**Introducción**

El servicio Azure Backup proporciona una solución sencilla, segura y rentable para realizar copias de seguridad de los datos. Los administradores implementan el agente de Microsoft Azure Recovery Services (MARS) para Azure Backup para recuperar sus datos de la nube de Microsoft Azure.

En este módulo, supongamos que su empresa almacena información de cumplimiento crítica en recursos compartidos de archivos de Azure Files. Es responsable de garantizar que este contenido se pueda recuperar en caso de pérdida de datos o daños en los mismos. Necesita configurar directivas de copia de seguridad y restauración que satisfagan las necesidades normativas de su empresa.

**Objetivos de aprendizaje**

En este módulo aprenderá a:

* Identificar las características y los casos de uso de Azure Backup.
* Configure las opciones de copia de seguridad del almacén de Azure Recovery Services.
* Implemente copias de seguridad de los archivos y carpetas locales.
* Configure el agente de Microsoft Azure Recovery Services para Azure Backup.

**Aptitudes evaluadas**

El contenido del módulo le ayuda a prepararse para el [examen AZ-104: Administrador de Microsoft Azure](https://learn.microsoft.com/es-es/certifications/exams/az-104). Los conceptos del módulo tratan los siguientes aspectos:

Supervisión y copia de seguridad de los recursos de Azure (10-15 %)

* Implementación de la copia de seguridad y la recuperación
  + Cree un almacén de Azure Recovery Services.
  + Cree y configure una directiva de copia de seguridad.
  + Realizar operaciones de copia de seguridad y restauración mediante Azure Backup.
  + Configurar y revisar los informes de copia de seguridad.

**Descripción de las ventajas de Azure Backup**

Azure Backup es el servicio de Azure que puede usar para realizar una copia de seguridad de los datos (protegerlos) y recuperarlos en la nube de Microsoft. Azure Backup reemplaza su solución de copia de seguridad local o remota existente por una solución confiable, segura y rentable basada en la nube.

Azure Backup ofrece varios componentes que se descargan e implementan en el equipo o servidor adecuados, o en la nube. El componente, o agente, que se implemente depende de lo que quiera proteger. Todos los componentes de Azure Backup (sin importar si va a proteger los datos de forma local o en la nube) se pueden usar para realizar una copia de seguridad de datos en un almacén de Azure Recovery Services.

**Introducción a Azure Backup**

Interfaz de usuario gráfica

Descripción generada automáticamente con confianza media

<https://youtu.be/elODShatt-c>

**Aspectos que debe saber sobre Azure Backup**

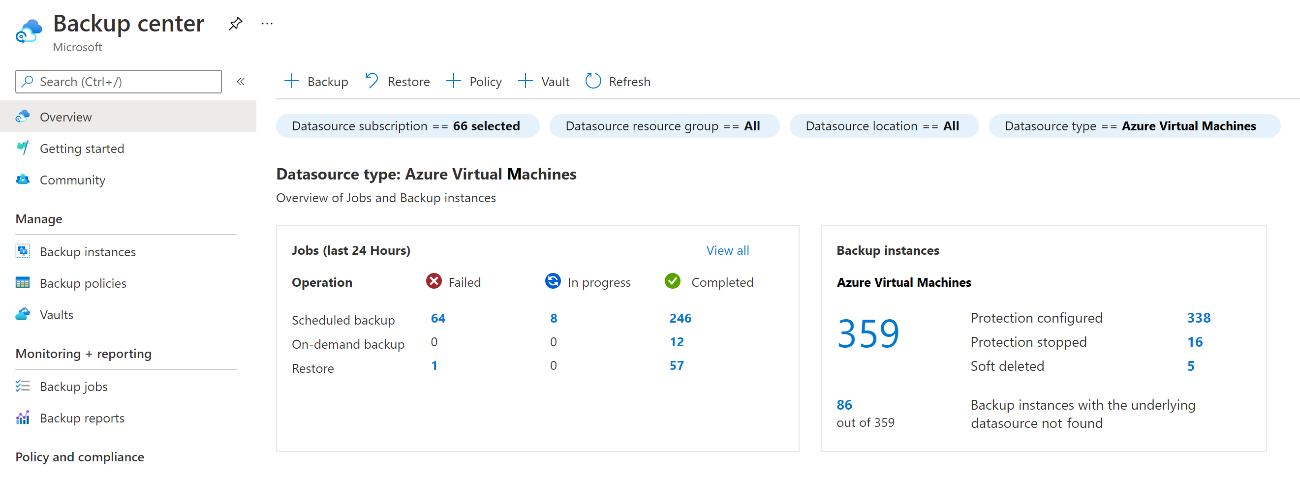
Echemos un vistazo a algunas de las muchas ventajas que obtiene de la implementación de Azure Backup.

