



# **Realizar backups y restaurar los datos de los equipos virtuales**

BlueXP backup and recovery

NetApp  
April 18, 2024

# Tabla de contenidos

- Realizar backups y restaurar los datos de los equipos virtuales . . . . . 1
  - Proteja los datos de los equipos virtuales . . . . . 1
  - Registre el host del plugin de SnapCenter para VMware vSphere . . . . . 2
  - Crear una política para realizar backups de almacenes de datos . . . . . 3
  - Backup de almacenes de datos en Amazon Web Services . . . . . 4
  - Backup de almacenes de datos en Microsoft Azure . . . . . 5
  - Realizar backups de almacenes de datos en Google Cloud Platform . . . . . 6
  - Realizar backup de almacenes de datos en StorageGRID . . . . . 7
  - Gestionar la protección de datos de almacenes de datos y equipos virtuales . . . . . 7
  - Restaura datos de máquinas virtuales desde el cloud. . . . . 9

# Realizar backups y restaurar los datos de los equipos virtuales

## Proteja los datos de los equipos virtuales

El backup y recuperación de datos de BlueXP para máquinas virtuales ofrece funcionalidades de protección de datos al realizar backups de almacenes de datos y restaurar máquinas virtuales.

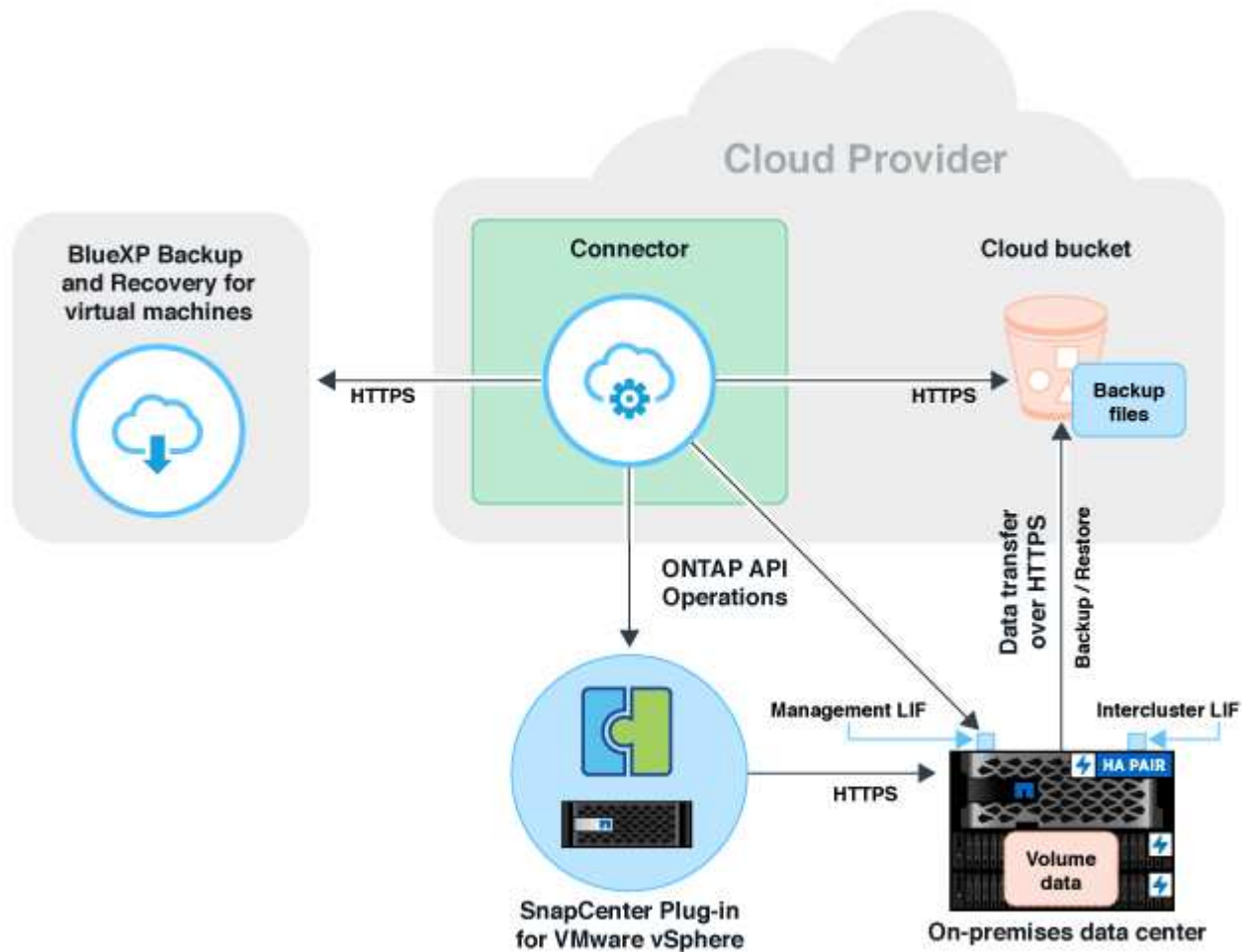
Es posible realizar backups de almacenes de datos en Amazon Web Services S3, Microsoft Azure Blob, Google Cloud Platform y StorageGRID y restaurar máquinas virtuales en el host del plugin de SnapCenter para VMware vSphere en las instalaciones. El backup y recuperación de BlueXP para máquinas virtuales también admite el modelo de puesta en marcha de proxy de conector.

