**Introducción**

Azure Backup ofrece copias de seguridad independientes y aisladas para proteger frente a la destrucción accidental de datos en las máquinas virtuales. Los administradores pueden implementar servicios de Azure para cumplir con sus requisitos de copia de seguridad, incluidos el agente de Microsoft Azure Recovery Services (MARS) para Azure Backup, Microsoft Azure Backup Server (MABS), las instantáneas de discos administrados de Azure y Azure Site Recovery.

Su empresa tiene varias cargas de trabajo críticas de máquinas virtuales que se ejecutan en Azure. Es el responsable de garantizar que la empresa puede recuperar estas máquinas virtuales en caso de pérdida o daños en los datos. Usa las funciones integradas de Azure Backup para ayudar a proteger estas máquinas virtuales. Su configuración utiliza Azure Backup para cargas de trabajo locales y de Azure.

En este módulo, obtendrá información sobre las diferentes estrategias de copia de seguridad de máquinas virtuales. estas estrategias funcionan tanto para máquinas virtuales locales como para Azure. Revise cómo Azure Backup proporciona muchas opciones para la copia de seguridad y la recuperación. También obtendrá información sobre otras estrategias, como instantáneas, eliminación temporal y Azure Site Recovery.

El objetivo de este módulo es equiparle con los conocimientos y las aptitudes necesarios para usar Azure Backup y Recovery Services de forma eficaz.

**Objetivos de aprendizaje**

En este módulo aprenderá a:

* Identifique características y casos de uso de las distintas copias de seguridad de máquinas virtuales de Azure.
* Configurar las instantáneas de máquina virtual y las opciones de copia de seguridad.
* Implementar la copia de seguridad y la restauración de máquinas virtuales, incluida la eliminación temporal.
* Realizar una recuperación de sitio a sitio mediante Azure Site Recovery.
* Compare las distintas opciones de copia de seguridad de máquinas virtuales.

**Exploración de las opciones para proteger los datos de la máquina virtual**

Para proteger sus datos realice copias de seguridad a intervalos regulares. Azure proporciona varias opciones de copia de seguridad para que las máquinas virtuales admitan diferentes escenarios y requisitos de configuración.

**Aspectos que se deben conocer sobre las opciones de copia de seguridad de las máquinas virtuales**

Vamos a examinar cuatro opciones para realizar copias de seguridad de las máquinas virtuales: Azure Backup, Azure Site Recovery e instantáneas e imágenes de discos administrados de Azure. En la tabla siguiente se resumen estas opciones y se proporcionan escenarios para usar los distintos métodos. Mientras revisa estas opciones, piense en qué método puede servir para los requisitos del escenario empresarial presentado en este módulo.

| **Opción de copia de seguridad de Azure** | **Escenarios de configuración** | **Descripción** |
| --- | --- | --- |
| **Azure Backup** | *Copia de seguridad de máquinas virtuales de Azure que ejecutan cargas de trabajo de producción*  *Creación de copias de seguridad coherentes con la aplicación para máquinas virtuales Windows y Linux* | Azure Backup toma una instantánea de la máquina virtual y almacena los datos como puntos de recuperación en almacenes de recuperación con redundancia geográfica. Cuando se realiza una restauración desde un punto de recuperación, se puede restaurar toda la máquina virtual o solo determinados archivos. |
| **Azure Site Recovery** | *Recuperación rápida y sencilla de aplicaciones específicas*  *Replicación en la región de Azure que prefiera* | Azure Site Recovery protege las máquinas virtuales ante desastres graves en los que toda una región experimente una interrupción debido a un desastre natural importante o a una interrupción del servicio generalizada. |
| **Discos administrados de Azure: instantánea** | *Copia de seguridad rápida y sencilla de las máquinas virtuales que usan discos administrados de Azure en cualquier momento*  *Compatibilidad con entornos de desarrollo y prueba* | Una instantánea de disco administrado de Azure es una copia completa de solo lectura de un disco administrado que, de forma predeterminada, se almacena como disco administrado estándar. Una instantánea existe independientemente del disco de origen y se pueden usar para crear discos administrados. Cada instantánea se factura en función del tamaño real utilizado. Si crea una instantánea de un disco administrado con una capacidad de 64 GB que solo usa 10 GB, se le facturan 10 GB. |
| **Discos administrados de Azure: imagen** | *Creación de una imagen a partir del disco duro virtual personalizado en una cuenta de almacenamiento de Azure o directamente desde una máquina virtual generalizada (a través de Sysprep)*  *Creación de cientos de máquinas virtuales mediante la imagen personalizada sin copiar ni administrar ninguna cuenta de almacenamiento* | Los discos administrados de Azure también admiten la creación de una imagen personalizada administrada. Este proceso captura una única imagen que contiene todos los discos administrados asociados a una máquina virtual, incluyendo tanto el sistema operativo como los discos de datos. |

