Usa la protección frente al ransomware de BlueXP

BlueXP ransomware protection

NetApp
March 22, 2024

Tabla de contenidos

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.

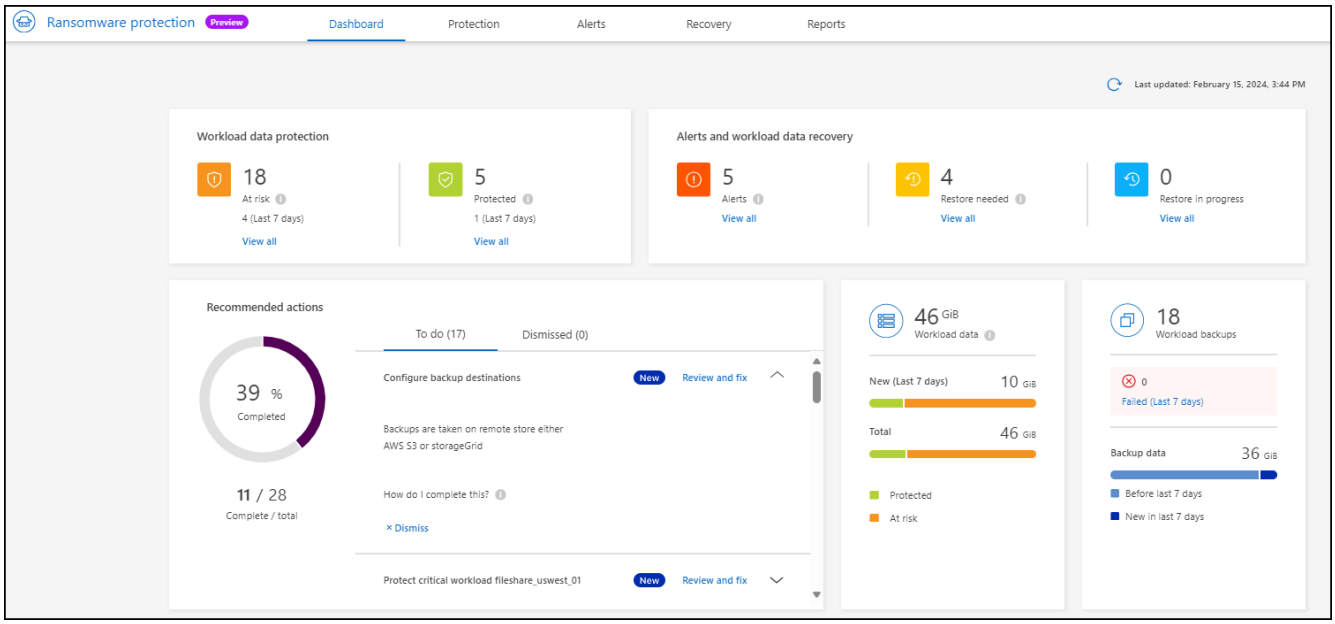
También puede usar la consola para revisar y actuar sobre las recomendaciones de protección.

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 desestimarlo. 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 "Protege las cargas de trabajo contra ataques de ransomware".
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 "Configure las opciones de protección".
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 "Protege las cargas de trabajo contra ataques de ransomware".
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 "Protege las cargas de trabajo contra ataques de ransomware".
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 "Protege las cargas de trabajo contra ataques de ransomware".
Revisar nuevas alertas	Existen nuevas alertas.	Revise las nuevas alertas. Consulte "Responder a una alerta de ransomware detectada".

Pasos

1. 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.

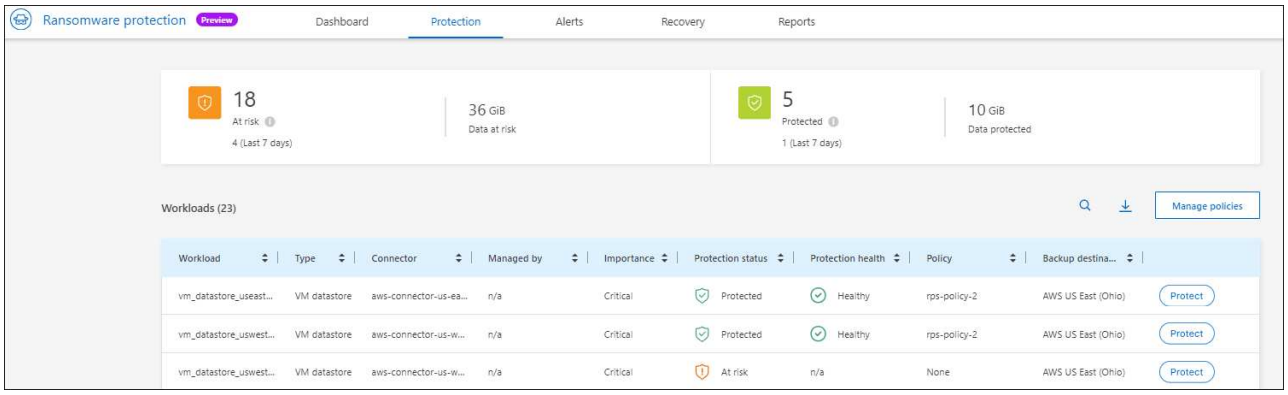
Mira la protección contra ransomware de las cargas de trabajo

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:

