VEEAM
IT JUST WORKS!™

Las 10 mejores prácticas para la Disponibilidad de datos de VMware

Eric Siebert
VMware vExpert

AVAILABILITY
for the Always-On Enterprise™

Resumen

Realizar un backup de sus máquinas virtuales (VMs, por sus siglas en inglés) puede parecer un proceso sencillo, pero es más complejo de lo que se ve a simple vista. Realizar backups de los servidores físicos es un proceso bastante simple: solo instala un agente en un servidor y lo agrega a la programación de backups. Sin embargo, para realizar backups eficientes a las VMs, necesita utilizar técnicas y funciones diseñadas específicamente para entornos virtuales. Si trata a las VMs como servidores físicos cuando les realiza backups o las restaura, desperdicia recursos y hace que las ventanas de backup sean más extensas de lo necesario. La virtualización es un cambio revolucionario en el centro de datos y, una vez implementada, necesita cambiar sus procedimientos y métodos para aprovechar sus fortalezas y arquitectura única.

La arquitectura de la virtualización ofrece muchas ventajas para el backup y la recuperación del servidor. Cambia las técnicas tradicionales utilizadas para realizar backups a los servidores al aprovechar las funciones de la virtualización y así lograr backups y recuperaciones ágiles y más eficientes. También brinda más flexibilidad y más opciones para realizar backups, restaurar VMs e implementar la recuperación ante desastres (DR, por sus siglas en inglés). En este documento técnico, ofreceremos 10 consejos para ayudar en la implementación del backup y la recuperación en un entorno virtual, incluidos los métodos, técnicas y configuración adecuados, así como también el aprovechamiento de las funciones desarrolladas en Veeam® Backup & Replication™ para que pueda llevar sus backups al siguiente nivel.

1 – Realice sus backups desde el nivel de infraestructura de VMware

Cuando realice backups de las VMs, no debería hacerlo con el mismo método que utilizó para realizar backups de sus servidores físicos. A los servidores físicos tradicionalmente se les realiza backups utilizando un agente instalado en el SO guest del host. El servidor de backup se conecta al agente para copiar los datos desde allí. Este método también funcionará en una VM, pero ignorar la capa de la virtualización cuando realiza backups es ineficiente y una pérdida de valiosos recursos de host. La mejor manera de realizar backups de las VM es en la capa de la virtualización. Para eso, necesita una aplicación de backup que esté desarrollada y optimizada para la virtualización.

Una aplicación de backup que reconoce la virtualización no tiene que incluir el SO guest de la VM en el backup. En su lugar, la aplicación puede conectarse directamente al archivo del disco de la VM para realizarle un backup. Esto significa que no hay sobrecarga de recursos en la VM mientras le realiza un backup, y las cargas de trabajo no se verán afectadas mientras se estén ejecutando los backups. Esto también puede reducir o eliminar el uso de recursos en el host. Como resultado, puede realizar backups de más VMs de manera simultánea y el host tiene más recursos disponibles para las cargas de trabajo de las VMs. Además, su solución de backup debería aprovechar las APIs de VMware vSphere para Data Protection, que ofrece integración con Change Block Tracking para permitir que el hipervisor mantenga un registro de los bloques del disco que han cambiado entre los ciclos de backup o replicación para obtener operaciones más rápidas.

Al tiempo las empresas se virtualizan cada vez más, su solución de backup debería reflejar eso y trabajar al nivel de infraestructura de VMware. Veeam Backup & Replication fue desarrollado desde su concepción para realizar backups a los entornos de VMware, específicamente. Está completamente integrado con VMware y opera en la capa de virtualización para una máxima eficiencia.

