Por gentileza de:

veeam

Copia de seguridad y recuperación de Kubernetes

para dummies®
A Wiley Brand

Descubre por qué la copia de seguridad nativa de Kubernetes es importante

Aprende a proteger tus aplicaciones de Kubernetes

Crea políticas automatizadas para la copia de seguridad de Kubernetes

Steve Kaelble

3.ª edición especial de Veeam®

Acerca de Veeam

Veeam es el líder en la copia de seguridad y recuperación antes desastres de Kubernetes. Veeam Kasten ayuda a las empresas a superar los retos relacionados con la gestión de las copias de seguridad de las operaciones del día 2 para ejecutar aplicaciones en Kubernetes con confianza. Para obtener más información, visita https://www.veeam.com/products/cloud/kubernetes-data-protection.html?ad=menu-solutions y echa un vistazo a los detalles de la última versión de Veeam Kasten en http://docs.kasten.io. Sigue a Veeam en X en https://twitter.com/veeam.

Copia de seguridad y recuperación de Kubernetes

3.ª edición especial de Veeam®

por Steve Kaelble

para dummies®
A Wiley Brand

Copia de seguridad y recuperación de Kubernetes Para Dummies®, 3.ª edición especial de Veeam®

Una publicación de
John Wiley & Sons, Inc.
111 River St., Hoboken, NJ 07030-5774
www.wiley.com

ISBN 978-1-394-35362-0 (pbk); ISBN 978-1-394-35363-7 (ebk); ISBN 978-1-394-35364-4 (ePub)

Para obtener información general sobre nuestros productos y servicios, o sobre cómo crear un libro *Para Dummies* personalizado para tu empresa u organización, ponte en contacto con el Departamento de Desarrollo Empresarial en EE. UU. en el teléfono +1 (877) 409 4177, ponte en contacto con info@dummies.biz, o visita www.wiley.com/go/custompub. Para obtener información sobre licencias de la marca Para Dummies para productos o servicios, ponte en contacto con BrandedRights&Licenses@Wiley.com.

Agradecimientos del editor

Entre algunas de las personas que han ayudado a comercializar este libro figuran las siguientes:

Editora del proyecto: Rebecca Senninger

Editora de adquisiciones: Traci Martin

Director editorial: Rev Mengle

Representante de expansión comercial: Matt Cox

Editor de producción: Saikarthick Kumarasamy

Índice

Introducción

No hace falta que nadie te diga que la nube es el lugar de moda. La adopción y el uso de la nube nativa están en lo más alto (perdón por el juego de palabras). Kubernetes está en todas partes, a punto de convertirse en la próxima plataforma empresarial favorita y la base para todo tipo de aplicaciones, todo ello por buenas razones. Es portátil, ágil, escalable, increíblemente fiable: el sueño de cualquier desarrollador.

Sin embargo, *no* lo es todo para la protección de tus datos. De hecho, parte de la magia arquitectónica que hace que sea tan fantástica también crea nuevos retos en la gestión y protección de datos. La protección que ofrece a tus aplicaciones no se extiende automáticamente a tus datos, y no puedes limitarte simplemente a adaptar las arquitecturas de copia de seguridad heredadas a un ecosistema nativo de la nube.

Necesitas una solución de copia de seguridad verdaderamente nativa de la nube; una que no solo hable el lenguaje de Kubernetes, sino que viva en este nuevo y apasionante planeta. Y necesitas conocer las mejores prácticas que garanticen una evolución fluida hacia la adopción y el uso de la nube nativa.

Acerca del libro

Copia de seguridad y recuperación de Kubernetes Para Dummies, edición especial de Veeam, es tu guía para llegar a una solución. Explica detalladamente desde el principio cómo surgió Kubernetes. Te permite saber exactamente por qué tu copia de seguridad de mañana no puede funcionar igual que lo hacía ayer.

Con este libro aprenderás a implementar y hacer copias de seguridad de tus aplicaciones de Kubernetes. Entre otras cosas, encontrarás enfoques centrados en las aplicaciones para recuperarlas y garantizar la seguridad, trabajar en un entorno de multiinquilino, transformar el soporte para la restauración y aprovechar al máximo la movilidad de las aplicaciones nativas de la nube.

Este libro está repleto de medidas prácticas para proteger tus datos en un ecosistema en constante evolución, a la vez que facilita la vida tanto a los desarrolladores como a los operadores. Y ofrece ideas para que puedas hacer una verdadera revolución y, a la vez, que todo siga su curso sin problemas.

Algunas suposiciones obvias

Al preparar este libro, hemos hecho algunas suposiciones sobre ti, esa persona que ha dedicado su tiempo a leer estas páginas.

- Puede que te gusten los aspectos técnicos de las cosas o que formes parte del equipo de DevOps de aplicaciones nativas de la nube.
- Es posible que te encuentres en el lado administrativo, pero que te sientas intrigado por las oportunidades que ofrece la nube nativa o te preocupen sus riesgos.
- En cualquier caso, te has comprometido a garantizar el éxito de tu organización en esta frontera en constante expansión.

Iconos utilizados en este libro

Para ayudarte a navegar por este libro, hemos incluido algunos iconos en los márgenes. Piensa en ellos como alertas que te avisan de los términos que debes tener especialmente en cuenta.

RECUERDA

Si lo deseas, puedes saltarte cosas, pero presta especial atención a estos párrafos, ya que incluyen algunos de los puntos más importantes.

CONSEJO

Prometemos información práctica y junto a este icono encontrarás algunas ideas útiles.

ADVERTENCIA

Las copias de seguridad de los datos pueden constituir todo un reto. Este icono te avisa de áreas con las que debes tener especial cuidado para evitar problemas.

CUESTIONES TÉCNICAS

Estos párrafos concretos profundizan en los detalles. (Si te gustan los detalles técnicos, estos párrafos te encantarán).

Más allá del libro

Este libro pretende ser un elemento de reflexión, una introducción a los conceptos con una muestra de detalles. Si devoras el libro y te quedas con hambre, visita `https://www.veeam.com/products/cloud/kubernetes-data-protection.html`, donde podrás consultar más recursos, información y libros blancos.

EN ESTE CAPÍTULO

- Elegir aplicaciones nativas de la nube y en contenedores
- Optar por Kubernetes
- Descubrir todas las ventajas
- Desmontar los mitos sobre Kubernetes

Capítulo 1
Comprender Kubernetes y las aplicaciones nativas de la nube

Según una famosa declaración de Apple, «hay una aplicación para eso» en un eslogan registrado para el iPhone que se convirtió en un meme popular. No podría haber sido más profética: las apps se encargan un creciente número de tareas diarias para consumidores y empresas. Hoy en día, son cada vez más los desarrolladores de aplicaciones que adoptan las arquitecturas basadas en contenedores y que hacen uso de la tecnología del entorno Kubernetes.

En este capítulo hablamos sobre el creciente uso de las aplicaciones nativas de la nube y basadas en contenedores y destacamos el ascenso de Kubernetes. Veremos cuáles son las ventajas de adoptar una arquitectura nativa de Kubernetes y exploraremos algunos mitos en torno a lo que se ha convertido en la forma más eficaz de implementar aplicaciones empresariales modernas.

Seguimiento del auge de las aplicaciones nativas de la nube

¿Dónde encajan las aplicaciones basadas en contenedores en tu organización en estos momentos? ¿Qué nos depara el futuro? Según los estudios, estamos viviendo el auge de las aplicaciones nativas de la nube y en contenedores.

Kubernetes ha conseguido una adopción generalizada por su habilidad para automatizar la implementación, escala y gestión de las aplicaciones en contenedores. Según una encuesta de ESG de abril de 2023, Kubernetes ha madurado, ya que el 66 % de los encuestados afirmaron que ya utilizan Kubernetes para gestionar y orquestar sus contenedores (https://go.veeam.com/wp-ar-enterprise-kubernetes-protection).

La Encuesta Anual 2023 de la Cloud Native Computing Foundation (https://www.cncf.io/reports/cncf-annual-survey-2023/) se hace eco de estos resultados, que muestran que entre sus encuestados, Kubernetes ha solidificado su estatus de tecnología principal: un 84 % utiliza ya o está pensando en usar Kubernetes, así como la popularidad cada vez mayor de las implementaciones de nube híbrida.

Otra conclusión clave de esta encuesta es que la falta de formación es el mayor reto, citado por el 46 % de los que aún tienen que implementar contenedores en producción, y el 28 % de los que utilizan contenedores de forma limitada. Una vez que los contenedores se utilicen para casi todas las aplicaciones, la seguridad se convertirá en el principal reto.

El estado de la implementación de aplicaciones con estado frente a aplicaciones sin estado con Kubernetes está claro, el informe «Data on Kubernetes 2021» (https://dok.community/dokc-2021-report/#:~:text=Key%20Findings,2x%20or%20greater%20productivity%20gains) indica que ya el 90 % de los encuestados creía que Kubernetes estaba preparado para cargas de trabajo con estado y una gran mayoría (70 %) las estaba ejecutando en producción, con las bases de datos a la cabeza de la lista. Las empresas señalaron los considerables beneficios para la normalización, la coherencia y la gestión como principales impulsores.

Ejecución en Kubernetes

RECUERDA

Kubernetes, que debutó como código abierto en 2015, se ha convertido rápidamente en la plataforma más habitual para la programación y orquestación de contenedores. De hecho, se está convirtiendo rápidamente en la base de casi todas las aplicaciones, dondequiera que se implementen. Va camino de unirse a Linux y vSphere como plataforma empresarial preferida.

Kubernetes implementa y mantiene aplicaciones y las aumenta en función de diversas métricas, como la CPU y la memoria. Sus bloques de construcción se conocen como *primitivas*, y define los recursos informáticos y de almacenamiento como objetos. Los objetos más importantes de la API de Kubernetes incluyen:

- Clústeres
- Nodos
- Etiquetas y selectores
- Conjunto de réplica
- Implementación

La solidez de Kubernetes permite a los usuarios implementar, ampliar y gestionar aplicaciones en contenedores. Su extensibilidad y portabilidad le han granjeado una gran popularidad en el ecosistema del procesamiento en la nube. Además, Kubernetes también ofrece a los usuarios la flexibilidad de elegir qué lenguaje de programación, o marco, utilizar, y permite a los usuarios supervisar y registrar errores.

BREVE HISTORIA DE KUBERNETES

Merece la pena recordar cómo Kubernetes ha llegado hasta donde está hoy. El nombre Kubernetes significa *timonel* o *piloto* en griego, y tiene cierta etimología en común con la palabra cibernética. Fue obra de un grupo de ingenieros de Google en 2014 y originalmente se conocía como «Proyecto 7».

(Un dato más para los aficionados a la ciencia ficción: Ese nombre en clave original hacía honor al personaje de Star Trek Siete de Nueve, que en su día formó parte del poderoso colectivo Borg, lo que enlaza con el hecho de que Kubernetes estuviera influenciado por un sistema anterior de Google llamado Borg).

RECUERDA

En última instancia, seguir esta ruta aumenta la productividad, pone las aplicaciones en producción más rápidamente y reduce los costes. Kubernetes automatiza muchos procesos de implementación, gestión y ampliación. Puedes aprovechar la magia de Kubernetes para crear clústeres de hosts que ejecuten contenedores y gestionarlos en nubes públicas, privadas o híbridas. Y cabe esperar que todo funcione excepcionalmente bien, con pocas preocupaciones por el tiempo de inactividad de la aplicación.

