Realice backups y restauraciones de datos de aplicaciones en las instalaciones

BlueXP backup and recovery

NetApp
October 09, 2024

Tabla de contenidos

Realice backups y restauraciones de datos de aplicaciones en las instalaciones

Proteja los datos de las aplicaciones locales

El backup y recuperación de datos de BlueXP para aplicaciones proporciona funcionalidades de protección de datos para copias Snapshot consistentes con aplicaciones de ONTAP principal en las instalaciones al proveedor de cloud.

También puede realizar backups de Oracle, Microsoft SQL, SAP HANA, MongoDB, MySQL, además, datos de aplicaciones PostgreSQL de sistemas ONTAP en las instalaciones hasta Amazon Web Services, Microsoft Azure, Google Cloud Platform y StorageGRID.

Si desea más información sobre el backup y la recuperación de datos de BlueXP para aplicaciones, consulte:

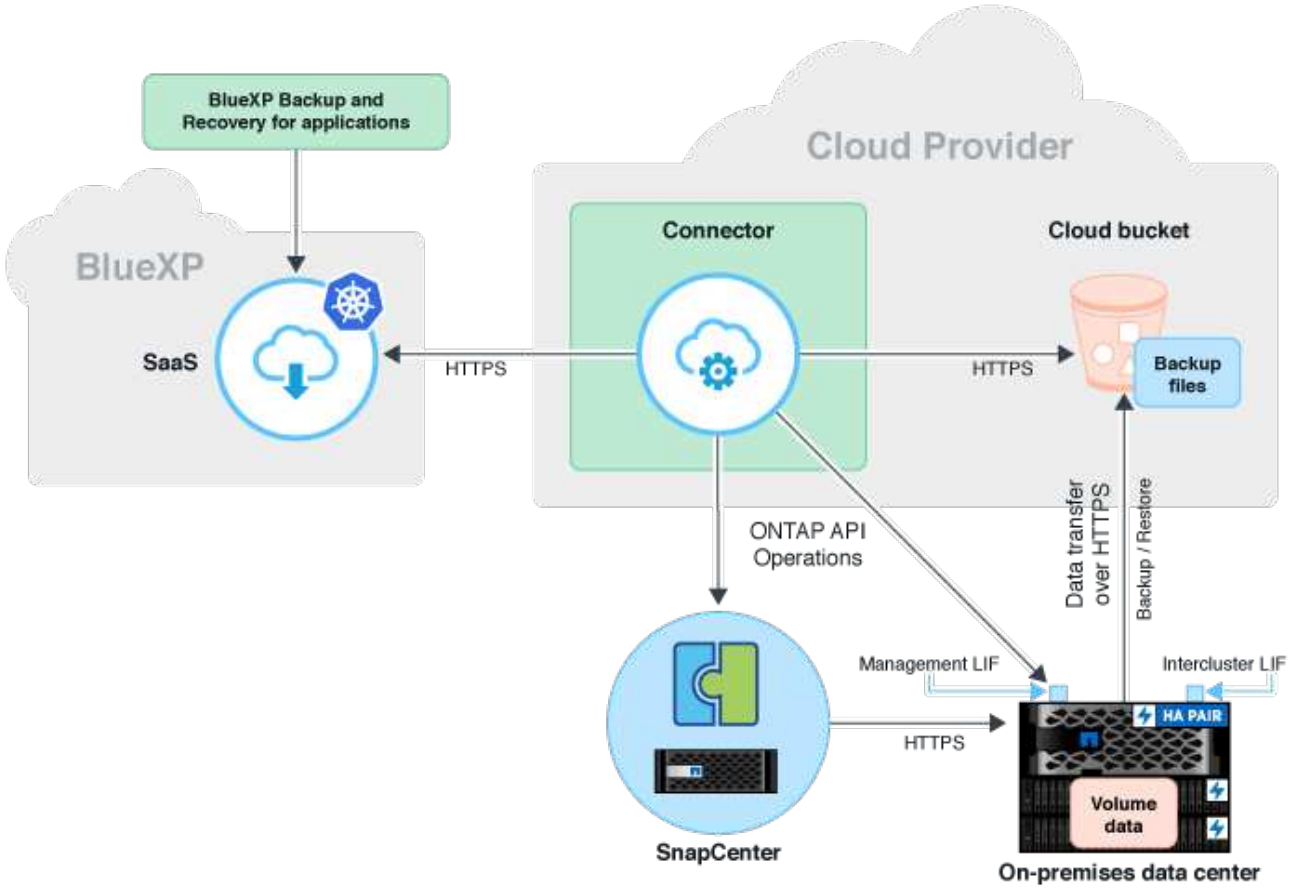
- "Backup para aplicaciones con backup y recuperación de datos de BlueXP y SnapCenter"
- "Podcast de backup y recuperación de datos de BlueXP para aplicaciones"

Requisitos

Lea los siguientes requisitos para asegurarse de que tiene una configuración compatible antes de empezar a realizar el backup de los datos de la aplicación en el proveedor de cloud.

