



# Documentación de protección contra ransomware de BlueXP

BlueXP ransomware protection

NetApp  
March 22, 2024

# Tabla de contenidos

- Documentación de protección contra ransomware de BlueXP ..... 1
- Notas de la versión: Novedades de la vista previa de la protección frente al ransomware de BlueXP ..... 2
  - 5 de marzo de 2024 ..... 2
  - 6 de octubre de 2023 ..... 2
- Manos a la obra ..... 4
  - Obtén más información sobre la versión previa de la protección frente al ransomware de BlueXP ..... 4
  - Requisitos previos de protección contra ransomware de BlueXP ..... 9
  - Inicio rápido para la protección frente al ransomware de BlueXP ..... 9
  - Configura la protección contra el ransomware de BlueXP ..... 10
  - Accede a la protección frente al ransomware de BlueXP ..... 11
  - Detecta cargas de trabajo en la protección frente al ransomware de BlueXP ..... 12
  - Configura las opciones de protección contra ransomware de BlueXP ..... 13
  - Preguntas frecuentes sobre la protección contra ransomware de BlueXP ..... 18
- Usa la protección frente al ransomware de BlueXP ..... 21
  - Usa la protección frente al ransomware de BlueXP ..... 21
  - Vea de un vistazo el estado de las cargas de trabajo mediante la consola ..... 21
  - Protege las cargas de trabajo contra ataques de ransomware ..... 24
  - Responder a una alerta de ransomware detectada ..... 31
  - Recuperarse de un ataque de ransomware (después de neutralizar los incidentes) ..... 33
- Conocimiento y apoyo ..... 40
  - Regístrese para recibir soporte ..... 40
  - Obtenga ayuda ..... 44
- Avisos legales ..... 50
  - Derechos de autor ..... 50
  - Marcas comerciales ..... 50
  - Estadounidenses ..... 50
  - Política de privacidad ..... 50
  - Código abierto ..... 50

# Documentación de protección contra ransomware de BlueXP

# Notas de la versión: Novedades de la vista previa de la protección frente al ransomware de BlueXP

Descubre las novedades de la versión previa de la protección frente al ransomware de BlueXP.

## 5 de marzo de 2024

Esta versión previa de la protección contra ransomware de BlueXP incluye las siguientes actualizaciones:

- **Gestión de políticas de protección:** Además de usar políticas predefinidas, ahora puede crear, cambiar y eliminar políticas. ["Obtenga más información sobre la gestión de políticas"](#).
- **Inmutabilidad en almacenamiento secundario (DataLock):** Ahora puede hacer que la copia de seguridad sea inmutable en el almacenamiento secundario usando la tecnología NetApp DataLock en el almacén de objetos. ["Obtén más información sobre la creación de políticas de protección"](#).
- **Copia de seguridad automática en NetApp StorageGRID:** Además de usar AWS, ahora puede elegir StorageGRID como destino de copia de seguridad. ["Obtenga más información sobre la configuración de destinos de backup"](#).
- **Características adicionales para investigar posibles ataques:** Ahora puedes ver más detalles forenses para investigar el posible ataque detectado. ["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, todos los volúmenes para una carga de trabajo o incluso algunos archivos del volumen, todo en un único flujo de trabajo. ["Descubre cómo recuperarse de un ataque de ransomware \(después de que se hayan neutralizado los incidentes\)"](#).

["Obtén más información sobre la protección frente al ransomware de BlueXP"](#).

## 6 de octubre de 2023

El servicio de protección frente al ransomware de BlueXP es una solución de SaaS que protege datos, detecta posibles ataques y recupera datos desde un ataque de ransomware.

Para la versión de vista previa, el servicio protege las cargas de trabajo basadas en aplicaciones de Oracle, MySQL, almacenes de datos de máquinas virtuales y recursos compartidos de archivos en el almacenamiento NAS en las instalaciones, así como Cloud Volumes ONTAP en AWS (mediante el protocolo NFS) en las cuentas de BlueXP de forma individual y crea backups de los datos en el almacenamiento en cloud de Amazon Web Services.

El servicio de protección frente a ransomware de BlueXP ofrece un uso completo de diversas tecnologías de NetApp para que su administrador de seguridad de datos o el ingeniero de operaciones de seguridad puedan lograr los siguientes objetivos:

- Mira la protección contra ransomware en todas tus cargas de trabajo de un vistazo.
- Obtenga información sobre las recomendaciones de protección frente al ransomware
- Mejora la postura de protección basándose en las recomendaciones de protección frente al ransomware de BlueXP.
- Asigna políticas de protección frente al ransomware para proteger tus principales cargas de trabajo y

datos de alto riesgo frente a ataques de ransomware.

- Supervise el estado de sus cargas de trabajo frente a ataques de ransomware y busque anomalías en los datos.
- Evalúa rápidamente el impacto de los incidentes de ransomware en tu carga de trabajo.
- Recupérese de forma inteligente de los incidentes de ransomware restaurando los datos y garantizando que no se produzca la reinfección de los datos almacenados.

["Obtén más información sobre la protección frente al ransomware de BlueXP".](#)

# Manos a la obra

## Obtén más información sobre la versión previa de la protección frente al ransomware de BlueXP

Los ataques de ransomware pueden bloquear el acceso a tus sistemas y los datos, y los atacantes pueden solicitar un rescate a cambio de la liberación de datos o descifrado. Según IDC, no es raro que las víctimas de ransomware sufran múltiples ataques de ransomware. El ataque puede interrumpir el acceso a los datos entre un día y varias semanas.

La protección frente al ransomware de BlueXP es un servicio de orquestación para la protección, detección y recuperación de ransomware. Para la versión de vista previa, el servicio protege las cargas de trabajo basadas en aplicaciones de Oracle, MySQL, almacenes de datos de máquinas virtuales, también se pueden compartir archivos en el almacenamiento NAS en las instalaciones, así como en Cloud Volumes ONTAP en Amazon Web Services (mediante el protocolo NFS) en cuentas de BlueXP y se realizan backups de los datos en el almacenamiento en cloud de Amazon Web Services o en NetApp StorageGRID.

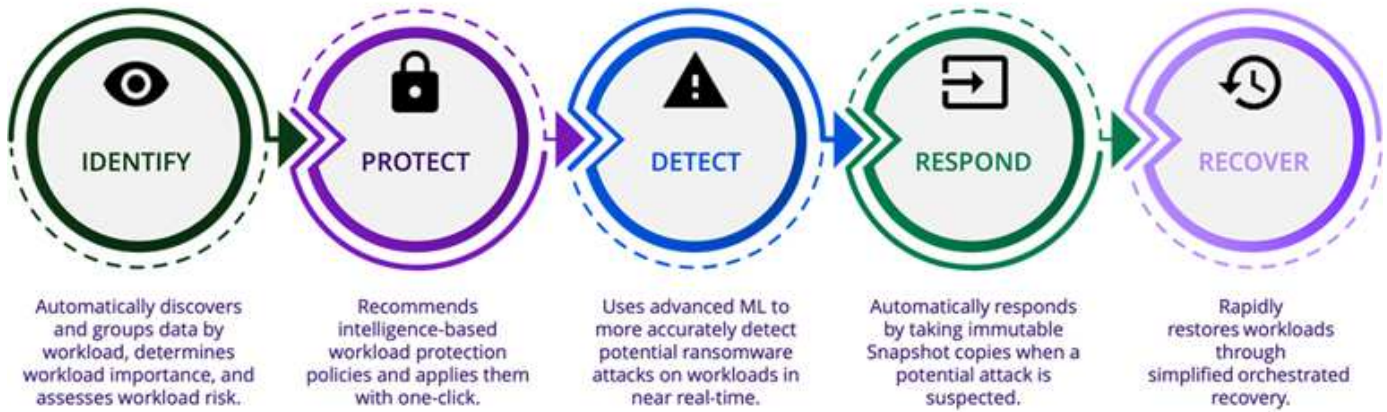


ESTA DOCUMENTACIÓN SE PROPORCIONA COMO UNA PREVISUALIZACIÓN TECNOLÓGICA. Con esta oferta de vista previa, NetApp se reserva el derecho de modificar los detalles, el contenido y la línea de tiempo de la oferta antes de la disponibilidad general.

## Todo lo que puedes hacer con la protección frente al ransomware de BlueXP

El servicio de protección frente a ransomware de BlueXP proporciona un uso completo de diversas tecnologías de NetApp para que el administrador de almacenamiento, el administrador de seguridad de los datos o el ingeniero de operaciones de seguridad puedan lograr los siguientes objetivos:

- **Identifica** todas las cargas de trabajo basadas en aplicaciones, de uso compartido o gestionadas por VMware en el NAS on-premises de NetApp con entornos de trabajo NFS en BlueXP, en cuentas de BlueXP, espacios de trabajo y conectores BlueXP. A continuación, el servicio categoriza la prioridad de los datos y te ofrece recomendaciones para llevar a cabo mejoras en la protección frente a ransomware.
- **Proteja** sus cargas de trabajo habilitando copias de seguridad y copias snapshot en sus datos.
- **Detectar** anomalías que podrían ser ataques de ransomware.
- \* Responder\* a posibles ataques de ransomware iniciando automáticamente una copia snapshot de NetApp ONTAP.
- \* Recuperar\* 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 optar por recuperar volúmenes, carpetas o archivos específicos. El servicio ofrece recomendaciones sobre las mejores opciones.



## Beneficios de usar la protección frente al ransomware de BlueXP

La protección frente al ransomware de BlueXP ofrece las siguientes ventajas:

- Detecta las cargas de trabajo y los conjuntos de datos, analiza la prioridad en función del índice de uso y clasifica su importancia relativa.
- Evalúa tu posición de protección frente al ransomware y lo muestra en una consola fácil de entender.
- Proporciona recomendaciones sobre los siguientes pasos según el análisis de la postura de detección y protección.
- Aplica recomendaciones de protección de datos impulsadas por IA/ML con acceso con un solo clic.
- Protege los datos en las principales cargas de trabajo basadas en aplicaciones, como MySQL, Oracle, almacenes de datos de VMware y recursos compartidos de archivos.
- Detecta ataques de ransomware en datos en tiempo real en almacenamiento principal mediante tecnología de IA.
- Inicia acciones automatizadas en respuesta a posibles ataques detectados creando copias Snapshot e iniciando alertas sobre actividad anormal.
- Aplica una recuperación selectiva para cumplir con las políticas del objetivo de punto de recuperación. La protección contra ransomware de BlueXP orquesta la recuperación de incidentes de ransomware mediante diversos servicios de recuperación de NetApp, incluidos el backup y la recuperación de datos de BlueXP (anteriormente Cloud Backup).

## Coste

NetApp no te cobra por usar la versión preliminar de la protección contra ransomware de BlueXP.

## Licencia

La versión previa de la protección contra ransomware de BlueXP no requiere ninguna licencia especial. Todas las licencias de vista previa son licencias de evaluación.



Para la versión de vista previa, NetApp ayuda a configurar la evaluación y las licencias necesarias.

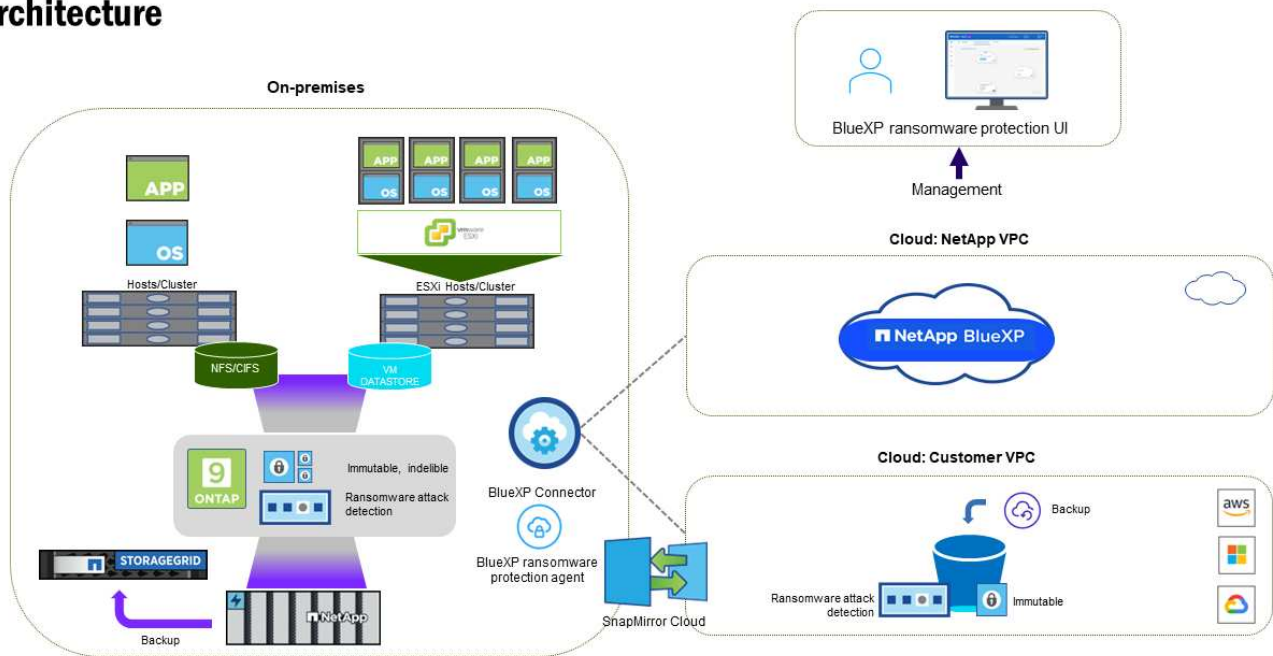
La vista previa de la protección contra ransomware de BlueXP requiere las siguientes licencias:

- ONTAP
- Tecnología autónoma de protección frente a ransomware de NetApp. Consulte ["Información general sobre la protección de ransomware autónoma"](#) para obtener más detalles.
- Servicio de backup y recuperación de datos de BlueXP

## Funcionamiento de la protección frente al ransomware de BlueXP

En un nivel alto, la protección contra el ransomware de BlueXP funciona así.