| **Prestación** | **Descripción** |
| --- | --- |
| **Descarga de la copia de seguridad local** | Azure Backup ofrece una solución sencilla para hacer copias de seguridad de los recursos locales en la nube. Obtenga copias de seguridad a corto y largo plazo sin necesidad de implementar complejas soluciones de copias de seguridad locales. |
| **Copia de seguridad de máquinas virtuales IaaS de Azure** | Azure Backup proporciona copias de seguridad independientes y aisladas para evitar la destrucción accidental de datos originales. Las copias de seguridad se almacenan en un almacén de Azure Recovery Services con administración integrada de puntos de recuperación. La configuración y la escalabilidad son sencillas, las copias de seguridad están optimizadas y puede restaurarlas fácilmente cuando sea necesario. |
| **Obtención de una transferencia de datos ilimitados** | Azure Backup no limita la cantidad de datos de entrada y salida que se transfieren ni cobra por ellos. Datos de salida hacen referencia a los datos transferidos desde un almacén de Recovery Services durante una operación de restauración. Si realiza una copia de seguridad inicial sin conexión mediante el servicio Azure Import/Export para importar grandes cantidades de datos, hay un costo asociado a los datos de entrada. |
| **Protección de los datos** | el cifrado de datos permite la transmisión y el almacenamiento seguros de los datos del cliente en la nube pública. La frase de contraseña de cifrado se almacena localmente y nunca se transmite ni se almacena en Azure. Si es necesario restaurar datos, solo cuenta con la frase de contraseña o clave de cifrado. |
| **Obtención de copias de seguridad consistentes entre aplicaciones** | una copia de seguridad coherente con la aplicación significa un punto de recuperación que tiene todos los datos necesarios para restaurar la copia de seguridad. Azure Backup proporciona copias de seguridad consistentes entre aplicaciones, lo que garantiza que no se van a necesitar correcciones adicionales para restaurar los datos. La restauración de datos coherentes con la aplicación reduce el tiempo de restauración, lo que permite volver rápidamente a un estado de ejecución. |
| **Retención de los datos a corto y largo plazo** | Puede usar los almacenes de Azure Recovery Services para la retención de datos tanto a corto como a largo plazo. Azure no limita el tiempo que los datos pueden permanecer en un almacén de Recovery Services. Puede conservarlos el tiempo que desee. Azure Backup tiene un límite de 9.999 puntos de recuperación por instancia protegida. |
| **Administración automática del almacenamiento** | Los entornos híbridos a menudo requieren un almacenamiento heterogéneo, con algunas instancias locales y algunas instancias en la nube. Con Azure Backup, la implementación de dispositivos de almacenamiento local no supone ningún costo. Azure Backup asigna y administra automáticamente el almacenamiento de copias de seguridad. El servicio usa un modelo de pago por uso, por lo que solo paga por el almacenamiento que consume. |
| **Varias opciones de almacenamiento** | Azure Backup ofrece dos tipos de replicación para mantener la alta disponibilidad de los datos y el almacenamiento.  El **almacenamiento con redundancia local (LRS)** replica los datos tres veces (crea tres copias de los datos) en una unidad de escalado de almacenamiento de un centro de datos. Todas las copias de los datos se encuentran en la misma región. LRS es una opción de bajo costo para proteger los datos contra errores de hardware local.  El **almacenamiento con redundancia geográfica (GRS)** es la opción de replicación predeterminada y recomendada. GRS replica los datos en una región secundaria (a cientos de kilómetros de la ubicación principal de los datos de origen). GRS cuesta más que LRS, pero proporciona un mayor nivel de durabilidad de los datos, aunque se produzca una interrupción regional. |

