GUÍA DEL COMPRADOR PARA LA COPIA DE SEGURIDAD Y LA RECUPERACIÓN

ÍNDICE

INTRODUCCIÓN

La copia de seguridad y la recuperación necesitan una reconsideración radical. Cuando se diseñaron las forzosas soluciones actuales hace más de una década, los entornos de TI estaban explosionando, la heterogeneidad era creciente, y la copia de seguridad era la protección de último recurso. El objetivo era proporcionar una póliza de seguro de bajo coste para los datos y como soporte de este heterogéneo entorno multinivel cada vez más complejo. La respuesta fue combinar soluciones de copia de seguridad y de recuperación bajo una estructura de gestión de proveedores común y minimizar los costes moviendo los datos a través de la infraestructura o los soportes.

Las constantes subyacentes eran que las copias de seguridad necesitan ser fiables y que las restauraciones han de ser rápidas y fiables.

¿Qué es lo que ha cambiado? En primer lugar, los departamentos de TI han evolucionado hacia modelos de nube privada, con virtualización y arquitecturas convergentes en sustitución de las arquitecturas multinivel. En segundo lugar, la cantidad de datos gestionados ha explosionado y, por tanto, la TI tiene que afrontar el reto de hacer más con menos. Actualmente los equipos están compuestos por menos roles especializados y más roles generales. Por último, las nubes públicas e híbridas han abierto nuevos casos de uso de los datos, como pueden ser analíticas y pruebas/desarrollo, pero se enfrentan a retos para gestionar dichos datos.

Cualquier profesional de TI que considere invertir en copia de seguridad debería preguntarse qué antiguos supuestos son aún relevantes y si un nuevo enfoque es mejor. En esta guía, discutiremos la copia de seguridad y la recuperación y la emergencia de la Gestión de datos en la nube, que proporciona oportunidades para proteger los datos, capturar nuevo valor y hacer que los datos se encuentren disponibles siempre y donde sea necesario.

Agradecimientos especiales a aquellos miembros de la comunidad de TI que han proporcionado su perspectiva sobre estos temas.

> Estamos en una nueva era en la que las empresas están impulsando los cambios dentro de la TI. Las soluciones han de cubrir en primer lugar las necesidades empresariales y luego las necesidades técnicas.
>
> **Andrea Mauro, @Andrea_Mauro, http://vinfrastructure.it**