No es de extrañar que Kubernetes se haya adoptado con tanta rapidez. En el apartado siguiente se describen algunas de sus ventajas. Pero, como ocurre con todo lo que gana popularidad rápidamente, algunas personas se lanzan sin saber muy bien en qué se están metiendo.

En el caso de Kubernetes, esto ha dado lugar a lo que podríamos llamar retos de producción del «Día 2»; en particular, la gestión de datos, la seguridad y la observabilidad. Has eliminado muchas de las dificultades relacionadas con alcanzar una alta disponibilidad y escalabilidad de los servicios de las aplicaciones. Pero no puedes extender automáticamente estas ventajas para cubrir tus datos, lo que significa que debes dar prioridad a la gestión de los datos de las aplicaciones de Kubernetes.

Ver las ventajas

RECUERDA

A los equipos de desarrollo les encanta la mayor agilidad, portabilidad y fiabilidad que obtienen gracias a Kubernetes. Por eso, no es de extrañar que se haya producido una rápida entrada de aplicaciones a la plataforma. No solo las aplicaciones sin estado, sino también las aplicaciones con estado, incluidas las aplicaciones impulsadas por una base de datos NoSQL y las aplicaciones que utilizan una base de datos relacional para su *backend*.

Estas son algunas de las ventajas que ofrece el uso de la infraestructura nativa de la nube y Kubernetes:

- Podrás acceder fácilmente a los ordenadores, el almacenamiento y las redes que necesites para respaldar un rápido crecimiento.
- El almacenamiento es fácil de usar, y el autoservicio es un juego de niños. Con Kubernetes, las bases de datos relacionales y NoSQL pueden integrarse fácilmente y sin problemas.
- Los cambios en las aplicaciones en contenedores pueden implementarse fácilmente. Las mejoras y actualizaciones de las aplicaciones, incluso las más complejas, se pueden llevar a cabo con rapidez.

» La plataforma permite ampliar los requisitos de forma casi instantánea.

Consulta la figura 1-1 para echar un vistazo al ecosistema Kubernetes.

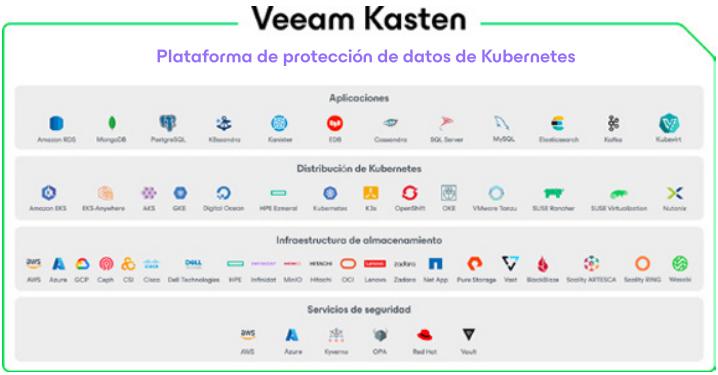

FIGURA 1-1: El ecosistema de Kubernetes.

Explorando los mitos

Mucha gente te dirá que las aplicaciones que se ejecutan en la plataforma Kubernetes deben tener una arquitectura sin estado. Y cuando Kubernetes estaba en pañales, había algo de verdad en esta creencia. Pero como ocurre con todo lo relacionado con la tecnología, las cosas cambian rápidamente, y esa realidad de antaño es ahora un mito.

La realidad actual es que el soporte para el almacenamiento y las aplicaciones con estado ha alcanzado su madurez. Kubernetes se ha convertido en una plataforma ideal para aplicaciones con y sin estado, y para proteger tu aplicación Kubernetes con estado, necesitas una copia de los datos en una ubicación completamente diferente y totalmente independiente.

ADVERTENCIA

Y ahí reside el posible problema. Los desarrolladores de aplicaciones pueden acceder a un aprovisionamiento de almacenamiento dinámico de baja fricción y autoservicio, lo cual es estupendo. Pero no es raro encontrar un uso extensivo del almacenamiento en clústeres Kubernetes que no está necesariamente construido para aplicaciones con estado.

Lo que lo hace problemático es que el uso generalizado de bases de datos relacionales y no relacionales en Kubernetes puede dejar tus datos expuestos si no dispones de los sistemas de gestión de datos adecuados. Y eso significa R-I-E-S-G-O para el negocio.

Este riesgo no es obvio para todo el mundo, y es bastante fácil ver por qué. Al fin y al cabo, una de las mejores cosas de ejecutar aplicaciones en Kubernetes es su alta disponibilidad frente a problemas de software, dificultades con el servidor o fallos en la región. Si estás ejecutando una aplicación con estado, esto hace que sea mucho más fácil ejecutar servicios de datos replicados a través de dominios con fallos.

RECUERDA

La conclusión es que esa alta disponibilidad no es lo mismo que una copia de seguridad. El hecho de que hayas conseguido una alta disponibilidad no significa que tengas una copia de seguridad de tu carga de trabajo en una ubicación diferente. La replicación mejora la disponibilidad de los datos y protege contra fallos parciales de la infraestructura, pero no protege contra la pérdida o corrupción de los datos, ya sea malintencionada o accidental. Este libro trata de cómo conseguir esa protección.

EN ESTE CAPÍTULO

- Por qué son importantes las copias de seguridad nativas
- Tener en cuenta nuevos patrones de implementación
- Adaptar al mundo DevOps
- Aliviar el estrés de los operadores
- Abordar las lagunas en la protección de datos
- Conectar a múltiples servicios de datos

Capítulo 2
Crear una protección de datos nativa para Kubernetes

Tu organización depende del tiempo de actividad de las aplicaciones y Kubernetes es ideal para esto. Aun así, ¿qué pasaría si perdieras todos los datos de tu empresa?

En este capítulo te explicamos exactamente por qué necesitas soluciones de copia de seguridad nativas de Kubernetes. Exploramos muchos de los factores que las hacen absolutamente esenciales, desde los diferentes patrones de implementación hasta las prácticas conocidas como DevOps. Sigue leyendo para descubrir cómo las copias de seguridad nativas de la nube pueden aliviar el estrés de los operadores y darles un mayor margen para la innovación, abordar las lagunas en la protección de datos y garantizar que estés en una buena posición incluso cuando tus aplicaciones acceden a múltiples servicios de datos diferentes.

Reconocer la necesidad

Nadie necesita recordarte la importancia de las copias de seguridad. Independientemente de tu papel en el panorama tecnológico, es probable que en algún momento te hayas despertado de un mal sueño relacionado con una pérdida catastrófica de datos.

ADVERTENCIA

Son muchos los escenarios de fallos que podrían convertir ese mal sueño en una pesadilla de la vida real. Existen borrados accidentales, malentendidos generales de la plataforma, *ransomware* y otras actividades maliciosas. Muchos peligros amenazan tus datos y, ¿cómo sobreviviría tu empresa sin ellos?

RECUERDA

No queremos quitarte el sueño, pero no cabe duda de que Kubernetes es un mundo completamente nuevo y, por muy diversos motivos, puede empeorar las razones existentes por las que se pierden datos en la nube. Es algo complejo, que todavía desconoce mucha gente, y las responsabilidades administrativas no están tan centralizadas. Eso hace que sea más probable que se produzcan accidentes.

ADVERTENCIA

Existen excelentes herramientas para la infraestructura basada en la virtualización, pero necesitarás un nuevo conjunto de herramientas para los entornos no virtualizados. Resulta tentador asignar la responsabilidad a cada equipo de aplicaciones, pero dividir la responsabilidad de las copias de seguridad aumenta tanto el riesgo como el tiempo de recuperación. El tiempo es, por supuesto, dinero. En este caso, el coste medio por hora de fallo de una aplicación crítica es de medio millón de dólares.

Por lo tanto, es mucho mejor contar con una solución de copia de seguridad nativa de la nube. Para realizar copias de seguridad y proteger las aplicaciones basadas en Kubernetes, necesitas una solución de copia de seguridad nativa de Kubernetes.

Cómo trabajar con diferentes modelos de implementación

No es necesario que nadie te diga que Kubernetes ha cambiado las reglas del juego. Es algo revolucionario y popular, una forma diferente de arquitectura que ha desplazado a la capa de abstracción, lo que ha aumentado la flexibilidad para mejorar el funcionamiento de las cargas de trabajo. Existen diferencias fundamentales entre la plataforma Kubernetes y casi todas las infraestructuras informáticas anteriores.

Lo que no ha cambiado, sin embargo, son los requisitos en torno a las copias de seguridad. En todas las plataformas, no solo Kubernetes, cada administrador debe tener un plan de seguridad.

Una de las reglas atemporales que puede hacer frente eficazmente a cualquier escenario de fallos es la llamada regla de copia de seguridad 3-2-1. Este planteamiento ayuda a responder a dos preguntas importantes: ¿Cuántos archivos de copia de seguridad debo tener y dónde debo guardarlos? La regla de copia de seguridad 3-2-1 proporciona las respuestas:

- **3:** Ten al menos tres copias de tus datos.
- **2:** Guarda las copias en dos soportes distintos.
- **1:** Guarda una copia de seguridad fuera de las instalaciones.

RECUERDA

Empieza por el hecho de que no asignas aplicaciones en contenedores a servidores o máquinas virtuales (MV). A diferencia de las MV, todo lo que necesita un contenedor es un sistema operativo, programas y bibliotecas de apoyo, y recursos de sistema suficientes para ejecutar un programa específico.

Teniendo esto en cuenta, puedes poner dos o tres veces más aplicaciones en un solo servidor con contenedores que con una MV. Los contenedores también permiten crear un entorno operativo portátil y coherente para el desarrollo, las pruebas y la implementación. Kubernetes distribuye los componentes de la aplicación entre todos los servidores utilizando su propia política de colocación para aumentar el rendimiento y la tolerancia a fallos.

Si abordas estas situaciones con un sistema tradicional de gestión de datos, lo más probable es que fracases. Puede que consigas realizar copias de seguridad, pero si utilizas herramientas que no están diseñadas de forma nativa para la nube, las cosas empezarán a ponerse difíciles cuando llegue el momento de la recuperación.

A esto se añade el hecho de que las aplicaciones nativas de la nube se benefician de la naturaleza dinámica de su entorno. Para mejorar el equilibrio de la carga, los contenedores pueden reprogramarse sobre la marcha o ampliarse en diferentes nodos. Las nuevas implementaciones se llevan a cabo de forma constante, y los componentes se añaden y eliminan continuamente.

RECUERDA

En otras palabras, la aplicación cambia con regularidad. Lo que necesitas es una solución de copia de seguridad que entienda los patrones arquitectónicos nativos de la nube, una que no tenga problemas cuando

no haya estabilidad en las direcciones IP, una que adore el cambio tanto como lo hace tu aplicación Kubernetes nativa de la nube.

Las soluciones de copia de seguridad tradicionales que funcionan bien en un entorno de servidores y máquinas virtuales pueden ser como peces de agua dulce en un océano salado si las arrojas al entorno de Kubernetes. Para cumplir requisitos como el descubrimiento dinámico de las aplicaciones, la copia de seguridad instantánea, la recuperación de la integración de plataformas y la capacidad de capturar todo el contexto de la aplicación, lo que necesitas es una copia de seguridad nativa de Kubernetes.

