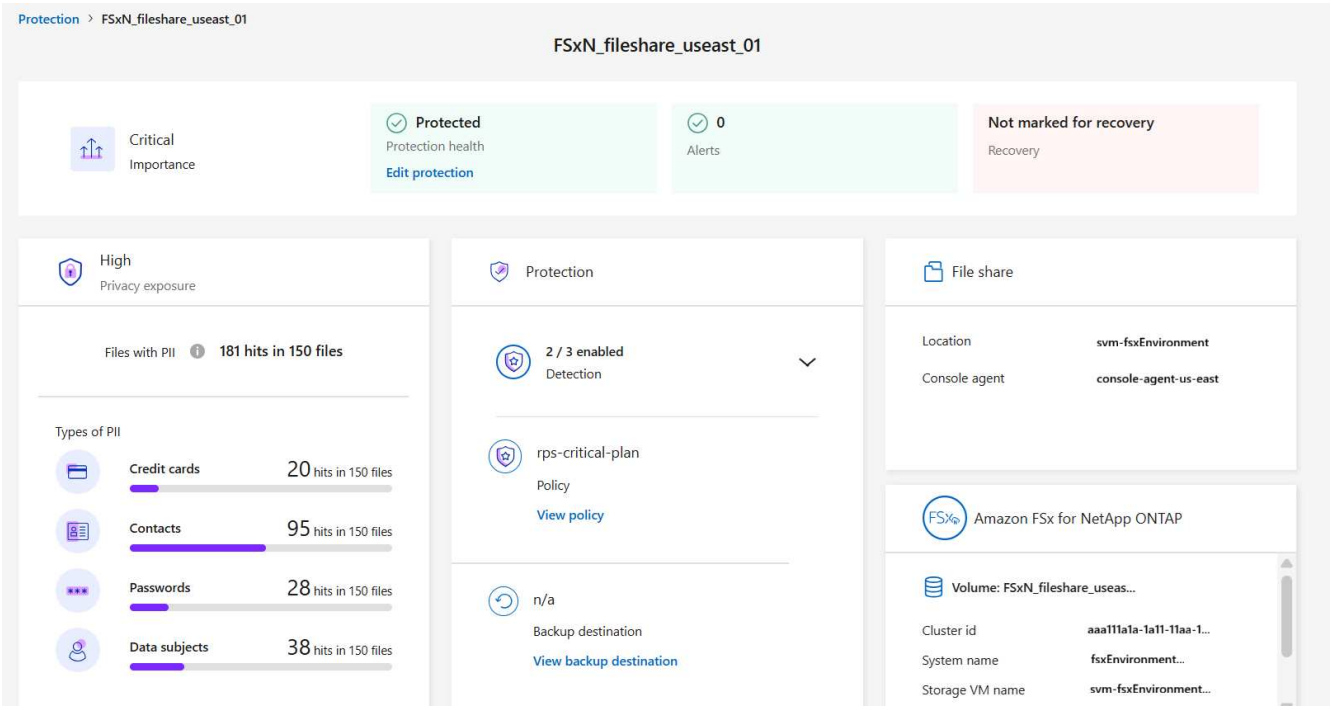
- **Alto**: Más del 70% de los archivos contienen información personal identificable
- **Medio**: Más del 30% y menos del 70% de los archivos contienen información de identificación personal (PII)
- **Bajo**: Más del 0% y menos del 30% de los archivos contienen información personal identificable

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"

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 área de Notificaciones. Ransomware Resilience toma una instantánea inmediatamente. Revise el riesgo potencial en la pestaña **Alertas** de resiliencia ante ransomware.

Si Ransomware Resilience detecta un posible ataque, aparece una notificación en la configuración de notificaciones de la consola y se envía un correo electrónico a la dirección configurada. El correo electrónico incluye información sobre la gravedad, la carga de trabajo afectada y un enlace a la alerta en la pestaña **Alertas** de resiliencia ante ransomware.

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.

Ransomware Resilience proporciona información llamada *evidencia* sobre lo que causó que se emitiera la alerta, como la siguiente:

- 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
- Cuando el cifrado es alto, sin cambios en la extensión del archivo

Una alerta se clasifica como una de las siguientes:

- **Ataque potencial**: se produce una alerta cuando Autonomous Ransomware Protection detecta una nueva extensión y la ocurrencia se repite más de 20 veces en las últimas 24 horas (comportamiento predeterminado).
- **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 los entornos SAN, las advertencias solo se basan en 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" .

Una alerta puede tener uno de los siguientes estados:

- **Nuevo**
- **Inactivo**

Un incidente de alerta puede tener los siguientes estados:

- **Nuevo**: Todos los incidentes se marcan como "nuevos" cuando se identifican por primera vez.
- **Descartado**: si sospecha que la actividad no es un ataque de ransomware, puede cambiar el estado a "Descartado".

Después de descartar un ataque, no puedes revertir su estado. Si descarta una carga de trabajo, todas las copias instantáneas tomadas automáticamente en respuesta al posible ataque de ransomware se eliminarán de forma permanente.

- **Desestimando**: El incidente está en proceso de ser desestimado.
- **Resuelto**: El incidente ha sido solucionado.
- **Resuelto automáticamente**: para alertas de baja prioridad, el incidente se resuelve automáticamente si no se han tomado medidas al respecto dentro de cinco días.

Si configuró un sistema de gestión de eventos y seguridad (SIEM) en Ransomware Resilience en la página Configuración, Ransomware Resilience envía detalles de alerta a su sistema SIEM.

Ver alertas

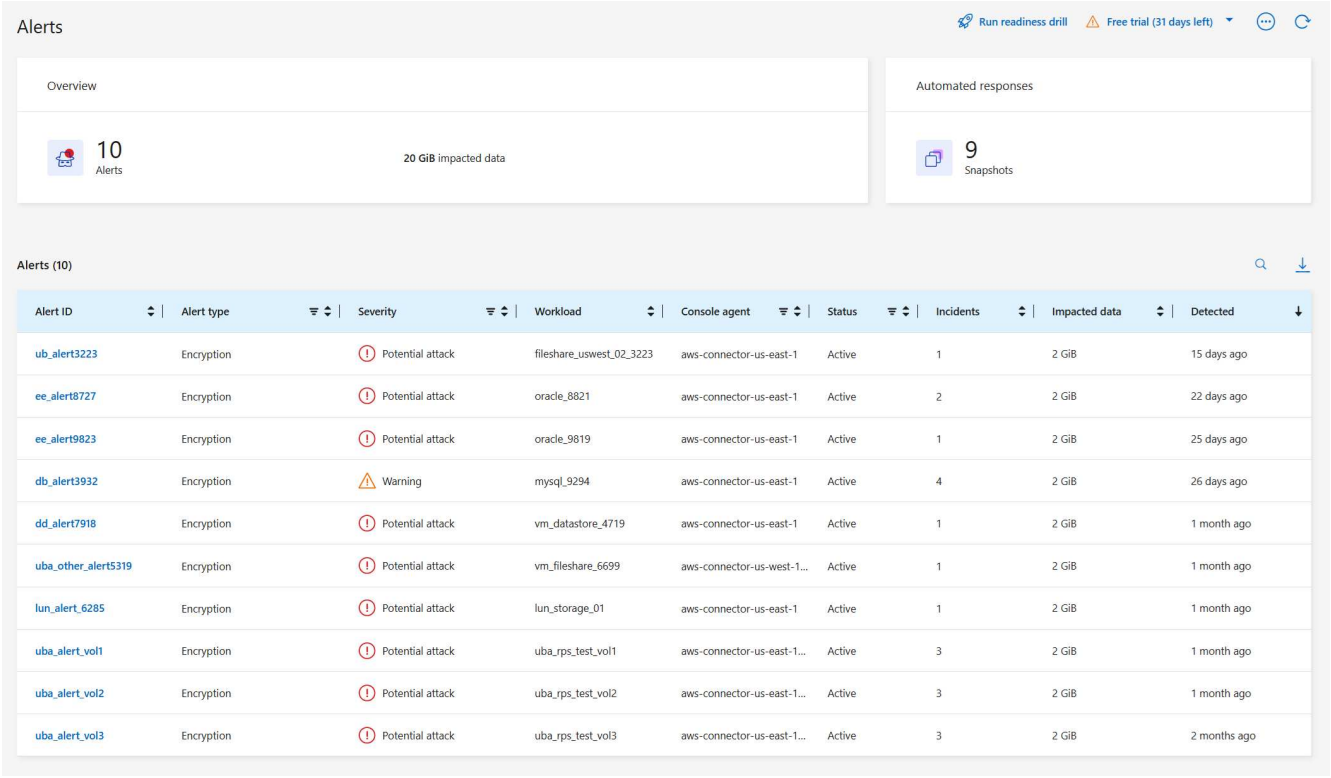
Puede acceder a las alertas desde el Panel de resiliencia ante ransomware o desde la pestaña **Alertas**.

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 resiliencia ante ransomware, revise el panel 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 ataque potencial, envía una notificación por correo electrónico a los usuarios suscritos según sus preferencias de notificación de suscripción. El correo electrónico contiene información sobre la alerta, incluida la gravedad y los recursos afectados.

Puede recibir notificaciones por correo electrónico sobre alertas de resiliencia ante ransomware. Esta función le ayuda a mantenerse informado sobre las alertas, su gravedad y los recursos afectados.

Para suscribirse a las notificaciones por correo electrónico, consulte "Establecer la configuración de notificaciones por correo electrónico" .

1. En Ransomware Resilience, vaya a la página **Configuración**.
2. En **Notificaciones**, busque la configuración de notificaciones por correo electrónico.
3. Introduzca la dirección de correo electrónico donde desea recibir alertas.
4. Guarde sus cambios.

Ahora recibirá notificaciones por correo electrónico cuando se generen nuevas 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. Ver el correo electrónico.
2. En el correo electrónico, seleccione **Ver alerta** e inicie 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, haga clic en **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.

Debe haber configurado un agente de actividad del usuario y habilitado una política de protección con detección de comportamiento del usuario para ver alertas a nivel de usuario. Cuando la detección del comportamiento del usuario está habilitada, la columna **Usuario sospechoso** aparece en el panel de Alertas; no se muestra cuando la detección del comportamiento del usuario no está habilitada. Para habilitar la detección de usuarios sospechosos, consulte"Actividad sospechosa del usuario" .

Si utiliza NetApp Data Infrastructure Insights (DII) Workload Security, se recomienda que utilice los mismos agentes de Workload Security para la resiliencia frente al ransomware. No es necesario implementar agentes de seguridad de carga de trabajo separados para Ransomware Resilience; sin embargo, usar los mismos agentes de seguridad de carga de trabajo requiere una relación de emparejamiento entre la organización de la consola de Ransomware Resilience y el inquilino de seguridad de carga de trabajo de almacenamiento DII. Comuníquese con su representante de cuenta para habilitar este emparejamiento.

