Guía del comprador de soluciones de recuperación ante desastres como servicio

INFORMACIÓN BÁSICA

Usar una ubicación local como destino de la recuperación ante desastres es caro y complicado. La recuperación ante desastres como servicio distribuida sin complicaciones en la cloud pública global tiene ventajas integradas que la convierten en un destino perfecto para la recuperación ante desastres.

CONSIDERACIONES PRINCIPALES

1. ¿Qué objetivos de tiempo de recuperación (RTO) necesitan las diferentes aplicaciones?
2. ¿El servicio ofrece automatización y coordinación de la conmutación por error?
3. ¿Sería muy complicado cambiar de plataforma las aplicaciones?
4. ¿Puede realizar pruebas de recuperación ante desastres sin interrupciones?
5. ¿Qué fiabilidad ofrece la infraestructura del sitio de recuperación ante desastres?

Muchas organizaciones son conscientes de la importancia de implementar una solución de recuperación ante desastres (DR) o se ven obligadas a hacerlo para cumplir las normativas gubernamentales. Mantener una ubicación local separada para que funcione como destino de la recuperación ante desastres supone un arduo esfuerzo; además, se necesita una gran inversión para su implementación y mantenimiento, especialmente teniendo en cuenta que no se utiliza a diario. La recuperación ante desastres como servicio (DRaaS) que se ejecuta en una cloud pública elástica con automatización integrada permite reducir el hardware infrautilizado y las tareas de mantenimiento, simplificar la implementación en caso de desastre y aumentar la fiabilidad de la solución de DR mediante pruebas que no causan interrupciones.

Las soluciones de DR locales a menudo resultan caras, y es necesario contar con amplios conocimientos para implementarlas, mantenerlas y utilizarlas. Implementar un sitio de DR local implica pagar íntegramente por el espacio físico, el hardware y el software de DR, pero usarlos solo cuando falla el centro de datos principal. Por tanto, es difícil para los responsables de la toma de decisiones de TI justificar los elevados gastos de dichas iniciativas. Incluso después de implementar la solución de DR, las pruebas suelen exigir mucho trabajo y causar interrupciones. Como resultado, muchas organizaciones no garantizan la protección de sus aplicaciones esenciales en caso de desastre. Para superar estos desafíos, muchas se plantean trasladarse a la cloud pública. Con esta guía, se pretende ayudar a las organizaciones a comprender los factores clave que deben tener en cuenta a la hora de considerar la cloud pública como una solución para sus necesidades de DR.

MODELOS DE SOLUCIONES DE RECUPERACIÓN ANTE DESASTRES

1. **Copia de seguridad solo de los datos**
   Estas soluciones replican los datos de las organizaciones en un sitio local secundario o en la cloud. Sin embargo, dejan a las organizaciones expuestas a largos tiempos de inactividad durante los desastres, ya que las aplicaciones no tienen infraestructura en la que funcionar. Tampoco incluyen pruebas de DR sencillas, y requieren bastante trabajo manual una vez adquirida la infraestructura.

2. **DR automática en un sitio local o en una coubicación**
   Las soluciones de este tipo reducen los esfuerzos manuales, pero requieren una alta inversión de capital en espacio físico, hardware y software que se usarán poco. Además, es más difícil de ampliar.

3. **DR automática en centros de datos propiedad de los proveedores de DRaaS**
   Estas soluciones ofrecen casi tantas ventajas como la DR automática en un sitio local; además, cuentan con una mejor estructura de costes que se corresponde con el bajo uso del objetivo de DR.

   Los clientes de estas soluciones deben valorar la fiabilidad de la infraestructura de DR y la estabilidad financiera del proveedor de DRaaS.

4. **DR automática en una megacloud global**
   Estas soluciones ofrecen casi tantas ventajas como la DR automática en un sitio local; además, cuentan con una mejor estructura de costes que se corresponde con el bajo uso del objetivo de DR.

   Los clientes de estas soluciones disfrutan de las ventajas de un riesgo menor gracias a la fiabilidad de la infraestructura, la disponibilidad global y la estabilidad financiera del proveedor de megacloud. Sin embargo, para implementar algunas de estas soluciones, es necesario que los clientes cambien de plataforma sus aplicaciones.