- ONTAP 9.8 o posterior
- BlueXP
- SnapCenter Server 4,6 o posterior
  - Debe utilizar SnapCenter Server 4,7 o posterior si desea utilizar las siguientes funciones:
    - Proteja los backups del almacenamiento secundario en las instalaciones
    - Proteja las aplicaciones SAP HANA
    - Proteja las aplicaciones de Oracle y SQL que se encuentran en el entorno VMware
    - Exportación de almacenamiento de una copia de seguridad
    - Desactivar las copias de seguridad
    - Cancele el registro del servidor SnapCenter
  - Debe utilizar SnapCenter Server 4,9 o posterior si desea utilizar las siguientes funciones:
    - Montar los backups de base de datos de Oracle
    - Restaure al almacenamiento alternativo
  - Debe utilizar el servidor de SnapCenter 4.9P1 si desea proteger aplicaciones MongoDB, MySQL y PostgreSQL
- Debe haber al menos un backup por aplicación disponible en SnapCenter Server
- Al menos una política diaria, semanal o mensual en SnapCenter sin etiqueta ni misma etiqueta que la de la política en BlueXP

En la siguiente imagen se muestra cada componente al realizar backups en cloud y las conexiones que necesita preparar entre ellos:



Registre el servidor SnapCenter

Solo un usuario con el rol de administrador de SnapCenter puede registrar el host en el que se ejecuta SnapCenter Server 4.6 o una versión posterior. Puedes registrar varios hosts de servidor de SnapCenter en BlueXP.

Pasos

1. En la interfaz de usuario de BlueXP, haga clic en **Protección** > **copia de seguridad y recuperación** > **aplicaciones**.
2. En el menú desplegable **Configuración**, haga clic en **servidores SnapCenter**.
3. Haga clic en **Registrar servidor SnapCenter**.
4. Especifique los siguientes detalles:
   a. En el campo servidor SnapCenter, especifique el FQDN o la dirección IP del host SnapCenter Server.
   b. En el campo Puerto, especifique el número de puerto en el que se está ejecutando el host del servidor SnapCenter.

      Debe asegurarse de que el puerto está abierto para que se produzca la comunicación entre SnapCenter Server y BlueXP.

   c. En el campo Etiquetas, especifique un nombre de sitio, un nombre de ciudad o cualquier nombre personalizado con el que desee etiquetar el servidor SnapCenter.

Las etiquetas están separadas por comas.

d. En el campo Username and Password, especifique las credenciales del usuario con el rol SnapCenterAdmin.

5. Seleccione el conector en la lista desplegable **Connector**.
6. Haga clic en **Registrar**.

Después de terminar

Haga clic en **copia de seguridad y restauración** > **aplicaciones** para ver todas las aplicaciones protegidas con el host de servidor SnapCenter registrado. De forma predeterminada, las aplicaciones se detectan automáticamente cada día, a medianoche.

Las aplicaciones admitidas y sus configuraciones son:

- Base de datos de Oracle:
  - Backups completos (datos + registro) creados con al menos una programación diaria, semanal o mensual
  - SAN, NFS, VMDK-SAN, VMDK-NFS Y RDM
- Base de datos Microsoft SQL Server:
  - Independientes, instancias de clústeres de conmutación por error y grupos de disponibilidad
  - Backups completos creados con al menos un programa diario, semanal o mensual
  - SAN, VMDK-SAN, VMDK-NFS Y RDM
- Base de datos SAP HANA:
  - Contenedor único 1.x
  - Contenedor de base de datos múltiple 2.x.
  - Replicación de sistemas HANA (HSR)

    Debe tener al menos un backup en las ubicaciones primaria y secundaria. Puede decidir realizar un error proactivo o una conmutación por error diferida al secundario.

  - Recursos de volúmenes sin datos (NDV), como los binarios de HANA, el volumen de registro de archivos de HANA, el volumen compartido de HANA, etc.
- MongoDB
- MySQL
- PostgreSQL

No se muestran las siguientes bases de datos:

- Bases de datos que no tienen backups
- Bases de datos que solo tienen políticas bajo demanda o por hora
- Bases de datos de Oracle que residen en NVMe

Crear una política para realizar backups de aplicaciones

Debe crear una política para realizar un backup de los datos de la aplicación en el cloud.

Antes de empezar

- Si desea mover backups del almacén de objetos al almacenamiento de archivado, asegúrese de utilizar la versión de ONTAP requerida.
  - Si utiliza Amazon Web Services, debe usar ONTAP 9.10.1 o una versión posterior
  - Si utiliza Microsoft Azure, debe usar ONTAP 9.10.1 o una versión posterior
  - Si utiliza Google Cloud, debería utilizar ONTAP 9.12.1 o una versión posterior
  - Si utiliza StorageGRID, debe usar ONTAP 9.12.1 o una versión posterior
- Debe configurar el nivel de acceso de archivado para cada proveedor de cloud.

Pasos

1. En la interfaz de usuario de BlueXP, haga clic en **Protección** > **copia de seguridad y recuperación** > **aplicaciones**.
2. En el menú desplegable Configuración, haga clic en **Directivas** > **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 copias de seguridad 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 **copias de seguridad de nivel a archivado**.
7. Haga clic en **Crear**.

No se puede editar ni eliminar una directiva asociada a una aplicación.

Realice backup de los datos de las aplicaciones en las instalaciones en Amazon Web Services

Complete algunos pasos para hacer una copia de seguridad de los datos de las aplicaciones desde ONTAP en Amazon Web Services.

BlueXP admite el bloqueo de datos y la protección frente al ransomware. Si el clúster de ONTAP se ejecuta en ONTAP 9.11.1 o una versión posterior y no ha configurado almacenamiento de archivado, puede proteger los backups frente a amenazas de sobrescritura, eliminación y ransomware.