Ver actividad maliciosa

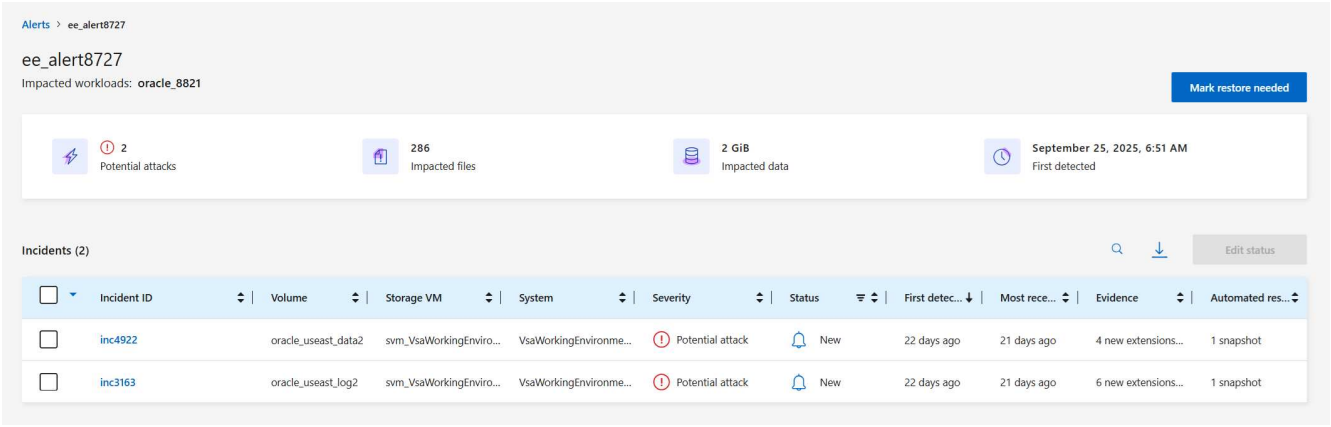
Cuando Autonomous Ransomware Protection activa una alerta en Ransomware Resilience, puedes ver los siguientes detalles:

- 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
- 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 ha configurado la detección de usuarios sospechosos para ver el comportamiento anómalo de los usuarios, puede ver datos a nivel de usuario y bloquear usuarios específicos. Para habilitar la configuración de usuarios sospechosos, consulte"Configurar los ajustes de resiliencia frente al ransomware" .

Pasos

1. En el menú Resiliencia ante ransomware, seleccione **Alertas**.
2. Seleccione una alerta.
3. Revise los incidentes en la alerta.
4. Para bloquear a un usuario sospechoso en su entorno, seleccione **Bloquear** debajo del nombre del usuario.

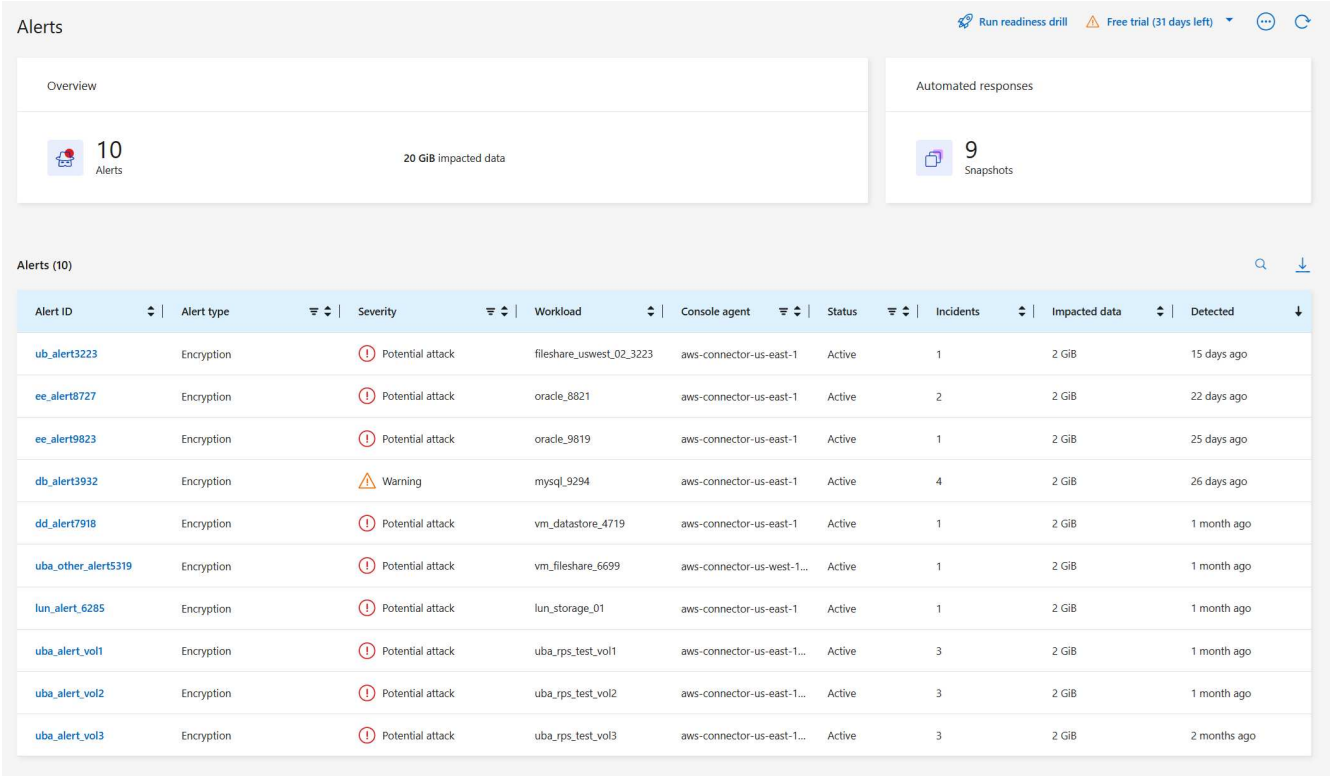
Marcar los incidentes de ransomware como listos para recuperación (después de que se neutralizan los incidentes)

Después de detener el ataque, notifique a su administrador de almacenamiento que los datos están listos para que puedan comenzar la recuperación.

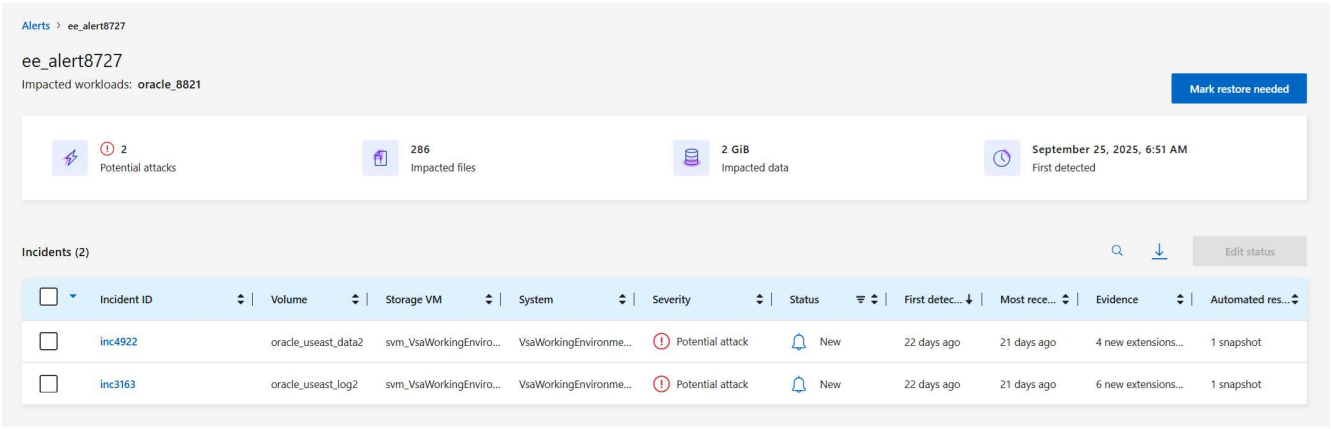
Rol de consola requerido Para realizar esta tarea, necesita el rol de administrador de organización, administrador de carpeta o proyecto, o administrador de resiliencia ante ransomware. "Obtenga información sobre las funciones de resiliencia ante ransomware para la NetApp Console" .

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.

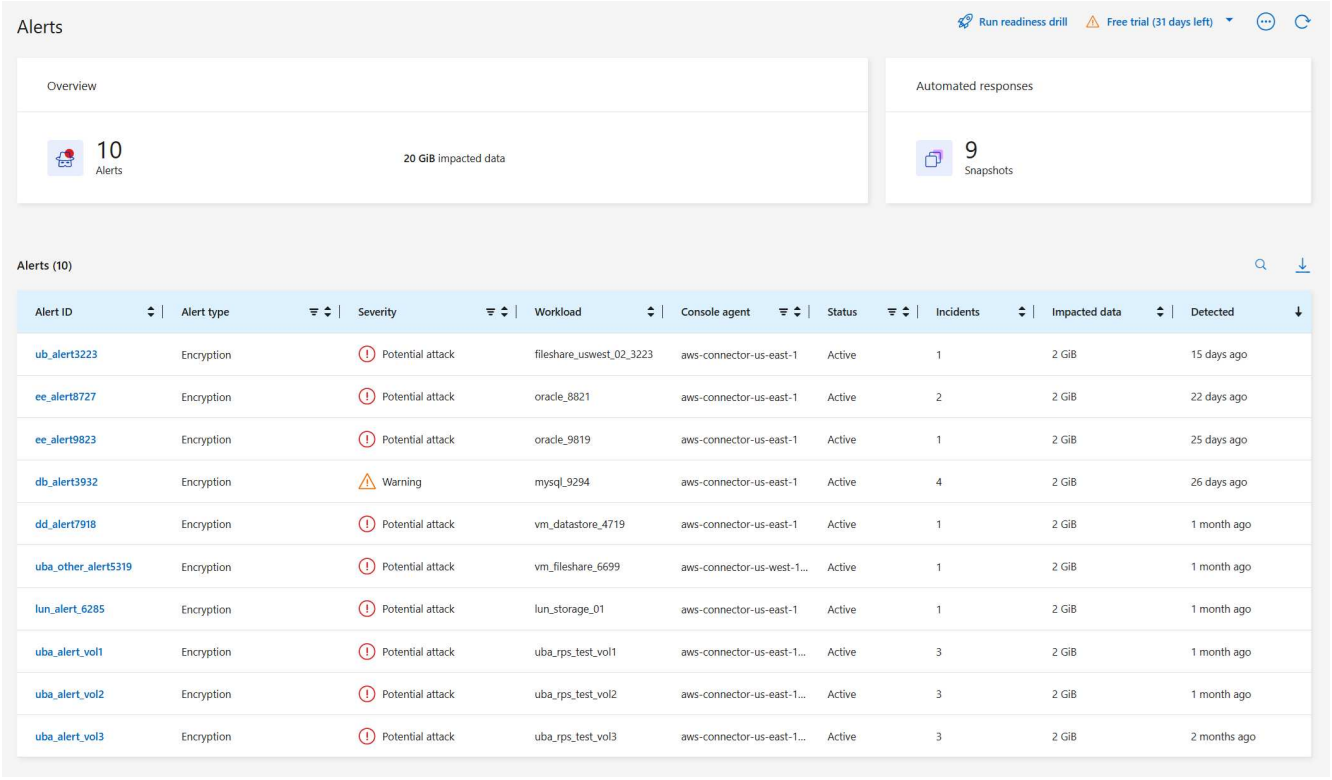
Si descarta una carga de trabajo, todas las copias instantáneas tomadas automáticamente en respuesta a un posible ataque de ransomware se eliminan de forma permanente.