**Aspectos que se deben tener en cuenta al crear imágenes frente a instantáneas**

Es importante comprender las diferencias y ventajas de crear una copia de seguridad de imagen e instantánea de un disco administrado de Azure.

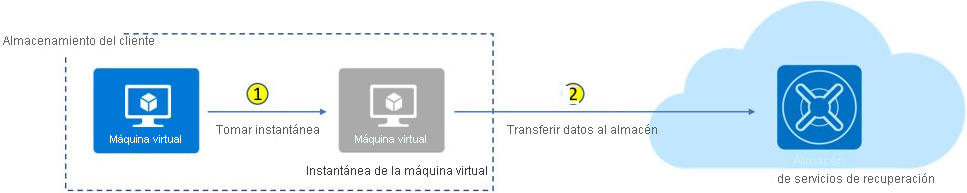
* **Las imágenes**. Con los discos administrados de Azure, es posible tomar una imagen de una máquina virtual generalizada que se ha desasignado. La imagen incluye todos los discos conectados a la máquina virtual. Puede utilizar la imagen para crear una máquina virtual que incluya todos los discos.
* **Las instantáneas**. Una instantánea es una copia de un disco en el momento dado en que se toma. La instantánea se aplica solo a un disco y no tiene conocimiento de ningún disco que no sea el que contiene. Las copias de seguridad de instantáneas son problemáticas para las configuraciones que requieren la coordinación de varios discos, como el seccionado. En este caso, las instantáneas deben coordinarse entre sí, pero esta funcionalidad no se admite actualmente.
* **Las copias de seguridad del disco del sistema operativo**. Si tiene una máquina virtual con un solo disco (el disco del sistema operativo), puede tomar una instantánea o una imagen del disco. Puede crear una máquina virtual a partir de una instantánea o una imagen.

**Creación de instantáneas de máquina virtual en Azure Backup**

Un trabajo de Azure Backup crea una instantánea para la máquina virtual en dos fases:

* Fase 1: Toma de una instantánea de los datos de la máquina virtual
* Fase 2: Transferencia de la instantánea a un almacén de Azure Recovery Services

En el siguiente diagrama se muestra este proceso.



Una vez completado el trabajo de Azure Backup, puede usar puntos de recuperación para la instantánea a fin de restaurar la máquina virtual o archivos específicos.

**Aspectos que se deben conocer sobre las instantáneas y los puntos de recuperación**

Echemos un vistazo más de cerca a las características de las instantáneas y los puntos de recuperación en Azure Backup.

* De forma predeterminada, Azure Backup mantiene las instantáneas durante dos días para reducir los tiempos de copia de seguridad y restauración. La retención local reduce el tiempo necesario para transformar y copiar datos de nuevo desde un almacén de Azure Recovery Services.
* Puede establecer el valor de retención de instantáneas predeterminado de uno y cinco días.
* Las instantáneas incrementales se almacenan como blobs en páginas de Azure (Discos de Azure).
* Los puntos de recuperación de una instantánea de máquina virtual solo están disponibles una vez completadas ambas fases del trabajo de Azure Backup.
* Los puntos de recuperación se muestran para la instantánea de máquina virtual en Azure Portal y se etiquetan con un *tipo de punto de recuperación*.
* Después de tomar una instantánea por primera vez, los puntos de recuperación se identifican con el tipo de punto de recuperación de **instantáneas**.
* Una vez que se haya transferido la instantánea al almacén de Azure Recovery Services, el tipo de punto de recuperación cambiará a **instantánea y almacén**.

**Aspectos que se deben tener en cuenta al usar instantáneas y puntos de recuperación**

Estas son algunas ventajas y consideraciones importantes sobre el uso de instantáneas y puntos de recuperación.