Pasos

1. En la interfaz de usuario de BlueXP, haga clic en **Protección** > **copia de seguridad y recuperación** > **aplicaciones**.
2. Haga clic en ••• Corresponde a la aplicación 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. Tras agregar el entorno de trabajo para una de las aplicaciones, se puede reutilizar para todas las demás aplicaciones que residen en el mismo clúster de ONTAP.

a. Seleccione la SVM y haga clic en **Agregar entorno de trabajo**.
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.

   El backup y la recuperación de BlueXP solo admiten el administrador de clústeres.

c. Haga clic en **Agregar entorno de trabajo**.

5. Seleccione **Amazon Web Services** como proveedor de la nube.
   a. Especifique la cuenta de AWS.
   b. En el campo AWS Access Key, especifique la clave.
   c. En el campo AWS Secret Key, especifique la contraseña.
   d. Seleccione la región en la que desea crear los backups.
   e. Especifique el espacio de IP.
   f. Seleccione el nivel de archivado si ha configurado el almacenamiento de archivado en la política.

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

6. Configurar el bloqueo de datos y la protección frente al ransomware.
7. Revise los detalles y haga clic en **Activar copia de seguridad**.

Realice backups de los datos de las aplicaciones en las instalaciones en Microsoft Azure

Completa unos pasos para hacer un backup de los datos de las aplicaciones desde ONTAP en Microsoft Azure.

BlueXP admite el bloqueo de datos y la protección frente al ransomware. Si el clúster de ONTAP se ejecuta en ONTAP 9.12.1 o una versión posterior y no ha configurado almacenamiento de archivado, puede proteger los backups frente a amenazas de sobrescritura, eliminación y ransomware.

Pasos

1. En la interfaz de usuario de BlueXP, haga clic en **Protección** > **copia de seguridad y recuperación** > **aplicaciones**.
2. Haga clic en ••• Corresponde a la aplicación 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. Tras agregar el entorno de trabajo para una de las aplicaciones, se puede reutilizar para todas las demás aplicaciones que residen en el mismo clúster de ONTAP.

   a. Seleccione la SVM y haga clic en **Agregar entorno de trabajo**.
   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.

El backup y la recuperación de BlueXP solo admiten el administrador de clústeres.

c. Haga clic en **Agregar entorno de trabajo**.

5. Seleccione **Microsoft Azure** como proveedor de cloud.
   a. Especifique el ID de suscripción de Azure.
   b. Seleccione la región en la que desea crear los backups.
   c. Cree un grupo de recursos nuevo o utilice un grupo de recursos existente.
   d. Especifique el espacio de IP.
   e. Seleccione el nivel de archivado si ha configurado el almacenamiento de archivado en la política.

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

6. Configurar el bloqueo de datos y la protección frente al ransomware.
7. Revise los detalles y haga clic en **Activar copia de seguridad**.

Realice backups de los datos de las aplicaciones en las instalaciones en Google Cloud Platform

Completa algunos pasos para hacer una copia de seguridad de los datos de las aplicaciones desde ONTAP en Google Cloud Platform.

Pasos

1. En la interfaz de usuario de BlueXP, haga clic en **Protección** > **copia de seguridad y recuperación** > **aplicaciones**.
2. Haga clic en ••• Corresponde a la aplicación 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. Tras agregar el entorno de trabajo para una de las aplicaciones, se puede reutilizar para todas las demás aplicaciones que residen en el mismo clúster de ONTAP.

   a. Seleccione la SVM y haga clic en **Agregar entorno de trabajo**.
   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.

      El backup y la recuperación de BlueXP solo admiten el administrador de clústeres.

   c. Haga clic en **Agregar entorno de trabajo**.
5. Seleccione **Google Cloud Platform** como proveedor de cloud.

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.
f. 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**.

Realice backups de los datos de las aplicaciones en las instalaciones en StorageGRID

Complete unos pasos para hacer un backup de los datos de las aplicaciones desde ONTAP en StorageGRID.

BlueXP admite el bloqueo de datos y la protección frente al ransomware. Si el clúster de ONTAP se ejecuta en ONTAP 9.11.1 o una versión posterior, los sistemas StorageGRID abarcan la versión 11.6.0.3 o posterior y si no ha configurado almacenamiento de archivado, puede proteger los backups contra la sobrescritura, la eliminación y las amenazas de ransomware.

Antes de empezar

Al realizar una copia de seguridad de datos en StorageGRID, debe haber un conector disponible en las instalaciones. Tendrá que instalar un conector nuevo o asegurarse de que el conector seleccionado actualmente reside en las instalaciones. El conector se puede instalar en un sitio con o sin acceso a Internet.

Para obtener más información, consulte "Crear conectores para StorageGRID".

Pasos

1. En la interfaz de usuario de BlueXP, haga clic en **Protección** > **copia de seguridad y recuperación** > **aplicaciones**.
2. Haga clic en ••• Corresponde a la aplicación 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. Tras agregar el entorno de trabajo para una de las aplicaciones, se puede reutilizar para todas las demás aplicaciones que residen en el mismo clúster de ONTAP.

   a. Seleccione la SVM y haga clic en **Agregar entorno de trabajo**.
   b. En el asistente Agregar entorno de trabajo:
      i. Especifique la dirección IP de la LIF de gestión de clúster.
      ii. Especifique las credenciales del usuario del clúster de ONTAP.