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

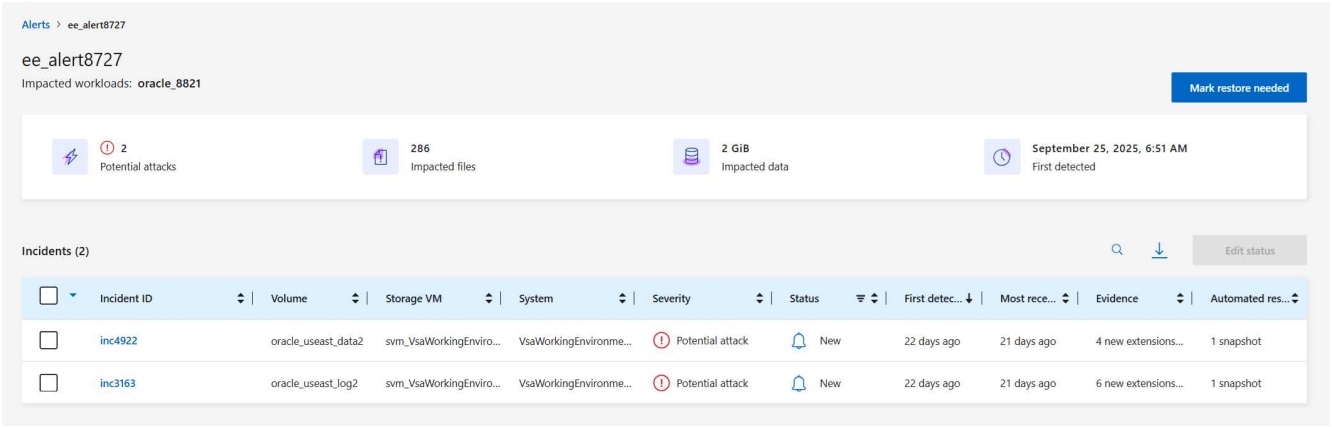
Rol de consola requerido Para realizar esta tarea, necesita el rol de administrador de organización, administrador de carpeta o proyecto, o administrador de resiliencia ante ransomware. "Obtenga información sobre las funciones de resiliencia ante ransomware para la NetApp Console" .

Pasos

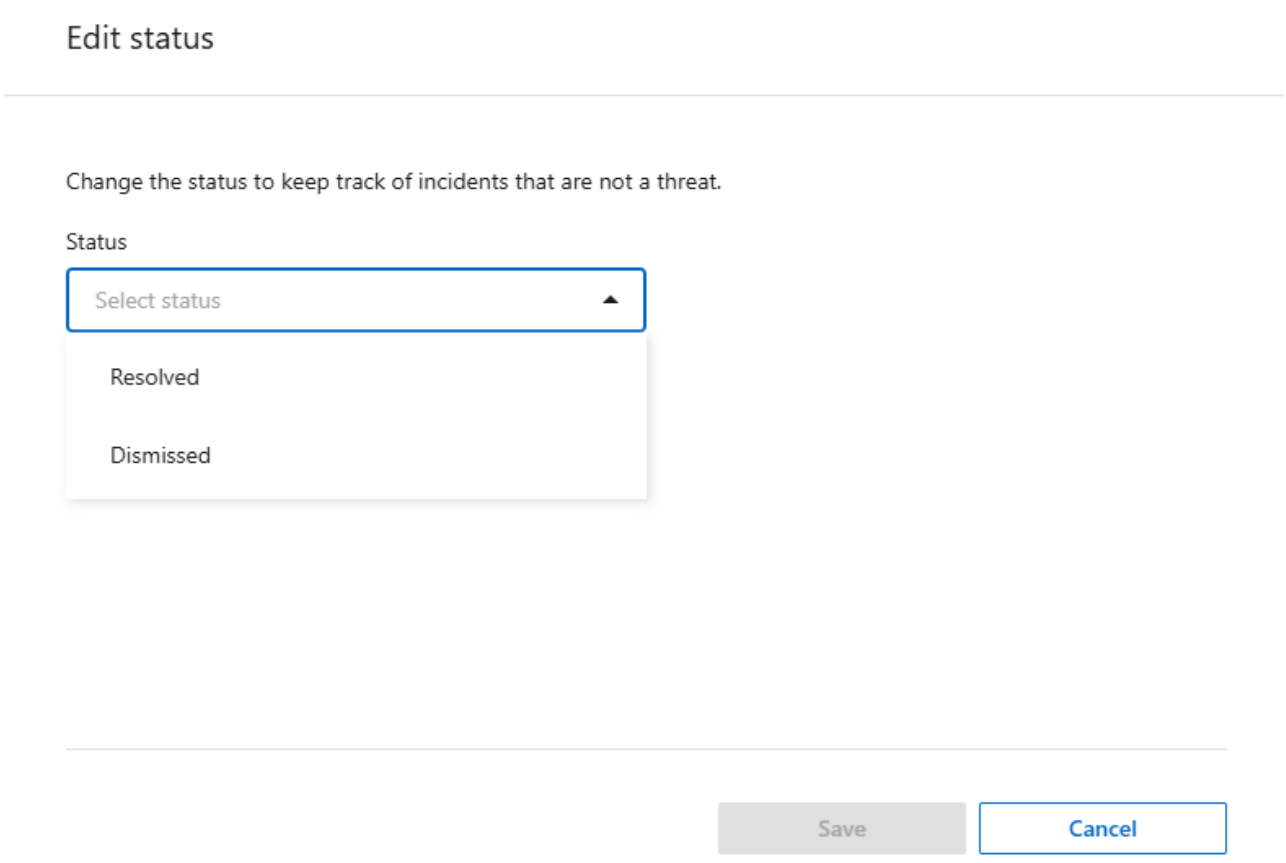
1. En el menú Resiliencia ante ransomware, seleccione **Alertas**.



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.

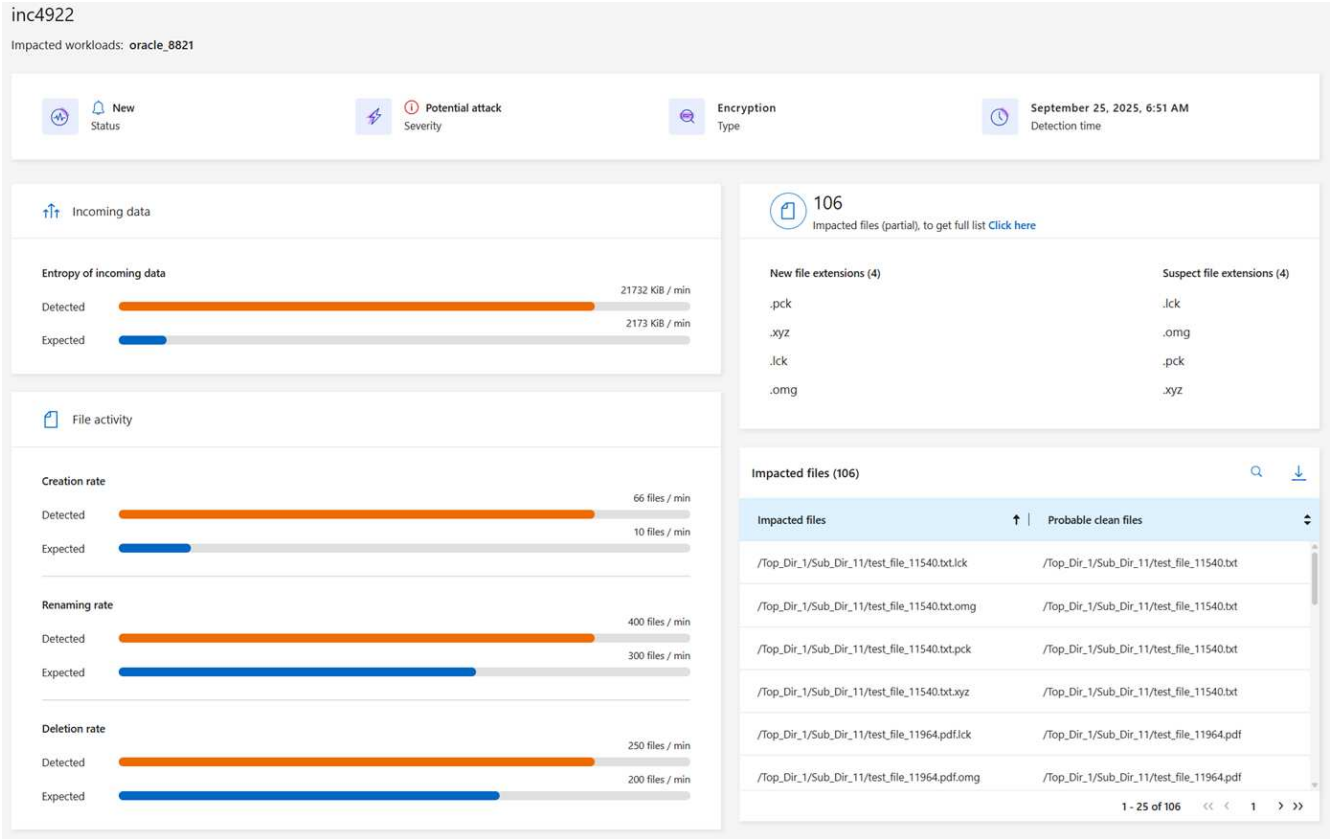
Rol de consola requerido Para realizar esta tarea, necesita el rol de administrador de organización, administrador de carpeta o proyecto, o administrador de resiliencia ante ransomware. "Obtenga información sobre las funciones de resiliencia ante ransomware para la NetApp Console" .

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.

Recupérese de un ataque de ransomware (después de neutralizar los incidentes) 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 administrada por SnapCenter, Ransomware Resilience restaura la aplicación o la máquina virtual a su estado anterior y a su última transacción mediante el proceso consistente con la aplicación o la máquina virtual. La restauración consistente con la aplicación o la máquina virtual agrega cualquier dato que no haya llegado al almacenamiento (por ejemplo, datos en caché o en una operación de E/S) a los datos en el volumen.
- Si la aplicación o la máquina virtual *no* está administrada por SnapCenter y está administrada por NetApp Backup and Recovery o Ransomware Resilience, Ransomware Resilience realiza una restauración consistente ante fallas, donde se restauran todos los datos que estaban en el volumen en el mismo punto en el tiempo, por ejemplo, si el sistema falla.

  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:

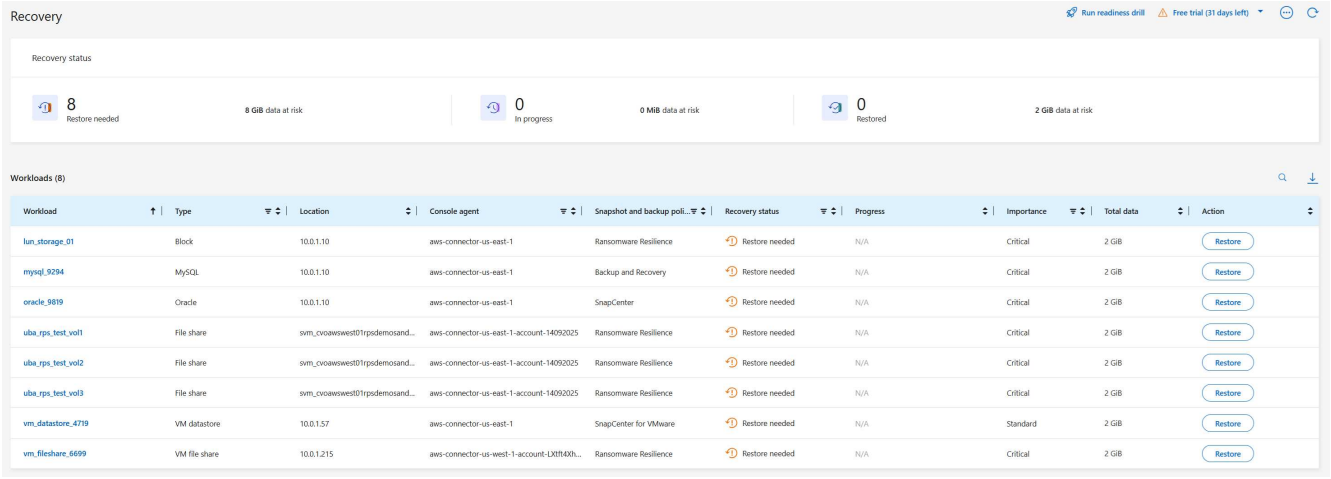
- **Se necesita restaurar**: Es necesario restaurar la carga de trabajo.
- **En progreso**: La operación de restauración está actualmente en curso.
- **Restaurado**: La carga de trabajo ha sido restaurada.
- **Error**: No se pudo completar el proceso de restauración de la carga de trabajo.

