Descripción general de las funciones en Azure Backup

Azure Backup es el servicio basado en Azure que puede usar para realizar una copia de seguridad (o proteger) y restaurar sus datos en la nube de Microsoft. Azure Backup reemplaza su solución de respaldo local o fuera de sitio existente con una solución basada en la nube que es confiable, segura y competitiva en costos. Azure Backup ofrece múltiples componentes que descarga e implementa en la computadora, el servidor o la nube apropiados. El componente o agente que implementa depende de lo que desea proteger. Todos los componentes de Azure Backup (independientemente de si está protegiendo los datos en las instalaciones o en la nube) pueden utilizarse para hacer una copia de seguridad de los datos en una bóveda de Servicios de recuperación en Azure. Consulte la tabla de componentes de copia de seguridad de Azure (más adelante en este artículo) para obtener información sobre qué componente usar para proteger datos, aplicaciones o cargas de trabajo específicos.

Vea una descripción general de video de Azure Backup

¿Por qué usar Azure Backup?

Las soluciones de copia de seguridad tradicionales han evolucionado para tratar la nube como un punto final o destino de almacenamiento estático, similar a los discos o cintas. Si bien este enfoque es simple, es limitado y no aprovecha al máximo una plataforma en la nube subyacente, lo que se traduce en una solución costosa e ineficiente. Otras soluciones son costosas porque terminas pagando por el tipo de almacenamiento o almacenamiento incorrecto que no necesitas. Otras soluciones a menudo son ineficientes porque no le ofrecen el tipo o la cantidad de almacenamiento que necesita, o las tareas administrativas requieren demasiado tiempo. Por el contrario, Azure Backup ofrece estos beneficios clave:

Gestión automática de almacenamiento : los entornos híbridos a menudo requieren un almacenamiento heterogéneo, algunos en las instalaciones y otros en la nube. Con Azure Backup, no hay costo para usar dispositivos de almacenamiento locales. Azure Backup asigna y administra automáticamente el almacenamiento de la copia de seguridad, y utiliza un modelo de pago según uso. Pay-as-you-use significa que solo paga por el almacenamiento que consume. Para obtener más información, consulte el artículo sobre precios de Azure .

Escalado ilimitado : Azure Backup usa la potencia subyacente y la escala ilimitada de la nube de Azure para ofrecer alta disponibilidad, sin gastos de mantenimiento ni supervisión. Puede configurar alertas para proporcionar información sobre eventos, pero no necesita preocuparse por la alta disponibilidad de sus datos en la nube.

Múltiples opciones de almacenamiento : un aspecto de alta disponibilidad es la replicación de almacenamiento. Azure Backup ofrece dos tipos de replicación: almacenamiento localmente redundante y almacenamiento geo redundante . Elija la opción de almacenamiento de respaldo según la necesidad:

- El almacenamiento localmente redundante (LRS) replica sus datos tres veces (crea tres copias de sus datos) en un centro de datos emparejado en la misma región. LRS es una opción de bajo costo para proteger sus datos de fallas de hardware local.
- El almacenamiento redundante geográfico (GRS) replica sus datos en una región secundaria (a cientos de millas de distancia de la ubicación principal de los datos de origen). GRS cuesta más que LRS, pero GRS proporciona un mayor nivel de durabilidad para sus datos, incluso si hay una interrupción regional.

Transferencia de datos ilimitada : Azure Backup no limita la cantidad de datos entrantes o salientes que transfiere. Azure Backup tampoco carga los datos que se transfieren. Sin embargo, si utiliza el servicio Importación / Exportación de Azure para importar grandes cantidades de datos, existe un costo asociado con los datos entrantes. Para obtener más información sobre este costo, consulte Flujo de trabajo de copia de seguridad sin conexión en Azure Backup . Los datos de salida se refieren a los datos transferidos desde una bóveda de Servicios de recuperación durante una operación de restauración.1

Cifrado de datos: el cifrado de datos permite la transmisión y el almacenamiento seguro de sus datos en la nube pública. Almacena la frase de cifrado localmente y nunca se transmite ni almacena en Azure. Si es necesario restaurar alguno de los datos, solo tiene frase de contraseña de cifrado o clave.

