



➤ Escenarios de desastre en tu E-Commerce

Te damos la solución

Cualquier administrador con cierta experiencia en la materia sabe que nada es infalible y, tarde o temprano, surge ese problema inesperado que se escapa a todas las previsiones y planes de contingencia. En el caso de plataformas de E-Commerce pueden ocurrir infinidad de problemas inesperados que deriven en una pérdida completa de servicio, incluso en el caso de que todas las piezas de la plataforma de TI sean altamente disponibles por sí mismas:



Un certificado de CA caducado dentro del código fuente que provoca que falle la conectividad con servicios de terceros o, incluso, con la base de datos principal.



Una modificación en el ERP empresarial provoca una sobrecarga inesperada en la base de datos de E-Commerce, tumbando la web de clientes.



Una tabla de la base de datos degrada su rendimiento repentinamente al pasar de un número determinado de filas, afectando a la carga de todas las páginas del catálogo.



Un fallo de su proveedor de comunicaciones deja a sus servidores de E-Commerce aislados de Internet, imposibilitando a los clientes acceder al mismo.



Un administrador del catálogo lanza accidentalmente una sincronización masiva de productos desde el ERP en plena hora punta de pedidos, provocando una ralentización masiva de la web y, eventualmente, la pérdida de servicio.



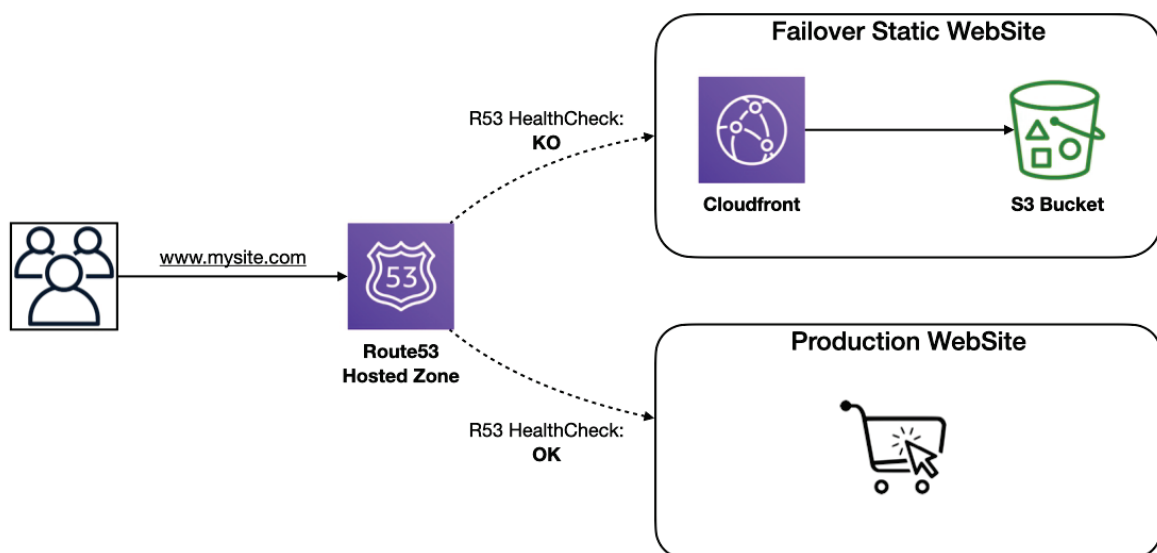
Un nuevo API desarrollado recientemente contiene un bug no detectado en la fase de QA que provoca que los procesos se queden bloqueados pero sin fallar o devolver una respuesta al cliente.



Como consecuencia de esto, el pool de hilos configurado en el servidor de aplicaciones termina por agotarse ejecutando peticiones de este nuevo API que no generan trabajo útil. Al agotarse el pool, el servidor de aplicaciones deja de atender nuevas peticiones provocando una caída total del servicio.