      El backup y la recuperación de BlueXP solo admiten el administrador de clústeres.

c. Haga clic en **Agregar entorno de trabajo**.

5. Seleccione **StorageGRID**.
   a. Especifique el FQDN del servidor StorageGRID y el puerto en el que se está ejecutando el servidor StorageGRID.

      Introduzca los detalles en el formato FQDN:PORT.

   b. En el campo Access Key, especifique la clave.
   c. En el campo Secret Key, especifique la contraseña.
   d. Especifique el espacio de IP.
   e. Especifique el nivel de archivado si ha configurado el almacenamiento de archivado en la política.

Si selecciona…	Realice lo siguiente…
AWS	i. Seleccione la dirección StorageGRID de la lista desplegable o añada el clúster de StorageGRID. ii. Especifique la cuenta de AWS. iii. En el campo AWS Access Key, especifique la clave. iv. En el campo AWS Secret Key, especifique la contraseña. v. Seleccione la región en la que desea crear los backups. vi. Haga clic en **Guardar**.
Azure	i. Seleccione el clúster de StorageGRID en la lista desplegable o añada el clúster. ii. Especifique el ID de suscripción de Azure. iii. Seleccione la región en la que desea crear los backups. iv. Cree un grupo de recursos nuevo o utilice un grupo de recursos existente. v. Haga clic en **Guardar**.

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

6. Configurar el bloqueo de datos y la protección frente al ransomware.
7. Revise los detalles y haga clic en **Activar copia de seguridad**.

Gestione la protección de aplicaciones

Puedes gestionar la protección de aplicaciones consultando políticas, viendo backups, consultando los cambios en el diseño de la base de datos, las políticas y los grupos de

recursos, y supervisando todas las operaciones desde la interfaz de usuario de BlueXP.

Ver políticas

Puede ver todas las políticas. Para cada una de estas políticas, al ver los detalles, se muestran todas las aplicaciones asociadas.

Pasos

1. Haga clic en **copia de seguridad y recuperación** > **aplicaciones**.
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 aplicaciones asociadas.

   No se puede editar ni eliminar una directiva asociada a una aplicación.

También puede ver políticas de SnapCenter ampliadas para la nube, ejecutando el `Get-SmResources` Cmdlet en SnapCenter.
La información sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando el nombre del comando Get-Help.

Ver backups en el cloud

Puede ver los backups en la nube en la interfaz de usuario de BlueXP.

Pasos

1. Haga clic en **copia de seguridad y recuperación** > **aplicaciones**.
2. Haga clic en ••• Corresponde a la aplicación y haga clic en **Ver detalles**.

   El tiempo que se tardará en incluir los backups depende de la programación de replicación predeterminada de ONTAP.

- Para bases de datos de Oracle, tanto los backups de datos como de registros, se muestra el número de cambio de sistema (SCN) para cada backup, fecha de finalización de cada backup. Es posible seleccionar solamente el backup de datos y restaurar la base de datos a la ubicación original. Es posible montar el backup de datos y el backup de registro en una ubicación alternativa.
- Para las bases de datos de Microsoft SQL Server, solo se muestran los backups completos y la fecha de finalización de cada backup. Es posible seleccionar el backup y restaurar la base de datos a la ubicación original o alternativa.
- Para la instancia de Microsoft SQL Server, se muestran los backups de las bases de datos en esa instancia.
- Para las bases de datos SAP HANA, solo se muestran los backups de datos y la fecha de finalización de cada backup. Puede seleccionar el backup y realizar la exportación de almacenamiento en un determinado host.
- Para MongoDB, MySQL y PostgreSQL, solo se muestran los backups de datos y la fecha de finalización de cada backup. Puede seleccionar el backup y realizar la exportación de almacenamiento en un determinado host.

Los backups creados antes de habilitar la protección cloud no se enumeran para la restauración.

También puede ver estos backups ejecutando el `Get-SmBackup` Cmdlet en SnapCenter.
La información sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando el nombre del comando Get-Help.

Desactivar copia de seguridad

Es posible eliminar todos los backups que se mueven al almacén de objetos tanto de SnapCenter como del almacén de objetos.

Pasos

1. Haga clic en **copia de seguridad y recuperación** > **aplicaciones**.
2. Haga clic en ••• Correspondiente a la aplicación y haga clic en Desactivar copia de seguridad.

   De forma predeterminada, la casilla de comprobación está seleccionada y elimina todos los backups que se mueven al almacén de objetos tanto de SnapCenter como del almacén de objetos.

   Si desactiva la casilla de comprobación, los backups se conservan solo en el almacén de objetos, pero esos backups no se pueden utilizar para la restauración a nivel de la aplicación. Más tarde, cuando active el backup para esta aplicación, los backups que retienen en el almacén de objetos no aparecen para restaurar.

3. Haga clic en **Desactivar copia de seguridad**.

Cambio del diseño de la base de datos

Cuando se añaden volúmenes a la base de datos, el servidor de SnapCenter etiqueta las snapshots de los volúmenes nuevos automáticamente según la política y la programación. Estos volúmenes nuevos no tendrán el extremo de almacén de objetos y debe actualizar los volúmenes ejecutando los siguientes pasos:

Pasos

1. Haga clic en **copia de seguridad y recuperación** > **aplicaciones**.
2. En el menú desplegable **Configuración**, haga clic en **servidores SnapCenter**.
3. Haga clic en ••• Corresponde al servidor SnapCenter que aloja la aplicación y haga clic en **Actualizar**.

