



Estrategia de respaldo para recursos de SQL Server

SnapCenter software

NetApp

November 06, 2025

Tabla de contenidos

Estrategia de respaldo para recursos de SQL Server	1
Definir una estrategia de respaldo para los recursos de SQL Server	1
Tipo de backups admitido	1
Programaciones de copias de seguridad para el complemento para SQL Server	3
Número de trabajos de respaldo necesarios para las bases de datos	4
Convenciones de nombres de copias de seguridad para el complemento para SQL Server	4
Opciones de retención de copias de seguridad para el complemento para SQL Server	5
¿Durante cuánto tiempo se deben conservar las copias de seguridad del registro de transacciones en el sistema de almacenamiento de origen?	5
Varias bases de datos en el mismo volumen	5
Verificación de copia de seguridad mediante el volumen de almacenamiento principal o secundario para el complemento para SQL Server	6
Cuándo programar trabajos de verificación	6

Estrategia de respaldo para recursos de SQL Server

Definir una estrategia de respaldo para los recursos de SQL Server

Definir una estrategia de respaldo antes de crear sus trabajos de respaldo le ayudará a garantizar que tenga los respaldos que necesita para restaurar o clonar con éxito sus bases de datos. Su acuerdo de nivel de servicio (SLA), su objetivo de tiempo de recuperación (RTO) y su objetivo de punto de recuperación (RPO) determinan en gran medida su estrategia de respaldo.

Un SLA define el nivel de servicio esperado y aborda muchas cuestiones relacionadas con el servicio, incluida la disponibilidad y el rendimiento del servicio. El RTO es el tiempo en el que se debe restaurar un proceso comercial después de una interrupción en el servicio. Un RPO define la estrategia para la antigüedad de los archivos que deben recuperarse del almacenamiento de respaldo para que las operaciones normales se reanuden después de una falla. El SLA, RTO y RPO contribuyen a la estrategia de respaldo.

Tipo de backups admitido

Para realizar copias de seguridad de las bases de datos del sistema y del usuario de SQL Server mediante SnapCenter, es necesario elegir el tipo de recurso, como bases de datos, instancias del servidor SQL y grupos de disponibilidad (AG). Se aprovecha la tecnología de instantáneas para crear copias en línea, de solo lectura, de los volúmenes en los que residen los recursos.

Puede seleccionar la opción de solo copia para especificar que SQL Server no trunque los registros de transacciones. Debe utilizar esta opción cuando también esté administrando SQL Server con otras aplicaciones de respaldo. Mantener los registros de transacciones intactos permite que cualquier aplicación de respaldo restaure las bases de datos del sistema. Las copias de seguridad de solo copia son independientes de la secuencia de copias de seguridad programadas y no afectan los procedimientos de copia de seguridad y restauración de la base de datos.

Tipo de copia de seguridad	Descripción	Opción de solo copia con tipo de copia de seguridad
Copia de seguridad completa y copia de seguridad de registros	<p>Realiza una copia de seguridad de la base de datos del sistema y trunca los registros de transacciones.</p> <p>SQL Server trunca los registros de transacciones eliminando las entradas que ya están confirmadas en la base de datos.</p> <p>Una vez completada la copia de seguridad completa, esta opción crea un registro de transacciones que captura la información de las transacciones. Por lo general, deberías elegir esta opción. Sin embargo, si el tiempo de respaldo es corto, puede elegir no ejecutar una copia de seguridad del registro de transacciones con una copia de seguridad completa.</p> <p>No se puede crear una copia de seguridad del registro para las bases de datos del sistema master y msdb. Sin embargo, puede crear copias de seguridad de registros para la base de datos del sistema modelo.</p>	<p>Realiza una copia de seguridad de los archivos de base de datos del sistema y de los registros de transacciones sin truncar los registros.</p> <p>Una copia de seguridad de solo copia no puede servir como base diferencial o copia de seguridad diferencial y no afecta a la base diferencial. Restaurar una copia de seguridad completa de solo copia es lo mismo que restaurar cualquier otra copia de seguridad completa.</p>
Copia de seguridad completa de la base de datos	<p>Realiza una copia de seguridad de los archivos de base de datos del sistema.</p> <p>Puede crear una copia de seguridad completa de la base de datos para las bases de datos del sistema maestro, modelo y msdb.</p>	<p>Realiza una copia de seguridad de los archivos de base de datos del sistema.</p>