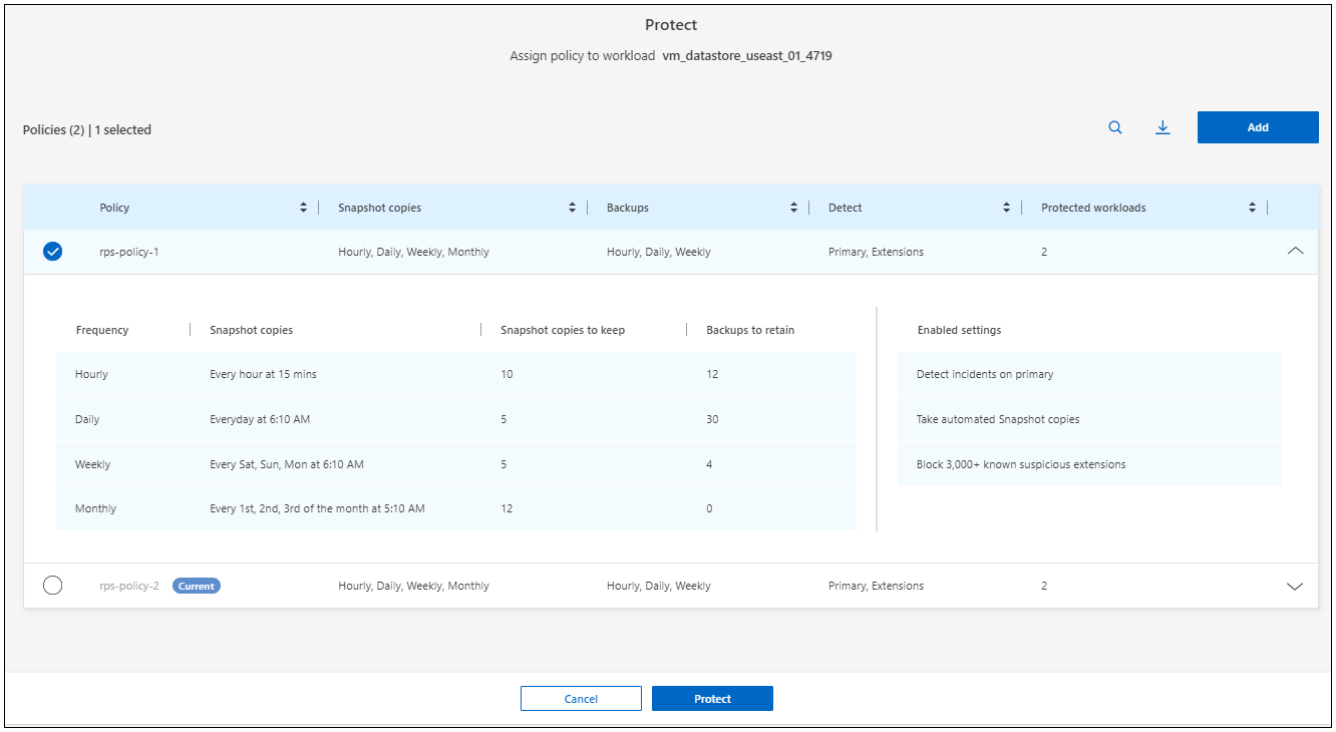
Nivel de política	Snapshot	Frecuencia	Retención (días)	N.o de copias Snapshot	Número máximo total de copias snapshot
Política de carga de trabajo crítica	Cada trimestre	Cada 15 min	3	288	309
	Todos los días	Cada 1 días	14	14	309
	Semanal	Cada 1 semanas	35	5	309
	Mensual	Cada 30 días	60	2	309

Nivel de política	Snapshot	Frecuencia	Retención (días)	N.o de copias Snapshot	Número máximo total de copias snapshot
Política de carga de trabajo importante	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
Política de carga de trabajo estándar	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

1. 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, selecciona **Protección**.
2. 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

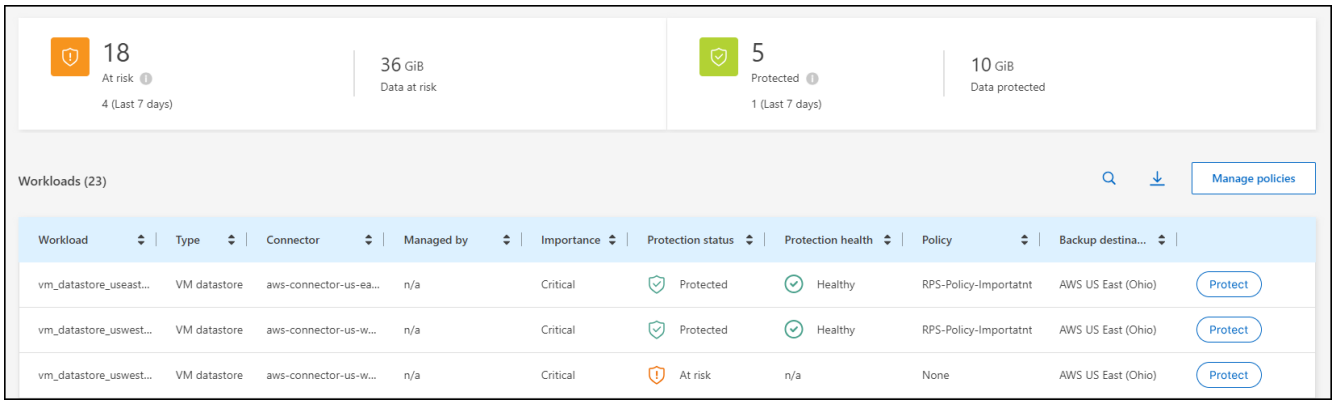
Si las políticas existentes no satisfacen sus necesidades empresariales, puede crear una nueva política de protección. Puede crear su propia política desde cero o utilizar una política existente y modificar su configuración.

