Commvault

Cloud Rewind™
Formerly Appranix

eBOOK

Logra la Resiliencia de Aplicaciones en la Nube con Recuperaciones Hiperrápidas

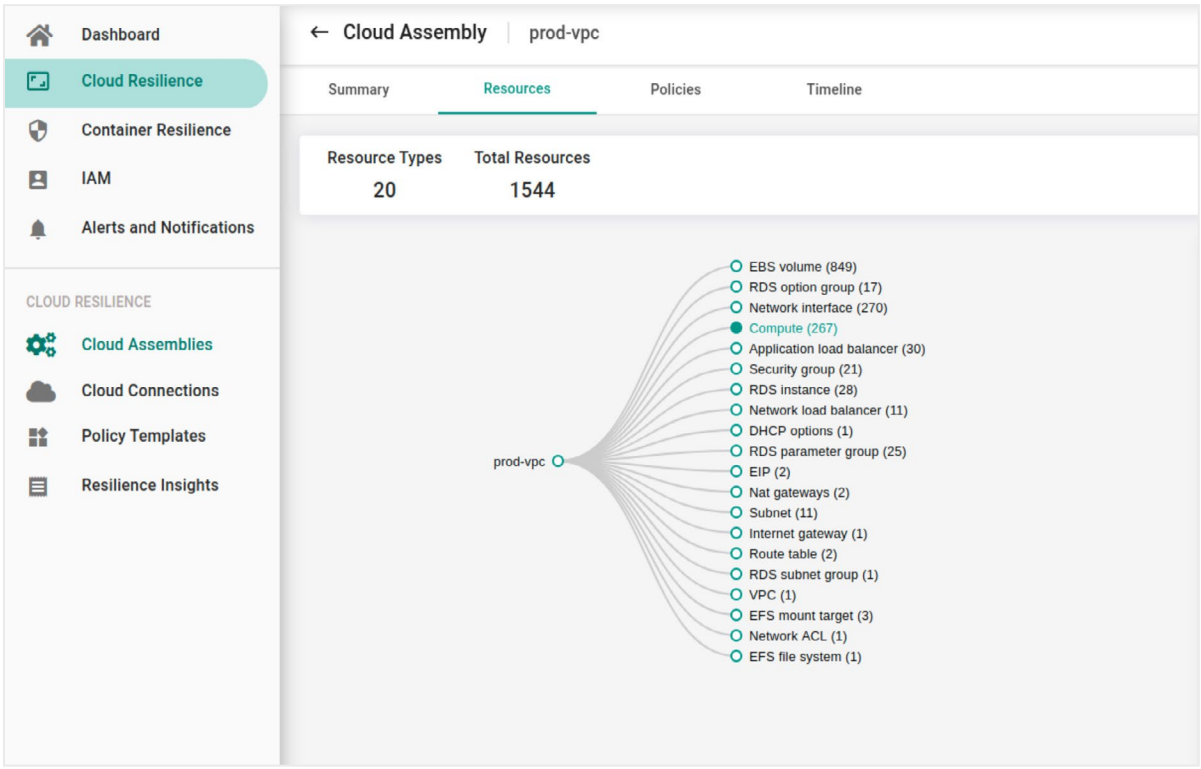
Tabla de Contenidos

RECUPERACIÓN HIPERRÁPIDA DE ENTORNOS DE APLICACIONES EN LA NUBE

Las organizaciones preparadas para la nube han cambiado rápidamente a un modelo operativo descentralizado para sus aplicaciones y servicios. Las arquitecturas de software también se han vuelto más distribuidas, aprovechando los recursos en la nube disponibles en diferentes zonas de la misma. Los ingenieros de fiabilidad han adoptado ciclos de lanzamiento más dinámicos y rápidos a través de prácticas DevOps para satisfacer las demandas crecientes de los clientes. Además, los recursos de nube programables han permitido que los entornos se escalen automáticamente para cumplir con los requisitos de rendimiento de las aplicaciones empresariales críticas.