* **Considere la posibilidad de realizar una recuperación después de la fase 1**. Use la instantánea capturada en la fase 1 del trabajo de Azure Backup para restaurar la máquina virtual a partir de la instantánea. La fase 2 transfiere la instantánea al almacén de Recovery Services, por lo que se pueden crear puntos de recuperación. No tiene por qué esperar a que se complete la fase 2 para realizar una restauración completa a partir de la instantánea.
* **Considere el tipo de disco, el ajuste de tamaño y los precios**. Realice una copia de seguridad de discos SSD estándar, discos HDD estándar y discos SSD Premium. Use tamaños de disco de hasta 32 TB. Para las cuentas de almacenamiento premium, las instantáneas tomadas para los puntos de recuperación de instantánea se consideran en el límite de 10 TB de espacio asignado.

**Nota**

Azure Backup no recomienda cambiar el tamaño de los discos.

* **Considere la retención de instantáneas y el ahorro de costos**. Configure cuánto tiempo Azure Backup conservará las instantáneas en función de las necesidades de restauración. En función de los requisitos, puede establecer el valor de retención de instantáneas en un mínimo de un día. Esta configuración puede ayudar a reducir los costos de retención de instantáneas, si no realiza restauraciones con frecuencia.

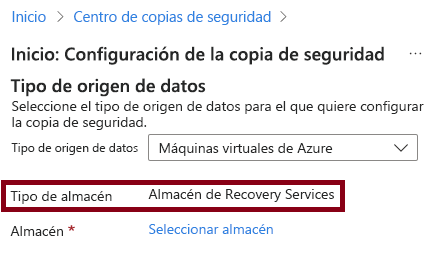
**Configuración de las opciones de copia de seguridad del almacén de Azure Recovery Services**

Un almacén de Azure Recovery Services es una entidad de almacenamiento de Azure que aloja datos. Normalmente, los datos son copias de datos o información de configuración de máquinas virtuales, cargas de trabajo, servidores o estaciones de trabajo. Puede usar almacenes de Recovery Services para organizar los datos de copia de seguridad y minimizar la sobrecarga de administración.

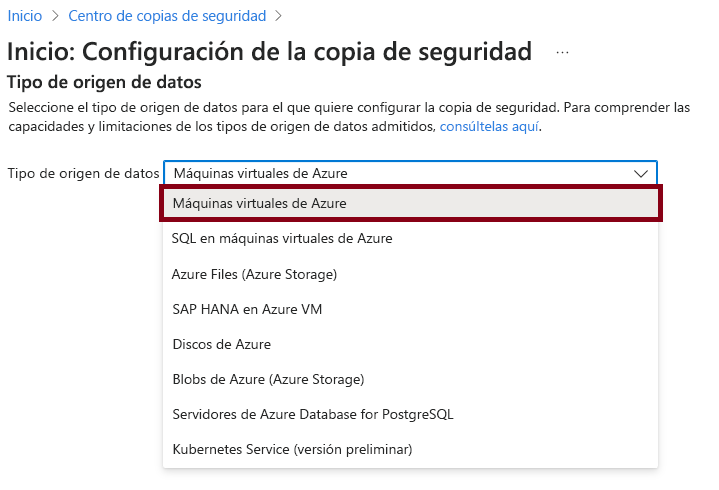
**Aspectos que debe conocer sobre los almacenes de Recovery Services**

A continuación, se explican algunas características de los almacenes de Recovery Services.

* Un almacén de Recovery Services almacena datos de copia de seguridad de varios servicios de Azure, como máquinas virtuales de IaaS (Linux o Windows), y bases de datos de Azure SQL.
* Los almacenes de Azure Recovery Services admiten System Center Data Protection Manager (DPM), Windows Server y Microsoft Azure Backup Server (MABS), entre otros.
* En Azure Portal, puede usar un almacén de Azure Recovery Services para realizar copias de seguridad de las máquinas virtuales de Azure:



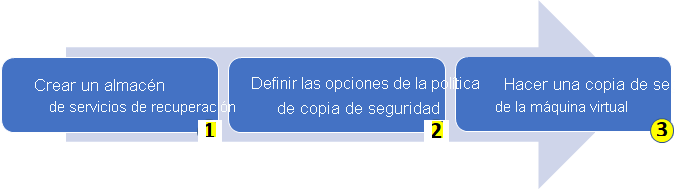
* El almacén de Recovery Services se puede usar para realizar copias de seguridad de máquinas virtuales locales, incluidas las siguientes: Hyper-V, VMware, Estado del sistema y Reconstrucción completa.



