Backup de servidores físicos con Veeam: las mejores prácticas y su configuración

Matthias Mehrtens,
Arquitecto de soluciones, Veeam Software

Hoy en día, la mayoría de las organizaciones confían en las infraestructuras de TI virtualizadas. Veeam® les ayuda a proporcionar y aumentar la Disponibilidad de las cargas de trabajo críticas que se ejecutan en sus sistemas. Debido a diversos factores, como configuraciones complejas de hardware y regulaciones de cumplimiento normativo, algunos servidores físicos no se pueden virtualizar, junto con los extremos (estaciones de trabajo y equipos portátiles) que podrían no ser protegidos en su totalidad al utilizar soluciones de backup diseñadas para sistemas virtualizados. Por lo tanto, los incidentes cotidianos, como problemas en la conexión, los fallos del hardware, la corrupción de archivos, el ransomware o incluso el robo pueden poner en riesgo los datos de una organización.

Veeam Agent *for Microsoft Windows* resuelve estos problemas ya que cierra la brecha que enfrentan algunas empresas con entornos grandes y heterogéneos y permite una mayor movilidad de cargas de trabajo al ofrecer Disponibilidad para cargas de trabajo basadas en la nube. ¡Y esto no se limita a los sistemas físicos! Veeam Agent *for Microsoft Windows* también puede manejar máquinas virtuales y aplicaciones que, por ejemplo, no admiten una snapshot de hipervisor o, por cualquier otro motivo, no se pueden proteger en la capa de virtualización.

En este documento se describen los conceptos principales detrás de Veeam Agent *for Microsoft Windows*, como la forma en que los agentes se pueden administrar de forma centralizada mediante la integración de Veeam Backup & Replication™ y mucho más.

Contenido

Dónde buscar al elegir el backup para cargas de trabajo físicas

En la actualidad, la protección de la carga de trabajo física podría considerarse una obviedad con tantos proveedores que han establecido soluciones durante años. Sin embargo, la variedad de elección NO siempre significa variedad de calidad. Hay muchos aspectos clave para la protección de datos de calidad y es difícil proporcionar protección cuando faltan algunos de esos aspectos. En Veeam creemos que las organizaciones deben tener múltiples opciones, no solo en lo que se refiere a los modos de backup, sino también a las opciones de recuperación. La capacidad para crear backups de la granularidad elegida y restaurarlos cuando sea necesario a cualquier medio adecuado es crucial para las empresas de cualquier tamaño.

A continuación analizaremos más a fondo las tecnologías de backup y recuperación que creemos que son cruciales a la hora de considerar una solución para cualquier tipo de protección de datos.

Beneficios de un backup basado en imágenes con reconocimiento de aplicaciones

Los agentes de Veeam están aprovechando, en principio, la misma tecnología utilizada por Veeam para hacer backups de cargas de trabajo virtuales: backups basados en imágenes que crean copias de backup de cada disco conectado a un equipo protegido. Este beneficio permite hacer backups muy rápidos y sencillos, así como restauraciones rápidas a sistemas de recuperación completa como, por ejemplo, la restauración al hardware reemplazado debido a algún tipo de mal funcionamiento en el equipo original.

Otro beneficio de un enfoque basado en imágenes es la portabilidad de los archivos de backup porque pueden ser restaurados casi en cualquier lugar. Esta probada tecnología Veeam proporciona una movilidad única de los backups, lo que permite mover las cargas de trabajo del entorno físico al virtual o a la nube y viceversa con solo utilizar una de las muchas opciones de restauración ofrecidas. Los archivos de backup creados por Veeam Agent *for Microsoft Windows* son independientes. Incluso sin una infraestructura del backup existente, las restauraciones siguen siendo factibles.

En cuanto al conocimiento a nivel de aplicaciones específicas, Veeam Agent *for Microsoft Windows* añade el mismo motor de procesamiento de invitados/guest que se encuentra en Veeam Backup & Replication, lo que ayuda a brindar la potencia y la flexibilidad necesarias para garantizar la Disponibilidad de sus estaciones de trabajo y servidores físicos de Windows. También:

- Garantiza que las aplicaciones empresariales sean detectadas y bloqueadas durante el backup
- Proporciona backups de registros simples para bases de datos corporativas (MS-SQL y Oracle)
- Permite restauraciones granulares de archivos y aplicaciones.

NOTA: El procesamiento con reconocimiento de aplicaciones solo está disponible en la Server edition.

Un backup incremental para siempre con seguimiento de bloques modificado

Para evitar la transferencia completa de los datos de todos los discos cada vez que se realiza un backup (por ejemplo, diario), que sería esencialmente necesario si realiza imágenes completas de los discos del equipo sin una inteligencia añadida, Veeam Agent *for Microsoft Windows* aprovecha el seguimiento de bloques de cambios en cada uno de los discos del equipo. Esto asegura que, después de un backup completo inicial, solo se leerán los bloques que hayan cambiado desde la última ejecución del backup y se transferirán al nuevo archivo de backup incremental (ver **Figura 1**).

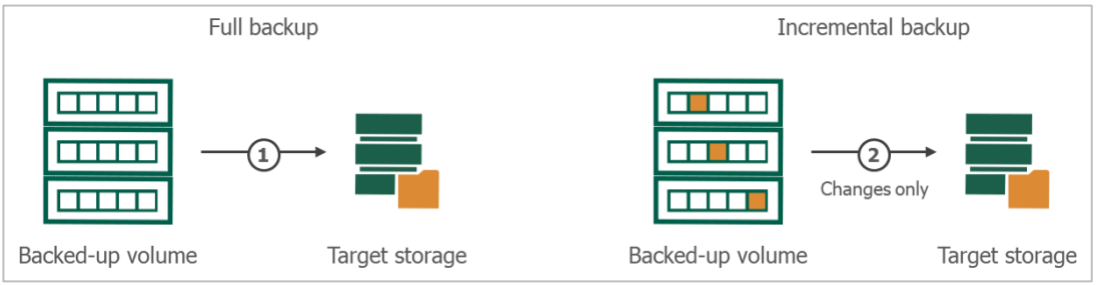

***Figura 1**: Seguimiento de bloques modificados*

Esta tecnología permite la creación de cadenas de backup siempre incrementales muy poderosas para siempre donde solo un backup completo inicial es obligatorio. Todas las ejecuciones subsiguientes del backup son incrementales y solo incluyen cambios en el proceso. Luego, tan pronto como expira el primer backup completo debido a la retención elegida, el archivo de backup incremental más antiguo se fusionará automáticamente con el archivo de backup completo existente y se sobrescribirán los bloques caducados (si los hay) dentro.

Sin embargo, la función de crear cadenas de backup siempre incrementales para siempre es opcional. Por ejemplo, se puede desactivar si hay razones para no utilizar esa opción y crear archivos de backup completos con regularidad. Esto se hace ya sea con una nueva lectura de los datos de la fuente completa (**backup full activo**) o mediante la creación programada de **backups completos sintéticos** de los archivos de la cadena de backup existentes.