### Antes de empezar

Lea los siguientes requisitos para asegurarse de que tiene una configuración compatible antes de empezar a realizar backups de almacenes de datos y máquinas virtuales en un proveedor de cloud.

- Plugin de SnapCenter para VMware vSphere 4.6P1 o posterior
  - Se debe usar el plugin de SnapCenter para VMware vSphere 4.7P1 o versiones posteriores para realizar backups de almacenes de datos desde el almacenamiento secundario en las instalaciones.
- ONTAP 9.8 o posterior
- BlueXP
- Se admiten almacenes de datos NFS y VMFS. No se admiten vVols.
- Para admitir VMFS, el host del plugin de SnapCenter para VMware vSphere debe ejecutarse en la versión 4,9 o posterior. Asegúrese de realizar un backup del almacén de datos de VMFS si el host del plugin de SnapCenter para VMware vSphere se actualizó de una versión anterior a la versión 4,9.
- Debe haber al menos un backup en el plugin de SnapCenter para VMware vSphere 4.6P1.
- Al menos una política diaria, semanal o mensual en el plugin de SnapCenter para VMware vSphere sin etiqueta ni etiqueta de la política de máquinas virtuales en BlueXP.
- Para la política predefinida, el nivel de programación debe ser el mismo para el almacén de datos del plugin de SnapCenter para VMware vSphere y del cloud.
- Compruebe que no haya volúmenes de FlexGroup en el almacén de datos debido a que no se admiten el backup y la restauración de volúmenes de FlexGroup.
- Desactive "**\_Recent**" en los grupos de recursos necesarios. Si tiene activado "**\_Recent**" para el grupo de recursos, las copias de seguridad de esos grupos de recursos no se pueden utilizar para la protección de datos en la nube y, posteriormente, no se pueden utilizar para la operación de restauración.
- Asegúrese de que el almacén de datos de destino donde se restaurará la máquina virtual tenga espacio suficiente para acomodar una copia de todos los archivos de equipos virtuales, como VMDK, VMX, VMDSX, etc.
- Asegúrese de que el almacén de datos de destino no tenga archivos obsoletos de máquinas virtuales en formato RESTORE\_XXX\_XXXXXX\_FILENAME de los errores anteriores de la operación de restauración. Debe eliminar los archivos obsoletos antes de activar una operación de restauración.
- Para implementar un conector con proxy configurado, asegúrese de que todas las llamadas de conector salientes se enruten a través del servidor proxy.