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

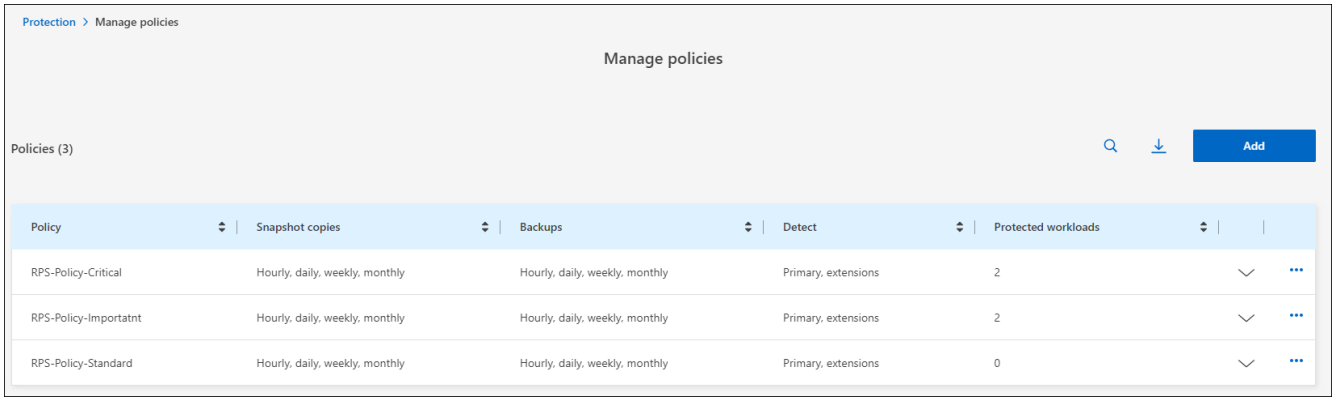
Puede crear una política al gestionarla o durante el proceso de asignación de una política a una carga de trabajo.

Pasos para crear una política durante la gestión de políticas

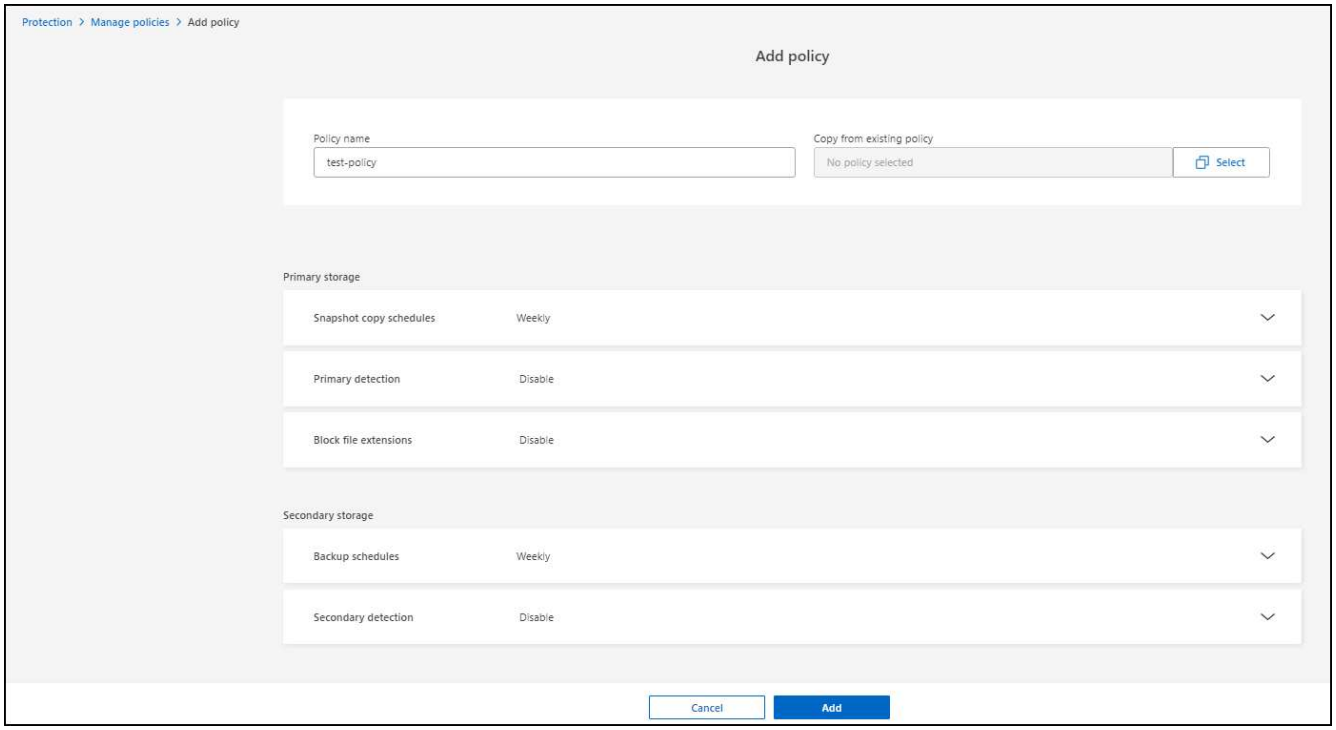
1. En el menú de protección contra ransomware de BlueXP, selecciona **Protección**.