**Implementación del Centro de copias de seguridad para Azure Backup**

El Centro de copias de seguridad para Azure Backup proporciona una única experiencia de administración unificada en Azure. Las empresas pueden gobernar, supervisar, operar y analizar sus copias de seguridad a escala. La interfaz del Centro de copias de seguridad es coherente con las experiencias de administración nativas de Azure.

En Azure Portal, busque **Centro de copias de seguridad** y vaya al panel del Centro de copias de seguridad:



**Aspectos que debe tener en cuenta al usar el Centro de copias de seguridad**

Tenga en cuenta las siguientes ventajas de implementar el Centro de copias de seguridad para Azure Backup.

* **Tenga en cuenta la variedad de funcionalidades**. Este centro está diseñado para funcionar bien en entornos de Azure grandes y distribuidos. Puede usar el Centro de copias de seguridad para administrar de forma eficaz las copias de seguridad que abarcan varios tipos de cargas de trabajo, almacenes, suscripciones, regiones e inquilinos.
* **Tenga en cuenta la administración centrada en orígenes de datos**. El Centro de copias de seguridad proporciona vistas y filtros que se centran en los orígenes de datos de los que se realiza la copia de seguridad, como máquinas virtuales y bases de datos. Un propietario de recursos o un administrador de copias de seguridad pueden administrar elementos de copia de seguridad en distintos almacenes. El administrador también puede filtrar las vistas por propiedades específicas del origen de datos, como la suscripción del origen de datos, el grupo de recursos y las etiquetas.
* **Tenga en cuenta las experiencias conectadas**. El Centro de copias de seguridad proporciona integraciones nativas a los servicios de Azure existentes que permiten la administración a escala. El Centro de copias de seguridad usa la experiencia de Azure Policy para ayudarle a controlar las copias de seguridad. Usa los libros de Azure de Azure Monitor y los registros de Azure Monitor (Log Analytics) para ayudarle a ver informes detallados sobre las copias de seguridad. No es necesario que conozca los nuevos principios para usar las diversas características que ofrece el Centro de copias de seguridad. También puede detectar recursos de la comunidad desde el Centro de copias de seguridad.
* **Tenga en cuenta los escenarios admitidos**. El Centro de copias de seguridad se admite actualmente en muchos escenarios:
  + Copia de seguridad de Azure Virtual Machines, incluida la copia de seguridad de SQL y SAP HANA en Azure Virtual Machines
  + Copia de seguridad de Azure Files, copia de seguridad de Azure Blob Storage y copia de seguridad de discos administrados de Azure
  + Copia de seguridad del servidor de Azure Database for PostgreSQL

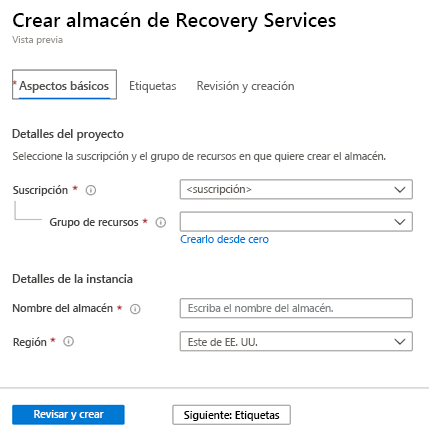
**Configuración de las opciones de copia de seguridad del almacén de Azure Recovery Services**

El **almacén de Recovery Services** es una entidad de almacenamiento de Azure que aloja datos. Los almacenes de Recovery Services facilitan la tarea de organizar los datos de copia de seguridad, al mismo tiempo que reduce al mínimo su sobrecarga administrativa.