2 – Asegure sus VMs y datos críticos usando la regla 3-2-1

Sus VMs y, más importante aún, sus datos son cruciales para su negocio y no puede permitirse perderlos. Los backups son como una póliza de seguros para sus datos, y no querrá usarlos jamás. Sin embargo, cuando sí tiene que usarlos, es fundamental que funcionen correctamente y que pueda restaurar lo que necesite. Los fallos no son una opción cuando se trata de recuperar datos. Si su método principal de recuperación falla de alguna manera, necesita un plan de backup. Dado que muchas organizaciones no prueban habitualmente la recuperabilidad de sus backups, puede encontrarse en una situación en la que necesite un plan b o, incluso, un plan c para recuperar los datos que perdió.

La regla 3-2-1 garantizará que cuente con múltiples opciones para restaurar sus datos, y así sus backups no tengan ni un solo fallo. Considere esto como un backup de su backup; si algo le sucede a un backup, tiene un plan b. La regla 3-2-1 funciona así:

- **Tenga al menos tres copias de datos** (esto significa que debería tener al menos dos backups adicionales además de sus datos principales). Si algo le sucede a un backup, cuenta con otro al cual recurrir.
- **Guarde las copias en dos tipos de medios diferentes** (esto asegura que un problema o fallo en uno de los dispositivos no afectará la recuperabilidad en el otro). Por ejemplo, puede guardar un backup en cinta y otro en disco o cualquier otro destino, tal como un proveedor de nube, dispositivo USB, SAN/NAS, etc.
- **Conserve una copia de backup remota** (esta es la más importante). No deje que un evento local como un incendio o una inundación le impida el acceso a sus datos principales y a todas sus copias de backup al mismo tiempo. Puede hacer Backups secundarios sobre unidades de cinta, replicar a otra oficina o incluso a la nube, pero siempre es conveniente asegurarse de que existe una copia remota a una distancia razonable o dicho de otra forma una separación física entre sus entornos de Backup.

Veeam Backup & Replication posee una serie de funcionalidades que le garantizan que puede cumplir con la regla 3-2-1 y salvaguardar sus backups.

3 – Cómo proteger sus datos de backup y evitar perderlos

Sus backups sirven fundamentalmente como copia de su centro de datos completo, todos almacenados en una ubicación conveniente (o más si sigue la regla 3-2-1). Aunque esta es solo la naturaleza de un destino de backup, necesita asegurarse de que sus datos permanezcan seguros dondequiera que se encuentren. Se le da mucha atención al tema de asegurar hosts, redes, sistemas operativos y aplicaciones, pero también necesita prestarle atención a la seguridad de sus backups. ¿Qué hace para asegurar sus backups, que generalmente se encuentran fuera de sus puntos de seguridad tradicionales? Si alguien quisiera obtener sus backups, podría restaurar las VMs fácilmente y acceder a las aplicaciones y datos dentro de ellas. Esta amenaza podría venir desde dentro o fuera de su red porque los archivos pueden ser copiados fácilmente a través de las redes o transportados en pequeñísimos dispositivos USB. Además, si sus datos se van del sitio, tanto a otra ubicación como a la nube, tiene que confiar en que alguien más se los protegerá por usted.

Como resultado, necesita asegurarse de que extienda sus prácticas de seguridad para incluir sus repositorios de backup y reducir el riesgo de que alguien que no debe vea sus datos confidenciales. Puede lograr esto de muchas maneras, pero quizás la manera más simple sea la de cifrar sus repositorios de backup a través de su aplicación de backup. También podría considerar cifrar sus datos a través de un hardware mediante un hardware de almacenamiento que admita cifrados. Sin embargo, esto puede ser más costoso. También debería limitar de manera estricta el acceso a sus repositorios de backup solo a los administradores necesarios y revisar su acceso. Si realiza backups fuera de su centro de datos a una ubicación remota o proveedor de la nube, necesita trabajar con su proveedor de servicios para asegurarse de que tenga suficientes controles de seguridad en el lugar para mantener sus datos seguros.

Veeam Backup & Replication brinda un cifrado de 256 bits AES incorporado y de extremo a extremo, lo que le ofrece la posibilidad de cifrar sus Backups en orígen, en tránsito y en destino, para ayudarle a garantizar que su empresa no termine saliendo en los titulares de las noticias por incumplimiento de la seguridad.

