CLOUDFLARE

DOCUMENTO TÉCNICO

Resiliencia de la red y los servicios de Cloudflare

Contenido

Información general

Internet se basa en sistemas imperfectos que están diseñados para dar prioridad al tiempo activo por encima de cualquier otra cosa. Protocolos como TCP y BGP se basan en los principios de los sistemas distribuidos — prever fallos y tenerlos en cuenta — e Internet fue diseñado en consecuencia. Sin embargo, aún existen puntos débiles que pueden repercutir negativamente. Los proveedores de red deben poder planificar los fallos, detectarlos cuando se produzcan y mitigar el impacto que experimentan los usuarios.

Debido a la naturaleza en tiempo real de muchas aplicaciones en Internet, las redes no solo deben abarcar la mayor parte posible de la red de Internet, sino que también deben responder y mitigar el impacto en tiempo real. Las interrupciones del servicio que duran varios minutos son inaceptables, dado que los clientes esperan que se solucionen en cuestión de segundos.

Cloudflare ofrece servicios de infraestructura de red esenciales para ayudar a las organizaciones a proteger y comunicarse a través de Internet. Hemos desarrollado nuestra red y los servicios que proporciona para mantener el más alto nivel de excelencia operativa. Cloudflare procesa una media de más de 84 millones de solicitudes HTTP y 61 millones de consultas DNS por segundo, lo que le permite prestar servicio a millones de propiedades y usuarios de Internet.

¿Cómo proporciona Cloudflare un servicio fiable a esta escala dadas las características impredecibles de Internet?

La respuesta proviene de la arquitectura de la red de Cloudflare, que funciona con capacidades de resiliencia diseñadas para funcionar de forma independiente y hacer frente a todo tipo de interrupciones. Nuestras capacidades de procesamiento, redes y almacenamiento, junto con nuestros procesos operativos, están diseñadas para que Cloudflare sea tan fiable como el clásico tono de llamada de la red telefónica tradicional. Cloudflare ofrece el "tono de nube" metafórico para los servicios de red y seguridad de los que dependen los clientes, independientemente de las condiciones de Internet en un momento dado.

Este documento técnico analiza los desafíos de operar en tiempo real en Internet, y cómo Cloudflare está en una posición única para resolver esos desafíos.

La vida en un mundo imperfecto

Internet es un lugar imperfecto y, sin embargo, las organizaciones lo necesitan para desarrollar su negocio y gestionar entidades que vinculen usuarios, datos y dispositivos distribuidos con aplicaciones en la nube. Cualquier interrupción del servicio tiene graves implicaciones. A lo largo de los años, Cloudflare ha informado sobre una serie de importantes interrupciones del servicio de Internet en todo el mundo, que van desde accidentes hasta ataques DDoS, pasando por desastres naturales, entre otros.

Internet es una red diversa que se ha desarrollado como un conjunto de miles de redes participantes de diversos tamaños y capacidades, conectadas entre sí de manera flexible. Estas redes presentan distintos niveles de servicio. Algunas funcionan en la medida de lo posible, como un apoyo ofrecido de forma voluntaria, mientras que otras operan como parte de sus servicios comerciales. A través de acuerdos mutuos para intercambiar tráfico, que puede estar o no destinado a hosts de su propia red, Internet funciona como una estructura global gracias a la participación benévola de los intercambios regionales y locales de Internet y los proveedores de servicios.

Sin embargo, esta diversidad conlleva un grado de imprevisibilidad. La ruta que sigue cualquier paquete se basa en una secuencia de las mejores estimaciones y los mejores esfuerzos para su entrega. En ausencia de datos en tiempo real o modelos predictivos sobre las condiciones reales de la red en un momento dado, un paquete suele dar su siguiente salto utilizando rutas predeterminadas o la ruta presuntamente más corta. Ninguna de estas opciones considera el estado del servicio de red en sus decisiones de enrutamiento. Esto significa que los paquetes suelen estar sujetos a una serie de condiciones adversas:

- En el nivel más básico, las redes pueden experimentar fallos temporales y caídas de tensión que reducen el rendimiento y provocan la pérdida de paquetes.
- A medida que las redes se saturan, la congestión perjudica el rendimiento y la experiencia del usuario.
- Si bien estos tipos de ralentizaciones pueden producirse en condiciones operativas normales, un número cada vez mayor de interrupciones son causadas intencionadamente por terceros malintencionados, que consumen de forma maliciosa los recursos disponibles.

