MÁS SOBRE ERIC SIEBERT
Haga clic aquí para obtener más información sobre el autor

MÁS INFORMACIÓN SOBRE EL SOFTWARE DE VEEAM
Haga clic aquí para obtener más información sobre el patrocinador

escrito por Eric Siebert

LAS 10 MEJORES PRÁCTICAS para la Protección de Datos VMware

VEEAM
www.veeam.com

No dude en publicar esto en su blog o enviarlo por correo a quien crea que pueda beneficiarle su lectura.

¡GRACIAS!

Tabla de contenidos

Resumen

Hacer backups de sus máquinas virtuales (MV) puede parecer un proceso simple y sencillo, pero realmente es más complicado de lo que parece a simple vista. Hacer backup de servidores físicos es bastante sencillo; no tiene más que instalar un agente en un servidor y agregarlo al calendario de backup. Pero hacer backup de MVs de manera eficiente necesita usar técnicas y características que hayan sido diseñadas específicamente para los entornos virtuales. Si trata las máquinas virtuales de idéntica forma a como lo hace cuando hace backup o restaura servidores físicos, malgastará recursos y alargará la ventana de backup más de lo necesario. La virtualización es la responsable del cambio de juego en el centro de datos, y una vez implementada, será necesario cambiar sus procedimientos y métodos para poder así aprovechar sus puntos fuertes y su arquitectura única.

La arquitectura de virtualización ofrece muchas ventajas a las operaciones de backup y recuperación en servidores. Cambia las técnicas tradicionales utilizadas para hacer copia de seguridad de servidores para aprovechar las características de la virtualización, simplificando el proceso de backup y recuperación para hacerlo más eficiente. También proporciona una mayor flexibilidad y opciones a la hora de realizar copias de seguridad, restaurar máquinas virtuales e implementar la recuperación ante desastres. En este documento técnico se ofrecen 10 consejos para ayudarle en la implementación de las copias de seguridad y el proceso de recuperación en un entorno virtual. Este incluye los métodos, técnicas y configuraciones adecuadas para ello, así como el uso de las funciones incluidas en Veeam Backup & Replication™ versión 5 para llevar sus procesos de respaldo un paso más adelante.

1

No haga backup de las MVs en la capa del SO huésped

> **"El resultado es que puede hacer backup de más MVs simultáneamente y el host dispone de más recursos para sus MVs"**

Cuando aborda el método que utilizará para realizar la copia de seguridad de sus MVs, no debe mantener el mismo sistema con el que creaba las copias de respaldo de sus servidores físicos. La copia de seguridad de los servidores físicos se realiza tradicionalmente mediante el uso de un agente instalado en el sistema operativo (OS) huésped del host, y el servidor de backup se conecta al agente para copiar los datos desde este. Este método seguiría funcionando en una MV, pero ignorar la capa de virtualización cuando ejecuta sus backups es poco eficiente y un gasto inútil de los valiosos recursos del host. La mejor forma de hacer backup de las MVs es hacerlo en la capa de virtualización, y para ello necesita una aplicación de backup que se haya diseñado y optimizado específicamente para un entorno virtualizado. Al adoptar la virtualización, una aplicación de backup no tiene por qué involucrar al sistema operativo huésped (guest) de la MV en el proceso de copia. En lugar de eso, la aplicación puede conectar directamente con el archivo de disco de la MV para copiarlo.

Con este sistema se consigue que no se produzca ninguna sobrecarga de recursos en la MV mientras se está realizando la copia de seguridad, y la carga de trabajo no se ve afectada mientras se ejecutan los procesos de copia. Además, dependiendo del método de backup utilizado, es posible reducir o eliminar de igual modo la utilización de recursos en el host. El resultado es que pueden copiarse más MVs simultáneamente y el host dispone de más recursos disponibles para sus MVs. Veeam Backup & Replication fue diseñado partiendo de cero específicamente para realizar backups de entornos Vmware, y opera al nivel de la capa de virtualización para conseguir la eficiencia máxima en el backup. Por lo tanto, asegúrese de que al adoptar la virtualización, cambia sus métodos de backup y utiliza una aplicación que sea capaz de operar en la capa de virtualización para lograr la máxima eficiencia.

