



DISEÑO DE UN ENTORNO PRODUCTIVO BASADO EN CONTENEDORES (KUBERNETES)

Autor: José Luis Pérez Pajuelo

Director/es: Francisco Javier Rodríguez Martínez

I. INTRODUCCIÓN Y CONTEXTO

Antiguamente, la mayor parte de las aplicaciones de software eran monolíticas, y se ejecutaban como un solo proceso, o como un pequeño número de procesos distribuidos en un número determinado de servidores.

Actualmente, muchos de estos sistemas todavía están implementados en las empresas, lo que supone que tengan ciclos lentos, cuya actualización además se suele dar con baja frecuencia. Al final de cada ciclo de estos lanzamientos, los desarrolladores empaquetan todo el sistema y se lo entregan a los de “operaciones”, que terminan por implementarlo, para pasar a monitorear el resultado. En el caso de que se produzcan fallos de hardware, estos equipos de operaciones los migran manualmente a los servidores que quedan sin errores, siendo este el ciclo tradicional.

Hoy en día, estas grandes aplicaciones monolíticas van dando paso a otros procesos más pequeños, cuya ejecución es independiente, y cuya monitorización y reparación es más rápida y directa. Son los que se conocen como microservicios.

Como los microservicios no están acoplados entre ellos, se pueden desarrollar, implementar, actualizar, y escalar individualmente, al igual que sucede con las reparaciones. Esto permite el cambio rápido y constante de componentes tantas veces como sea necesario, y con ello, se consiguen mantener los requerimientos de los clientes, que cada día más, demandan unos entornos operativos muy específicos, bien en términos de velocidad, de capacidad, o de seguridad como es el caso de las fuerzas y cuerpos de seguridad de cualquier país preocupado por sus operaciones.

En este entorno descrito, donde cada vez existe un mayor número de componentes desplegados y centros de datos cada vez más grandes, cada día es más difícil configurar, administrar y mantener los sistemas en su conjunto, funcionando sin que aparezcan problemas en los sistemas, y sin que los mismos estén sometidos a riesgos que comprometan su seguridad.



En este sentido mencionado anteriormente, cada vez más se hace necesario desarrollar procesos de automatización, que incluyan una programación automática de estos numerosos componentes a esos servidores afectados, una configuración automática, la supervisión y manejo de los fallos que puedan generarse, así como el establecimiento de nuevas arquitectura para evitar los problemas de seguridad congénitos. Aquí es donde entran en juego los llamados Kubernetes.

Los Kubernetes permiten a los desarrolladores desplegar sus aplicaciones ellos mismos, sin necesidad de asistencia de los equipos de operaciones, y además, conociendo sus posibles vulnerabilidades, realizar un diseño acorde a las necesidades y requisitos para que el beneficio no sólo sea en términos de desarrollos, sino para que los equipos de desarrolladores vean su labor facilitada, monitoreando y reprogramando todas esas aplicaciones en caso de un fallo de hardware.

EL significado de Kubernetes (del griego) es *piloto o timonel*, y eso es lo que hace esta herramienta, una dirección de distintos aspectos del sistema. Kubernetes abstrae la infraestructura de hardware y expone todo el centro de datos como un enorme recurso computacional, que permite desplegar y ejecutar sus componentes de software sin tener que conocer los servidores reales que se encuentran debajo. Al desplegar una aplicación de múltiples componentes, a través de Kubernetes, se selecciona un servidor para cada componente, lo implementa y le permite encontrar y comunicarse fácilmente con todos los demás componentes de su aplicación.

Esto hace que Kubernetes sea ideal para la mayoría de los centros de datos pequeños o locales, pero donde comienza a destacar es cuando se usa en centros de datos más grandes, como los contruidos y operados por los proveedores de la nube. Kubernetes les permite ofrecer a los desarrolladores una plataforma simple para desplegar y ejecutar cualquier tipo de aplicación, y no requiere que los propios administradores de los proveedores de la nube sepan nada sobre las decenas de miles de aplicaciones que se ejecutan en su hardware.

Con cada vez más y más grandes compañías que asumen el modelo Kubernetes como la mejor opción de ejecutar aplicaciones, convirtiéndose en una forma estándar de ejecutar dichas aplicaciones tanto en la nube, como en las infraestructuras locales, pero que debe asegurar en ciertos contextos, unos parámetros de seguridad que cada día se hacen más necesarios, por no apuntar obligatorios, en ciertos sectores productivos.

I. DESARROLLO Y RESULTADOS

El desarrollo del trabajo, así como el resultado aproximado del mismo consistiría en realizar unas propuestas arquitectónicas en un entorno productivo, basado en Kubernetes, para lograr la división de la red de clúster de Kubernetes. Dos sistemas



propuestos para realizar la segmentación, y una estrategia para proporcionar una separación entre contenedores basada en el host.

Las demandas de seguridad de la computación en la nube varían, en función de los entornos en los que se realicen los procesos. A medida que las autoridades policiales españolas trabajan con mayores demandas de seguridad en tecnologías de la información, el nivel de aceptación de riesgos se complica, y en este contexto, las soluciones deben abordar problemas que, para la mayoría de los operadores de computación en la nube, no tiene una importancia vital.

De esta manera, las propuestas de este trabajo pueden no parecer adecuadas para otros entornos con una demanda de seguridad menor, ya que muchos riesgos, como los ataques de escape, pueden ser aceptables para estos entornos menos sensibles, pero la perspectiva a abordar se centrará en estos riesgos en el mismo. Las propuestas son principalmente adecuadas para las partes que operan en la nube y proveedores de PaaS.

II. CONCLUSIONES

Las arquitecturas y esquemas propuestos en el trabajo son un intento de estudiar tanto la agilidad de la contenerización, como un grado aceptable de seguridad con respecto a la separación de las aplicaciones. Estas propuestas proporcionan los medios para utilizar contenedores orquestados utilizando un grado de separación adaptable y son, a su vez, una prueba conceptual de cómo Docker y Kubernetes pueden utilizarse incluso en entornos productivos y a la vez exigentes en cuestiones de seguridad. Si bien las propuestas no proporcionan el mismo grado de separación en comparación con la arquitectura de virtualización de línea de base, parece que proporcionan una separación suficiente para una operación sensible y productiva.