CUESTIONES TÉCNICAS

Para comprender un poco mejor esta evolución, ten en cuenta que los sistemas físicos requerían un enfoque basado en agentes para proteger los datos y el sistema operativo. Cuando llegó la virtualización, muchos de esos mismos proveedores de copias de seguridad simplemente trasladaron sus agentes al mundo virtual. Esto creaba una sobrecarga en las máquinas virtuales a la hora de realizar la copia de seguridad, ya que las trataba como máquinas físicas en su nuevo entorno.

Quedó claro que la mejor forma de proteger estas cargas de trabajo virtuales era en la capa de virtualización a través de API. Esto permitió crear copias de seguridad coherentes con la aplicación de forma rápida y eficaz, sin afectar al rendimiento de la máquina virtual.

En pocas palabras, se está repitiendo una vez más la misma historia en el mundo de Kubernetes. En teoría, podrías tomar tu proceso de virtualización o copia de seguridad física y proteger parte de tu entorno y de tus datos de Kubernetes. Algunos, pero no todos, podrían estar protegidos, lo que complica bastante las cosas a la hora de la recuperación.

Desplazarse a la izquierda (Shift Left)

Muchos visualizan la filosofía DevOps como un símbolo de infinito, el «8» tumbado que crea un bucle infinito de movimiento de izquierda a derecha, de izquierda a derecha, y así sucesivamente. También se puede considerar casi como una pista de carreras, lo que encaja con el hecho de que DevOps trata sobre ciclos de desarrollo de aplicaciones de alta velocidad.

RECUERDA

Cuando se visualiza DevOps con imágenes infinitas, es habitual pensar que el desarrollo está a la izquierda y las operaciones, a la derecha. La filosofía DevOps, cuando se utiliza en el mundo de Kubernetes, aúna las necesidades y los requisitos de los desarrolladores y las operaciones de una forma que tradicionalmente nunca había sido así. Ocurre más en

el lado izquierdo de ese bucle, de ahí el término «desplazamiento a la izquierda» (Shift Left).

De hecho, Kubernetes se centra en los desarrolladores y sus aplicaciones, y en esa carrera constante a través de los ciclos de desarrollo. Debido al diseño de la plataforma, las soluciones de copia de seguridad deben centrarse más en las aplicaciones que en la infraestructura.

En este entorno, los desarrolladores definen, como código, tanto los componentes de la aplicación como los requisitos de infraestructura, el almacenamiento y los equilibradores de carga. El requisito de protección de datos debe integrarse y hablar el mismo idioma que su código. Esto les permite definir los sistemas de protección en lugar de la práctica tradicional de dejarlo en manos del administrador de la infraestructura o las copias de seguridad.

CONSEJO

Necesitas una forma de introducir las tareas de gestión de datos en el proceso de desarrollo cotidiano. Así ya no es solo responsabilidad del equipo de operaciones. Una buena forma de conseguirlo es a través de una API. La plataforma de copia de seguridad debe priorizar la API con una API nativa de la nube.

Hablamos de una API nativa de Kubernetes frente a las antiguas API REST o SOAP. La autenticación y la autorización se realizan sin problemas y se consigue una integración más sencilla de las aplicaciones y los flujos de trabajo. Los desarrolladores y operadores pueden utilizar herramientas que conocen bien, como kubectl.

Solucionar los problemas de los operadores

La virtualización se centra en abstraer el *hardware* físico y aprovecharlo para construir múltiples máquinas virtuales que alberguen cargas de trabajo monolíticas. En cambio, las cargas de trabajo nativas de la nube se centran por completo en la aplicación y no en la máquina virtual. Esto simplifica las operaciones de gestión al centrarse en las aplicaciones como unidad operativa, separando la infraestructura o los almacenes de datos.

CONSEJO

Es esencial contar con una herramienta de copia de seguridad que permita flexibilidad y la posibilidad de elegir el enfoque. No todas las organizaciones necesitarán una API para controlar sus flujos de trabajo de copia de seguridad. Algunas necesitarán un panel de control para poder llegar hasta Kubernetes.

La integración profunda de Kubernetes puede ocultar la complejidad de la plataforma subyacente. Puedes eliminar o reducir el trabajo manual o de integración centrándote en la experiencia del usuario y revisando los flujos de trabajo de copia de seguridad para aplicaciones nativas de la nube.

Piensa que, en el pasado, una sola aplicación podría haber utilizado unas pocas máquinas virtuales, mientras que las aplicaciones en contenedores de hoy en día se componen normalmente de cientos de recursos diferenciados de Kubernetes, entre ellos, la configuración, los discos y los Secrets.

Se trata de solo una aplicación. Ahora piensa en todas las aplicaciones de un clúster; tu operador deberá comprender y proteger millones de componentes. Es decir, a menos que la aplicación sea la unidad operativa de la copia de seguridad.

ADVERTENCIA

Es probable que un sistema de copia de seguridad heredado preste atención a la infraestructura, como los discos y volúmenes, y pase por alto los recursos de Kubernetes. Esa es la receta para que se produzcan muchos errores en las guías de estrategias de recuperación, donde faltarán relaciones que den lugar a tiempos de recuperación muy elevados.

Lo que se necesitaría en esta desafortunada situación es un proceso manual para averiguar qué copias de seguridad son necesarias para la restauración, y luego otro complejo proceso manual para conectar los volúmenes restaurados de nuevo a las aplicaciones de Kubernetes. Eso supondría una enorme carga para las operaciones, incluso si no se ha producido ningún cambio en los objetos de Kubernetes entre la copia de seguridad y la restauración (y eso no es probable).

Cerrar las brechas

Es difícil superar a Kubernetes a la hora de mantener las aplicaciones en funcionamiento aunque se produzcan interrupciones parciales en la infraestructura. La tolerancia a fallos es un buen argumento de venta, pero es importante no tener una falsa sensación de seguridad y pasar por alto la necesidad de copias de seguridad y restauración, recuperación ante desastres, movilidad de aplicaciones y protección contra *ransomware*.

RECUERDA

Una vez más, una alta disponibilidad y replicación no equivale a las copias de seguridad. Sigues corriendo el riesgo de que los datos se dañen o se borren, ya sea de forma accidental o por un acto malintencionado. Si eso ocurre, puede propagarse a todas las réplicas y provocar una pérdida de datos catastrófica.

Pero como Kubernetes se ejecuta a menudo en nubes públicas, ¿no hace que el almacenamiento sea a prueba de fallos? No, eso es un mito. Las soluciones de almacenamiento en la nube más fiables prometen un tiempo de actividad muy fiable, pero la protección de los datos es tu responsabilidad.

Los proveedores de almacenamiento locales pueden ofrecer instantáneas de volumen, ¿no? Sí, pero estas instantáneas son con frecuencia vulnerables a los fallos del *hardware*. Y si se elimina un volumen, las instantáneas relacionadas suelen eliminarse automáticamente.

Aquí es donde entra en juego la regla de la copia de seguridad 3-2-1 descrita anteriormente en el apartado «Cómo trabajar con diferentes modelos de implementación». Seguir esta regla te protegerá contra la mayoría de los escenarios de fallo (si no todos), especialmente cuando empieces a añadir protección de inmutabilidad a tus copias externas.

CUESTIONES TÉCNICAS

Sin altos privilegios de seguridad en Kubernetes, normalmente no tendrás acceso a acciones como la desactivación de la actividad del sistema de archivos. Pero si dispones de un sistema de copia de seguridad nativo de Kubernetes con permisos bien definidos y control de acceso basado en funciones, puedes obtener enganches de desactivación de las cargas de trabajo de la base de datos y Kubernetes, lo que permite obtener el mismo resultado sin comprometer la seguridad.

Lo importante es que los desarrolladores y el departamento de operaciones colaboren, o al menos, que lo hagan más estrechamente que en el pasado. El denominador común que une sus intereses es hacer lo que sea correcto para los datos.

La recuperación en caso de desastre es otro aspecto clave a tener en cuenta. Las copias de seguridad son fundamentales cuando nos encontramos ante escenarios de fallos que pueden recuperarse dentro del mismo clúster, pero la recuperación ante desastres implica poner en marcha las cargas de trabajo en una ubicación completamente distinta.

Integrar los ecosistemas

CUESTIONES TÉCNICAS

La *persistencia políglota* es un término que se refiere al uso de múltiples tecnologías de almacenamiento de datos para diferentes necesidades de almacenamiento de datos a través de una aplicación o dentro de componentes más pequeños de una aplicación. Y no solo hablamos de bases de datos relacionales y no relacionales, sino también de áreas de almacenamiento como el flujo de datos por lotes y las colas de mensajes.

Estas diferentes necesidades de almacenamiento de datos pueden surgir en una empresa con múltiples aplicaciones, o en componentes individuales de una aplicación que necesitan almacenar datos de forma diferente entre sí. La persistencia políglota va en aumento a medida que Kubernetes se va imponiendo.

La buena noticia es que, a pesar de esta complejidad, puedes obtener unas copias de seguridad más enriquecidas de estas cargas de trabajo mediante la integración contra Kubernetes para el descubrimiento automatizado de las cargas de trabajo. Esto significa que la solución de copia de seguridad puede tener en cuenta los requisitos de la aplicación y elegir lo fundamental de la captura (como instantáneas de volumen, copias de seguridad coherentes con la aplicación y volcados lógicos).

Con un único servicio de datos convertido en algo del pasado, los metadatos de Kubernetes pueden permitir que la solución de copia de seguridad distinga automáticamente la relación entre múltiples servicios de datos independientes.


RECUERDA

Controlar la topología de la aplicación permite a la solución de copia de seguridad nativa de Kubernetes capturar una copia coherente de toda la pila de aplicaciones, tanto dentro de los servicios como entre ellos. Eso le permite identificar y recopilar datos de las réplicas para reducir el impacto de la aplicación. El rendimiento y la eficiencia mejoran, y el aprovechamiento del paralelismo de Kubernetes optimiza el rendimiento de la restauración.

Otro ángulo de la complejidad: cada vez más organizaciones ejecutan muchos clústeres de Kubernetes en distintos entornos. La plataforma de copia de seguridad debe, por tanto, interoperar con el resto del ecosistema de infraestructuras nativas de la nube.


RECUERDA

En última instancia, obtendrás una mejor experiencia de usuario, ayudarás a los equipos operativos a ser más eficientes y reducirás costes, todo ello al mismo tiempo. Un elemento de esa experiencia de usuario mejorada es el hecho de que los desarrolladores y operadores pueden seguir utilizando las herramientas nativas de la nube a las que se han acostumbrado. Por ejemplo, integración con Prometheus para supervisar y alertar, e integración con las API de Kubernetes para el RBAC, el registro y la auditoría que se necesitan en la realización de los análisis de causa raíz.

EN ESTE CAPÍTULO

- Centrarse en la aplicación en su conjunto
- Explorar y ampliar la arquitectura
- Garantizar la recuperabilidad
- Facilitar las operaciones
- Mantener una seguridad estricta en un entorno multiinquilino
- Restaurar con éxito manteniendo la portabilidad

Capítulo 3
Las mejores prácticas para la copia de seguridad de Kubernetes

Como se ha descrito en los capítulos 1 y 2, el entorno Kubernetes es un mundo en sí mismo. Lo que hacías antes con la copia de seguridad no es suficiente y puede que ni siquiera funcione.