Copia de seguridad consistente con la aplicación : ya sea para hacer una copia de seguridad de un servidor de archivos, una máquina virtual o una base de datos SQL, necesita saber que un punto de recuperación tiene todos los datos necesarios para restaurar la copia de seguridad. Azure Backup proporciona copias de seguridad coherentes con las aplicaciones, lo que garantiza que no se necesitan soluciones adicionales para restaurar los datos. La restauración de los datos consistentes de la aplicación reduce el tiempo de restauración, lo que le permite regresar rápidamente al estado de ejecución.

Retención a largo plazo : en lugar de cambiar copias de seguridad de un disco a cinta y mover la cinta a una ubicación externa, puede usar Azure para la retención a corto y largo plazo. Azure no limita la cantidad de tiempo que los datos permanecen en una bóveda de Servicios de copia de seguridad o recuperación. Puede mantener los datos en una bóveda durante el tiempo que desee. Azure Backup tiene un límite de 9999 puntos de recuperación por instancia protegida. Consulte la sección Copia de seguridad y retención en este artículo para obtener una explicación de cómo este límite puede afectar sus necesidades de copia de seguridad.

¿Qué componentes de Azure Backup debo usar?

Si no está seguro de qué componente de Azure Backup funciona para sus necesidades, consulte la siguiente tabla para obtener información sobre lo que puede proteger con cada componente. Azure Portal proporciona un asistente, que está integrado en el portal, para guiarlo a través de la elección del componente para descargar e implementar. El asistente, que es parte de la creación de la bóveda de Servicios de recuperación, lo guía por los pasos para seleccionar un objetivo de copia de seguridad y elegir los datos o la aplicación que desea proteger.1

Componente	Beneficios	Límites	¿Qué está protegido?	¿Dónde están almacenadas las copias de seguridad?
Agente de copia de seguridad de Azure (MARS)	• Copia de seguridad de archivos y carpetas en el sistema operativo Windows físico o virtual (las máquinas virtuales pueden ser locales o en Azure) • No se requiere servidor de respaldo por separado.	• Copia de seguridad 3 veces por día • No es consciente de la aplicación; solo archivo, carpeta y restauración de nivel de volumen, • Sin soporte para Linux.	• Archivos, • Carpetas, • Estado del sistema	Bóveda de servicios de recuperación
System Center DPM	• Instantáneas con reconocimiento de aplicaciones (VSS) • Flexibilidad total para cuando tomar copias de seguridad • Granularidad de recuperación (todos) • Puede usar la bóveda de Servicios de recuperación • Soporte de Linux en VM de Hyper-V y VMware	No se puede realizar una copia de seguridad de la carga de trabajo de Oracle.	• Archivos, • Carpetas, • Volúmenes, • VMs, • Aplicaciones, • Cargas de trabajo	• Bóveda de servicios de recuperación, • Disco conectado localmente • Cinta (solo local)

Componente	Beneficios	Límites	¿Qué está protegido?	¿Dónde están almacenadas las copias de seguridad?
	• Copia de seguridad y restauración de VMware VM utilizando DPM 2012 R2			
Servidor de copia de seguridad Azure	• Instantáneas con reconocimiento de aplicaciones (VSS) • Flexibilidad total para cuando tomar copias de seguridad • Granularidad de recuperación (todos) • Puede usar la bóveda de Servicios de recuperación • Soporte de Linux en VM de Hyper-V y VMware • Copia de seguridad y restauración de VMware VM • No requiere una licencia de System Center	• No se puede realizar una copia de seguridad de la carga de trabajo de Oracle. • Siempre requiere suscripción de Azure en vivo • No se admite la copia de seguridad en cinta	• Archivos, • Carpetas, • Volúmenes, • VMs, • Aplicaciones, • Cargas de trabajo	• Bóveda de servicios de recuperación, • Disco adjunto localmente

Componente	Beneficios	Límites	¿Qué está protegido?	¿Dónde están almacenadas las copias de seguridad?
Azure IaaS VM Backup	• Copias de seguridad nativas para Windows / Linux • No se requiere instalación específica del agente • Copia de seguridad a nivel de la estructura sin necesidad de una infraestructura de respaldo	• Copia de seguridad de máquinas virtuales una vez al día • Restaurar máquinas virtuales solo a nivel de disco • No se puede realizar una copia de seguridad en las instalaciones	• VMs, • Todos los discos (usando PowerShell)	Bóveda de servicios de recuperación

¿Cuáles son los escenarios de implementación para cada componente?