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, revise los totales de "Restauración necesaria" en el panel de Alertas y seleccione **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 administrada por SnapCenter

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.

El estado de la aplicación cambiará si es necesario para la restauración. La aplicación se restaurará a su estado anterior desde los archivos de control, si están incluidos en la copia de seguridad. Una vez finalizada la restauración, la aplicación se abre en modo LECTURA-ESCRITURA.

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 Resiliencia contra 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. **Ámbito de restauración**: consistente con la aplicación (o, para SnapCenter para máquinas virtuales, el ámbito de restauración es "Por máquina virtual")
6. **Fuente**: Seleccione la flecha hacia abajo junto a Fuente para ver los detalles. 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 la ubicación original o alternativa.
   b. Seleccione el sistema.
   c. Seleccione la máquina virtual de almacenamiento.
8. Si el destino original no tiene suficiente espacio para restaurar la carga de trabajo, aparece una fila de "Almacenamiento temporal". Puede seleccionar el almacenamiento temporal para restaurar los datos de la carga de trabajo. Los datos restaurados se copiarán del almacenamiento temporal a la ubicación original.

Haga clic en la **flecha hacia abajo** en la fila de almacenamiento temporal y configure el clúster de destino, la máquina virtual de almacenamiento y el nivel local.

9. Seleccione **Guardar**.
10. Seleccione **Siguiente**.
11. Revise sus selecciones.
12. Seleccione **Restaurar**.
13. 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 no administrada por SnapCenter

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

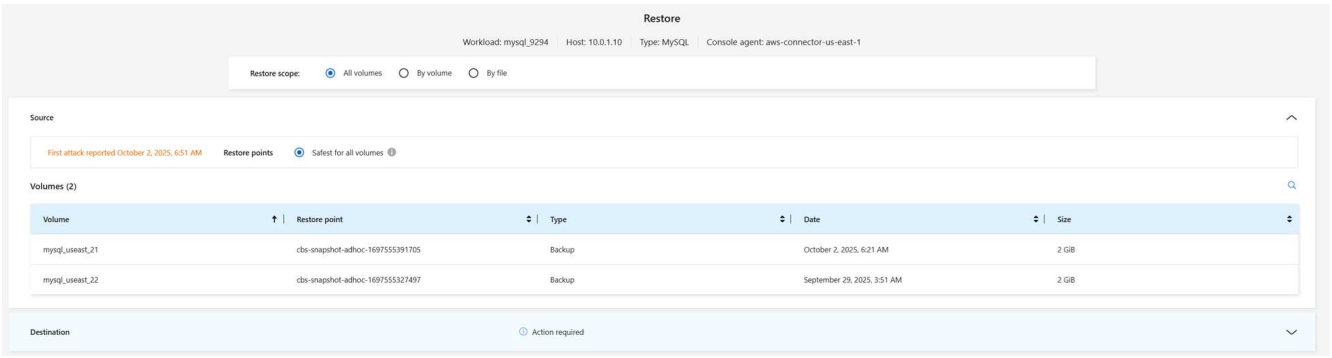
1. En el menú Resiliencia ante ransomware, seleccione **Recuperación**.
2. Revise la información de la carga de trabajo en la página **Recuperación**.
3. Seleccione una carga de trabajo que esté en el estado "Se necesita restaurar".
4. Para restaurar, seleccione **Restaurar**.
5. **Alcance de restauración**: 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.

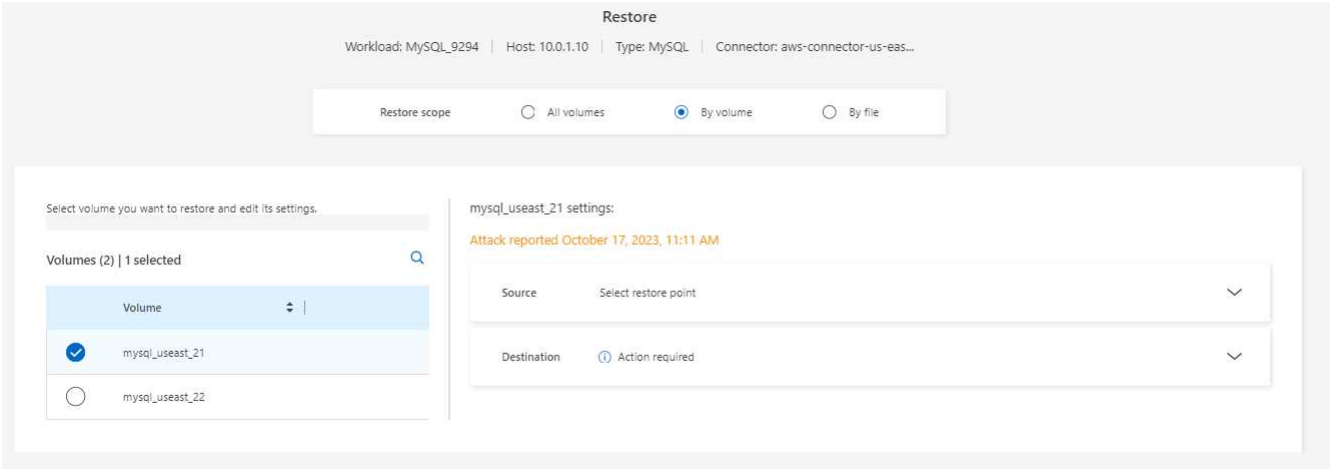
> El nuevo nombre del volumen aparece como prefijo + nombre del volumen original + nombre de la copia de seguridad + fecha de la copia de seguridad.

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.

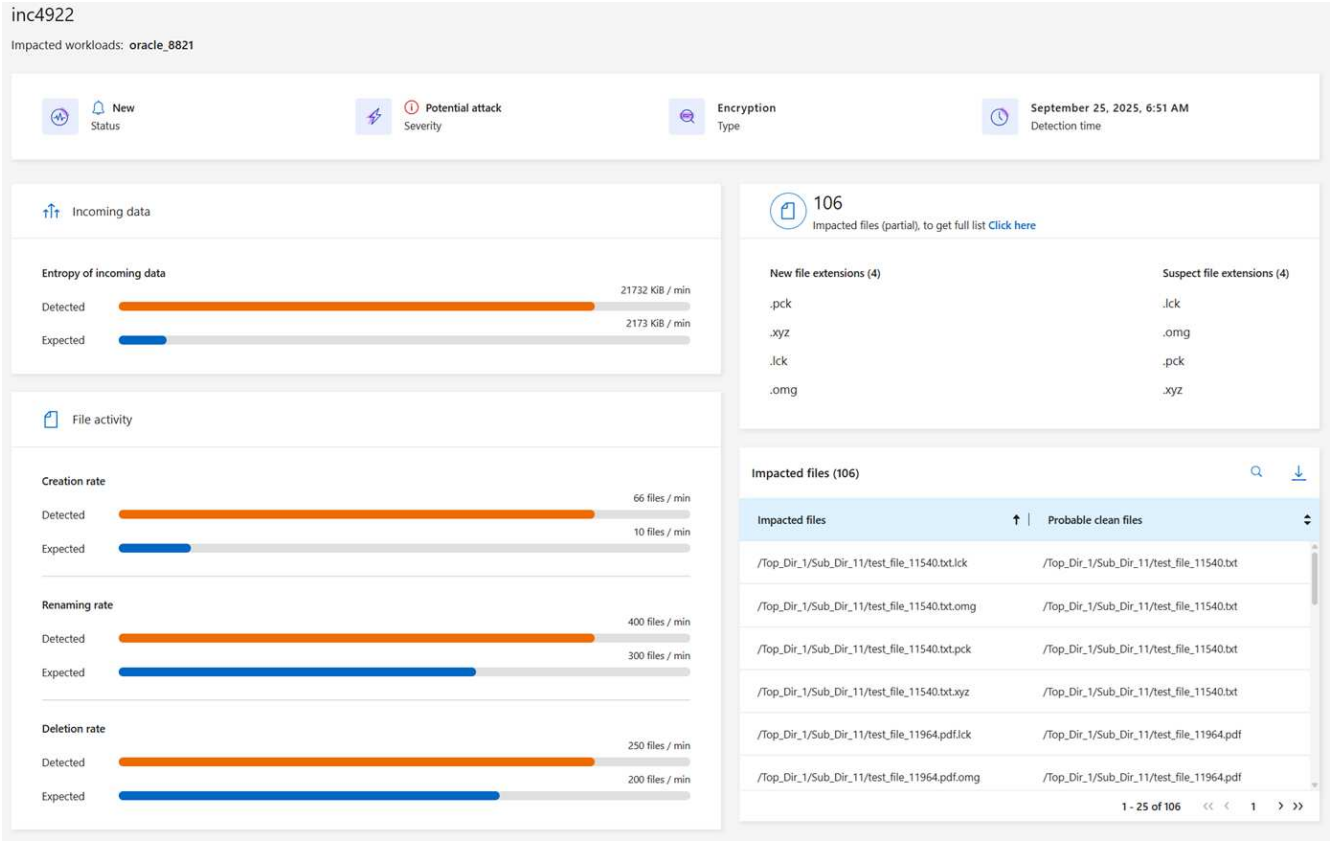
Puede restaurar una carga de trabajo de la aplicación a nivel de archivo en el mismo sistema o en uno diferente.

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.