2 Aproveche las APIs vStorage

> **"Permite realizar backups más rápidamente ya que los datos se leen en la red de almacenamiento, y además reduce la utilización de la red en el host"**

Las vStorage APIs for Array Integración (VAAI) se incorporarón a vSphere para permitir que aplicaciones de terceros pudieran integrarse fácilmente con las funciones de vSphere relacionadas con el almacenamiento.

Estas APIs fueron desarrollada para reemplazar a VMware Consolidated Backup (VCB) y permiten a las aplicaciones de backup interactuar directamente con vSphere. Se agrupan en distintas categorías, siendo VAAI for Data Protection (VADP) la que más beneficios brinda a las aplicaciones de backup y recuperación. Tal vez la característica más notable de VADP sea la función Changed Block Tracking (CBT), que permite a las aplicaciones buscar rápidamente los bloques del disco virtual de una MV que han cambiado a partir de un punto determinado en el tiempo. Este es un asunto primordial, puesto que en condiciones normales serían las propias aplicaciones las que deberían ocuparse de esta tarea, lo que inevitablemente puede llevar su tiempo. Al ser capaces de obtener esta información al instante, se acelera en gran medida las operaciones de backup y de replicación incremental, lo que se traduce en ventanas de backup más breves y en la posibilidad de conseguir una Protección casi Continua de Datos (near-CDP) sin necesidad de adquirir costoso hardware de almacenamiento. Existen también otras características de las VAAIs que benefician las operaciones de backup, tales como, la capacidad de agregar en caliente el disco de una MV de destino a una MV de origen que esté ejecutando una aplicación de backup, de forma que pueda copiarse sin necesidad de pasar por la red para leer el disco virtual. Esto permite realizar backups más rápidamente, puesto que los datos se leen desde la red de almacenamiento, y se reduce la utilización de la red en el servidor host. Las VAAIs suponen un gran beneficio para todas las funciones relacionadas con el almacenamiento en vSphere, y utilizar aplicaciones que no las aprovechen resulta en una reducción de la eficacia. Veeam Backup & Replication fue una de las primeras aplicaciones de backup en abrazar las VAAIs y aprovechar al máximo la eficiencia que brindan. Si desea realizar backups de la manera más eficiente posible, asegúrese de que su solución de copia de seguridad es capaz de aprovechar las VAAIs.

3

"Quiescing" de la máquina virtual y VSS para una protección definitiva

> **"Es preferible un estado consistente del sistema de archivo porque el sistema operativo se encuentra en el estado adecuado para realizar su copia."**

El quiescing (pausa o modo inactivo) es una función crítica en las aplicaciones de backup y replicación. Esta función asegura que la información y aplicaciones de una máquina virtual se encuentran en un estado en el que pueden copiarse de forma que su restauración posterior sea posible y correcta. Esto es de extrema importancia en el caso de datos transaccionales que residan en servidores de correo y bases de datos. El quiescing es en esencia una palabra estrambótica para llamar a la pausa o detención temporal de la MV, en donde cualquier escritura pendiente y datos contenidos en la memoria puedan copiarse a disco antes de que comience el proceso de backup. Este proceso es llevado a cabo por el sistema operativo, además de las aplicaciones que soporten el ser pausadas (quiescing). Una vez que se ha aplicado el comando de pausa a la MV, se crea una instantánea (snapshot) de la MV para congelar su disco, de forma que pase a ser de sólo lectura y pueda iniciarse el proceso de backup. Si no se hace un quiescing previo de la MV antes de iniciar el proceso de backup, es probable que en el restore, algunos de los contenidos resulten dañados o hayan quedado inservibles, ya que los archivos abiertos no estaban preparados adecuadamente para añadirse al backup. En Windows, el quiescing de las MVs es gestionado por Volume Shadow-Copy Service (VSS) de Microsoft. Está integrado en Windows y trabaja con el sistema operativo y las aplicaciones a fin de prepararlas para los snapshots y backups. Existen varios estados de consistencia asociados al modo inactivo a la hora de restaurar datos: consistencia de caídas (crash), de sistema de archivo y de aplicación.

