CIRCUNSTANCIAS

- **Fecha del reporte:** 2023-07-06
- **Fecha de inicio:** 2023-07-05 17:13
- **Fecha de detección:** 2023-07-05 17:21
- **Fecha de corrección:** 2023-07-05 18:59
- **Duración:** 116'

IMPACTO

Pérdida de servicio en el producto Location Identity Platform afectando a los clientes activos en el producto.

Las causas de la pérdida de servicio no se han debido a ningún ciberataque dirigido ni inespecífico por lo que no se ha producido brecha de seguridad alguna.

MITIGACIÓN

Se procedió a desactivar la infraestructura redundante en el cloud Azure para que las latencias entre los dos sistemas no afectaran a las instancias presentes.

También se amplió la capacidad del sistema de sincronización MQTT para aliviar el backpressure de las sincronización y garantizar la consistencia en el momento de relanzar la redundancia en Azure.

Así mismo el equipo de seguridad evaluó los sistemas de detección de intrusos para descartar cualquier interferencia adicional, tal y como está estipulado en el procedimiento de incidencias.

INCIDENCIA

A las 09:22 h de la mañana se reportó una incidencia de red en el cloud de Azure sito en Paises Bajos debido a la situación atmosférica.

El equipo de respuesta rápido identificó un aumento de las latencias de red y un mantenimiento del servicio que mostraba estar funcionando correctamente.

Los sistemas de Ironchip conmutan automáticamente cuando un cloud pierde servicio pero no están preparados para la casuística en que haya degradación de red y no caída de servicio.

El incremento de las latencias provocó una situación de backpressure en la sincronización entre los nodos MQTT de sincronización entre AWS y Azure.

Los sistemas de detección de caída identificaban ambos clouds como disponibles pero la sincronización fallida causó la indisponibilidad de los sistemas a las 17:13 horas.

Cuando se identificó el problema, se procedió a eliminar el entorno de Azure en favor del de AWS y a aumentar el tamaño de los servicios MQTT para acelerar la resolución del backpressure mitigando la incidencia.

LECCIONES APRENDIDAS

Los sistemas de detección de pérdida de servicio en la infraestructura redudante multicloud deben de tener en cuenta no sólo la pérdida de servicio si no también la degradación de la comunicación, la latencia y el backpressure en la sincronización.

En caso de latencias significativas la copia primaria debe de deshechar la secundaria para preservar correctamente el servicio e incrementar la capacidad de procesamiento de los sistemas de sincronización.

De esta forma, los sistemas siguen manteniendo la funcionalidad en caso de problemas en red y no solo en caso de pérdida de servicio como estaba contemplado hasta este momento.

SIGUIENTES PASOS

Se va a proceder a implementar un proceso automatizado capáz de medir la degradación de la conectividad de red en los entornos redundantes para deshechar el entorno degradado si uno de los entornos no es capaz de sincronizar a timempo los cambios desde el maestro.

Se va también a definir un procedimiento para los servicios de guardia de cara a verificar la información de degradado de red que proveen los suministradores de los servicios cloud para estar sobre aviso de esta casuística.