Factor 1: Identificar los objetivos de tiempo de recuperación de las diferentes aplicaciones

Aunque es cierto que las organizaciones pueden proteger todas sus aplicaciones, hacerlo puede resultar muy caro. En lugar de eso, deben clasificar sus aplicaciones en base a sus objetivos de tiempo de recuperación (RTO), que es el periodo de tiempo durante el cual se puede tolerar que la aplicación no esté en línea. Para algunas soluciones DRaaS, el RTO se cuenta en minutos; para otras, en horas, y las hay que lo cuentan en días.

Las diferentes necesidades de las empresas determinan los diferentes niveles de RTO. Pocas veces será aceptable que una aplicación que genera ingresos esté inactiva durante mucho tiempo. Sin embargo, aplicaciones como las de recursos humanos pueden pasar desactivadas 8 horas o más sin que ello cause una gran impacto empresarial. Como es lógico, cuanto más cortos son los requisitos de RTO de una aplicación, más caro es recuperarla en el plazo requerido. Por tanto, las organizaciones deben empezar por proteger las aplicaciones esenciales y, si queda suficiente presupuesto, proteger las aplicaciones de nivel inferior. Así pues, el nivel deseado de RTO debe ser el factor principal a la hora de seleccionar una solución DRaaS basada en la cloud.

Factor 2: Determinar si el servicio ofrece automatización y coordinación de la conmutación por error

Es relativamente fácil hacer copias de seguridad de los datos en la cloud. Sin embargo, las organizaciones que confían solamente en las copias de seguridad se exponen a riesgos importantes en caso de desastre. Si lo único que se copia en la cloud son los datos, las organizaciones se deben encargar de configurar todo el entorno, activar instancias informáticas, trasladar datos al servicio de almacenamiento de cloud apropiado y configurar la red. Muchas de estas tareas requieren bastante trabajo manual y tiempo de ejecución. Para las aplicaciones con un RTO de dos días o más, no es un problema. Sin embargo, para las aplicaciones que generan ingresos, normalmente es demasiado tiempo.

Para las aplicaciones más esenciales, las organizaciones deben escoger servicios basados en la cloud que ofrezcan una coordinación y automatización de conmutación por error para la recuperación ante desastres. Dichos servicios implementan un entorno de DR según un procedimiento predefinido. Activan los nodos obligatorios, encienden las máquinas virtuales en la secuencia correcta según las dependencias adecuadas, ejecutan scripts y asignan redes IP automáticamente, con muy poca intervención humana. Así se garantiza que las aplicaciones esenciales estén en funcionamiento a tiempo y se minimiza el impacto que puede tener un desastre en la empresa.

CASOS DE USO DE LA RECUPERACIÓN ANTE DESASTRES COMO SERVICIO (DRAAS)

1. **DR totalmente nueva**
   Está pensada para las organizaciones que solo tengan copias de seguridad o que no cuenten con ningún plan de DR.
2. **Ampliación de los planes de DR existentes**
   Algunas organizaciones ya han implementado una solución de DR local, pero solo la usan para proteger una pequeña cantidad de cargas de trabajo. Gracias a DRaaS, estos clientes pueden proteger el resto de las cargas de trabajo en la cloud y continuar utilizando sus planes de DR sin tener que modificarlos.
3. **Sustitución de la DR existente**
   A algunas organizaciones se les exige reducir su espacio local o «trasladarse a la cloud». DRaaS es la solución lógica para trasladar el sitio de DR local a la cloud.
4. **DR entre clouds de distintas regiones**
   Incluso las clouds públicas más grandes sufren interrupciones; por lo que la recuperación ante desastres es importante para los clientes que ejecutan sus aplicaciones en la cloud. Los clientes de soluciones DRaaS pueden proteger sus aplicaciones en clouds de diversas regiones.

Factor 3: Evaluar el grado de complicación que implica cambiar de plataforma las aplicaciones

La mayoría de aplicaciones modernas basadas en microservicios no dependen de una cloud pública en particular para funcionar. No obstante, las aplicaciones tradicionales, que aún predominan en muchas organizaciones, normalmente se implementan como máquinas virtuales. Cada hipervisor tiene su propio formato de máquina virtual, y las de las clouds públicas, en muchos casos, no tienen el mismo formato que las máquinas virtuales locales de las organizaciones. Para poder usar las aplicaciones escritas e implementadas en un hipervisor en otro hipervisor distinto, es necesario cambiar de plataforma las máquinas virtuales. El proceso de cambio de plataforma suele ser largo y complicado, y las organizaciones pueden dedicarle muchos meses. Y lo que es más importante, durante este proceso, las aplicaciones de las organizaciones no están protegidas en caso de desastre.