La misión de Cloudflare es ayudar a mejorar Internet. Con ese fin, desarrollamos infraestructura para que Internet sea más rápido, fiable y seguro. Esto es posible gracias a los servicios desde y a través de la red de Cloudflare, una de las redes más grandes del mundo que opera en nuestros propios servidores nativos (sin virtualización), una red troncal privada y una presencia global masiva a la que puede acceder, de media, el 95 % de la población mundial en menos de 50 m/s.[1]

Los clientes a menudo quieren entender cómo lo hacemos. ¿Cómo diseña Cloudflare servicios a tal escala, sin renunciar a la seguridad ni al rendimiento, y con la fiabilidad que necesitan las organizaciones? La respuesta proviene de un conjunto de objetivos Estrella Polar, que establecen cómo desarrollamos nuestra infraestructura para mantener el rendimiento a pesar de las fuerzas disruptivas, tanto externas como internas.

Cómo diseña Cloudflare la resiliencia

Muchas organizaciones se centran en mejorar la disponibilidad tratando de reaccionar mejor o más rápidamente ante los fallos. Para ello, es necesario invertir constantemente en sus capacidades y procesos de conmutación por error y someterlos a pruebas. Si bien estos son objetivos válidos, Cloudflare piensa de manera diferente. Nuestros equipos de ingeniería de resiliencia dedican un enorme esfuerzo a reducir los escenarios en los que se requiere una respuesta de recuperación ante desastres.

La ingeniería de resiliencia de Cloudflare parte de una premisa sencilla: **¿cómo crearías una infraestructura crítica que siga funcionando aun en caso de fallos?**

Cuando inevitablemente se producen fallos, los servicios resilientes de Cloudflare detectan y aíslan los fallos para que no afecten a la disponibilidad del servicio. Los fallos se resuelven fuera de banda desde nuestra prestación de servicios. Nos esforzamos para que toda nuestra cartera de servicios sea resistente a fallos.

Para comprender los principios de la resiliencia, es útil definir primero los conceptos fundamentales que subyacen a las rutas de tráfico con Cloudflare y los objetivos de diseño de los sistemas clave. En el nivel más abstracto, la arquitectura de Cloudflare se puede dividir en dos segmentos: **el plano de control y el plano de datos.** Cada uno tiene una resiliencia y una postura ante desastres únicas.

Resiliencia del plano de control

El plano de control proporciona la interfaz de gestión que establece la fuente de veracidad para la configuración de los servicios de red y seguridad en el entorno del cliente. El plano de control en sí no procesa el tráfico (que es la función del plano de datos). Indica al plano de datos qué políticas aplicar y gestiona las configuraciones en diferentes centros de datos.

Los servicios del plano de control de Cloudflare suelen implementarse en una topografía más tradicional y centralizada en tres centros de datos lógicamente relacionados, pero independientes, en una región principal (p. ej., Estados Unidos). Estos tres centros de datos se replican con una capacidad equivalente en una región secundaria (p. ej., la Unión Europea). Los servicios del plano de control están diseñados para ser resilientes y mantener una prestación de servicios coherente en caso de fallo de un único centro de datos en la ubicación principal. La pérdida de centros de datos adicionales en la ubicación principal activaría una conmutación por error a los centros de datos de la otra región (p. ej., en Europa frente a Estados Unidos).

De acuerdo con el enfoque de Cloudflare en la resiliencia antes de la recuperación, seguimos invirtiendo en mejorar nuestra postura de resiliencia.

Por ejemplo:

- Cada vez utilizamos más las dos regiones del plano de control en una configuración activa-activa, lo que aumenta simultáneamente nuestra capacidad y capacidad de respuesta, así como nuestra tolerancia a los fallos. En consecuencia, podemos hacer frente a más tipos de fallos sin interrupción del servicio ni necesidad de conmutación por error.
- También estamos aumentando la granularidad de cómo movemos los servicios entre los distintos sitios del plano de control, lo que nos permite responder con más precisión a los problemas de la infraestructura local.