La siguiente imagen muestra cada componente y las conexiones que necesita preparar entre ellos:



## Registre el host del plugin de SnapCenter para VMware vSphere

Debe registrar el host del plugin de SnapCenter para VMware vSphere en BlueXP para que se muestren los almacenes de datos y las máquinas virtuales. Solo un usuario con acceso administrativo puede registrar el host del plugin de SnapCenter para VMware vSphere.



Puede registrar varios hosts del plugin de SnapCenter para VMware vSphere en BlueXP. Sin embargo, una vez registrado, no es posible quitar el host del plugin de SnapCenter para VMware vSphere.

### Pasos

1. En la interfaz de usuario de BlueXP, haga clic en **Protección > copia de seguridad y recuperación > Máquinas virtuales**.
2. En el menú desplegable **Configuración**, haga clic en **SnapCenter Plug-in for VMware vSphere**.

3. Haga clic en **Registrar el plugin de SnapCenter para VMware vSphere**.
4. Especifique los siguientes detalles:
  - a. En el campo SnapCenter Plug-in for VMware vSphere, especifique la dirección FQDN o IP del host del plugin de SnapCenter para VMware vSphere.
  - b. En el campo Port, especifique el número de puerto en el que ejecuta el host del plugin de SnapCenter para VMware vSphere.  
  
Debe asegurarse de que la comunicación esté abierta entre el host del plugin de SnapCenter para VMware vSphere en las instalaciones que se ejecuta en el puerto 8144 predeterminado y la instancia de conector de BlueXP, que puede estar ejecutándose en cualquier proveedor de cloud (Amazon Web Services, Microsoft Azure, Google Cloud Platform) o en las instalaciones.
  - c. En el campo Username and Password, especifique las credenciales del usuario de vCenter con el rol administrator.
5. Haga clic en **Registrar**.

### Después de terminar

Haga clic en **Backup and recovery > Virtual Machines** para ver todos los almacenes de datos y las máquinas virtuales que están protegidas mediante el host del plugin de SnapCenter registrado para VMware vSphere.

## Crear una política para realizar backups de almacenes de datos

Puede crear una directiva o utilizar una de las siguientes directivas predefinidas que están disponibles en BlueXP.

### Antes de empezar

- Debe crear políticas si no desea editar las políticas predefinidas.
- Para mover backups del almacén de objetos al almacenamiento de archivado, debe ejecutar ONTAP 9.10.1 o una versión posterior y Amazon Web Services o Microsoft Azure debe ser el proveedor de cloud.
- Debe configurar el nivel de acceso de archivado para cada proveedor de cloud.

### Acerca de esta tarea

BlueXP ofrece las siguientes políticas predefinidas:

Nombre de la directiva	Etiqueta	Valor de retención
LTR diario de 1 años (retención a largo plazo)	Todos los días	366
5 años diarios	Todos los días	1830
7 años de SERVICIO semanal	Semanal	370
10 años cada mes LTR	Mensual	120

## Pasos

1. En la página Virtual Machines, en la lista desplegable Settings, seleccione **Policies**.
2. Haga clic en **Crear directiva**.
3. En la sección Policy Details, especifique el nombre de la política.
4. En la sección Retention, seleccione uno de los tipos de retención y especifique la cantidad de backups que desea retener.
5. Seleccione Primary o Secondary como origen de almacenamiento de backup.
6. (Opcional) Si desea mover backups del almacén de objetos al almacenamiento de archivado después de un determinado número de días para la optimización de costes, seleccione la casilla de verificación **Tier backups to Archival** e introduzca el número de días después de los cuales se debe archivar la copia de seguridad.
7. Haga clic en **Crear**.



No es posible editar ni eliminar una política, que está asociada con un almacén de datos.

