

Cómo hacer un backup de un cloud server

Cómo hacer un backup de un cloud server. ¿Cómo hacer una copia de seguridad del servidor en la nube? Descúbrelo aquí.

Como la computación en la nube se hizo popular, una copia de seguridad del servidor dejó de ser un proceso analógico de dos etapas y se convirtió en una compleja serie de pasos ejecutados por un software especializado en la copia de seguridad del servidor en la nube.

Pero, ¿cuáles son las principales diferencias entre admitir un servidor físico y uno virtual? En este artículo, cubriremos este tema junto con una revisión de los proveedores que ofrecen aplicaciones para realizar una copia de seguridad efectiva del servidor en la nube.

Copia de seguridad del servidor físico vs servidor en la nube

Si no está familiarizado con las copias de seguridad de servidores virtuales, este proceso puede parecer complejo a primera vista.

La verdad es que gracias al desarrollo constante de aplicaciones especializadas en copias de seguridad, una copia de seguridad del servidor en la nube es más rápida y más eficiente que la copia de seguridad de un servidor físico.

Hagamos una comparación entre ambos tipos de copias de seguridad para tener una idea clara de sus diferencias.

Servidor físico

Aunque hay varias formas de hacer una copia de seguridad de un servidor físico, el método más común requiere un agente de

software en el cliente que lea y recopile los datos para realizar una copia de seguridad. Luego, el software utiliza una red IP para transferir la copia al servidor de respaldo.

Posteriormente, el mismo servidor de respaldo envía el respaldo a su destino final. Es necesario mencionar que cada archivo dentro de la copia de seguridad se coloca en una base de datos en caso de que necesite ser restaurado.

Servidor virtual

Desde el punto de vista conceptual, la copia de seguridad  de un servidor virtual puede parecer similar al método de copia de seguridad del servidor físico, pero conlleva una mayor complejidad.

Si sigue el método tradicional de respaldo de un servidor físico en uno virtual, el problema sería que el software de respaldo podría tener algunos problemas para identificar si el servidor es físico o virtual.

Entonces, el administrador de la copia de seguridad no sabría en qué máquina física se encuentra la máquina virtual y esto podría hacer que programe varias copias de seguridad de la misma máquina host. Esta situación afectaría el rendimiento de todas las máquinas virtuales ubicadas en el host.

La solución a este escenario fue la creación de instantáneas: una imagen instantánea de un momento particular de la copia del archivo de disco de la máquina virtual.

Una instantánea conserva el sistema de archivos del disco, así como la memoria de la máquina virtual. En caso de que algo salga mal con la copia de seguridad, el administrador puede volver a la instantánea guardada y restaurarla.

Este método de alguna manera ciega al agente de software que ejecuta la copia de seguridad, ya que ignora los datos de la máquina virtual. Por lo tanto, los datos que incluyen archivos

eliminados y espacios en blanco también son seguros.

Para evitar esta copia de seguridad de datos innecesaria, es necesario utilizar herramientas de deduplicación de datos, mapeo de bloques activos y detección de espacios en blanco para identificar los archivos eliminados y excluirlos de las copias de seguridad. Esto también permite a los proveedores desarrollar copias de seguridad incrementales de imágenes de máquinas virtuales.

¡No pierda sus datos! Tener una estrategia de respaldo 3-2-1

No existe un método perfecto para la protección de datos, pero la Estrategia de copia de seguridad 3-2-1 es la más efectiva para reducir el riesgo de una pérdida fatal de sus datos.

La estrategia 3-2-1 consiste en tener al menos tres copias de sus datos. Las copias 1 y 2 deben estar en dispositivos locales, por ejemplo, su computadora y un disco duro externo.

La copia 3 debe estar fuera del sitio, por ejemplo, una solución de respaldo en línea. Una copia de seguridad en línea escanea sus datos continuamente para mantenerlos actualizados y guardados en un centro de datos. En este caso, es necesario verificar sus actualizaciones regularmente para asegurarse de que los archivos más recientes estén seguros en línea.

También es una buena práctica mover la copia 2 (almacenada en el disco duro externo) a una ubicación diferente. Solo imagine un incendio desafortunado en la oficina donde están su computadora y su disco duro externo. En este caso, perderá sus copias 1 y 2 en el mismo incidente.

Servicios de copia de seguridad del

servidor en la nube

¿Necesita hacer una copia de seguridad del servidor en la nube efectiva y segura? Lo primero que debe tener es un software de respaldo confiable.