### Architecture





Función	Descripción
<b>IDENTIFICAR</b>	<ul style="list-style-type: none"> <li>• Encuentra todos los datos de NAS (montajes NFS) en las instalaciones de los clientes conectados a BlueXP.</li> <li>• Identifica los datos de los clientes de las API de servicios de ONTAP y los asocia con las cargas de trabajo. Más información acerca de "ONTAP" y.. "Software SnapCenter".</li> <li>• Detecta el nivel de protección actual de cada volumen de copias de Snapshot de NetApp y políticas de backup, así como cualquier funcionalidad de detección integrada. A continuación, el servicio asocia esta postura de protección con las cargas de trabajo mediante el backup y recuperación de datos de BlueXP, el asesor digital de BlueXP, los servicios de ONTAP y tecnologías de NetApp como la protección autónoma frente a ransomware, FPolicy, las políticas de backup y las políticas de Snapshot. Más información acerca de "Protección autónoma de ransomware" y.. "Backup y recuperación de BlueXP", "Asesor digital de BlueXP", y. "FPolicy de ONTAP".</li> <li>• Asigna una prioridad empresarial a cada carga de trabajo en función de los niveles de protección detectados automáticamente y recomienda políticas de protección para las cargas de trabajo en función de su prioridad empresarial.</li> <li>• La protección frente al ransomware también aprende las asociaciones de políticas y recomienda tus políticas personalizadas en cargas de trabajo similares.</li> </ul>
<b>PROTEGER</b>	<ul style="list-style-type: none"> <li>• Supervisa activamente las cargas de trabajo y orquesta el uso de las API de backup y recuperación de datos de BlueXP y ONTAP mediante la aplicación de políticas a cada una de las cargas de trabajo identificadas.</li> </ul>
<b>DETECTAR</b>	<ul style="list-style-type: none"> <li>• Detecta posibles ataques con un modelo de aprendizaje automático (ML) integrado que detecta actividad y cifrado potencialmente anómalos.</li> <li>• Proporciona detección de doble capa que comienza con la detección de posibles ataques de ransomware en el almacenamiento principal y la respuesta a actividades anormales realizando copias Snapshot adicionales automatizadas para crear los puntos de restauración de datos más cercanos. El servicio ofrece la capacidad de obtener más información para identificar posibles ataques con mayor precisión sin que ello afecte al rendimiento de las cargas de trabajo principales.</li> <li>• Determina los archivos y mapas sospechosos específicos que atacan a las cargas de trabajo asociadas mediante las tecnologías ONTAP, protección autónoma contra ransomware y FPolicy.</li> </ul>
<b>RESPONDER</b>	<ul style="list-style-type: none"> <li>• Muestra datos relevantes, como la actividad de los archivos, la actividad del usuario y la entropía, para ayudarte a realizar revisiones forenses sobre el ataque.</li> <li>• Inicia rápidas copias Snapshot usando tecnologías y productos de NetApp como ONTAP, protección autónoma frente a ransomware y FPolicy.</li> </ul>

Función	Descripción
<b>RECUPERAR</b>	<ul style="list-style-type: none"> <li>• Determina la mejor copia Snapshot o backup y recomienda el mejor punto de recuperación real (RPA) mediante el uso de las tecnologías y servicios de backup y recuperación de datos de BlueXP, ONTAP, protección autónoma frente a ransomware y FPolicy.</li> <li>• Orquesta la recuperación de cargas de trabajo que incluyen máquinas virtuales, recursos compartidos de archivos y bases de datos con coherencia de aplicaciones.</li> </ul>

## Destinos de copia de seguridad, entornos de trabajo y orígenes de datos compatibles

Utiliza la vista previa de la protección de ransomware de BlueXP para ver lo resilientes que son tus datos ante un ciberataque a los siguientes tipos de destinos de backup, entornos de trabajo y fuentes de datos:

### Destinos de copia de seguridad soportados

- Amazon Web Services (AWS) S3
- StorageGRID de NetApp
- Entornos de trabajo compatibles \*
- NAS de ONTAP en las instalaciones (con el protocolo NFS)
- ONTAP Select
- Cloud Volumes ONTAP en AWS (con el protocolo NFS)

### Fuentes de datos

Para la versión de vista previa, el servicio protege las siguientes cargas de trabajo basadas en aplicaciones:

- Recursos compartidos de archivos NetApp
- Almacenes de datos VMware
- Bases de datos (para la versión preliminar, Oracle y MySQL)

## Términos que pueden ayudarte con la protección contra el ransomware

Te puedes beneficiar si comprendes alguna terminología en lo que respecta a la protección contra ransomware.

- **Protección:** La protección en la protección contra ransomware de BlueXP significa garantizar que las copias Snapshot y las copias de seguridad inmutables se produzcan de forma regular en un dominio de seguridad diferente mediante políticas de protección.
- **Carga de trabajo:** Una carga de trabajo en la vista previa de protección contra ransomware de BlueXP puede incluir bases de datos MySQL u Oracle, almacenes de datos de VMware o recursos compartidos de archivos.

# Requisitos previos de protección contra ransomware de BlueXP

Comience a usar la protección frente al ransomware de BlueXP verificando la preparación de su entorno operativo, inicio de sesión, acceso a red y navegador web.

Para utilizar la versión previa de la protección contra ransomware de BlueXP, necesitarás estos requisitos previos:

- Una cuenta en NetApp StorageGRID o AWS S3 para los destinos de backup y los permisos de acceso establecidos

Consulte la ["Lista de permisos de AWS"](#) para obtener más detalles.

- ONTAP 9.11.1 y versiones posteriores
  - Permisos de la ONTAP del administrador de clústeres
  - Una licencia de la protección autónoma frente a ransomware de NetApp, utilizada por la protección frente a ransomware de BlueXP, habilitada en la instancia de ONTAP en las instalaciones, según la versión de ONTAP que esté utilizando. Consulte ["Información general sobre la protección de ransomware autónoma"](#).

Para obtener más información sobre las licencias, consulte ["Obtén más información sobre la protección frente al ransomware de BlueXP"](#).

- En BlueXP:
  - Debe configurarse un conector BlueXP por cada cloud privado virtual (VPC) o en una región en las instalaciones en BlueXP. Consulte ["Documentación de BlueXP para configurar el Connector"](#).



Si tienes varios BlueXP Connectors, el servicio analizará los datos en todos los conectores más allá de los que se muestren actualmente en la interfaz de usuario de BlueXP.

- El servicio de backup y recuperación de BlueXP con backup habilitado en el entorno de trabajo
- Un entorno de trabajo BlueXP con almacenamiento on-premises NAS de NetApp
- Una cuenta de BlueXP con al menos un conector activo que se conecta a clústeres de ONTAP en las instalaciones. Todos los entornos de trabajo y origen deben estar en la misma cuenta de BlueXP.
- Una cuenta de usuario de BlueXP con privilegios de administrador de cuenta para detectar recursos
- ["Requisitos estándar de BlueXP"](#)

## Inicio rápido para la protección frente al ransomware de BlueXP

Aquí tienes una descripción general de los pasos necesarios para empezar a utilizar la protección contra ransomware de BlueXP. Los vínculos de cada paso le llevan a una página que proporciona más detalles.

**1**

### Revise los requisitos previos

"Asegúrese de que su entorno cumpla estos requisitos".

**2**

### Configura el servicio de protección contra ransomware

- "Preparar NetApp StorageGRID o Amazon Web Services como destino de backup".
- "Configura un conector en BlueXP".
- "Configurar destinos de copia de seguridad".
- "Detecta cargas de trabajo en BlueXP".

**3**

### El futuro

Después de configurar el servicio, esto es lo que puede hacer a continuación.

- "Ver el estado de la protección de las cargas de trabajo en la consola".
- "Proteja las cargas de trabajo".
- "Responde a la detección de posibles ataques de ransomware".
- "Recuperarse de un ataque (después de neutralizar los incidentes)".

## Configura la protección contra el ransomware de BlueXP

Para utilizar la protección contra ransomware de BlueXP, sigue algunos pasos para configurarla.

Antes de comenzar, revise "[requisitos previos](#)" garantizar que su entorno está listo.

### Preparar el destino de la copia de seguridad

Prepare uno de los siguientes destinos de copia de seguridad:

- StorageGRID de NetApp
- Amazon Web Services

Después de configurar las opciones en el destino de backup, lo configurarás más adelante como destino de backup en el servicio de protección contra ransomware de BlueXP.

### Preparar StorageGRID para que se convierta en destino de backup

Si desea usar StorageGRID como destino de backup, consulte "[Documentación de StorageGRID](#)" Para obtener más detalles acerca de StorageGRID.

### Prepare AWS para que se convierta en destino de backup

- Configura una cuenta en AWS.
- Configurar "[Permisos de AWS](#)" En AWS.

Para obtener más información sobre la gestión de su almacenamiento de AWS en BlueXP, consulte ["Gestione sus bloques de Amazon S3"](#).

## Configure BlueXP

El siguiente paso es configurar BlueXP y el servicio de protección contra ransomware de BlueXP.

Revisar ["Requisitos estándar de BlueXP"](#).

### Crear un conector en BlueXP

Debe ponerse en contacto con su representante de ventas de NetApp para probar este servicio. Una vez que uses BlueXP Connector, incluirá las funcionalidades adecuadas para el servicio de protección frente a ransomware.

Para crear un conector en BlueXP antes de utilizar el servicio, consulte la documentación de BlueXP que se describe ["Cómo crear un conector BlueXP"](#).



Si tienes varios BlueXP Connectors, el servicio analizará los datos en todos los conectores más allá de los que se muestren actualmente en la interfaz de usuario de BlueXP. Este servicio detecta todos los espacios de trabajo y todos los conectores asociados a esta cuenta.

### Accede a la protección frente al ransomware de BlueXP

Utilizarás NetApp BlueXP para iniciar sesión en el servicio de protección contra ransomware de BlueXP. En la navegación izquierda de BlueXP, selecciona **Protección > Protección contra ransomware**.

Para obtener más información, consulte ["Accede a la protección frente al ransomware de BlueXP"](#).

### Configura los destinos de backup en la protección frente al ransomware de BlueXP

Utiliza la opción de destinos de backup de protección contra ransomware de BlueXP para configurar destinos de backup. Para obtener más información, consulte ["Configure las opciones de configuración"](#).

## Accede a la protección frente al ransomware de BlueXP

Utilizarás NetApp BlueXP para iniciar sesión en el servicio de protección contra ransomware de BlueXP.

Para iniciar sesión en BlueXP, puede utilizar sus credenciales del sitio de soporte de NetApp o puede registrarse para iniciar sesión en cloud de NetApp con su correo electrónico y una contraseña. ["Obtenga más información sobre cómo iniciar sesión"](#).

### Pasos

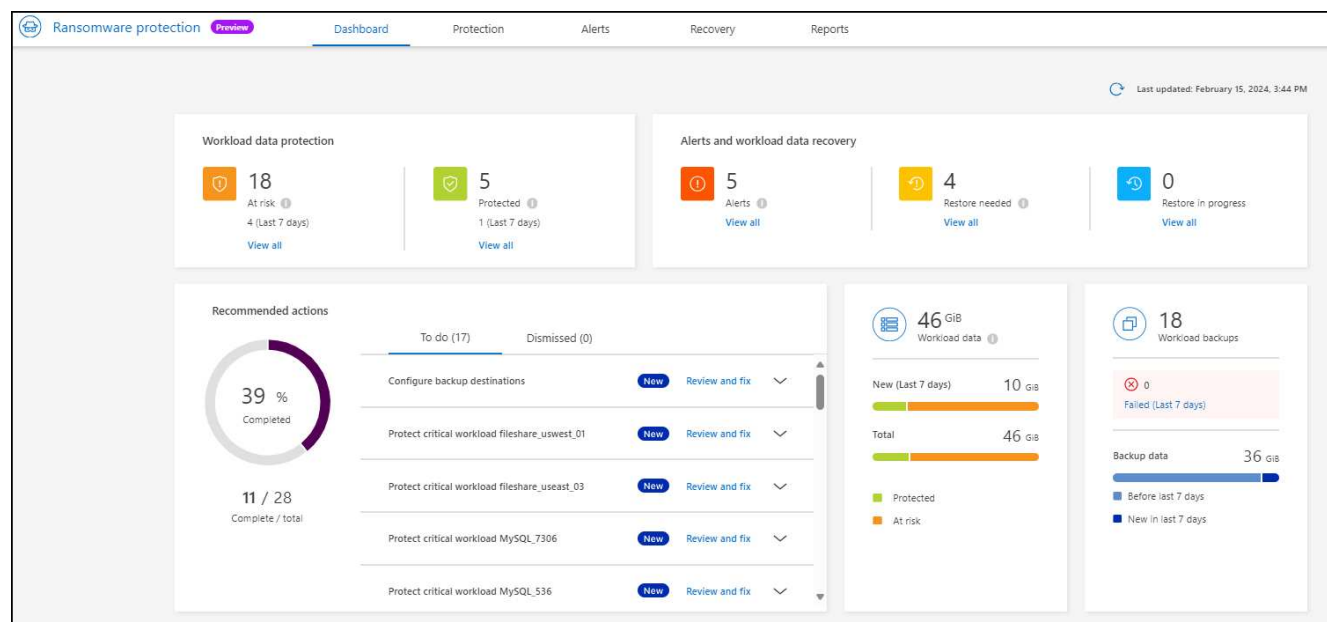
1. Abra un explorador web y vaya al ["Consola BlueXP"](#).

Aparece la página de inicio de sesión de NetApp BlueXP.

2. Inicie sesión en BlueXP.
3. En la navegación izquierda de BlueXP, selecciona **Protección > Protección contra ransomware**.

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

De lo contrario, se mostrará la consola de protección contra ransomware de BlueXP.



#### 4. Comience a utilizar el servicio.

- Si no tienes un conector BlueXP o no es el indicado para esta vista previa, es posible que debas ponerte en contacto con el Soporte de NetApp o seguir mensajes para registrarte en esta vista previa.
- Si eres nuevo en BlueXP y no has usado ningún conector, cuando seleccionas «**Protección contra ransomware**», aparecerá un mensaje sobre la inscripción. Continúe y envíe el formulario. NetApp se pondrá en contacto con usted para informarse sobre su solicitud de evaluación.
- Si eres un usuario de BlueXP con un conector existente, cuando seleccionas «**Protección contra ransomware**», aparecerá un mensaje sobre la inscripción.
- Si ya estás participando en la vista previa, al seleccionar “**Protección contra ransomware**”, puedes continuar con el servicio. Si aún no lo ha hecho, debe seleccionar la opción **Descubrir cargas de trabajo**.

## Detecta cargas de trabajo en la protección frente al ransomware de BlueXP

Para utilizar la protección frente al ransomware de BlueXP, el servicio debe detectar primero los datos. Durante la detección, la protección frente al ransomware de BlueXP analiza todos los volúmenes y archivos en entornos de trabajo en todos los conectores y espacios de trabajo de BlueXP dentro de una cuenta.



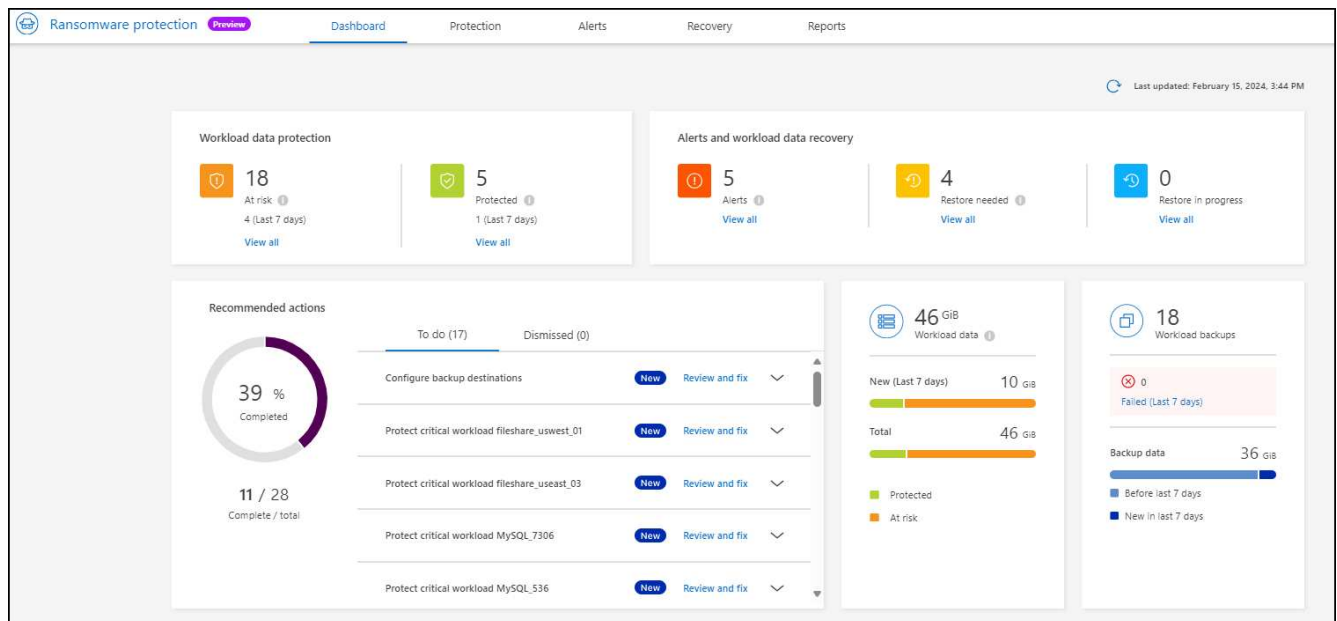
Para la versión preliminar, la protección frente al ransomware BlueXP evalúa las aplicaciones MySQL, las aplicaciones de Oracle, los almacenes de datos de VMware y los recursos compartidos de archivos.