Este capítulo se centra en algunas de las mejores prácticas para gestionar las copias de seguridad de tus aplicaciones de Kubernetes. Analiza las diferencias en la arquitectura que requieren un enfoque centrado en la aplicación, examina de qué forma se puede garantizar la recuperabilidad y explora cómo un sistema de copia de seguridad nativo facilita las operaciones a medida que la aplicación se amplía y se reduce. Destaca la importancia de los aspectos que hay que tener en cuenta de cara a la seguridad, incluso cuando el entorno multiinquilino complica las cosas. Y aborda los retos que plantean los objetos y las API en constante evolución, así como la importancia de la portabilidad.

Captar la aplicación

A grandes rasgos, la aplicación es el verdadero centro de atención. La infraestructura es vital, pero su función es hacer que la aplicación esté

disponible y sea flexible. Siempre ha sido así, pero este hecho adquiere un significado especial en el contexto de Kubernetes centrado en los desarrolladores, las aplicaciones que crean y la velocidad a la que las desarrollan y actualizan.

Una plataforma tan centrada en el desarrollador y en la aplicación requiere una solución de copia de seguridad que también haga lo mismo. Como se ha explicado en los capítulos 1 y 2, tu copia de seguridad debe ser nativa de Kubernetes para que funcione de forma adecuada con las aplicaciones en contenedores del mundo Kubernetes.

CONSEJO

Centrarse en la aplicación significa comprender cómo se construye Kubernetes en lugar de enfocarse hacia la infraestructura. Exige una captura completa de la aplicación para proteger todos sus componentes sin que falte ningún recurso, filtro o etiqueta.

Aprovechar la arquitectura

Este libro se centra específicamente en la copia de seguridad de Kubernetes, una parte esencial del gran éxito en esta plataforma. Para ello, no hace falta profundizar demasiado en la arquitectura de Kubernetes, pero es útil dedicarle algo de tiempo para poder tener una idea de cómo implementar una buena estrategia de copia de seguridad.

Conectar los componentes

En la figura 3-1 se muestran algunos de los principales componentes de una aplicación de Kubernetes. Entre otras cosas, verás Pods, servicios, certificados, Secrets y volúmenes persistentes.

Una aplicación en producción constará de cientos de componentes como estos. La pregunta es: ¿cuál es la mejor manera de proteger y restaurar los datos y el resto de componentes internos? ¿Cómo se puede hacer esto a gran escala?

CONSEJO

Te alegrará saber que no todo depende de ti. Elige la plataforma de copia de seguridad adecuada e interactúa automáticamente con el plano de control de Kubernetes a través del servidor API. Mediante esta integración, la solución de copia de seguridad descubrirá las aplicaciones de Kubernetes que se ejecutan en el clúster. A continuación, se integra con la infraestructura subyacente de procesamiento, red y almacenamiento.

Lo primero es descubrir la relación entre el almacenamiento y las aplicaciones. Después, se trata de encontrar la mejor manera de capturar los datos de la aplicación almacenados en volúmenes persistentes, junto con todos los recursos de la aplicación relacionados. Esto debe gestionarse de forma eficaz y coherente.

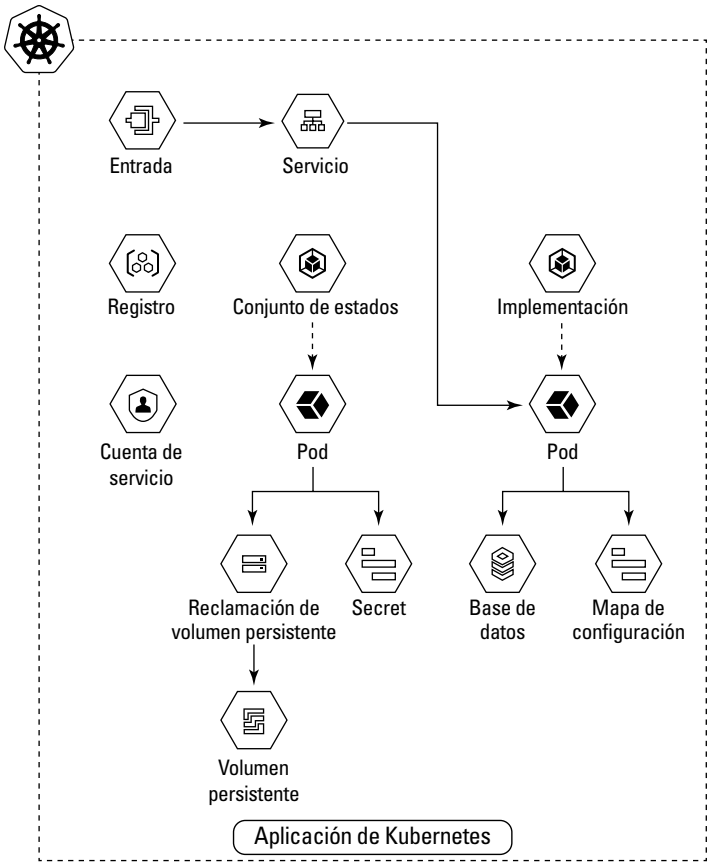

FIGURA 3-1: Una aplicación de Kubernetes básica es una colección de componentes interrelacionados que deben interactuar con el sistema de copia de seguridad y recuperación.

Lo siguiente es determinar la ubicación de los datos de la copia de seguridad. Puede estar dentro del sistema de almacenamiento para permitir una recuperación rápida o, si utilizas uno de los principales proveedores de la nube, mediante instantáneas duraderas. En la mayoría de los casos, sin embargo, es mejor almacenar los datos de copia de seguridad en un sistema de almacenamiento de objetos situado en un dominio de fallos diferente, que pueda permitir la georreplicación para la recuperación ante desastres. «Más vale prevenir que curar» es una manera sencilla, pero adecuada, de actuar.

CONSEJO

La regla de las copias de seguridad 3-2-1 que se explicó en el capítulo 2 es una buena norma a seguir para planificar las copias de seguridad. Necesitas al menos tres copias de tus datos, que deben almacenarse en dos soportes diferentes, y una copia debe guardarse fuera de las instalaciones. Tus datos corren un riesgo mucho mayor si no sigues este planteamiento básico.

Cuando se trata de la integración del almacenamiento en Kubernetes, tienes un par de cosas más en las que pensar:

- El almacenamiento se representa como volúmenes persistentes que están disponibles para que los usen los contenedores. Necesitas proteger estos datos de negocio clave.
- ¿Dónde vas a guardar esos datos? ¿Usarás un almacenamiento local en bloque? Quizá pienses en una plataforma de almacenamiento de objetos, como Amazon S3 o el almacenamiento blob de Microsoft Azure, si estás ejecutando Kubernetes en las instalaciones o fuera de ellas. La elección del almacenamiento secundario para las copias de seguridad debe incluir flexibilidad, capacidad de elección y facilidad de uso.

Así pues, tu lista básica de tareas pendientes en este ámbito incluye:

- Descubrir la relación entre las aplicaciones y su almacenamiento.
- Determinar cómo capturarás los datos de las aplicaciones en volúmenes persistentes.
- Decidir dónde guardarás las copias de seguridad para asegurarte de que cumples las directrices 3-2-1.

RECUERDA

Sea cual sea la plataforma que utilices para proteger las aplicaciones de Kubernetes, esta debe descubrir automáticamente todos los componentes que se ejecutan en el clúster y tratar esa aplicación como la unidad de atomicidad. Es vital que la aplicación incluya el estado que abarca todos los volúmenes de almacenamiento y bases de datos, así como los datos configurables en objetos de Kubernetes, como los ConfigMaps y los Secrets.

Ampliar

En una aplicación que se ejecuta en Kubernetes hay mucho bajo el capó. Las aplicaciones se dividen en cientos de componentes diferentes con sus propios ciclos de vida, gracias a todos los microservicios y soporte de Kubernetes, desde la configuración hasta la gestión de los Secrets. Esta complejidad es en gran medida visible solo para Kubernetes.

Se necesita una solución de copia de seguridad nativa de la nube para gestionar todos los millones de componentes de los grandes clústeres y comprender las relaciones entre las aplicaciones, los datos que utilizan y el estado de Kubernetes relacionado. Solo una solución nativa en la nube puede capturar todo esto a escala.

RECUERDA

Al igual que Kubernetes y las aplicaciones nativas de la nube se crean para llevar a cabo con facilidad ampliaciones y reducciones en respuesta a la carga, las soluciones de copia de seguridad deben ser capaces de hacer lo mismo. Esto es lo que debes esperar de tu solución de copia de seguridad:

- Adopta el mismo patrón arquitectónico nativo de la nube para poder ampliarse con los cambios en las aplicaciones y los clústeres.
- Se reduce a cero cuando no se utiliza.
- Hace estas cosas automáticamente, sin necesidad de intervención manual por parte del operario.

RECUERDA

Con una plataforma de copia de seguridad que crezca a la vez que el clúster conseguirás el mejor rendimiento. Pero también ahorrarás dinero, porque su consumo de recursos está vinculado a las necesidades actuales, que varían de forma instantánea, en lugar de a la carga máxima. Además, como el sistema de copia de seguridad se amplía de forma lineal con el crecimiento de la aplicación y el clúster, es mucho más fluido. No hay saltos de función como los que verías en un modelo basado en un dispositivo.

Los retos de la ampliación se vuelven aún más complejos al aumentar el uso del multiclúster de Kubernetes. Puede haber miles de espacios de nombres por clúster y cientos de recursos de Kubernetes por espacio de nombres.

Verás varios clústeres en distintos entornos, como desarrollo, preparación y producción. Pero también hay divisiones entre los límites de las aplicaciones, la seguridad y los equipos. Y los clústeres se implementan en múltiples zonas de disponibilidad, regiones, nubes y centros de datos locales.

Todo esto supondría una enorme carga operativa si se tuviera que gestionar manualmente. Para ser sinceros, ni siquiera es posible, a menos que se disponga de una plataforma de copia de seguridad nativa de la nube que pueda gestionar operaciones multiclúster y ofrecer visibilidad global de todo ello.

Estos son los pasos esenciales que debes dar en relación con la ampliación:

- Asegúrate de que tu solución de copia de seguridad pueda ampliarse y reducirse en función de las aplicaciones que protege.
- Determina cómo responderá tu solución a los retos del multiclúster de Kubernetes.

Planificar la recuperabilidad

La recuperabilidad es el santo grial del que trata este libro. Requiere una cantidad considerable de planificación y ejecución; es mucho más que limitarse a volver a crear objetos de Kubernetes y volúmenes de almacenamiento.

CONSEJO

Al fin y al cabo, tu aplicación basada en contenedores es compleja, con muchos componentes de Kubernetes. El primer paso es crear un plan de ejecución que se ocupe de lo siguiente:

- Verificar las dependencias del clúster.
- Crear nuevas vistas de Kubernetes de los datos que deben restaurarse.
- Determinar la infraestructura informática y el clúster de Kubernetes donde se iniciará la recuperación, como una recuperación de zona de disponibilidad cruzada.

Con ese plan en marcha, tendrás que identificar las fuentes de datos de la copia de seguridad, como son el almacenamiento de los objetos, las instantáneas y las copias de seguridad. Debes preparar el almacenamiento de destino, lo que implica la reasignación de la clase de almacenamiento y los cambios en la plataforma de almacenamiento, entre otras cosas.