Un estado consistente de caída no involucra ningún proceso de pausa (quiescing) y es equivalente a haber interrumpido la alimentación de una MV sin haberla apagado correctamente. Un estado consistente del sistema de archivo es mejor porque el sistema operativo se encuentra en un estado adecuado para realizar su copia. Por último, el mejor estado es el consistente con la aplicación, en el que las aplicaciones también se han preparado adecuadamente para el proceso de copia de seguridad. Veeam Backup & Replication hace un uso completo del modo inactivo, aprovechando VSS a través de las funciones de quiescing integradas en VMware Tools. Además, Veeam también desarrolló su propio método para trabajar directamente con VSS en aplicaciones en las que VMware Tools no soporta el modo inactivo.

4

No haga un aprovisionamiento insuficiente para los recursos objetivos de backup

> **“Es mejor equivocarse en exceso al determinar el tamaño del hardware de su servidor de backup.”**

Las operaciones de backup pueden consumir gran cantidad de recursos en cualquier área del centro de datos. Como resultado, la mayoría de las empresas buscan las ventanas de backup más breves posibles para así provocar el menor impacto en las cargas de trabajo de producción. Puede disponer de almacenamiento, servidores y dispositivos de red todo lo rápidos que quiera, pero el servidor de backup puede convertirse fácilmente en un cuello de botella si no dispone de los recursos necesarios para digerir todos los datos que fluyen dentro y fuera de este. Como era de esperar, las operaciones de backup pueden impactar enormemente en los recursos de red y almacenamiento, ya que el servidor de backup mueve datos desde los servidores de origen a destinos de cinta o disco. Pero los procesos de backup no implican únicamente el traslado de datos desde el punto A al punto B; el servidor de backup también es el responsable de algunas funciones avanzadas, como la deduplicación, la compresión, y es el encargado de determinar qué bloques de disco necesitan copiarse y cuáles no. Por lo tanto, además de implicar un alto nivel de utilización del disco y de la red, el servidor de backup normalmente también consumirá gran cantidad de recursos de CPU y memoria.

Debería asegurarse de que dimensiona el tamaño de su servidor de backup de manera adecuada para no crear un cuello de botella en cualquier área de recursos. Asegúrese también de que le dota con la suficiente capacidad de proceso (CPU) y memoria para que pueda tener bajo control los datos que se transfieren y lograr un rendimiento máximo reduciendo las ventanas de backup. Es mejor equivocarse en exceso al determinar el tamaño de los recursos hardware de su servidor de backup. Si su servidor de backup es una máquina virtual, le será más fácil ajustar sus recursos de hardware para encontrar el equilibrio perfecto. Puede realizar cambios fácilmente en el hardware virtual hasta que encuentre la configuración que le ofrezca el mejor resultado sin llegar a un exceso innecesario de asignación de recursos. Veeam recomienda para el servidor de backup una CPU de por lo menos 4 a 8 núcleos para conseguir la mejor eficiencia de backup.

5

No necesita hardware de almacenamiento costoso para conseguir near-CDP

> **"Como resultado, obtener near-CDP en la capa de virtualización ya es una realidad y es una alternativa más asequible para la replicación del almacenamiento."**

Para muchas empresas es suficiente con disponer de protección near-CDP (Protección casi Continua de los Datos) y además les ofrece una solución de recuperación ante fallos aceptable para sus aplicaciones críticas. Antes, para conseguir near-CDP había que confiar en un hardware de almacenamiento costoso y añadir además al sistema un software de replicación. Este gestionaría la replicación de los datos de la MV en la capa de almacenamiento desde un sistema de almacenamiento a otro, de forma que estuviera preparado para utilizarse como backup en caso de ser necesario. La arquitectura de virtualización permite utilizar otros métodos para lograr este mismo objetivo. Debido a que las máquinas virtuales se encapsulan en archivos de disco virtual, la replicación también se puede realizar en la capa de virtualización que se encuentra entre la capa de hardware y la capa del sistema operativo. Aunque llevar a cabo la replicación en la capa de virtualización puede no ser tan eficaz como dejar que se ocupe de ello el array de almacenamiento, todavía puede desempeñar el trabajo de manera eficaz.