El servicio evalúa el nivel de protección existente, incluida la protección actual del backup, las copias Snapshot y las opciones de protección autónoma frente a ransomware de NetApp. Según la evaluación, el servicio te recomienda cómo mejorar tu protección frente al ransomware.

#### Pasos

1. En la navegación izquierda de BlueXP, selecciona **Protección > Protección contra ransomware**.
2. Seleccione **Descubrir cargas de trabajo** en la página de destino inicial.

El servicio detecta los datos de la carga de trabajo y muestra el estado de la protección de datos en la consola.



## Configura las opciones de protección contra ransomware de BlueXP

Si desea configurar un destino de backup, revise las recomendaciones en la consola.

### Agregue un destino de copia de seguridad

La protección frente al ransomware de BlueXP puede identificar cargas de trabajo que aún no tienen backups y también cargas de trabajo que todavía no tengan destinos de backup asignados.

Para proteger esas cargas de trabajo, debe añadir un destino de backup. Es posible elegir uno de los siguientes destinos de backup:

- StorageGRID de NetApp
- Amazon Web Services (AWS)

Puede añadir un destino de backup en función de una acción recomendada en la consola.

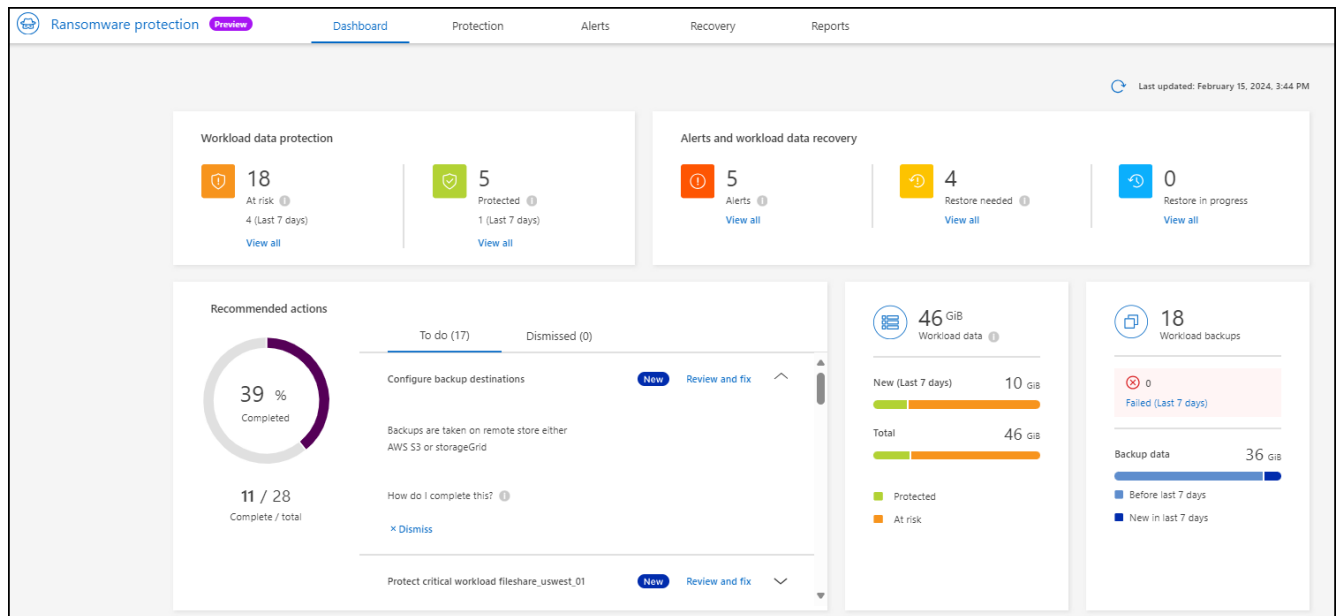
### Acceda a las opciones de destino de copia de seguridad desde las acciones recomendadas del panel de control

La consola ofrece muchas recomendaciones. Una recomendación podría ser configurar un destino de copia de seguridad.

#### Pasos

1. En la navegación izquierda de BlueXP, selecciona **Protección > Protección contra ransomware**.

2. Revise el panel de acciones recomendadas de la consola.



3. Desde el Panel de Control, seleccione **Revisar y corregir** para la recomendación de “Configurar destinos de copia de seguridad”.

4. Continúe con las instrucciones dependiendo del proveedor de copias de seguridad.



## Añada StorageGRID como destino de backup

Para configurar NetApp StorageGRID como destino de backup, introduzca la siguiente información.

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



### Add backup destination

Name	backup-dest1	▼
Provider	<span style="color: blue; font-size: small;">i</span> Action required	▲
Select a provider to back up to the cloud.		
<div style="display: flex; justify-content: space-around; gap: 20px;"> <div style="text-align: center;">  <p>Amazon Web Services</p> </div> <div style="text-align: center;">  <p>StorageGRID</p> </div> </div>		
Provider settings	Defined by provider selection	▼
Networking	Defined by provider selection	▼
Backup lock	Defined by provider selection	▼

Cancel
Add

3. Seleccione **StorageGRID**.

4. Seleccione la flecha hacia abajo junto a cada ajuste e introduzca o seleccione valores:

- **Configuración del proveedor:**

- Cree un nuevo bloque o traiga su propio bloque que almacenará los backups.
- Nodo de puerta de enlace StorageGRID Nombre de dominio completo, puerto, clave de acceso a StorageGRID y credenciales de clave secreta.

- **Networking:** Elige el espacio IP.

- El espacio IP es el clúster donde residen los volúmenes del que se desea incluir en un backup. Las LIF entre clústeres de este espacio IP deben tener acceso a Internet saliente.

- \* Bloqueo de respaldo\*: Elija si desea que el servicio proteja las copias de seguridad de ser modificadas o eliminadas. Esta opción utiliza la tecnología DataLock de NetApp. Cada copia de seguridad se bloqueará durante el período de retención, o durante un mínimo de 30 días, más un período de búfer de hasta 14 días.



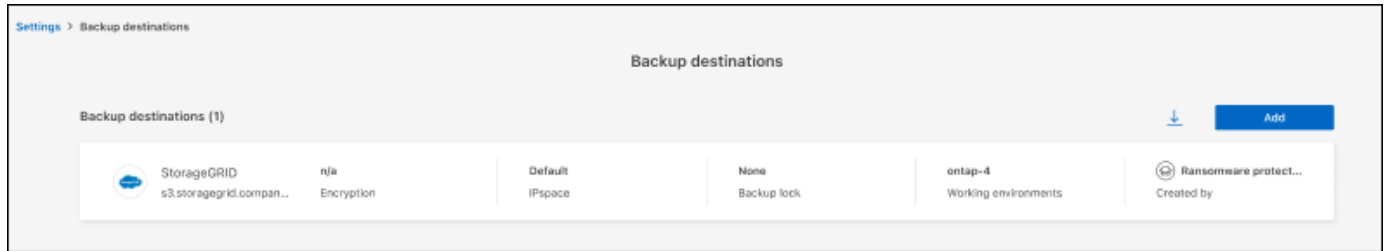
Si configura ahora el ajuste de bloqueo de copia de seguridad, no es posible cambiarlo más tarde después de configurar el destino de copia de seguridad.

- **Modo de cumplimiento:** Los usuarios no pueden sobrescribir ni eliminar los archivos de copia de seguridad 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.





## Añada Amazon Web Services como destino de backup

Para configurar AWS como destino de backup, introduzca la siguiente información.

Para obtener más información sobre la gestión de su almacenamiento de AWS en BlueXP, consulte "[Gestione sus bloques de Amazon S3](#)".

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

### Add backup destination

Name	backup-dest1	▼
Provider	<span style="color: blue; font-size: small;">(i) Action required</span>	▲
<p style="font-size: small; color: gray;">Select a provider to back up to the cloud.</p> <div style="display: flex; justify-content: space-around; align-items: center; margin-top: 10px;"> <div style="text-align: center; border: 1px solid #ccc; padding: 10px; width: 150px;">               Amazon Web Services         </div> <div style="text-align: center; border: 1px solid #ccc; padding: 10px; width: 150px;">               StorageGRID         </div> </div>		
Provider settings	Defined by provider selection	▼
Networking	Defined by provider selection	▼
Backup lock	Defined by provider selection	▼

Cancel
Add

3. Seleccione **Amazon Web Services**.

4. Seleccione la flecha hacia abajo junto a cada ajuste e introduzca o seleccione valores:

- **Configuración del proveedor:**

- Crea un nuevo bloque, selecciona un bloque existente si ya existe uno en BlueXP o trae tu propio bloque que almacenará los backups.
- Cuenta, región, clave de acceso y clave secreta de AWS para las credenciales de AWS

"Si desea traer su propio cubo, consulte [Agregar cubos S3](#)".

- **Cifrado:** Si está creando un nuevo depósito de S3, introduzca la información de clave de cifrado que le haya proporcionado el proveedor. Si eligió un depósito existente, la información de cifrado ya estará disponible.

De forma predeterminada, los datos del bloque se cifran con claves gestionadas por AWS. Puede seguir utilizando claves administradas por AWS o puede gestionar el cifrado de sus datos utilizando sus propias claves.

- **Redes:** Elige el espacio IP y si vas a usar un Punto Final Privado.

- El espacio IP es el clúster donde residen los volúmenes del que se desea incluir en un backup. Las LIF entre clústeres de este espacio IP deben tener acceso a Internet saliente.

- Opcionalmente, seleccione si va a utilizar un punto final privado de AWS (PrivateLink) que haya configurado previamente.

Si desea utilizar AWS PrivateLink, consulte ["AWS PrivateLink para Amazon S3"](#).

- **\* Bloqueo de respaldo\***: Elija si desea que el servicio proteja las copias de seguridad de ser modificadas o eliminadas. Esta opción utiliza la tecnología DataLock de NetApp. Cada copia de seguridad se bloqueará durante el período de retención, o durante un mínimo de 30 días, más un período de búfer de hasta 14 días.



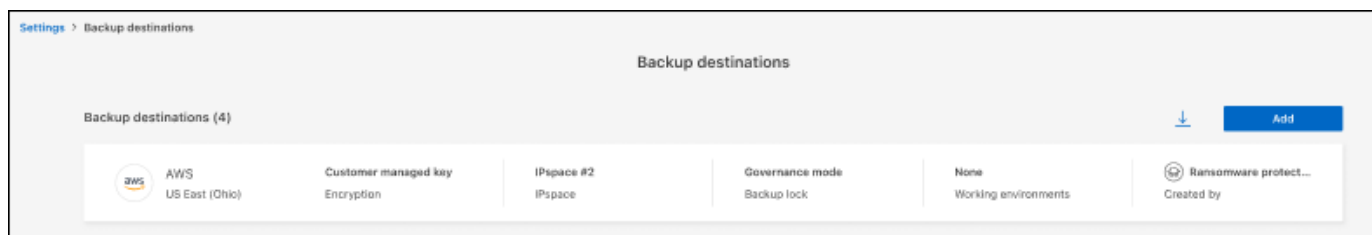
Si configura ahora el ajuste de bloqueo de copia de seguridad, no es posible cambiarlo más tarde después de configurar el destino de copia de seguridad.

- **Modo de gobierno**: Los usuarios específicos (con el permiso S3:BypassGovernanceRetention) pueden sobrescribir o eliminar archivos protegidos durante el período de retención.
- **Modo de cumplimiento**: Los usuarios no pueden sobrescribir ni eliminar los archivos de copia de seguridad 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.



## Preguntas frecuentes sobre la protección contra ransomware de BlueXP

Estas preguntas frecuentes pueden ser de ayuda si solo está buscando una respuesta rápida a una pregunta.

### Acceso

#### ¿Cuál es la URL de protección contra ransomware de BlueXP?

Para la URL, en un navegador, introduzca: ["https://console.bluexp.netapp.com/"](https://console.bluexp.netapp.com/) Para acceder a la consola BlueXP.

#### ¿Necesitas una licencia para usar la protección contra ransomware de BlueXP?

No se requiere un archivo de licencia de NetApp (NLF). La versión previa de la protección contra ransomware de BlueXP no requiere ninguna licencia especial. Todas las licencias de vista previa son licencias de evaluación.

Para la versión previa de este servicio, se requiere una licencia de servicio de backup y recuperación de BlueXP.



Para la versión de vista previa, NetApp ayuda a configurar la evaluación y las licencias necesarias.

### ¿Cómo habilitas la protección contra ransomware de BlueXP?

La protección frente al ransomware de BlueXP no requiere habilitación. La opción de protección frente a ransomware se habilita automáticamente en la navegación de la izquierda de BlueXP.

Para la versión de vista previa, debes registrarte o ponerte en contacto con tu representante de ventas de NetApp para probar este servicio. Una vez que utilices BlueXP Connector, incluirá las prestaciones adecuadas para el servicio.

### ¿La protección contra ransomware de BlueXP está disponible en modos estándar, restringido y privado?

Por el momento, la protección contra ransomware de BlueXP solo está disponible en modo estándar. Manténgase atento para obtener más información.

Para ver una explicación sobre estos modos en todos los servicios de BlueXP, consulte ["Modos de implementación de BlueXP"](#).

- ¿Cómo se manejan los permisos de acceso?\*\*\*  
Solo los administradores de cuentas tienen la capacidad de iniciar el servicio y detectar cargas de trabajo (porque esto implica comprometerse con el uso de un recurso). Cualquier rol puede realizar interacciones posteriores.
- ¿Qué resolución de dispositivo es la mejor?\*\*\*  
La resolución de dispositivo recomendada para la protección contra ransomware de BlueXP es 1920x1080 o superior.
- ¿Qué navegador debo usar?\*\*\*  
Cualquier navegador moderno funcionará.

## Interacción con otros servicios

### ¿La protección contra ransomware de BlueXP es consciente de las configuraciones de protección hechas en NetApp ONTAP?

Sí, la protección frente a ransomware de BlueXP detecta las programaciones de Snapshot establecidas en ONTAP.

### Si estableces una política usando la protección contra ransomware de BlueXP, ¿tienes que hacer cambios futuros solo en este servicio?

Te recomendamos que realices cambios de política en el servicio de protección contra ransomware de BlueXP.

## Cargas de trabajo

- ¿Qué compone una carga de trabajo?\*\*\*  
Una carga de trabajo incluye todos los volúmenes que utiliza una única instancia de aplicación. Por ejemplo, una instancia de Oracle DB desplegada en ora3.host.com puede tener vol1 y vol2 para sus datos y registros, respectivamente. Esos volúmenes juntos constituyen la carga de trabajo para esa instancia específica de la instancia de Oracle DB.

### ¿Cómo prioriza la protección contra ransomware de BlueXP los datos de carga de trabajo?

La prioridad de los datos para la versión Preview viene determinada por las copias snapshot realizadas y las copias de seguridad programadas.

La prioridad de la carga de trabajo se determina en las siguientes frecuencias de Snapshot:

- **Crítico:** Copias instantáneas tomadas menos de 1 por hora (programa de protección altamente agresivo)
- **Importante:** Copias instantáneas tomadas menos de 1 por día pero más de 1 por hora
- **Estándar:** Copias instantáneas tomadas más de 1 por día

#### **Nuevo volumen añadido, pero aún no aparece**

Si añadió un volumen nuevo a su entorno, inicie la detección nuevamente y aplique políticas de protección para proteger ese nuevo volumen.

#### **La consola no muestra todas mis cargas de trabajo. ¿Qué podría estar mal?**

Actualmente, solo se admiten volúmenes NFS. Los volúmenes iSCSI, los volúmenes CIFS y otras configuraciones no compatibles se filtran y no aparecen en la consola.