   Se detectan los volúmenes nuevos.

4. Haga clic en ••• Correspondiente a la aplicación y haga clic en **Actualizar protección** para activar la protección en nube para el nuevo volumen.
   - Si se añade un volumen de almacenamiento a la aplicación después de configurar el proveedor de cloud, SnapCenter Server etiquetará las snapshots para nuevos backups en los que reside la aplicación.
   - Debe eliminar manualmente la relación de almacén de objetos si ninguna otra aplicación utiliza el volumen eliminado.
   - Si actualiza el inventario de aplicaciones, este contendrá la distribución de almacenamiento actual de la aplicación.

Cambio de política o grupo de recursos

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

Pasos

1. Haga clic en **copia de seguridad y recuperación** > **aplicaciones**.
2. Haga clic en ••• Corresponde a la aplicación y haga clic en **Actualizar protección**.

Cancele el registro del servidor SnapCenter

Pasos

1. Haga clic en **copia de seguridad y recuperación** > **aplicaciones**.
2. En el menú desplegable **Configuración**, haga clic en **servidores SnapCenter**.
3. Haga clic en ••• Corresponde al servidor SnapCenter y haga clic en **Unregister**.

   De forma predeterminada, la casilla de comprobación está seleccionada y elimina todos los backups que se mueven al almacén de objetos tanto de SnapCenter como del almacén de objetos.

   Si desactiva la casilla de comprobación, los backups se conservan solo en el almacén de objetos, pero esos backups no se pueden utilizar para la restauración a nivel de la aplicación. Más tarde, cuando active el backup para esta aplicación, los backups que retienen en el almacén de objetos no aparecen para restaurar.

Supervisar trabajos

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

Pasos

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.

Configurar los certificados de CA

Es posible configurar un certificado firmado de CA si se desea incluir la seguridad adicional en el entorno.

Configure el certificado firmado de SnapCenter CA en el conector BlueXP

Debe configurar el certificado firmado de CA de SnapCenter en el conector de BlueXP para que este pueda verificar el certificado de SnapCenter.

Antes de empezar

Debe ejecutar el siguiente comando en el conector de BlueXP para obtener el *<base_mount_path>*:
`sudo docker volume ls | grep snapcenter_volume | awk {'print $2'} | xargs sudo docker volume inspect | grep Mountpoint`

Pasos

1. Inicie sesión en el conector.
   `cd <base_mount_path> mkdir -p server/certificate`
2. Copie los archivos CA raíz y CA intermedios en el directorio *<base_mount_path>/server/certificate*.

   Los archivos de CA deben tener el formato .pem.
3. Si tiene archivos CRL, realice los siguientes pasos:
   a. `cd <base_mount_path> mkdir -p server/crl`
   b. Copie los archivos CRL en el directorio *<base_mount_path>/server/crl*.
4. Conéctese a cloudmanager_snapcenter y modifique el enableCACert en config.yml a true.
   `sudo docker exec -t cloudmanager_snapcenter sed -i 's/enableCACert: false/enableCACert: true/g' /opt/netapp/cloudmanager-snapcenter/config/config.yml`
5. Reinicie el contenedor cloudmanager_snapcenter.
   `sudo docker restart cloudmanager_snapcenter`

Configurar el certificado firmado por CA para BlueXP Connector

Si SSL 2way está habilitado en SnapCenter, debe realizar los siguientes pasos en el conector para utilizar el certificado CA como certificado de cliente cuando el conector se conecta con el SnapCenter.

Antes de empezar

Debe ejecutar el siguiente comando para obtener *<base_mount_path>*:
`sudo docker volume ls | grep snapcenter_volume | awk {'print $2'} | xargs sudo docker volume inspect | grep Mountpoint`

Pasos

1. Inicie sesión en el conector.
   `cd <base_mount_path> mkdir -p client/certificate`
2. Copie el certificado firmado por CA y el archivo de claves en *<base_mount_path>/client/certificate* en el conector.

   El nombre del archivo debe ser certificate.pem y key.pem. El certificate.pem debe tener toda la cadena de certificados como la CA intermedia y la CA raíz.
3. Cree el formato PKCS12 del certificado con el nombre certificate.p12 y conserve en *<base_mount_path>/client/certificate*.

   Ejemplo: openssl pkcs12 -inkey key.pem -in certificate.pem -export -out certificate.p12
4. Conéctese a cloudmanager_snapcenter y modifique el sendCACert en config.yml a true.
   `sudo docker exec -t cloudmanager_snapcenter sed -i 's/sendCACert: false/sendCACert: true/g' /opt/netapp/cloudmanager-snapcenter/config/config.yml`
5. Reinicie el contenedor cloudmanager_snapcenter.
   `sudo docker restart cloudmanager_snapcenter`
6. Realice los siguientes pasos en el SnapCenter para validar el certificado enviado por el conector.

a. Inicie sesión en el host del servidor de SnapCenter.
b. Haga clic en **Inicio** > **Iniciar búsqueda**.
c. Escriba mmc y presione **Enter**.
d. Haga clic en **Sí**.
e. En el menú Archivo, haga clic en **Agregar/quitar Snap-in**.
f. Haga clic en **Certificados** > **Añadir** > **Cuenta de ordenador** > **Siguiente**.
g. Haga clic en **Computadora local** > **Finalizar**.
h. Si no tiene más complementos para agregar a la consola, haga clic en **OK**.
i. En el árbol de la consola, haga doble clic en **Certificados**.
j. Haga clic con el botón derecho en la tienda **Trusted Root Certification Authority**.
k. Haga clic en **Importar** para importar los certificados y siga los pasos del **Asistente de importación de certificados**.