Ingeniería de caos

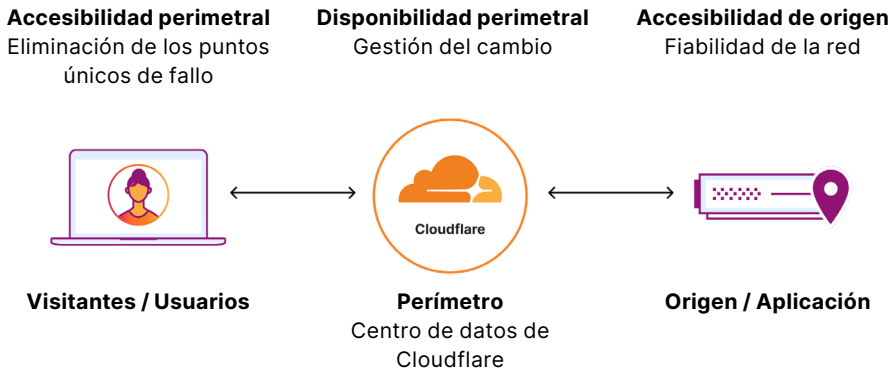
La resiliencia no es una actividad que se pueda configurar y dar por terminada. Incluso los planes de resiliencia más sólidos pueden resultar ineficaces debido a la "deriva" del sistema, es decir, la acumulación lenta y a menudo imperceptible de cambios que pueden degradar los comportamientos previstos e introducir modos de fallo imprevistos. Para abordar este riesgo de forma proactiva, la ingeniería de caos de Cloudflare analiza sistemáticamente las posibles vulnerabilidades relacionadas con la deriva.

Resiliencia del plano de datos

El plano de datos procesa el tráfico de los clientes de Cloudflare de acuerdo con las políticas establecidas desde el plano de control. Aunque los servicios del plano de datos reciben instrucciones del plano de control, no dependen de este para funcionar. Todas las políticas se mantienen a través de Quicksilver, nuestro almacén de pares clave-valor distribuido globalmente, para garantizar que los servicios sigan operativos con una configuración conocida en caso de que se produzca una interrupción de la comunicación con el plano de control.

Anycast desempeña un papel importante en la redundancia del centro de datos. Los centros de datos de Cloudflare, ubicados en más de 330 ciudades, son autónomos a nivel local y, sin embargo, son intercambiables entre sí mediante Anycast y BGP. Esto se debe a que cada centro de datos puede procesar localmente cualquier servicio, sin depender de los servicios de otro centro de datos. Con Anycast, todos los centros de datos son, en la práctica, redundantes entre sí. Como todos los centros de datos participan en Anycast, no es necesario indicar al cliente que cambie a un centro de datos alternativo en otra dirección IP.

Ya sea un consumidor que visita un sitio web protegido por Cloudflare, un empleado que accede a aplicaciones conectadas a Internet o una oficina que se conecta a su WAN, todos estos escenarios utilizan BGP para encontrar el centro de datos Cloudflare Anycast más cercano. Si el centro de datos elegido dejara de estar disponible, BGP se resolvería automáticamente al siguiente mejor centro de datos de Cloudflare.



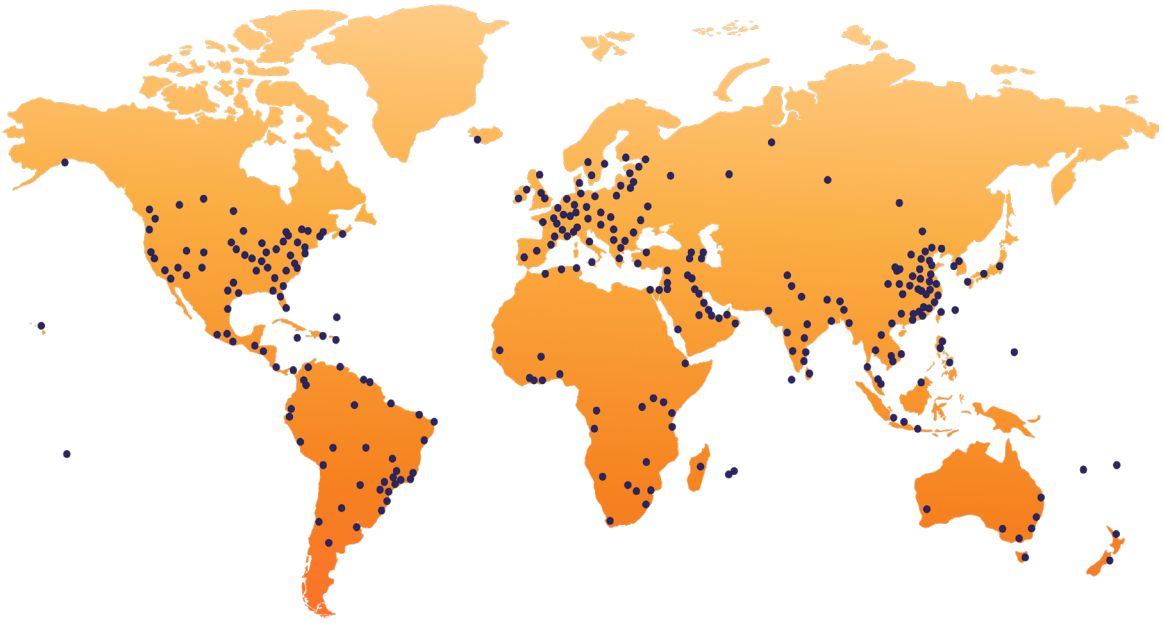
Cloudflare aborda la resiliencia del plano de datos resolviendo tres problemas diferentes:

- Accesibilidad perimetral: garantiza que el tráfico de los usuarios finales pueda llegar a los centros de datos y eliminar los puntos únicos de fallo en la entrada del tráfico
- Disponibilidad perimetral: mantenimiento de la calidad del código y el tiempo activo del software mediante una gestión de cambios rigurosa
- Accesibilidad de origen: enrutamiento adaptable a las aplicaciones de los clientes para garantizar que no se produzcan pérdidas en las rutas de salida

Accesibilidad perimetral

La accesibilidad perimetral es la capacidad de los usuarios finales de llegar a la red de Cloudflare. Podría decirse que es la pieza más importante del espacio del problema de la resiliencia. Si los proveedores de acceso a Internet (ISP) o los centros de datos dejan de funcionar, la accesibilidad perimetral se reduce o degrada, lo que impide o ralentiza el acceso de los usuarios a su destino en Internet. Cloudflare aborda los problemas de accesibilidad perimetral de cuatro maneras fundamentales:

1. Red Anycast



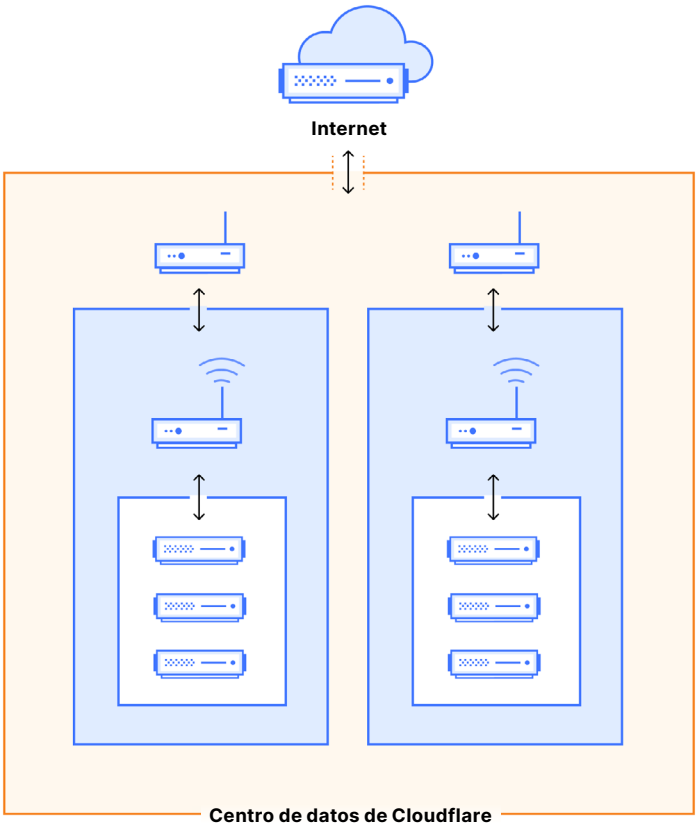
Nuestra arquitectura de red, que se basa en gran medida en la tecnología Anycast, incorpora un mejor rendimiento de red con resiliencia. Anycast, la superpotencia de ingeniería de Cloudflare, significa que el espacio IP se anuncia en todas partes. Si alguno de nuestros puntos de presencia (PoP) está desconectado, el tráfico simplemente se redirigirá a otras ubicaciones en lugar de interrumpirse. El hecho de que Cloudflare esté presente en tantas ciudades de todo el mundo e interconectado con redes locales significa que procesamos el tráfico de los clientes lo más cerca posible del usuario. Por ejemplo, aunque se desconecte el tránsito de un ISP o se produzca un corte de suministro eléctrico en un centro de datos, el tráfico no se ve afectado.