## Backup de almacenes de datos en Amazon Web Services

Puede realizar backups y archivar uno o varios almacenes de datos en Amazon Web Services para mejorar la eficiencia del almacenamiento y la transición cloud.

Si el almacén de datos está asociado con una política de archivado, tiene la opción de seleccionar el nivel de archivado. Los niveles de archivado admitidos son Glacier y Glacier Deep.

### Antes de empezar

Asegúrese de haber cumplido con todos los "requisitos" antes de realizar backups de almacenes de datos en el cloud.

## Pasos

1. En la interfaz de usuario de BlueXP, haga clic en **Protección > copia de seguridad y recuperación > Máquinas virtuales**.
2. Haga clic en **...** Corresponde al almacén de datos del que desea realizar la copia de seguridad y haga clic en **Activar copia de seguridad**.
3. En la página asignar directiva, seleccione la directiva y haga clic en **Siguiente**.
4. Agregue el entorno de trabajo.

Configura el LIF de gestión de clústeres que quieras que detecte BlueXP. Después de añadir el entorno de trabajo para uno de los almacenes de datos, se puede reutilizar para todos los demás almacenes de datos que residen en el mismo clúster de ONTAP.

- a. Haga clic en **Agregar entorno de trabajo** correspondiente a la SVM.
  - b. En el asistente Agregar entorno de trabajo:
    - i. Especifique la dirección IP de la LIF de gestión del clúster.
    - ii. Especifique las credenciales del usuario del clúster de ONTAP.
  - c. Haga clic en **Agregar entorno de trabajo**.
5. Seleccione **Amazon Web Services** para configurarlo como proveedor de la nube.

- a. Especifique la cuenta de AWS.
- b. En el campo AWS Access Key, especifique la clave para el cifrado de datos.
- c. En el campo AWS Secret Key, especifique la contraseña para el cifrado de datos.
- d. Seleccione la región en la que desea crear los backups.
- e. Especifique las direcciones IP de la LIF de administración del clúster que se han agregado como entornos de trabajo.
- f. Seleccione el nivel de archivado.

Se recomienda definir el nivel de archivado porque se trata de una actividad única y no se puede configurar más tarde.

6. Revise los detalles y haga clic en **Activar copia de seguridad**.

## Backup de almacenes de datos en Microsoft Azure

Puede realizar backups de uno o varios almacenes de datos en Microsoft Azure si integra el host del plugin de SnapCenter para VMware vSphere con BlueXP. Esto ayudará a los administradores de VM a realizar backups y archivar datos de forma rápida y sencilla para lograr la eficiencia del almacenamiento, así como a acelerar la transición al cloud.

Si el almacén de datos está asociado con una política de archivado, se ofrecerá una opción para seleccionar el nivel de archivado. El nivel de archivado compatible es Azure Archive Blob Storage.

### Antes de empezar

Asegúrese de haber cumplido con todos los ["requisitos"](#) antes de realizar backups de almacenes de datos en el cloud.

### Pasos

1. En la interfaz de usuario de BlueXP, haga clic en **Protección > copia de seguridad y recuperación > Máquinas virtuales**.
2. Haga clic en **...** Corresponde al almacén de datos del que desea realizar la copia de seguridad y haga clic en **Activar copia de seguridad**.
3. En la página asignar directiva, seleccione la directiva y haga clic en **Siguiente**.
4. Agregue el entorno de trabajo.

Configura el LIF de gestión de clústeres que quieras que detecte BlueXP. Después de añadir el entorno de trabajo para uno de los almacenes de datos, se puede reutilizar para todos los demás almacenes de datos que residen en el mismo clúster de ONTAP.

- a. Haga clic en **Agregar entorno de trabajo** correspondiente a la SVM.
- b. En el asistente Agregar entorno de trabajo:
  - i. Especifique la dirección IP de la LIF de gestión del clúster.
  - ii. Especifique las credenciales del usuario del clúster de ONTAP.
- c. Haga clic en **Agregar entorno de trabajo**.
5. Seleccione **Microsoft Azure** para configurarlo como proveedor de cloud.