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



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



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.

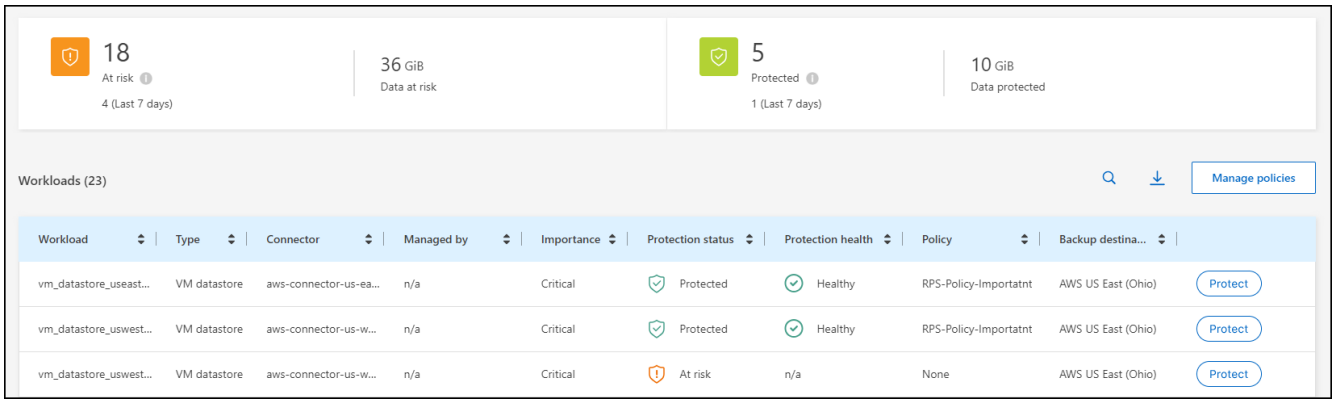
Si decide copiar y modificar una política existente, debe cambiar al menos una configuración para que sea única.

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*.

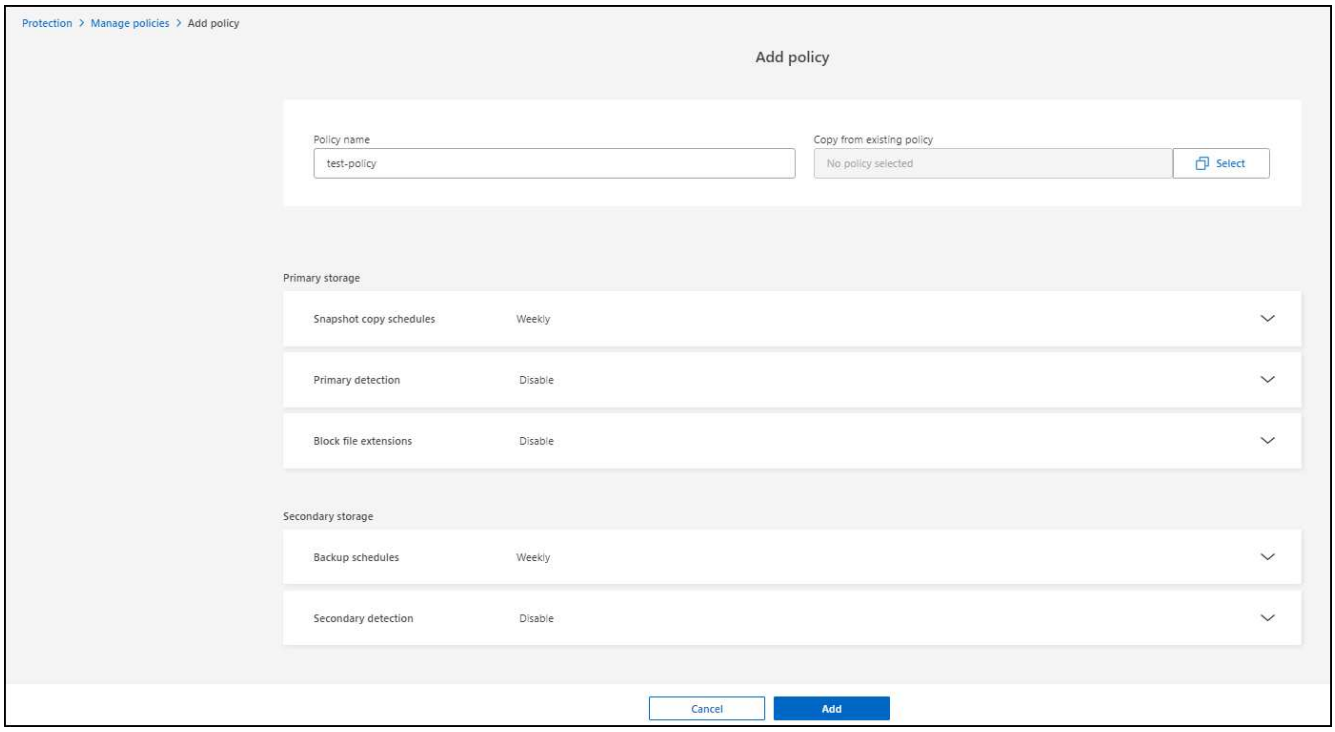
       Esta opción utiliza la tecnología DataLock de NetApp, que bloquea los backups en el almacenamiento secundario. El período de tiempo durante el que el archivo de copia de seguridad está bloqueado (y retenido) se denomina período de retención de DataLock. Se basa en el programa de políticas de backup y 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**.