4 – Aproveche los controles basados en la política para una protección de datos más inteligente

Cuando se trata de realizar cualquier cosa en la vida, ¿lo haría de la manera difícil o fácil? Realizar casi cualquier cosa de la manera difícil y obtener los mismos resultados generalmente es una pérdida de tiempo y de recursos, sin contar que lo deja vulnerable al error y al olvido humano. El centro de datos virtual está repleto de complejidades ocultas que pueden aumentar la administración, reducir la eficiencia, ocasionar problemas e inactividad no deseados. Un entorno virtual prácticamente pide una automatización que permita asegurar el cumplimiento, a la vez que reduce los esfuerzos de administración y garantiza que las cosas funcionen de la manera más fluida posible. Un administrador vSphere entendido siempre busca maneras de trabajar más inteligentemente en lugar de más arduamente, y utilizar cualquier tipo de automatización o controles basados en la política es la manera fácil, además de que garantiza coherencia.

La administración de almacenamiento basada en políticas (SPBM, por sus siglas en inglés), presentada en vSphere 5.5 con VSAN y más tarde para almacenamiento compartido en vSphere 6.0 con Volúmenes virtuales (VVols, por sus siglas en inglés), le permite definir los requisitos de almacenamiento para VMs basadas en la función de las matrices del almacenamiento o en las capacidades de hardware. La SPBM trata íntegramente sobre automatización y asegura que las VMs cumplan y se adapten adecuadamente a los recursos de almacenamiento. Cuando se trata de proteger VMs, se pueden crear políticas basadas en niveles específicos de RAID u otros atributos de disponibilidad de almacenamiento que se adaptan a sus requisitos de SLA. Otra función menos conocida de vSphere que puede ayudarle a simplificar y organizar la manera en la que interactúa con las VMs es la función de las etiquetas. Esta le permite personalizar la clasificación de sus VMs. Las etiquetas personalizadas se pueden crear y asignar a las VMs, y le permiten clasificarlas según los contenedores de vSphere no estándar (por ejemplo, según la aplicación, el rol, la ubicación, el departamento, etc.). Esto se puede usar con las funciones de vSphere o las aplicaciones de terceros que puedan realizar algún tipo de acción en las VMs con determinadas etiquetas.

Veeam Backup & Replication se integra completamente con el uso de etiquetas de vSphere que pueden aprovecharse cuando se configuran los trabajos de backup, de forma que le permiten personalizar las opciones de backup de manera más eficiente según la etiqueta asignada a cada VM.

5 – Conozca el impacto que tienen las nuevas funciones y arquitecturas de vSphere en la protección de datos

Mientras VMware continúa desarrollando vSphere para que se ajuste a su visión de centro de datos definido por el software, presentan muchas funciones y arquitecturas nuevas que cambian radicalmente la manera en la que se hacen las cosas en vSphere. Ninguna parte de vSphere se ha visto más afectada que el almacenamiento, con la presentación por parte de VMware de sus nuevas arquitecturas de almacenamiento de VSAN y VVols, cuyo propósito es reemplazar el datastore VMFS tradicional. La red también ha evolucionado con la nueva arquitectura de redes NSX y las infraestructuras hiper-convergentes (tales como EVO:Rail) son las últimas tendencias que unen servidores, almacenamiento y redes en un modelo de dispositivo único. Con todos estos cambios, puede preguntarse qué impacto tienen en la implementación de la protección de datos. ¿Está haciendo las cosas de manera incorrecta o ineficiente ahora? ¿Qué cambios debería hacer para adaptarse a estos cambios en vSphere?