Sin embargo, todos estos cambios han generado enormes desafíos para los equipos de servicios de operaciones compartidas que gestionan la resiliencia, la seguridad y los costes. La pregunta más urgente ahora, especialmente cuando los entornos en la nube son propensos a ciberataques cada vez más frecuentes, es cómo estos entornos de aplicaciones dinámicos y de escalado automático pueden recuperarse rápidamente de los tiempos de inactividad utilizando la infraestructura nativa de la nube para mantener los SLA empresariales prometidos.

POR QUÉ UN MODELO TRADICIONAL DE BCDR DE CENTROS DE DATOS NO ES ADECUADO PARA APLICACIONES EN LA NUBE



Las aplicaciones ya no dependen de unos pocos servidores o un conjunto único de bases de datos críticas. Considera el siguiente ejemplo de una aplicación en la nube de tres capas con escalado automático, que consta de dos máquinas virtuales y una base de datos. Está compuesta por al menos veinte (20) tipos de recursos e instancias de nube distintos. Los sistemas tradicionales de backup y recuperación fueron diseñados para proteger solo los discos de las máquinas virtuales, las bases de datos y los sistemas de archivos. Para ofrecer resiliencia para la aplicación completa en la nube, todos los recursos deben estar protegidos para poder recuperarlos en cualquier momento y en cualquier región de la nube. Los sistemas de backup y recuperación "legacy" no se diseñaron para proteger todos estos recursos en la nube utilizados por aplicaciones dinámicas, distribuidas y de escalado automático que dependen de una infraestructura en la nube definida por software.

LA PROLIFERACIÓN DEL RANSOMWARE CAMBIA LA RECUPERACIÓN DE APLICACIONES

A medida que los ataques de ransomware se multiplican y se vuelven cada vez más sofisticados, las recuperaciones de entornos en la nube se vuelven cada vez más difíciles. Lo más importante es que los nuevos ataques de ransomware también apuntan a los productos de backup y sus consolas de gestión. Como la mayoría de los productos BCDR se instalan en la misma cuenta de nube del dominio principal que los sistemas de producción, si un ataque de ransomware toma el control de toda la cuenta en la nube, ni siquiera es posible acceder a las consolas de los sistemas de backup y recuperación para poder recuperar los entornos de aplicaciones. Este es, quizás, uno de los modelos críticos que las organizaciones deben replantearse al rediseñar la arquitectura para la resiliencia de las aplicaciones, en lugar de solo el backup y recuperación de datos.

Dado que los sistemas de aplicaciones en la nube están compuestos por múltiples servicios de infraestructura en la nube, los usuarios que realizan recuperaciones de ataques de ransomware necesitan un conocimiento tremendo para poder reconstruir las máquinas virtuales, bases de datos, redes, multitud de servicios en la nube y las configuraciones de nube asociadas para recuperarlos adecuadamente. Típicamente, componentes clave de los entornos de aplicaciones, como las redes privadas virtuales (VPCs), balanceadores de carga, puertas de enlace, grupos de seguridad, grupos de parámetros de bases de datos, etc., deben ser ensamblados manualmente con anticipación por los equipos de operaciones en la nube antes de incluso involucrarse con los sistemas BCDR para la recuperación de datos.

EL DESCUBRIMIENTO CONTINUO DE RECURSOS EN LA NUBE ES CLAVE PARA UNA MEJOR RESILIENCIA

Los entornos de nube dinámicos y de escalado automático introducen enormes desafíos para los equipos de operaciones a la hora de mantenerlos seguros y resilientes. Como múltiples equipos de desarrollo se sirven por sí mismos de la mayoría de los recursos de infraestructura en la nube, los entornos de aplicaciones en la nube se expanden a un ritmo más rápido que el modelo tradicional de un centro de datos. Estos entornos programables y en constante cambio necesitan un sistema que descubra continuamente todos los recursos que pertenecen a una aplicación. Las organizaciones también tienen muchas cuentas en la nube para aislar sus entornos de desarrollo, producción y pruebas según sus necesidades empresariales. Hoy en día, no es raro que haya cientos de cuentas en la nube. La complejidad de múltiples cuentas en la nube, junto con entornos que cambian rápidamente, hace que sea difícil para los equipos centralizados confiar en sistemas de protección y recuperación tradicionales y no centrados en la aplicación, ya que estos sistemas simplemente dependen de que los usuarios seleccionen los recursos correctos y apliquen la protección manualmente para sus aplicaciones.