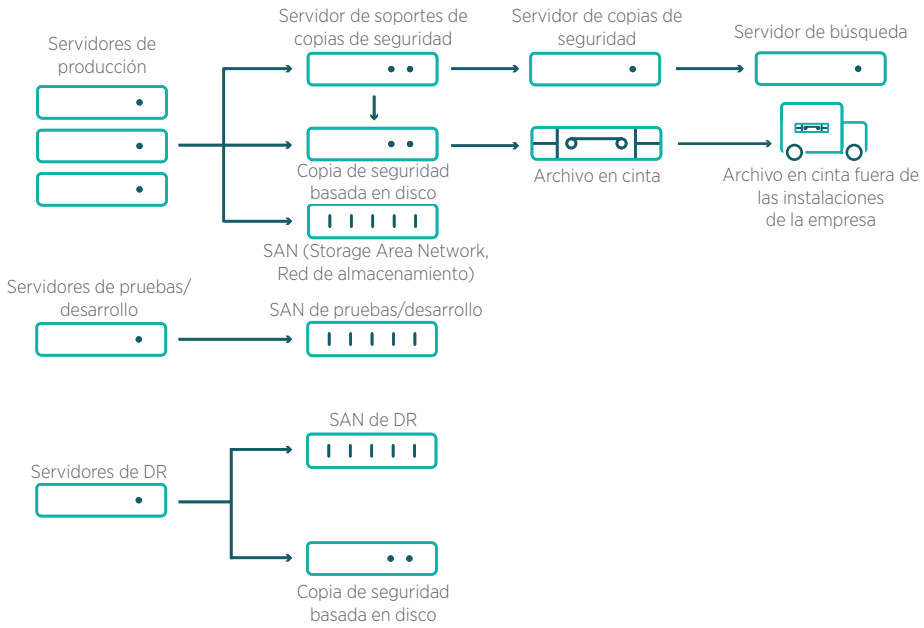
QUÉ ERA LO QUE IMPORTABA ANTERIORMENTE

REQUISITOS Y RETOS DE LA COPIA DE SEGURIDAD TRADICIONAL

El primer lote de soluciones de copia de seguridad y recuperación se crearon para afrontar los retos de niveles de aplicación basados en una infraestructura heterogénea. Las soluciones de copia de seguridad y recuperación, como plataforma de último recurso, se convirtieron en el punto de la consolidación lógica. Los sistemas de copia de seguridad necesitaban mover grandes cantidades de datos a través de entornos en expansión y gestionarlos a través de niveles de soportes para controlar los costes. Los sistemas de copia de seguridad tradicionales también habían de satisfacer requisitos de conservación de los datos a largo plazo, utilizando generalmente archivos en cinta fuera de las instalaciones de la empresa.

Veremos los requisitos y las restricciones retrocediendo más de 10 años. Dichos requisitos y restricciones todavía se aplican frecuentemente en muchos centros de datos debido a la "deuda técnica" o a soluciones aún en funcionamiento que no justifican su revisión desde una perspectiva empresarial.

GESTIÓN DE SUS DATOS ACTUALMENTE



Complejidad de los entornos actuales - múltiples sistemas, proveedores y arquitecturas.

FLEXIBILIDAD DEL TRABAJO Y LA PROGRAMACIÓN

Históricamente el foco se encontraba a menudo en las ventanas de copia de seguridad y las programaciones del trabajo. Estas áreas eran necesarias para lograr los RPO (Objetivo de Punto de Recuperación) y RTO (Objetivo de Tiempo de Recuperación) deseados para una empresa. Desafortunadamente, esto convertía frecuentemente a los ingenieros en "programadores de trabajo divinizados" - una complicación inesperada de las complejas arquitecturas.

> RPO and RTO son los héroes ocultos cuando se trata de la recuperación de una interrupción del negocio en TI. Poder tener la confianza de que puede cumplir o superar el SLA que usted tiene con la empresa es lo que marca la diferencia entre esperanza y estrategia real y probada.
>
> **Eric Wright, @Discoposse, http://discoposse.com**

El Objetivo de Punto de Recuperación (Recovery Point Objective, RPO) define el punto en el tiempo utilizado para la restauración y está determinado por la frecuencia de las copias de seguridad. En el caso de un fallo del sistema primario, un RPO inferior significa menos pérdidas de datos. Los sistemas de copia de seguridad y recuperación consiguen RPOs bajos gracias a la realización de copias de seguridad más frecuentes a expensas de un mayor tráfico viajando a través de la red y más copias de datos almacenadas. En el caso de aplicaciones para misiones críticas, los RPOs necesitan encontrarse disponibles como puntos en el tiempo medidos en minutos en lugar de horas o días.

El Objetivo de Tiempo de Recuperación (Recovery Time Objective, RTO) define cuánto se tarda en recuperar un objeto como puede ser un archivo, un servidor o un centro de datos. Un menor RTO significa menos tiempo de inactividad en caso de un fallo del sistema primario, pero a expensas de utilizar soportes de acceso más caros y rápidos, como puede ser un disco, así como switches de red costosos para mover de nuevo los datos a donde se pueda acceder a ellos.

Representación visual de RPO y RTO

REPLICACIÓN

La replicación es la capacidad de copiar datos desde una ubicación primaria a una ubicación secundaria. A menudo se refiere a una recuperación de desastres porque protege frente a un fallo a nivel de todo el emplazamiento en la ubicación primaria. La replicación está relacionada únicamente de forma indirecta con RPO y RTO; el supuesto es que la mayoría de los fallos se producen a nivel de subsistemas más que a nivel del emplazamiento. No obstante, la replicación es un requisito común para aplicaciones críticas.

> La protección de los datos es una parte vital de cada Plan de continuidad de la empresa, ya que la pérdida o el deterioro de los datos podría tener un inmenso impacto. Aunque existen diferentes soluciones para resolver distintos aspectos de recuperabilidad y redundancia de los datos, lo más importante es tener un enfoque claro para lograr unos buenos RPO y RTO.
>
> **Andrea Mauro, @Andrea_Mauro, http://vinfrastructure.it**

TRADUCCIÓN DE LOS REQUISITOS DE LA EMPRESA

Con todo ello en mente, el requisito clave para cualquier solución de copia de seguridad y de recuperación es coger los requisitos a nivel de la empresa para tiempo de recuperación y recuperación de datos, conocidos de otro modo como Acuerdos de Nivel de Servicio (Service Level Agreements, SLA), y traducirlos a un conjunto de instrucciones para ubicar, conservar y extinguir datos en diferentes soportes de almacenamiento.