La replicación de una MV es similar, en esencia, a su backup, pero con la diferencia principal de que los backups son un evento diario mientras que la replicación es un proceso continuo. La replicación consiste básicamente en realizar backups incrementales con una frecuencia muy elevada. Veeam Backup & Replication desde su concepción ha tenido la capacidad de replicar máquinas virtuales de un host origen a un host de destino. Near-CDP se define como un objetivo de punto de recuperación (RPO) lo más cercano posible a cero, por lo general menor de 30 minutos. Sin embargo, en VMware VI3, obtener protección near-CDP no era demasiado práctico, porque la cantidad de tiempo y los recursos necesarios para calcular los datos que habían sufrido variación entre los ciclos de replicación, para a continuación copiarlos, podían ser elevados. vSphere cambió todo eso con la nueva función CBT que convirtió las operaciones de backup y replicación incremental en un proceso mucho más rápido. El resultado es que conseguir protección near-CDP en la capa de virtualización es ya una realidad y una alternativa más asequible para la replicación del almacenamiento.

6

Sacar el máximo partido a sus backups - hacer que sus repositorios de backup trabajen para usted

> **"La forma en la que consiguen esto es realmente ingeniosa, el servidor de copia de seguridad se convierte en un servidor NFS convirtiéndose los repositorios de backups en el almacenamiento propiamente dicho."**

Las copias de seguridad son muy parecidas a una póliza de seguros, le siguen costando dinero y necesita la seguridad que proporcionan, pero no obtendrá nada de ellas a no ser que se produzca una emergencia. Con la virtualización es muy común hacer copias de seguridad de disco a disco, y opcionalmente pasarlas también a cinta. Las copias de seguridad de sus MVs se acumulan en los repositorios de disco de destino ocupando un valioso espacio en disco y recursos, y suelen ser completamente ignoradas. Pero dado que estas residen en el disco, dispone de un historial de copias de sus MVs operativas que podría utilizar para determinados propósitos. Imagine que necesitara rápidamente un sandbox (entorno de prueba) para probar una actualización, o un entorno aislado para hacer otro tipo de pruebas o solucionar problemas. Esas copias de sus MVs son candidatas perfectas para ello, y si las aísla convenientemente de su propia red virtual, podría hacer lo que quisiera sobre ellas sin alterar en ningún caso el entorno de producción. Veeam ha hecho esto posible con su novedosa tecnología vPower™ que forma parte de la versión 5 de Veeam Backup & Replication. El modo en el que realmente implementan esta función es realmente ingenioso, puesto que el servidor de copia de seguridad se convierte en un servidor NFS con los repositorios de backup como dispositivos de almacenamiento. Cualquier servidor ESX/ESXi puede conectarse a él usando el cliente NFS y acceder a las copias de la MV que se encuentran en el repositorio. Las imágenes de backup son de sólo lectura, y cualquier cambio realizado sobre ellas mientras están activadas es guardado en un archivo delta independiente que después de todo es descartado. Las MVs puestas en marcha desde el repositorio son mantenidas en un entorno aislado del resto de la red usando para ello vSwitches que no poseen NICs físicos asignados, y un appliance de enrutamiento especial permite el acceso a las redes externas. El poder hacer uso real de sus backups para otros propósitos que no sean el de la simple restauración ocasional le permite sacar el máximo partido a su inversión en backup.

7 *Use la deduplicación y compresión de datos para reducir el tamaño del backup*

> **"Otro beneficio de la deduplicación es que los bloques de disco vacíos que han sido asignados a una MV, pero aún no han sido escritos por el sistema operativo huésped, son ignorados y no se copian."**

