CASO DE ESTUDIO

Leap Second

ALUMNO: Adrián Bennasar Polzin.

PROFESOR: Bartolome Capó Capó.

ASIGNATURA: 21757 – GSII

CURSO: 2021-2022

La empresa es consciente de que tendrá una demanda mayor en la próxima temporada alta de Agosto y añade más servidores, por lo tanto esto es un primer punto positivo porque llevan a cabo una Gestión de la capacidad. Tras hablar de la expansión de servidores para dar contexto previo, el artículo pasa a hablar de una incidencia:

Se detecta la incidencia por primera vez a través de las alarmas que monitorizan los sistemas. Por lo tanto se trata de una empresa que utiliza Gestión de alarmas, Gestión de disponibilidad y Gestión de nivel de servicio. Gracias a la Gestión de alarmas es posible detectar fallos sin depender de que los usuarios del servicio avisen por lo tanto se puede actuar con más rapidez ante fallos.

Cuando se confirma el fallo con la Gestión de alamas inmediatamente se realiza la apertura de partes de incidencia, asignación de recursos humanos a las tareas de diagnosis, contención y resolución y el control de la información histórica.

El CAU indentifica las incidencias y las registra. En este momento se debería consultar una Knowledge Database para ver si esta incidencia ha ocurrido anteriormente y ya se sabe qué causa el problema y cuáles son las soluciones.

La empresa debe combinar la Gestión de Incidentes, Gestión de Problemas, Gestión de Cambios, Gestión de Versiones, Gestión de Configuraciones y la CMDB junto con la KB para ser capaz de solucionar problemas de manera efectiva y eficiente. La base de datos de conocimientos se podría dividir en BB.DD Errores Conocidos, BB.DD Problemas y BB.DD Incidentes.

El CAU debe intentar realizar un diagnóstico propio y si lo consigue, aplicar el guión correspondiente a ese diagnóstico. Sin embargo parece ser que no es capaz de solucionar el problema por si solo por lo tanto escala la incidencia al nivel 2º, donde los de operaciones, desarrollo y sistemas intentarán solucionarlo.

La empresa debe contar con procesos de Gestión de Incidentes y Gestión de Problemas para tener claro cómo actuar ante una situación de este tipo en lugar de improvisar.

En el 2º nivel los de sistemas hacen un diagnóstico de manera que creen que se trata de un problema de conectividad entre servidores de disponibilidad y servidores de BBDD.

Por otra parte, se llama a los de desarrollo para averiguar si se podria tratar de un problema de una versión subida recientemente del servicio de disponibilidad. Por lo tanto la empresa utiliza Gestión de cambios/versiones y Gestión de configuración.

Se calcula a estas alturas que ya se han provocado unas pérdidas del orden de los 100000 euros, por lo tanto la empresa cuenta con una Gestión de la contabilidad y mide el coste de sus servicios y el dinero que les generan estos, por lo tanto son conscientes del dinero que ganan o pierden dependiendo de la situación y pueden tomar medidas en función de esto.

La empresa debe seguir el esquema de 3 pasos de la Gestión de errores: Detección, Contención y Resolución.

Se toma una medida de contención desactivando la web temporalmente y redirigiendo a los clientes de otros paises a servidores cloud. Esto permite que el servicio continúe dentro de una determinada ventana de calidad, contenta a los usuarios y permite a los administradores concentrar todad su actividad en la diagnosis correcta y la resolución adecuada. En este caso han utilizado una medida de contención de tipo manual, sin embargo también existen de tipo automático.

Se encuentra una solución en el 3er nivel, concretamente una parte del equipo de sistemas averigua que se trata de un bug llamado leap second, a través de la investigación en la web, donde encuentran un artículo específico relacionado con el problema. En este momento deben informar al nivel 2, y el nivel 2 debe informar al CAU que se ha solucionado el problema. También se debe registrar este bug en la base de conocimiento, ya que si se ha tardado tanto tiempo en darse cuenta de que el problema consistía en esto, significa que aún no tenían registrado este bug.

Si no hubieran encontrado una solución en el nivel 3 interno en la empresa, el siguiente paso a seguir hubiera sido informar al nivel 2 igualmente, y escalar el problema al suministrador (que se clasifica dentro del nivel 3 también) y entonces seguir buscando soluciones mientras se espera a la respuesta del suministrador.

(Cabe mencionar que la división en niveles no es siempre igual en cada empresa y puede variar de muchas maneras, pero centrándome en el esquema visto en la asignatura, que pretende ilustrar una división estándar general, considero que en este caso de estudio los empleados que encuentran el bug en internet se deberían clasificar como nivel 3, separándolos del resto de empleados que aparecen en el artículo).

Han conseguido solucionar el problema en el nivel 3 dentro de la empresa, por lo tanto no ha sido necesario escalar a suministradores.

Tras resolver la incidencia, el CAU debe ejecutar el cierre de la indicencia y realizar los avisos generales correspondientes.

Imagino que los servidores no se activan inmediatamente de cara a producción para volver a dar servicio a los clientes, sino que primero se controlan durante un tiempo para comprobar que funcionan correctamente tras la resolución del problema.

Hay que destacar que en ningún momento se mencionan medidas de seguridad aplicadas en los servidores ya en uso, ni tampoco medidas de seguridad que se implementen en los nuevos servidores desplegados. La empresa debe contar con una Gestión de la seguridad de la información.

Por otra parte, quizás deberían realizar mejor la Gestión de los suministradores con el objetivo de obtener sus servicios más rápido, ya que no han tenido disponible el servicio de cloud al completo en un momento en que lo han necesitado y el hecho de no tenerlo ha provocado que los clientes usen un servicio precario.