Componente	¿Se puede implementar en Azure?	¿Se puede implementar en las instalaciones?	Soporte de almacenamiento de destino
Agente de copia de seguridad de Azure (MARS)	**Sí** El agente de copia de seguridad de Azure se puede implementar	**Sí** El agente de respaldo se puede implementar en	Bóveda de servicios de recuperación

Componente	¿Se puede implementar en Azure?	¿Se puede implementar en las instalaciones?	Soporte de almacenamiento de destino
	en cualquier máquina virtual de Windows Server que se ejecute en Azure.	cualquier VM de Windows Server o máquina física.3	
System Center DPM	**Sí** Obtenga más información sobre cómo proteger cargas de trabajo en Azure utilizando System Center DPM .	**Sí** Obtenga más información sobre cómo proteger las cargas de trabajo y las máquinas virtuales en su centro de datos .	Disco conectado localmente Bóveda de servicios de recuperación, cinta (solo local)
Servidor de copia de seguridad Azure	**Sí** Obtenga más información acerca de cómo proteger las cargas de trabajo en Azure utilizando Azure Backup Server .	**Sí** Obtenga más información acerca de cómo proteger las cargas de trabajo en Azure utilizando Azure Backup Server .	Disco conectado localmente Bóveda de servicios de recuperación
Azure IaaS VM Backup	**Sí** Parte de la tela Azure	**No** Use System Center DPM para hacer una copia de seguridad	Bóveda de servicios de recuperación

Componente	¿Se puede implementar en Azure?	¿Se puede implementar en las instalaciones?	Soporte de almacenamiento de destino
	Especializado para la copia de seguridad de máquinas virtuales de infraestructura como servicio (IaaS) de Azure .	de las máquinas virtuales en su centro de datos.	

¿Qué aplicaciones y cargas de trabajo se pueden respaldar?

La siguiente tabla proporciona una matriz de datos y cargas de trabajo que se pueden proteger utilizando Azure Backup. La columna de la solución Azure Backup tiene enlaces a la documentación de implementación para esa solución.

Datos o carga de trabajo	Entorno de origen	Solución de copia de seguridad de Azure
Archivos y carpetas	Servidor de windows	Agente de copia de seguridad de Azure , System Center DPM (+ agente de Azure Backup), Azure Backup Server (incluye el agente de Azure Backup)

Datos o carga de trabajo	Entorno de origen	Solución de copia de seguridad de Azure
Archivos y carpetas	Computadora con Windows	Agente de copia de seguridad de Azure , System Center DPM (+ agente de Azure Backup), Azure Backup Server (incluye el agente de Azure Backup)
Máquina virtual Hyper-V (Windows)	Servidor de windows	System Center DPM (+ agente de Azure Backup), Azure Backup Server (incluye el agente de Azure Backup)
Máquina virtual Hyper-V (Linux)	Servidor de windows	System Center DPM (+ agente de Azure Backup), Azure Backup Server (incluye el agente de Azure Backup)
Máquina virtual VMware	Servidor de windows	System Center DPM (+ agente de Azure Backup), Azure Backup Server (incluye el agente de Azure Backup)

Datos o carga de trabajo	Entorno de origen	Solución de copia de seguridad de Azure
Microsoft SQL Server	Servidor de windows	System Center DPM (+ agente de Azure Backup), Azure Backup Server (incluye el agente de Azure Backup)
Microsoft SharePoint	Servidor de windows	System Center DPM (+ agente de Azure Backup), Azure Backup Server (incluye el agente de Azure Backup)
Microsoft Exchange	Servidor de windows	System Center DPM (+ agente de Azure Backup), Azure Backup Server (incluye el agente de Azure Backup)
Máquinas virtuales IaaS de Azure (Windows)	corriendo en Azure	Azure Backup (extensión de VM)
Máquinas virtuales Azure IaaS (Linux)	corriendo en Azure	Azure Backup (extensión de VM)

Soporte de Linux

La siguiente tabla muestra los componentes de Azure Backup que tienen soporte para Linux.

