




arsys

Contenedores y protección de datos empresariales

Gracias a los contenedores, las empresas pueden acelerar su estrategia de protección de datos. Veremos cómo.

A man in a dark sweater and trousers is walking through a server room aisle, holding a laptop. The room is filled with rows of server racks on both sides, illuminated by blue light. The perspective is from a low angle, looking down the aisle towards the man.

Los contenedores son facilitadores sin igual que hacen posible que la informática y el almacenamiento se estén trasladando rápidamente al Cloud. Son una tecnología imprescindible para cualquier empresa, pero, aunque las herramientas de orquestación de contenedores como Kubernetes son útiles para aprovechar la capacidad de escala y la portabilidad, se muestran insuficientes para proteger los datos.

Una de las razones de esta aparente desventaja de los contenedores es que han sido diseñados para ser algo temporal, no persistente, y su vida útil a menudo es más corta que la de los datos que crean (aunque suene paradójico). Por cuestiones de cumplimiento, ciberseguridad o protección contra intrusiones, es necesario hacer backup de esos datos y almacenarlos.

Además, es necesario contar con capacidad de replicación para migrar clústeres enteros entre entornos de prueba, desarrollo y producción, para así poder volver a estados previos de manera rápida si no se obtuvieran los resultados esperados. Siempre pueden pasar cosas inesperadas durante una migración y, por tanto, es necesario contar con backup y protección de datos, sin duda. Kubernetes no es inmune a los fallos en la protección de datos.

Los entornos de **Kubernetes** deben tener un enfoque centrado en las aplicaciones en lugar de en la infraestructura, y las empresas necesitan una solución de backup polivalente y eficaz. Diseñar y aplicar una estrategia de protección de datos en contenedores y observar las mejores prácticas de backup son aspectos cruciales en la actualidad con esta tecnología.

Las mejores prácticas de backup

Como comentamos, los contenedores son herramientas extremadamente flexibles, rápidas y ágiles que están revolucionando la computación. Pero también son construcciones efímeras que puede que no persistan en el tiempo tanto como los datos que generan. Esto implica que es imperativo disponer de estrategias adecuadas de backup y respaldo de la información que se centren en: arquitectura, capacidad de recuperación, operaciones, seguridad y portabilidad.

1 Arquitectura

Cualquier herramienta o plataforma que se encargue de proteger las aplicaciones de Kubernetes ha de descubrir automáticamente todos los componentes de la aplicación que se ejecutan en el clúster, y tratar a la aplicación como una unidad atómica. Asimismo, ha de tener en cuenta todos los datos de configuración y, en general, todo aquello que es necesario para poder replicar al 100% dicha aplicación.

2 Capacidad de recuperación

Evidentemente, cualquier aplicación o plataforma que permita gestionar estas recuperaciones ha de ser capaz de llevar a cabo su tarea en el momento en que sea necesario, y en el entorno preciso. También se necesita disponer de la flexibilidad necesaria como para restaurar un subconjunto de una aplicación, simplemente. La cuestión es que la restauración debe ser algo sencillo y potente a la vez, que permita seleccionar el momento adecuado de restauración del backup.

3 Operaciones

Cualquier plataforma de backup nativa en Kubernetes se debe poder utilizar a escala, y ofrecer a los equipos de operaciones las capacidades de flujo de trabajo necesarias, cumpliendo con todos los requisitos.

4 Seguridad.

Tendrán que existir tanto los controles de gestión de identidad y acceso, como el control de acceso basado en roles. Este tipo de control de acceso permite a diferentes personas dentro de un equipo de operaciones adoptar un enfoque de menores privilegios en las tareas comunes, como la monitorización.

5 Portabilidad

Una plataforma de gestión de datos nativa en el Cloud ha de ser flexible a la hora de dar soporte a diferentes distribuciones y ofrecer capacidades que permitan la portabilidad de cargas de trabajo y aplicaciones entre entornos diversos. Por tanto, se necesitan capacidades de portabilidad en múltiples casos de uso, entre los que se incluye la restauración, la clonación y la migración de aplicaciones.

Para aprovechar al máximo las capacidades de Kubernetes y, en general, de los contenedores, es preciso que la protección de datos sea capaz de adaptarse y acoplarse, por decirlo así, a estas tecnologías. De este modo, las empresas pueden acelerar con confianza su estrategia de protección de datos.

Managed Kubernetes, nuestra solución de infraestructura gestionada de contenedores

Kubernetes es un sistema complejo en su administración. Requiere cierto nivel de conocimientos y expertise y, por este motivo, hemos creado Managed Kubernetes, nuestra solución de infraestructura gestionada de contenedores. Con ella es sencillo desplegar un proyecto Kubernetes en unos pocos clics y el usuario estará encargado de desplegar y operar su infraestructura de contenedores sobre la plataforma.

Para más
información sobre
este servicio visita
arsys.es/servidores/kubernetes



arsys

www.arsys.es

-  www.facebook.com/arsys.es
-  twitter.com/arsys
-  www.linkedin.com/company/arsys-internet/
-  www.instagram.com/arsys.es/