Por supuesto, hay muchas opciones en el mercado. Antes de elegir un servicio de respaldo, debe considerar parámetros como la restauración del nivel de archivo de autoservicio del inquilino, el respaldo de autoservicio a pedido del inquilino, una buena interfaz de usuario web y el respaldo y recuperación de autoservicio multiempresa, entre otros.

Aquí presentamos una comparación de cuatro proveedores cuyos servicios se encuentran entre las opciones más aceptables en términos de precio y calidad con respecto al software de respaldo.

VMcom

VMcom Backup Appliance es un software para admitir aplicaciones virtualizadas y datos que se ejecutan en VMware. Además de proteger la información de sus máquinas virtuales, también le permite controlar el acceso a inquilinos específicos.

A diferencia de otros proveedores, una de las grandes ventajas que ofrece el software VMcom es la tenencia múltiple como solución en la nube pública. Esto significa que cualquier proveedor de nube pública de VMware puede otorgar permisos a usuarios seleccionados para restaurar y respaldar máquinas virtuales específicas. Otra ventaja de VMcom es que ofrece una restauración de nivel de archivo de autoservicio para inquilinos tanto para Windows como para Linux, y el cliente no necesita pagar licencias adicionales.

De esta manera, los usuarios mismos realizan la restauración y la copia de seguridad a través de una excelente interfaz de

usuario web accesible en cualquiera de los paquetes de VMcom .

El software VMcom se entrega en dos modos de pago flexibles: un pago único para una licencia perpetua basada en el zócalo de la CPU y una licencia de pago mensual basada en VM.

Veeam



Veeam es otra opción de copia de seguridad en la nube, al igual que VMcom, sus servicios incluyen copia de seguridad sin agente de máquinas virtuales VMware, implementación inicial rápida, soporte de seguimiento de bloque modificado, deduplicación integrada y compresión. La fortaleza de Veeam es su llamada hiperdisponibilidad para todas las cargas de trabajo posibles: virtual, física y en la nube.

Sin embargo, no ofrece cuotas de almacenamiento por inquilino, administración del plan de respaldo de autoservicio de inquilino y respaldo de autoservicio a pedido del inquilino.

Aunque ofrece restauración de nivel de archivo de autoservicio para inquilinos, solo está disponible para Windows y el usuario debe pagar las licencias de Microsoft. La interfaz de usuario web, la copia de seguridad de autoservicio multiusuario y la recuperación también están disponibles en la versión Enterprise.

Nakivo

Entre las características que ofrece Nakivo se encuentran la copia de seguridad de VM, la replicación, la copia de seguridad en la nube, la deduplicación global, la recuperación instantánea de VM y los objetos, la copia de seguridad y la verificación de captura. Otros puntos fuertes son su interfaz web fácil de usar, no requiere licencias adicionales de Microsoft y tiene una implementación inicial rápida basada en una plantilla OVF.

Sin embargo, al igual que Veeam, carece de las características

principales de múltiples inquilinos, especialmente la copia de seguridad y recuperación de autoservicio de múltiples inquilinos y la restauración del nivel de archivo de autoservicio de inquilinos.

Acronis VE

Junto con VMcom, quizás Acronis VE es uno de los software de respaldo más equilibrados en términos de servicios y características. También tiene una copia de seguridad y recuperación de autoservicio para múltiples inquilinos y cubre servicios tales como cuotas de almacenamiento de inquilinos, gestión del plan de copia de seguridad de autoservicio y soporte de seguimiento de bloque modificado.

Las desventajas de Acronis VE son que no tiene una implementación inicial rápida y requiere múltiples máquinas virtuales de Windows. Además, sus usuarios necesitan licencias adicionales de Microsoft y su interfaz de usuario web tiene una funcionalidad bastante limitada. Además, el usuario debe pagar un costo adicional por el servicio integrado de deduplicación y compresión.

Conclusión

Acronis, Nakivo, Vea y VMcom, todos tienen fortalezas y debilidades. Sin embargo, VMcom Backup Appliance es altamente multiinquilino, lo que le da al administrador central la capacidad de crear entornos dentro de un solo dispositivo.

Además, cada inquilino puede asignar privilegios específicos para respaldar y recuperar objetos vSphere y datos de almacenamiento. Además, el costo-beneficio de VMcom es el más aceptable en comparación con el resto de los proveedores. ¡No omita la copia de seguridad de su servidor en la nube y elija!

Leer también: [¿Qué es BaaS? Backup as a Service, definición, concepto, significado](#); [Copia de seguridad, restauración y](#)

[recuperación de Bare Metal: 7 cosas que los profesionales de TI deben saber](#); [Diferencias entre BaaS y DRaaS](#) ; [Servicios en la nube](#)