## **Políticas de protección**

#### **¿Coexisten las políticas de ransomware de BlueXP con los otros tipos de políticas de cargas de trabajo?**

En este momento, el backup y recuperación de datos de BlueXP (Cloud Backup) admite una política de backup por volumen. Por ello, el backup y la recuperación de BlueXP y la protección frente a ransomware de BlueXP comparten las políticas de backup.

Las copias Snapshot no están limitadas y se pueden añadir por separado en cada servicio.

# Usa la protección frente al ransomware de BlueXP

## Usa la protección frente al ransomware de BlueXP

Gracias a la protección frente al ransomware de BlueXP, podrás ver el estado de las cargas de trabajo y proteger las cargas de trabajo.

- ["Detecta cargas de trabajo en la protección frente al ransomware de BlueXP"](#).
- ["Ver la protección y el estado de la carga de trabajo desde la Consola"](#).
  - Revisa y actúa en cuanto a las recomendaciones de protección contra ransomware.
- ["Proteja las cargas de trabajo"](#):
  - Asigna una política de protección contra ransomware a las cargas de trabajo.
  - Aumenta la protección de las aplicaciones para evitar futuros ataques de ransomware.
  - Cree, cambie o elimine una política de protección.
- ["Responde a la detección de posibles ataques de ransomware"](#).
- ["Recupérese de un ataque"](#) (después de neutralizar los incidentes).
- ["Configure las opciones de protección"](#).

## Vea de un vistazo el estado de las cargas de trabajo mediante la consola

La consola de protección frente a ransomware de BlueXP proporciona información de un vistazo sobre el estado de protección de tus cargas de trabajo. Puede determinar rápidamente cargas de trabajo que están en riesgo o protegidas, identificar cargas de trabajo afectadas por un incidente o en recuperación y medir el grado de protección observando cuánto almacenamiento está protegido o en riesgo.

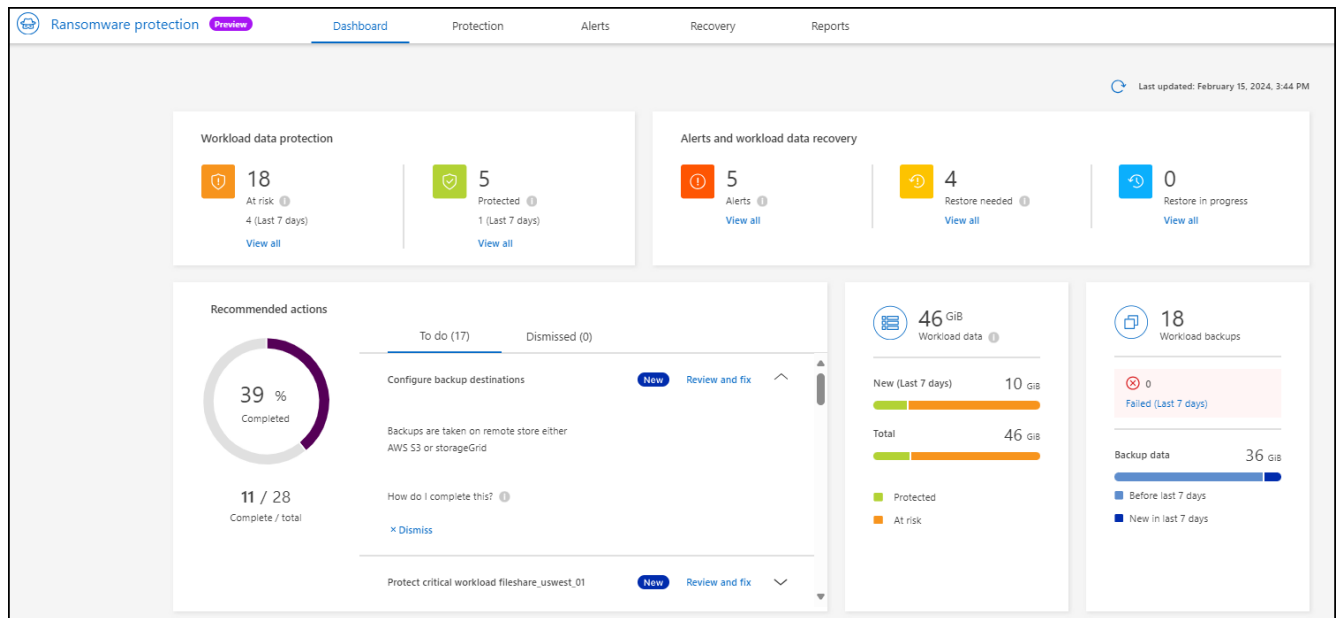
También puede usar la consola para revisar y actuar sobre las recomendaciones de protección.

### Revisar el estado de la carga de trabajo mediante la consola

#### Pasos

1. En la navegación izquierda de BlueXP, selecciona **Protección > Protección contra ransomware**.

Después de la detección, la consola muestra el estado de la protección de datos de las cargas de trabajo.



2. En Dashboard, puede ver y realizar cualquiera de las siguientes acciones en cada uno de los paneles:

- **Protección de datos de carga de trabajo:** Haga clic en **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 "[Proteja las cargas de trabajo](#)".
- **Alertas y recuperación de datos de carga de trabajo:** Haga clic en **Ver todo** para ver los incidentes activos que han impactado en su carga de trabajo, están listos para la recuperación después de que los incidentes se neutralizan o están en recuperación. Consulte "[Responder a una alerta detectada](#)".

Un incidente se clasifica en uno de los siguientes estados:

- Afectado (se muestra en la página Alertas)
- Listo para la recuperación (se muestra en la página Recuperación)
- Recuperando (se muestra en la página Recovery)
- Recovery Failed (se muestra en la página Recovery)
- Recuperado (se muestra en la página Recovery)
- **Acciones recomendadas:** Para aumentar la protección, revise cada recomendación y haga clic en **Revisar y arreglar**.

Consulte "[Revise las recomendaciones de protección en la consola](#)" o "[Proteja las cargas de trabajo](#)".

Cualquier recomendación que se haya agregado desde la última vez que visitó el Panel de Control se indica con "Nuevo" durante al menos 24 horas. Las acciones se enumeran en orden de prioridad con las más importantes en la parte superior. Puede revisar y actuar en cada uno de ellos o descartarlo.

El número total de acciones no incluye acciones descartadas.

- **Datos de carga de trabajo:** Monitorea los cambios en la cobertura de protección durante los últimos 7 días.
- **Copias de seguridad de la carga de trabajo:** Monitorea los cambios en las copias de seguridad de la carga de trabajo creadas por el servicio que han fallado o se han completado correctamente en los últimos 7 días.



## Revise las recomendaciones de protección en la consola

La protección frente al ransomware de BlueXP evalúa la protección de tus cargas de trabajo y recomienda acciones para mejorar esa protección.

Puede revisar una recomendación y actuar sobre ella, lo que cambia el estado de la recomendación a Finalizado. O, si quieres actuar sobre ello más tarde, puedes desestimarla. Al ignorar una acción, la recomendación se mueve a una lista de acciones descartadas, que puede revisar más adelante.

Aquí hay una muestra de las recomendaciones que ofrece el servicio.

Recomendación	Descripción	Cómo resolver
Añade una política de protección contra ransomware	La carga de trabajo actualmente no está protegida.	Asigne una política a la carga de trabajo. Consulte " <a href="#">Protege las cargas de trabajo contra ataques de ransomware</a> ".
Configurar destinos de copia de seguridad	La carga de trabajo no tiene ningún destino de backup.	Añada destinos de backup a esta carga de trabajo para protegerla. Consulte " <a href="#">Configure las opciones de protección</a> ".
Haga una política más fuerte.	Es posible que algunas cargas de trabajo no tengan suficiente protección. Refuerce la protección en las cargas de trabajo con una política.	Aumenta la retención, agrega copias de seguridad, aplica copias de seguridad inmutables, bloquea extensiones de archivos sospechosos, habilita la detección en el almacenamiento secundario y mucho más. Consulte " <a href="#">Protege las cargas de trabajo contra ataques de ransomware</a> ".
Protege las cargas de trabajo de aplicaciones cruciales o importantes contra el ransomware.	La página Proteger muestra las cargas de trabajo de la aplicación críticas o importantes (según el nivel de prioridad asignado) que no están protegidas.	Asigne una política a estas cargas de trabajo. Consulte " <a href="#">Protege las cargas de trabajo contra ataques de ransomware</a> ".
Protege las cargas de trabajo de archivos compartidos cruciales o importantes contra el ransomware.	La página Protection muestra cargas de trabajo críticas o importantes del tipo File Share o Datastore que no están protegidas.	Asigne una política a cada una de las cargas de trabajo. Consulte " <a href="#">Protege las cargas de trabajo contra ataques de ransomware</a> ".
Revisar nuevas alertas	Existen nuevas alertas.	Revise las nuevas alertas. Consulte " <a href="#">Responder a una alerta de ransomware detectada</a> ".

### Pasos

1. En la navegación izquierda de BlueXP, selecciona **Protección > Protección contra ransomware**.
2. En el panel Acciones recomendadas, selecciona una recomendación y selecciona **Revisar y corregir**.
3. Para descartar la acción hasta más tarde, selecciona **Descartar**.

La recomendación se borra de la lista de tareas pendientes y aparece en la lista de rechazados.



Más adelante, puede cambiar un elemento despedido a un elemento de tarea. Cuando marca un elemento como finalizado o cambia un elemento descartado a una acción de tarea, las acciones totales aumentan en 1.

4. Para revisar la información sobre cómo actuar sobre las recomendaciones, seleccione el icono **INFORMACIÓN**.

## Protege las cargas de trabajo contra ataques de ransomware

Puedes proteger las cargas de trabajo contra ataques de ransomware completando las siguientes acciones mediante la protección contra ransomware de BlueXP.

- Ver la protección de cargas de trabajo existentes.
- Asignar una política a una carga de trabajo.
  - Aumente la protección de la aplicación para evitar futuros ataques RW.
  - Cambie la protección de una carga de trabajo que estaba protegida previamente en el servicio RW.
- Gestione las políticas (solo las que haya creado).

La protección frente al ransomware de BlueXP asigna una prioridad a cada carga de trabajo durante la detección. La prioridad de la carga de trabajo se determina en las siguientes frecuencias de Snapshot:

- **Crítico:** Copias instantáneas tomadas menos de 1 por hora (programa de protección altamente agresivo)
- **Importante:** Copias instantáneas tomadas menos de 1 por día pero más de 1 por hora
- **Estándar:** Copias instantáneas tomadas más de 1 por día

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

- **Protegido:** Se aplica una política.
- **En riesgo:** No se aplica ninguna política.
- **En progreso:** Se está aplicando una política pero aún no se ha completado.
- **Fallo:** Se aplica una política pero no funciona.

**Protección de la salud:** Una carga de trabajo puede tener uno de los siguientes estados de protección de la salud:

- **Healthy:** La carga de trabajo tiene la protección habilitada y se han completado las copias de seguridad y las copias de Snapshot.
- **En progreso:** Las copias de seguridad o las copias snapshot están en curso.
- **Fallo:** Las copias de seguridad o las copias de Snapshot no se han completado correctamente.
- **N/A:** La protección no está habilitada o es suficiente en la carga de trabajo.

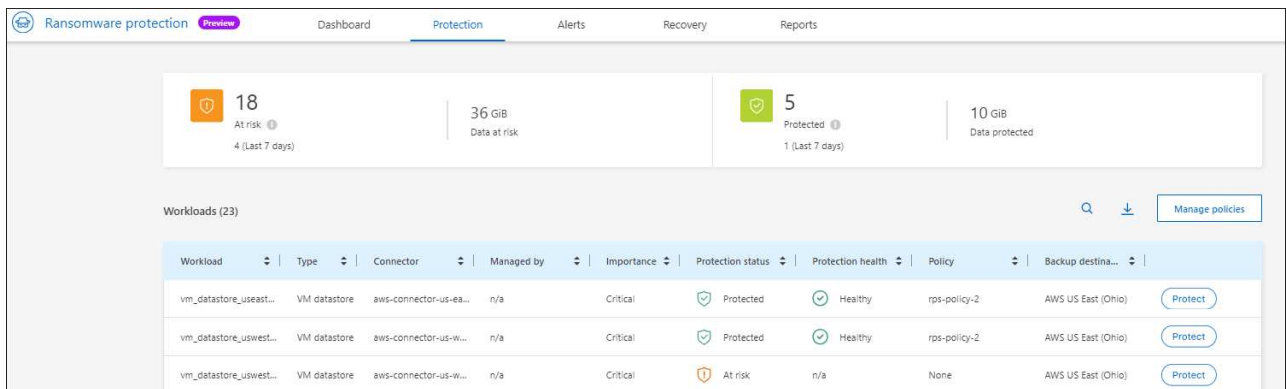
## Mira la protección contra ransomware de las cargas de trabajo

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

- Cargas de trabajo de máquinas virtuales
- Cargas de trabajo de recursos compartidos de archivos

### Pasos

1. En la navegación izquierda de BlueXP, selecciona **Protección > Protección contra ransomware**.
2. Debe realizar una de las siguientes acciones:
  - En el panel de protección de datos del panel, seleccione **Ver todo**.
  - En el menú, selecciona **Protección**.



3. En esta página, puede asignar una política a una carga de trabajo.

## Asigne una política de protección predefinida a las cargas de trabajo

Para ayudar a proteger los datos, se puede asignar una política de protección contra ransomware existente a una o más cargas de trabajo. También puede asignar una política diferente a una carga de trabajo que ya tenga una política.

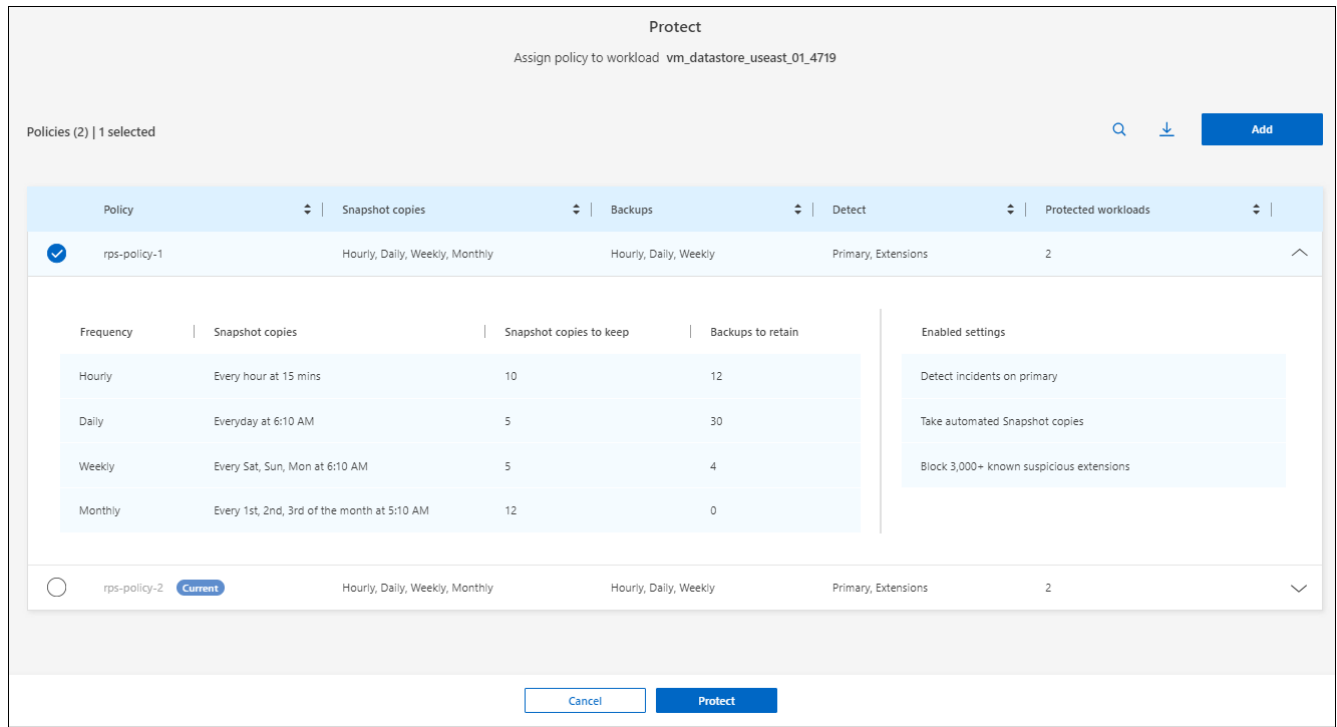
La protección contra ransomware de BlueXP incluye las siguientes políticas predefinidas que se alinean con la prioridad de carga de trabajo:

Nivel de política	Snapshot	Frecuencia	Retención (días)	N.o de copias Snapshot	Número máximo total de copias snapshot
<b>Política de carga de trabajo crítica</b>	Cada trimestre	Cada 15 min	3	288	309
	Todos los días	Cada 1 días	14	14	309
	Semanal	Cada 1 semanas	35	5	309
	Mensual	Cada 30 días	60	2	309

Nivel de política	Snapshot	Frecuencia	Retención (días)	N.o de copias Snapshot	Número máximo total de copias snapshot
<b>Política de carga de trabajo importante</b>	Cada trimestre	Cada 30 minutos	3	144	165
	Todos los días	Cada 1 días	14	14	165
	Semanal	Cada 1 semanas	35	5	165
	Mensual	Cada 30 días	60	2	165
<b>Política de carga de trabajo estándar</b>	Cada trimestre	Cada 60 min	3	72	93
	Todos los días	Cada 1 días	14	14	93
	Semanal	Cada 1 semanas	35	5	93
	Mensual	Cada 30 días	60	2	93

### Pasos

- Con la protección contra ransomware de BlueXP, realice una de las siguientes acciones:
  - En el panel de protección de datos del panel, seleccione **Ver todo**.
  - En el panel Recomendación del panel de control, seleccione una recomendación sobre la asignación de una política y seleccione **Revisar y corregir**.
  - En el menú, seleccione **Protección**.
- En la página Protección, revise las cargas de trabajo y seleccione **Proteger** junto a la carga de trabajo.  
Aparece una lista de políticas.