Restaure los datos de las aplicaciones en las instalaciones

Restaurar base de datos de Oracle

Es posible restaurar una base de datos de Oracle en la ubicación original o en la ubicación alternativa. Para una base de datos RAC, los datos se restauran en el nodo en las instalaciones donde se creó el backup.

Solo es compatible una base de datos completa con restauración de archivos de control. Si los registros de archivo no están presentes en el AFS, debe especificar la ubicación que contiene los registros de archivo necesarios para la recuperación.

No se admite la restauración de archivos individuales (SFR).

- Pasos*

1. En la interfaz de usuario de BlueXP, haga clic en **Protección** > **copia de seguridad y recuperación** > **aplicaciones**.
2. En el campo **filtro por**, seleccione el filtro **Tipo** y, en la lista desplegable, seleccione **Oracle**.
3. Haga clic en **Ver detalles** correspondiente a la base de datos que desea restaurar y haga clic en **Restaurar**.
4. En la página Restore options, especifique la ubicación donde desea restaurar los archivos de base de datos.

Si…	Realice lo siguiente…
Desea restaurar a la ubicación original	a. Seleccione **Restaurar a la ubicación original**. b. Si la instantánea se encuentra en el almacenamiento de archivado, seleccione la prioridad para restaurar los datos desde el almacenamiento de archivado. c. Haga clic en **Siguiente**. d. Seleccione **Estado de la base de datos** si desea cambiar el estado de la base de datos al estado requerido para realizar operaciones de restauración y recuperación. Los distintos estados de una base de datos, del más alto al más bajo, son open, mounted, started y shutdown. ◦ Si la base de datos está en un estado más alto, pero el estado debe cambiarse a un estado más bajo para realizar una operación de restauración, debe seleccionar esta casilla de comprobación. ◦ Si la base de datos está en un estado más bajo, pero el estado debe cambiarse a uno más alto para realizar la operación de restauración, el estado de la base de datos se modifica automáticamente aunque no seleccione la casilla de comprobación. ◦ Si una base de datos está en el estado open y, para restaurarla, la base de datos necesita que esté en el estado mounted, el estado de la base de datos se modifica únicamente si selecciona esta casilla de comprobación. e. Especifique el alcance de recuperación. ◦ Seleccione **All Logs** si desea recuperar la última transacción. ◦ Seleccione **Until SCN (System Change Number)** si desea recuperar un SCN específico. ◦ Seleccione **Fecha y hora** si desea recuperar un dato y una hora específicos. Debe especificar la fecha y la hora de la zona horaria del host de la base de datos. ◦ Seleccione **No recovery** si no desea recuperar. Si los registros de archivos no están presentes en el sistema de archivos activo, debe especificar la ubicación que contiene los registros de archivos necesarios para la

Si…	Realice lo siguiente…
Desea restaurar temporalmente a otro almacenamiento y, a continuación, copiar los archivos restaurados en la ubicación original	a. Seleccione **Restaurar a la ubicación original**. b. Si la instantánea se encuentra en el almacenamiento de archivado, seleccione la prioridad para restaurar los datos desde el almacenamiento de archivado. c. Selecciona **Cambiar ubicación de almacenamiento**. Si selecciona **Cambiar ubicación de almacenamiento**, puede agregar un sufijo al volumen de destino. Si no ha seleccionado la casilla de comprobación, se agrega de forma predeterminada **_restore** al volumen de destino. d. Haga clic en **Siguiente**. e. En la página Storage mapping, especifique los detalles de la ubicación de almacenamiento alternativo donde los datos restaurados del almacén de objetos se almacenarán temporalmente. Si selecciona un sistema ONTAP en las instalaciones y si no ha configurado la conexión del clúster con el almacenamiento de objetos, se le pedirá información adicional sobre el almacén de objetos. f. Haga clic en **Siguiente**. g. Seleccione **Estado de la base de datos** si desea cambiar el estado de la base de datos al estado requerido para realizar operaciones de restauración y recuperación. Los distintos estados de una base de datos, del más alto al más bajo, son open, mounted, started y shutdown. ◦ Si la base de datos está en un estado más alto, pero el estado debe cambiarse a un estado más bajo para realizar una operación de restauración, debe seleccionar esta casilla de comprobación. ◦ Si la base de datos está en un estado más bajo, pero el estado debe cambiarse a uno más alto para realizar la operación de restauración, el estado de la base de datos se modifica automáticamente aunque no seleccione la casilla de comprobación. Si una base de datos está en el estado open y, para restaurarla, la base de datos necesita que esté en el estado mounted,

Si…	Realice lo siguiente…
Desea restaurar a una ubicación alternativa	a. Seleccione **Restaurar a ubicación alternativa**. b. Si la instantánea se encuentra en el almacenamiento de archivado, seleccione la prioridad para restaurar los datos desde el almacenamiento de archivado. c. Si desea restaurar en almacenamiento alternativo, realice lo siguiente: i. Selecciona **Cambiar ubicación de almacenamiento**. Si selecciona **Cambiar ubicación de almacenamiento**, puede agregar un sufijo al volumen de destino. Si no ha seleccionado la casilla de comprobación, se agrega de forma predeterminada **_restore** al volumen de destino. ii. Haga clic en **Siguiente**. iii. En la página Storage mapping, especifique los detalles de la ubicación de almacenamiento alternativo donde los datos del almacén de objetos deben restaurarse. d. Haga clic en **Siguiente**. e. En la página Host de Destino, seleccione el host en el que se montará la base de datos. i. (Opcional) Para el entorno NAS, especifique el FQDN o la dirección IP del host al que se van a exportar los volúmenes restaurados del almacén de objetos. ii. (Opcional) Para el entorno SAN, especifique los iniciadores del host al que se van a asignar las LUN de los volúmenes restaurados desde el almacén de objetos. f. Haga clic en **Siguiente**.