Tipo de copia de seguridad	Descripción	Opción de solo copia con tipo de copia de seguridad
Copia de seguridad del registro de transacciones	<p>Realiza una copia de seguridad de los registros de transacciones truncados, copiando solo las transacciones que se confirmaron desde que se realizó la copia de seguridad del registro de transacciones más reciente.</p> <p>Si programa copias de seguridad frecuentes del registro de transacciones junto con copias de seguridad completas de la base de datos, puede elegir puntos de recuperación granulares.</p>	<p>Realiza una copia de seguridad de los registros de transacciones sin truncarlos.</p> <p>Este tipo de backup no afecta la secuencia de los backups de registros regulares. Las copias de seguridad de registros de solo copia son útiles para realizar operaciones de restauración en línea.</p>

Programaciones de copias de seguridad para el complemento para SQL Server

La frecuencia de copia de seguridad (tipo de programación) se especifica en las políticas; una programación de copia de seguridad se especifica en la configuración del grupo de recursos. El factor más crítico a la hora de determinar la frecuencia o el cronograma de una copia de seguridad es la tasa de cambio del recurso y la importancia de los datos. Es posible que hagas una copia de seguridad de un recurso muy utilizado cada hora, mientras que es posible que hagas una copia de seguridad de un recurso poco utilizado una vez al día. Otros factores incluyen la importancia del recurso para su organización, su Acuerdo de Nivel de Servicio (SLA) y su Objetivo de Punto de Recuperación (RPO).

Un SLA define el nivel de servicio esperado y aborda muchas cuestiones relacionadas con el servicio, incluida la disponibilidad y el rendimiento del servicio. Un RPO define la estrategia para la antigüedad de los archivos que deben recuperarse del almacenamiento de respaldo para que las operaciones normales se reanuden después de una falla. El SLA y el RPO contribuyen a la estrategia de protección de datos.

Incluso para un recurso muy utilizado, no es necesario ejecutar una copia de seguridad completa más de una o dos veces al día. Por ejemplo, las copias de seguridad periódicas del registro de transacciones podrían ser suficientes para garantizar que tenga las copias de seguridad que necesita. Cuanto más a menudo realice copias de seguridad de sus bases de datos, menos registros de transacciones tendrá que utilizar SnapCenter en el momento de la restauración, lo que puede generar operaciones de restauración más rápidas.

Los programas de respaldo constan de dos partes, como se indica a continuación:

- Frecuencia de respaldo

La frecuencia de las copias de seguridad (con qué frecuencia se deben realizar las copias de seguridad), denominada *tipo de programación* para algunos complementos, es parte de una configuración de políticas. Puede seleccionar la frecuencia de respaldo para la política: horaria, diaria, semanal o mensual. Si no selecciona ninguna de estas frecuencias, la política creada será solo a pedido. Puede acceder a las políticas haciendo clic en **Configuración > Políticas**.

- Programaciones de copias de seguridad

Las programaciones de copias de seguridad (exactamente cuándo se deben realizar las copias de seguridad) son parte de la configuración de un grupo de recursos. Por ejemplo, si tiene un grupo de recursos que tiene una política configurada para realizar copias de seguridad semanales, puede configurar la programación para realizar copias de seguridad todos los jueves a las 10:00 p. m. Puede acceder a los programas de grupos de recursos haciendo clic en **Recursos > Grupos de recursos**.

Número de trabajos de respaldo necesarios para las bases de datos

Los factores que determinan la cantidad de trabajos de respaldo que necesita incluyen el tamaño de la base de datos, la cantidad de volúmenes utilizados, la tasa de cambio de la base de datos y su Acuerdo de Nivel de Servicio (SLA).

Para las copias de seguridad de bases de datos, la cantidad de trabajos de copia de seguridad que elija generalmente dependerá de la cantidad de volúmenes en los que colocó sus bases de datos. Por ejemplo, si coloca un grupo de bases de datos pequeñas en un volumen y una base de datos grande en otro volumen, puede crear un trabajo de respaldo para las bases de datos pequeñas y un trabajo de respaldo para la base de datos grande.

Convenciones de nombres de copias de seguridad para el complemento para SQL Server

Puede utilizar la convención de nombres de instantáneas predeterminada o utilizar una convención de nombres personalizada. La convención de nombres de copia de seguridad predeterminada agrega una marca de tiempo a los nombres de las instantáneas que le ayuda a identificar cuándo se crearon las copias.

La instantánea utiliza la siguiente convención de nombres predeterminada:

`resourcegroupname_hostname_timestamp`

Debes nombrar tus grupos de recursos de respaldo de forma lógica, como en el siguiente ejemplo:

`dts1_mach1x88_03-12-2015_23.17.26`

En este ejemplo, los elementos de sintaxis tienen los siguientes significados:

- *dts1* es el nombre del grupo de recursos.
- *mach1x88* es el nombre del host.
- *03-12-2015_23.17.26* es la fecha y la marca de tiempo.