- a. Especifique el ID de suscripción de Azure.
- b. Seleccione la región en la que desea crear los backups.
- c. Crear un grupo de recursos nuevo o utilizar un grupo de recursos existente.
- d. Especifique las direcciones IP de la LIF de administración del clúster que se han agregado como entornos de trabajo.
- e. Seleccione el nivel de archivado.

Se recomienda configurar el nivel de archivado porque se trata de una actividad única y no se le permitirá configurarla más adelante.

6. Revise los detalles y haga clic en **Activar copia de seguridad**.

## Realizar backups de almacenes de datos en Google Cloud Platform

Puede realizar backups de uno o varios almacenes de datos en Google Cloud Platform mediante la integración del host del plugin de SnapCenter para VMware vSphere con BlueXP. Esto ayudará a los administradores de VM a realizar backups y archivar datos de forma rápida y sencilla para lograr la eficiencia del almacenamiento, así como a acelerar la transición al cloud.

### Antes de empezar

Asegúrese de haber cumplido con todos los ["requisitos"](#) antes de realizar backups de almacenes de datos en el cloud.

### Pasos

1. En la interfaz de usuario de BlueXP, haga clic en **Protección > copia de seguridad y recuperación > Máquinas virtuales**.
2. Haga clic en **...** Corresponde al almacén de datos del que desea realizar la copia de seguridad y haga clic en **Activar copia de seguridad**.
3. En la página asignar directiva, seleccione la directiva y haga clic en **Siguiente**.
4. Agregue el entorno de trabajo.

Configura el LIF de gestión de clústeres que quieras que detecte BlueXP. Después de añadir el entorno de trabajo para uno de los almacenes de datos, se puede reutilizar para todos los demás almacenes de datos que residen en el mismo clúster de ONTAP.

- a. Haga clic en **Agregar entorno de trabajo** correspondiente a la SVM.
  - b. En el asistente Agregar entorno de trabajo:
    - i. Especifique la dirección IP de la LIF de gestión del clúster.
    - ii. Especifique las credenciales del usuario del clúster de ONTAP.
  - c. Haga clic en **Agregar entorno de trabajo**.
5. Seleccione **Google Cloud Platform** para configurarlo como proveedor de la nube.
    - a. Seleccione Google Cloud Project en el que desea que se cree el bucket de Google Cloud Storage para los backups.



- b. En el campo Google Cloud Access Key, especifique la clave.
  - c. En el campo Google Cloud Secret Key, especifique la contraseña.
  - d. Seleccione la región en la que desea crear los backups.
  - e. Especifique el espacio de IP.
6. Revise los detalles y haga clic en **Activar copia de seguridad**.

## Realizar backup de almacenes de datos en StorageGRID

Puede realizar backups de uno o varios almacenes de datos en StorageGRID si integra el host del plugin de SnapCenter para VMware vSphere con BlueXP. Esto ayudará a los administradores de VM a realizar backups y archivar datos de forma rápida y sencilla para lograr la eficiencia del almacenamiento, así como a acelerar la transición al cloud.

### Antes de empezar

Asegúrese de haber cumplido con todos los "requisitos" antes de realizar backups de almacenes de datos en el cloud.

### Pasos

1. En la interfaz de usuario de BlueXP, haga clic en **Protección > copia de seguridad y recuperación > Máquinas virtuales**.
2. Haga clic en **...** Corresponde al almacén de datos del que desea realizar la copia de seguridad y haga clic en **Activar copia de seguridad**.
3. En la página asignar directiva, seleccione la directiva y haga clic en **Siguiente**.
4. Agregue el entorno de trabajo.