Para más información sobre cómo crear un almacén de Azure Recovery Services, consulte [Configuración de las opciones de copia de seguridad del almacén de Azure Recovery Services](https://learn.microsoft.com/es-es/training/modules/configure-file-folder-backups/4-setup-recovery-service-vault-backup-options).

**Copia de seguridad de las máquinas virtuales**

Para usar Azure Backup para proteger las máquinas virtuales de Azure, siga un proceso sencillo de tres pasos: crear un almacén, definir las opciones de copia de seguridad y desencadenar el trabajo de copia de seguridad.



**Paso 1: Creación de un almacén de Recovery Services**

El primer paso consiste en crear un almacén de Azure Recovery Services para las copias de seguridad de las máquinas virtuales. El almacén debe crearse dentro de la suscripción de Azure y en la región donde desea almacenar los datos.

También debe especificar cómo quiere que se replique el almacenamiento, ya sea con redundancia geográfica (valor predeterminado) o con redundancia local.

* **Con redundancia geográfica** (GRS): (valor predeterminado) Use GRS cuando Azure sea el punto de conexión de almacenamiento de copia de seguridad principal.
* **Con redundancia local** (LRS): si Azure **no es** el punto de conexión de almacenamiento de copia de seguridad principal, use LRS para reducir los costos de almacenamiento.

**Paso 2: Definición de las opciones de directiva de copia de seguridad**

Después de crear el almacén, debe definir la directiva de copia de seguridad. La directiva especifica cuándo se deben tomar las instantáneas de datos y cuánto tiempo se conservan las instantáneas.

La máquina virtual se protege tomando instantáneas de los datos a intervalos definidos. Las instantáneas generan puntos de recuperación que se almacenan en el almacén de Recovery Services.

Si es necesario reparar o recompilar la máquina virtual, puede restaurar la máquina mediante los puntos de recuperación guardados. En la directiva de copia de seguridad, puede especificar que se desencadene una copia de seguridad de una a cinco veces al día.

**Paso 3: Copia de seguridad de la máquina virtual**

El último paso consiste en ejecutar el proceso de trabajo de Azure Backup y crear las copias de seguridad.

Para ejecutar el trabajo de copia de seguridad, la extensión Azure Backup requiere que el agente de máquina virtual de Microsoft Azure esté presente en la máquina virtual de Azure.

* Si la máquina virtual se creó desde la galería de Azure, el agente se instala de forma predeterminada en la máquina.
* Si la máquina virtual se migró desde un centro de datos local, debe instalar manualmente el agente en la máquina.

Para más información, consulte [Instalación del agente de máquina virtual de Azure](https://learn.microsoft.com/es-es/azure/virtual-machines/extensions/agent-windows#install-the-vm-agent).

**Restauración de sus máquinas virtuales**

Al hacer una copia de seguridad de una máquina virtual, los datos de copia de seguridad y los puntos de recuperación se almacenan en su almacén de Recovery Services. Puede recuperar la máquina accediendo a la instantánea o restaurar datos a un momento dado específico mediante puntos de recuperación.



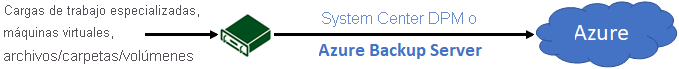
**Aspectos que debe saber sobre la restauración de máquinas virtuales**

Vamos a revisar algunos puntos sobre cómo restaurar las máquinas virtuales a partir de las instantáneas de copia de seguridad.

* Puede seleccionar puntos de recuperación para las instantáneas de máquina virtual en Azure Portal.
* Al desencadenar una operación de restauración, Azure Backup crea un trabajo para realizar un seguimiento de la operación de restauración.
* Azure Backup crea y muestra temporalmente notificaciones sobre la operación de restauración.
* Puede realizar un seguimiento de la operación de restauración supervisando las notificaciones del trabajo en Azure Portal.

**Implementación de System Center DPM y Azure Backup Server**

Otra opción para realizar copias de seguridad de las máquinas virtuales es usar System Center Data Protection Manager (DPM) o Microsoft Azure Backup Server (MABS). Puede usar estos servicios para realizar copias de seguridad de cargas de trabajo especializadas, máquinas virtuales o archivos, carpetas y volúmenes. Las cargas de trabajo especializadas pueden incluir datos de Microsoft SharePoint, Microsoft Exchange y SQL Server.