El principal problema con los sistemas de copia de seguridad y recuperación tradicionales es que la "traducción" de los requisitos de la empresa a instrucciones ejecutables de la plataforma requiere servicios profesionales. En otras palabras, las soluciones tradicionales tienen modelos operativos imperativos frente a declarativos. Además, una vez finalizada dicha traducción, estas soluciones tradiciones carecen de inteligencia para optimizar los recursos y evitar copias de seguridad fallidas. Esto, a su vez, conduce a un ajuste continuo y, en algunas ocasiones, al rediseño de la arquitectura.

La mejor forma de evaluar los RPO y RTO en su sistema actual es pedir a un ejecutivo que recoja algunos datos (usar diferentes tipos granulares) de puntos aleatorios en el tiempo. Cuantifique qué proximidad al RPO puede lograr y el RTO de la recuperación. Compare esto con el coste del tiempo de inactividad mientras se realiza la recuperación. Ésta ha sido siempre una de las áreas más exigentes de los sistemas de copia de seguridad y recuperación.

> Si no comprende sus requisitos de RPO y RTO, no entiende sus cargas de trabajo. Y si no comprende sus cargas de trabajo, no valora los datos de la empresa ni valora la empresa.
>
> **Dan Frith, @penguinpunk, http://www.penguinpunk.com**

COPIA DE SEGURIDAD EN CINTA Y CONSERVACIÓN A LARGO PLAZO

La copia de seguridad y la recuperación están diseñadas normalmente para la conservación de datos a corto plazo, hasta un período máximo de un mes. Para la conservación de datos a largo plazo, se utiliza el archivo, con unos marcos de tiempo habituales de 1 a 7 años. La conservación de datos a largo plazo es especialmente importante en empresas que requieren conformidad normativa, como pueden ser las instituciones sanitarias o financieras.

Hasta hace muy poco, la única opción económicamente viable para el archivo era la cinta. Para todos salvo para las empresas más grandes, la cinta implica manipulación manual, almacenamiento fuera de las instalaciones de la empresa, registro y rotación de las cintas. La restauración desde cinta requiere mucho tiempo, es manual y complicada, ya que las cintas se almacenan normalmente fuera de las instalaciones de la empresa, y la restauración de un simple archivo requiere un sistema más amplio o la restauración por volúmenes. Adicionalmente, las cintas se degradan con el tiempo y han de actualizarse a formatos de soportes más modernos.

La cinta también rebaja el valor de los datos al aislarlos. Los datos archivados en cinta normalmente están mal indexados y su accesibilidad es limitada. Al colocar sus activos estratégicos más valiosos en una "caja fuerte", sus datos quedan bloqueados y se reduce su valor para la empresa.

En algunos países, se exigió explícitamente el archivo en cinta para cumplir los requisitos de conservación de datos, legales y normativos. Además, un número creciente de agencias y jurisdicciones están adaptando las políticas de conservación de datos para especificar requisitos funcionales en lugar de soportes.

> Si es complejo, esto significa que puede hacerse incorrectamente de más formas. Cuanto más sencillo es el proceso, menos probabilidades existirán de configurarlo mal.
>
> **Eric Wright, @Discoposse, http://discoposse.com**

INSTALACIÓN Y CONFIGURACIÓN COMPLEJAS

La configuración y la instalación de software de copia de seguridad para empresas siempre ha sido un reto. Prácticamente todos los proveedores requieren servicios profesionales para instalar y configurar un sistema de copia de seguridad para que toda la funcionalidad prometida se encuentre disponible. Para poder utilizar el sistema, los administradores a menudo tienen que asistir a una formación de una semana. La copia de seguridad y la recuperación han de ser intuitivas para que un administrador medio pueda utilizarlas. Además de ser fácil de configurar y administrar, la copia de seguridad deberá estar automatizada en la mayor medida de lo posible. Esto garantiza que los nuevos sistemas estén automáticamente protegidos al añadirlos.