Opciones de recuperación simples, pero poderosas

Cualquier solución de backup sería inútil si no hubiera forma de restaurar a partir de otros backups. Veeam Agent *for Microsoft Windows* proporciona un conjunto completo de opciones de recuperación, entre las que se incluyen:

- Restauración de recuperación completa
  Restaura todo el sistema de hardware existente, reemplazado, nuevo o de máquinas virtuales "vacías"
- Restauración a nivel de volumen
  Restaura volúmenes únicos o múltiples en un equipo o máquina virtual existente (igual o diferente)
- Exportación como disco virtual[1]
  Exporta discos individuales como discos virtuales que se pueden conectar a máquinas virtuales (Microsoft Hyper-V o VMware vSphere)
- Restauración instantánea a Microsoft Hyper-V[1]
  Ejecute una máquina virtual Hyper-V directamente desde los archivos de backup creados por el agente
- Restauración a Microsoft Azure[1]
  Restaura el equipo como una máquina virtual en Microsoft Azure IaaS
- Restauración a Amazon EC2[1]
  Restaura el equipo como una máquina virtual en Amazon Elastic Compute Cloud (EC2) IaaS
- Recuperación de elementos de aplicación[1]
  Restaurar elementos de una sola aplicación (Microsoft SQL, Microsoft Exchange, Active Directory, SharePoint)
- Recuperación a nivel de archivos
  Restaura archivos o carpetas individuales en el equipo original u otra ubicación

[1] Solo disponible con Veeam® Backup & Replication.

Y todas estas opciones están a solo unos clics de distancia como se muestra en **Figura 2**:

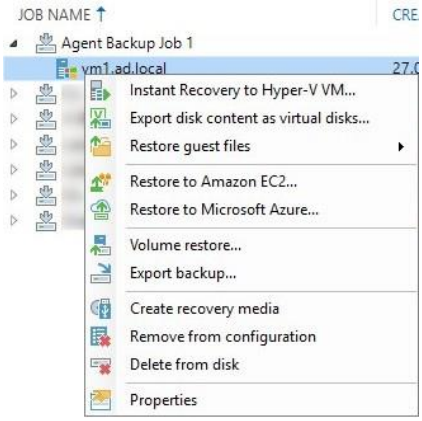

***Figura 2**: Opciones de restauración en el menú contextual de **Agent Backup** de Veeam Backup & Replication Console*

Múltiples modos de backup

Figura 3 muestra el cuadro de diálogo de selección del modo de backup de Veeam Agent *for Microsoft Windows.*

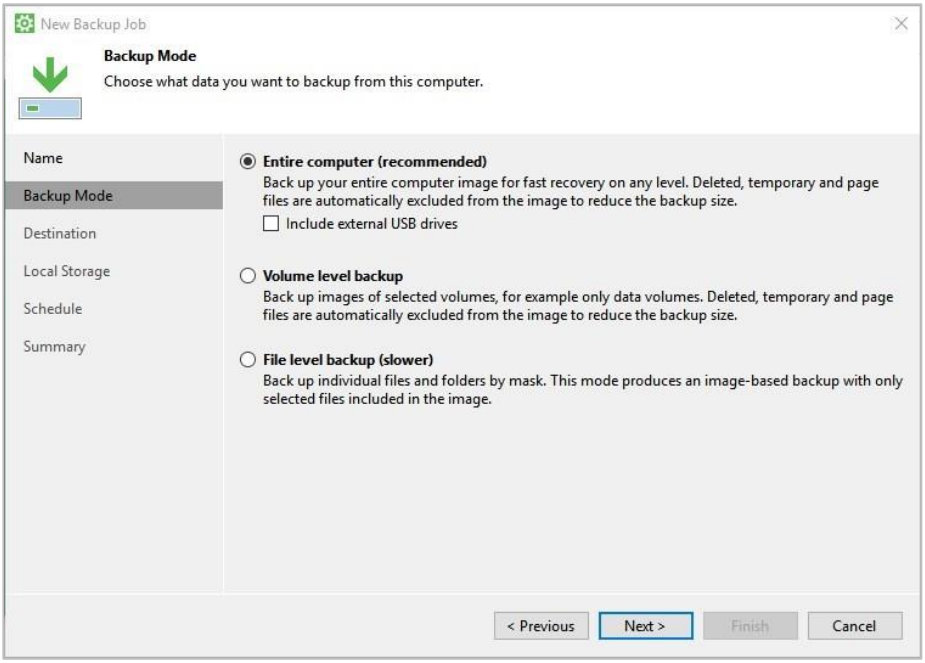

***Figura 3:** Modos de backup del trabajo de backup de agente*

Equipo completo

Este es el modo recomendado para crear un backup basado en imagen de todos los discos mientras se eliminan, archivos temporales y de página se excluyen automáticamente de la imagen para reducir el tamaño del backup. También incluye una opción para realizar backups de unidades USB externas conectadas al equipo (compatible solo con unidades con soporte para VSS de Microsoft).

Backup a nivel de volumen

El enfoque a nivel de imagen sigue siendo aplicable cuando se selecciona un **backup a nivel de volumen** y se seleccionan directamente los volúmenes para el backup. Ejemplo de esto sería si se hiciera un backup solo de volúmenes de datos específicos, pero no del disco del sistema (de arranque) del propio sistema operativo (o viceversa). Sin embargo, tenga en cuenta que cuando el sistema o disco de arranque se excluye del backup, la restauración de recuperación completa del equipo desde dicho backup no estará disponible.

Backup a nivel de archivo

Para situaciones en las que no es necesario o no es posible continuar con el enfoque de backup a nivel de imagen, Veeam Agent *for Microsoft Windows* puede configurarse para crear backups a nivel de archivos en su lugar. Sin embargo, este enfoque reducirá el desempeño de backup, ya que el sistema de archivos debe comprobar si hay archivos modificados para crear backups incrementales. Y si, por ejemplo, un archivo grande ha sido modificado solo en partes desde que se realizó el último backup (por ejemplo, 100 MB de cambios dentro de un archivo de 10 GB), la cantidad total de datos del archivo (10 GB en este caso) tendría procesarse y transferirse porque no habría un seguimiento del bloque de cambios disponible en el modo de backup a nivel de archivo. Esto aumenta la cantidad de datos a procesar en un factor de 100, en comparación con un backup basado en imagen como en este ejemplo.

Con la opción de backup basado en archivos también viene la capacidad de excluir o incluir uno o varios archivos o carpetas para los casos en los que se desea proteger solo un subconjunto de los archivos de datos existentes. Estas exclusiones o inclusiones pueden configurarse con nombres explícitos de archivos o carpetas, comodines o variables del entorno del sistema.

El backup a nivel de archivo permite incluir o excluir archivos o carpetas específicas por medio de la especificación de máscaras de archivo (como, por ejemplo,*.**log**) o variables de entorno del sistema.