Puede realizar copias de seguridad de las máquinas virtuales y las aplicaciones en el almacenamiento de System Center DPM o MABS y, a continuación, realizar una copia de seguridad del almacenamiento DPM o MABS en un almacén de Azure Recovery Services.

**Aspectos que debe conocer saber sobre el uso de System Center DPM y MABS**

Vamos a examinar los detalles de configuración para usar System Center DPM o MABS para realizar copias de seguridad de los datos.

* Al configurar la protección para una máquina o una aplicación en System Center DPM o MABS, opta por hacer la copia de seguridad en el disco local de DPM o MABS para el almacenamiento a corto plazo, y en Azure para la protección en línea. Especifica cuándo ejecutar la copia de seguridad en el almacenamiento local de DPM o MABS y cuándo ejecutar la copia de seguridad en línea en Azure.
* Para proteger sus máquinas locales, la instancia de System Center DPM o MABS debe estar ubicada de forma local.
* Para proteger las máquinas virtuales de Azure, la instancia de MABS debe ejecutarse como una máquina virtual de Azure y debe estar en Azure.
* El agente de protección de System Center DPM / MABS debe estar instalado en cada máquina que quiera proteger. Para obtener más información, consulte [Implementación del agente de protección de System Center DPM](https://learn.microsoft.com/es-es/system-center/dpm/deploy-dpm-protection-agent) e [Instalación del agente de protección de DPM (para MABS)](https://learn.microsoft.com/es-es/azure/backup/backup-azure-microsoft-azure-backup#install-and-update-the-data-protection-manager-protection-agent).
* Las máquinas de las que desea realizar una copia de seguridad deben agregarse a un [*grupo de protección* de System Center DPM](https://learn.microsoft.com/es-es/system-center/dpm/create-dpm-protection-groups).
* Cuando se desencadena la copia de seguridad, se realiza una copia de seguridad del disco de la carga de trabajo protegida en los discos de MABS o DPM locales, según la programación especificada. A continuación, el agente MARS que se ejecuta en la instancia de DPM o MABS realiza una copia de seguridad de los discos de DPM y MABS en el almacén de Recovery Services.

**Aspectos que se deben tener en cuenta al usar System Center DPM y MABS**

La elección de System Center DPM o MABS para la solución de copia de seguridad conlleva varias ventajas.

* **Considere la posibilidad de realizar copias de seguridad optimizadas con reconocimiento de aplicaciones**. Realice una copia de seguridad de los datos en MABS o System Center DPM para habilitar las copias de seguridad optimizadas con reconocimiento de aplicaciones para aplicaciones comunes. Estas aplicaciones pueden incluir SQL Server, Exchange y SharePoint. La optimización se puede lograr para copias de seguridad de archivos, carpetas o volúmenes y copias de seguridad del estado de la máquina. Las copias de seguridad de estado de la máquina pueden ser de reconstrucción completa o del estado del sistema.
* **Considere la posibilidad de realizar copias de seguridad simplificadas para máquinas locales**. Implemente System Center DPM o MABS para evitar instalar el agente de Microsoft Azure Recovery Services (MARS) en cada máquina local de la que se vaya a realizar una copia de seguridad. Las máquinas locales ejecutan automáticamente el agente de **protección** de System Center DPM (y MABS). El agente de MARS solo se ejecuta en la instancia de MABS o DPM.
* **Tenga en cuenta la flexibilidad y la programación**. Configure System Center DPM o MABS para obtener flexibilidad y opciones de programación más pormenorizadas para ejecutar las copias de seguridad.
* **Tenga en cuenta la administración consolidada**. Administre las copias de seguridad de varias máquinas recopilándolas en grupos de protección en una sola consola. Agrupar máquinas es útil cuando las aplicaciones están distribuidas por niveles en varias máquinas y quiere realizar una copia de seguridad de ellas al mismo tiempo.