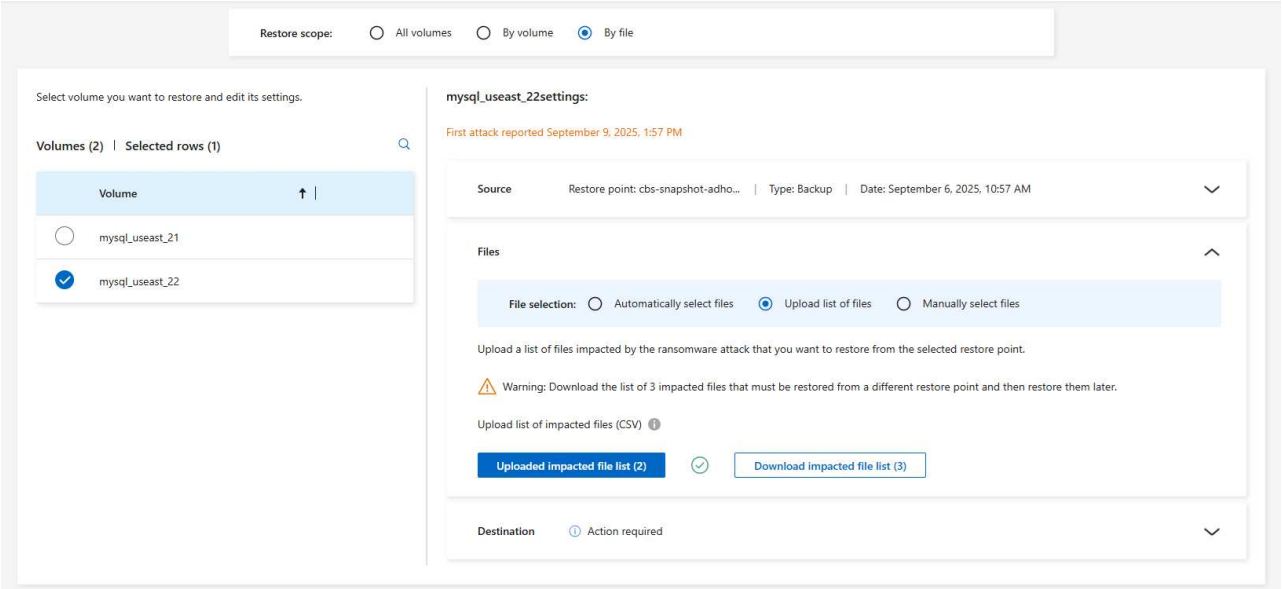
Pasos para restaurar esos archivos

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

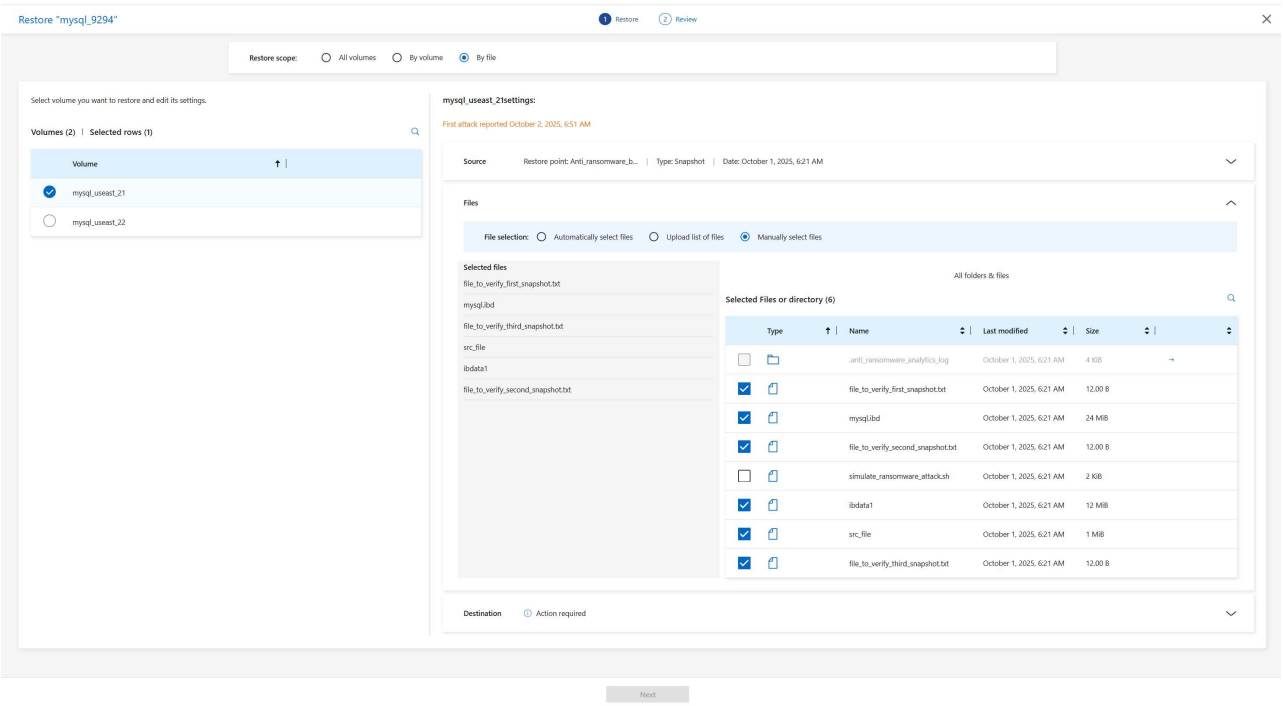
detalles. Seleccione el punto de restauración que desea utilizar para restaurar los datos.

> 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.

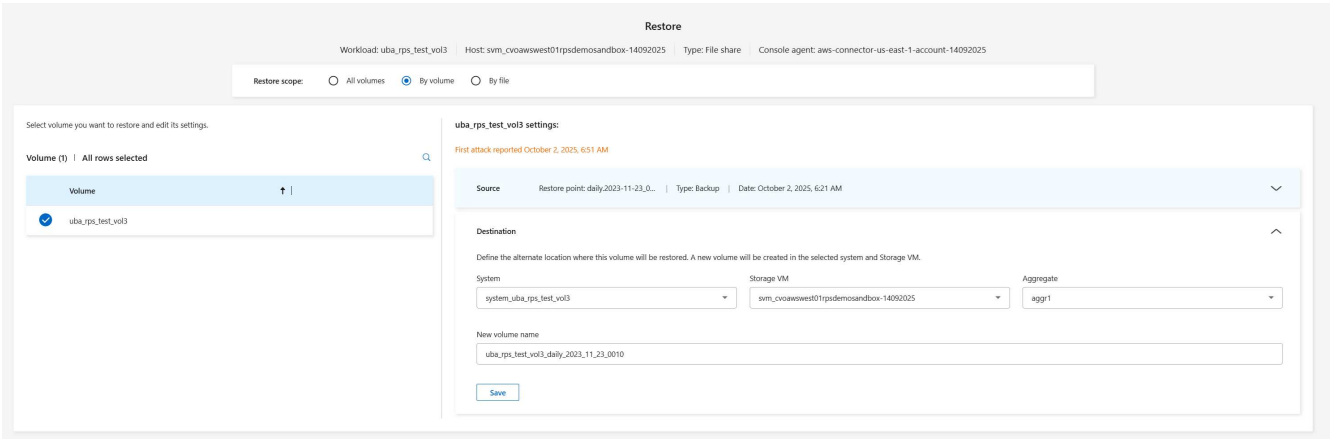
   b. Seleccione el sistema.
   c. Seleccione la máquina virtual de almacenamiento.
   d. Opcionalmente, introduzca la ruta.

      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.

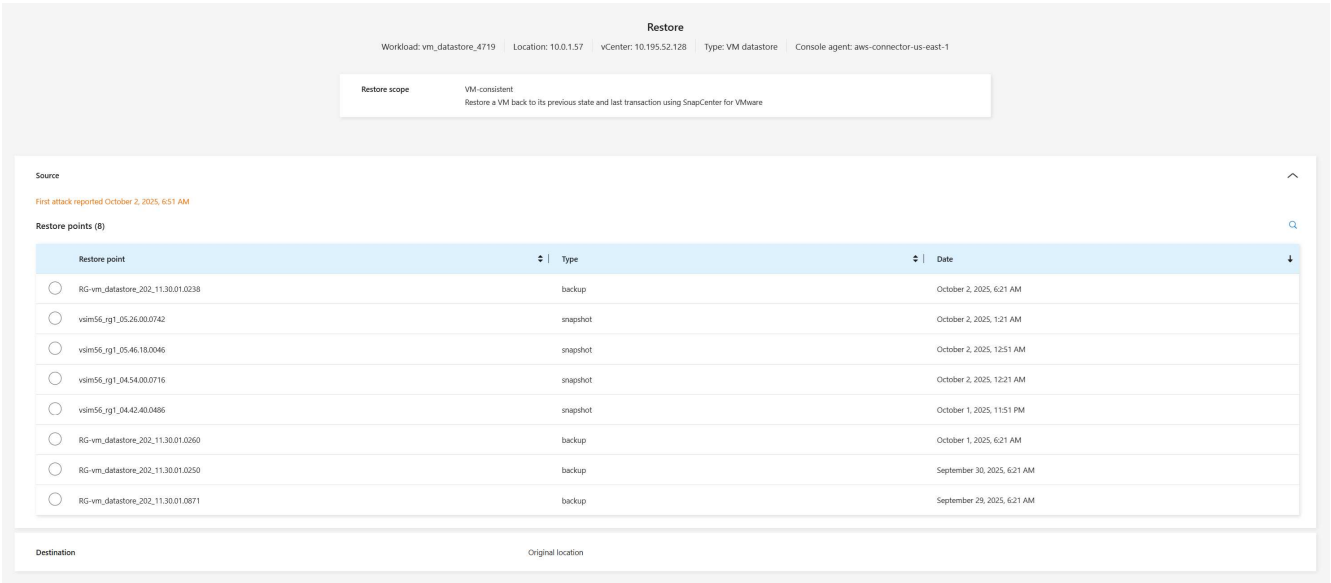
> Si no especifica una ruta para la restauración, los archivos se restaurarán a un nuevo volumen en el directorio de nivel superior.

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.

Descargar informes de NetApp Ransomware Resilience

Puede exportar datos de protección y descargar archivos CSV o JSON que muestran detalles de simulacros de preparación para ataques, protección, alertas y recuperación.

Antes de descargar los archivos, debes actualizar los datos, lo que también actualiza los datos que aparecerán en los archivos.

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:

- **Protección**: Contiene 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.

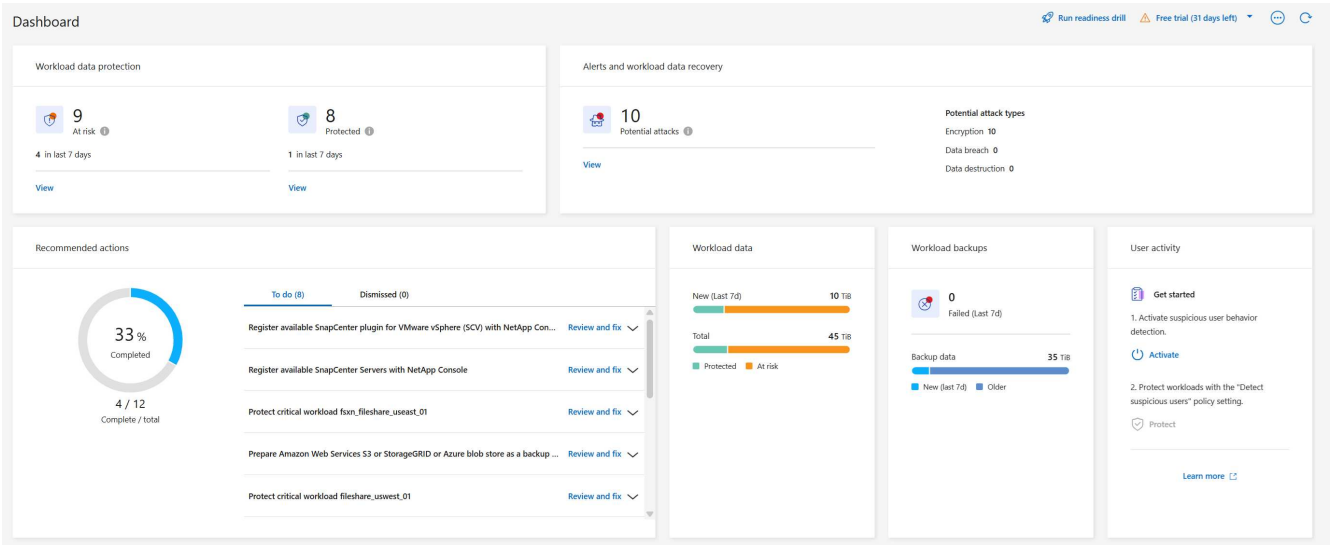
> Puede descargar informes de simulacros de preparación únicamente desde la página **Informes**.