Por otro lado, los desarrolladores de aplicaciones no llevan un registro de todos los recursos de infraestructura en la nube utilizados para sus aplicaciones, por lo que no pueden ayudar a los ingenieros de fiabilidad (SREs) en momentos críticos de recuperación. Por lo general, varias pipelines de DevOps modifican los entornos de nube centralizados, lo que dificulta aún más la recuperación por parte de los SREs en momentos de necesidad urgente. Se necesita un sistema que descubra continuamente los recursos en la nube y esté centrado en la aplicación, y que tenga la capacidad de comprender los recursos del sistema mediante el mapeo de dependencias automatizado para proteger adecuadamente todos los recursos de nube relevantes. De esta manera, es posible recuperar rápidamente o realizar un “failover” de las aplicaciones, datos, configuraciones, estado y dependencias para mantener el tiempo de actividad de las aplicaciones.

PROTEGE EL ESTADO DE TU ENTORNO EN LA NUBE CON UN SISTEMA DE APRENDIZAJE CONTINUO

Gartner estima que un entorno en la nube típico experimenta más de 50 cambios de configuración por día. Es importante crear un repositorio inmutable de metadatos de configuración de nube de todos los entornos de aplicaciones críticas en la nube. También es crucial alojar los metadatos de configuración de nube en un

sistema de resiliencia de aplicaciones en la nube ubicado en una nube diferente para lograr niveles adicionales de resiliencia. Estos cofres de metadatos de configuración deben ser segmentables por servicios de aplicación y deben estar registrados para la recuperación en cualquier momento y en cualquier región de la nube. Deben ser lo suficientemente granulares para permitir que los equipos de operaciones soliciten un solo recurso en cualquier momento, de manera que una instancia específica de un servicio en la nube pueda ser recuperada rápidamente en caso de fallo.

Un sistema de aprendizaje continuo es clave para mantener un registro de los cambios, de manera que, en caso de fallo, los sistemas de aplicaciones en la nube distribuidos puedan ser recreados basándose en lo que había en el entorno de producción. Un sistema de descubrimiento continuo y aprendizaje de metadatos elimina completamente la necesidad de evaluaciones manuales y los riesgos asociados con metadatos desconectados durante el proceso de recuperación.

RECUPERACIONES HIPERRÁPIDAS DE TODO EL ENTORNO CON DR-AS-CODE

La parte más compleja de la recuperación es identificar los recursos correctos de cómputo, almacenamiento, PaaS e infraestructura de red correspondientes a un conjunto de aplicaciones y secuenciarlos para una recuperación orquestada. Esto se llama un “Plan Técnico de Recuperación”, o TDP por sus siglas en inglés. También existe un aspecto no técnico del plan de recuperación que se refiere a la movilización de recursos humanos y organizativos para la validación de las aplicaciones después de las recuperaciones. Los TDPs suelen constar de varias páginas y requieren la colaboración de varios profesionales operativos para identificar lo que se ejecuta en producción, en términos de configuraciones, dependencias, secuencias y scripts. Las organizaciones que han utilizado productos BCDR tradicionales te dirán lo complejos que son los TDPs y por qué no realizan pruebas de recuperación con frecuencia.