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

Vamos a revisar algunas características de los almacenes de Recovery Services.

* El almacén de Recovery Services se puede usar para realizar copias de seguridad de recursos compartidos de archivos de Azure Files o archivos y carpetas locales.
* Los almacenes de Recovery Services almacenan datos de copia de seguridad de varios servicios de Azure, como máquinas virtuales de IaaS (Linux o Windows), y Azure SQL en máquinas virtuales de Azure.
* Los almacenes de Recovery Services admiten System Center Data Protection Manager, Windows Server y Azure Backup Server, entre otros.
* En Azure Portal, puede crear un almacén de Recovery Services desde el panel del Centro de copias de seguridad.



Para completar la configuración inicial, debe especificar la suscripción, el grupo de recursos y la región geográfica, junto con un nombre para identificar el almacén.

**Nota**

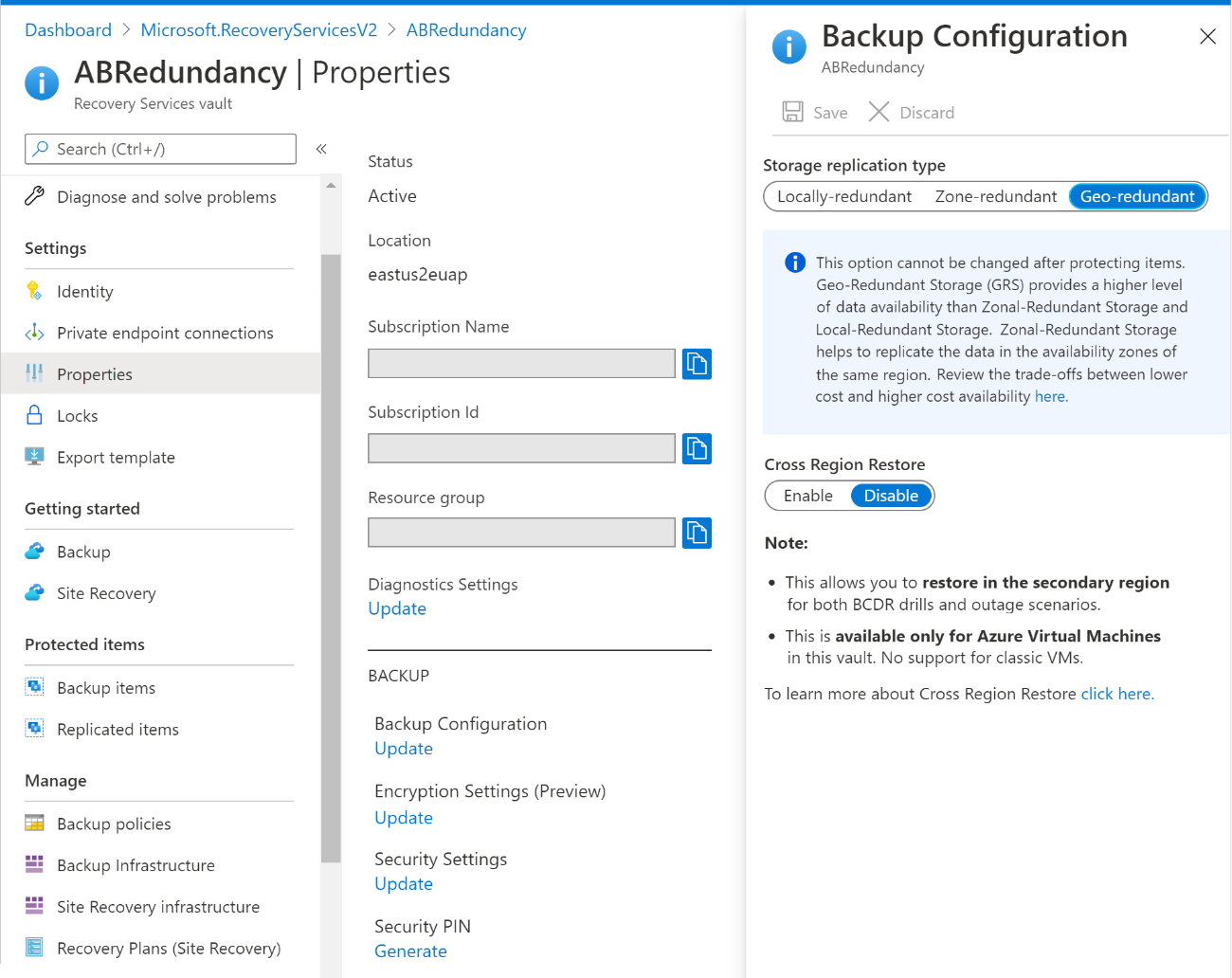
Dentro de una suscripción de Azure, puede crear hasta 500 almacenes de Recovery Services por región.