Configura el LIF de gestión de clústeres que quieras que detecte BlueXP. Después de añadir el entorno de trabajo para uno de los almacenes de datos, se puede reutilizar para todos los demás almacenes de datos que residen en el mismo clúster de ONTAP.

- a. Haga clic en **Agregar entorno de trabajo** correspondiente a la SVM.
  - b. En el asistente Agregar entorno de trabajo:
    - i. Especifique la dirección IP de la LIF de gestión del clúster.
    - ii. Especifique las credenciales del usuario del clúster de ONTAP.
  - c. Haga clic en **Agregar entorno de trabajo**.
5. Seleccione **StorageGRID**.
- a. Especifique la IP del servidor de almacenamiento.
  - b. Seleccione la clave de acceso y la clave secreta.
6. Revise los detalles y haga clic en **Activar copia de seguridad**.

## Gestionar la protección de datos de almacenes de datos y equipos virtuales

Es posible ver políticas, almacenes de datos y máquinas virtuales antes de realizar un backup y restaurar datos. En función de los cambios en la base de datos, políticas o

grupos de recursos, podrás ver las actualizaciones en la interfaz de usuario de BlueXP.

## Ver políticas

Puede ver todas las directivas predefinidas predeterminadas. Para cada una de estas políticas, al ver los detalles, se enumeran todas las políticas y máquinas virtuales asociadas.

1. En la interfaz de usuario de BlueXP, haga clic en **Protección > copia de seguridad y recuperación > Máquinas virtuales**.
2. En el menú desplegable **Configuración**, haga clic en **Directivas**.
3. Haga clic en **Ver detalles** correspondiente a la directiva cuyos detalles desea ver.

Se muestran las políticas y las máquinas virtuales asociadas.

## Ver almacenes de datos y máquinas virtuales

Se muestran los almacenes de datos y las máquinas virtuales que están protegidas mediante el host del plugin de SnapCenter para VMware vSphere registrado.

### Pasos

1. En la interfaz de usuario de BlueXP, haga clic en **Protección > copia de seguridad y recuperación > Máquinas virtuales > Configuración > complemento SnapCenter para VMware vSphere**.
2. Haga clic en el host del plugin de SnapCenter para VMware vSphere para el que desee ver los almacenes de datos y las máquinas virtuales.

## Desproteger los almacenes de datos

Es posible desproteger un almacén de datos que ya estaba protegido anteriormente. Puede anular la protección de un almacén de datos cuando desee eliminar los backups del cloud o ya no quiera hacerlo en el cloud. El almacén de datos puede volver a protegerse una vez que la desprotección se haya realizado correctamente.

### Pasos

1. En la interfaz de usuario de BlueXP, haga clic en **Protección > copia de seguridad y recuperación > Máquinas virtuales**.
2. Haga clic en **...** Correspondiente al almacén de datos que desea desproteger y haga clic en **Desproteger**.

## Edite la instancia del plugin de SnapCenter para VMware vSphere

Puede editar los detalles del host del plugin de SnapCenter para VMware vSphere en BlueXP.

### Pasos

1. En la interfaz de usuario de BlueXP, haga clic en **Protección > copia de seguridad y recuperación > Máquinas virtuales > Configuración > complemento SnapCenter para VMware vSphere**.
2. Haga clic en **...** Y seleccione **Editar**.
3. Modifique los detalles según sea necesario.
4. Haga clic en **Guardar**.

## Actualice los recursos y los backups

Si desea ver los almacenes de datos y los backups más recientes que se han añadido a la aplicación, debe actualizar los recursos y los backups. De este modo, se iniciará la detección de los recursos y backups y se mostrarán los detalles más recientes.

1. Haga clic en **copia de seguridad y recuperación > Máquinas virtuales**.
2. En el menú desplegable **Configuración**, haga clic en **SnapCenter Plug-in for VMware vSphere**.
3. Haga clic en **...** Correspondiente al host del plugin de SnapCenter para VMware vSphere y haga clic en **Refresh Resources and Backups**.