Componente	Soporte de Linux (respaldado por Azure)
Agente de copia de seguridad de Azure (MARS)	No (solo agente basado en Windows)
System Center DPM	• Copia de seguridad consistente de archivos de máquinas virtuales invitadas de Linux en Hyper-V y VMWare • Restauración de máquina virtual VM de Hyper-V y VMWare VM *La copia de seguridad compatible con archivos no está disponible para Azure VM*
Servidor de copia de seguridad Azure	• Copia de seguridad consistente de archivos de máquinas virtuales invitadas de Linux en Hyper-V y VMWare • Restauración de máquina virtual VM de Hyper-V y VMWare VM *La copia de seguridad compatible con archivos no está disponible para Azure VM*
Azure IaaS VM Backup	Copia de seguridad coherente con la aplicación utilizando el marco de trabajo anterior al script y post-script Recuperación de archivos granulares Restauración de todos los discos VM Restauración de VM

Uso de máquinas virtuales de almacenamiento premium con Azure Backup

Azure Backup protege las máquinas virtuales de almacenamiento Premium. Azure Premium Storage es un almacenamiento basado en unidades de estado sólido (SSD) diseñado para soportar cargas de trabajo intensivas de E / S. El almacenamiento premium es atractivo para las cargas de trabajo de máquinas virtuales (VM). Para obtener más información sobre Almacenamiento Premium, consulte el artículo Almacenamiento Premium: Almacenamiento de alto rendimiento para cargas de trabajo de máquinas virtuales Azure .

Copia de seguridad de máquinas virtuales de almacenamiento premium

Al realizar una copia de seguridad de las máquinas virtuales de almacenamiento Premium, el servicio de copia de seguridad crea una ubicación temporal provisional, denominada "AzureBackup-", en la cuenta de Almacenamiento Premium. El tamaño de la ubicación de ensayo es igual al tamaño de la instantánea del punto de recuperación. Asegúrese de que la cuenta de Almacenamiento Premium tenga suficiente espacio libre para acomodar la ubicación temporal de almacenamiento. Para obtener más información, consulte el artículo, limitaciones de almacenamiento premium . Una vez que la tarea de copia de seguridad finaliza, la ubicación provisional se elimina. El precio de almacenamiento utilizado para la ubicación de almacenamiento es coherente con todos los precios de almacenamiento Premium .

Nota

No modifique ni edite la ubicación de ensayo.

Restaurar máquinas virtuales de almacenamiento premium

Las máquinas virtuales de almacenamiento premium pueden restaurarse en Almacenamiento Premium o en almacenamiento normal. Restaurar un punto de recuperación de VM de Almacenamiento Premium de regreso a Almacenamiento Premium es el proceso típico de restauración. Sin embargo, puede ser rentable restaurar un punto de recuperación de VM de Almacenamiento Premium a almacenamiento estándar. Este tipo de restauración se puede usar si necesita un subconjunto de archivos de la máquina virtual.

Uso de máquinas virtuales de disco administradas con Azure Backup

Azure Backup protege las máquinas virtuales de disco administradas. Los discos administrados le permiten administrar cuentas de almacenamiento de máquinas virtuales y simplificar enormemente el aprovisionamiento de VM.

Copia de seguridad de máquinas virtuales de disco administradas

Realizar copias de seguridad de máquinas virtuales en discos administrados no es diferente de hacer copias de seguridad de las máquinas virtuales de Resource Manager. En Azure Portal, puede configurar el trabajo de copia de seguridad directamente desde la vista de máquina virtual o desde la vista de bóveda de Servicios de recuperación. Puede realizar una copia de seguridad de las máquinas virtuales en los discos administrados a través de las colecciones de RestorePoint creadas sobre los discos administrados. Azure Backup también admite la copia de seguridad de máquinas virtuales de disco administradas cifradas mediante el cifrado de disco Azure (ADE).

Restaurar máquinas virtuales de disco administradas

Azure Backup le permite restaurar una VM completa con discos administrados, o restaurar discos administrados a una cuenta de almacenamiento. Azure administra los discos administrados durante el proceso de restauración. Usted (el cliente) administra la cuenta de almacenamiento creada como parte del proceso de restauración. Al restaurar máquinas virtuales encriptadas administradas, las claves y los secretos de la máquina virtual deben existir en la bóveda de claves antes de iniciar la operación de restauración.