> Cualquier solución con un nivel suficiente de complejidad está condenada a asfixiarse en su propia deuda técnica. Centrémonos en soluciones fáciles de usar y sencillas de gestionar para ganar la confianza de TI y de la empresa.
>
> **Eric Shanks, @eric_shanks, theithollow.com**

COSTE

El coste de la copia de seguridad y la recuperación siempre ha significado una parte importante del presupuesto de TI. Los datos han crecido exponencialmente, al igual que el coste de la realización de copias de seguridad y el almacenamiento de los datos. En algunas ocasiones, la protección de datos incluso cuesta más que el almacenamiento primario. Las organizaciones de TI experimentadas a menudo tienen que duplicar o triplicar el coste de los datos primarios para cubrir los costes de protección y copia de seguridad de los datos.

¿QUÉ ES LO QUE IMPORTA ACTUALMENTE?

REQUISITOS Y RETOS DE LA COPIA DE SEGURIDAD MODERNA

Si usted construye una solución de copia de seguridad y recuperación actual, ¿qué aspecto tendría? ¿En qué se parecería a una solución de copia de seguridad tradicional? Los requisitos de soportar SLAs personalizables basándose en el RPO y el RTO, la recuperación de desastres y la capacidad de archivo seguirían siendo los mismos.

¿Qué es lo que sería diferente? Los departamentos de TI están adoptando cada vez más modelos de nube híbridos, por lo que necesitan una estructura (hiper)convergente con escalabilidad modular y niveles crecientes de virtualización. La solución debería reflejar asimismo que los equipos de TI de la empresa están adoptando tecnologías como pueden ser IoT, Big Data y DevOps para sacar el máximo provecho al valor de los datos. Y, por último, debería priorizar la seguridad, ya que los ataques de ransomware y la fuga de datos son amenazas en constante crecimiento.

> La virtualización permite proteger no solamente archivos y datos de aplicaciones sino también la máquina virtual (VM) completa - efectivamente una recuperación completa más sencilla.
>
> **Andrea Mauro, @Andrea_Mauro, http://vinfrastructure.it**

VIRTUALIZACIÓN

La mayoría de los sistemas de copia de seguridad estaban diseñados originalmente para soportar hosts físicos. La virtualización ha sido la última ola importante en la innovación informática. Antes de la virtualización, la memoria RAM y la CPU de los sistemas estaban infrautilizadas, lo que proporcionaba recursos durante las horas libres para procesos de copia de seguridad. La virtualización supuso que el uso global de la RAM y la CPU fuera impulsado extraordinariamente, y el almacenamiento pasó a una matriz central. Sin una planificación cuidadosa o tecnología más moderna, las copias de seguridad podrían empujar a los sistemas virtualizados más allá de sus recursos máximos.

> La virtualización ha acelerado la expansión de los entornos y el supuesto de que debería "simplemente funcionar" debido a lo fácil que se ha hecho disponer de un servidor. Automáticamente demos por hecho que deberíamos ser capaces de proteger y recuperar esos recursos con la misma rapidez con la que los suministramos.
>
> **Eric Wright, @Discoposse, http://discoposse.com**

SENCILLEZ Y AUTOMATIZACIÓN

Los departamentos de TI se están despojando de roles especializados, como pueden ser los administradores de copias de seguridad, y los están sustituyendo por roles más generalizados, como son los administradores de TI. Las soluciones de copia de seguridad y recuperación han de ser sencillas de utilizar, con interfaces de usuario perfectamente diseñadas, y no requerir una extensa formación para el uso diario.

Estas soluciones también necesitan aceptar operaciones declarativas, sin instrucciones de bajo nivel manejadas mediante heurística e inteligencia, requiriendo una intervención mínima por parte de los administradores. Las soluciones también han de ser fácilmente extensibles y automatizadas con interfaces API RESTful para aceptar herramientas de scripting como pueden ser Chef, Puppet y Ansible, entre otras.

> La automatización ya no es solo para tiendas de TI de vanguardia. Los administrados de TI de la vida diaria pronto estarán ejecutando llamadas de API para aprovisionar y gestionar la infraestructura que da soporte a sus aplicaciones. Una API robusta ha de ser parte de estas soluciones de centros de datos si quieren ser relevantes.
>
> **Eric Shanks, @eric_shanks, The IT Hollow**

VENTANAS DE COPIA DE SEGURIDAD MÁS CORTAS FRENTE A ENTORNOS MÁS GRANDES

Los datos continúan creciendo y los departamentos de TI modernos están gestionando más datos que nunca, mientras las ventanas de copia de seguridad siguen reduciéndose. Las copias de seguridad necesitan proteger más datos, de forma más fiable y en un período de tiempo más corto. Los nuevos enfoques, como son las copias de seguridad basadas en instantáneas, suprimen la necesidad de detener las aplicaciones para realizar las copias de seguridad y eliminan las cargas de recursos (de los agentes de copia de seguridad) sobre los hosts.