## Actualice la política o el grupo de recursos

Si existe un cambio en la política o el grupo de recursos, debe actualizar la relación de protección.

1. Haga clic en **copia de seguridad y recuperación > Máquinas virtuales**.
2. Haga clic en **...** Correspondiente al almacén de datos y haga clic en **Refresh Protection**.

## Cancele el registro del plugin de SnapCenter para el host de VMware vSphere

Todos los almacenes de datos y máquinas virtuales asociados con el host del plugin de SnapCenter para VMware vSphere estarán desprotegidos.

1. Haga clic en **copia de seguridad y recuperación > Máquinas virtuales**.
2. En el menú desplegable **Configuración**, haga clic en **SnapCenter Plug-in for VMware vSphere**.
3. Haga clic en **...** Correspondiente al host del plugin de SnapCenter para VMware vSphere y haga clic en **Anular registro**.

## Supervisar trabajos

Se crean trabajos para todas las operaciones de backup y recuperación de BlueXP. Puede supervisar todos los trabajos y todas las subtareas que se realizan como parte de cada tarea.

1. Haga clic en **copia de seguridad y recuperación > Supervisión de trabajos**.

Al iniciar una operación, aparece una ventana que indica que el trabajo se ha iniciado. Puede hacer clic en el enlace para supervisar el trabajo.

2. Haga clic en la tarea principal para ver las subtareas y el estado de cada una de estas subtareas.

## Restaure datos de máquinas virtuales desde el cloud

Puede restaurar datos de máquinas virtuales desde el cloud de nuevo al vCenter en las instalaciones. Es posible restaurar el equipo virtual a la misma ubicación exacta desde donde se realizó el backup o a otra ubicación alternativa. Si se realizó el backup del equipo virtual mediante la normativa de archivado, se puede establecer la prioridad de restauración de archivado.



No es posible restaurar máquinas virtuales que abarquen diferentes almacenes de datos.

## Antes de empezar

- Asegúrese de haber cumplido con todos los "requisitos" antes de restaurar máquinas virtuales desde la nube.
- Si va a restaurar a una ubicación alternativa:
  - Asegúrese de que los vCenter de origen y de destino están en modo vinculado.
  - Compruebe que los detalles del clúster de origen y de destino se añadan en BlueXP Canvas y en vCenter en modo vinculado en el host del plugin de SnapCenter para VMware vSphere.
  - Asegúrate de que se agregue el entorno de trabajo (WE) correspondiente a la ubicación alternativa en BlueXP Canvas.

## Pasos

1. En la interfaz de usuario de BlueXP, haga clic en **Protección > Backup y recuperación > Virtual Machines > SnapCenter Plug-in for VMware vSphere** y seleccione el host del complemento de SnapCenter para VMware vSphere.



Si la máquina virtual de origen se mueve a otra ubicación (vMotion) y el usuario activa una restauración de esa máquina virtual desde BlueXP, la máquina virtual se restaura en la ubicación de origen desde donde se realizó el backup.

1. Es posible restaurar la máquina virtual a la ubicación original o a una ubicación alternativa desde el almacén de datos o desde máquinas virtuales:

Si desea restaurar la máquina virtual...	Realice lo siguiente...
a la ubicación original del almacén de datos	<ol style="list-style-type: none"><li>1. Haga clic en <b>...</b> Corresponde al almacén de datos que desea restaurar y haga clic en <b>Ver detalles</b>.</li><li>2. Haga clic en <b>Restaurar</b> correspondiente a la copia de seguridad que desea restaurar.</li><li>3. Seleccione la máquina virtual que desea restaurar desde la copia de seguridad y haga clic en <b>Siguiente</b>.</li><li>4. Asegúrese de que <b>Original</b> está seleccionado y haga clic en <b>Continuar</b>.</li><li>5. Si la máquina virtual está protegida mediante una directiva en la que se configuran los ajustes de archivado, seleccione la opción <b>Prioridad de restauración de archivado</b> y haga clic en <b>Siguiente</b>.  La prioridad de restauración de archivado compatible con Amazon Web Services es alta, estándar y baja, y la prioridad de restauración de archivado compatible con Microsoft Azure es alta y estándar.</li><li>6. Revise los detalles y haga clic en <b>Restaurar</b>.</li></ol>