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

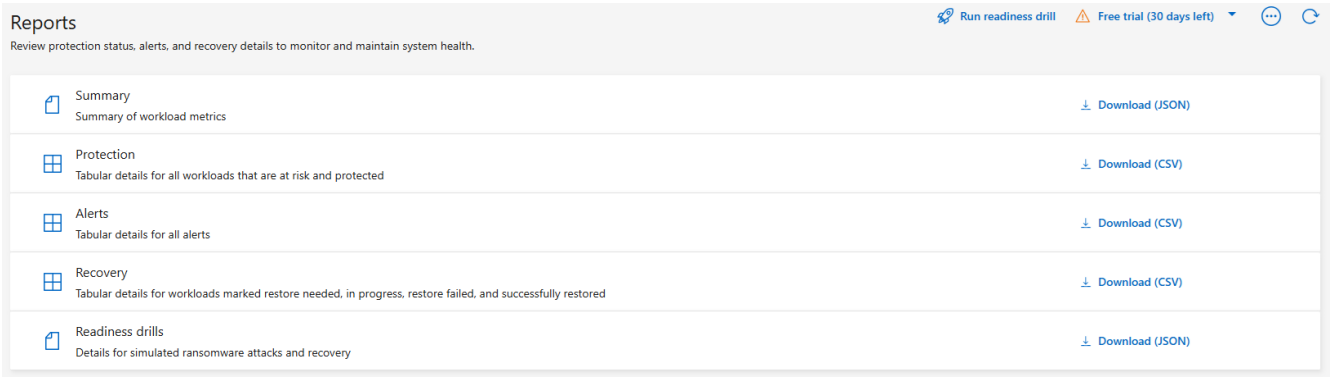
Los archivos CSV o JSON incluyen datos de todas las cargas de trabajo en todos los sistemas de consola.

Pasos

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



2. Desde el Panel de Control u otra página, seleccione *Actualizar* Opción 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**.


Reports
Review protection status, alerts, and recovery details to monitor and maintain system health.
Run readiness drill
Free trial (30 days left)
Summary
Summary of workload metrics
Download (JSON)
Protection
Tabular details for all workloads that are at risk and protected
Download (CSV)
Alerts
Tabular details for all alerts
Download (CSV)
Recovery
Tabular details for workloads marked restore needed, in progress, restore failed, and successfully restored
Download (CSV)
Readiness drills
Details for simulated ransomware attacks and recovery
Download (JSON)

Conocimiento y apoyo

Regístrese para recibir asistencia

Es necesario registrarse para recibir soporte técnico específico para la NetApp Console y sus soluciones de almacenamiento y servicios de datos. También es necesario registrarse para obtener soporte técnico para habilitar flujos de trabajo clave para los sistemas Cloud Volumes ONTAP .

Registrarse para recibir soporte no habilita el soporte de NetApp para un servicio de archivos de un proveedor de nube. Para obtener asistencia técnica relacionada con un servicio de archivos de un proveedor de nube, su infraestructura o cualquier solución que utilice el servicio, consulte "Obtener ayuda" en la documentación de ese producto.

- "Amazon FSx para ONTAP"
- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

Descripción general del registro de soporte

Existen dos formas de registro para activar el derecho a recibir ayuda:

- Registrar el número de serie de su cuenta de la NetApp Console (su número de serie 960xxxxxxxx de 20 dígitos ubicado en la página Recursos de soporte en la consola).

  Esto sirve como su ID de suscripción de soporte único para cualquier servicio dentro de la Consola. Cada cuenta de consola debe estar registrada.

- Registrar los números de serie de Cloud Volumes ONTAP asociados con una suscripción en el mercado de su proveedor de nube (son números de serie 909201xxxxxxxx de 20 dígitos).

  Estos números de serie se conocen comúnmente como *números de serie PAYGO* y son generados por la NetApp Console en el momento de la implementación de Cloud Volumes ONTAP .

El registro de ambos tipos de números de serie permite funciones como la apertura de tickets de soporte y la generación automática de casos. El registro se completa agregando cuentas del sitio de soporte de NetApp (NSS) a la consola como se describe a continuación.

Registrar la NetApp Console para obtener soporte de NetApp

Para registrarse para recibir soporte y activar el derecho a soporte, un usuario de su cuenta de NetApp Console debe asociar una cuenta del sitio de soporte de NetApp con su inicio de sesión de consola. La forma de registrarse para el soporte de NetApp depende de si ya tiene una cuenta del sitio de soporte de NetApp (NSS).

Cliente existente con una cuenta NSS

Si es cliente de NetApp con una cuenta NSS, simplemente necesita registrarse para recibir soporte a través de la consola.

Pasos

1. Seleccione **Administración** > **Credenciales**.
2. Seleccione **Credenciales de usuario**.
3. Seleccione **Agregar credenciales NSS** y siga las instrucciones de autenticación del Sitio de soporte de NetApp (NSS).
4. Para confirmar que el proceso de registro fue exitoso, seleccione el ícono de Ayuda y seleccione **Soporte**.

   La página **Recursos** debería mostrar que su cuenta de consola está registrada para recibir soporte.

   Tenga en cuenta que otros usuarios de la consola no verán este mismo estado de registro de soporte si no han asociado una cuenta del sitio de soporte de NetApp con su inicio de sesión. Sin embargo, eso no significa que su cuenta no esté registrada para recibir soporte. Siempre que un usuario de la organización haya seguido estos pasos, su cuenta quedará registrada.

Soy cliente actual pero no tengo cuenta NSS

Si es un cliente existente de NetApp con licencias y números de serie existentes pero *no* una cuenta NSS, debe crear una cuenta NSS y asociarla con su inicio de sesión de la consola.

Pasos

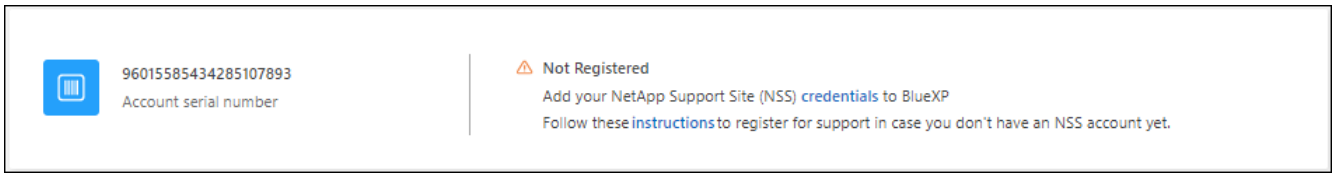
1. Cree una cuenta en el sitio de soporte de NetApp completando el "Formulario de registro de usuario del sitio de soporte de NetApp"
   a. Asegúrese de seleccionar el nivel de usuario apropiado, que normalmente es **Cliente de NetApp /Usuario final**.
   b. Asegúrese de copiar el número de serie de la cuenta de la consola (960xxxx) utilizado anteriormente para el campo de número de serie. Esto acelerará el procesamiento de la cuenta.
2. Asocie su nueva cuenta NSS con su inicio de sesión de la consola completando los pasos a continuaciónCliente existente con una cuenta NSS .

Completamente nuevo en NetApp

Si es nuevo en NetApp y no tiene una cuenta NSS, siga cada paso a continuación.

Pasos

1. En la parte superior derecha de la Consola, seleccione el ícono Ayuda y seleccione **Soporte**.
2. Localice el número de serie de su ID de cuenta en la página de Registro de soporte.



3. Navegar a "Sitio de registro de soporte de NetApp" y seleccione *No soy un cliente registrado de NetApp *.
4. Llene los campos obligatorios (aquellos con asteriscos rojos).
5. En el campo **Línea de productos**, seleccione **Administrador de nube** y luego seleccione su proveedor de facturación correspondiente.
6. Copie el número de serie de su cuenta del paso 2 anterior, complete la verificación de seguridad y luego confirme que leyó la Política de privacidad de datos global de NetApp.

Se envía inmediatamente un correo electrónico al buzón proporcionado para finalizar esta transacción segura. Asegúrese de revisar sus carpetas de correo no deseado si el correo electrónico de validación no llega en unos minutos.

7. Confirme la acción desde el correo electrónico.

   Al confirmar, se envía su solicitud a NetApp y se recomienda que cree una cuenta en el sitio de soporte de NetApp .

8. Cree una cuenta en el sitio de soporte de NetApp completando el "Formulario de registro de usuario del sitio de soporte de NetApp"
   a. Asegúrese de seleccionar el nivel de usuario apropiado, que normalmente es **Cliente de NetApp /Usuario final**.
   b. Asegúrese de copiar el número de serie de la cuenta (960xxxx) utilizado anteriormente para el campo de número de serie. Esto acelerará el procesamiento.

Después de terminar

NetApp debería comunicarse con usted durante este proceso. Este es un ejercicio de incorporación único para nuevos usuarios.

Una vez que tenga su cuenta del sitio de soporte de NetApp , asocie la cuenta con su inicio de sesión de consola completando los pasos a continuación.Cliente existente con una cuenta NSS .

Asociar credenciales NSS para la compatibilidad con Cloud Volumes ONTAP

Es necesario asociar las credenciales del sitio de soporte de NetApp con su cuenta de consola para habilitar los siguientes flujos de trabajo clave para Cloud Volumes ONTAP:

- Registro de sistemas Cloud Volumes ONTAP de pago por uso para obtener soporte

  Es necesario proporcionar su cuenta NSS para activar el soporte para su sistema y obtener acceso a los recursos de soporte técnico de NetApp .

- Implementación de Cloud Volumes ONTAP cuando trae su propia licencia (BYOL)

  Es necesario proporcionar su cuenta NSS para que la consola pueda cargar su clave de licencia y habilitar la suscripción por el período que compró. Esto incluye actualizaciones automáticas para renovaciones de plazos.

- Actualización del software Cloud Volumes ONTAP a la última versión

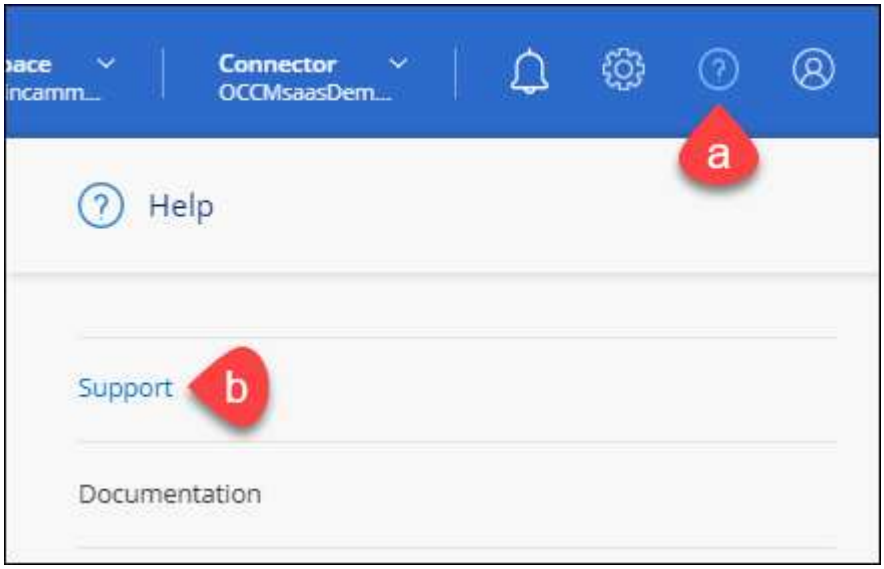
La asociación de credenciales NSS con su cuenta de NetApp Console es diferente a la asociación de una cuenta NSS con un inicio de sesión de usuario de consola.