Introducido en vSphere 5.5, VSAN transforma el almacenamiento del lado del servidor en una matriz de almacenamiento compartido que puede distribuirse entre muchos hosts ESXi. Con el SAN ubicado dentro de un servidor, los recursos de almacenamiento se encuentran mucho más cerca del host, lo cual es bueno para las cargas de trabajo de las VMs porque acorta la ruta E/S. Sin embargo, esto puede ser un arma de doble filo porque las operaciones de backup pueden ejercer mucha más presión de recursos en un host, que puede afectar el rendimiento general. Además, cambia la lógica del backup necesaria para tomar datos de la forma más eficiente. Como resultado, querrá aprovechar los controles de QoS (Calidad de servicio) que pueden limitar las operaciones de backup y asegurar que su aplicación de backup reconozca VSAN. Con VVols en vSphere 6.0, esta nueva arquitectura de almacenamiento incluye muchos componentes nuevos entre una matriz de hosts y almacenamientos pero es más transparente para las aplicaciones de backup. Existen algunas APIs nuevas incluidas en VSAN y VVols, por lo que necesita asegurarse de que su aplicación de backup soporte y utilice estas funciones de la manera más eficiente.

Puede estar seguro de que Veeam Backup & Replication está altamente optimizado para VSAN y VVols. Aprovecha al máximo las últimas APIs de vSphere para integrarse con estas nuevas arquitecturas de almacenamiento, por medio de una lógica inteligente y avanzada, y una selección óptima de proxies virtuales.

6 – Cómo aprovechar la nube como parte de su estrategia de protección de datos

La nube sirve como extensión interconectada y remota para su centro de datos virtual del que puede hacer uso para brindar alternativas adicionales a realizar todo en el lugar. Cuando se trata de la protección de datos, la nube puede usarse como repositorio remoto que puede eliminar la necesidad de que tenga que instalar su propio centro de datos de recuperación, que puede ser muy costoso de mantener. Aunque la nube generalmente no es un buen destino para el almacenamiento principal de backup, sirve como buen complemento para una solución de backup principal existente cuando se usa en un modelo de capas, que hace que múltiples copias de sus backups estén disponibles (regla 3-2-1). La mayoría de los fabricantes de soluciones de backup y proveedores de Servicios en la nube han hecho muy simple la integración entre centros de datos y aplicaciones en el sitio e infraestructura y servicios basados en la nube de modo que pueda llevar sus datos a la nube y viceversa fácilmente.

Cuando se trata de crear una estrategia en la nube, puede considerar tener backups de corto plazo (políticas de retención más cortas) en el Site Principal o local y almacenar en la nube Backups con períodos de retención más largos. Además, en lugar de solo usar la nube como almacenamiento en frío de sus VMs, podría usarla como un destino de replicación para que sirva como sitio de contingencia para ejecutar sus VMs, si fuera necesario. La nube brinda muchas posibilidades y sirve como un excelente complemento para su estrategia de protección de datos.
Al analizar proveedores de la nube, debe tener en cuenta que la fijación de precios generalmente se basa en el consumo de recursos y necesita comprender los costos en los que se incurrirá, ya que las operaciones de backup y restauración pueden necesitar de muchos recursos. En particular, mire las tasas de acceso y salida: puede descubrir que, si bien llevar datos a la nube es relativamente económico, recuperar grandes cantidades de datos puede ser mucho más costoso.

Cualquiera que sea la estrategia de nube que elija, Veeam Cloud Connect brinda una forma completamente integrada, rápida y segura de realizar backups y restauraciones desde la nube para que pueda llevar sus backups fuera del sitio sin el costo y la complejidad de administrar una infraestructura remota.

7 – Asegúrese de cumplir con todos los requisitos para proteger sus aplicaciones críticas