5. Revise los detalles y haga clic en **Restaurar**.

La opción **Restore to alternate location** monta la copia de seguridad seleccionada en el host dado. Debe abrir manualmente la base de datos.

Después de montar el backup, no se podrá volver a montar hasta que se desmonte. Puede utilizar la opción **Unmount** de la interfaz de usuario para desmontar la copia de seguridad.

Para obtener información sobre cómo abrir la base de datos Oracle, consulte, "Artículo de base de

conocimientos".

Restaurar base de datos de SQL Server

Puede restaurar una base de datos de SQL Server a la ubicación original o a la ubicación alternativa.

No se admiten la restauración de archivos únicos (SFR), la recuperación de backups de registros y la propagación de grupos de disponibilidad.

Pasos

1. En la interfaz de usuario de BlueXP, haga clic en **Protección** > **copia de seguridad y recuperación** > **aplicaciones**.
2. En el campo **filtro por**, seleccione el filtro **Tipo** y, en la lista desplegable, seleccione **SQL**.
3. Haga clic en **Ver detalles** para ver todas las copias de seguridad disponibles.
4. Seleccione la copia de seguridad y haga clic en **Restaurar**.
5. En la página Restore options, especifique la ubicación donde desea restaurar los archivos de base de datos.

Si…	Realice lo siguiente…
Desea restaurar a la ubicación original	a. Seleccione **Restaurar a la ubicación original**. b. Si la instantánea se encuentra en el almacenamiento de archivado, seleccione la prioridad para restaurar los datos desde el almacenamiento de archivado. c. Haga clic en **Siguiente**.

Si…	Realice lo siguiente…
Desea restaurar temporalmente a otro almacenamiento y, a continuación, copiar los archivos restaurados en la ubicación original	a. Seleccione **Restaurar a la ubicación original**. b. Si la instantánea se encuentra en el almacenamiento de archivado, seleccione la prioridad para restaurar los datos desde el almacenamiento de archivado. c. Selecciona **Cambiar ubicación de almacenamiento**. Si selecciona **Cambiar ubicación de almacenamiento**, puede agregar un sufijo al volumen de destino. Si no ha seleccionado la casilla de comprobación, se agrega de forma predeterminada **_restore** al volumen de destino. d. Haga clic en **Siguiente**. e. En la página Storage mapping, especifique los detalles de la ubicación de almacenamiento alternativo donde los datos restaurados del almacén de objetos se almacenarán temporalmente. f. Haga clic en **Siguiente**.
Desea restaurar a una ubicación alternativa	a. Seleccione **Restaurar a ubicación alternativa**. b. Si la instantánea se encuentra en el almacenamiento de archivado, seleccione la prioridad para restaurar los datos desde el almacenamiento de archivado. c. Haga clic en **Siguiente**. d. En la página Destination host, seleccione un nombre de host, proporcione un nombre de base de datos (opcional), seleccione una instancia y especifique las rutas de restauración. La extensión de archivo proporcionada en la ruta alternativa debe ser la misma que la del archivo de base de datos original. e. Haga clic en **Siguiente**.

Si…	Realice lo siguiente…
Desea restaurar temporalmente en otro almacenamiento y, a continuación, copiar los archivos restaurados en la ubicación alternativa	a. Seleccione **Restaurar a ubicación alternativa**. b. Si la instantánea se encuentra en el almacenamiento de archivado, seleccione la prioridad para restaurar los datos desde el almacenamiento de archivado. c. Selecciona **Cambiar ubicación de almacenamiento**. Si selecciona **Cambiar ubicación de almacenamiento**, puede agregar un sufijo al volumen de destino. Si no ha seleccionado la casilla de comprobación, se agrega de forma predeterminada **_restore** al volumen de destino. d. Haga clic en **Siguiente**. e. En la página Storage mapping, especifique los detalles de la ubicación de almacenamiento alternativo donde los datos restaurados del almacén de objetos se almacenarán temporalmente. f. Haga clic en **Siguiente**. g. En la página Destination host, seleccione un nombre de host, proporcione un nombre de base de datos (opcional), seleccione una instancia y especifique las rutas de restauración. La extensión de archivo proporcionada en la ruta alternativa debe ser la misma que la del archivo de base de datos original. h. Haga clic en **Siguiente**.

6. En la opción **Pre-operations**, seleccione una de las siguientes opciones:
   - Seleccione **Sobrescribir la base de datos con el mismo nombre durante la restauración** para restaurar la base de datos con el mismo nombre.
   - Seleccione **mantener la configuración de replicación de bases de datos SQL** para restaurar la base de datos y mantener la configuración de replicación existente.
7. En la sección **Post-operations**, para especificar el estado de la base de datos para restaurar registros transaccionales adicionales, seleccione una de las siguientes opciones:
   - Seleccione **operativo, pero no disponible** si está restaurando todas las copias de seguridad necesarias ahora.