NOTA: Si solo desea excluir determinadas carpetas del backup, puede seguir utilizando el backup a nivel de volumen, ya que también admite la exclusión de carpetas basadas en comodines o en variables de entorno del sistema (por ejemplo, **%WINDIR%**, que suele dirigir a la carpeta **C:\Windows**).

Conocimiento a nivel de aplicaciones específicas opcional

A veces puede haber razones para deshabilitar el conocimiento a nivel de aplicaciones específicas dentro de la configuración de Veeam Agent *for Microsoft Windows.* Esto da como resultado que las aplicaciones del equipo no se llevan a un estado consistente (en reposo) antes del backup real y solo creará un backup **sin consistencia de aplicación**. Tenga en cuenta que, aunque este enfoque todavía crea backups recuperables, algunas opciones de restauración no estarán disponibles, por lo que algunas aplicaciones (especialmente las bases de datos) podrían sufrir de datos de aplicación corruptos o incoherentes después de restaurarse a partir de dicho backup y algunas incluso podrían no iniciarse en absoluto por la misma razón.

Céntrese en la recuperación simple

Como resultado, se recomienda pensar siempre dos veces antes de pasar por alto cualquiera de los conceptos básicos al no usar el modo de backup en **todo el equipo.** En la mayoría de los casos, dicha configuración reducirá el número y la simplicidad de las opciones de restauración que probablemente necesite en caso de que haya habido una interrupción o falla que requiera recuperarse desde el backup. Como el tiempo siempre es corto en tales situaciones de emergencia, cuantas más opciones de restauración estén disponibles y más simples sean, más fácil y rápido será todo el proceso de recuperación.

Ediciones de licencia

Veeam Agent *for Microsoft Windows* está disponible en tres ediciones de licencia diferentes, denominadas.

Free: Ofrece una solución simple para realizar un backup de los equipos portátiles y de escritorio basados en Windows. Ideal para uso personal, pero no limitado para esto.

Workstation: Le da derecho a recibir soporte técnico 24.7.365 y agrega características para la protección del usuario móvil y el soporte para la administración remota; agrega la capacidad de crear backups completos sintéticos y usar los repositorios de Veeam Cloud Connect como destinos para el backup.

Server: Todas las características de Workstation edition, además del soporte completo de servidor mediante el procesamiento con reconocimiento de aplicaciones y el programador de trabajos centrado en el servidor, ofrece una cantidad ilimitada de trabajos de backup con cualquier objetivo soportado y Veeam Volume Change Tracking (controlador CBT) para los sistemas operativos de Windows Server.

Tabla 1 proporciona una rápida comparativa entre las características de estas ediciones:

Cuerpo de texto básico	**Free**	**Workstation**	**Server**
Recuperación instantánea de VM a Hyper-V	✓	✓	✓
Restaure a Azure o Amazon EC2	✓	✓	✓
Cifrado por parte de la fuente	✓[2]	✓[2]	✓[2]
Backups completos sintéticos		✓	✓
Configuración y administración remota		✓	✓
Procesamiento con reconocimiento de aplicaciones			✓
Procesamiento del registro de transacciones			✓
Indexado de archivos y búsqueda de catálogo			✓
Controlador CBT (solo para OS de servidor)			✓
Soporte técnico 24.7.365			✓

Tabla 1: *Descripción general de las ediciones*

Para obtener más información, lea esta guía comparativa. https://www.veeam.com/es-lat/products-edition-comparison.html.

Según los requisitos de implementación y administración, existen diferentes conjuntos de componentes de software que se deben instalar en una estación de trabajo o servidor para ser protegido por Veeam Agent *for Microsoft Windows*. Por esta razón, existen tres modos diferentes de operación en los que se puede implementar y administrar Veeam Agent *for Microsoft Windows* para proporcionar flexibilidad para muchos casos de uso diferentes.

[2] Si se utiliza un repositorio de backup de Veeam como destino de backup en modo independiente, el cifrado del lado de origen no estará disponible. Sin embargo, el cifrado de los datos de backup se puede habilitar en el repositorio de Veeam.

Modos de administración

Veeam Backup & Replication le permite gestionar de forma centralizada todos los aspectos de Veeam Agent *for Microsoft Windows* y sus instalaciones. Esto significa que los componentes de administración de la configuración local (administración de trabajos de backup, interfaz de usuario, opciones de restauración, etc.) no estarán disponibles localmente en la máquina protegida porque estas tareas serán controladas centralmente por el servidor de backup de Veeam Backup & Replication. Esto se conoce como el modo ***administrado por el servidor de backup***.

Por otra parte, si el paquete de instalación de Veeam Agent *for Microsoft Windows* se instala manualmente en un ordenador físico o virtual que no esté administrado por Veeam Backup & Replication, necesitará más componentes disponibles y configurables en el ordenador local. Esto se conoce como el modo ***independiente***.

Una tercera opción, denominada modo ***administrado por agente***, se asemeja a una mezcla especial de los dos modos anteriores y es el único modo disponible para Workstation edition y que se combina con la administración central.

Técnicamente, puede elegir uno de los modos descritos anteriormente de forma individual para cada equipo protegido. Pero existen, por supuesto, ciertos escenarios en los que un modo específico debería ser la opción preferida. Aquí hay un breve resumen y una lista de ejemplos de casos de uso para cada modo:

Independiente

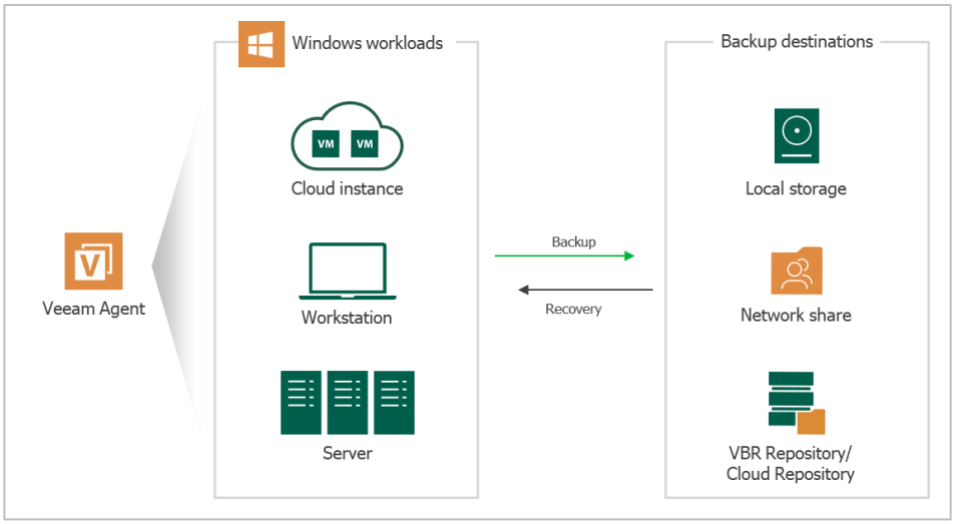

Figura 4: *Modo* ***independiente*** *sin administración central*

Obviamente, este modo está dirigido a proteger equipos independientes, tanto físicos como virtuales, que no forman parte de una infraestructura del backup administrada de forma centralizada. Cualquier usuario con permisos administrativos locales podrá configurar backups y restauraciones según sea necesario. Ejemplos de casos de uso:

- Estaciones de trabajo personales, físicas o virtuales, o equipos de servidor en casa
- Servidores o estaciones de trabajo corporativos físicos o virtuales, que se administran individualmente
- Equipos virtuales en nubes públicas, que se administran individualmente

El modo **independiente** está disponible para todas las ediciones de Veeam Agent *for Microsoft Windows.* Aunque obviamente no hay una administración central disponible para este modo, los trabajos de backup configurados localmente en un equipo agente en modo **independiente** pueden escribir sus datos de backup en repositorios de backup administrados por Veeam Backup & Replication.