Con el tiempo, sus repositorios de backup pueden crecer mucho y antes de que se de cuenta se habrá quedado sin espacio físico para almacenar sus copias de seguridad. Cuando esto sucede, su única opción es adquirir más almacenamiento o limitar el número de copias de seguridad que almacena en su repositorio. Ninguna de las soluciones es deseable, así que para evitar esa situación debería usar tecnologías que ayuden a reducir el tamaño de los datos que se almacenan en sus repositorios de backup. Estas tecnologías son la deduplicación de datos (que evita que sean copiados en el repositorio de backups bloques de datos duplicados) y la compresión de datos (que comprime los datos de su repositorio de backup para que ocupen menos espacio). Otro beneficio de la deduplicación es que los bloques de disco vacíos que han sido asignados a una MV pero aún no han sido escritos por el sistema operativo huésped son ignorados y no son copiados. Existen distintos métodos para llevar a cabo la deduplicación y no todos los productos de backup la soportan o la incluyen de forma nativa. Uno de los métodos más frecuentes es el sistema en línea donde la deduplicación se realiza en tiempo real, el cálculo de códigos hash se realiza antes de que los bloques sean almacenados en el repositorio de backup y, si coinciden con un bloque de disco ya almacenado, son referenciados con el bloque guardado y no se copian al repositorio. Aunque esto resulta beneficioso a la hora de reducir los tamaños de backup, puede causar una sobrecarga extra mientras los backups están en ejecución, ya que los cálculos hash deben efectuarse en cada bloque de disco. Veeam Backup & Replication le permite seleccionar entre varias opciones de deduplicación que utilizan distintos tamaños de bloque a la hora de calcular los códigos hash, con lo que puede elegir si desea la máxima deduplicación a costa de ralentizar las copias de seguridad, o la mínima deduplicación para obtener un mayor rendimiento y velocidad en el proceso. Veeam Backup & Replication también soporta múltiples niveles de compresión que variarán la cantidad de compresión aplicada para satisfacer las necesidades del entorno. El proceso de compresión requiere de una gran cantidad potencia de proceso (CPU) y puede incrementar la duración de los backups, así que se recomienda al menos disponer de CPUs de 8 núcleos en el servidor de backup para utilizar el máximo nivel de compresión.

8

Verificar sus backups para garantizar que pueden restaurarse adecuadamente

> **“La verificación automática es posible arrancando la MV de respaldo directamente desde el repositorio de backup y comprobando el latido de la misma y las respuestas obtenidas mediante ping desde las herramientas VMware Tools”**

No hay nada peor que hacer copia de seguridad de los servidores durante meses y meses para descubrir, cuando es necesario hacer una restauración crítica, que los datos que ha estado respaldando no son útiles una vez que se restauran. El único sentido de hacer copias de seguridad es que un día pueda contar con ellas para restaurar los datos cuando se produzca un desastre, o incluso cuando por error se eliminen datos, de lo contrario la carga de trabajo será inútil. Si no es capaz de restaurar los datos correctamente ¿por qué tan siquiera copiarlos desde un principio? El proceso de comprobar las copias de seguridad implica algo más que hacer una simple verificación de los datos en su medio de backup, lo que sólo confirmaría que los bloques de disco se han guardado correctamente en el dispositivo de destino. Si para empezar, existiera algún problema con los datos en el origen, este problema se copiaría junto con los datos al dispositivo de respaldo inevitablemente. Este problema puede ir desde, algún servidor que no haya sido pausado o puesto en modo inactivo adecuadamente antes de ser copiado, a la existencia de archivos críticos corruptos o eliminados en un servidor. Por ello, la única forma de garantizar verdaderamente que sus copias de seguridad funcionan correctamente es restaurar los datos a un servidor y comprobar que todo funciona de la forma esperada. La virtualización puede facilitar este proceso considerablemente, puesto que no necesita contar con hardware físico libre para restaurar en él todo un servidor; las MVs pueden restaurarse fácilmente en hosts con capacidad libre. Pero esto puede convertirse en un proceso que lleva demasiado tiempo si se realiza con regularidad. Veeam reconoció el problema y ha convertido la comprobación de los backups, con su nueva tecnología SureBackup incluida en Veeam Backup & Replication versión 5, en una parte automatizada integrada en el mismo proceso de backup. La verificación automática es posible arrancando la MV de respaldo directamente desde el repositorio de backup y comprobando el latido de la misma y las respuestas obtenidas mediante ping desde las herramientas VMware Tools. Adicionalmente pueden ejecutarse scripts de prueba para comprobar que las aplicaciones se ejecutan adecuadamente y que puede accederse a los datos. La única cosa más importante que las copias de seguridad son los restores de los backups. Tener la tranquilidad de saber que dispone de copias de seguridad operativas es una buena política de seguro con la que contar cuando los datos deben restaurarse.