¿Cuáles son las características de cada componente de respaldo?

Las siguientes secciones proporcionan tablas que resumen la disponibilidad o el soporte de varias características en cada componente de Azure Backup. Consulte la información que sigue a cada tabla para obtener ayuda o detalles adicionales.

Almacenamiento

Característica	Agente de copia de seguridad de Azure	System Center DPM	Servidor de copia de seguridad Azure	Azure IaaS VM Backup
Bóveda de servicios de recuperación				
Almacenamiento de disco				
Almacenamiento en cinta				
Compresión (en la bóveda de Servicios de recuperación)				
Respaldo incremental				
Deduplicación de disco				

La bóveda de Servicios de recuperación es el destino de almacenamiento preferido para todos los componentes. System Center DPM y Azure Backup Server también ofrecen la opción de tener una copia de disco local. Sin embargo, solo System Center DPM brinda la opción de escribir datos en un dispositivo de almacenamiento en cinta.

Compresión

Las copias de seguridad se comprimen para reducir el espacio de almacenamiento requerido. El único componente que no usa compresión es la extensión de VM. La extensión de VM copia todos los datos de copia de seguridad desde su cuenta de almacenamiento a la bóveda de Servicios de recuperación en la misma región. No se usa compresión al transferir los datos. La transferencia de datos sin compresión infla ligeramente el almacenamiento utilizado. Sin embargo, almacenar los datos sin compresión permite una restauración más rápida, en caso de que necesite ese punto de recuperación.

Desduplicación de disco

Puede aprovechar la deduplicación cuando implementa System Center DPM o Azure Backup Server en una máquina virtual Hyper-V . Windows Server realiza la deduplicación de datos (a nivel de host) en discos duros virtuales (VHD) que están conectados a la máquina virtual como almacenamiento de respaldo.

Nota

La desduplicación no está disponible en Azure para ningún componente de copia de seguridad. Cuando System Center DPM y Backup Server se implementan en Azure, los discos de almacenamiento conectados a la VM no se pueden deduplicar.

Copia incremental explicada

Todos los componentes de Azure Backup admiten copia de seguridad incremental independientemente del almacenamiento de destino (disco, cinta, bóveda de Servicios de recuperación). La copia de seguridad incremental asegura que las copias de seguridad sean eficientes en el almacenamiento y el tiempo, al transferir solo los cambios realizados desde la última copia de seguridad.

Comparación de copia de seguridad completa, diferencial e incremental

El consumo de almacenamiento, el objetivo de tiempo de recuperación (RTO) y el consumo de red varían para cada tipo de método de respaldo. Para mantener bajo el costo total de propiedad (TCO) de la copia de seguridad, debe comprender cómo elegir la mejor solución de respaldo. La siguiente imagen compara copia de seguridad completa, copia de seguridad diferencial y copia de seguridad incremental. En la imagen, la fuente de datos A está compuesta por 10 bloques de almacenamiento A1-A10, que se respaldan mensualmente. Los bloques A2, A3, A4 y A9 cambian en el primer mes y el bloque A5 cambia en el mes siguiente.

Con **Full Backup** , cada copia de seguridad contiene todo el origen de datos. La copia de seguridad completa consume una gran cantidad de ancho de banda de red y almacenamiento, cada vez que se transfiere una copia de seguridad.

La copia de seguridad diferencial almacena solo los bloques que cambiaron desde la copia de seguridad completa inicial, lo que da como resultado una menor cantidad de consumo de red y almacenamiento. Las copias de seguridad diferenciales no retienen copias redundantes de datos sin cambios. Sin embargo, dado que los bloques de datos que permanecen sin cambios entre las copias de seguridad posteriores se transfieren y almacenan, las copias de seguridad diferenciales son ineficientes. En el segundo mes, se realizan copias de seguridad de los bloques modificados A2, A3, A4 y A9. En el tercer mes, estos mismos bloques se respaldan nuevamente, junto con el bloque modificado A5. Los bloques modificados se seguirán respaldando hasta que se realice la siguiente copia de seguridad completa.