3. Para ver los detalles, haga clic en la flecha hacia abajo de una política.
4. Seleccione una política para asignar a la carga de trabajo.
5. Seleccione **Proteger**.
6. Revise el panel de acciones recomendadas de la consola, que muestra la acción como «Completada».

## Cree una política de protección

Si las políticas existentes no satisfacen sus necesidades empresariales, puede crear una nueva política de protección. Puede crear su propia política desde cero o utilizar una política existente y modificar su configuración.

Puede crear normativas que rijan el almacenamiento principal y secundario y tratar el almacenamiento primario y secundario de manera igual o diferente.

Puede crear una política al gestionarla o durante el proceso de asignación de una política a una carga de trabajo.

### Pasos para crear una política durante la gestión de políticas

1. En el menú de protección contra ransomware de BlueXP, selecciona **Protección**.

18 At risk (4 Last 7 days) | 36 GiB Data at risk | 5 Protected (1 Last 7 days) | 10 GiB Data protected

Workloads (23) Manage policies

Workload	Type	Connector	Managed by	Importance	Protection status	Protection health	Policy	Backup destina...
vm_datastore_useast...	VM datastore	aws-connector-us-aa...	n/a	Critical	Protected	Healthy	RPS-Policy-Importatnt	AWS US East (Ohio)
vm_datastore_uswest...	VM datastore	aws-connector-us-w...	n/a	Critical	Protected	Healthy	RPS-Policy-Importatnt	AWS US East (Ohio)
vm_datastore_uswest...	VM datastore	aws-connector-us-w...	n/a	Critical	At risk	n/a	None	AWS US East (Ohio)

2. En la página Protección, selecciona **Administrar políticas**.

Protection > Manage policies

Manage policies

Policies (3) Add

Policy	Snapshot copies	Backups	Detect	Protected workloads
RPS-Policy-Critical	Hourly, daily, weekly, monthly	Hourly, daily, weekly, monthly	Primary, extensions	2
RPS-Policy-Importatnt	Hourly, daily, weekly, monthly	Hourly, daily, weekly, monthly	Primary, extensions	2
RPS-Policy-Standard	Hourly, daily, weekly, monthly	Hourly, daily, weekly, monthly	Primary, extensions	0

3. En la página Administrar políticas, selecciona **Agregar**.

Protection > Manage policies > Add policy

Add policy

Policy name: test-policy

Copy from existing policy: No policy selected Select

Primary storage

- Snapshot copy schedules: Weekly
- Primary detection: Disable
- Block file extensions: Disable

Secondary storage

- Backup schedules: Weekly
- Secondary detection: Disable

Cancel Add

4. Introduzca un nombre de política nuevo o introduzca un nombre de política existente para copiarlo. Si introduce un nombre de política existente, elija qué política desea copiar.



Si decide copiar y modificar una política existente, debe cambiar al menos una configuración para que sea única.

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

◦ **Almacenamiento primario:**

- **Programaciones de copias snapshot:** Elija las opciones de programación, el número de copias snapshot que desea conservar y seleccione habilitar la programación.
- **Detección primaria:** Habilita el servicio para detectar incidentes de ransomware en el almacenamiento primario.
- **Extensiones de archivo de bloque:** Permite que este tenga el bloqueo de servicio conocido extensiones de archivo sospechosas. El servicio realiza copias Snapshot automatizadas cuando está habilitada la detección primaria.

◦ **Almacenamiento secundario:**

- **Horarios de copia de seguridad:** Elija opciones de programación para el almacenamiento secundario y habilite el horario.
- **Detección secundaria:** Habilita el servicio para detectar incidentes de ransomware en el almacenamiento secundario.
- **Bloquear copias de seguridad:** Elija esta opción para evitar que las copias de seguridad en el almacenamiento secundario se modifiquen o eliminen durante un cierto período de tiempo. Esto también se denomina *almacenamiento inmutable*.

Esta opción utiliza la tecnología DataLock de NetApp, que bloquea los backups en el almacenamiento secundario. El período de tiempo durante el que el archivo de copia de seguridad está bloqueado (y retenido) se denomina período de retención de DataLock. Se basa en el programa de políticas de backup y la configuración de retención que haya definido, además de un búfer de 14 días. Cualquier política de retención de DataLock que sea inferior a 30 días se redondea a un mínimo de 30 días.

6. Seleccione **Agregar**.

### Pasos para crear una política durante la asignación de la política de protección

1. En el menú de protección contra ransomware de BlueXP, selecciona **Protección**.

The screenshot displays the ransomware protection dashboard. At the top, there are two summary cards: one for 'At risk' data (18 items, 36 GiB) and one for 'Protected' data (5 items, 10 GiB). Below these is a table of workloads with columns for Workload, Type, Connector, Managed by, Importance, Protection status, Protection health, Policy, and Backup destination. Each row includes a 'Protect' button.

Workload	Type	Connector	Managed by	Importance	Protection status	Protection health	Policy	Backup destina...	
vm_datastore_useast...	VM datastore	aws-connector-us-ea...	n/a	Critical	Protected	Healthy	RPS-Policy-Importatnt	AWS US East (Ohio)	Protect
vm_datastore_uswest...	VM datastore	aws-connector-us-w...	n/a	Critical	Protected	Healthy	RPS-Policy-Importatnt	AWS US East (Ohio)	Protect
vm_datastore_uswest...	VM datastore	aws-connector-us-w...	n/a	Critical	At risk	n/a	None	AWS US East (Ohio)	Protect

2. En la página Protección, selecciona **Proteger**.

3. En la página Proteger, selecciona **Añadir**.

Protection > Manage policies > Add policy

### Add policy

Policy name

Copy from existing policy No policy selected Select

**Primary storage**

Snapshot copy schedules	Weekly	▼
Primary detection	Disable	▼
Block file extensions	Disable	▼

**Secondary storage**

Backup schedules	Weekly	▼
Secondary detection	Disable	▼

Cancel
Add

4. Complete el proceso, que es lo mismo que crear una política desde la página Gestionar políticas.

## Asigne una política de protección diferente

Puede seleccionar una política de protección diferente para una carga de trabajo.

Puede que desee aumentar la protección para evitar futuros ataques de ransomware cambiando la política de protección.

### Pasos

1. En el menú de protección contra ransomware de BlueXP, selecciona **Protección**.
2. En la página Proteger, seleccione una carga de trabajo y seleccione **Proteger**.
3. En la página Protect, seleccione una política diferente para la carga de trabajo.
4. Para cambiar cualquier detalle de la política, seleccione la flecha hacia abajo a la derecha y cambie los detalles.
5. Seleccione **Guardar** para finalizar el cambio.

## Editar una política existente

Solo es posible cambiar los detalles de una política cuando la política no está asociada con una carga de trabajo.

### Pasos

1. En el menú de protección contra ransomware de BlueXP, selecciona **Protección**.
2. En la página Protección, selecciona **Administrar políticas**.
3. En la página Administrar políticas, seleccione la opción **Acciones** para la política que desea cambiar.
4. En el menú Acciones, selecciona **Editar política**.
5. Cambie los detalles.



6. Selecciona **Guardar** para finalizar el cambio.

## Eliminar una política

Es posible eliminar una política de protección que actualmente no esté asociada a ninguna carga de trabajo.

### Pasos

1. En el menú de protección contra ransomware de BlueXP, selecciona **Protección**.
2. En la página Protección, selecciona **Administrar políticas**.
3. En la página Administrar políticas, seleccione la opción **Acciones** para la política que desea eliminar.
4. En el menú Acciones, selecciona **Eliminar política**.

## Responder a una alerta de ransomware detectada

Si la protección frente al ransomware de BlueXP detecta un posible ataque, aparece una alerta en el panel de protección contra ransomware de BlueXP y en las notificaciones de BlueXP en la parte superior derecha que indican un posible ataque de ransomware. El servicio también inicia inmediatamente la creación de una copia snapshot. En este punto, deberías analizar el riesgo potencial en la pestaña **Alertas** de protección contra ransomware de BlueXP.

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

Cada alerta podría tener varios incidentes en volúmenes diferentes con estados diferentes, así que asegúrese de revisar todos los incidentes.

El servicio proporciona información llamada *Evidence* sobre qué causó que se emitiera la alerta, como la siguiente:

- Las extensiones de archivo se han creado o cambiado
- Se ha producido la creación del archivo y se ha aumentado en un porcentaje mostrado
- Se ha suprimido el archivo y se ha aumentado en un porcentaje mostrado

Una alerta se basa en los siguientes tipos de comportamiento:

- **Ataque potencial:** Una alerta se produce 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:
  - La detección de una nueva extensión no se ha identificado antes y el mismo comportamiento no se repite las veces suficientes para declararla como un ataque.
  - Se observa una alta entropía.
  - Las operaciones de lectura/escritura/cambio de nombre/eliminación de archivos han experimentado un aumento del 100% de la actividad más allá de la línea base.

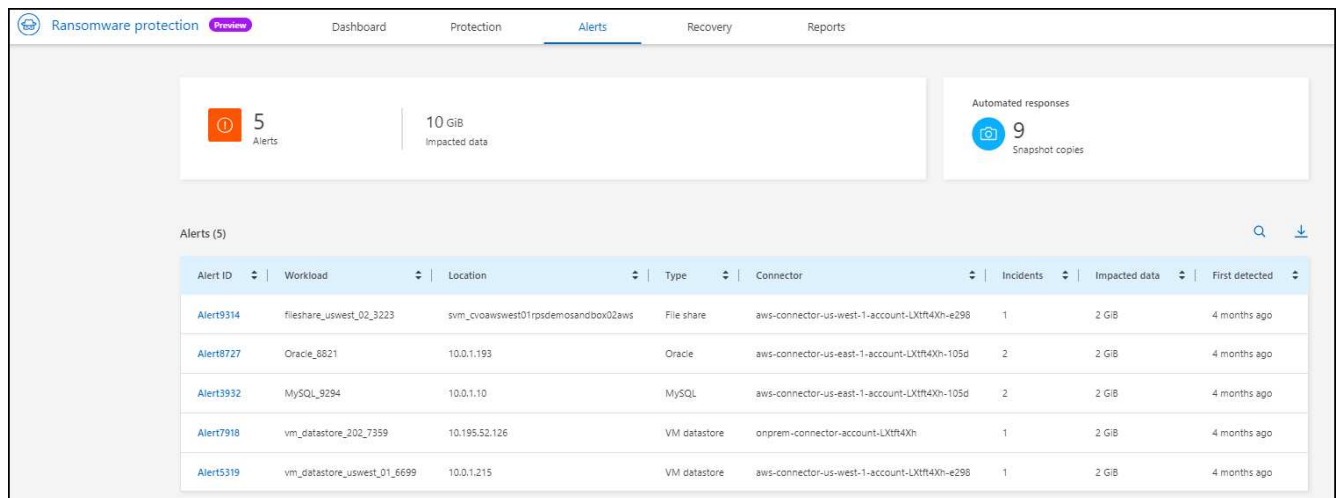
La evidencia se basa en la información de la Protección Autónoma contra el ransomware de ONTAP. Para obtener más información, consulte ["Información general sobre la protección de ransomware autónoma"](#).

## Ver las alertas

Puedes acceder a alertas desde el Panel de protección contra ransomware de BlueXP o desde la pestaña \* Alertas \*.

### Pasos

1. En la consola de protección contra ransomware de BlueXP, revisa el panel Alertas.
2. Selecciona **Ver todo** debajo de una de las estatuas.
3. Haga clic en una alerta para revisar todos los incidentes en cada volumen de cada alerta.
4. Para revisar alertas adicionales, haga clic en **Alert** en las rutas de navegación en la parte superior izquierda.
5. Revise las alertas en la página Alertas.



Alert ID	Workload	Location	Type	Connector	Incidents	Impacted data	First detected
Alert9314	fileshare_uswest_02_3223	svm_cvoawswest01rpsdemosandbox02aws	File share	aws-connector-us-west-1-account-LXtf4Xh-e298	1	2 GiB	4 months ago
Alert8727	Oracle_8821	10.0.1.193	Oracle	aws-connector-us-east-1-account-LXtf4Xh-105d	2	2 GiB	4 months ago
Alert3932	MySQL_9294	10.0.1.10	MySQL	aws-connector-us-east-1-account-LXtf4Xh-105d	2	2 GiB	4 months ago
Alert7918	vm_datastore_202_7359	10.195.52.126	VM datastore	onprem-connector-account-LXtf4Xh	1	2 GiB	4 months ago
Alert5319	vm_datastore_uswest_01_6699	10.0.1.215	VM datastore	aws-connector-us-west-1-account-LXtf4Xh-e298	1	2 GiB	4 months ago

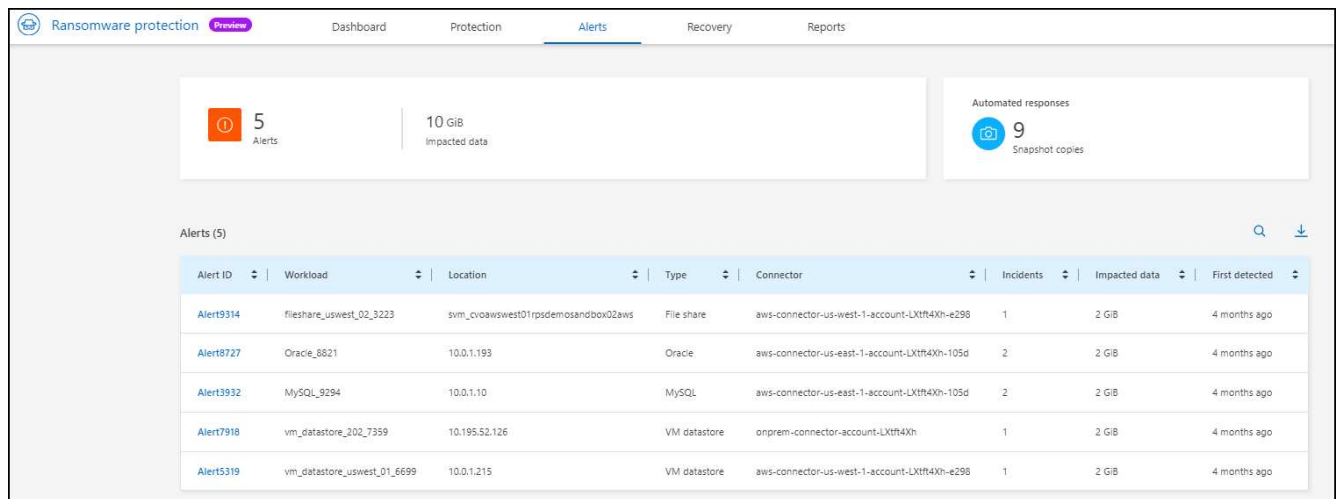
6. Continúe con [Marcar los incidentes de ransomware como listos para la recuperación \(después de neutralizar los incidentes\)](#).