Estas credenciales de NSS están asociadas con su ID de cuenta de consola específica. Los usuarios que pertenecen a la organización de la Consola pueden acceder a estas credenciales desde **Soporte > Administración de NSS**.

- Si tiene una cuenta de nivel de cliente, puede agregar una o más cuentas NSS.
- Si tiene una cuenta de socio o revendedor, puede agregar una o más cuentas NSS, pero no se pueden agregar junto con cuentas de nivel de cliente.

Pasos

1. En la parte superior derecha de la Consola, seleccione el ícono Ayuda y seleccione **Soporte**.



2. Seleccione **Administración de NSS > Agregar cuenta NSS**.
3. Cuando se le solicite, seleccione **Continuar** para ser redirigido a una página de inicio de sesión de Microsoft.

   NetApp utiliza Microsoft Entra ID como proveedor de identidad para servicios de autenticación específicos de soporte y licencias.

4. En la página de inicio de sesión, proporcione su dirección de correo electrónico y contraseña registradas en el sitio de soporte de NetApp para realizar el proceso de autenticación.

   Estas acciones permiten que la consola utilice su cuenta NSS para cosas como descargas de licencias, verificación de actualizaciones de software y futuros registros de soporte.

   Tenga en cuenta lo siguiente:

   - La cuenta NSS debe ser una cuenta de nivel de cliente (no una cuenta de invitado o temporal). Puede tener varias cuentas NSS a nivel de cliente.
   - Solo puede haber una cuenta NSS si esa cuenta es una cuenta de nivel de socio. Si intenta agregar cuentas NSS de nivel de cliente y existe una cuenta de nivel de socio, recibirá el siguiente mensaje de error:

     "El tipo de cliente NSS no está permitido para esta cuenta porque ya hay usuarios NSS de otro tipo".

   Lo mismo ocurre si tiene cuentas NSS de nivel de cliente preexistentes e intenta agregar una cuenta de nivel de socio.

   - Tras iniciar sesión correctamente, NetApp almacenará el nombre de usuario NSS.

     Esta es una identificación generada por el sistema que se asigna a su correo electrónico. En la página **Administración de NSS**, puede mostrar su correo electrónico desde el ••• menú.

   - Si alguna vez necesita actualizar sus tokens de credenciales de inicio de sesión, también hay una opción **Actualizar credenciales** en el ••• menú.

     Al utilizar esta opción se le solicitará que inicie sesión nuevamente. Tenga en cuenta que el token de

estas cuentas caduca después de 90 días. Se publicará una notificación para avisarle de esto.

Obtener ayuda

NetApp proporciona soporte para NetApp Console y sus servicios en la nube de diversas maneras. Hay amplias opciones de autoayuda gratuitas disponibles las 24 horas del día, los 7 días de la semana, como artículos de la base de conocimientos (KB) y un foro comunitario. Su registro de soporte incluye soporte técnico remoto mediante tickets web.

Obtenga soporte para un servicio de archivos de un proveedor de nube

Para obtener soporte técnico relacionado con un servicio de archivos de un proveedor de nube, su infraestructura o cualquier solución que utilice el servicio, consulte la documentación de ese producto.

- "Amazon FSx para ONTAP"
- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

Para recibir soporte técnico específico para NetApp y sus soluciones de almacenamiento y servicios de datos, utilice las opciones de soporte que se describen a continuación.

Utilice opciones de autosuficiencia

Estas opciones están disponibles de forma gratuita, las 24 horas del día, los 7 días de la semana:

- Documentación

  La documentación de la NetApp Console que estás viendo actualmente.

- "Base de conocimientos"

  Busque en la base de conocimientos de NetApp para encontrar artículos útiles para solucionar problemas.

- "Comunidades"

  Únase a la comunidad de la NetApp Console para seguir las discusiones en curso o crear otras nuevas.

Cree un caso con el soporte de NetApp

Además de las opciones de autosoporte anteriores, puede trabajar con un especialista de soporte de NetApp para resolver cualquier problema después de activar el soporte.

Antes de empezar

- Para utilizar la función **Crear un caso**, primero debe asociar sus credenciales del sitio de soporte de NetApp con su inicio de sesión de la consola. "Aprenda a administrar las credenciales asociadas con su inicio de sesión en la consola" .
- Si está abriendo un caso para un sistema ONTAP que tiene un número de serie, entonces su cuenta NSS debe estar asociada con el número de serie de ese sistema.

Pasos

1. En la NetApp Console, seleccione **Ayuda > Soporte**.
2. En la página **Recursos**, elija una de las opciones disponibles en Soporte técnico:

    a. Seleccione **Llámenos** si desea hablar con alguien por teléfono. Serás dirigido a una página en netapp.com que enumera los números de teléfono a los que puedes llamar.

    b. Seleccione **Crear un caso** para abrir un ticket con un especialista de soporte de NetApp :

    - **Servicio**: Seleccione el servicio con el que está asociado el problema. Por ejemplo, * NetApp Console* cuando es específico de un problema de soporte técnico con flujos de trabajo o funcionalidad dentro de la consola.
    - **Sistema**: si corresponde al almacenamiento, seleccione * Cloud Volumes ONTAP* o **On-Prem** y luego el entorno de trabajo asociado.

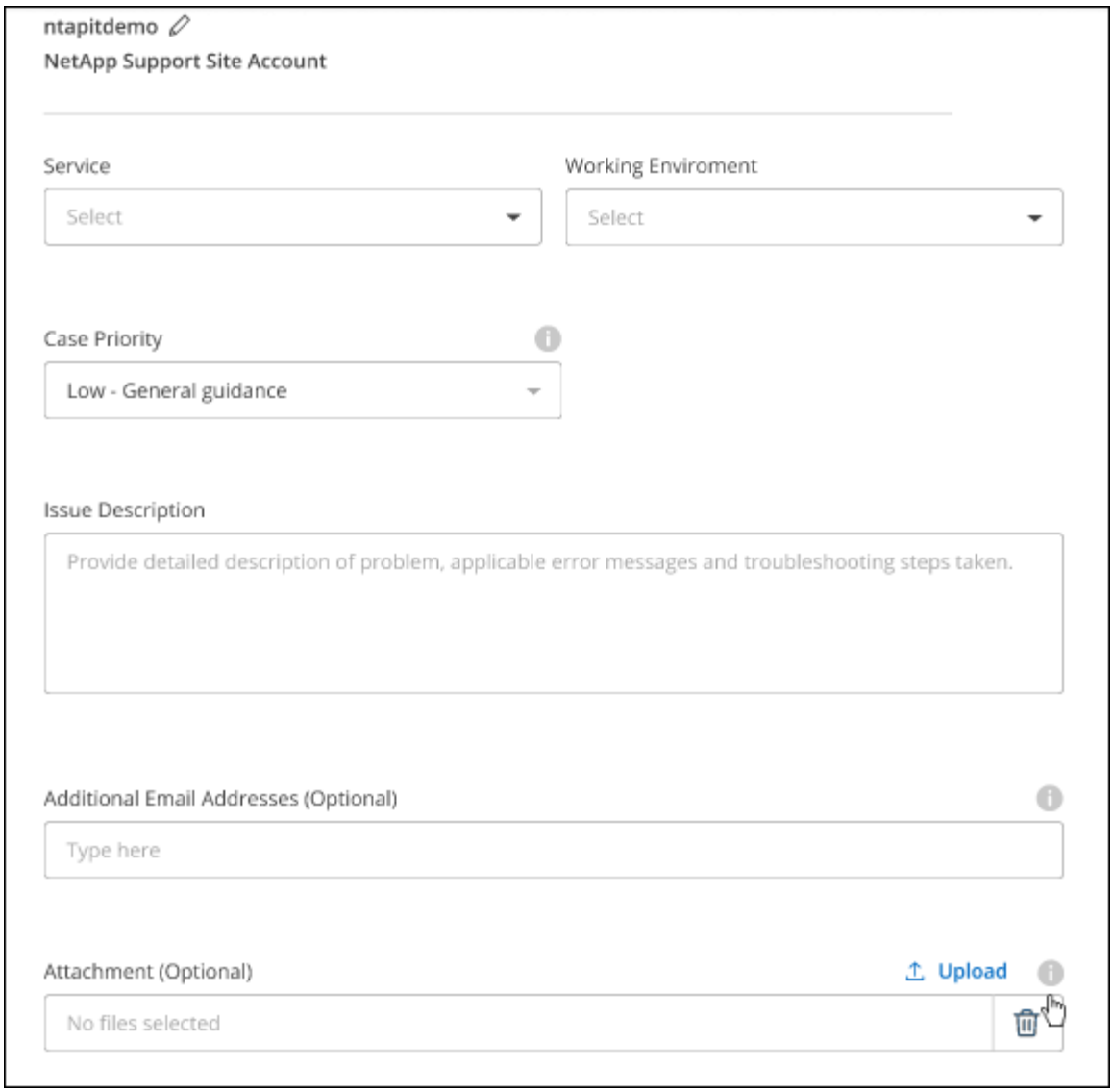
      La lista de sistemas está dentro del alcance de la organización de la consola y del agente de consola que ha seleccionado en el banner superior.

    - **Prioridad del caso**: elija la prioridad del caso, que puede ser Baja, Media, Alta o Crítica.

      Para obtener más detalles sobre estas prioridades, pase el mouse sobre el ícono de información junto al nombre del campo.

    - **Descripción del problema**: proporcione una descripción detallada de su problema, incluidos los mensajes de error aplicables o los pasos de solución de problemas que realizó.
    - **Direcciones de correo electrónico adicionales**: Ingrese direcciones de correo electrónico adicionales si desea informar a otra persona sobre este problema.
    - **Adjunto (opcional)**: cargue hasta cinco archivos adjuntos, uno a la vez.

      Los archivos adjuntos están limitados a 25 MB por archivo. Se admiten las siguientes extensiones de archivo: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx y csv.



Después de terminar

Aparecerá una ventana emergente con su número de caso de soporte. Un especialista de soporte de NetApp revisará su caso y se comunicará con usted pronto.

Para obtener un historial de sus casos de soporte, puede seleccionar **Configuración > Cronología** y buscar acciones llamadas "crear caso de soporte". Un botón en el extremo derecho le permite ampliar la acción para ver detalles.

Es posible que encuentres el siguiente mensaje de error al intentar crear un caso:

"No está autorizado a crear un caso contra el servicio seleccionado"

Este error podría significar que la cuenta NSS y la empresa registrada con la que está asociada no son la misma empresa registrada para el número de serie de la cuenta de la NetApp Console (es decir, 960xxxx) o el número de serie del entorno de trabajo. Puede buscar ayuda utilizando una de las siguientes opciones:

- Envíe un caso no técnico a https://mysupport.netapp.com/site/help

Gestione sus casos de soporte

Puede ver y administrar casos de soporte activos y resueltos directamente desde la Consola. Podrás gestionar los casos asociados a tu cuenta NSS y a tu empresa.

Tenga en cuenta lo siguiente:

- El panel de gestión de casos en la parte superior de la página ofrece dos vistas:
  - La vista de la izquierda muestra el total de casos abiertos en los últimos 3 meses por la cuenta de usuario NSS que usted proporcionó.
  - La vista de la derecha muestra el total de casos abiertos en los últimos 3 meses a nivel de su empresa en función de su cuenta de usuario NSS.

  Los resultados en la tabla reflejan los casos relacionados con la vista que usted seleccionó.
- Puede agregar o eliminar columnas de interés y puede filtrar el contenido de columnas como Prioridad y Estado. Otras columnas sólo proporcionan capacidades de clasificación.