Administrado por el servidor de backup

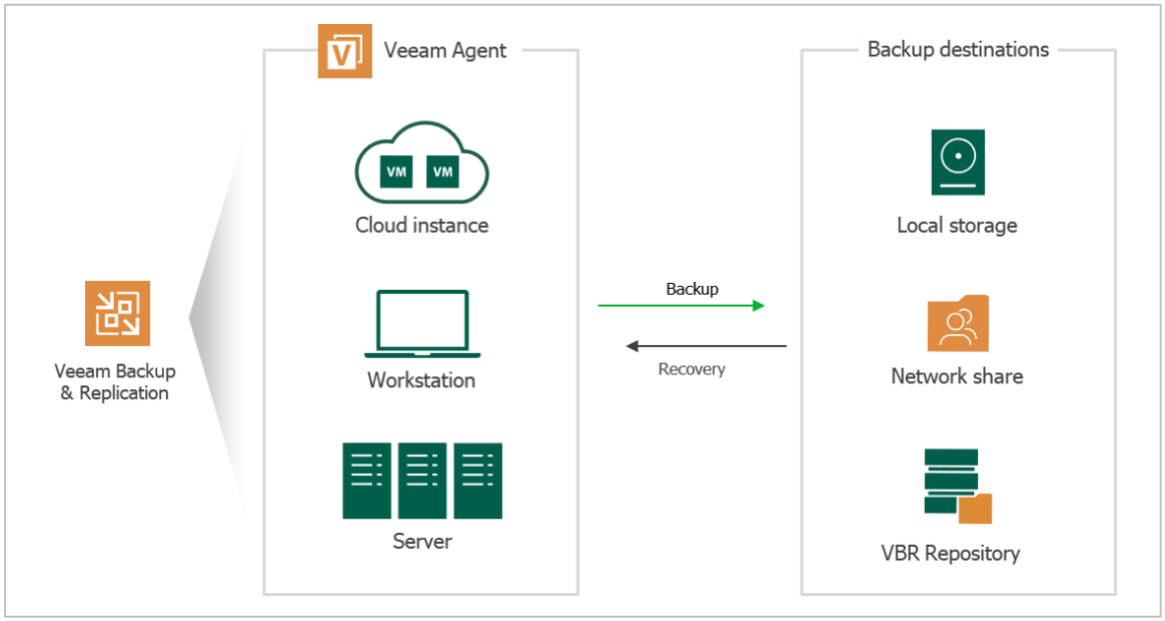

Figura 5: *Modo administrado por el servidor de backup*

Este modo requiere que exista una infraestructura Veeam Backup & Replication para la implementación, configuración y administración del agente. Los usuarios locales de equipos protegidos por Veeam Agent *for Microsoft Windows* en este modo no tienen opción para realizar o configurar backups o restauraciones (no existe una interfaz de usuario disponible localmente). Todo estará bajo el control del servidor de backup de Veeam Backup & Replication, el cual administra el equipo.

Ejemplos de casos de uso:

- Servidores o clústeres corporativos físicos o virtuales, administrados centralmente
- Máquinas virtuales o clústeres en la nube pública con administración central
- Son máquinas virtuales que no pueden protegerse mediante soluciones de backup centradas en la virtualización debido a la falta de soporte o compatibilidad con los sistemas snapshot de aplicaciones (es decir, Veeam Agent *for Microsoft Windows* se encarga donde los backups de VM de Veeam Backup & Replication podrían no ser adecuados).

La administración mediante el modo de ***servidor de backup*** está disponible únicamente para Server edition y es el único modo que admite protección de clústeres de failover de Microsoft (consulte https://www.veeam.com/kb2463 para obtener más información).

Administrado por agente

Al ser una mezcla de los dos modos anteriores, este modo está construido para la protección de los equipos que requieren capacidades y administración de backup/restauración central, pero que igualmente requieren de un usuario local para poder tener cierto control. También es adecuado para equipos que no tienen una conexión de red permanente a la infraestructura del backup central.

Aunque se requiere que todas las opciones de configuración del agente se definan de forma centralizada en un servidor de backup de Veeam, es el equipo local el que ejecuta los backups de forma programada (incluso si el servidor de backup no está disponible en ese momento), utilizando su propia base de datos de configuración y el motor de programación después de haber extraído su configuración del servidor de backup. Un usuario local tiene una interfaz de usuario limitada, que permite crear backups al instante (además de los backups regulares creados en base a un programa definido centralmente), así como realizar restauraciones a nivel de archivo o de volumen. Los ejemplos de casos de uso incluyen:

- Servidores de bases de datos o aplicaciones físicas o virtuales corporativas (en las instalaciones o en la nube pública) gestionados por administradores dedicados de aplicaciones o bases de datos que necesitan la capacidad de realizar backups o restauraciones al instante sin ayuda del personal de infraestructura o de operaciones de backup
- Estaciones de trabajo corporativas
- Equipos de extremos móviles sin conexión continua a la red corporativa

El modo ***administrado por agente*** está disponible para las ediciones de servidor y de estaciones de trabajo.

Tipos de instalación del agente

Como el ***modo independiente*** obviamente maneja todas las tareas de administración y configuración localmente en el equipo protegido, se requiere de la instalación completa de todos los componentes de Veeam Agent *for Microsoft Windows*. Esto incluye un motor de base de datos local para almacenar información de configuración y registro (al utilizar Microsoft SQL Express LocalDB) y se conoce como el tipo de instalación de ***agente completo.***

Si, a diferencia de lo anterior, la configuración y la administración se llevan a cabo de forma centralizada, tal como se describe en el modo de ***administrado por servidor de backup***, solo se requiere un conjunto más pequeño de componentes, denominado tipo de instalación de ***agente ligero***.

Eventualmente, en el modo de ***administrado por agente***, se instalarán todos los componentes del tipo de instalación de ***agente completo*** más un pequeño servicio de instalación/mantenimiento (Veeam Installer Service). Sin embargo, todos los componentes de la interfaz de usuario local se deshabilitarán en este modo (es decir, las opciones de configuración se pueden revisar pero no cambiar en el equipo local), y Veeam Agent *for Microsoft Windows* extraerá regularmente su configuración de un servidor central de backup de Veeam Backup & Replication. Además, la capacidad de iniciar manualmente un backup al instante (fuera de la programación) así como varias opciones de restauración está disponible a través del agente local GUI/CLI y no requieren acceso a la consola central de Veeam Backup & Replication.