     Este es el comportamiento predeterminado, que deja la base de datos preparada para su uso

revirtiendo las transacciones no comprometidas. No podrá restaurar registros de transacciones adicionales hasta que cree un backup.

- Seleccione **no operativo, pero disponible** para dejar la base de datos no operativa sin revertir las transacciones no comprometidas.

  Pueden restaurarse registros de transacciones adicionales. No podrá utilizar la base de datos hasta que esta se recupere.

- Seleccione **modo de sólo lectura y disponible** para dejar la base de datos en modo de sólo lectura.

  Esta opción deshace las transacciones no comprometidas, pero guarda las acciones deshechas en un archivo en espera para que puedan revertirse los efectos de recuperación.

Si se habilita la opción Undo directory, se restauran más registros de transacciones. Si la operación de restauración para el registro de transacciones no se realiza correctamente, pueden revertirse los cambios. La documentación de SQL Server contiene más información.

8. Haga clic en **Siguiente**.
9. Revise los detalles y haga clic en **Restaurar**.

Restaurar la base de datos SAP HANA

Es posible restaurar una base de datos SAP HANA a cualquier host.

- Pasos*

1. En la interfaz de usuario de BlueXP, haga clic en **Protección** > **copia de seguridad y recuperación** > **aplicaciones**.
2. En el campo **Filtrar por**, selecciona el filtro **Tipo** y en el menú desplegable selecciona **HANA**.
3. Haga clic en **Ver detalles** correspondiente a la base de datos que desea restaurar y haga clic en **Restaurar**.
4. En la página Restore options, especifique una de las siguientes opciones:
   a. Para el entorno NAS, especifique el FQDN o la dirección IP del host al que se van a exportar los volúmenes restaurados del almacén de objetos.
   b. Para el entorno SAN, especifique los iniciadores del host al que se van a asignar las LUN de los volúmenes restaurados desde el almacén de objetos.
5. Si la instantánea se encuentra en el almacenamiento de archivado, seleccione la prioridad para restaurar los datos desde el almacenamiento de archivado.
6. Si no hay suficiente espacio en el almacenamiento de origen o el almacenamiento de origen está inactivo, selecciona **Cambiar ubicación de almacenamiento**.

   Si selecciona **Cambiar ubicación de almacenamiento**, puede agregar un sufijo al volumen de destino. Si no ha seleccionado la casilla de comprobación, se agrega de forma predeterminada **_restore** al volumen de destino.

7. Haga clic en **Siguiente**.
8. En la página Storage mapping, especifique los detalles de la ubicación de almacenamiento alternativo donde se almacenarán los datos restaurados del almacén de objetos.
9. Haga clic en **Siguiente**.

10. Revise los detalles y haga clic en **Restaurar**.

Esta operación solo hace la exportación de almacenamiento del backup seleccionado en el host determinado. Debe montar manualmente el sistema de archivos y activar la base de datos. Después de utilizar el volumen, el administrador de almacenamiento puede eliminar el volumen del clúster de ONTAP.

Para obtener información sobre cómo abrir la base de datos SAP HANA, consulte la, "TR-4667: Automatización de las operaciones de copia y clonado del sistema SAP HANA con SnapCenter".

Restaurar bases de datos MongoDB, MySQL y PostgreSQL

Es posible restaurar bases de datos MongoDB, MySQL y PostgreSQL en cualquier host.

- Pasos*

1. En la interfaz de usuario de BlueXP, haga clic en **Protección** > **copia de seguridad y recuperación** > **aplicaciones**.
2. En el campo **Filtrar por**, seleccione el filtro **Tipo** y en el menú desplegable seleccione **MongoDB**, **MySQL** o **PostgreSQL**.
3. Haga clic en **Ver detalles** correspondiente a la base de datos que desea restaurar y haga clic en **Restaurar**.
4. En la página Restore options, especifique una de las siguientes opciones:
   a. Para el entorno NAS, especifique el FQDN o la dirección IP del host al que se van a exportar los volúmenes restaurados del almacén de objetos.
   b. Para el entorno SAN, especifique los iniciadores del host al que se van a asignar las LUN de los volúmenes restaurados desde el almacén de objetos.
5. Si la instantánea se encuentra en el almacenamiento de archivado, seleccione la prioridad para restaurar los datos desde el almacenamiento de archivado.
6. Si no hay suficiente espacio en el almacenamiento de origen o el almacenamiento de origen está inactivo, selecciona **Cambiar ubicación de almacenamiento**.

   Si selecciona **Cambiar ubicación de almacenamiento**, puede agregar un sufijo al volumen de destino. Si no ha seleccionado la casilla de comprobación, se agrega de forma predeterminada **_restore** al volumen de destino.

7. Haga clic en **Siguiente**.
8. En la página Storage mapping, especifique los detalles de la ubicación de almacenamiento alternativo donde se almacenarán los datos restaurados del almacén de objetos.
9. Haga clic en **Siguiente**.
10. Revise los detalles y haga clic en **Restaurar**.

Esta operación solo hace la exportación de almacenamiento del backup seleccionado en el host determinado. Debe montar manualmente el sistema de archivos y activar la base de datos. Después de utilizar el volumen, el administrador de almacenamiento puede eliminar el volumen del clúster de ONTAP.