9 Recuperación granular desde un backup a nivel de imagen

> **"El resultado es la posibilidad de restaurar rápida y fácilmente elementos de la aplicación con un mínimo esfuerzo."**

Para lograr la máxima eficiencia, las copias de seguridad en un entorno virtual se hacen a nivel de imagen.

Pero, ¿qué pasa cuando necesita recuperar archivos individuales o elementos de aplicación? En la mayoría de los sistemas operativos huésped de MVs, el servidor de backup puede montar el archivo de disco virtual de la copia de seguridad de forma que sea posible restaurar archivos individuales. Una vez que la imagen de disco virtual está montada, puede navegar por ella y seleccionar los archivos que quiere restaurar, que son copiados seguidamente al destino que usted elija. Veeam Backup & Replication soporta recuperación instantánea a nivel de archivo de forma que puedan restaurarse archivos individuales rápidamente desde un punto de backup cualquiera en el tiempo. Esto permite la restauración de archivos individuales, pero ¿qué ocurre con elementos de aplicación individuales que estén contenidos en un único archivo de aplicaciones transaccionales como puedan ser Microsoft Exchange y SQL Server? Restaurar por completo una gran base de datos implica un proceso demasiado largo y complejo para que unos cuantos mensajes de correo y algunos registros contenidos en ella sean recuperados y restaurados en la base de datos original. Afortunadamente, existen métodos para restaurar elementos de aplicación sin tener que restaurar todo el archivo en el que residen. Veeam Backup & Replication contiene una función especial llamada Universal Application-Item Recovery (U-AIR™) que le permite restaurar objetos individuales de aplicaciones conocidas como Microsoft Active Directory, Exchange y SQL Server. ¿Cómo es esto posible? En pocas palabras, U-AIR aprovecha la capacidad de poder iniciar o arrancar una MV directamente desde el repositorio de backup y mantenerla aislada del resto de la red. Una vez que la MV está en marcha, se accede a la aplicación de manera que puedan copiarse los registros seleccionados desde la MV a su ubicación original. El resultado es la posibilidad de restaurar rápida y fácilmente elementos de la aplicación con un mínimo esfuerzo. Como puede ver, los backups a nivel de imagen en la capa de virtualización son muy versátiles y son capaces de posibilitar restores de elementos de aplicación, archivo e imagen desde un único backup de imagen.

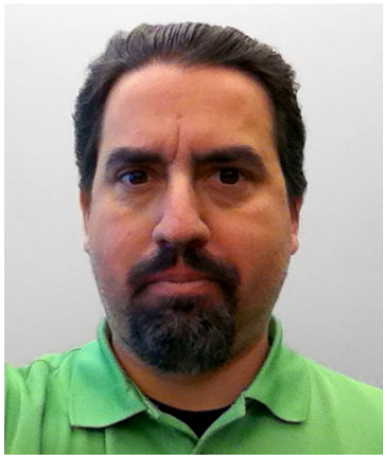
10

Evite la compleja situación de asignar permisos a los administradores de backup para toda su información sensible

> **“Se consigue asegurar más sus datos de aplicación y eliminar posibles vulnerabilidades procedentes del interior de su SO (huésped) y aplicaciones.”**