La creación del almacén de Recovery Services puede tardar varios minutos. Puede supervisar el estado de la operación en el área **Notificaciones** del Centro de copias de seguridad.

**Aspectos que debe saber sobre la configuración de almacenes de Recovery Services**

Azure Backup administra automáticamente el almacenamiento del almacén. En función de la configuración, debe especificar cómo se replica el almacenamiento.

* Si usa Azure Backup para recursos compartidos de archivos de Azure Files, no es necesario configurar el tipo de replicación del almacenamiento. La copia de seguridad de Azure Files se basa en instantáneas, y no se transfieren datos al almacén. Las instantáneas se almacenan en la misma cuenta de almacenamiento de Azure que el recurso compartido de archivos del que se ha realizado la copia de seguridad.
* Puede configurar la replicación para los almacenes de Recovery Services desde el panel del Centro de copias de seguridad en **Propiedades**>**Configuración de copia de seguridad**>**Actualización**.



* Hay tres opciones de replicación de almacenamiento: con redundancia geográfica, con redundancia local y con redundancia de zona. En la tabla siguiente se proporcionan recomendaciones para los tipos de replicación.

| **Tipo de replicación** | **Recomendación** |
| --- | --- |
| **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. |
| **Con redundancia de zona** | Si necesita disponibilidad de datos sin tiempo de inactividad en una región y necesita garantizar la residencia de datos, use ZRS. |

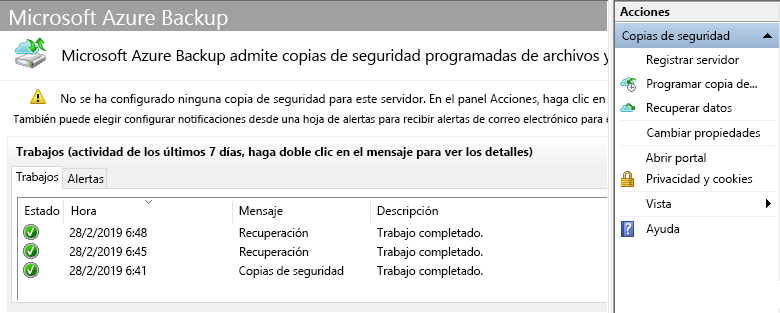
* También puede especificar cómo se deben restaurar los datos en una región secundaria emparejada de Azure habilitando la **Restauración entre regiones**.

**Importante**

Debe cambiar el tipo de replicación de almacenamiento del almacén de Recovery Services antes de intentar configurar una copia de seguridad en el almacén. Después de configurar una copia de seguridad, la opción para modificar el tipo de replicación está deshabilitada.

**Uso del agente de Microsoft Azure Recovery Services (MARS)**

Azure Backup usa el agente de Microsoft Azure Recovery Services (MARS) para realizar copias de seguridad de archivos, carpetas y datos del sistema de las máquinas locales y las máquinas virtuales de Azure. El agente de MARS es un agente completo que ofrece muchas ventajas para realizar copias de seguridad y restaurar los datos.