**Comparación del agente de MARS y Azure Backup Server**

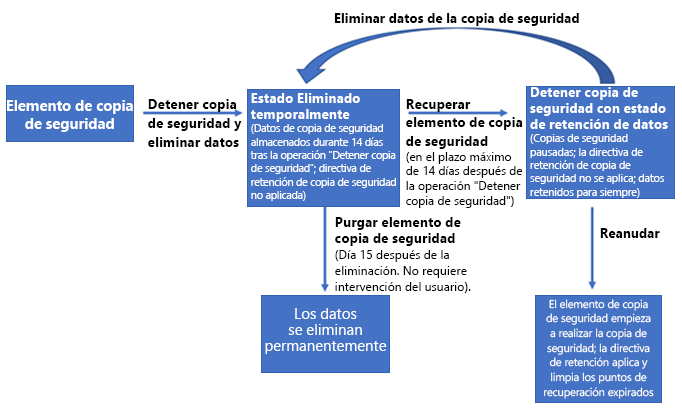
Existen ventajas y límites para usar los distintos componentes de Copia de seguridad de Azure. En esta sección, comparamos el agente de copia de seguridad de Microsoft Azure Recovery Services (MARS) y Microsoft Azure Backup Server, que usa el agente de protección de System Center DPM.

En la tabla siguiente se resumen las características y restricciones, y se identifica qué datos están protegidos por la copia de seguridad y dónde se almacenan las copias de seguridad en la configuración.

| **Componente** | **Ventajas** | **Límites** | **Datos protegidos** | **Copias de seguridad almacenadas** |
| --- | --- | --- | --- | --- |
| **Agente de copia de seguridad MARS** | *Copia de seguridad de archivos y carpetas en máquinas físicas o virtuales que ejecutan Windows*  *No se necesita ningún servidor de copia de seguridad independiente* | - Copias de seguridad desencadenadas 3 veces al día - Sin reconocimiento de aplicaciones - Solo restauración de archivos, carpetas y niveles de volumen - No es compatible con Linux | Archivos y carpetas | Almacén de Azure Recovery Services |
| **Azure Backup Server** | *Instantáneas con reconocimiento de aplicaciones*  *Flexibilidad total para cuando se desencadenan las copias de seguridad*  *Granularidad de recuperación*  *Compatibilidad con Linux en máquinas virtuales de Hyper-V y VMware*  *Copia de seguridad y restauración de máquinas virtuales de VMware*  *No se requiere licencia de System Center* | - Siempre se requiere una suscripción de Azure activa - No hay copias de seguridad para cargas de trabajo de Oracle - No se admite la copia de seguridad en cinta | Archivos, carpetas, volúmenes, máquinas virtuales, aplicaciones y cargas de trabajo | Almacén de Recovery Services o disco conectado localmente |

**Implementación de la eliminación temporal para las máquinas virtuales**

Azure Storage ahora ofrece la opción de *eliminación temporal* para objetos de Blob de Azure. Con esta característica, puede recuperar más fácilmente los datos cuando se modifican o eliminan.



La eliminación temporal de máquinas virtuales protege las copias de seguridad de las máquinas virtuales frente a la eliminación no deseada. Incluso después de que se eliminen las copias de seguridad, se conservan en estado de eliminación temporal durante 14 días adicionales.

**Importante**

La eliminación temporal solo protege los datos de copia de seguridad eliminados. Si se elimina una máquina virtual sin una copia de seguridad, la característica de eliminación temporal no conservará los datos. Todos los recursos deben protegerse con Azure Backup para garantizar una resistencia total.

**Aspectos que debe saber sobre la eliminación temporal de copias de seguridad**

Revise los detalles siguientes relacionados con la implementación de la eliminación temporal para las copias de seguridad de la máquina virtual.

* **Detenga del trabajo de copia de seguridad**. Para poder eliminar o conservar los datos de copia de seguridad de la máquina virtual, debe detener el trabajo de copia de seguridad activo. Después de detener el trabajo de copia de seguridad en Azure Portal, puede elegir eliminar o conservar los datos de copia de seguridad.
* **Aplique el estado de eliminación temporal**. Para evitar que los datos de copia de seguridad de la máquina virtual se eliminen permanentemente, seleccione **Eliminar datos de copia de seguridad** seguido de **Detener copia de seguridad**. El estado de eliminación temporal se aplica a los datos de copia de seguridad, y los datos se conservan durante 14 días. Si aplica el estado a una máquina virtual, se dice que la máquina está *eliminada temporalmente*.
* **Vea los datos de eliminación temporal en el almacén**. Durante el período de retención de 14 días, el almacén de Recovery Services muestra la máquina virtual eliminada temporalmente con un icono de **eliminación temporal** rojo.