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



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. Selecciona **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.

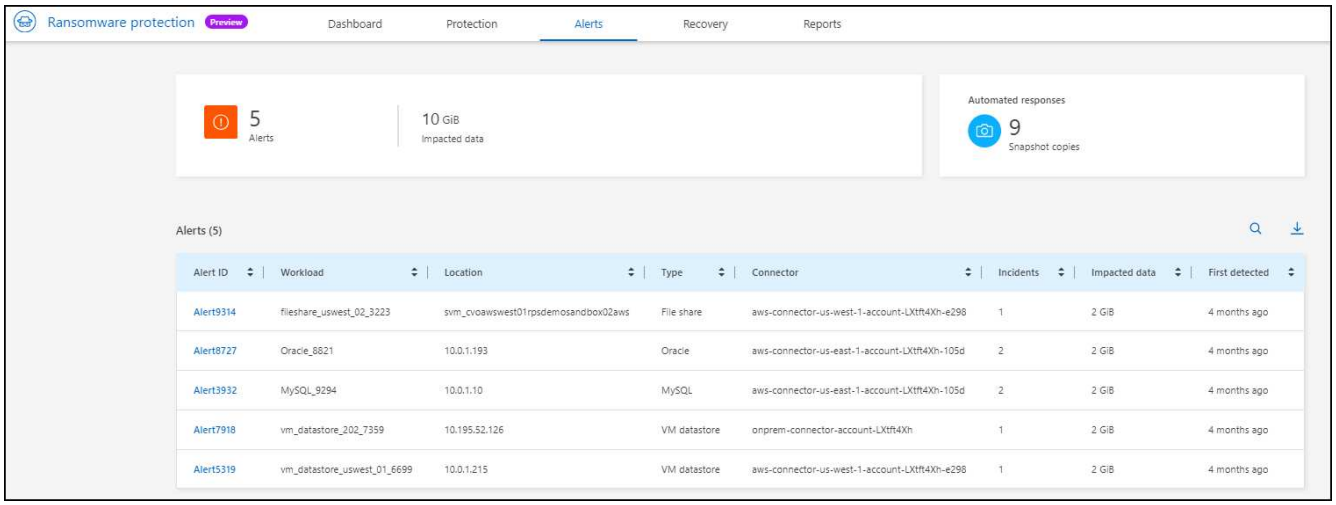
La evidencia se basa en la información de la Protección Autónoma contra el ransomware de ONTAP. Para obtener más información, consulte "Información general sobre la protección de ransomware autónoma".

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.



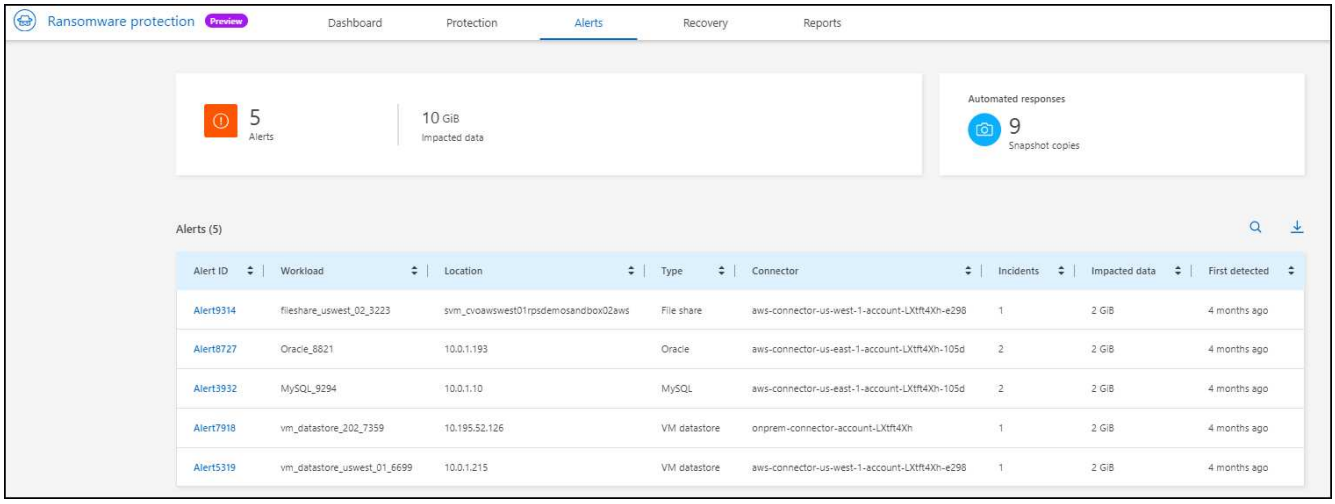
6. Continúe con Marcar los incidentes de ransomware como listos para la recuperación (después de neutralizar los incidentes).