USO DE LA NUBE Y AGILIDAD DE APLICACIONES

Otra tendencia actual es el uso creciente o el uso planificado de la Nube para ejecutar cargas de trabajo ágiles o aplicaciones nativas de la Nube. El almacenamiento y el archivo en la Nube están además reduciendo su coste rápidamente. Así pues, los departamentos de TI de las empresas no pueden ignorar la futura exigencia de que los datos estén o bien ubicados en la nube o bien fácilmente orquestados a y desde la nube o una nube privada. Las nuevas funciones como el archivo en la nube pueden constituir un método elegante para migrar datos a la nube. Normalmente, los datos de la producción residen en un sistema de copia de seguridad local.

Muchos clientes utilizan la cinta debido al requisito de que existan múltiples copias de seguridad almacenadas independientemente de la ubicación de datos principal. La replicación en la nube satisface este requisito y a menudo permite la eliminación de las copias de seguridad en cinta, a menos que sean exigidas por la normativa.

CONTROLES DE SEGURIDAD Y ACCESO

El robo de datos y otros modos de ciberdelincuencia continúan proliferando en sofisticación y frecuencia. Las amenazas para la seguridad pueden originarse actualmente dentro del cortafuego o en la nube. Los datos que se encuentran en una nube híbrida han de asegurarse con encriptación en descanso y en vuelo, y necesitan disponer de controles de acceso adecuados para evitar el robo y los daños.

SEGURIDAD DE LAS COPIAS DE SEGURIDAD Y RANSOMWARE

El robo de copias de seguridad es una de las herramientas favoritas de los hackers y de los ladrones de identidad. Se requieren medidas especiales para evitar la manipulación y garantizar la conformidad normativa de los datos sensibles. Entre otros elementos, examine su sistema de copia de seguridad para comprobar si es vulnerable a problemas de seguridad subyacentes del sistema operativo.

ZDNET estima el coste de los ataques de ransomware a IT en 1000 millones de dólares solamente en este año. ¿Está preparado?

El ransomware es software malicioso que bloquea el acceso a sus sistemas hasta que no pague dinero para eliminar el código. Aunque las estimaciones varían, más del 40 por ciento de las organizaciones posiblemente experimentan un ataque de ransomware cada año. Un sistema de copia de seguridad y recuperación debería poderle permitir una recuperación rápida y de confianza. La falta de un sistema que permita la recuperación eficaz de un ataque de ransomware puede tener impactos financieros y de reputación importantes sobre su empresa.

¿QUÉ DEBERÍA IMPORTARLE A USTED?

SELECCIÓN DE UNA SOLUCIÓN DE COPIA DE SEGURIDAD Y RECUPERACIÓN PARA HOY Y PARA EL FUTURO

El cambio de proveedores de copia de seguridad siempre requiere cierto nivel de esfuerzo técnico u organizativo. Así pues, si está considerando un cambio, he aquí algunas preguntas que ha de plantearse: ¿La solución de copia de seguridad es algo que ha estado funcionando años con muy pocos cambios? ¿Es algo creado a partir de adquisiciones de múltiples empresas que se han juntado apresuradamente? ¿Requiere múltiples sistemas e interfaces para gestionar la copia de seguridad y la recuperación, la replicación, el archivo y la conformidad?

La innovación en la copia de seguridad empieza por reconocer que un nuevo enfoque ha de alinearse con los extraordinarios cambios tecnológicos y el crecimiento de los datos en los centros en la última década. Actualmente, existen nuevos enfoques de los visionarios del sector, que comprenden las necesidades empresariales actuales y la rapidez de los cambios en el sector.

> La nube puede utilizarse como un objetivo de bajo coste y a largo plazo para los datos de copia de seguridad o los datos de archivo. En este caso, el riesgo de dependencia podría ser mínimo debido a que simplemente puede mover sus datos a otro proveedor de la nube.
>
> **Andrea Mauro, @Andrea_Mauro, http://vinfrastructure.it**

Le recomendaríamos tener en cuenta los elementos de las secciones anteriores para determinar si aún son relevantes para su empresa. Asimismo, existen elementos adicionales específicos si está considerando una solución para ayer, para hoy y para el futuro.