Factor 4: Determinar la necesidad de realizar pruebas de DR que no causen interrupciones

La creación de un plan de DR es un proceso continuo. Los centros de datos no son estáticos, es decir, a lo largo del tiempo las aplicaciones existentes se actualizan o sustituyen, o se añaden otras nuevas. Esto se traduce en *discrepancias* entre el plan de DR original de la organización y el real, que se mantiene actualizado con los cambios de las aplicaciones.

Para garantizar que tal situación no ocurra, las organizaciones deben realizar pruebas en su plan de DR con frecuencia; según las prácticas recomendadas, esto debería hacerse al menos una vez por trimestre. Puesto que estas pruebas no son desastres de verdad, no deberían afectar a las aplicaciones activas de las organizaciones. En otras palabas, es necesario que estas pruebas no causen interrupciones.

Además, algunas organizaciones están obligadas por ley a realizar pruebas de DR y presentar los resultados en una auditoría. Una buena solución DRaaS debe ofrecer a los clientes una serie completa de pruebas sin interrupciones e informes detallados que se generen a partir de esas pruebas.

Factor 5: Garantizar la fiabilidad de la infraestructura del sitio de DR

Por último, muchos proveedores ofrecen recuperación ante desastres como servicio. Pero su escala y sofisticación varía. Muchos proveedores carecen de la escalabilidad, la fiabilidad, la estabilidad financiera y la disponibilidad global con las que cuentan los principales proveedores de cloud. Dado que las organizaciones necesitan confiar en las soluciones de DR en los momentos críticos, cuando sus principales centros de datos no están activos, la fiabilidad de la infraestructura de DR es un factor clave que se ha de tener en cuenta.

RECURSOS

Obtenga más información sobre el servicio VMware Cloud on AWS en el sitio web de VMware Cloud on AWS.

Para obtener más información sobre la recuperación ante desastres como servicio, consulte los vídeos de demostración y mucho más en el sitio web de VMware Site Recovery.

Consulte el resumen de la solución VMware Cloud on AWS y el documento VMware Cloud on AWS: Coste total de propiedad.

Vea demostraciones informativas, vídeos con descripciones y seminarios web, o escuche la opinión de nuestros clientes: VMware Cloud on AWS en YouTube.

Lea nuestras últimas publicaciones en el blog VMware Cloud on AWS.

Síganos en Twitter @vmwarecloudaws y mándenos un saludo con el hashtag #VMWonAWS.

Empiece ahora mismo con VMware Cloud on AWS: https://cloud.vmware.com/vmc-aws/get-started.

Lea la documentación técnica sobre VMware Cloud on AWS.

Conclusión

A medida que las organizaciones adoptan las clouds públicas para DRaaS, deben tener en cuenta varios factores en su estrategia de DR. Una buena solución DRaaS debe poder ofrecer los RTO que necesitan las aplicaciones esenciales. También debe ofrecer automatización y coordinación del proceso de conmutación por error y pruebas sin interrupciones. Lo ideal es que estas acciones se lleven a cabo sin tener que cambiar de plataforma las aplicaciones y ejecutándolas en una cloud pública fiable.

VMware Site Recovery™ para VMware Cloud™ on AWS ofrece a los clientes un servicio de DR completo. Gracias a Site Recovery, los clientes tienen acceso a una infraestructura fiable y global, que cuenta con la interfaz que ya conocen de vSphere y vCenter, y que no requiere cambios de plataforma. Además, al aprovechar soluciones de DR probadas y validadas como VMware Site Recovery Manager™ (SRM), los clientes pueden automatizar y coordinar la conmutación por error, la conmutación por recuperación y la asignación de la red IP, así como llevar a cabo pruebas sin interrupciones a partir de las que se generan informes exhaustivos.

Obtenga más información en cloud.vmware.com/es/vmware-site-recovery.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
C/ Rafael Botí, 26 - 2.ª planta, 28023 Madrid, España. Tel. +34 914125000 Fax +34 914125001 www.vmware.com/es