**Nota**

Cuando un almacén de Recovery Services contiene elementos eliminados temporalmente, el almacén no se puede eliminar. En primer lugar, elimine o recupere todos los elementos eliminados temporalmente y, a continuación, elimine el almacén.

* **Recupere elementos de copia de seguridad**. Para poder restaurar una máquina virtual eliminada temporalmente, debe recuperar los datos de la copia de seguridad.
* **Restaure los elementos**. Después de recuperar el elemento de copia de seguridad, puede restaurar la máquina virtual seleccionando **Restaurar máquina virtual** en el punto de recuperación elegido en la copia de seguridad.
* **Reanude las copias de seguridad**. Una vez completado el proceso de recuperación, el estado del trabajo de copia de seguridad volverá a **Detener copia de seguridad con conservación de datos** y,después, podrá seleccionar **Reanudar copia de seguridad**. La operación de reanudación recupera el elemento de copia de seguridad en estado *activo* según la directiva de copia de seguridad seleccionada por el usuario. La directiva define las programaciones de copia de seguridad y retención.

**Implementación de Azure Site Recovery**

**Información general sobre Azure Site Recovery**

Azure Site Recovery es un servicio que ayuda a garantizar la continuidad empresarial mediante la replicación de cargas de trabajo de un sitio primario a una ubicación secundaria.

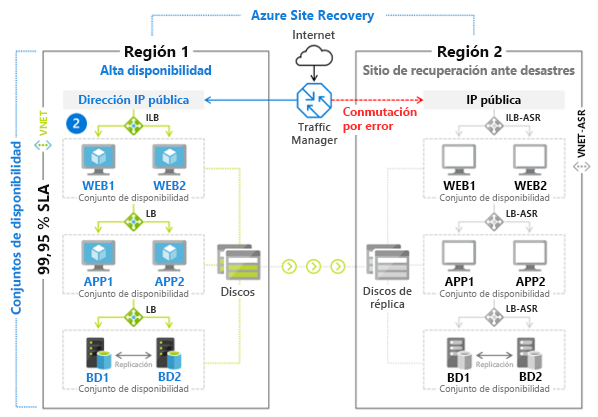
Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

<https://youtu.be/94LDYjBhz5c>

Supongamos que trabaja para una gran empresa de comercio electrónico que se basa en gran medida en su plataforma en línea para generar ingresos. Un día, una gran tormenta azota la región donde se encuentra su centro de datos principal, provocando uja interrupción de la alimentación y dejando su sitio web inaccesible. Esta interrupción da lugar a pérdidas financieras significativas y daños a la reputación de su empresa. Para evitar estos incidentes en el futuro, decida implementar Azure Site Recovery. Al replicar las cargas de trabajo en una ubicación secundaria, puede asegurarse de que las aplicaciones sigan siendo accesibles. Puede seguir sirviendo a sus clientes y minimizar el impacto en su negocio.

En la siguiente ilustración se muestran dos regiones conectadas por Azure Traffic Manager. Azure Site Recovery se implementa para habilitar la conmutación por error de la región 1 a la región 2.



**Aspectos que debe saber sobre Azure Site Recovery**

Azure Site Recovery admite muchas configuraciones y complementa varios servicios de Azure. Puede implementar Site Recovery para realizar copias de seguridad de las máquinas virtuales y las máquinas físicas en los escenarios siguientes:

* Replicación de las máquinas virtuales de Azure de una región de Azure a otra
* Replicación de máquinas virtuales de VMware locales, máquinas virtuales de Hyper-V, servidores físicos (Windows y Linux) y máquinas virtuales de Azure Stack en Azure
* Replicación de las instancias de Windows de AWS en Azure
* Replicación de las máquinas virtuales locales de VMware, de Hyper-V administradas por System Center VMM y los servidores físicos en un sitio secundario

**Aspectos que debe tener en cuenta al usar Site Recovery**

Hay muchas ventajas para implementar Azure Site Recovery. Cuando revise las siguientes características, considere cómo el servicio puede admitir los requisitos empresariales.