2. Todos los servicios de Cloudflare se ejecutan en todas las ubicaciones

Además de Anycast, los centros de datos de Cloudflare están diseñados para procesar el tráfico de forma local, sin depender de cadenas de proxy a otros sistemas informáticos. Ejecutamos casi todos los servicios en cada máquina. Esto significa que se puede desconectar un centro de datos sin afectar al cliente. Las máquinas del centro de datos son intercambiables entre sí, ya que hay cientos de ellas ejecutando el mismo servicio y capaces de sustituir a una en caso de que falle.

3. Puntos de presencia en múltiples centros de datos de colocación

El diseño y las ubicaciones de los centros de datos de Cloudflare reflejan las necesidades de nuestros clientes. Una red Anycast nos permite añadir / eliminar centros de datos a nuestra discreción, pero debemos supervisar constantemente el rendimiento del cliente. Hemos adaptado las topologías de nuestros centros de datos para permitir que las secciones de capacidad informática (colocaciones) fallen de forma independiente unas de otras. Estos centros de datos (con múltiples colocaciones) se denominan puntos de presencia de colocación (multiusuario) o ubicaciones MCP.



Estas ubicaciones bifurcan la conectividad de Internet de la conectividad informática interna para permitir que los centros de datos se desconecten individualmente. Esto significa que, incluso si se produce un problema con una colocación, todo el punto de presencia de una región puede permanecer en línea, lo que proporciona un mayor tiempo activo y rendimiento al cliente. Este tipo de centro de datos también elimina los puntos únicos de fallo al tener dispositivos redundantes en la capa conectada a Internet. Si un enrutador conectado a Internet (perimetral) falla, el otro enrutador perimetral puede asumir el tráfico y garantizar que la ubicación siga operativa.

Este modelo operativo ayuda a las ubicaciones MCP a evitar mover el tráfico a menos que sea absolutamente necesario y aumenta aún más el tiempo activo de los clientes de Cloudflare.

4. Cloudflare Traffic Manager

Los centros de datos MCP trabajan juntos para formar la red más amplia de Cloudflare. Esta red aprovecha Anycast para ayudar a garantizar el servicio del tráfico de los clientes. Anycast se ha mejorado con una gestión determinista del tráfico para garantizar que las solicitudes de los clientes se atiendan donde podamos hacerlo, con el mejor rendimiento posible. Este sistema de gestión de tráfico, Traffic Manager, funciona sondeando continuamente la red de Cloudflare y desviando automáticamente el tráfico de los centros de datos que experimentan una sobrecarga de la CPU. De esta forma, se evita la congestión en los centros de datos con mucho tráfico. En su lugar, el tráfico se enruta de forma inteligente a otro centro de datos que pueda gestionarlo.

Disponibilidad perimetral

La disponibilidad perimetral se refiere a la capacidad de Cloudflare para procesar el tráfico una vez que llega a nuestra red. Cuando los cambios en las herramientas de red o en el software provocan cambios no deseados, la disponibilidad puede disminuir y afectar a la experiencia del usuario. Para evitar incidentes derivados del cambio de código, Cloudflare ha invertido mucho en los siguientes controles de implementación:

1. Embudo de implementación

Cuando se implementa software, para garantizar la calidad del código hay que empezar por realizar un seguimiento y limitar la capacidad de los desarrolladores y clientes para incorporar cambios en el ecosistema. Cloudflare limita el número de formas en que cualquiera puede realizar cambios en nuestra infraestructura para que podamos supervisar de cerca cada cambio y asegurarnos de que pasan una serie de pruebas antes de su implementación en producción.

2. Gestión de cambios del radio de impacto

Otra forma en que Cloudflare respalda la disponibilidad perimetral durante la implementación es limitando las implementaciones a los centros de datos de prueba, o grupos de prueba, antes de su implementación generalizada. Es lo que llamamos gestión del radio de impacto.