Incremental Backup logra un alto almacenamiento y eficiencia de red al almacenar solo los bloques de datos que cambiaron desde la copia de seguridad anterior. Con la copia de seguridad incremental, no es necesario realizar copias de seguridad completas regulares. En el ejemplo, después de tomar la copia de seguridad completa durante el primer mes, los bloques modificados A2, A3, A4 y A9 se marcan como cambiados y se transfieren durante el segundo mes. En el tercer mes, el único bloque modificado A5 se marca y transfiere. Mover menos datos ahorra almacenamiento y recursos de red, lo que reduce el TCO.

Seguridad

Característica	Agente de copia de seguridad de Azure	System Center DPM	Servidor de copia de seguridad Azure	Azure IaaS VM Backup
Seguridad de red (a Azure)				
Seguridad de datos (en Azure)				

Seguridad de la red

Todo el tráfico de respaldo de sus servidores a la bóveda de Servicios de recuperación se cifra con el Estándar de cifrado avanzado 256. Los datos de la copia de seguridad se envían a través de un enlace HTTPS seguro. Los datos de la copia de seguridad también se almacenan en la bóveda de Servicios de recuperación en forma cifrada. Solo usted, el cliente de Azure, tiene la frase de contraseña para desbloquear esta información. Microsoft no puede descifrar los datos de copia de seguridad en ningún momento.

Advertencia

Una vez que establezca la bóveda de Servicios de recuperación, solo usted tendrá acceso a la clave de cifrado. Microsoft nunca mantiene una copia de su clave de cifrado y no tiene acceso a la clave. Si la clave está fuera de lugar, Microsoft no puede recuperar los datos de la copia de seguridad.

Seguridad de datos

La copia de seguridad de las máquinas virtuales Azure requiere la configuración del cifrado *dentro de* la máquina virtual. Use BitLocker en máquinas virtuales Windows y **dm-crypt** en máquinas virtuales Linux. Azure Backup no encripta automáticamente los datos de respaldo que provienen de esta ruta.

Red

Característica	Agente de copia de seguridad de Azure	System Center DPM	Servidor de copia de seguridad Azure	Azure IaaS VM Backup
Compresión de red (al **servidor de copia** de**seguridad**)				

Característica	Agente de copia de seguridad de Azure	System Center DPM	Servidor de copia de seguridad Azure	Azure IaaS VM Backup
Compresión de red (a la **bóveda de Servicios de recuperación**)				
Protocolo de red (al **servidor de respaldo**)		TCP	TCP	
Protocolo de red (a la **bóveda de Servicios de recuperación**)	HTTPS	HTTPS	HTTPS	HTTPS

La extensión de VM (en IaaS VM) lee los datos directamente de la cuenta de almacenamiento de Azure a través de la red de almacenamiento, por lo que no es necesario comprimir este tráfico.

Si utiliza un servidor System Center DPM o Azure Backup Server como servidor de copia de seguridad secundario, comprima los datos que van desde el servidor primario hasta el servidor de respaldo. Comprimir datos antes de realizar una copia de seguridad en DPM o Azure Backup Server, ahorra ancho de banda.

Red de regulación

El agente de Azure Backup ofrece aceleración de red, que le permite controlar cómo se usa el ancho de banda de la red durante la transferencia de datos. La limitación puede ser útil si necesita hacer una copia de seguridad de los datos durante las horas de trabajo, pero no desea que el proceso de copia de seguridad interfiera con el resto del tráfico de Internet. La limitación para la transferencia de datos se aplica a las actividades de copia de seguridad y restauración.

Respaldo y retención

Azure Backup tiene un límite de 9999 puntos de recuperación, también conocidos como copias de seguridad o instantáneas, por *instancia protegida* . Una instancia protegida es una computadora, servidor (físico o virtual) o carga de trabajo configurada para hacer una copia de seguridad de los datos en Azure. Para obtener más información, consulte la sección ¿Qué es una instancia protegida?. Una instancia está protegida una vez que se ha guardado una copia de seguridad de los datos. La copia de seguridad de los datos es la protección. Si los datos de origen se perdieron o se dañaron, la copia de seguridad podría restaurar los datos de origen. La siguiente tabla muestra la frecuencia de copia de seguridad máxima para cada componente. La configuración de su política de respaldo determina la rapidez con la que consume los puntos de recuperación. Por ejemplo, si crea un punto de recuperación cada día, puede retener los puntos de recuperación durante 27 años antes de que se agote. Si toma un punto de recuperación mensual, puede retener puntos de recuperación durante 833 años antes de que se agote. El servicio de copia de seguridad no establece un límite de tiempo de caducidad en un punto de recuperación.