GESTIÓN DE DATOS EN LA NUBE

La Gestión de datos en la nube está diseñada para orquestar datos de aplicaciones de misión crítica a través de nubes privadas y públicas a la vez que se unifica la copia de seguridad, la recuperación instantánea, la replicación, la búsqueda, las analíticas, el archivo, la conformidad y la gestión de los datos de copia en un tejido escalable. Las soluciones construidas para la generación de la nube eliminan la complejidad de los sistemas del pasado gracias a un motor de políticas automatizado que gestiona los datos a lo largo de su ciclo de vida en todas las funciones de gestión de los datos. La visión es proporcionar un tejido de software enraizado en una plataforma en la nube independiente de los proveedores, lo cual impide el bloqueo del proveedor a cualquier nube particular.

> El bloqueo es siempre un reto, pero tenemos que aceptar que es parte del trato. Siempre que disponga de procesos que le proporcionen la máxima flexibilidad posible, el riesgo de bloqueo podrá reducirse. La Nube es un inmenso activo para la copia de seguridad y la recuperación, tanto para datos en frío como para potencialmente la recuperación de estilo entorno de pruebas. Por buenas razones, la nube pública será algo grande en la mente de cada CIO, tanto para cargas de trabajo activas como para la recuperación.
>
> **Eric Wright, @Discoposse, http://discoposse.com**

SOPORTE DEL ECOSISTEMA

Muchas empresas se dirigen a la virtualización al 100%. Una solución de copia de seguridad y recuperación moderna debería estar diseñada para ser compatible, estar optimizada e integrarse con los entornos virtualizados. Los métodos como pueden ser flash pueden manejar grandes volúmenes de datos en entornos virtuales sin afectar a la producción. Busque características como puede ser la búsqueda indexada global, que permitan un acceso rápido a los datos y la recuperación granular instantánea.

No obstante, muchas empresas no están totalmente virtualizadas. Una solución de copia de seguridad y recuperación potente proporciona plena funcionalidad para entornos físicos y le permite gestionar todos los entornos desde una sola interfaz.

La copia de seguridad de dispositivos de almacenamiento conectado en red (Network Access Storage, NAS) debería hacerse con un método independiente del proveedor, sin plugins específicos de proveedores o formatos de almacenamiento exclusivos. Adicionalmente, esto debería hacerse en un formato nativo, al contrario que NDMP, que no requiera "desempaquetado" antes de una restauración. Una solución ideal requiere copias de seguridad completas periódicas pero es incremental para siempre. Por último, todas las funcionalidades de la plataforma de copia de seguridad deberían encontrarse disponibles para copias de seguridad de NAS.

MOTOR DE POLÍTICAS DECLARATIVAS Y AUTOMATIZACIÓN

Con una menor especialización entre los administradores de TI, la copia de seguridad sencilla se ha convertido en un elemento no negociable para muchas organizaciones. Las soluciones de copia de seguridad y recuperación han de ser utilizables por todos los miembros del equipo.

Mientras la arquitectura tradicional ha confiado en el modelo imperativo, el modelo declarativo es sencillo de comprender y puede alinearse fácilmente con los objetivos de la empresa. Con un modelo declarativo, un administrador introduce su estado deseado para una carga de trabajo en un motor de políticas. Una vez establecida la política, el sistema inteligente la ejecuta. Irónicamente, un motor de políticas potente incluso elimina algunas de las necesidades tradicionales de automatización, ya que el sistema puede tratar los requisitos con menos pasos manuales.