Durante este tipo de eventos en los que no hay un problema inherente al diseño de arquitectura sino que se trata de circunstancias de tiempo de ejecución que provocan caídas graves e inesperadas de la plataforma de comercio electrónico, suele haber un elemento en común: La mala imagen empresarial que se da al usuario final cuando la web no responde o responde con un error genérico que no da ninguna certidumbre.

Para conseguir mejorar esta situación de incertidumbre y mala imagen empresarial en circunstancias extraordinarias, una solución de bajo coste y rápida implementación sería la disposición de una web estática con un contenido personalizado y acorde a la estética de la web principal, que se ofrezca a los usuarios automáticamente en caso de catástrofe en el sistema de E-Commerce productivo. El diagrama de arquitectura sería el siguiente:



Maintenance Web Page
Route53 Routing

➤ La Solución Propuesta

a continuación se apoya en los siguientes servicios de Amazon Web Services:



Simple Storage Service (S3)

Este servicio proporciona el alojamiento de los contenidos del sitio de emergencia. El coste del almacenamiento es residual para una simple web estática de emergencia (0,023 \$/GB en el momento de escribir este artículo), no requiere de ningún tipo de mantenimiento por parte del usuario y los datos están replicados en múltiples zonas de disponibilidad de AWS dentro de una misma región geográfica, garantizando la disponibilidad y durabilidad de los contenidos.



Amazon Cloudfront

La red de distribución de contenidos de AWS se encargará de la negociación de SSL y la disposición del dominio personalizado, así como de cachear los contenidos de la web de emergencia en ubicaciones geográficas cercanas a los usuarios finales para mejorar los tiempos de respuesta.



Esta red de distribución de contenidos conforma el punto de entrada a la web de emergencia y tiene su origen de datos en S3.



Route53 Healthchecks

Este servicio de monitorización permitirá enviar sondas sencillas al sitio principal desde múltiples ubicaciones geográficas, generando una métrica sintética que proporcionará la lógica necesaria para el reenvío condicional de usuarios vía DNS.



Route53 Hosted Zones

Este servicio proporciona una infraestructura de DNS altamente disponible con servidores de nombres distribuidos geográficamente por los múltiples datacenters de AWS en todo el mundo, y será el encargado de reenviar a los usuarios al E-Commerce productivo o la página de mantenimiento según determinen las sondas del healthcheck anterior.

Una vez funcionando la solución propuesta, el escenario de fallo catastrófico sería el siguiente:

-  **1** Mientras las sondas tengan un resultado satisfactorio, el servicio de DNS enviará a los usuarios a la aplicación principal.
-  **2** En caso de que el sitio principal sea incapaz de atender a las peticiones de las sondas de verificación, la lógica del healthcheck se invertirá y el servicio de DNS enviará a los usuarios a Cloudfront, que recuperará los contenidos de S3, cacheandolos y sirviendolos desde la ubicación de borde más cercana al usuario final.

Los usuarios reciben un contenido estéticamente consistente con la tienda online que esperaban encontrar, pero indicando que se está trabajando en recuperar el servicio, dándoles certidumbre acerca de lo que ocurre y facilitando que estos vuelvan a visitar nuestra tienda en los próximos minutos. Todo ello sin necesidad de intervención manual.

NOTA

Esta solución se apoya en el uso de TTLs de DNS bajos. Cuanto menor sea el TTL de los registros DNS, mayor será el tiempo de reacción ante un fallo catastrófico en el datacenter principal. Un TTL en torno a los 60s permitirá reaccionar rápidamente a los cambios que se presenten a la vez que permite que se cacheen un gran número de solicitudes durante la actividad normal de la web.

-  **3** Una vez recuperada la normalidad en el sitio principal, las sondas ejecutarán con normalidad y la lógica del healthcheck retornará al punto inicial, derivando en que los usuarios serán de nuevo dirigidos hacia el sitio principal. Se ha conseguido mantener el sitio vivo y con un mensaje de tranquilidad para los usuarios ante una situación catastrófica en el datacenter principal sin necesidad de que ningún técnico tenga que intervenir, permitiéndole además centrarse en resolver los problemas del sitio principal.