Cuando se trata de proteger cualquier aplicación que sea crítica para usted o para su negocio, no puede permitir que haya ningún percance, ya que puede ser muy costoso. Necesita asegurarse de que está haciendo todo lo necesario para realizar backups a las aplicaciones y garantizar que los datos sean 100 % recuperables en todo momento. Las aplicaciones de bases de datos y de correo electrónico en particular pueden ser las más complicadas para realizar backups y recuperar de forma correcta, ya que tienen requisitos de manipulación especiales que debe utilizar. Una de las partes más cruciales del proceso de backup es la inactividad, una función que asegura que los datos y aplicaciones que se ejecutan dentro de una VM estén en un estado adecuado (consistente) para realizarles un backup y que posteriormente y en caso de necesidad, puedan restaurarse de manera correcta. La inactividad pausa temporalmente una VM, por lo que cualquier escritura y dato pendiente en la memoria pueden escribirse en el disco antes de que comience el backup. Si no se deja una VM inactiva antes de realizarle un backup, puede descubrir que, tras la restauración, algo de la VM se ha corrompido o no se puede usar porque los archivos abiertos no se prepararon correctamente, , es decir no se ha realizado el Backup en un estado consistente.

Otra técnica especial utilizada durante el backup de la base de datos es el truncamiento de los registros de transacción que registran todas las transacciones y modificaciones realizadas a una base de datos que puede usar para recuperar una base de datos, si lo necesita. Los registros de transacción deben truncarse de manera regular para evitar que se hagan demasiado grandes. Una vez que se completa un backup de una base de datos de manera exitosa, los registros de transacción pueden truncarse porque el backup puede servir como un punto de recuperación. Después del backup, los registros de transacción se pueden usar para recuperación hasta que se complete el siguiente backup.

La recuperación granular es otro requisito clave que ofrece la capacidad de restaurar solo un subconjunto de datos, en lugar de una base de datos entera o un almacén de objetos de correo electrónico. Por ejemplo, si solo quiere restaurar algunos registros de una base de datos o un correo electrónico de un archivo de correo sin sobrescribir el original, su aplicación de backup tiene que admitir la recuperación granular.

Veeam Backup & Replication admite por completo backups consistentes con la aplicación y la transacción, lo que garantiza que a sus datos críticos se les realizó un backup de manera correcta. También admite el truncamiento de registros con el procesamiento de imagen con reconocimiento de aplicaciones. Para la recuperación, las aplicaciones de Veeam Explorer™ le permiten a los usuarios de Veeam restaurar objetos individuales para aplicaciones populares como Microsoft Active Directory, Exchange y SQL Server con un esfuerzo mínimo.

8 – Sepa que realizarle un backup a una VM a nivel del disco aún le brinda muchísimas opciones de restauración

En un entorno virtual, los backups se realizan a nivel de imagen de disco virtual para una máxima eficiencia. Aunque esto es muy bueno para la eficiencia, las solicitudes de restauración en la vida real generalmente se centran en restaurar objetos desde dentro de una VM, en lugar de la VM completa. Entonces, ¿qué sucede cuando necesita recuperar archivos individuales o elementos de aplicaciones? Cuando realiza backups a nivel de imagen, aún cuenta con la capacidad de ver dentro de la imagen del disco porque puede montarse a través de la aplicación de backup y acceder a ella por medio del sistema de archivos del SO dentro de la imagen. Esto le permite ver los archivos dentro de la imagen y restaurar archivos individuales según sea necesario. Además, le permite acceder a los almacenes de datos a nivel de la aplicación, tales como un archivo de base de datos o de correo electrónico. Sin embargo, restaurar una inmensa base de datos puede llevar mucho tiempo o ser difícil para que una pequeña cantidad de correos electrónicos o registros dentro de ella pueda restaurarse. Como resultado, su aplicación de backup necesita entender el formato de archivo de la aplicación para que pueda mirar dentro y restaurar solo los elementos que necesita.

Fuera de las bases de datos y los correos electrónicos, otra restauración común a nivel de la aplicación es con Microsoft Active Directory, que es una parte fundamental de cualquier infraestructura de Windows. Con Active Directory (AD), generalmente no es recomendable restaurar la estructura y datos completos de AD y debe tenerse especial cuidado para evitar interrumpir algo. Para lograr esta delicada restauración, una aplicación de backup debe poder acceder y buscar AD de forma nativa para que pueda restaurar cualquier objeto borrado a su ubicación original. Puede ver que los backups a nivel de imagen le brindan la capacidad de realizar muchos tipos diferentes de restauraciones en base a los requisitos para un escenario particular de recuperación. Si necesita restaurar una VM completa, un disco virtual de VM particular, uno o más archivos dentro de una VM, o un registro único de correo electrónico o base de datos, su aplicación de backup debe estar equipada para manipular estos escenarios de restauración más granulares.