Si desea restaurar la máquina virtual...	Realice lo siguiente...
a una ubicación alternativa del almacén de datos	<ol style="list-style-type: none"> <li>Haga clic en <b>...</b> Corresponde al almacén de datos que desea restaurar y haga clic en <b>Ver detalles</b>.</li> <li>Haga clic en <b>Restaurar</b> correspondiente a la copia de seguridad que desea restaurar.</li> <li>Seleccione la máquina virtual que desea restaurar desde la copia de seguridad y haga clic en <b>Siguiente</b>.</li> <li>Selecciona <b>Alternativa</b>.</li> <li>Seleccione la opción alternativa de vCenter Server, el host ESXi, el almacén de datos y la red.</li> <li>Proporcione un nombre para la VM después de la restauración y haga clic en <b>Continuar</b>.</li> <li>Si la máquina virtual está protegida mediante una directiva en la que se configuran los ajustes de archivado, seleccione la opción <b>Prioridad de restauración de archivado</b> y haga clic en <b>Siguiente</b>.  La prioridad de restauración de archivado compatible con Amazon Web Services es alta, estándar y baja, y la prioridad de restauración de archivado compatible con Microsoft Azure es alta y estándar.</li> <li>Revise los detalles y haga clic en <b>Restaurar</b>.</li> </ol>
a la ubicación original de las máquinas virtuales	<ol style="list-style-type: none"> <li>Haga clic en <b>...</b> Corresponde a la máquina virtual que desea restaurar y haga clic en <b>Restaurar</b>.</li> <li>Seleccione el backup mediante el cual desea restaurar la máquina virtual.</li> <li>Asegúrese de que <b>Original</b> está seleccionado y haga clic en <b>Continuar</b>.</li> <li>Si la máquina virtual está protegida mediante una directiva en la que se configuran los ajustes de archivado, seleccione la opción <b>Prioridad de restauración de archivado</b> y haga clic en <b>Siguiente</b>.  La prioridad de restauración de archivado compatible con Amazon Web Services es alta, estándar y baja, y la prioridad de restauración de archivado compatible con Microsoft Azure es alta y estándar.</li> <li>Revise los detalles y haga clic en <b>Restaurar</b>.</li> </ol>

Si desea restaurar la máquina virtual...	Realice lo siguiente...
a una ubicación alternativa de las máquinas virtuales	<ol style="list-style-type: none"> <li>1. Haga clic en <b>...</b> Corresponde a la máquina virtual que desea restaurar y haga clic en <b>Restaurar</b>.</li> <li>2. Seleccione el backup mediante el cual desea restaurar la máquina virtual.</li> <li>3. Seleccione <b>Alternativa</b>.</li> <li>4. Seleccione la opción alternativa de vCenter Server, el host ESXi, el almacén de datos y la red.</li> <li>5. Proporcione un nombre para la VM después de la restauración y haga clic en <b>Continuar</b>.</li> <li>6. Si la máquina virtual está protegida mediante una directiva en la que se configuran los ajustes de archivado, seleccione la opción <b>Prioridad de restauración de archivado</b> y haga clic en <b>Siguiente</b>.  La prioridad de restauración de archivado compatible con Amazon Web Services es alta, estándar y baja, y la prioridad de restauración de archivado compatible con Microsoft Azure es alta y estándar.</li> <li>7. Revise los detalles y haga clic en <b>Restaurar</b>.</li> </ol>

## 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 INTERRUPCIÓN 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.