Deje que su motor de políticas piense por usted

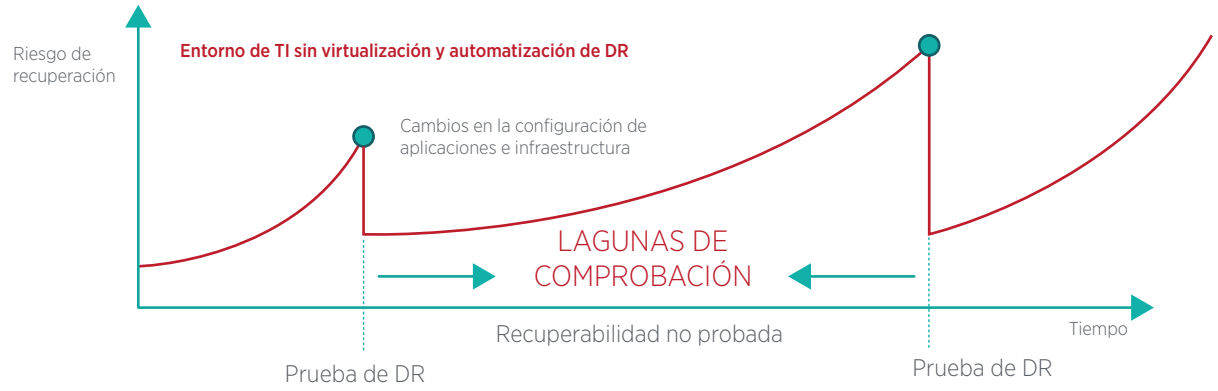
Las políticas de SLA le permiten reducir múltiples configuraciones implementadas manualmente a una sola política fácil de configurar y de mantenimiento cero.

Más allá de eso, una solución con una arquitectura API-first permite una automatización adicional. Conecte con servicios de terceros para automatizar la protección de datos, la recuperación y otros flujos de trabajo de gestión de datos personalizados.

> La automatización es crítica. La automatización significa consistencia y reducción de la necesidad de gastar un valioso tiempo de ingeniería realizando procesos diarios -- todo, desde las tareas de menor importancia hasta los procesos de aprovisionamiento y protección más complejos. Una hora gastada automatizando un proceso puede ahorrar literalmente semanas.
>
> **Eric Wright, @Discoposse, http://discoposse.com**

Adicionalmente, la automatización permite la validación periódica de las copias de seguridad - un requisito para mitigar el riesgo de "lagunas de comprobación" según se muestra a continuación. Si las copias de seguridad no se comprueban regularmente, el departamento de TI no podrá garantizar su validez para la empresa.

Riesgo en el tiempo



Sin la comprobación periódica, garantizar restauraciones fiables es imposible.

Más allá de eso, una solución con una arquitectura API-first permite una automatización adicional. Conecte con servicios de terceros para automatizar la protección de datos, la recuperación y otros flujos de trabajo de gestión de datos personalizados.

SEGURIDAD Y CONFORMIDAD

La gestión de datos ha de ser segura en dos dimensiones -- gestión y datos

La gestión incluye la capacidad de configurar acceso de roles al uso de los datos, generación de informes de conformidad y la posibilidad de monitorizar eventos del sistema, tareas operativas, capacidad, registros y eventos de los usuarios.

Los datos seguros implican la encriptación tanto en descanso como al vuelo, la gestión de claves y la capacidad para recuperarse instantáneamente de violaciones como puede ser el ransomware. Si usted se encuentra dentro de un sector con estrictas políticas de seguridad como HIPAA, su solución de copia de seguridad deberá estar diseñada para alinearse con estos requisitos.

FÁCIL ESCALABILIDAD

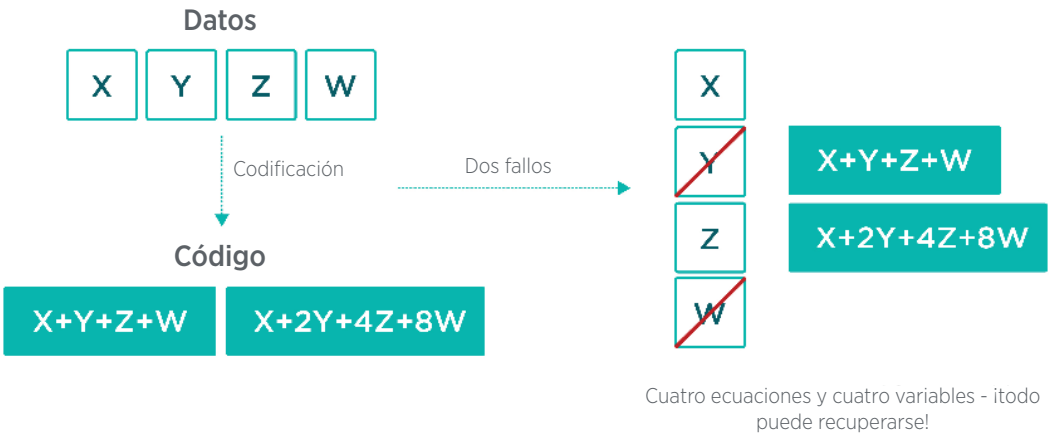
Como los entornos primarios modernos con los que son compatibles, las soluciones de copia de seguridad y recuperación necesitan poderse escalar rápida y fácilmente si no quieren correr el riesgo de ser un cuello de botella para el crecimiento. Así pues, una solución moderna ha de construirse utilizando hardware no especializado y software escalable con gestión de grupos sencilla. Esta solución debería poder escalarse desde TB de datos a PB de datos con un rendimiento y una usabilidad consistentes.