Veeam Backup & Replication lleva esta restauración al extremo con 47 escenarios de restauración diferentes, que varían de un grupo de VMs en una vApp a una VM completa y todo el recorrido hacia abajo hasta los archivos individuales y los elementos a nivel de la aplicación para que pueda manipular casi cualquier escenario de restauración.

9 – Sáquele el mayor provecho a sus backups: haga que sus repositorios de backup trabajen por usted

Los backups son muy parecidos a las pólizas de seguro: son una inversión continua que le cuesta dinero y debe contar con la seguridad que le brindan pero realmente no obtiene nada a cambio a menos que tenga algún percance. Con la virtualización, es común hacer backups disco a disco y, opcionalmente, barrerlos a la cinta también. Sus backups de VM solo están ahí en sus repositorios de disco de destino, consumiendo espacio y recursos del disco valiosos y se ignoran completamente. Sin embargo, debido a que se encuentran en el disco, de hecho usted cuenta con copias utilizables del historial de sus VMs disponibles que podrían usarse para ciertos propósitos. Imagine que necesitara un SandBox rápido para evaluar una actualización de una aplicación o un entorno aislado para hacer algunas pruebas o solucionar problemas: aquellas copias de backup son candidatas perfectas, y si las aislara en sus propias redes virtuales, podría realizar lo que quisiera sin causar interrupciones en el entorno de producción.

Veeam ha hecho esto posible en Veeam Backup & Replication con la creación de Virtual Lab que usa el servidor de backup como un servidor NFS, con los repositorios de backup comportándose como dispositivos de almacenamiento. Cualquier host ESXi puede conectarse a él y acceder a los backups de VMs que estén en el repositorio. Las imágenes de backup son de solo lectura y cualquier cambio que se les realice mientras se ejecutan, se descartan con posterioridad. Las VMs que se ejecutan desde el repositorio se mantienen aisladas del resto de la red, y un dispositivo de enrutamiento especial permite el acceso a las redes externas. Esto también le permite verificar de manera automática sus backups, por lo que puede asegurarse de que son recuperables. Ya abordamos la regla 3-2-1, pero cuando se realizan backups con Veeam, se transforma en la regla 3-2-1-0, donde el "0" significa "0 errores" durante la verificación de recuperabilidad automática de cada backup con SureBackup® y Sure Replica de Veeam.

De hecho, poder usar sus backups para otros propósitos fuera de la restauración ocasional de forma que podrá maximizar el retorno de la inversión en su backup.

10 – No se quede corto: haga sus cuentas de backup

La planificación de la capacidad para sus backups es importante para asegurarse de que pueda seguir cumpliendo con el programa de retención que ha fijado, tanto por elección propia o como resultado de un SLA. La planificación de la capacidad para sus repositorios de backup no es una tarea sencilla porque los entornos virtuales tienden a expandirse rápidamente debido a la proliferación de VMs. ¿Tiene alguna idea de cuánto le durará su capacidad actual? ¿Sabe cómo le afectará el agregarle cinco VMs más? Si se queda corto, o tiene costos no planeados en los que debe incurrir para expandirla, o la longitud de su retención debe cortarse. Ninguna es la situación más conveniente. Como resultado, hacer las cuentas de backup para descubrir cuándo deberá incrementar el almacenamiento que está destinado a su repositorio de backup de retención puede ser un desafío. Las cuentas de backup no son tan directas como la planificación de la capacidad de almacenamiento tradicional porque existen muchos factores que pueden afectar sus cálculos. Estos incluyen los índices de compresión de backup, la longitud de retención de backup, la frecuencia de backup y las tasas de cambio en los datos para backups incrementales. Lo que necesita es una aplicación de backup inteligente que pueda hacer las cuentas por usted.