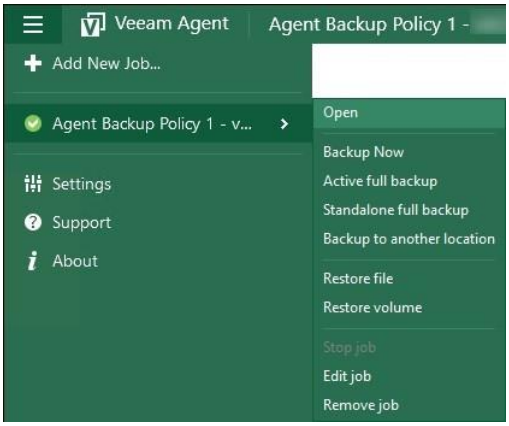

Figura 6: *Opciones de backup y restauración disponibles localmente en modo* ***administrado por agente***

En cuanto a los componentes instalados, la única diferencia entre el ***modo administrado por agente*** y el ***modo independiente*** es que el servicio de instalación de Veeam no se instala en el independiente. Por lo tanto, la instalación de Veeam Agent *for Microsoft Windows* se sigue considerando del tipo de ***agente completo***.

Tabla 2 proporciona una descripción general rápida de los tipos de instalación de los dos agentes y de los componentes incluidos relacionados con los tres modos de administración.

	Agente completo	**Agente ligero**
Independiente	Veeam Agent *for Microsoft Windows* • Interfaz de usuario local completa y motor de programación • Base de datos local (MS SQL Express) Controlador CBT (opcional, solo servidores) LocalDB de MS SQL Express, administración. Objetos y tipos CLR	
Administrado por servidor de backup		Veeam Installer Service Veeam Agent *for Microsoft Windows* • Sin interfaz de usuario local • Sin base de datos local Controlador CBT (opcional, solo servidores)
Administrado por agente	Veeam Installer Service Veeam Agent *for Microsoft Windows* • Motor de programación local • Base de datos local (MS SQL Express) • Configuración y programación extraídos del servidor central de backup Opciones de configuración deshabilitadas en la interfaz gráfica de usuario local Controlador CBT (opcional, solo servidores) LocalDB de MS SQL Express, administración. Objetos y tipos CLR	

Tabla 2: *Componentes instalados basados en el modo de administración*

Gestión e implementación de agentes centrales

Veeam Backup & Replication ofrece un control completo sobre la protección de los equipos que utilizan Veeam Agent *for Microsoft Windows*, lo que abarca la implementación del software del agente, así como la administración de configuraciones del agente, programaciones, destinos de backup y, por supuesto, recuperaciones.

Grupos de protección

Dos de los principales objetivos de cualquier esfuerzo de administración central en TI es estandarizar las configuraciones en muchos equipos e implementar, administrar, controlar y hacer cumplir estos estándares de una manera sencilla. En Veeam Backup & Replication, los **grupos de protección** son el punto de partida para ejecutar tareas de estandarización para todos los equipos que utilizan Veeam Agent *for Microsoft Windows*, tanto físicos como virtuales.

Un **grupo de protección (PG)** evalúa el alcance de equipos (= miembros del PG) y define si se debe instalar Veeam Agent *for Microsoft Windows* para estos miembros. El alcance de un PG puede basarse en diferentes fuentes, como se muestra en **Figure 7.**

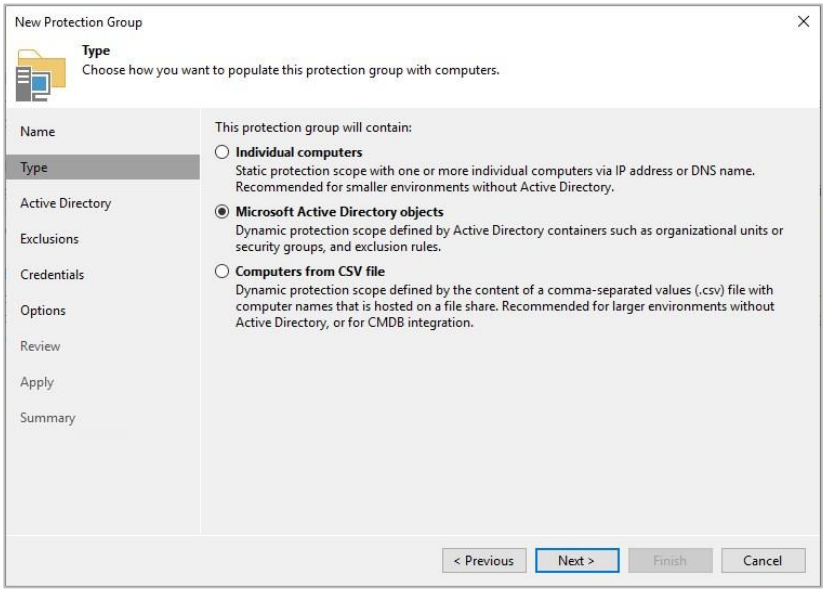

Figura 7: *Selección de origen del alcance del* ***grupo de protección***

Cuando se utilizan objetos de Active Directory como fuente de un PG, es posible seleccionar objetos contenedores como unidades organizativas o grupos de seguridad en lugar de (o además de) objetos individuales en el equipo. Esta es una opción muy poderosa ya que sigue la dinámica del objeto contenedor elegido:

- Cada vez que se agrega un equipo al contenedor seleccionado dentro de Active Directory, el PG respetará el cambio y los nuevos miembros del contenedor se procesarán automáticamente.

  Lo mismo se aplica al quitar objetos del equipo en los contenedores de Active Directory:

- El procesamiento de estos equipos a través del PG cesará automáticamente en función de la programación de PG.

Para añadir aún más flexibilidad, se pueden definir exclusiones dentro del PG para omitir ciertos equipos y/o contenedores del procesamiento PG. También pueden definirse exclusiones para las máquinas virtuales en general (si el alcance previsto del PG es solo para los equipos físicos), o para los equipos que han estado sin conexión por más de 30 días.

Para permitir la instalación del Veeam Agent *for Microsoft Windows* en el conjunto resultante de miembros de un **Grupo de Protección**, se requerirán credenciales con privilegios de administrador local para dichos miembros. Estas credenciales se pueden configurar para que sean las mismas (**cuenta maestra**) para todos los miembros del PG, así como individualmente por contenedor, grupo o equipos individuales.

Para definir cuándo se deben analizar los equipos del alcance del **grupo de protección** en busca de cambios, se puede configurar y programar en el cuadro de diálogo de la configuración del PG. También permite seleccionar un **servidor de distribución** como parte de la infraestructura Veeam Backup & Replication, el cual será responsable de la comunicación con los equipos miembros del PG en caso de que el servidor del backup central no pueda o no deba acceder a esos equipos directamente. La instalación y actualización automática de los componentes de Veeam Agent *for Microsoft Windows* también se pueden deshabilitar de ser necesario (**Figura 8**).