Para poder hacer backup de los datos de sus servidores, su servidor de backup tiene que tener acceso a ellos para poder leer la información. Esto quiere decir que sus administradores de backup deben tener acceso al sistema de archivo local y a las aplicaciones en cada uno de los servidores de los que desee hacer copia de seguridad. Además, si está ejecutando agentes de backup específicos para aplicaciones como Microsoft Exchange & SQL Server para poder copiar los datos de la capa de aplicación, necesitará también otorgar el acceso a todos los datos contenidos en la aplicación. Desde el punto de vista de la seguridad esto puede suponer un problema, puesto que el sistema se apoya en la confianza inherente de que los administradores no accederán de forma maliciosa a los datos sensibles a los que tienen acceso. La virtualización ha cambiado esta situación, puesto que ya no es necesario acceder al sistema operativo o a la aplicación para hacer backup de los datos que allí residen. En lugar de instalar dentro del sistema operativo “huésped” un agente de backup y dar permisos de acceso al administrador, su aplicación de backup puede acceder a los datos desde el exterior del sistema operativo huésped y leerlos en la capa de virtualización. Esto se conoce como un backup a nivel de imagen, dado que se copia la imagen completa del disco virtual a nivel de bloque, en lugar de leer archivos individuales como hacen los agentes de backup de sistema operativo. El resultado es que ya no tiene que asignar permisos a los administradores de backup dentro del sistema de archivos del SO (huésped) o de aplicaciones que se ejecutan en la MV. Veeam Backup & Replication con U-AIR hace posible la recuperación de elementos de aplicación individuales a pesar de no utilizar agentes de aplicación específicos, y los propietarios de la aplicación mantienen el control de sus datos en todo momento. Este sistema garantiza aún más la seguridad de sus datos de aplicación y elimina posibles vulnerabilidades procedentes del interior de su SO (huésped) y aplicaciones. Veeam vPower está revolucionando la forma en la que se realizan los procesos de copia de seguridad y recuperación en los entornos virtualizados, ofreciendo mayor flexibilidad, mejor seguridad y un incremento en la fiabilidad de sus datos más valiosos.

Acerca del autor



Eric Siebert es autor y blogger con más de 25 años de experiencia en el sector de la TI, especializado en administración y virtualización del servidor. Es un miembro muy activo de los foros de soporte VMware VMTN, donde ha conseguido el status de gurú ayudando a otros con sus retos de virtualización.

Siebert ha publicado varios libros entre los que incluyen su reciente, **"Maximum vSphere"** de Pearson Publishing, y ha editado vídeos de formación en la serie Train Signal. También mantiene su propio portal web de información sobre VMware VI3, vSphere-land, y es un blogger habitual y articulista colaborador de los sitios web de TechTarget SearchServerVirtualization y SearchVMware. Siebert participó en el VMworld de 2008 y 2010, y ha sido reconocido por VMware como vExpert en 2009 y 2010.

VEEAM

#1 VMware Backup

100% Reliability | Best RTOs | Best RPOs

SureBackup™ | InstantRestore™ | SmartCDP™

vPower™
Virtualization-Powered Data Protection™

5 Patents Pending!

VMware vSphere

5 Patentes Pendientes!

NUEVO Veeam Backup & Replication™ v5

vPower facilita este cambio de juego en las capacidades de Veeam Backup & Replication v5:

- **Instant VM Recovery**— restaura una máquina virtual completa EN MINUTOS ejecutándola directamente desde el archivo de copia de seguridad
- **U-AIR™ (Universal Application-Item Recovery)**— recupera objetos individuales desde CUALQUIER aplicación, o CUALQUIER Sistema Operativo
- **SureBackup™ Recovery Verification**— comprueba automáticamente la recuperabilidad de TODAS las copias de seguridad, de TODAS las máquinas virtuales, en TODO momento

Para más información, visite www.veeam.com/vPower

Veeam ONE

Solución para la administración VMware

vPower

Virtualization-Powered Data Protection

Veeam Reporter 4.0 *for VMware*

Informes empresariales, gestión de cambios y planificación de la capacidad para VMware

Veeam Monitor 5.0 *for VMware*

La solución de referencia para la monitorización, planificación de la capacidad y resolución de problemas en toda su infraestructura VMware.

Veeam nworks Management Pack 5.5 for Microsoft Ops Mgr *for VMware*

Monitorización VMware con Microsoft System Center

Veeam Smart Plug-in 5.5 for HP Operations Mgr *for VMware*

Monitorización del entorno VMware con HP Operations Manager

Veeam Backup & Replication v5 *for VMware*

Virtualization-Powered Data Protection™

Veeam Backup & Replication ofrece una solución 2 en 1 con backup y replicación para máquinas virtuales ejecutándose en servidores ESX(i) VMware. Al aprovechar el entorno virtual y la tecnología pendiente de patente Veeam vPower™, Veeam Backup & Replication supera las limitaciones de la protección de datos y recuperación ante desastres tradicional para proporcionar un sistema de recuperación rápido, flexible y fiable para todas sus aplicaciones, servicios y datos virtualizados.