## Marcar los incidentes de ransomware como listos para la recuperación (después de neutralizar los incidentes)

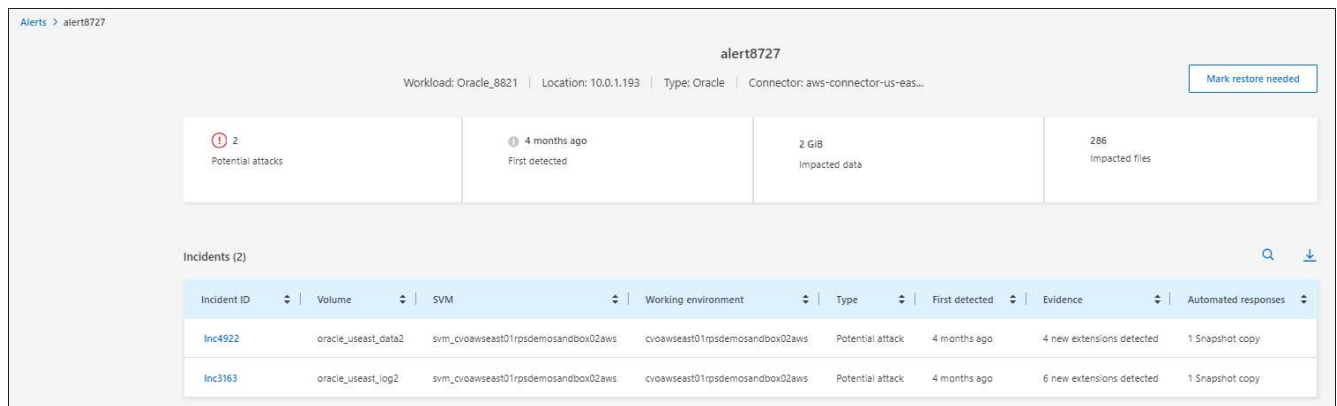
Una vez que haya mitigado el ataque y esté listo para recuperar cargas de trabajo, debe comunicarse con el equipo de administrador de almacenamiento que los datos están listos para la recuperación, de modo que puedan iniciar el proceso de recuperación.

### Pasos

1. En el menú de protección contra ransomware de BlueXP, selecciona **Alertas**.



- En la página Alerts, seleccione la alerta.
- Revise los incidentes en la alerta.



- Si determina que los incidentes están listos para la recuperación, seleccione **Marcar restauración necesaria**.
- Confirme la acción y seleccione **Mark restore needed**.
- Para iniciar la recuperación de la carga de trabajo, seleccione **Recuperar** carga de trabajo en el mensaje o seleccione la pestaña **Recuperar**.

## Resultado

Una vez que se marca la alerta para la recuperación, la alerta pasa de la pestaña Alertas a la pestaña Recuperación.

## Recuperarse de un ataque de ransomware (después de neutralizar los incidentes)

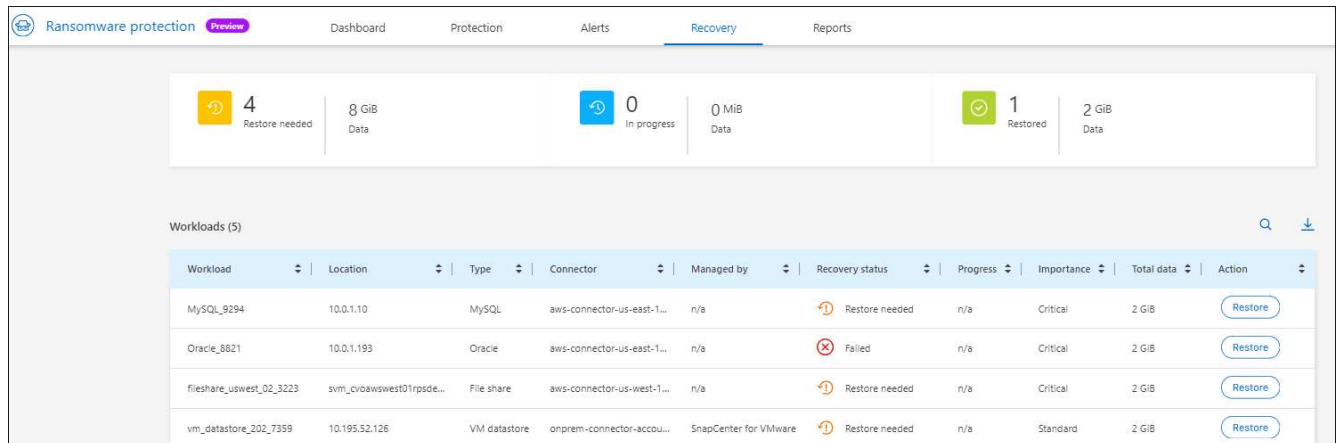
Después de que las cargas de trabajo se hayan marcado como «listas para la recuperación», la protección contra el ransomware de BlueXP recomienda un punto de recuperación real (RPA) y orquesta el flujo de trabajo para una recuperación resistente a los fallos.

## Permite ver las cargas de trabajo que están listas para restaurarse

Revise las cargas de trabajo que se encuentran en el estado de recuperación «Restauración necesaria».

### Pasos

1. Debe realizar una de las siguientes acciones:
  - Desde el Panel de Control, revise los totales “Restaurar necesario” en el panel Alertas y seleccione **Ver todo**.
  - En el menú, seleccione **Recuperación**.
2. Revise la información de la carga de trabajo en la página **Recovery**.



The screenshot shows the 'Recovery' page in the BlueXP interface. At the top, there are navigation tabs: Dashboard, Protection, Alerts, Recovery (selected), and Reports. Below the navigation, there are three summary cards: '4 Restore needed' (8 GiB Data), '0 In progress' (0 MiB Data), and '1 Restored' (2 GiB Data). Below these cards is a table titled 'Workloads (5)' with columns: Workload, Location, Type, Connector, Managed by, Recovery status, Progress, Importance, Total data, and Action. The table contains four rows of workload data.

Workload	Location	Type	Connector	Managed by	Recovery status	Progress	Importance	Total data	Action
MySQL_9294	10.0.1.10	MySQL	aws-connector-us-east-1...	n/a	Restore needed	n/a	Critical	2 GiB	Restore
Oracle_8821	10.0.1.193	Oracle	aws-connector-us-east-1...	n/a	Failed	n/a	Critical	2 GiB	Restore
fileshare_uswest_02_3223	svm_cvbawswest01rpsde...	File share	aws-connector-us-west-1...	n/a	Restore needed	n/a	Critical	2 GiB	Restore
vm_datastore_202_7359	10.195.52.126	VM datastore	onprem-connector-accou...	SnapCenter for VMware	Restore needed	n/a	Standard	2 GiB	Restore

## Recuperar una carga de trabajo

Gracias a la protección frente al ransomware de BlueXP, el administrador de almacenamiento puede determinar la mejor forma de recuperar las cargas de trabajo, ya sea desde el punto de restauración recomendado o desde su punto de restauración preferido.

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

- Recuperar todos los volúmenes
- Recuperar una aplicación en el nivel de volumen o a nivel de archivo y carpeta.
- Recupere un recurso compartido de archivos en el nivel de volumen, directorio o archivo/carpeta.
- Recuperación de un almacén de datos en el nivel de máquina virtual.

El proceso difiere levemente en función del tipo de carga de trabajo.

### Pasos

1. En el menú de protección contra ransomware de BlueXP, selecciona **Recuperación**.
2. Revise la información de la carga de trabajo en la página **Recovery**.
3. Seleccione una carga de trabajo que esté en el estado «Restore needed».
4. Para restaurar, seleccione **Restaurar**.
5. **Restore Scope**: Seleccione el tipo de restauración que desea completar:
  - Todos los volúmenes
  - Por volumen

- Por archivo: Puede especificar una carpeta o archivos individuales para restaurar.

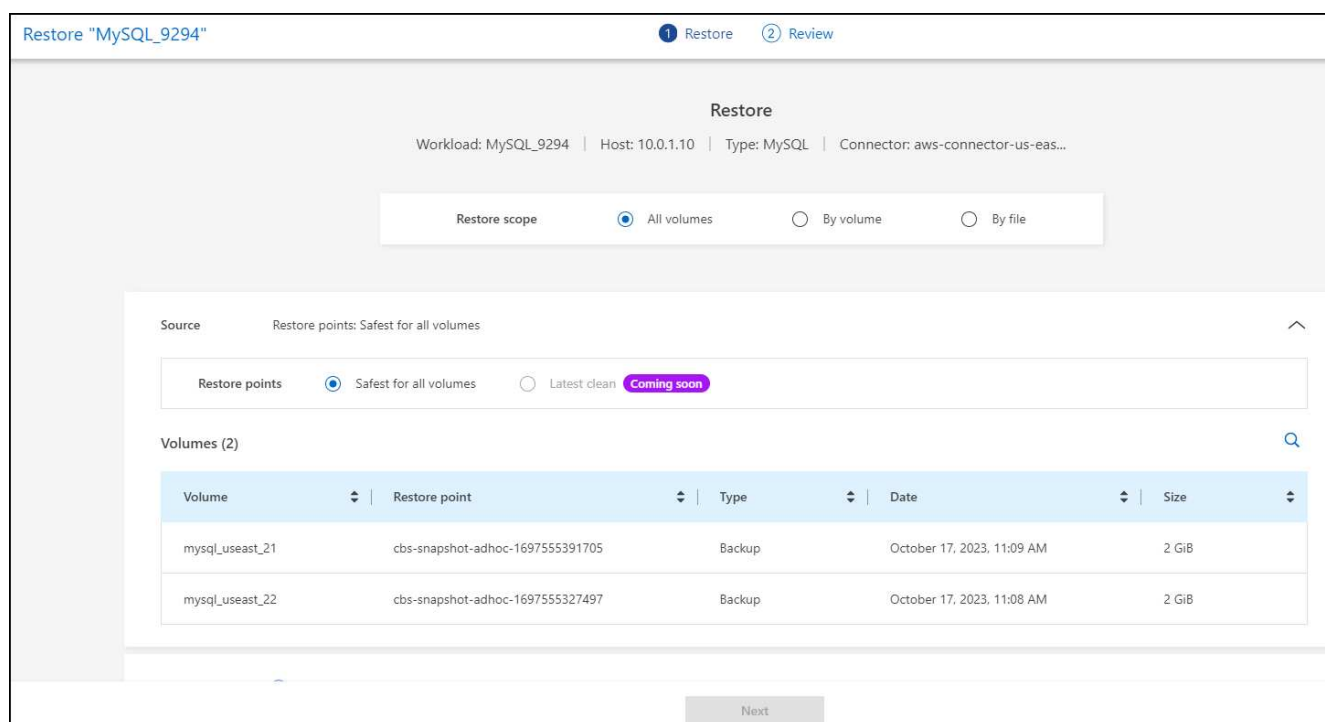


Puede seleccionar hasta 100 archivos o una sola carpeta.

6. Continúe con uno de los siguientes procedimientos, dependiendo de si eligió una aplicación, volumen o archivo.

## Restaura todos los volúmenes

1. En la página Restaurar, en Restore Scope, seleccione **All volumes**.



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



La protección frente al ransomware de BlueXP identifica el mejor punto de restauración como el último backup antes del incidente y muestra una indicación de «el más seguro para todos los volúmenes». Esto significa que todos los volúmenes se restaurarán a una copia antes del primer ataque en el primer volumen detectado.

3. **Destino:** Selecciona la flecha hacia abajo junto a Destino para ver los detalles.
  - a. Seleccione el entorno de trabajo.
  - b. Seleccione la Storage VM.
  - c. Seleccione el agregado.
  - d. Cambie el prefijo del volumen que se antepone a todos los volúmenes nuevos.

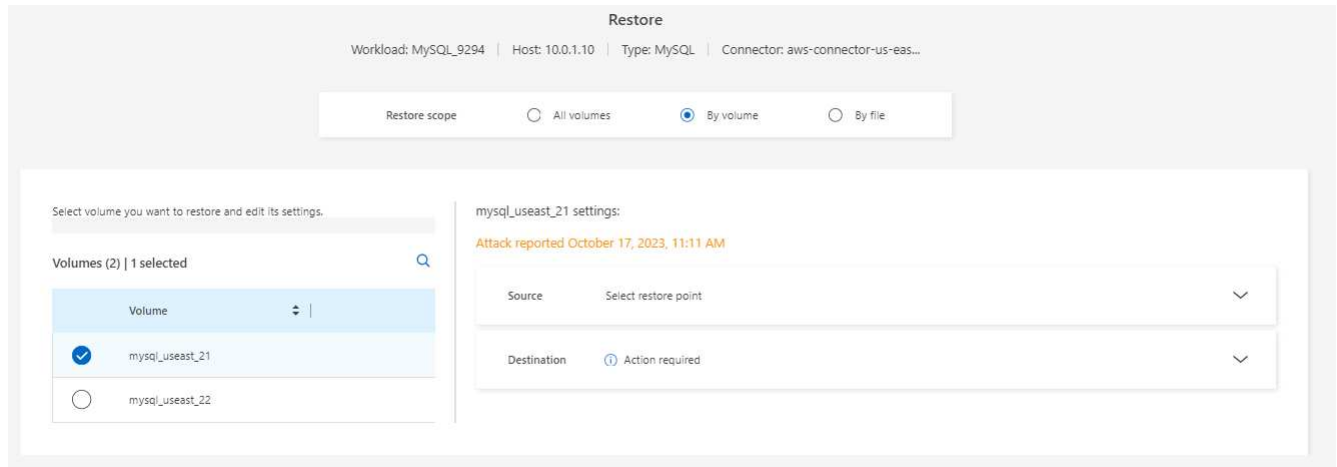


El nombre del volumen nuevo aparece como prefijo + nombre del volumen original + nombre de backup + fecha de backup.

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

## Restaurar una carga de trabajo de la aplicación en el nivel de volumen

1. En la página Restaurar, en Restore Scope, seleccione **by volume**.



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.



La protección frente al ransomware de BlueXP identifica el mejor punto de restauración como el último backup antes del incidente y muestra una indicación «recomendada».

4. **Destino:** Seleccione la flecha hacia abajo junto a Destino para ver los detalles.
  - a. Seleccione el entorno de trabajo.
  - b. Seleccione la Storage VM.
  - c. Seleccione el agregado.
  - d. Revise el nombre del nuevo volumen.



El nombre del volumen nuevo aparece como nombre del volumen original + nombre de backup + fecha de backup.

5. Seleccione **Guardar**.
6. Seleccione **Siguiente**.
7. Revise las selecciones.
8. Seleccione **Restaurar**.
9. En el menú superior, seleccione **Recuperación** para revisar la carga de trabajo en la página de

recuperación donde el estado de la operación se mueve a través de los estados.

## Restaura una carga de trabajo de la aplicación en el nivel de archivo

1. En la página Restaurar, en Restore Scope, seleccione **Por archivo**.
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.