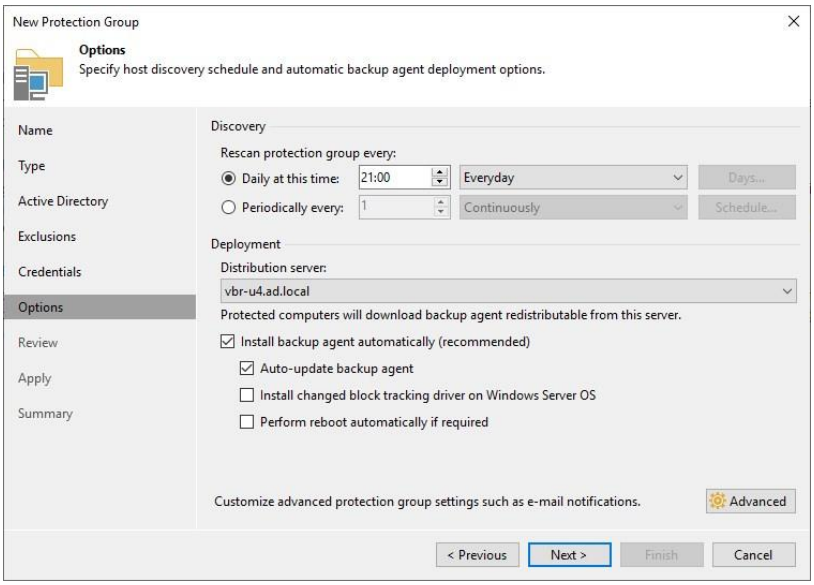

Figura 8: *Opciones de descubrimiento e implementación en los* ***grupos de protección***

Trabajos de backup de agente

Para crear backups en equipos que se han agregado a los **grupos de protección**, se requiere al menos un trabajo de backup de agente, ya que el trabajo de backup define la programación del backup y el destino donde se almacenarán los datos de ese backup.

Los trabajos de backup del agente administrados de forma centralizada se crean y configuran en el servidor de backup de Veeam Backup & Replication. Estos trabajos le permiten elegir entre los modos ***administrados por el servidor de backup*** y los ***administrados por agente***, como se muestra en **Figura 9**.

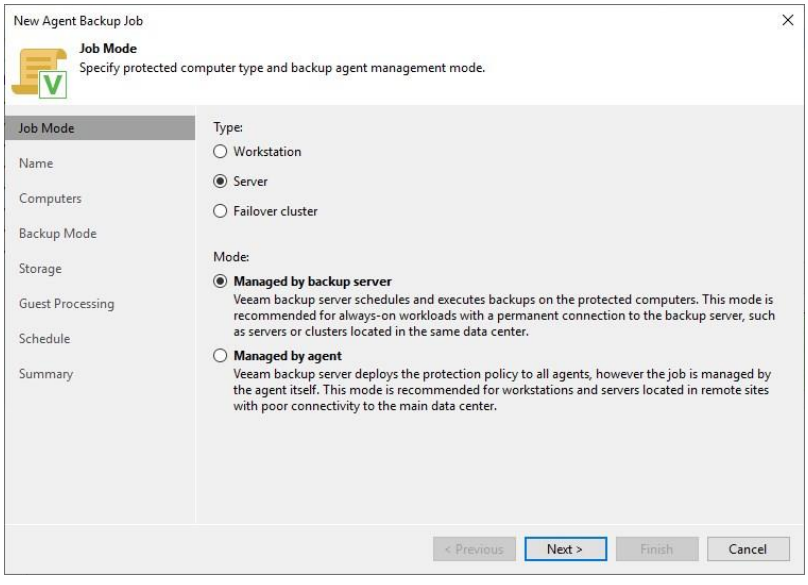

Figura 9: *Diálogo de* ***Nuevo trabajo de backup del agente*** *en la consola de Veeam Backup & Replication*

Tenga en cuenta que solo los trabajos de tipo ***Servidor*** (es decir, para agentes con Server edition en el servidor) proporcionan la capacidad de habilitar el procesamiento con reconocimiento de aplicaciones, como se muestra en el paso **Procesamiento de invitados/guest** en el cuadro de diálogo del asistente.

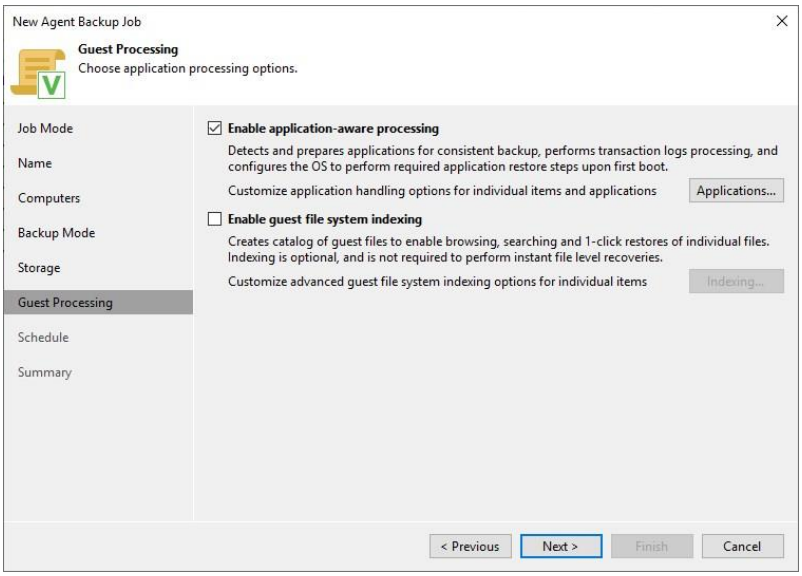

Figura 10: *Opciones de procesamiento de invitados/guest de un trabajo tipo Servidor*

En el último paso del asistente de configuración de trabajos de backup, se muestran las poderosas opciones de programación disponibles en los trabajos de backup administrados por Veeam Backup & Replication (**Figura 11**).