CONSEJO

Determina si es necesario transformar el plan. Ten en cuenta aspectos como la regeneración de certificados TLS, los cambios de DNS y la edición de Secrets obsoletos. A continuación, debes actualizar los componentes de la aplicación de Kubernetes para que reflejen los nuevos recursos de almacenamiento que creará la recuperación.

Cuando finalice toda esta planificación, la plataforma de copia de seguridad debe traducir el plan en las llamadas a la API de Kubernetes adecuadas para crear los recursos que se necesitarán (por ejemplo, llamadas para crear un equilibrador de carga o para recrear un Secret). Todos los recursos y microservicios que forman parte de una aplicación nativa en la nube deben volver a implementarse con la configuración correcta. En la figura 3-2 podrás visualizar este proceso.

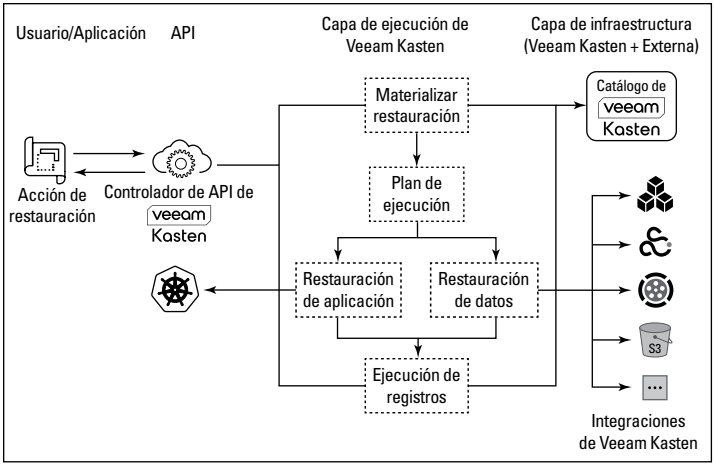

FIGURA 3-2: El proceso de restauración, incluidas las llamadas a la API que crean todos los recursos necesarios.

En definitiva, se trata de que puedas restaurar todos los componentes de la aplicación donde quieras, y debes disponer de la granularidad necesaria para poder restaurar solo un subconjunto de la aplicación si lo deseas: el volumen de datos, por ejemplo. Asegúrate de que tu solución de copia de seguridad te permita elegir la copia de la aplicación en el momento adecuado. ¿Y sería mucho pedir que todo esto fuera lo más sencillo posible? En absoluto.

Para resumir, la recuperación ante desastres requiere una planificación cuidadosa combinada con la herramienta adecuada para ejecutarla:

- Crea tu plan de ejecución centrado en las dependencias del clúster, las vistas de los datos y dónde se iniciará la recuperación.
- Identifica las fuentes de los datos y el almacenamiento de destino.
- Determina si es necesaria la transformación y cómo se actualizarán los componentes.
- Conviértelo todo en llamadas a la API de Kubernetes.

Centrarse en las operaciones

Recuerda algunas de las cosas que hacen que Kubernetes sea tan popular: A los desarrolladores les resulta rápido y sencillo implementar las aplicaciones, actualizarlas y hacer todo esto a escala. Lo último que

quieres es tener una plataforma de copia de seguridad que obstaculice esa eficacia. Eso sería frustrante en el mejor de los casos y, en el peor, podría inspirar a los desarrolladores a buscar la manera de sortear los procesos de mejores prácticas.

CONSEJO

De hecho, garantizar que todo el mundo siga las mejores prácticas operativas es siempre un reto, sobre todo cuando se utilizan nuevas herramientas, servicios y capacidades en una infraestructura dinámica. Tu plataforma de copia de seguridad nativa de Kubernetes debe:

- Poder utilizarse a escala.
- Proporcionar a los equipos de operaciones las funciones de flujo de trabajo que necesitan.
- Cumplir todos los requisitos de conformidad y control.
- No dar dolores de cabeza a los desarrolladores.

Desde el punto de vista de los desarrolladores, no debería ser necesario realizar cambios en el código, el empaquetado, la cadena de herramientas ni en la implementación. Los operadores también deben poder ofrecer a los desarrolladores funciones de autoservicio.

RECUERDA

Por ejemplo, los desarrolladores deben poder restaurar sus propias aplicaciones, además de poder personalizar y ampliar las operaciones de copia de seguridad de sus servicios de datos. Deben tener control sobre la coordinación entre servicios y la puesta en modo inactivo, así como el uso de herramientas personalizadas o de proveedores de bases de datos. Además, las interacciones de los desarrolladores con la plataforma de copia de seguridad deben basarse en la API.

En cuanto a los operadores, estarán encantados si la solución de copia de seguridad les libra de tener que centrarse en los cientos de componentes de Kubernetes que forman parte de la aplicación. Quieren políticas de copia de seguridad totalmente automatizadas que les permitan prestar atención a la aplicación en su conjunto en lugar de a los recursos individuales y la infraestructura de almacenamiento.

En lo que respecta a los detalles minuciosos de la política y todos los componentes de la aplicación que deben protegerse, esa labor solamente debería realizarse en el momento de ejecutar la política. A partir de ese momento, no debería existir la necesidad de llevar a cabo actualizaciones manuales para capturar todos los componentes a medida que cambia la aplicación (algo que, por supuesto, siempre hace).

TAREAS DE COPIA DE SEGURIDAD FRENTE A POLÍTICAS INTELIGENTES

¿Cuáles son las ventajas de establecer políticas de copia de seguridad inteligentes, en lugar de configurar tareas de copia de seguridad específicas? Piensa en las diferencias y compruébalo tú mismo.

Las tareas de copia de seguridad describen cada paso de la pila de *software*, hasta el momento de ejecutar la tarea. Las tareas de copia de seguridad pasan por alto en su mayor parte la arquitectura del centro de datos y necesitan ser guiadas para no obstaculizar las cargas de trabajo ni afectar a la capacidad de la red.

Las políticas, en cambio, se centran más en los resultados. En lugar de dictar calendarios o cambios imperativos, se define un objetivo de punto de recuperación o un resultado deseado. Una vez establecida, la política está siempre en marcha, siempre atenta a los problemas y necesidades, y preparada para garantizar el resultado deseado.

Puedes ver qué opción está más automatizada y cuál necesita más atención humana. Y esa atención humana no solo requiere tiempo, sino que además introduce esa desafortunada tendencia de los humanos a cometer errores cuando tienen mucho que configurar y recordar.

CONSEJO

He aquí otra de las mejores prácticas para ayudar a mantener las cosas lo más sencillas posible. Crea unas extensas políticas de copia de seguridad basadas en etiquetas capaces de detectar automáticamente las nuevas aplicaciones en cuanto aparezcan.

Por ejemplo, establece una política que coincida con todas las aplicaciones que utilizan MongoDB, o una política que gobierne las aplicaciones implementadas a través de la herramienta Helm. Juega bien tus cartas y no obligarás a los equipos de operaciones a crear procesos manuales de control de cambios. Y lo que es igualmente importante, tendrás la seguridad de que las aplicaciones nunca dejarán de cumplir los acuerdos de nivel de servicio de copia de seguridad a medida que se creen o se retiren.

En pocas palabras, busca una solución de copia de seguridad que ofrezca a todos lo que quieren y lo que necesitan. De hecho, es posible implementar una plataforma que satisfaga las necesidades tanto de los equipos de operaciones de contenedores como de los desarrolladores, así que no te conformes con menos.

En cuanto a las operaciones, estas son tus principales tareas:

- Asegúrate de que tu solución de copia de seguridad es realmente una solución y no un problema. Debe aumentar la eficacia, satisfacer las necesidades del flujo de trabajo y cumplir los requisitos.
- Determina los aspectos que podrían beneficiarse de unas políticas inteligentes y evita la necesidad de crear tareas de copia de seguridad específicos.
- Crea unas políticas que descubran por sí mismas las nuevas aplicaciones que se ajustan a su enfoque.

Garantizar la seguridad

Tanto si llevas a cabo una implementación en una nube pública como si utilizas una infraestructura local o cualquier tipo de entorno híbrido, la seguridad tiene que ser una prioridad. Si echas un vistazo a los titulares de un día cualquiera, está claro que la seguridad es ahora más importante que nunca. Y el aumento de los entornos multiinquilino te da una razón más para vigilar la seguridad.

Proteger por capas

En el lado positivo, Kubernetes incorpora muchas funciones de seguridad, incluidas políticas de red que protegen los componentes internos de las aplicaciones y los servicios de datos asociados a ellos. Kubernetes no solo bloquea el acceso a estos componentes desde fuera del clúster, sino que también añade una señal de parada a las aplicaciones no fiables que se ejecutan en el mismo clúster.

RECUERDA

Esto es bueno, pero también significa que no vas a poder ejecutar soluciones de copia de seguridad fuera de los clústeres de Kubernetes. No podrán descubrir las aplicaciones — ni acceder a ellas para, por ejemplo, ponerlas en modo inactivo — sin debilitar las políticas de aislamiento. La respuesta es una solución nativa de Kubernetes bien diseñada que sea capaz de integrarse en el plano de control.

Otro reto con el que puedes encontrarte es la necesidad de capacidades de autoservicio, ya que los desarrolladores asumen cada vez más responsabilidades relacionadas con la infraestructura. La implementación de tu sistema de copia de seguridad debe incluir controles en torno a la gestión de identidades y accesos, y no puedes prescindir del control de acceso basado en funciones (RBAC). Esa es la manera de controlar qué usuarios y grupos obtienen qué niveles específicos de acceso, restricciones o privilegios de usuario con respecto a la plataforma de copia de seguridad.

El alcance de los accesos, de hecho, debe concederse utilizando las mismas funciones y herramientas definidos por Kubernetes. Eso es mejor

que introducir un mayor número de sistemas de gestión de funciones que tus equipos tendrán que aprender a usar.

En lo que respecta al equipo de operaciones, necesitas un enfoque de mínimos privilegios para las tareas frecuentes, como la supervisión de las copias de seguridad, la verificación del éxito y la integridad de las copias de seguridad, y la gestión de las restauraciones solicitadas. Puedes crear casos de uso específicos según tus necesidades. Puedes conceder un permiso para que los desarrolladores hagan restauraciones rápidas y clones a partir de instantáneas, mientras que el acceso a las copias de seguridad en el almacenamiento secundario externo está reservado solamente para personas determinadas.

Además, tu plataforma de copia de seguridad nativa de la nube tiene que poder integrarse profundamente en los sistemas de gestión de identidades y accesos de la nube, los sistemas de gestión de claves y la gestión de certificados. Además, un sistema de gestión de datos que sea realmente nativo de Kubernetes se integrará en la solución de autenticación del proveedor de la nube sin necesidad de gestión adicional de usuarios o grupos, ni de nuevas herramientas o API para políticas RBAC.

CONSEJO

Ten en cuenta que Kubernetes delega el cifrado de los datos al sistema de almacenamiento subyacente y a la plataforma de copia de seguridad. Debes estar seguro de que los datos de tu aplicación nunca se almacenen ni transfieran en texto simple. Por este motivo, la plataforma de copia de seguridad debe:

- Comprender la gestión de certificados de Kubernetes.
- Funcionar con sistemas de gestión de claves integrados en el almacenamiento.
- Admitir claves de cifrado gestionadas por el cliente a través de la interfaz de Secrets de Kubernetes.

Por poner el almacenamiento de objetos como ejemplo, si tienes una implementación de aplicaciones de Kubernetes a nivel local que descarga copias de seguridad en AWS S3, tus datos llegarán de aquí a allá a través de una conexión a Internet externa. La plataforma de copia de seguridad debe garantizar el cifrado de los datos mediante un protocolo como TLS.