A la hora de seleccionar un proveedor de software de copias de seguridad, es importante conocer la facilidad para escalar la solución y el tamaño máximo hasta el que puede escalarse. Los metadatos y los datos deberían distribuirse por todos los nodos dentro del grupo y admitir desduplicación global. Ningún nodo de gestión sencillo debería ser un punto de fallo, y el sistema debería tener capacidad de autorreparación. Cuando el sistema tenga un fallo de nodo, averigüe si las restauraciones del sistema son tan eficientes como cuando el sistema es totalmente funcional.

Normalmente, las soluciones de copia de seguridad también tienen una cantidad específica de datos de los que es posible hacer una copia de seguridad. Una vez alcanzado dicho límite, es necesario un sistema independiente. Una solución realmente escalable debería permitirle añadir nodos de copia de seguridad que aprovechen la tecnología actual y puedan escalarse al entorno completo. Esto le permitirá encontrar datos de una sola fuente y aprovechar la desduplicación global. La adición de nodos debería ser un proceso sencillo que no requiera días de reequilibrado de los datos o servicios profesionales para su gestión.

La eficiencia de los datos es otro componente importante de una solución escalable. Las soluciones de copia de seguridad modernas utilizan métodos de codificación, como la codificación de borrado, que son tolerantes a fallos e incrementan la capacidad de almacenamiento sin afectar al rendimiento.

Eficiencia de los datos a través de la codificación de borrado



Cuatro ecuaciones y cuatro variables - ¡todo puede recuperarse!

Métodos de protección modernos que permiten reconstrucciones más rápidas con menores gastos generales de espacio de almacenamiento.

COSTE FRENTE A VALOR

La comprensión del coste real de las copias de seguridad es extraordinariamente difícil. Usted necesita saber de cuántos datos dispone, el tipo de datos (estructurados o no estructurados), la cantidad de granularidad requerida para los RPO y durante cuánto tiempo se almacenarán las copias de seguridad. El coste de las copias de seguridad incluye el software y el hardware, el coste de la WAN para replicación y copia de seguridad, los costes de coubicación y los costes de las pérdidas de ingresos y de productividad de la empresa durante la ventana de recuperación.

INMUTABILIDAD

Según se ha descrito anteriormente, los ataques de ransomware se están convirtiendo en cada vez más comunes. Disponer de copias de seguridad inmutables que no puedan ser encriptadas mediante ransomware es una parte crítica de la estrategia de protección. Pregunte a su proveedor de copias de seguridad si le puede garantizar que las copias son inmutables y no pueden ser encriptadas por ransomware incluso si el sistema no está bien configurado.

MÁS ALLÁ DE LA PROTECCIÓN

La protección de los datos ya no es simplemente una cuestión de seguridad. La mayoría de las empresas esperan actualmente aprovechar su plataforma de copia de seguridad y recuperación para casos de uso adicionales - archivo en la nube, entornos de pruebas/desarrollo, migración a la nube y más.

Al mismo tiempo, estos nuevos y a menudo casos de uso secundarios no deben menoscabar el objetivo principal - añadir funcionalidad que menoscabe los objetivos principales de copia de seguridad y recuperación no es factible operativamente.

En resumen, busque plataformas que puedan ayudarle a aprovechar sus datos para casos de uso que vayan más allá de la copia de seguridad y la recuperación para impulsar iniciativas empresariales. Asegúrese de las funcionalidades adicionales no sean simplemente características de “casilla de verificación” sino que puedan proporcionar un valor real a su empresa.

CONCLUSIÓN

A la hora de considerar soluciones de copia de seguridad y recuperación, la solución ha de ser sencilla y escalable. Ha de proporcionar portabilidad y accesibilidad de los datos en una era de la nube. El coste total de propiedad debería ser inferior que cuando usted está pagando por su sistema antiguo y ofrecer funciones innovadoras.