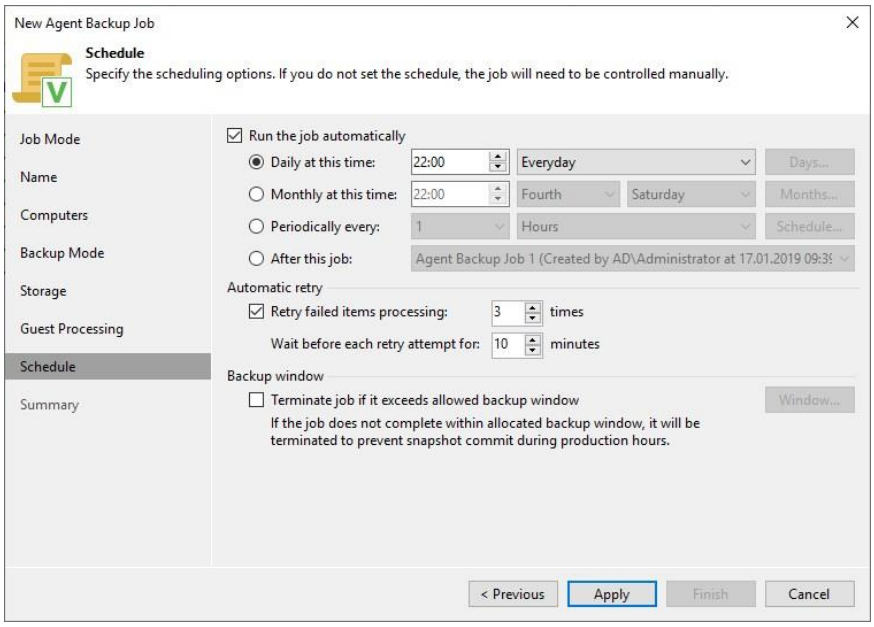

Figura 11: *Opciones de programación de trabajos* ***administrados por el Servidor de backup***

Destinos del backup

Si está familiarizado con Veeam Backup & Replication, ya debe saber que se pueden usar muchos destinos diferentes para almacenar sus valiosos datos de backup. Veeam Agent *for Microsoft Windows* también admite una variedad de destinos de backup configurables, dependiendo del modo de administración, como se muestra en **Tabla 3**.

Cuerpo de texto básico	**Independiente**	**Administrado por el Servidor de backup**	**Administrado por Agente**
Almacenamiento local	✓		✓
Carpeta compartida	✓	✓[1]	✓
Repositorio de backup de Veeam	✓	✓	✓
Repositorio de Veeam Cloud Connect	✓[2]		
Microsoft OneDrive	✓		

Tabla 3: *Destinos del backup*

NOTA: Consulte la sección **Siguiente lanzamiento** a continuación para obtener información acerca de los destinos de backup adicionales que serán compatibles con la próxima versión de Veeam Agent *for Microsoft Windows*.

1 Si está configurado como **repositorio de backup** en Veeam Backup & Replication

2 Para conocer las limitaciones, lea más aquí. https://helpcenter.veeam.com/docs/agentforwindows/userguide/cloud_connect.html

Cifrado

Para agregar protección adicional a los datos de backup creados por Veeam Agent *for Microsoft Windows*, por ejemplo, para cumplir con las normativas legales o las directivas corporativas, puede optar por cifrar los archivos de backup en la **Configuración avanzada** de la configuración de destino del trabajo del backup, como se muestra en **Figura 12.**

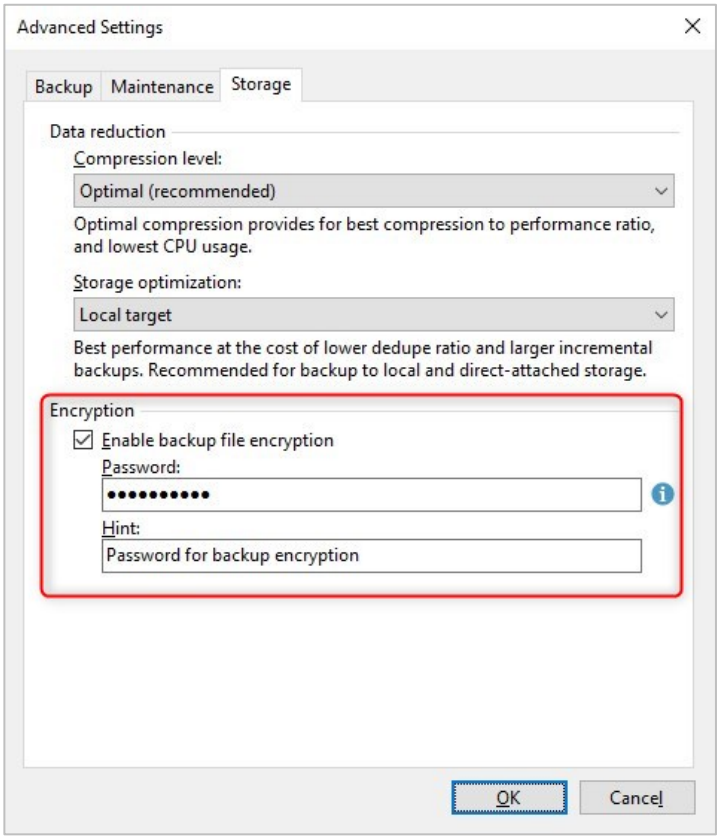

Figura 12: *Configuración de* ***cifrado***

Todo lo que se requiere es una contraseña, que debe recordar para descifrar y restaurar los datos de backup cifrados. Se puede almacenar una frase clave opcional junto con la contraseña misma, que puede ayudarle a recuperar la contraseña cuando más la necesite.

Si se selecciona un repositorio de backup de Veeam como destino del backup de un trabajo de backup de Veeam Agent *for Microsoft Windows* en modo **independiente**, el cifrado no se puede configurar en la configuración del trabajo del agente (**Figura 13**). Esto se debe a que el cifrado de datos ubicado en los repositorios de backup de Veeam es gestionado por los administradores que trabajan con Veeam Backup & Replication.

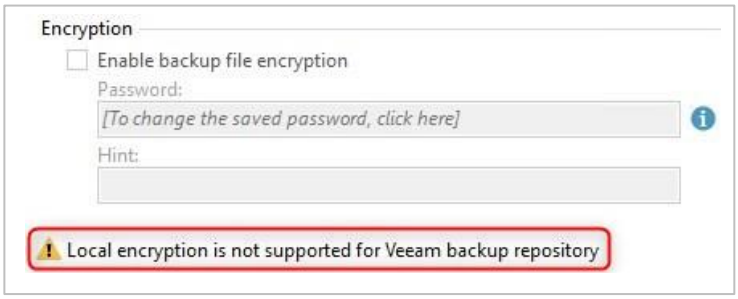

Figura 13: *El cifrado local no está disponible para los repositorios de backup de Veeam*

Dicho esto, el cifrado todavía se puede habilitar para estos archivos de backup de **agente**, pero debe configurarlo el administrador de backups dentro de los parámetros de **configuración** del repositorio (**Figura 14**).