El proceso de cifrado no termina cuando los datos llegan al lugar donde se almacenan. Tu sistema debe asegurarse de que también esté cifrado allí, porque si no está cifrado en reposo, no hay seguridad. No basta con implementar RBAC y las políticas correspondientes; también se necesitan algoritmos de cifrado probados, como AES-256-GCM, con claves

de cifrado por aplicación. De lo contrario, corres el riesgo de que se produzcan fugas de datos accidentales o incluso copias malintencionadas.

ADVERTENCIA

Y hablando de riesgos maliciosos, tu sistema debe estar siempre alerta ante los ataques de *malware* y *ransomware* dirigidos a Kubernetes. La amenaza crece continuamente, ya que muchas aplicaciones de Kubernetes están orientadas a clientes externos.

Teniendo esto en cuenta, echa un vistazo a la protección conocida como *inmutabilidad*, que protege contra cualquier modificación y borrado de tus copias de seguridad en el almacenamiento de objetos, incluido el cifrado o borrado malintencionado. Esto ayuda a neutralizar la amenaza de *ransomware*.

Con todo esto en su conjunto se puede apreciar la necesidad de una solución de copia de seguridad que sea nativa de Kubernetes, pero que también pueda crear copias de seguridad fiables que sean independientes de Kubernetes y del sistema de almacenamiento. Debe disponer de integraciones profundas que permitan restauraciones rápidas y automatizadas.

La seguridad es una labor crítica y aquí te ofrecemos algunas consideraciones claves:

- Integra una solución de copia de seguridad nativa de Kubernetes en el plano de control.
- Crea capacidades de autoservicio que no comprometan la seguridad.
- Asegúrate de que tu solución ofrezca siempre cifrado y otras capas de protección.

Convivir con los entornos multiinquilino

Si pensamos en productos heredados, los sistemas de copia de seguridad suelen ser específicos de los administradores, y pueden ser pocas las personas que usen todo el sistema. Podría haber usuarios que solo necesitan visualizar y muchos menos que tengan todos los permisos. En cuanto a las restauraciones, puede que tengas que hacer una solicitud o preguntar a alguien.

Los clústeres de Kubernetes tienden a ser multiinquilino, y siempre hay desarrolladores y equipos de desarrolladores que se añaden y eliminan dinámicamente en el sistema. Tienen sus propios espacios y sus propias aplicaciones, y todo el mundo tiene que ocuparse básicamente de sus propios asuntos.

CONSEJO

Cualquier sistema de copia de seguridad en este entorno debe ser de autoservicio, y los desarrolladores deben tener control sobre la red, el cortafuegos, el aprovisionamiento de almacenamiento y las restauraciones,

pero solo para sus propias aplicaciones. El sistema debe tener un tipo de alcance que solamente permita a los desarrolladores tener visibilidad y acceso a las aplicaciones que les pertenezcan.

Por ejemplo, si un desarrollador es propietario de la aplicación X, solo debería ver la aplicación X, y definitivamente, no la aplicación Y, que pertenece a otro desarrollador distinto. Y ese desarrollador de la aplicación Y no debería poder tener ninguna visibilidad o acceso a la aplicación X.

¿Cómo se consigue esto? Entre otras cosas, dispones de un control de acceso basado en funciones (como ya hemos visto anteriormente en este capítulo). Algunos desarrolladores necesitan permiso para las copias de seguridad y la restauración, mientras que otros pueden tener acceso solo a restaurar con la copia de seguridad a cargo de una persona distinta. Algunos solo tienen acceso de visualización. La idea es establecer varios grupos diferentes, cada uno con su propio acceso adecuado.

¿Cómo se puede automatizar algo así? Las herramientas como Open Policy Agent (OPA) permiten esencialmente expresar la política como código.

CONSEJO

La clave es que el enfoque debe ser nativo de Kubernetes. Lo que no quieres son unos sistemas independientes para gestionar a los usuarios, como un sistema RBAC fuera de la plataforma. El sistema de copias de seguridad debe heredar las API para que no haya herramientas ni gestión de usuarios adicionales. Cualquier otra cosa sería demasiado engorrosa.

Estos son algunos aspectos clave con respecto a los entornos multiinquilino:

- Asegúrate de que tus opciones de autoservicio limiten a los desarrolladores solamente a sus propias aplicaciones.
- Procura ser coherente para no tener que mantener sistemas distintos de gestión de usuarios.

Transformar el soporte para la restauración

No cabe duda de que Kubernetes está evolucionando rápidamente. Cada tres meses aproximadamente se publica una nueva versión, lo que significa que los objetos pueden cambiar rápidamente. A esto se añade el hecho de que las organizaciones pueden saltarse versiones cuando hacen actualizaciones, ya que es posible que no hayan estado al día con todas las actualizaciones intermedias. Y piensa también en la portabilidad que conllevan los entornos basados en contenedores de Kubernetes. ¿Cómo haces que todo esto funcione?

Seguir el ritmo del cambio

ADVERTENCIA

La tendencia hacia unos ciclos cada vez más cortos entre las distintas versiones crea situaciones en las que puedes tener una copia de seguridad de, digamos, hace un mes o un año, y que no reconozca los objetos que han cambiado. Y no se trata solo de las API de Kubernetes, sino también de recursos personalizados u otro tipo de componentes. Si esto ocurre e intentas llevar a cabo una restauración con una versión de la API que el sistema ya no admite, la restauración fallará.

CONSEJO

Por eso el sistema necesita poder transformar las características y descriptores de los componentes del sistema de las versiones antiguas a las actualizadas. Por ejemplo, debe ser capaz de hacer evolucionar la API de un objeto de la versión antigua a la versión más reciente. O gestionar un certificado de corta duración. O Secrets que deban ser actualizados.

La transformación también es clave cuando los clústeres de Kubernetes se trasladan de un lugar a otro (como se explica en el siguiente apartado sobre portabilidad). ¿Pasar de una nube local a una nube pública? La transformación permite que el proceso de restauración sea sencillo y portátil.

En este entorno acelerado y dinámico, no puedes pasar por alto el hecho de que las cosas se queden obsoletas o caduquen, o que cambien las versiones de la API, o se actualice alguna otra cosa, o tu clúster aproveche la portabilidad de Kubernetes. Cuando restauras, también debes ser capaz de transformar.

Así que, con respecto a la transformación, ten en cuenta estos aspectos clave:

- Asegúrate de que tu solución adopta la transformación para poder seguir el ritmo cada vez más acelerado de las nuevas versiones.
- Utiliza la transformación para facilitar la portabilidad.

Facilitar la portabilidad

La portabilidad es una de las muchas capacidades positivas que proporciona Kubernetes, y una plataforma de copia de seguridad puede utilizar esta potente función para poner en práctica un gran número de casos de uso. Consulta la figura 3-3 para ver algunas de las posibilidades.

Estos son algunos de los posibles casos de uso de la portabilidad:

- En todos los namespaces en el mismo clúster
- En todos los sistemas de almacenamiento

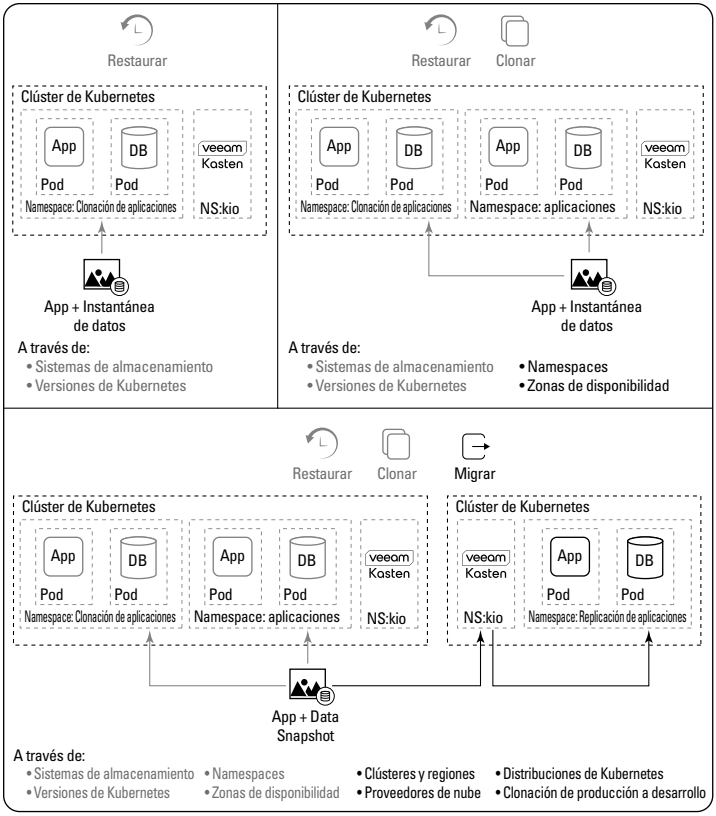

FIGURA 3-3: El poder de la portabilidad en las copias de seguridad nativas de Kubernetes.

- En todos los clústeres, distribuciones y versiones de Kubernetes
- En todas las zonas de disponibilidad de una misma región
- En todas las regiones de la misma nube
- En todos los entornos de nube o híbridos
- En todos los entornos de prueba y desarrollo

RECUERDA

Como sabes, hay mucha diversidad de ecosistemas en Kubernetes, tanto a nivel local como en la nube. Además, cada vez más empresas utilizan un modelo de nube híbrida para ejecutar aplicaciones basadas en contenedores. Teniendo esto en cuenta, tu plataforma de copia de seguridad y gestión de datos debe ser capaz de migrar aplicaciones entre clústeres

de origen y destino que podrían estar funcionando en infraestructuras diferentes.

Consulta la figura 3-4 para ver a qué te enfrentas al migrar una carga de trabajo de Elastic Kubernetes Service (EKS) de Amazon a Azure Kubernetes Service (AKS) de Microsoft.

```
kind: StorageClass
apiVersion: storage.k8s.io/v1
metadata:
      name: gp2
provisioner: kubernetes.io/aws-ebs
parameters:
      type: gp2
      fsType: ext4
```

```
kind: StorageClass
apiVersion: storage.k8s.io/v1
metadata:
      name: managed-premium-retain
provisioner: kubernetes.io/azure-disk
reclaimPolicy: Retain
parameters:
      storageaccounttype:
Premium_LRS
```

FIGURA 3-4: Migración de EKS a AKS y cómo debe transformarse la terminología.

La diferencia en las clases de almacenamiento es solo el principio en lo que respecta a las distintas distribuciones, incluso si estas se basan en la misma versión subyacente de Kubernetes. Es fundamental que tu plataforma de copia de seguridad pueda realizar restauraciones en estas distintas distribuciones y opciones de infraestructura, transformando automáticamente la copia de seguridad de la aplicación para adaptarla al entorno de restauración.

RECUERDA

Es una tarea pesada, pero vital. La plataforma de copia de seguridad tiene que ser capaz de comprender todas las dependencias de las aplicaciones y trasladarlas con éxito de un entorno a otro.

Para garantizar el éxito de la ejecución de la migración, debes contar con un plan de migración que garantice que las dependencias de la infraestructura, el clúster y las aplicaciones estén disponibles o se transformen en un recurso equivalente. Ten en cuenta que no solo debes migrar contenedores y volúmenes de almacenamiento, sino también gestionar la modificación en curso de elementos como FQDN, Secrets y direcciones DNS.