La protección frente al ransomware de BlueXP identifica el mejor punto de restauración como el último backup antes del incidente y muestra una indicación «recomendada».

- b. Seleccione hasta 100 archivos o una sola carpeta para restaurar.
4. **Destino:** Seleccione la flecha hacia abajo junto a Destino para ver los detalles.
    - a. Elija dónde restaurar los datos: Ubicación de origen original o una ubicación alternativa que pueda especificar.



Mientras que los archivos o directorios originales se sobrescribirán con los datos restaurados, los nombres de archivo y carpeta originales seguirán siendo los mismos a menos que especifique nuevos nombres.

- b. Seleccione el entorno de trabajo.
- c. Seleccione la Storage VM.
- d. Si lo desea, introduzca la ruta.

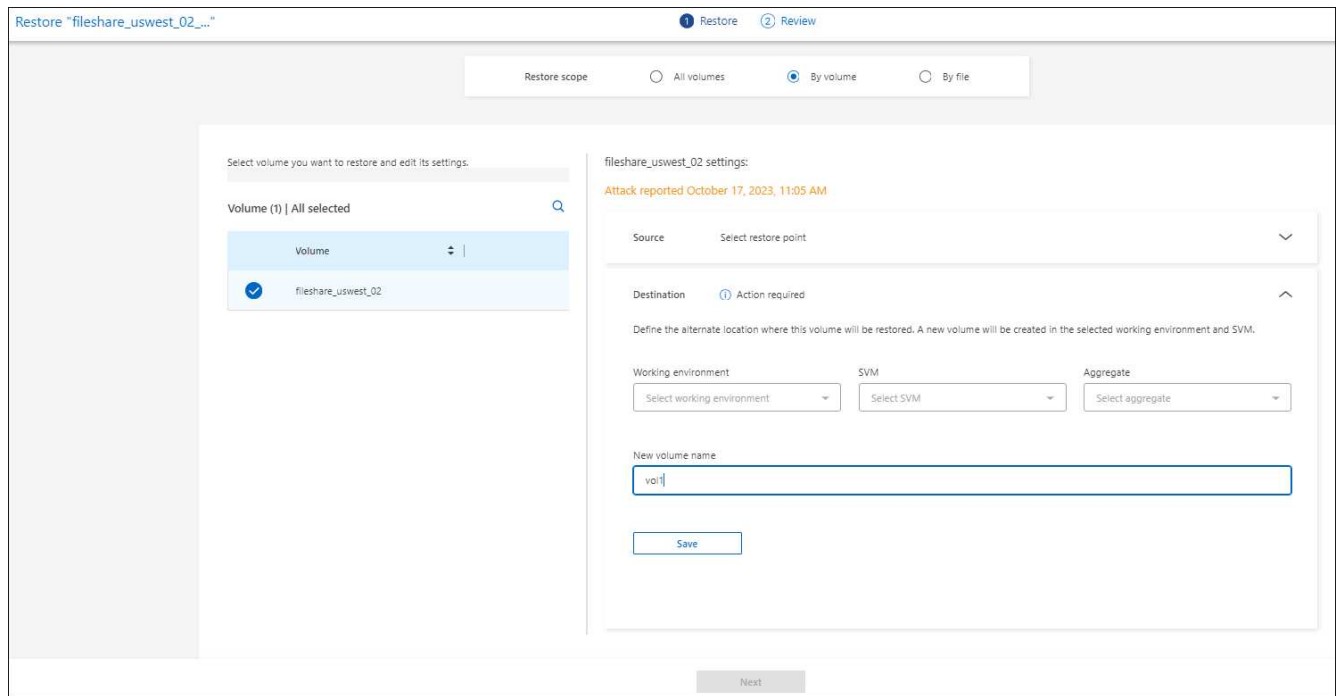


Si no especifica una ruta para la restauración, los archivos se restaurarán en un nuevo volumen en el directorio de nivel superior.

- e. Seleccione si desea que los nombres de los archivos o directorios restaurados sean los mismos que la ubicación actual o nombres diferentes.
5. Seleccione **Guardar**.
  6. Seleccione **Siguiente**.
  7. Revise las selecciones.
  8. Seleccione **Restaurar**.
  9. En el menú superior, seleccione **Recuperación** para revisar la carga de trabajo en la página de recuperación donde el estado de la operación se mueve a través de los estados.

## Restaura un recurso compartido de archivos o un almacén de datos en el nivel de volumen o archivos

1. Después de seleccionar un recurso compartido de archivos o un almacén de datos para restaurar, en la página Restaurar, en Restore Scope, seleccione **by volume** o **by file**.



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.



La protección frente al ransomware de BlueXP identifica el mejor punto de restauración como el último backup antes del incidente y muestra una indicación «recomendada».

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



Mientras que los archivos o directorios originales se sobrescribirán con los datos restaurados, los nombres de archivo y carpeta originales seguirán siendo los mismos a menos que especifique nuevos nombres.

- b. Seleccione el entorno de trabajo.
- c. Seleccione la Storage VM.
- d. Si lo desea, introduzca la ruta.



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

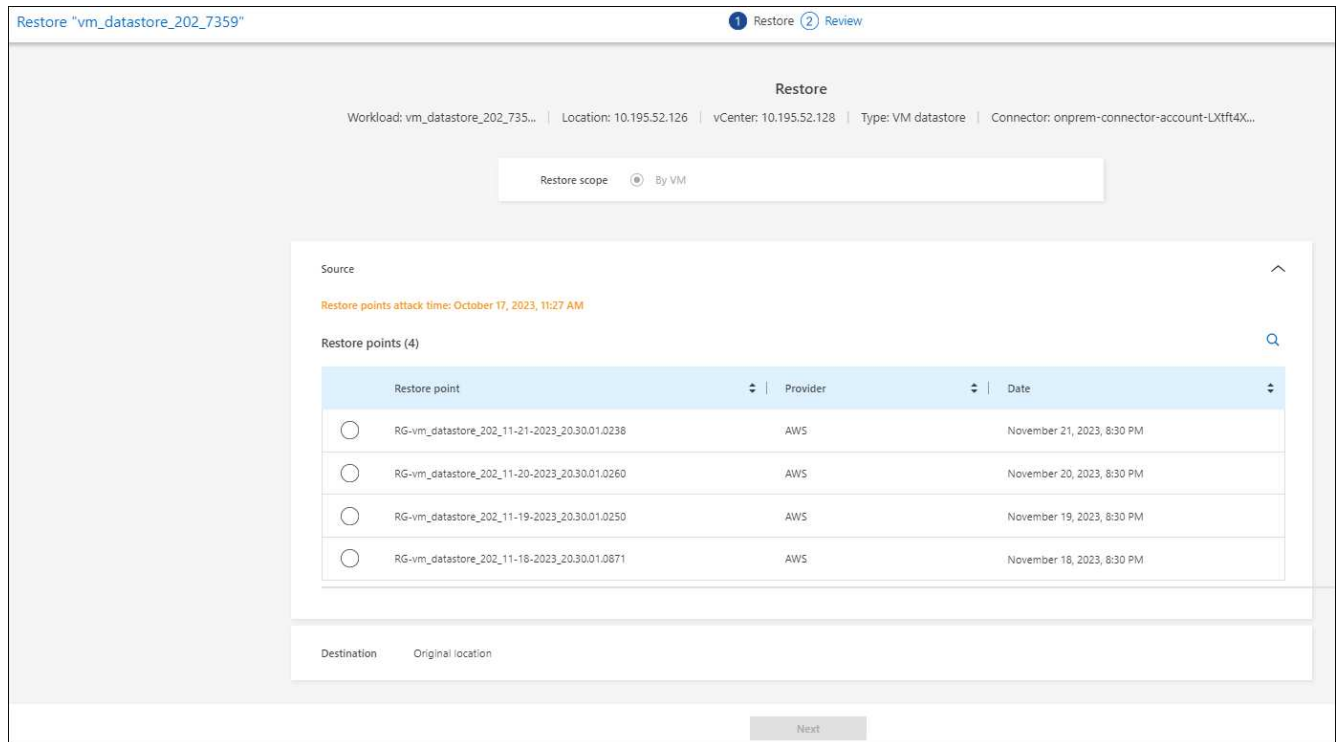
5. Seleccione **Guardar**.
6. Revise las selecciones.
7. Seleccione **Restaurar**.
8. En el menú, seleccione **Recuperación** para revisar la carga de trabajo en la página Recuperación donde el estado de la operación se mueve a través de los estados.



## Restaurar un recurso compartido de archivos de equipo virtual a nivel de máquina virtual

En la página Recovery después de seleccionar una VM para restaurar, continúe con estos pasos.

1. **Fuente:** Selecciona 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 las selecciones.
6. Seleccione **Restaurar**.
7. En 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.

# Conocimiento y apoyo

## Regístrese para recibir soporte

Es necesario registrarse en soporte para recibir soporte técnico específico para BlueXP y sus servicios y soluciones de almacenamiento. También es necesario registrar soporte para habilitar flujos de trabajo clave para los sistemas Cloud Volumes ONTAP.

Al registrarse para recibir soporte, no se habilita el soporte de NetApp para un servicio de archivos de proveedor de cloud. Para obtener soporte técnico relacionado con un servicio de archivos del proveedor de cloud, su infraestructura o cualquier solución que utilice el servicio, consulte «Obtener ayuda» en la documentación de BlueXP para ese producto.

- ["Amazon FSX para ONTAP"](#)
- ["Azure NetApp Files"](#)
- ["Cloud Volumes Service para Google Cloud"](#)

## Información general del registro de soporte

Existen dos formas de registro para activar el derecho de asistencia:

- Registro de la suscripción al soporte de ID de cuenta de BlueXP (número de serie de 20 dígitos xxxx960xxxxx que se encuentra en la página Recursos de asistencia técnica de BlueXP).

Esto sirve como su ID de suscripción de soporte único para cualquier servicio dentro de BlueXP. Debe registrarse cada suscripción de asistencia técnica a nivel de cuenta de BlueXP.

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

Estos números de serie se denominan comúnmente *PAYGO serial Numbers* y son generados por BlueXP en el momento de la implementación de Cloud Volumes ONTAP.

El registro de ambos tipos de números de serie permite funcionalidades, como abrir tickets de soporte y la generación automática de casos. Para completar el registro, añada cuentas del sitio de soporte de NetApp (NSS) a BlueXP, como se describe a continuación.

## Registra tu cuenta de BlueXP para recibir soporte de NetApp

Para registrarte para obtener soporte y activar el soporte, un usuario de tu cuenta de BlueXP debe asociar una cuenta en el sitio de soporte de NetApp a su inicio de sesión en BlueXP. La forma de registrarse para recibir soporte de NetApp depende de si ya tiene una cuenta del sitio de soporte de NetApp (NSS).

### Cliente existente con una cuenta de NSS

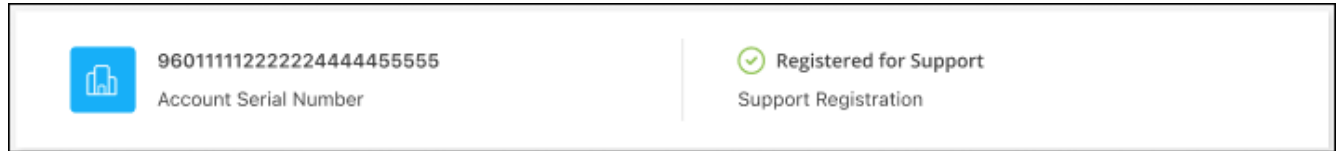
Si es cliente de NetApp con una cuenta de NSS, solo tiene que registrarse para recibir soporte a través de BlueXP.

### Pasos

1. En la parte superior derecha de la consola de BlueXP, seleccione el icono Configuración y seleccione **credenciales**.

2. Seleccione **Credenciales de usuario**.
3. Seleccione **Agregar credenciales NSS** y siga el aviso de autenticación del sitio de soporte de NetApp (NSS).
4. Para confirmar que el proceso de registro se ha realizado correctamente, seleccione el icono Ayuda y seleccione **Soporte**.

La página **Recursos** debe mostrar que su cuenta está registrada para soporte.



Tenga en cuenta que los otros usuarios de BlueXP 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 de BlueXP. Sin embargo, eso no significa que tu cuenta de BlueXP no esté registrada para el soporte técnico. Siempre y cuando un usuario de la cuenta haya seguido estos pasos, su cuenta se ha registrado.

### Cliente existente pero no cuenta NSS

Si eres un cliente existente de NetApp con licencias y números de serie existentes, pero *no* NSS, deberás crear una cuenta NSS y asociarla al inicio de sesión de BlueXP.

#### Pasos

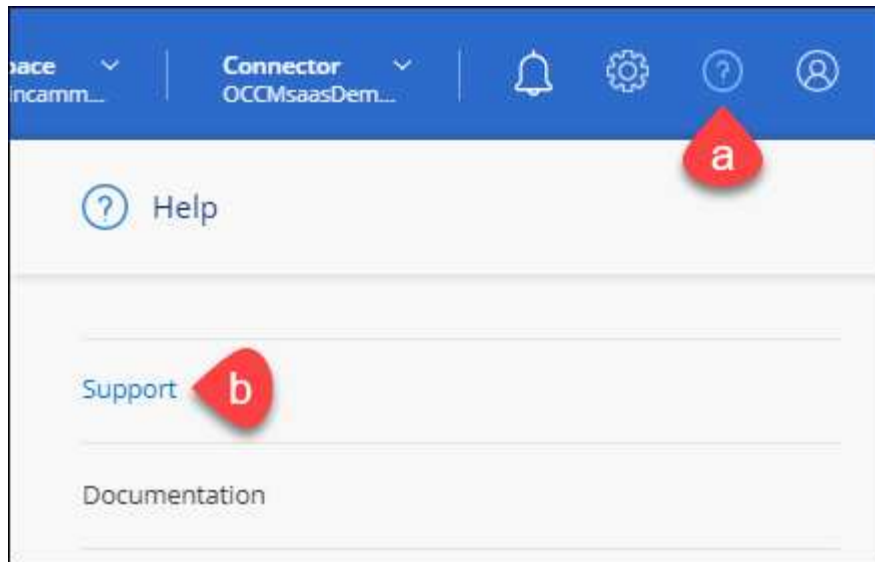
1. Complete el para crear una cuenta en la página de soporte de NetApp "[Formulario de registro de usuarios del sitio de soporte de NetApp](#)"
  - a. Asegúrese de seleccionar el nivel de usuario adecuado, que normalmente es **Cliente/Usuario final de NetApp**.
  - b. Asegúrese de copiar el número de serie de la cuenta BlueXP (960xxxx) utilizado anteriormente para el campo de número de serie. Esto agilizará el procesamiento de la cuenta.
2. Asocia tu nueva cuenta de NSS con tu inicio de sesión de BlueXP. Para ello, sigue los pasos que se muestran en [Cliente existente con una cuenta de NSS](#).

### Totalmente nuevo en NetApp

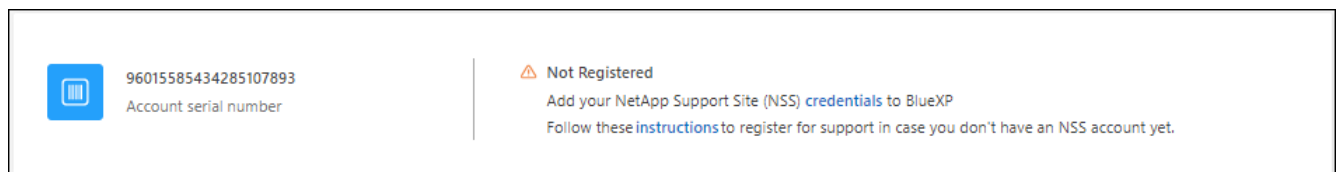
Si es totalmente nuevo en NetApp y no tiene una cuenta de NSS, siga cada paso que se indica a continuación.