Cuando se implementan los cambios en la red, pueden implementarse globalmente en cuestión de minutos. Si limitamos los cambios a un entorno de implementación y los implementamos de forma escalonada, podemos supervisar los efectos del cambio para detectar consecuencias previstas o imprevistas, antes de que afecten a zonas geográficas o poblaciones de usuarios más amplias.

Tenemos dos formas de limitar el impacto de los cambios de código:

- Limitar el número de ubicaciones que reciben cambios; y
- Limitar el número de usuarios que reciben cambios

Si limitamos el número de ubicaciones y máquinas que reciben cambios, podemos asegurarnos de que estamos realizando correctamente pruebas A/B del código dentro de una única ubicación para evaluar su estado antes de continuar. Además, al limitar el número de usuarios que reciben cambios, podemos probar primero las correcciones en poblaciones de usuarios más reducidas.

3. Implementación mediada por el estado

La implementación mediada por el estado es un sistema que evalúa de forma programática la idoneidad de una versión basándose en métricas preestablecidas que dan una señal de "adelante" o "no adelante" en función del impacto potencial. Esta serie de comprobaciones automáticas no solo puede evitar que se produzca una versión dañina, sino que también puede revertir una versión si detecta algún impacto.

Todos los productos y servicios implementados a través de Cloudflare deben tener un objetivo de nivel de servicio (SLO), que contiene tanto una métrica que representa el estado del producto como un objetivo por debajo del cual se consideraría que el producto no funciona correctamente.

Los SLO tienen tasas de consumo, o umbrales de fallo aceptables. Cualquier servicio medido por el estado proporcionará los SLO a un sistema automatizado como parte de la fusión de un cambio que se implementará. En cada ámbito de implementación establecido (planes gratuitos, un subconjunto de máquinas en Ashburn, etc.), el sistema automatizado:

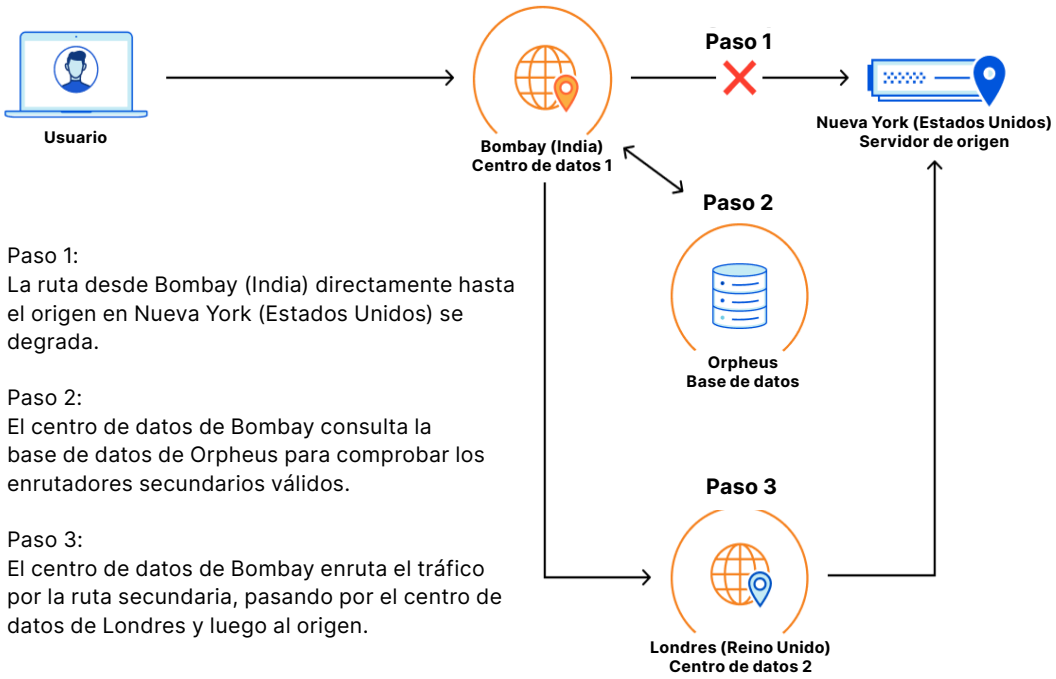
- En primer lugar, supervisará el SLO del servicio durante un periodo de tiempo determinado para asegurarse de que el estado no cae por debajo del umbral.
- Si el SLO se mantiene dentro de los rangos aceptables durante el periodo de prueba establecido, el sistema avanzará automáticamente con la implementación a una fase posterior.
- Sin embargo, si se incumple el SLO, el sistema detendrá automáticamente la implementación y realizará una reversión para mitigar automáticamente el impacto.