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

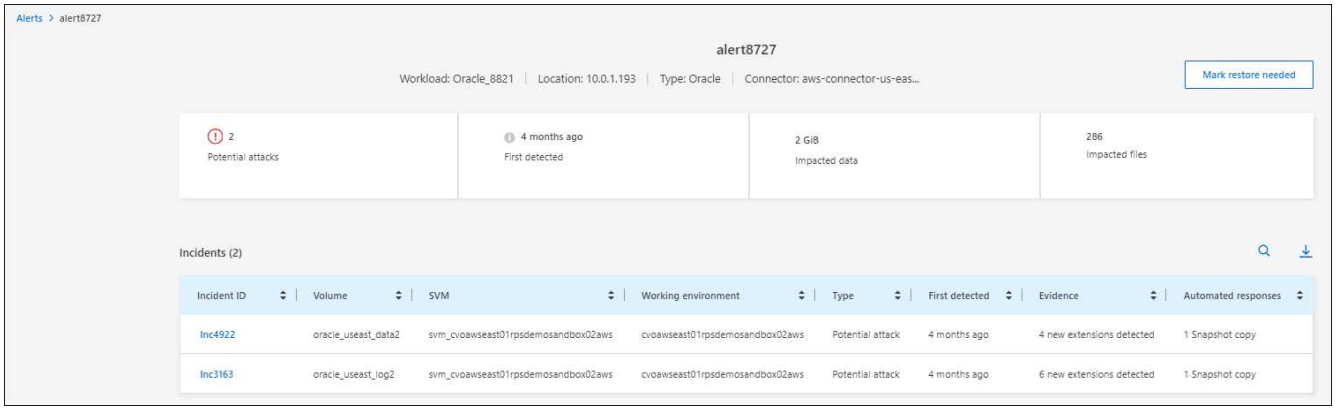
Una vez que haya mitigado el ataque y esté listo para recuperar cargas de trabajo, debe comunicarse con el equipo de administrador de almacenamiento que los datos están listos para la recuperación, de modo que puedan iniciar el proceso de recuperación.

Pasos

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



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



4. Si determina que los incidentes están listos para la recuperación, seleccione **Marcar restauración necesaria**.
5. Confirme la acción y seleccione **Mark restore needed**.
6. 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)

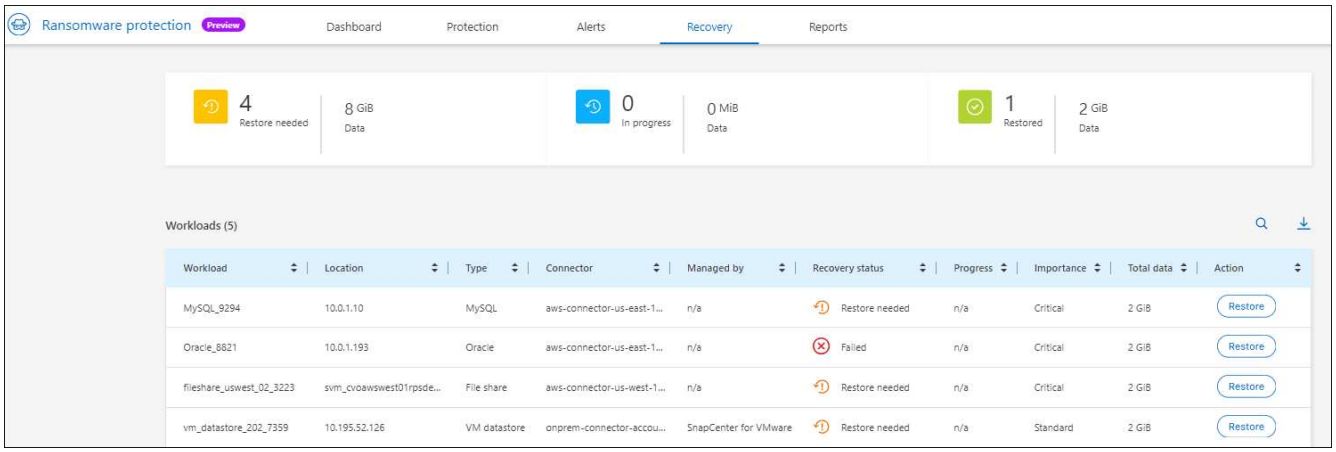
Después de que las cargas de trabajo se hayan marcado como «listas para la recuperación», la protección contra el ransomware de BlueXP recomienda un punto de recuperación real (RPA) y orquesta el flujo de trabajo para una recuperación resistente a los fallos.

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**.



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

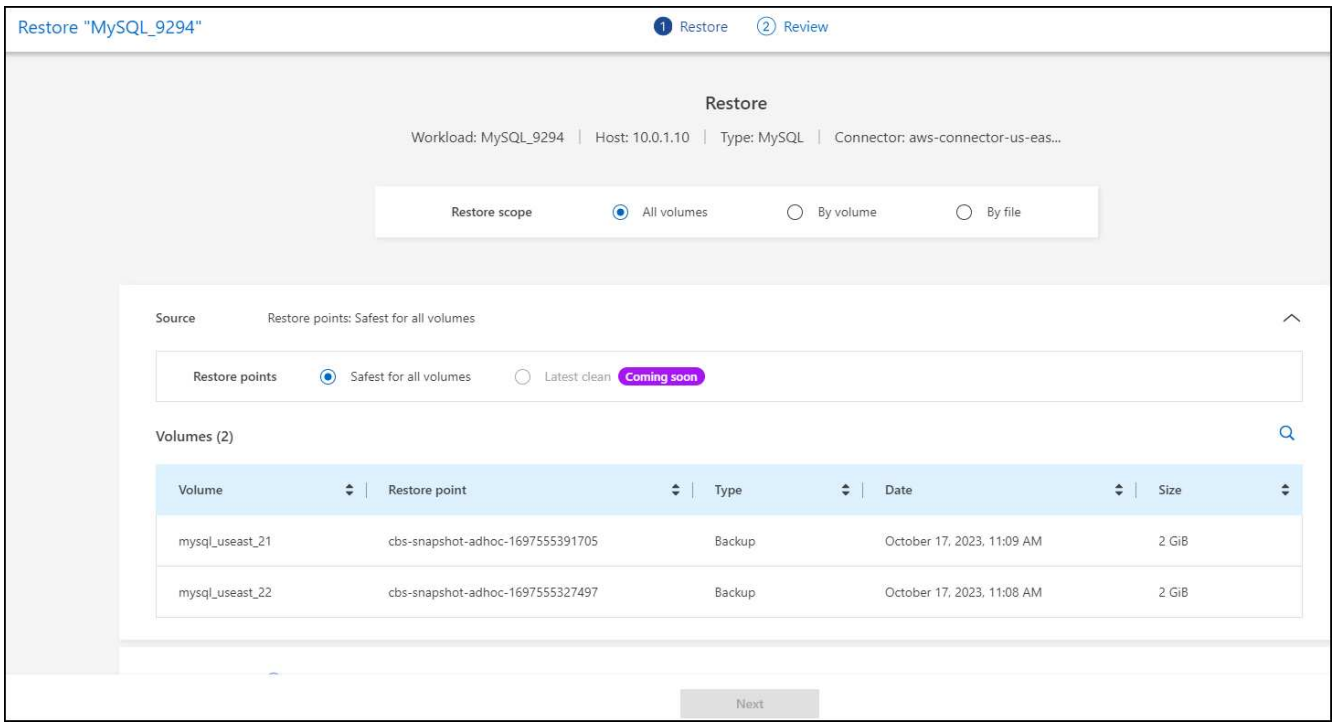
◦ Por archivo: Puede especificar una carpeta o archivos individuales para restaurar.