#### Pasos

1. En la parte superior derecha de la consola de BlueXP, seleccione el icono Ayuda y seleccione **Soporte**.



2. Busque el número de serie de su ID de cuenta en la página Support Registration.



3. Vaya a. "[Sitio de registro de soporte de NetApp](#)" Y seleccione **no soy un cliente registrado de NetApp**.
4. Rellene los campos obligatorios (aquellos con asteriscos rojos).
5. En el campo **línea de productos**, seleccione **Cloud Manager** y, a continuación, seleccione el proveedor de facturación correspondiente.
6. Copie el número de serie de su cuenta desde el paso 2 anterior, complete la comprobación de seguridad y confirme que ha leído la Política de privacidad de datos global de NetApp.

Se envía inmediatamente un correo electrónico al buzón de correo para finalizar esta transacción segura. Asegúrese de comprobar sus carpetas de spam si el correo electrónico de validación no llega en pocos minutos.

7. Confirme la acción desde el correo electrónico.

Confirmar envía su solicitud a NetApp y recomienda que cree una cuenta en la página de soporte de NetApp.

8. Complete el para crear una cuenta en la página de soporte de NetApp "[Formulario de registro de usuarios del sitio de soporte de NetApp](#)"
  - a. Asegúrese de seleccionar el nivel de usuario adecuado, que normalmente es **Cliente/Usuario final de NetApp**.
  - b. Asegúrese de copiar el número de serie de la cuenta (960xxxx) utilizado anteriormente para el campo de número de serie. Esto agilizará el procesamiento de la cuenta.

### Después de terminar

NetApp debería ponerse en contacto con usted durante este proceso. Este es un ejercicio de incorporación puntual para nuevos usuarios.

Cuando tengas tu cuenta en el sitio de soporte de NetApp, asocia la cuenta con el inicio de sesión de BlueXP siguiendo los pasos que se muestran a continuación [Cliente existente con una cuenta de NSS](#).

## Asocie credenciales de NSS para soporte de Cloud Volumes ONTAP

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

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

Se requiere que proporcione su cuenta de NSS para activar el soporte de su sistema y obtener acceso a los recursos de soporte técnico de NetApp.

- Puesta en marcha de Cloud Volumes ONTAP cuando usted traiga su propia licencia (BYOL)

Es necesario proporcionar su cuenta NSS para que BlueXP pueda cargar su clave de licencia y activar la suscripción para el plazo que adquirió. Esto incluye actualizaciones automáticas para renovaciones de términos.

- Actualizar el software Cloud Volumes ONTAP a la versión más reciente

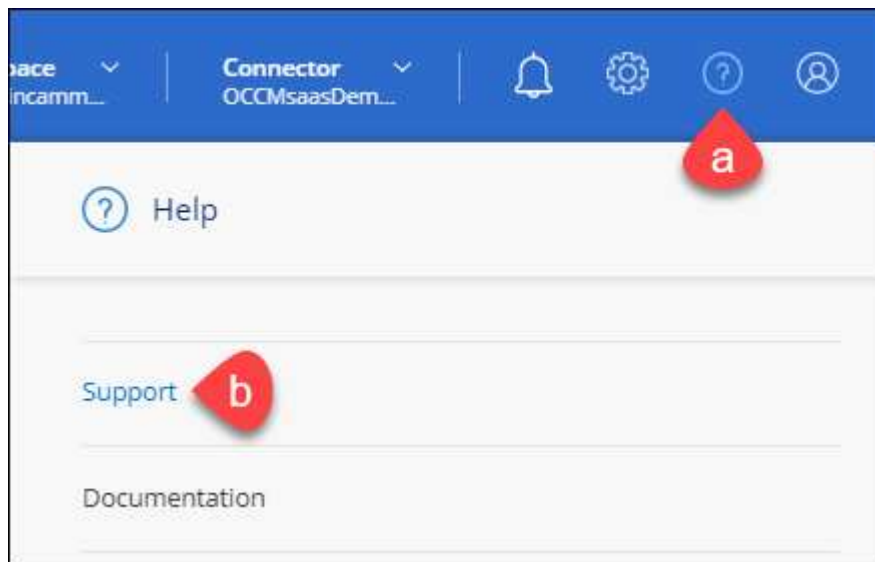
La asociación de credenciales de NSS con su cuenta de BlueXP es diferente de la cuenta de NSS asociada con un inicio de sesión de usuario de BlueXP.

Estas credenciales de NSS están asociadas con tu ID de cuenta de BlueXP específico. Los usuarios que pertenecen a la cuenta BlueXP pueden acceder a estas credenciales desde **Soporte > Gestión NSS**.

- Si tiene una cuenta de nivel de cliente, puede añadir una o varias cuentas de NSS.
- Si tiene una cuenta de partner o distribuidor, puede añadir una o varias cuentas de NSS, pero no se podrán añadir junto con las cuentas de nivel de cliente.

### Pasos

1. En la parte superior derecha de la consola de BlueXP, seleccione el icono Ayuda y seleccione **Soporte**.



2. Seleccione **Administración de NSS > Agregar cuenta de NSS**.
3. Cuando se le solicite, seleccione **continuar** para que se le redirija a una página de inicio de sesión de

Microsoft.

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

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

Estas acciones permiten a BlueXP utilizar 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 de NSS en el nivel del cliente.
- Sólo puede haber una cuenta NSS si esa cuenta es una cuenta de nivel de partner. Si intenta agregar cuentas de NSS de nivel de cliente y existe una cuenta de nivel de partner, obtendrá el siguiente mensaje de error:

"El tipo de cliente NSS no está permitido para esta cuenta, ya que ya hay usuarios NSS de tipo diferente."

Lo mismo sucede si tiene cuentas de NSS de nivel de cliente preexistentes e intenta añadir una cuenta de nivel de partner.

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

Se trata de un ID generado por el sistema que se asigna a su correo electrónico. En la página **NSS Management**, puede mostrar su correo electrónico desde **...** de windows

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

Con esta opción se le solicita que vuelva a iniciar sesión. Tenga en cuenta que el token de estas cuentas caduca después de 90 días. Se enviará una notificación para avisarle de ello.

## Obtenga ayuda

NetApp ofrece soporte para BlueXP y sus servicios cloud de diversas maneras. Hay disponibles amplias opciones de auto soporte gratuito las 24 horas del día, los 7 días de la semana, como artículos de la base de conocimiento (KB) y un foro de la comunidad. Su registro de soporte incluye soporte técnico remoto a través de tickets web.

### Obtenga soporte para un servicio de archivos de proveedores de cloud

Para obtener soporte técnico relacionado con un servicio de archivos del proveedor de cloud, su infraestructura o cualquier solución que utilice el servicio, consulte «Obtener ayuda» en la documentación de BlueXP para ese producto.

- ["Amazon FSX para ONTAP"](#)
- ["Azure NetApp Files"](#)

- ["Cloud Volumes Service para Google Cloud"](#)

Para recibir soporte técnico específico sobre BlueXP y sus soluciones y servicios de almacenamiento, use las opciones de soporte descritas a continuación.

## Utilice opciones de soporte automático

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

- Documentación

La documentación de BlueXP que está viendo actualmente.

- ["Base de conocimientos"](#)

Busque en la base de conocimientos de BlueXP para encontrar artículos útiles para resolver problemas.

- ["Comunidades"](#)

Únase a la comunidad de BlueXP para seguir los debates en curso o crear otros nuevos.

## 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 de.

### Antes de empezar

- Para utilizar la funcionalidad **Crear un caso**, primero debes asociar tus credenciales del sitio de soporte de NetApp con el inicio de sesión de BlueXP. ["Descubre cómo gestionar las credenciales asociadas con tu inicio de sesión de BlueXP"](#).
- Si abre un caso para un sistema ONTAP que tiene un número de serie, su cuenta de NSS deberá estar asociada con el número de serie de ese sistema.

### Pasos

1. En BlueXP, selecciona **Ayuda > Soporte**.
2. En la página **Recursos**, elija una de las opciones disponibles en Soporte técnico:
  - a. Selecciona **Llámanos** si quieres hablar con alguien por teléfono. Se le dirigirá a una página de netapp.com que enumera los números de teléfono a los que puede llamar.
  - b. Selecciona **Crear un caso** para abrir un ticket con un especialista en Soporte NetApp:
    - **Servicio:** Seleccione el servicio con el que está asociado el problema. Por ejemplo, cuando BlueXP es específico de un problema de soporte técnico con flujos de trabajo o funcionalidades dentro del servicio.
    - **Entorno de trabajo:** Si se aplica al almacenamiento, seleccione **Cloud Volumes ONTAP** o **On-Prem** y, a continuación, el entorno de trabajo asociado.

La lista de entornos de trabajo se encuentra dentro del ámbito de la cuenta BlueXP, el área de trabajo y el conector que ha seleccionado en el banner superior del servicio.

- **Prioridad de caso:** Elija la prioridad para el caso, que puede ser Baja, Media, Alta o crítica.

Para obtener más información sobre estas prioridades, pase el ratón sobre el icono de información

situado junto al nombre del campo.

- **Descripción del problema:** Proporcione una descripción detallada del problema, incluidos los mensajes de error aplicables o los pasos de solución de problemas que haya realizado.
- **Direcciones de correo electrónico adicionales:** Introduzca direcciones de correo electrónico adicionales si desea que alguien más conozca este problema.
- **Accesorio (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.

The screenshot shows a web form titled "NetApp Support Site Account" with the user "ntapitdemo". The form contains several sections: "Service" and "Working Environment" are dropdown menus both set to "Select"; "Case Priority" is a dropdown menu set to "Low - General guidance" with an information icon; "Issue Description" is a large text area with the placeholder "Provide detailed description of problem, applicable error messages and troubleshooting steps taken."; "Additional Email Addresses (Optional)" is a text input field with the placeholder "Type here" and an information icon; "Attachment (Optional)" is a file upload area showing "No files selected", an "Upload" button, and a trash icon.

### Después de terminar

Aparecerá una ventana emergente con el número de caso de soporte. Un especialista de soporte de NetApp revisará su caso y le pondrá en contacto con usted próximamente.

Para obtener un historial de sus casos de soporte, puede seleccionar **Ajustes > Línea de tiempo** y buscar acciones denominadas "Crear caso de soporte". Un botón situado en el extremo derecho le permite ampliar la acción para ver los detalles.



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

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

Este error podría significar que la cuenta NSS y la compañía de registro con la que está asociada no es la misma compañía de registro para el número de serie de la cuenta de BlueXP (es decir, 960xxxx) o el número de serie del entorno de trabajo. Puede solicitar ayuda utilizando una de las siguientes opciones:

- Usar el chat en el producto
- Envíe un caso no técnico en <https://mysupport.netapp.com/site/help>

## Gestione sus casos de soporte (vista previa)

Puede ver y gestionar los casos de soporte activos y resueltos directamente desde BlueXP. Es posible gestionar los casos asociados con su cuenta de NSS y con su empresa.

La gestión de casos está disponible como vista previa. Tenemos pensado perfeccionar esta experiencia y añadir mejoras en próximos lanzamientos. Envíenos sus comentarios mediante el chat en el producto.

Tenga en cuenta lo siguiente:

- La consola 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 ha proporcionado.
  - La vista de la derecha muestra el total de casos abiertos en los últimos 3 meses a nivel de su compañía en función de su cuenta NSS de usuario.

Los resultados de la tabla reflejan los casos relacionados con la vista seleccionada.

- Puede agregar o quitar columnas de interés y filtrar el contenido de columnas como prioridad y estado. Otras columnas proporcionan funciones de clasificación.

Consulte los pasos a continuación para obtener más información.

- En el nivel por caso, ofrecemos la posibilidad de actualizar las notas de un caso o cerrar un caso que no esté ya en estado cerrado o pendiente de cierre.

### Pasos

1. En BlueXP, selecciona **Ayuda > Soporte**.
2. Selecciona **Gestión de casos** y, si se te solicita, agrega tu cuenta de NSS a BlueXP.

La página **Administración de casos** muestra casos abiertos relacionados con la cuenta NSS asociada con su cuenta de usuario de BlueXP. Esta es la misma cuenta NSS que aparece en la parte superior de la página **NSS Management**.

3. Si lo desea, puede modificar la información que se muestra en la tabla:
  - En **Casos de la organización**, selecciona **Ver** para ver todos los casos asociados a tu empresa.
  - Modifique el rango de fechas eligiendo un rango de fechas exacto o eligiendo un marco de tiempo diferente.

Search: Cases opened on the last 3 months Create a case

Columns: Date created, Last updated, Status (5)

Filters: Last 7 days, Last 30 days, Last 3 months (selected)

Date created	Last updated	Priority	Status
December 22, 2022	December 29, 2022	Medium (P3)	Assigned
December 21, 2022	December 28, 2022	Medium (P3)	Active
December 15, 2022	December 27, 2022	Medium (P3)	Pending customer
December 14, 2022	December 26, 2022	Low (P4)	Solution proposed


- Filtre el contenido de las columnas.

Search: Cases opened on the last 3 months Create a case

Columns: Last updated, Priority, Status (5)

Filters: Last 7 days, Last 30 days, Last 3 months (selected)

Last updated	Priority	Status
December 29, 2022	Critical (P1)	Active
December 28, 2022	High (P2)	Pending customer
December 27, 2022	Medium (P3)	Solution proposed
December 26, 2022	Low (P4)	Pending closed
		Closed

- Seleccione para cambiar las columnas que aparecen en la tabla  y, a continuación, seleccione las columnas que desea mostrar.

Search: Cases opened on the last 3 months Create a case

Columns: Last updated, Priority, Status (5)

Filters: Last 7 days, Last 30 days, Last 3 months (selected)

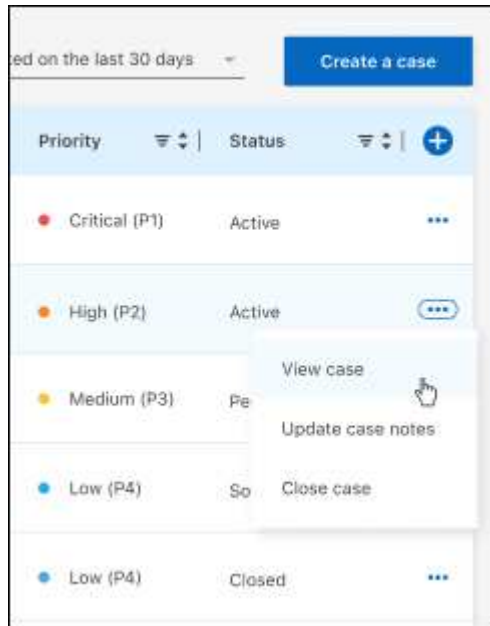
Last updated	Priority	Status
December 29, 2022	Critical (P1)	Last updated
December 28, 2022	High (P2)	Priority
December 27, 2022	Medium (P3)	Cluster name
December 26, 2022	Low (P4)	Case owner
		Opened by

4. Seleccione para gestionar un caso existente ... y seleccione una de las opciones disponibles:

- **Ver caso:** Ver todos los detalles sobre un caso específico.
- **Actualizar notas de 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:** Proporciona detalles sobre por qué estás cerrando el caso y selecciona **Cerrar caso**.



# Avisos legales

Los avisos legales proporcionan acceso a las declaraciones de copyright, marcas comerciales, patentes y mucho más.

## Derechos de autor

["https://www.netapp.com/company/legal/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. Los demás nombres de empresas y productos son marcas comerciales de sus respectivos propietarios.

["https://www.netapp.com/company/legal/trademarks/"](https://www.netapp.com/company/legal/trademarks/)

## Estadounidenses

Puede encontrar una lista actual 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/"](https://www.netapp.com/company/legal/privacy-policy/)

## Código abierto

Los archivos de notificación proporcionan información sobre los derechos de autor y las licencias de terceros que se utilizan en software de NetApp.

- ["Aviso para BlueXP"](#)

## Información de copyright

Copyright © 2024 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPTIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

## Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.