	Agente de copia de seguridad de Azure	**System Center DPM**	**Servidor de copia de seguridad Azure**	**Azure IaaS VM Backup**
Frecuencia de respaldo (a la bóveda de Servicios de recuperación)	Tres copias de seguridad por día	Dos copias de seguridad por día	Dos copias de seguridad por día	Una copia de seguridad por día

	Agente de copia de seguridad de Azure	System Center DPM	Servidor de copia de seguridad Azure	Azure IaaS VM Backup
Frecuencia de respaldo (en disco)	No aplica	• Cada 15 minutos para SQL Server • Cada hora para otras cargas de trabajo	• Cada 15 minutos para SQL Server • Cada hora para otras cargas de trabajo	No aplica
Opciones de retención	Diaria, semanal, mensual, anual	Diaria, semanal, mensual, anual	Diaria, semanal, mensual, anual	Diaria, semanal, mensual, anual
Puntos de recuperación máximos por instancia protegida	9999	9999	9999	9999
Periodo máximo de retención	Depende de la frecuencia de respaldo	Depende de la frecuencia de respaldo	Depende de la frecuencia de respaldo	Depende de la frecuencia de respaldo
Puntos de recuperación en el disco local	No aplica	• 64 para servidores de archivos, • 448 para servidores de aplicaciones	• 64 para servidores de archivos, • 448 para servidores de aplicaciones	No aplica

	Agente de copia de seguridad de Azure	System Center DPM	Servidor de copia de seguridad Azure	Azure IaaS VM Backup
Puntos de recuperación en cinta	No aplica	Ilimitado	No aplica	No aplica

¿Qué es una instancia protegida?

Una instancia protegida es una referencia genérica a una computadora con Windows, un servidor (físico o virtual) o una base de datos SQL que se ha configurado para realizar una copia de seguridad en Azure. Una instancia se protege una vez que configura una política de respaldo para la computadora, servidor o base de datos, y crea una copia de seguridad de los datos. Las copias subsiguientes de los datos de copia de seguridad para esa instancia protegida (que se llaman puntos de recuperación) aumentan la cantidad de almacenamiento consumido. Puede crear hasta 9999 puntos de recuperación para una instancia protegida. Si elimina un punto de recuperación del almacenamiento, no cuenta contra el total de 9999 puntos de recuperación. Algunos ejemplos comunes de instancias protegidas son máquinas virtuales, servidores de aplicaciones, bases de datos y computadoras personales que ejecutan el sistema operativo Windows. Por ejemplo:

- Una máquina virtual que ejecuta el hipervisor Hyper-V o Azure IaaS. Los sistemas operativos invitados para la máquina virtual pueden ser Windows Server o Linux.
- Un servidor de aplicaciones: el servidor de aplicaciones puede ser una máquina física o virtual que ejecuta Windows Server y cargas de trabajo con datos de los que se debe realizar una copia de seguridad. Las cargas de trabajo comunes son Microsoft SQL Server, el servidor de Microsoft Exchange, el servidor de Microsoft SharePoint y el rol del servidor de archivos en Windows Server. Para realizar una copia de seguridad de estas cargas de trabajo, necesita el Administrador de protección de datos de System Center (DPM) o el Servidor de copia de seguridad de Azure.

- Una computadora personal, estación de trabajo o computadora portátil con el sistema operativo Windows.

¿Qué es una bóveda de Servicios de recuperación?

Una bóveda de Servicios de recuperación es una entidad de almacenamiento en línea de Azure que se utiliza para almacenar datos como copias de seguridad, puntos de recuperación y políticas de respaldo. Puede usar las bóvedas de los Servicios de recuperación para mantener los datos de respaldo de los servicios de Azure y los servidores y estaciones de trabajo locales. Las bóvedas de los Servicios de recuperación facilitan la organización de los datos de la copia de seguridad y minimizan la sobrecarga de administración. Puede crear tantas bóvedas de Servicios de recuperación como desee, dentro de una suscripción.