  Vea los pasos a continuación para obtener más detalles.
- A nivel de caso, ofrecemos la posibilidad de actualizar notas de caso o cerrar un caso que aún no esté en estado Cerrado o Pendiente de cierre.

Pasos

1. En la NetApp Console, seleccione **Ayuda > Soporte**.
2. Seleccione **Administración de casos** y, si se le solicita, agregue su cuenta NSS a la consola.

   La página **Administración de casos** muestra los casos abiertos relacionados con la cuenta NSS que está asociada con su cuenta de usuario de la consola. Esta es la misma cuenta NSS que aparece en la parte superior de la página de **administración de NSS**.
3. Modifique opcionalmente la información que se muestra en la tabla:
   - En **Casos de la organización**, seleccione **Ver** para ver todos los casos asociados a su empresa.
   - Modifique el rango de fechas eligiendo un rango de fechas exacto o eligiendo un período de tiempo diferente.
   - Filtrar el contenido de las columnas.
   - Cambie las columnas que aparecen en la tabla seleccionando y luego elegir las columnas que desea mostrar.
4. Gestionar un caso existente seleccionando y seleccionando una de las opciones disponibles:
   - **Ver caso**: Ver detalles completos sobre un caso específico.
   - **Actualizar notas del caso**: proporcione detalles adicionales sobre su problema o seleccione **Cargar archivos** para adjuntar hasta un máximo de cinco archivos.

     Los archivos adjuntos están limitados a 25 MB por archivo. Se admiten las siguientes extensiones de archivo: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx y csv.
   - **Cerrar caso**: proporcione detalles sobre el motivo por el cual está cerrando el caso y seleccione **Cerrar caso**.

Preguntas frecuentes sobre la NetApp Ransomware Resilience

Estas preguntas frecuentes pueden ser útiles si simplemente busca una respuesta rápida a una pregunta sobre NetApp Ransomware Resilience.

Despliegue

¿Necesita una licencia para usar Ransomware Resilience?

Puede utilizar los siguientes tipos de licencia:

- Regístrese para una prueba gratuita de 30 días.
- Compre una suscripción de pago por uso (PAYGO) a NetApp Intelligent Services y Ransomware Resilience con Amazon Web Services (AWS) Marketplace, Google Cloud Marketplace y Microsoft Azure Marketplace.
- Traiga su propia licencia (BYOL), que es un archivo de licencia de NetApp (NLF) que obtiene de su representante de ventas de NetApp . Puedes usar el número de serie de la licencia para activar BYOL en la sección Licenses and subscriptions de la consola.

¿Cómo se habilita la resiliencia ante el ransomware?

Puede acceder a Ransomware Resilience desde la NetApp Console. Asegúrate de haber "roles de acceso" y "prerrequisitos". Si ha configurado correctamente un agente de consola, podrá entonces "descubrir cargas de trabajo".

Para obtener más información, consulte"Acceda a la resiliencia frente al ransomware" y"Guía de inicio rápido sobre resiliencia ante el ransomware" .

¿Está disponible la resiliencia ante el ransomware en modos estándar, restringido y privado?

Actualmente, la función de Resiliencia ante Ransomware solo está disponible en modo estándar.

Para obtener una explicación sobre estos modos en todos los servicios de datos de NetApp , consulte "Modos de implementación de la NetApp Console" .

Acceso

¿Cuál es la URL de Resiliencia contra el Ransomware?

En un navegador, ingrese "https://console.netapp.com/ransomware-resilience" para acceder a la consola.

¿Cómo se gestionan los permisos de acceso?

"Obtenga información sobre los roles de acceso a la consola para todos los servicios". La resiliencia ante el ransomware también tiene "roles de acceso dedicados".

¿Qué resolución de dispositivo es la mejor?

La resolución de dispositivo recomendada para Ransomware Resilience es 1920x1080 o superior.

¿Qué navegador debo usar?

Puedes acceder a la NetApp Console con cualquier navegador web moderno.

Interoperabilidad

¿Ransomware Resilience conoce las configuraciones de protección en ONTAP?

Sí, Ransomware Resilience descubre programaciones de instantáneas configuradas en ONTAP.

¿Cómo interactúa Ransomware Resilience con NetApp Backup and Recovery y SnapCenter?

La resiliencia ante el ransomware funciona con la función de copia de seguridad y recuperación para descubrir y establecer políticas de instantáneas y copias de seguridad para cargas de trabajo de archivos compartidos.

Ransomware Resilience funciona con SnapCenter o SnapCenter para VMware para descubrir y configurar políticas de instantáneas y copias de seguridad para cargas de trabajo de aplicaciones y máquinas virtuales.

Ransomware Resilience también funciona con Backup and Recovery y SnapCenter (incluido SnapCenter para VMware) para realizar una recuperación coherente con los archivos y la carga de trabajo.

Para licencias y facturación, Ransomware Resilience puede integrarse con Backup and Recovery incluso si no tiene una licencia separada para Backup and Recovery. Si tiene Backup and Recovery y Ransomware Resilience, cualquier dato común protegido por ambos productos se factura únicamente por Ransomware Resilience.

Cargas de trabajo

¿Qué se entiende por carga de trabajo en el contexto de la resiliencia ante el ransomware?

Una carga de trabajo es una aplicación, una máquina virtual o un recurso compartido de archivos. Una carga de trabajo incluye todos los volúmenes que utiliza una única instancia de aplicación.

Por ejemplo, considere una base de datos Oracle implementada en ora3.host.com con `vol1` que contienen datos y `vol2` Contiene registros. Los dos volúmenes constituyen la carga de trabajo para esa instancia de Oracle Database.

¿Cómo prioriza Ransomware Resilience los datos de la carga de trabajo?

La prioridad de la carga de trabajo (crítica, estándar, importante) está determinada por las frecuencias de instantáneas ya aplicadas a cada volumen asociado con la carga de trabajo y las copias de seguridad programadas.

"Obtenga información sobre la prioridad o importancia de la carga de trabajo" .

¿Qué cargas de trabajo admite Ransomware Resilience?

Ransomware Resilience puede identificar las siguientes cargas de trabajo: Oracle, recursos compartidos de archivos, almacenamiento en bloque, máquinas virtuales y almacenes de datos de máquinas virtuales.

Si utiliza SnapCenter o SnapCenter para VMware, todas las cargas de trabajo compatibles con estos productos también se identifican en Ransomware Resilience. Ransomware Resilience puede proteger y recuperar SnapCenter y las cargas de trabajo de SnapCenter de manera coherente con la carga de trabajo.

¿Cómo se asocian los datos a una carga de trabajo?

Ransomware Resilience descubre los volúmenes y las extensiones de archivo y los asocia con la carga de trabajo apropiada.

Si tiene SnapCenter o SnapCenter para VMware y ha configurado cargas de trabajo en Copia de seguridad y recuperación, entonces Ransomware Resilience descubre las cargas de trabajo administradas por SnapCenter y SnapCenter para VMware y sus volúmenes asociados.

¿Qué es una carga de trabajo protegida?

En Ransomware Resilience, una carga de trabajo muestra el estado **protegida** cuando tiene habilitada una política de *detección* primaria, lo que significa "Protección autónoma contra el ransomware (ARP)" está habilitado en todos los volúmenes relacionados con la carga de trabajo.

¿Qué es una carga de trabajo "en riesgo"?

Si una carga de trabajo no tiene habilitada una política de detección primaria, se la etiqueta como "en riesgo" incluso si tiene habilitada una política de copia de seguridad y de instantáneas. Para protegerte del ransomware, debes habilitar una "política de detección".

He añadido un nuevo volumen, pero aún no aparece. ¿Qué tengo que hacer?

Si ha añadido un nuevo volumen a su entorno, vuelva a iniciar la detección de la carga de trabajo. Una vez descubierto el volumen, "Aplicar políticas de protección para proteger el nuevo volumen".

Políticas de protección

¿Las políticas de resiliencia ante el ransomware coexisten con otros tipos de políticas de carga de trabajo?

En este momento, Backup and Recovery (Cloud Backup) admite una política de backup por volumen. Si configura la protección de copias de seguridad con Copia de seguridad y recuperación, comparte las políticas de copia de seguridad con Resiliencia contra ransomware.

Las copias instantáneas no están limitadas y se pueden agregar por separado desde cada servicio.

¿Qué políticas son necesarias en una estrategia de protección contra el ransomware?

A "estrategia de protección contra el ransomware" Requisitos:

- una política de detección de ransomware, y
- una política de instantáneas

No se requiere una política de respaldo en la estrategia de resiliencia frente al ransomware.

¿Ransomware Resilience conoce las configuraciones de protección en ONTAP?

Sí, Ransomware Resilience descubre programaciones de instantáneas configuradas en ONTAP. También descubre si ARP y FPolicy están habilitados en todos los volúmenes de una carga de trabajo detectada. La información que ve en el Panel de Resiliencia contra el Ransomware se recopila de otras soluciones y productos de NetApp .

¿Tiene en cuenta Ransomware Resilience las políticas ya establecidas en Backup and Recovery y SnapCenter?

Sí, si tiene cargas de trabajo administradas en Backup and Recovery o SnapCenter, las políticas administradas por esos productos se incorporan a Ransomware Resilience.

¿Es posible modificar las políticas heredadas de NetApp Backup and Recovery y/o SnapCenter?

No, no puede modificar las políticas administradas por Backup and Recovery o SnapCenter desde Ransomware Resilience. Usted administra cualquier cambio en esas políticas en Backup and Recovery o SnapCenter.

Si existen políticas de ONTAP (como ARP, FPolicy y snapshots), ¿se modifican en Ransomware Resilience?

No. Ransomware Resilience no modifica ninguna política de detección existente (configuración ARP, FPolicy) de ONTAP.

¿Qué sucede si agrega nuevas políticas en Backup and Recovery o SnapCenter después de registrarse en

Ransomware Resilience?

La función de Resiliencia ante Ransomware reconoce las políticas recién creadas y los cambios de políticas en Copia de seguridad y recuperación o SnapCenter.

¿Se pueden cambiar las políticas desde ONTAP?

Sí, puede cambiar las políticas de ONTAP en Ransomware Resilience. También puede crear nuevas políticas en Ransomware Resilience y aplicarlas a las cargas de trabajo. Esta acción reemplaza las políticas ONTAP existentes con las políticas creadas en Ransomware Resilience.

¿Se pueden deshabilitar las políticas en ONTAP?

Puede deshabilitar ARP en las políticas de detección utilizando la interfaz de usuario, las API o la CLI del administrador del sistema en ONTAP.

Puede deshabilitar FPolicy y las políticas de respaldo aplicando una política diferente que no las incluya.

Avisos legales

Los avisos legales proporcionan acceso a declaraciones de derechos de autor, marcas comerciales, patentes y más.

Copyright

"https://www.netapp.com/company/legal/copyright/"

Marcas comerciales

NETAPP, el logotipo de NETAPP y las marcas enumeradas en la página de Marcas comerciales de NetApp son marcas comerciales de NetApp, Inc. Otros nombres de empresas y productos pueden ser marcas comerciales de sus respectivos propietarios.

"https://www.netapp.com/company/legal/trademarks/"

Patentes

Puede encontrar una lista actualizada de las patentes propiedad de NetApp en:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Política de privacidad

"https://www.netapp.com/company/legal/privacy-policy/"

Código abierto

Los archivos de aviso proporcionan información sobre derechos de autor y licencias de terceros utilizados en el software de NetApp .

- "Aviso para la NetApp Console"