**Aspectos que debe saber sobre el agente de MARS**

Vamos a revisar algunas de las características del agente de MARS.

* Azure Backup para archivos y carpetas se basa en el agente de MARS que se va a instalar en el cliente de Windows o Windows Server.
* Los datos que están disponibles para la copia de seguridad dependen de dónde instale y ejecute el agente de MARS.
* Puede realizar copias de seguridad de archivos y carpetas en máquinas virtuales o máquinas físicas Windows. Las máquinas virtuales pueden residir en el entorno local o en Azure.
* El agente de MARS no requiere un servidor de copia de seguridad independiente.
* El agente de MARS no es compatible con aplicaciones. Puede restaurar los archivos y carpetas a partir de copias de seguridad o bien realizar una restauración de nivel de volumen.

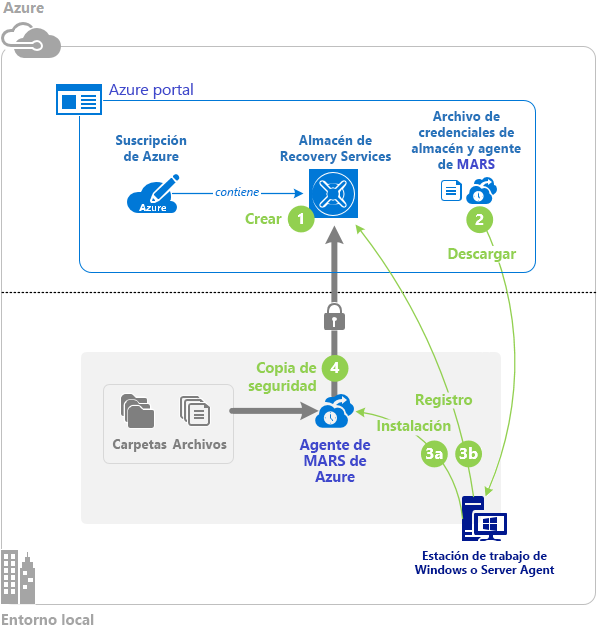
**Aspectos que debe tener en cuenta al usar el agente de MARS**

Puede implementar el agente de MARS en cualquier máquina virtual o máquina física de Windows Server. Los datos que están disponibles para la copia de seguridad dependen de dónde ejecute el agente de MARS. Hay varias maneras de ejecutar el agente de MARS.

| **Escenario de copia de seguridad** | **Implementación del agente de MARS** |
| --- | --- |
| **Copia de seguridad directa local** | *Ejecute el agente de MARS en las máquinas Windows locales para realizar una copia de seguridad de los datos de la máquina directamente en el almacén de Recovery Services en Azure*. |
| **Copia de seguridad de archivos o carpetas específicos** | *Ejecute el agente de MARS en máquinas virtuales de Azure para realizar copias de seguridad de archivos y carpetas específicos de la máquina virtual. Las máquinas virtuales de Azure deben ejecutar Windows en paralelo con la extensión Azure Virtual Machines Backup*. |
| **Copia de seguridad en MABS o System Center DPM** | *Ejecute el agente de MARS en una instancia de Microsoft Azure Backup Server (MABS) o en un servidor System Center Data Protection Manager (DPM). Realice una copia de seguridad de las máquinas y las cargas de trabajo en MABS o DPM mediante el agente de MARS para realizar copias de seguridad en un almacén de Recovery Services en Azure*. |

**Configuración de copias de seguridad de archivos y carpetas locales**

Vamos a revisar cómo usar el agente de MARS y Azure Backup para completar copias de seguridad de los archivos y carpetas locales. En el diagrama siguiente se muestran los pasos de nivel superior para usar el agente de MARS para Azure Backup.