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.

Restaure 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.

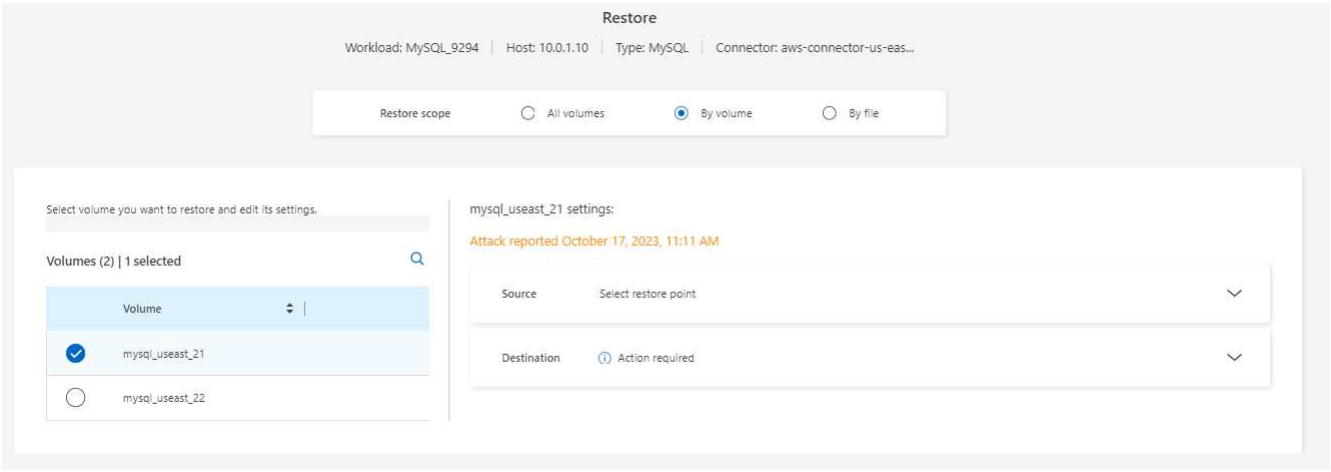
3. **Destino**: Selecciona la flecha hacia abajo junto a Destino para ver los detalles.
   a. Seleccione el entorno de trabajo.
   b. Seleccione la Storage VM.
   c. Seleccione el agregado.
   d. Cambie el prefijo del volumen que se antepondrá a todos los volúmenes nuevos.

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.

Restaure 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**: 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 «recomendada».

4. **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. 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.

Restaure 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**: 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 «recomendada».

   b. Seleccione hasta 100 archivos o una sola carpeta para restaurar.
4. **Destino**: Selecciona 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.