Las bóvedas de copia de seguridad, que se basan en Azure Service Manager, fueron la primera versión de la bóveda. Las bóvedas de los Servicios de recuperación, que agregan las características del modelo de Azure Resource Manager, son la segunda versión de la bóveda. Consulte el artículo de descripción general de la bóveda de Servicios de recuperación para obtener una descripción completa de las diferencias de características. Ya no puede crear el uso del portal para crear bóvedas de respaldo, pero las bóvedas de respaldo aún son compatibles. Debe usar el portal de Azure para administrar sus bóvedas de respaldo.

Importante

Puede actualizar sus bóvedas de Respaldo a bóvedas de Servicios de Recuperación. Para obtener detalles, consulte el artículo **Actualizar una bóveda de respaldo a una bóveda de Servicios de recuperación** . Microsoft lo alienta a actualizar sus bóvedas de seguridad a bóvedas de Servicios de recuperación.
Después del 30 de noviembre de 2017, ya no podrá usar PowerShell para crear bóvedas de respaldo y todas las bóvedas de respaldo restantes se actualizarán automáticamente a las bóvedas de los Servicios de recuperación.

¿En qué se diferencia Azure Backup de Azure Site Recovery?

Azure Backup y Azure Site Recovery están relacionados porque los servicios respaldan los datos y pueden restaurarlos. Sin embargo, estos servicios tienen diferentes propósitos para proporcionar continuidad comercial y recuperación ante desastres en su negocio. Use Azure Backup para proteger y restaurar datos en un nivel más granular. Por ejemplo, si se daña una presentación en una computadora portátil, debe usar Azure Backup para restaurar la presentación. Si desea replicar la configuración y los datos en una VM en otro centro de datos, use Azure Site Recovery.

Azure Backup protege los datos locales y en la nube. Azure Site Recovery coordina la replicación de máquina virtual y servidor físico, failover y failback. Ambos servicios son importantes porque su solución de recuperación ante desastres necesita mantener sus datos seguros y recuperables (Copia de seguridad) *y* mantener sus cargas de trabajo disponibles (Recuperación del sitio) cuando ocurren interrupciones.

Los siguientes conceptos pueden ayudarlo a tomar decisiones importantes sobre respaldo y recuperación ante desastres.

Concepto	Detalles	Apoyo	Recuperación de desastres (DR)
Objetivo de punto de recuperación (RPO)	La cantidad de pérdida de datos aceptable si es necesario realizar una recuperación.	Las soluciones de respaldo tienen una amplia variabilidad en su RPO aceptable.Las copias de seguridad de máquinas virtuales generalmente tienen un RPO de un día, mientras que las copias de seguridad de la base de datos tienen RPO de tan solo 15 minutos.	Las soluciones de recuperación de desastres tienen bajos RPO. La copia de DR puede estar retrasada unos segundos o unos minutos.
Objetivo de tiempo de recuperación (RTO)	La cantidad de tiempo que lleva completar una recuperación o restauración.	Debido al RPO más grande, la cantidad de datos que una solución de respaldo necesita procesar suele ser mucho mayor, lo que lleva a RTO más largos. Por ejemplo,	Las soluciones de recuperación de desastres tienen RTO más pequeños porque están más sincronizados con la fuente. Se necesitan procesar menos cambios.

Concepto	Detalles	Apoyo	Recuperación de desastres (DR)
		puede llevar días restaurar los datos de las cintas, según el tiempo que lleve transportar la cinta desde una ubicación externa.	
Retencion	Cuánto tiempo se deben almacenar los datos	Para escenarios que requieren recuperación operativa (corrupción de datos, borrado inadvertido de archivos, falla del sistema operativo), los datos de copia de seguridad generalmente se conservan durante 30 días o menos. Desde el punto de vista del cumplimiento, es posible que los datos deban almacenarse durante meses o incluso años. Los datos de respaldo son ideales para archivar en tales casos.	La recuperación de desastres solo necesita datos de recuperación operacional, lo que generalmente toma algunas horas o hasta un día. Debido a la captura de datos de grano fino utilizada en las soluciones DR, no se recomienda el uso de datos DR para la retención a largo plazo.

Próximos pasos