**Paso 1: Crear almacén de Recovery Services**

El primer paso es crear un almacén de Recovery Services para las copias de seguridad. El almacén debe crearse dentro de la suscripción de Azure, como se describe en la [sección anterior](https://learn.microsoft.com/es-es/training/modules/configure-file-folder-backups/4-setup-recovery-service-vault-backup-options).

**Paso 2: Descarga del agente de MARS y el archivo de credenciales**

En el panel del Centro de copias de seguridad, la página almacén de Recovery Services proporciona un vínculo para descargar el agente de MARS (agente de Recovery Services). Para completar la instalación del agente de MARS, también debe descargar el archivo de *credenciales del almacén*. Para obtener más información, consulte [Descarga del agente de MARS](https://learn.microsoft.com/es-es/azure/backup/install-mars-agent#download-the-mars-agent).

**Paso 3: Instalación y registro del agente de MARS**

El instalador del agente de MARS proporciona un asistente para configurar la ubicación de instalación, el servidor proxy y la información de la frase de contraseña. El archivo de credenciales descargado se usa para registrar el agente. El agente de MARS se instala en el equipo local.

**Importante**

Debe instalar la última versión del agente de MARS. Las versiones del agente de MARS anteriores a la 2.0.9083.0 deben actualizarse desinstalando el agente y volviéndolo a instalar.

**Paso 4: Configuración de copias de seguridad**

Ahora está listo para usar el agente de MARS para crear una directiva de copia de seguridad. Puede especificar cuándo se debe realizar la copia de seguridad, de qué datos se debe realizar, cuánto tiempo se deben conservar los elementos de copia de seguridad y otras opciones, como el límite de ancho de banda.

**Prueba de conocimientos**

Su empresa se prepara para usar Azure Backup y Recovery Services para sus recursos compartidos de archivos de Azure Files. Necesitan asegurarse de que la información crítica se pueda recuperar y proteger frente a errores. Está reuniendo el plan de configuración, incluidas las directivas de copia de seguridad y restauración para el cumplimiento normativo. Algunos equipos han enviado sus requisitos de configuración y sus preguntas para que los evalúe:

* El administrador de infraestructuras ha solicitado un resumen ejecutivo sobre Azure Backup.
* El departamento de facturación quiere saber si se deben comprar otros servicios de Azure como parte de la implementación de Azure Backup.
* El equipo de administración necesita un diagrama de flujo de los pasos para realizar copias de seguridad de los archivos y carpetas en Azure.

**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 primer paso para realizar copias de seguridad de los archivos y carpetas en Azure?**

1. Descargar el agente y el archivo de credenciales.
2. Crear el almacén de Azure Recovery Services.
3. Configurar la copia de seguridad.

**2. ¿Cuál de los servicios siguientes requiere Azure Backup?**

1. Un servidor de copia de seguridad dedicado.
2. Un contenedor de Azure Blob Storage.
3. Un almacén de Azure Recovery Services.

**3. ¿Qué opción describe con precisión Azure Backup?**

1. Azure Backup tiene una transferencia de datos ilimitados.
2. Azure Backup no proporciona cifrado de datos.
3. Azure Backup solo se puede utilizar en máquinas virtuales en la nube.
4. Final del formulario
5. B
6. C
7. A

**Resumen y recursos**

La copia de seguridad de recursos compartidos de archivos de Azure Files es una solución de copia de seguridad nativa basada en la nube que protege los datos en la nube. Azure Backup elimina la sobrecarga de mantenimiento adicional implicada en las soluciones de copia de seguridad locales. El servicio Azure Backup se integra fácilmente con Azure File Sync. Puede centralizar los datos de recursos compartidos de archivos junto con las copias de seguridad.

En este módulo, ha identificado las características y los casos de uso de Azure Backup. Ha revisado cómo crear y configurar opciones de copia de seguridad para un almacén de Azure Recovery Services. Ha explorado cómo implementar copias de seguridad de carpetas y archivos locales. Ha descubierto cómo configurar el agente de Microsoft Azure Recovery Services (MARS).