En resumen, la portabilidad depende de consideraciones como estas:

- Garantizar que tu solución de copia de seguridad y gestión de datos pueda migrar aplicaciones entre clústeres que operan en diferentes infraestructuras.
- Disponer de un plan de migración para garantizar que todas las dependencias estén disponibles o se transformen en un recurso equivalente.

EN ESTE CAPÍTULO

- Familiarizarse con el entorno de la nube
- Unir la copia de seguridad y la recuperación ante desastres
- Prosperar en un entorno multiclúster

Capítulo 4
Cómo lograr la movilidad de las aplicaciones nativas de la nube

Te podemos perdonar si has leído los tres capítulos anteriores y crees que es increíblemente complicado conseguir una copia de seguridad y una recuperación ante desastres de forma eficaz en el mundo actual basado en contenedores. No cabe ninguna duda de que se trata de una labor sofisticada, pero con las herramientas adecuadas no resulta tan desafiante. Lo que necesitas es un lugar centralizado desde el que gestionar el trabajo.

En este capítulo hablaremos de lo que más deseas: lograr la movilidad de las aplicaciones contando siempre con una copia de seguridad sólida y una recuperación ante desastres adecuada. Hablaremos también de las difusas líneas que separan la copia de seguridad de la recuperación, y los retos que se van superando a medida que el número de clústeres y recursos crece de manera exponencial.

Ponerse en marcha con la nube

CONSEJO

Para los que sean relativamente nuevos en el mundo de Kubernetes, la forma más fácil de acostumbrarse a la plataforma es ejecutando la solución en la nube pública. Encontrarás Kubernetes disponible como servicio de proveedores como Google, Microsoft y AWS.

Los proveedores de nubes públicas llevan a cabo el mantenimiento del servicio y se encargan de vigilar detalles como la rotación de los certificados, la versión y los parches. También ofrecen opciones de almacenamiento y gestionarán todo lo que esté en el clúster.

Puedes profundizar aún más en la composición y la arquitectura implementando tu propio clúster de Kubernetes. Arrancar desde cero es sin duda una opción, pero ten en cuenta que implementar tu propio clúster significa que todas las cosas que el proveedor de servicios gestionaría por ti en la nube pública pasarán a ser tu responsabilidad.

Líneas difusas

No habrías abierto este libro si no supieras lo vitales que son las copias de seguridad y la recuperación ante desastres para que tu organización tenga éxito (e incluso sobreviva). Desde luego esto no es ninguna novedad.

También es probable que ya sepas que las copias de seguridad y la recuperación no siempre han sido pan comido. En el pasado, y ciertamente antes de que Kubernetes llegara a escena en 2015, con frecuencia nos encontrábamos con plataformas independientes para diferentes funciones y con más de una copia de los datos.

RECUERDA

En el mundo de Kubernetes, el usuario actual quiere capturar los datos una sola vez. Debe existir un conjunto de datos que pueda utilizarse en múltiples contextos: para copias de seguridad y restauración, para recuperación ante desastres, para facilitar la movilidad de las aplicaciones, para pasar de un clúster a otro, y cosas similares. Las líneas que separan la copia de seguridad de la recuperación ante desastres son difusas, pero las herramientas que tienes a tu disposición te facilitarán el camino.

Estos conceptos hablan de la necesidad de ofrecer autoservicio a los desarrolladores y a los operadores que realizan múltiples tareas. Es importante debido a los múltiples casos de uso implicados, y nada de esto debería ser una opción de última hora. La portabilidad y la movilidad de las aplicaciones no deberían ser extremadamente complicadas, razón por la cual la compatibilidad con la transformación (como se ha explicado en el capítulo 3) es tan esencial.

Cuando se habla de moverse entre nubes o regiones distintas, estamos hablando de transformar las cosas. ¿Cómo se transforman las cosas en lo que respecta a las prestaciones necesarias para la movilidad? Es una de las capacidades básicas que se exigen a una plataforma de gestión de datos.

Añadir clústeres

Un gran número de organizaciones utilizan muchísimos clústeres. No es raro ver más de 50 clústeres en producción. Es probable que estas organizaciones empezaran a pequeña escala y después pensaran a lo grande, con clústeres de mayor capacidad o múltiples clústeres para distintos eventos, como pruebas, desarrollo, preparación y producción.

Los clústeres pueden ejecutar cargas de trabajo basadas en una serie de atributos. Por ejemplo, aplicaciones específicas, dominios de seguridad y preparación para la implementación, por unidad de negocio individual y quizás por divisiones geográficas.

Hay muchas buenas razones para adoptar un enfoque multiclúster. Entre las ventajas se incluyen la personalización de los clústeres para adaptarlos a los requisitos de la carga de trabajo (piensa en el tamaño de los nodos) y quizás la reducción del radio de alcance. Hoy en día, el estándar es el enfoque multiclúster; incluso muchos clústeres pequeños tienen tres, cinco o diez nodos.

RECUERDA

Si haces cuentas, el alcance de la tarea de gestionar esto es asombroso. Si a esto le sumamos el número de clústeres y aplicaciones y el número de recursos y volúmenes por aplicación, pronto queda claro que es imposible gestionarlos todos de forma independiente.

CONSEJO

Para ver una serie de casos prácticos instructivos que muestran detalles de implementación para la copia de seguridad y recuperación de Kubernetes, consulta `https://www.veeam.com/resources/customer-stories.html?product=product%3A68`.

Esto se debe a que estás gestionando copias de seguridad y permisos relacionados con los RBAC mencionados en capítulos anteriores. Los aspectos de multiinquilino y seguridad complican aún más las cosas.

Tu sistema de copia de seguridad y recuperación ante desastres debe proporcionar un lugar centralizado para gestionar toda esta complejidad, ofreciendo una visión global de lo que está sucediendo. Tienes que ser capaz de profundizar en diferentes contextos y favorecer la movilidad a través de estos clústeres.

Es importante facilitar a los operadores la gestión de todo esto desde un solo lugar. También es vital hacer más fácil la labor de los desarrolladores. Tu objetivo es simplificar, no solo añadiendo clústeres, sino permitiendo la movilidad de las aplicaciones multiclúster.

A continuación se exponen algunos de los requisitos de gestión de datos para operar sin problemas en entornos multiclúster:

- **Seguridad:** No solo para los datos, sino también para las operaciones, ofreciendo la visibilidad adecuada a los usuarios y sistemas pertinentes.
- **Fácil configuración:** Debes poder establecer operaciones multiclúster sin instalaciones complicadas, y debe ser sencillo configurar y gestionar las políticas y los recursos.
- **Descubrimiento automatizado:** Esto incluye el descubrimiento de las aplicaciones de Kubernetes, las políticas de copia de seguridad y cualquier cambio en todos los clústeres.
- **Visión global:** Insiste en contar con un único panel que te permita obtener una visión en tiempo real de la situación general.
- **Políticas y recursos globales:** Los equipos deben poder definir políticas globales (como la frecuencia de las copias de seguridad) y los recursos (como la ubicación del almacenamiento de destino).
- **Agrupación flexible de clústeres:** Permite a los usuarios definir fácilmente las agrupaciones lógicas flexibles y arbitrarias de los clústeres para la distribución de políticas y recursos globales.
- **Desglose de clúster único:** Dentro de esta capacidad de visión de conjunto, debes poder examinar de cerca cualquier clúster individual.


RECUERDA

Aquí está la moraleja de esta historia en particular. Necesitas un sistema de copia de seguridad y gestión de datos nativo de Kubernetes que elimine toda esta complejidad.

EN ESTE CAPÍTULO

- Conocer el ecosistema
- Adaptarse a la forma de trabajar de los operadores
- Habilitar políticas de auditoría y seguridad
- Lograr registros y aumentar la visibilidad
- Mantener actualizado el sistema de copias de seguridad

Capítulo 5
Instalarse en el ecosistema nativo de la nube

Un sistema de copias de seguridad eficaz necesita coordinar muchos puntos para que todo el mundo esté contento y tus datos estén seguros. El sistema tiene que encajar en los flujos de trabajo, las preferencias y las políticas de la organización. También necesita mantenerse a la vanguardia en un ecosistema que cambia a una velocidad vertiginosa.

Este capítulo trata de la necesidad de integrar el sistema en las herramientas que tus operadores prefieren utilizar y en las políticas de seguridad y las necesidades de auditoría ya implantadas. Explica cómo el sistema debe facilitar el registro y dar a los operadores visibilidad y capacidad de observación de su funcionamiento. También describe por qué las nuevas versiones deben producirse con una frecuencia asombrosa.

Comprender el ecosistema de la gestión de datos

Como se muestra en la figura 5-1, el ecosistema de la gestión de datos de Kubernetes consta de cuatro subcomponentes importantes que desempeñan un papel fundamental en la solución global:

- **Aplicaciones:** Para lograr una solución completa, las aplicaciones deben poder integrarse de forma óptima en los principales servicios de datos, incluidos los sistemas relacionales y NoSQL.
- **Distribuciones de Kubernetes:** Las distribuciones deben ser compatibles con las principales ofertas de Kubernetes gestionadas y basadas en la nube, así como con las principales distribuciones en el entorno local.
- **Apoyo a la infraestructura de almacenamiento:** Esto debería proporcionarse para las interfaces de almacenamiento en contenedores, así como para las integraciones directas de almacenamiento para una mayor eficiencia.
- **Servicios de seguridad:** La seguridad de Kubernetes debe abordar la protección de la infraestructura del clúster, la gestión del control de acceso, la protección de los datos confidenciales y la supervisión de vulnerabilidades y ataques de *ransomware*.

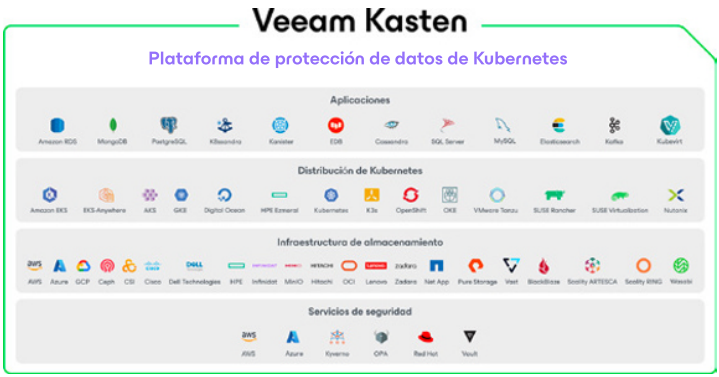

FIGURA 5-1: Las cuatro partes importantes del ecosistema de la gestión de datos de Kubernetes.

La coherencia de todo el espectro, las integraciones de las bases de datos, el descubrimiento automático de las aplicaciones, la movilidad *multicloud* y una potente interfaz de usuario basada en web completan las capacidades necesarias de una solución sólida.

Integración con Prometheus y Grafana

Los sistemas de copia de seguridad más antiguos han introducido muchas funciones útiles, como registros, informes, alertas y auditorías, pero no siempre han facilitado la vida a los operadores. Ahora bien, la medida del éxito de un buen sistema de copia de seguridad no debe ser solo cómo permite realizar las copias de seguridad, sino cómo consigue que no haya fricciones para los responsables de operaciones. ¿Cómo puede encajar en su flujo de trabajo y vivir felizmente en la infraestructura a la que están acostumbrados?