Veeam ONE™ brinda herramientas de análisis y monitorización de las infraestructuras de vSphere y descubre problemas potenciales que pueden afectar el rendimiento de sus backups y aplicaciones de producción. Veeam ONE puede alertarlo cuando el espacio del repositorio de backup alcance un determinado nivel e incluye un informe de Estimación de tasa de cambios de las VMs, que analiza de manera automática la tasa de cambios de sus VMs y calcula la cantidad potencial de espacio requerido en su repositorio de backup.

Hay más aspectos importantes en los Backups que solo contar con espacio suficiente para almacenarlos: también tiene que contar con suficientes recursos de host disponibles para que se completen dentro del marco temporal de ventana de backup deseado. El informe de Evaluación del rendimiento del datastore le ayudará a examinar el rendimiento de su datastore para identificar problemas potenciales que puedan ocurrir durante el proceso de backup debido a valores de latencia alta o de IOPs. Esta información es útil cuando se definen los umbrales de latencia para que pueda optimizar el rendimiento de procesamiento de su backup, aumentar la eficiencia de uso de recursos y minimizar el impacto en las cargas de trabajo de la producción. Veeam ONE es un excelente complemento para Veeam Backup & Recovery, y le brinda la visibilidad que se necesita para mantener un entorno de backup saludable.

Acerca del autor

Eric Siebert es un veterano en la industria de TI, orador, autor y bloguero con más de 25 años de experiencia que se ha centrado en la virtualización desde el año 2005. Siebert ha publicado libros que incluyen su más reciente, "Maximum vSphere", de Pearson Publishing, y ha publicado cientos de artículos y documentos técnicos para público de tecnología y socios de VMware. También ejecuta y mantiene su propio sitio web de información sobre VMware, vSphere-land.com. Siebert es un orador frecuente en las conferencias y eventos de la industria incluido VMworld, y ha sido reconocido como vExpert por VMware cada año desde el comienzo de los programas en el año 2009.

Acerca de Veeam Software

Veeam® reconoce los nuevos desafíos a los que se enfrentan empresas de todos los tamaños alrededor del mundo para habilitar Always-On Business™, que debe funcionar las 24 horas del día, los 7 de la semana y los 365 días del año. Para tratar esto, Veeam ha liderado un nuevo mercado de la Disponibilidad para empresas Always-On (Availability for the Always-On Enterprise™). A diferencia de las soluciones de "backups tradicionales" que proporcionan objetivos de punto de recuperación (RPO) y de tiempo de recuperación (RTO) de horas o días, Veeam ayuda a las empresas a cumplir con objetivos de tiempo y punto de recuperación (RTPO™) de menos de 15 minutos para todas las aplicaciones y datos. Esto se logra básicamente mediante un nuevo tipo de solución alternativa que brinda una recuperación de alta velocidad, elusión de pérdida de datos, protección verificada, datos aprovechados y visibilidad completa. Veeam Availability Suite™, que incluye Veeam Backup & Replication™, aprovecha las tecnologías de virtualización, almacenamiento y de la nube que le permiten al centro de datos moderno ayudar a las organizaciones a ahorrar tiempo, mitigar riesgos y reducir significativamente los costos operativos y de capital.

Fundada en 2006, Veeam cuenta en la actualidad con 34.500 ProPartners y más de 168.000 clientes a lo largo del mundo. La sede central global de Veeam se ubica en Baar, Suiza, y la empresa cuenta con oficinas en todo el mundo. Para obtener más información, visite http://www.veeam.com/es-lat.

MUY PRONTO DISPONIBLE

VEEAM
IT JUST WORKS!™

AVAILABILITY
for the Always-On Enterprise™

Nuevo Veeam® Availability Suite™ v9

RTPO <15 minutos para TODAS las aplicaciones y datos

Obtenga más información en vee.am/v9