Ahora es posible eliminar completamente los TDPs manuales con un modelo de infraestructura como código (IaC, por sus siglas en inglés) automatizado. En particular, para garantizar las recuperaciones, es importante utilizar IaC nativo de la nube en lugar de IaC neutral en la nube, de manera que la responsabilidad de ejecutar grandes recuperaciones de sistemas pase a manos del proveedor de nube, que cuenta con recursos escalables dinámicamente para completar las recuperaciones con éxito durante un tiempo de inactividad.

GESTIÓN DE COPIAS DE DATOS NATIVAS EN LA NUBE

Las plataformas en la nube tienen capacidades suficientes de gestión de datos para poder realizar copias de datos mucho más rápidas para backup, replicación y recuperación. No es necesario agregar capacidades adicionales de gestión de datos de proveedores de terceros. No es necesario cambiar el formato de almacenamiento de datos nativo de la aplicación a un formato común de datos de backup y pasar por el largo proceso de importación y exportación al sistema de archivos de backup neutral. Es posible realizar backups consistentes incrementales desde máquinas virtuales y bases de datos para reducir el coste de backup y recuperación ante desastres (DR). Los servicios sin servidor tienen capacidades de gestión de datos suficientes integradas para evitar copias costosas hacia y desde plataformas de gestión de datos adicionales en el entorno de nube.

Las plataformas de nube a gran escala realmente han abierto las puertas para una mayor resiliencia en comparación con el modelo de infraestructura de centro de datos. Las organizaciones globales pueden replicar literalmente los datos incrementales de una región de la nube a otra en cuestión de minutos. Esto no solo aumenta la resiliencia de los datos, sino que las copias múltiples y más económicas en todo el mundo permiten niveles mucho mejores de resiliencia de aplicaciones en caso de fallo.

MÁQUINA DEL TIEMPO PARA ENTORNOS DE APLICACIONES EN LA NUBE

La Máquina del Tiempo del Entorno de Aplicaciones en la Nube es un concepto simple en el que un sistema automatizado puede reunir todos los metadatos de los recursos de nube centrados en la aplicación desde una bóveda de seguridad, la aplicación desde un repositorio inmutable y los datos de la aplicación desde el almacenamiento y las bases de datos para una recuperación sincronizada en un punto específico del tiempo. Puedes imaginar estas máquinas del tiempo como CMDBs con registro diario que se actualizan automáticamente desde una perspectiva centrada en la aplicación, utilizando todas las capacidades nativas de la nube.

Sin embargo, la diferencia más importante entre una Máquina del Tiempo en la Nube y los antiguos CMDBs es que conoce las copias de datos en un punto específico del tiempo para las aplicaciones. Con el tiempo, una Máquina del Tiempo en la Nube se vuelve esencial para las organizaciones, ya que múltiples grupos dentro de una organización pueden acceder a ella fácilmente para realizar diversos “rollbacks”, recuperaciones y conmutaciones por error. Los sistemas BCDR tradicionales nunca han recopilado los metadatos de los sistemas de manera útil más allá de los requisitos básicos de backup de datos.

RESUMEN

La naturaleza dinámica, la complejidad y la velocidad de los cambios en las aplicaciones en la nube realmente requieren un nuevo modelo de resiliencia centrado en la aplicación, en lugar de los modelos de protección y recuperación o recuperación ante desastres “legacy”, que se crearon principalmente durante la era de los centros de datos. Tanto si las aplicaciones se han migrado a la nube o han sido creadas de forma nativa en las plataformas de nube, este nuevo modelo no solo ayuda a la rápida recuperación de todo el entorno de aplicaciones ante múltiples tiempos de inactividad, sino que también reduce drásticamente las pesadillas operativas, especialmente cuando equipos de operaciones más pequeños gestionan una cantidad mucho mayor de recursos en comparación con la última década.

ACERCA DE CLOUD REWIND™

Cloud Rewind proporciona resiliencia de aplicaciones en la nube con backup y recuperación de todo el entorno de nube, incluyendo todos los recursos, servicios y dependencias, en cualquier punto del tiempo y en cualquier región de la nube.