RECUERDA

En el ecosistema de Kubernetes, Prometheus es el referente para la supervisión y el almacenamiento de métricas de aplicaciones, *software* y *hardware* para realizar un seguimiento del estado del sistema, identificar problemas y solucionarlos. Grafana es una herramienta de visualización de código abierto que se utiliza a menudo con Prometheus. Tiene sentido que tu plataforma de copia de seguridad nativa de Kubernetes se integre con ambas. Los operadores dispondrán de los datos adecuados para crear cuadros de mando, generar activadores, configurar alertas y obtener unos conocimientos más visuales del estado general del sistema.

Aprender auditando

Con algo tan importante como los datos, siempre se quiere saber exactamente quién hizo qué con ellos, dónde y cuándo. Tu sistema de copia de seguridad debe ofrecerte esa visibilidad a efectos de auditoría en el futuro.


RECUERDA

En lugar de proporcionar su propio sistema de auditoría independiente, la solución de copia de seguridad de Kubernetes debería lograrlo conectándose a la auditoría de Kubernetes de forma transparente. Esto funciona bien en el entorno multiinquilino y permite que los permisos y la identidad de los usuarios lleguen hasta la infraestructura.

Un sistema de copia de seguridad debe estar en sintonía con el usuario para que aparezcan los registros de auditoría adecuados. No basta con saber que «el sistema de copia de seguridad hizo X». Necesitas saber que «el sistema de copia de seguridad hizo X en nombre del usuario Bob». Esa capacidad debe estar presente para lograr unas funciones de registro lo más eficaces y precisas posible.

Vinculación con las políticas y la seguridad de la red

Es importante no debilitar nunca la posición de seguridad de una aplicación. Por ejemplo, un contenedor que ejecute una base de datos en un sistema SQL no debe estar expuesto al mundo exterior solo para realizar copias de seguridad.

CONSEJO

Incluso si la base de datos es interna para la aplicación, un sistema de copia de seguridad integrado en el plano de control de Kubernetes podrá acceder a la base de datos sin exponerla al resto del mundo. Eso disminuye los peligros de *ransomware* y otros comportamientos maliciosos.

Avanzar en los registros

Todos los usuarios tendrán su propio sistema de registro. El sistema de copia de seguridad deberá poder ajustarse según los registros y modificarse para adaptarse a las necesidades de la organización.

También debería existir la posibilidad de extraer registros y, desde luego, no perderlos. Necesitas una interfaz consolidada con cualquiera que sea el sistema de registro de terceros que tengas en tu entorno.

Mejorar la observabilidad

La observabilidad implica comprender los aspectos de supervisión del sistema de copias de seguridad y disponer de los datos para correlacionar los eventos. Tu organización necesita detalles completos sobre las aplicaciones que no se comporten correctamente, o saber qué aplicaciones estaban ocupadas y provocaron que la copia de seguridad tardara más tiempo.

También es clave la observabilidad del *backend* de las operaciones de copia de seguridad cuando se envían datos a un almacén de objetos. Hay que poder controlarlo y seguir el flujo de los datos.

Estar al día con los ciclos de versiones de Kubernetes

Kubernetes se actualiza cada tres meses, lo que genera muchos cambios en los sistemas dependientes, incluidos los de copia de seguridad y recuperación. El sistema de copias de seguridad debe mantenerse al día para que la organización esté siempre protegida.

Todas las distribuciones comerciales complican las cosas, ya que tienen sus propios ciclos de versiones. Además, los clientes se actualizan muy a menudo porque saben que en tres o cuatro ciclos, si no antes, su versión quedará obsoleta.

RECUERDA

La copia de seguridad, por tanto, tiene que asegurarse de estar siempre al tanto de estos cambios para poder llevar a cabo su labor de protección. Teniendo en cuenta el rápido ritmo de los cambios que se producen alrededor de este entorno, actualizar una o dos veces al año simplemente no será suficiente.

De hecho, se lanzarán varias versiones al mes. Veeam, por ejemplo, suele publicar actualizaciones cada dos semanas y, en algunos casos, incluso con más frecuencia. Es la única manera de responder a los cambios del resto del ecosistema.

Capítulo 6
Diez puntos claves sobre las copias de seguridad de Kubernetes

Hay mucho que aprender sobre las copias de seguridad de Kubernetes, y en las cuarenta y pico páginas anteriores se ha hablado de ello con todo detalle. Pero si quieres ceñirte a los puntos más cruciales, sigue leyendo, ya que en este capítulo explicamos algunos de los aspectos claves.

Comprender la arquitectura

- **Estar al día con Kubernetes:** En el mundo conocido como Kubernetes, parpadeas un segundo y ya te has perdido un montón de cosas. Por ejemplo, cuando Kubernetes apareció por primera vez en 2015, las aplicaciones que se ejecutaban en la plataforma Kubernetes a menudo se diseñaban para que fueran sin estado, pero eso ya no ocurre. Este plano de control es un vehículo ideal para aplicaciones con y sin estado. Se trata de un gran avance, pero hay que tener cuidado con los datos.

- **Capacitar a los desarrolladores:** El objetivo de Kubernetes es hacer que las aplicaciones funcionen bien, y los desarrolladores te dirán que eso es también lo que quieren ellos. Pero mientras van en el asiento del conductor, se adentran en una carretera nueva con algunas curvas por las que nunca han pasado antes. Diseñan los componentes de las aplicaciones, pero también definen los requisitos de la infraestructura de un modo que quizá no hubieran hecho en el pasado. Existe un riesgo añadido, que es una de las razones por las que se necesitan copias de seguridad y recuperación sólidas para este ecosistema.

Centrarse en las operaciones

- **Diferenciar la implementación:** La infraestructura informática de Kubernetes es muy diferente de todo lo que ha existido hasta la fecha. La utilizas para crear aplicaciones en contenedores, cuyos componentes distribuirá Kubernetes entre varios nodos para mejorar el rendimiento y la tolerancia a los fallos. Lo que no estás haciendo es asignar estas aplicaciones en contenedores a servidores o máquinas virtuales. Tu solución de copia de seguridad debe comprender estos patrones arquitectónicos nativos de la nube para saber cómo realizar su trabajo con eficacia.
- **Crecer y decrecer:** Las aplicaciones en contenedores del entorno de Kubernetes pueden ampliarse y reducirse en función de la carga. Lo mismo debe ocurrir con la solución de copia de seguridad. Necesita tener el mismo patrón arquitectónico nativo de la nube para que pueda ampliarse con los cambios que se producen en la aplicación y en los clústeres. Eso garantiza su funcionamiento eficaz, además de que resulta ser lo más rentable.

Mejorar el sistema de copia de seguridad

- **Elegir un sistema nativo:** Ya sabes lo importantes que son las copias de seguridad y la recuperación ante desastres, pero no esperes conectar tus nuevas y relucientes aplicaciones con estado basadas en Kubernetes a una herramienta de copia de seguridad heredada creada para infraestructuras de virtualización. Es un tipo de tecnología totalmente diferente de lo que ocurre en Kubernetes. Tu única apuesta segura para la copia de seguridad de Kubernetes es un sistema de copia de seguridad nativo de Kubernetes que encaje a la perfección.

- **Confundir disponibilidad con copia de seguridad:** El tiempo de inactividad puede resultar increíblemente caro. Esa es una de las razones por las que a tanta gente le encanta ejecutar aplicaciones en contenedores en Kubernetes. Pero la replicación y los otros trucos de magia que hacen que esto ocurra no equivalen a una copia de seguridad. Tus datos siguen estando en peligro, a menos que te propongas protegerlos deliberadamente.
- **Mantenerlo recuperable:** La copia de seguridad y recuperación ante desastres nativa de Kubernetes presta especial atención a las relaciones y dependencias entre los numerosos componentes de un contenedor determinado. Kubernetes va a mover cosas todo el tiempo para mantener su funcionamiento y escalabilidad (piensa en la capacidad de ráfaga que necesitaría la aplicación de un comercio en el *Black Friday*). La copia de seguridad tiene que saber cómo aunar todo esto. Necesitarás un plan de recuperación detallado que incluya vistas de todos los datos que será necesario restaurar. Tendrás que identificar las fuentes de datos de la copia de seguridad, así como el almacenamiento de destino. Y tendrás que saber qué debe transformarse en la recuperación.

Mantener la seguridad

- **Conectarse a las medidas de seguridad nativas:** Kubernetes incorpora medidas de seguridad inteligentes que ayudan a dejar dentro a las personas adecuadas y fuera a las equivocadas. No solo a las personas, sino también a los componentes de las aplicaciones. Si tu solución de copia de seguridad y recuperación se ejecuta fuera de tus clústeres de Kubernetes, realmente no puede hacer su trabajo de descubrir y acceder a las aplicaciones.
- **Amar a tus vecinos:** ¿Has vivido alguna vez en un piso compartiendo paredes con los vecinos? Aprendes a equilibrar la confianza mutua con un nivel saludable de autoprotección. Así es como suelen ser los clústeres de Kubernetes, con aplicaciones que comparten espacios a través del entorno multiinquilino. Los desarrolladores necesitan acceso y visibilidad a sus propias aplicaciones, pero no a las de los demás. Y el sistema de copia de seguridad debe seguir las mismas reglas, empleando los mismos tipos de controles de acceso para garantizar que todo y todos permanezcan en el lugar que les corresponde.

Cambiar la velocidad de mejora

- **Mantenerse actualizado:** Algunas personas conducen sus coches hasta que han acumulado 150 000 o 200 000 kilómetros, mientras que a otras les gusta firmar un nuevo contrato de alquiler cada dos años. No encontrarás código informático con mucho kilometraje en el mundo de Kubernetes. Sus habitantes se mantienen al día de las últimas tendencias y tecnologías. Lo mismo debe hacer tu solución de copia de seguridad. Vas a encontrarte con nuevas versiones de forma muy regular, porque es la única forma de garantizar una protección continua en un mundo en el que las actualizaciones se suceden a un ritmo vertiginoso.

Copia de seguridad y restauración de Kubernetes, RD, movilidad de aplicaciones y protección frente a ransomware

Kubernetes es el *software* de infraestructura de más rápido crecimiento y se ha convertido en la plataforma líder de aplicaciones empresariales. Aunque Kubernetes proporciona una gran disponibilidad y escalabilidad de los servicios de las aplicaciones, estas ventajas no se extienden a tus datos. Por ello, la protección de los datos es una prioridad fundamental para las cargas de trabajo de Kubernetes. En este libro encontrarás la información y las herramientas que necesitas para proteger las aplicaciones de Kubernetes de manera adecuada.

En el interior...

- Comprender Kubernetes y las aplicaciones nativas de la nube
- Crear una protección de datos nativa para Kubernetes
- Las mejores prácticas para la copia de seguridad y recuperación de Kubernetes
- Cómo lograr la movilidad de las aplicaciones nativas de la nube
- El ecosistema nativo de la nube

Steve Kaelble es autor de muchos libros de la serie *Para Dummies* y sus artículos se han publicado también en revistas, periódicos e informes empresariales anuales. Cuando no se dedica al mundo *Para Dummies* ni a escribir artículos, participa en comunicaciones relacionadas con la sanidad.

Visita Dummies.com®
para ver vídeos, fotografías paso a paso, artículos con instrucciones o comprar productos.

ISBN: 978-1-394-35362-0

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.