Estos pasos garantizan que el estado de los clientes no se vea afectado por las implementaciones de código y que la duración sea lo más breve posible.

Accesibilidad de origen

La accesibilidad de origen se refiere a la capacidad de Cloudflare para llegar a los destinos, ya sea el origen de un cliente, un sitio SaaS o la red pública de Internet a través de Cloudflare Gateway. El enrutamiento de las solicitudes a su destino es crucial para que los usuarios accedan a la red de Cloudflare. Por ejemplo, Argo Smart Routing, la herramienta de Cloudflare que optimiza el rendimiento (concretamente, el tiempo hasta el primer byte), sondea constantemente la red de Cloudflare para encontrar la ruta más rápida hasta los orígenes.

Orpheus, la contraparte de Argo, tiene una filosofía similar pero una función diferente. Orpheus existe para establecer conexiones fiables a los servidores de origen. Orpheus analiza específicamente las métricas que afectan a la capacidad de Cloudflare para llegar al origen (en contraposición a la ruta más rápida al origen), y encontrará rutas que minimicen la pérdida de paquetes sin afectar al rendimiento de estado estable. Esto significa que cuando surgen problemas, el tráfico se enruta automáticamente alrededor de los errores detectados.



Paso 1:
La ruta desde Bombay (India) directamente hasta el origen en Nueva York (Estados Unidos) se degrada.

Paso 2:
El centro de datos de Bombay consulta la base de datos de Orpheus para comprobar los enrutadores secundarios válidos.

Paso 3:
El centro de datos de Bombay enruta el tráfico por la ruta secundaria, pasando por el centro de datos de Londres y luego al origen.

Antes de que Cloudflare lanzara Orpheus en 2021, podíamos enrutar con éxito a los orígenes el 99,9 % de las veces. Tras implementar Orpheus, nuestra capacidad de enrutamiento a los orígenes aumentó al 99,99 %. El próximo año, ampliaremos Orpheus para proteger más tipos de tráfico, actuar ante más escenarios de fallo y trabajar más rápido para reducir el tiempo que los usuarios se ven afectados.

Compromiso con la transparencia operativa

Incluso las redes más resistentes e innovadoras sufrirán interrupciones. Cuando se producen incidentes y los clientes se ven afectados, Cloudflare sigue un protocolo de comunicación de incidentes que incluye una investigación exhaustiva, un informe interno del incidente, otro externo y, si es necesario, actualizaciones del estado durante todo el periodo del impacto.

En determinados casos en los que los incidentes tengan tal repercusión (o supongan una innovación), se publicarán análisis posteriores en el blog de Cloudflare.

Conclusión

El esfuerzo de ingeniería que hay detrás de la red de Cloudflare no es una tarea fácil, pero es un trabajo que realizamos con orgullo para nuestros clientes. La recompensa es crear una plataforma de red que beneficie a nuestros clientes y a la comunidad de Internet en general.

En última instancia, priorizando la resiliencia no solo como una cuestión técnica, sino como una filosofía operativa fundamental, estamos haciendo algo más que reforzar las defensas, estamos construyendo activamente una empresa que está preparada de forma inherente para el futuro. El enfoque proactivo de pruebas y adaptaciones continuas nos permite evolucionar sin problemas junto con las demandas en constante cambio tanto de nuestros clientes como del panorama dinámico de Internet.

Entendemos que muchos de los conceptos que se representan en este documento se centran en conceptos de red a los que muchas empresas no están expuestas, ya que implican la arquitectura interna del funcionamiento de un entorno de nube a nivel de operador global.

Si deseas recibir información detallada sobre la ingeniería de resiliencia de Cloudflare, ponte en contacto con tu representante de Cloudflare.

+34 518 880 290 | enterprise@cloudflare.com | Cloudflare.com/es-es/

REV:BDES-8251.28OCT2025