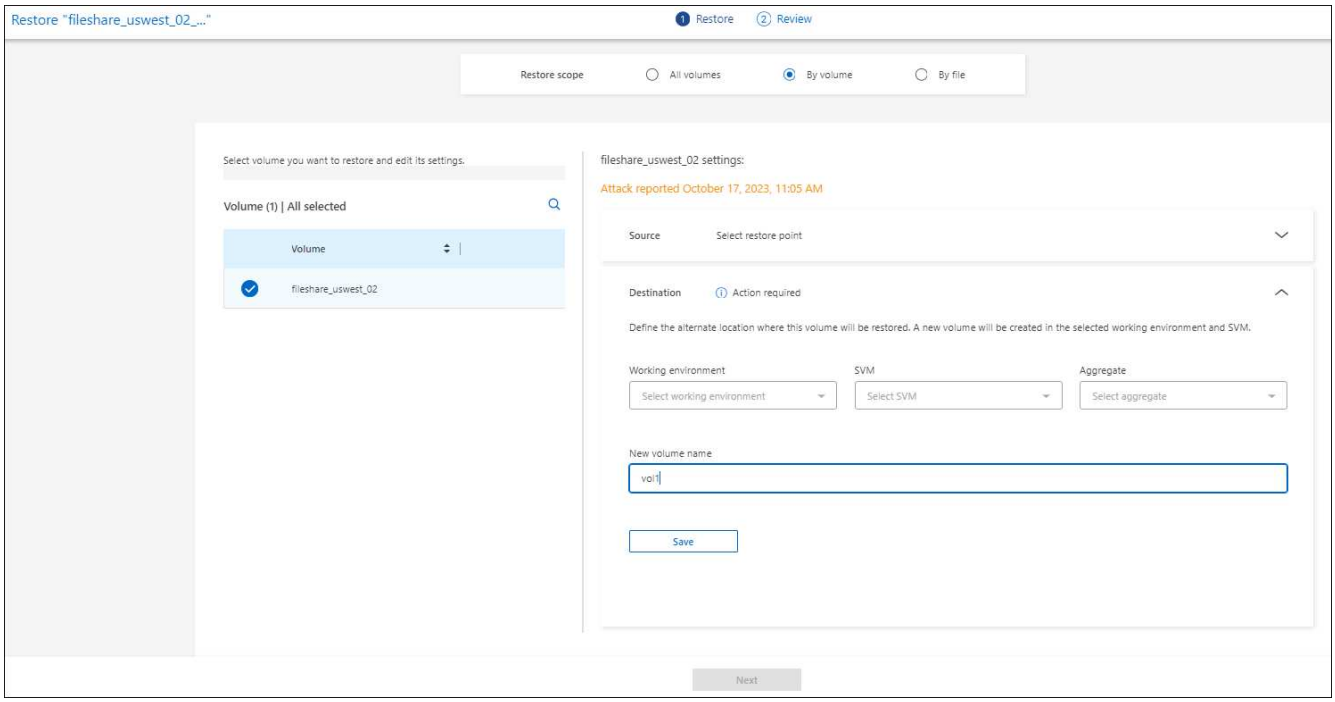
   b. Seleccione el entorno de trabajo.
   c. Seleccione la Storage VM.
   d. Si lo desea, introduzca la ruta.

      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.

Restaure 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**: 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 «recomendada».

4. **Destino**: Selecciona 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.

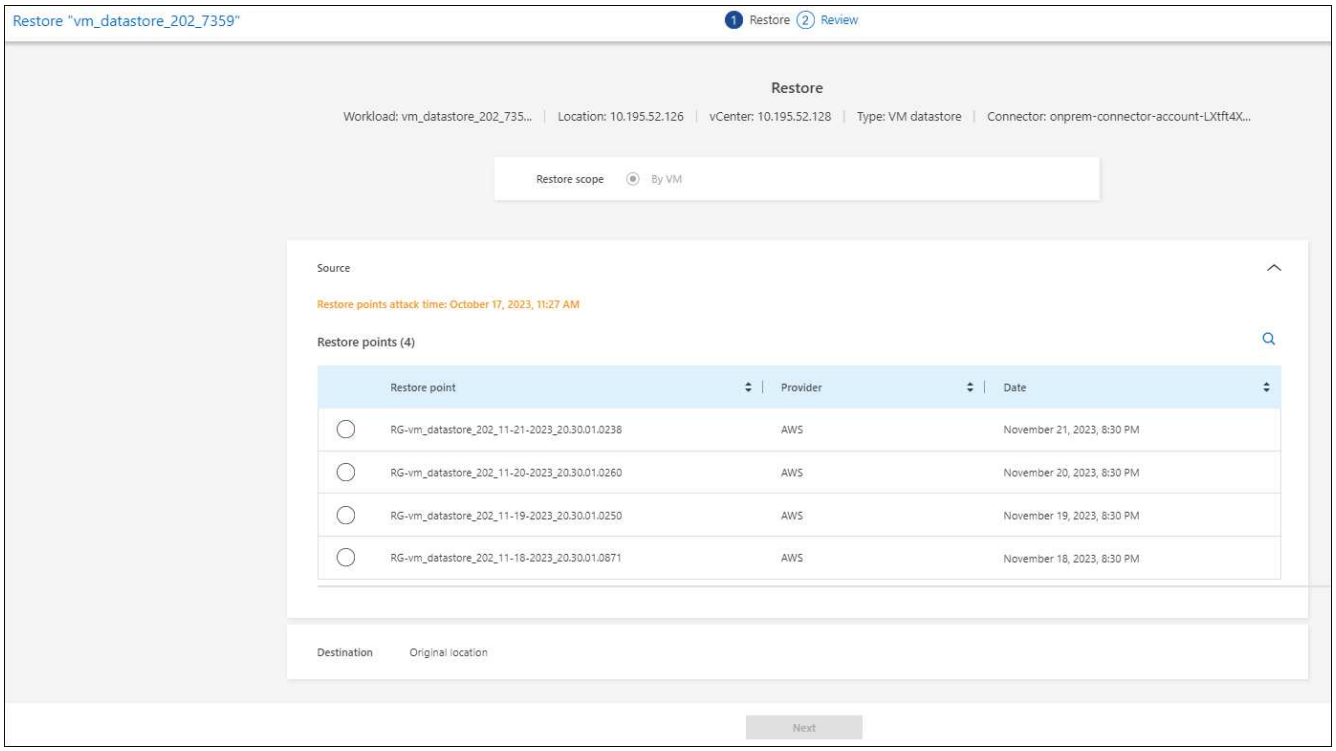
> Si no especifica una ruta para la restauración, los archivos se restaurarán en un nuevo volumen en el directorio de nivel superior.

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.