| **Característica** | **Descripción** |
| --- | --- |
| **Administración consolidada** | Configure y administre la replicación, la conmutación por error y la conmutación por recuperación desde una sola ubicación en Azure Portal. |
| **Costo y complejidad reducidos** | Haga la replicación en Azure para eliminar el costo y la complejidad de mantener un centro de datos secundario. |
| **Resistencia de replicación** | Organice la replicación sin interceptar los datos de la aplicación y obtenga la resistencia de Azure Storage. Cuando se produce la conmutación por error, las máquinas virtuales de Azure se crean en función de los datos replicados. |
| **Replicación continua** | Acceda a la replicación continua para máquinas virtuales de Azure y máquinas virtuales de VMware, y una frecuencia de replicación de tan solo 30 segundos para Hyper-V. |
| **Puntos de recuperación de instantáneas** | Permite replicar mediante puntos de recuperación con instantáneas coherentes con la aplicación, que capturan los datos del disco, todos los datos en que hay en la memoria y todas las transacciones en curso. |
| **Conmutación por error y reserva sencilla** | Ejecute conmutaciones por error planeadas para las interrupciones previstas sin pérdida de datos. Ejecute conmutaciones por error no planeadas con la mínima pérdida de datos, dependiendo de la frecuencia de replicación. Conmute por recuperación a su sitio principal fácilmente cuando vuelva a estar disponible. |
| **Integración** | Realice la integración con Azure para simplificar la administración de la red de una aplicación, lo que incluye la reserva de direcciones IP, la configuración de equilibradores de carga o la integración de Azure Traffic Manager, con el fin de que los cambios de red sean eficientes. |

**Comprobación de conocimiento**

Su empresa tiene cargas de trabajo críticas de máquinas virtuales que se ejecutan en Azure. Usa Azure Backup y otros servicios de Azure para ayudar a proteger las máquinas virtuales. Tiene la tarea de desarrollar un plan de configuración para recuperar máquinas virtuales y elementos de copia de seguridad. Algunos equipos han enviado sus requisitos de configuración y sus preguntas para que los evalúe:

* El equipo de infraestructura tiene una combinación de máquinas virtuales de Azure que ejecutan cargas de trabajo de producción, incluidos servidores Windows y servidores Linux.
* El equipo de ingeniería ha solicitado soporte técnico de copia de seguridad para sus discos de base de datos de desarrollo.
* Está investigando cómo se pueden restaurar las copias de seguridad en un estado de *eliminación temporal* para recuperarse de los errores de la máquina.

**Responda a las siguientes preguntas**

Elija la respuesta más adecuada para cada una de las siguientes preguntas. Después, seleccione **Comprobar las respuestas**.

Principio del formulario

**1. ¿Cuál es el mejor método de copia de seguridad para las máquinas virtuales de producción de la empresa?**

1. Instantáneas de discos administrados de Azure
2. Azure Backup
3. Azure Site Recovery

**2. ¿Qué opción debe recomendar para realizar copias de seguridad de los discos de base de datos de ingeniería?**

1. Copia de seguridad de la máquina virtual de Azure
2. Azure Site Recovery
3. Instantáneas de discos administrados de Azure

**3. Un ataque de malware reciente ha eliminado la copia de seguridad de varias máquinas virtuales. ¿Durante cuánto tiempo están disponibles los elementos de copia de seguridad en el estado de eliminación temporal?**

1. 14 días
2. Siete días
3. 30 días
   1. B
   2. C
   3. A

Final del formulario

**Resumen y recursos**

Azure Backup ofrece copias de seguridad independientes y aisladas para proteger frente a la destrucción accidental de datos en las máquinas virtuales.

En este módulo, ha identificado las características y los casos de uso de diferentes métodos de Azure Backup. Ha aprendido a configurar las instantáneas de discos administrados de Azure y las opciones de Azure Backup. Ha explorado cómo implementar la copia de seguridad y restauración de máquinas virtuales de Azure, incluida la *eliminación temporal*. Ha descubierto cómo completar la recuperación de sitio a sitio mediante Azure Site Recovery. Ha comparado el agente de Microsoft Azure Recovery Services (MARS) para Azure Backup y Microsoft Azure Backup Server (MABS).

Las principales conclusiones de este módulo son:

* Azure Site Recovery permite la conmutación por error y el acceso continuado a las aplicaciones en caso de interrupción. Esta protección se proporciona mediante la replicación de cargas de trabajo en una ubicación secundaria.
* Azure Backup proporciona copias de seguridad seguras para máquinas virtuales, lo que permite la restauración de máquinas virtuales completas o archivos específicos.
* Tanto Azure Site Recovery como Azure Backup ofrecen características como la administración consolidada, el costo y la complejidad reducidos y la resistencia de replicación.