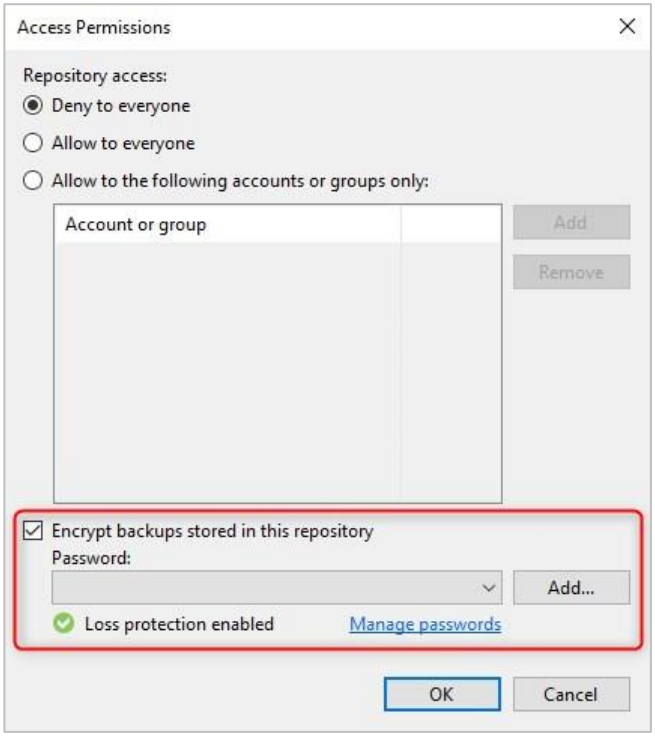

Figura 14*: Configuración de cifrado en un repositorio de backup de Veeam*

NOTA: La configuración resaltada en **Figura 14** solo se aplica a los backups de los agentes en el modo **independiente** . Cuando se utilizan trabajos de backup **administrados por agente** o **administrados por servidor**, esta configuración se ignorará y solo se aplicarán los valores de cifrado de la configuración del trabajo.

Realización de backups remotos: Conforme a la Regla 3-2-1

Es muy probable que ya esté familiarizado con la regla 3-2-1 de protección de datos:

> Cree siempre **3** **copias de sus datos**
>
> Almacene estas copias en **2** **tipos de medios diferentes**.
>
> Mueva **1** **copia de datos fuera del sitio**

Para ayudarle a seguir esta regla con Veeam Agent *for Microsoft Windows*, hay un tipo especial de trabajo backup disponible en Veeam Backup & Replication, el cual permite copiar los datos de backup del agente a un repositorio de Veeam secundario. Esta función es bien conocida en Veeam Backup & Replication para los backups de máquinas virtuales y ha estado allí durante mucho tiempo. Sin embargo, puede procesar backups creados por Veeam Agent *for Microsoft Windows* solo con trabajos de copia de backup para backups de equipos de Microsoft Windows. No puede agregar un backup de Veeam Agent como fuente adicional de un trabajo backup que procesa backups de VM.

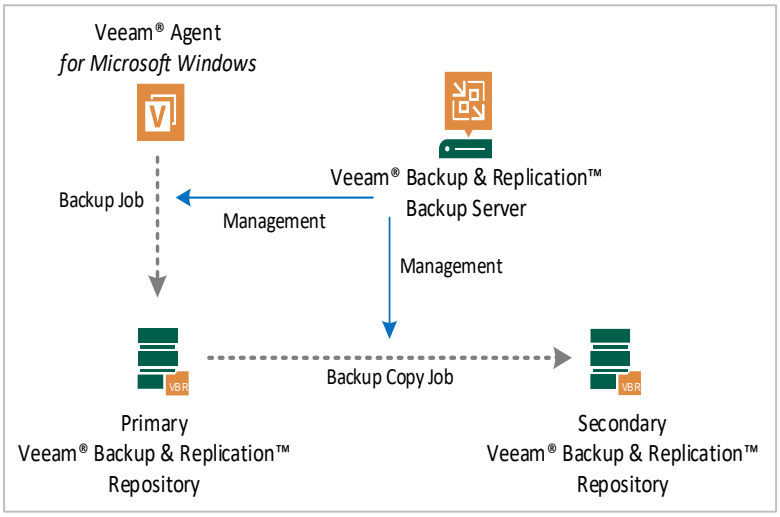

Figura 15: *Copia de backup*

Próxima versión

En el momento en que se escribió este white paper, ya había tenido la oportunidad de obtener una versión beta de la siguiente versión de Veeam Backup & Replication, que incluirá una nueva versión de Veeam Agent *for Microsoft Windows*.
Aquí hay algunos aspectos destacados de las características agregadas/mejoradas que puede esperar de esa versión.

- Compatibilidad con determinados dispositivos de deduplicación como destinos de backup
  - Veeam Agent *for Microsoft Windows* será capaz de utilizar dispositivos de almacenamiento HPE StoreOnce y Dell EMC Data Domain como objetivos de backup al aprovechar un servidor de portal administrado por Veeam Backup & Replication.
- Soporte para repositorios de Veeam Cloud Connect como destinos de backup en modo **administrado**
  - Actualmente, solo el modo **independiente** de Veeam Agent *for Microsoft Windows* admite repositorios Veeam Cloud Connect como destinos para backups (consulte **Tabla 3**). Con la próxima versión, la capacidad de enviar backups a estos repositorios se agregará a los modos ***administrados por agente*** y ***administrados por el servidor de backup***.

- Reanudar el backup/reanudar la sincronización de la caché del backup
  - La desconexión temporal de la red o la puesta en modo de **hibernación** o **suspensión** en una estación de trabajo ya no provocará errores en los trabajos backup o durante la sincronización del caché.
- Procesamiento de disco paralelo
  - Varios discos en el mismo equipo o máquina virtual se procesarán en paralelo (la versión actual solo permite el procesamiento secuencial de varios discos).

Epílogo

Este white paper se ha escrito para ofrecer una descripción general de cómo Veeam Agent *for Microsoft Windows* ayuda a proteger una variedad de cargas de trabajo físicas, virtuales y en la nube. Aunque cubrimos algunos temas en detalle, hubo otros que no. También hay algunos temas que no se mencionaron en absoluto. Espere más white papers con más información en el futuro.

¡Por favor, deje sus comentarios en nuestro dedicado foro de la comunidad Veeam!

Acerca del autor

Como arquitecto de soluciones en Veeam, Matthias está ayudando a clientes y a socios a planificar, diseñar e implementar estrategias y soluciones para proteger las cargas de trabajo de misión crítica. Matthias es licenciado en física y lleva más de 20 años en la industria de TI en varios puestos de operaciones, administración y consultoría.

Acerca de Veeam Software

Veeam es el líder mundial en la administración de datos en la nube. Veeam Availability Platform es la solución más completa para ayudar a los clientes a automatizar la administración de datos y garantizar la disponibilidad de los datos en cualquier lugar.

Tenemos más de 375,000 clientes en todo el mundo, de los que un 82% están incluidos en la lista Fortune 500 y un 67% están en la Global 2,000. Nuestros resultados de satisfacción del cliente (3.5 veces el promedio del sector) son los más altos en la industria. Nuestro ecosistema global incluye a más de 70,000 mil socios de canal; Cisco, Hewlett Packard Enterprise (HPE) y NetApp como canales exclusivos, además de cerca de 20,000 proveedores de servicios y de nube. Con su sede central en Baar, Suiza, Veeam tiene oficinas en más de 35 países.

Para más información, visite https://www.veeam.com/es-lat o siga la cuenta de Veeam en Twitter @veeam.