Como alternativa, puede especificar el formato del nombre de la instantánea mientras protege recursos o grupos de recursos seleccionando **Usar formato de nombre personalizado para copia de instantánea**. Por ejemplo, `customtext_resourcegroup_policy_hostname` o `resourcegroup_hostname`. De forma predeterminada, el sufijo de marca de tiempo se agrega al nombre de la instantánea.

Opciones de retención de copias de seguridad para el complemento para SQL Server

Puede elegir la cantidad de días durante los cuales desea conservar copias de seguridad o especificar la cantidad de copias de seguridad que desea conservar, hasta un máximo de 255 copias en ONTAP . Por ejemplo, su organización podría exigirle que conserve 10 días de copias de seguridad o 130 copias de seguridad.

Al crear una política, puede especificar las opciones de retención para el tipo de copia de seguridad y el tipo de programación.

Si configura la replicación de SnapMirror , la política de retención se refleja en el volumen de destino.

SnapCenter elimina las copias de seguridad retenidas que tienen etiquetas de retención que coinciden con el tipo de programación. Si se modificó el tipo de programación del recurso o del grupo de recursos, es posible que las copias de seguridad con la etiqueta del tipo de programación anterior aún permanezcan en el sistema.



Para la retención a largo plazo de copias de seguridad, debe utilizar la copia de seguridad SnapVault .

¿Durante cuánto tiempo se deben conservar las copias de seguridad del registro de transacciones en el sistema de almacenamiento de origen?

El complemento SnapCenter para Microsoft SQL Server necesita copias de seguridad del registro de transacciones para realizar operaciones de restauración actualizadas, que restauran su base de datos a un tiempo entre dos copias de seguridad completas.

Por ejemplo, si Plug-in para SQL Server realizó una copia de seguridad completa a las 8:00 a. m. y otra copia de seguridad completa a las 5:00 p. m., podría usar la última copia de seguridad del registro de transacciones para restaurar la base de datos a cualquier momento entre las 8:00 a. m. y las 5:00 p. m. Si los registros de transacciones no están disponibles, Plug-in para SQL Server solo puede realizar operaciones de restauración en un punto en el tiempo, que restauran una base de datos al momento en que Plug-in para SQL Server completó una copia de seguridad completa.

Por lo general, se necesitan operaciones de restauración actualizadas solo por uno o dos días. De forma predeterminada, SnapCenter conserva un mínimo de dos días.

Varias bases de datos en el mismo volumen

Puede colocar todas las bases de datos en el mismo volumen, porque la política de respaldo tiene una opción para establecer el máximo de bases de datos por respaldo (el valor predeterminado es 100).

Por ejemplo, si tiene 200 bases de datos en el mismo volumen, se crean dos instantáneas con 100 bases de datos en cada una de ellas.

Verificación de copia de seguridad mediante el volumen de almacenamiento principal o secundario para el complemento para SQL Server

Puede verificar copias de seguridad en el volumen de almacenamiento principal o en el volumen de almacenamiento secundario SnapMirror o SnapVault . La verificación mediante un volumen de almacenamiento secundario reduce la carga en el volumen de almacenamiento primario.

Cuando se verifica una copia de seguridad que se encuentra en el volumen de almacenamiento primario o secundario, todas las instantáneas primarias y secundarias se marcan como verificadas.

Se requiere la licencia de SnapRestore para verificar copias de respaldo en el volumen de almacenamiento secundario SnapMirror y SnapVault .

Cuándo programar trabajos de verificación

Si bien SnapCenter puede verificar las copias de seguridad inmediatamente después de crearlas, hacerlo puede aumentar significativamente el tiempo necesario para completar el trabajo de copia de seguridad y consume muchos recursos. Por lo tanto, casi siempre es mejor programar la verificación en un trabajo separado para un momento posterior. Por ejemplo, si realiza una copia de seguridad de una base de datos a las 5:00 p. m. todos los días, puede programar que la verificación se realice una hora más tarde, a las 6:00 p. m.

Por la misma razón, normalmente no es necesario ejecutar la verificación de respaldo cada vez que se realiza una copia de seguridad. Realizar una verificación a intervalos regulares pero menos frecuentes suele ser suficiente para garantizar la integridad de la copia de seguridad. Una misma tarea de verificación puede verificar varios backups a la vez.

Información de copyright

Copyright © 2025 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.