LIBRO BLANCO | DICIEMBRE DE 2016

Elección de la correcta solución de gestión de API para los usuarios empresariales

ca technologies

La oportunidad de API

Puede que la interfaz de programación de aplicaciones (API) sea un concepto anticuado; sin embargo, se está transformando a medida que aumenta el número de organizaciones que, debido a los requisitos móviles y en la nube, hacen públicos sus activos de información a desarrolladores externos. Empresas como eBay, Expedia y Salesforce están teniendo éxito de ventas en nuevos mercados porque publican los datos a sus desarrolladores a través de las interfaces de programación de aplicaciones. Según la página ProgrammableWeb.com, la cantidad de interfaces de programación de aplicaciones que se ofrecen de forma abierta en Internet supera ya las 16 000, cuando en el año 2005 solo eran 32.[1]

La apertura de las interfaces de programación de aplicaciones a los desarrolladores externos permite que muchas empresas tecnológicas nuevas se conviertan en plataformas mediante el fomento de comunidades de desarrolladores que se vinculan a sus recursos de datos o aplicaciones más importantes. Esto se traduce en un nuevo alcance (como el rápido crecimiento de Twitter), en ingresos (como AppExchange de Salesforce.com) o en la retención de usuarios finales (como Facebook).

El uso de interfaces de programación de aplicaciones para compartir información y funcionalidades con desarrolladores externos no se limita a las empresas tecnológicas nuevas. Cada vez son más las empresas que, impulsadas por las iniciativas de integración de los partners, de los dispositivos móviles y de la nube, utilizan interfaces de programación de aplicaciones para situarse a sí mismas en el centro de un ecosistema de desarrolladores y, de este modo, fomentar nuevas posibilidades relativas al alcance, los ingresos y la retención de clientes en torno a sus activos de información. No obstante, las empresas consolidadas, a diferencia de muchas de las nuevas, deben enfocar la publicación de las interfaces de programación de aplicaciones con sumo cuidado porque es mucho lo que ponen en juego, incluidos la reputación, el cumplimiento normativo y las necesidades paralelas de clientes, partners, empleados y accionistas.

El reto empresarial de la gestión de las API

La publicación de las interfaces de programación de aplicaciones en una comunidad de desarrolladores externa, sea de un partner o pública, presenta una serie de retos y riesgos para la empresa. ¿Cómo debe proteger los activos de información que se publican frente a infracciones o ataques? ¿Cómo puede ofrecer las interfaces de programación de aplicaciones como servicios fiables sin interrupciones que puedan repercutir en los usuarios? ¿Cómo debe controlar el acceso y el uso de interfaces de programación de aplicaciones de una forma uniforme y basada en políticas? ¿Cómo puede generar ingresos con las interfaces de programación de aplicaciones? ¿Cómo puede ayudar a los desarrolladores a conocer las interfaces de programación de aplicaciones y a gestionar sus accesos de manera autónoma? A pesar de que estas preguntas son relevantes tanto para las empresas nuevas como para aquellas consolidadas, son más acentuadas y apremiantes para las organizaciones de TI de las segundas. No solo porque estas empresas consolidadas no puedan permitirse daños en la reputación que puedan ocasionarse como consecuencia de una estrategia de gestión de API precipitada, sino por los procesos de TI pensados con detenimiento y por la protección que se debe conservar.

No importa qué tipo de interfaz de programación de aplicaciones desee publicar una empresa; en cualquier caso necesitará una solución de gestión de API que pueda abordar algunas áreas funcionales básicas:

- **Seguridad de la API:** las empresas no se pueden permitir usos indebidos o infracciones de la información ni de ningún recurso de aplicación que se hayan publicado mediante una API.
- **Gestión del ciclo de vida de la API:** las empresas necesitan una forma de garantizar que las actualizaciones de la API no se dañan cuando pasan a una versión superior de esta o se trasladan por entornos, ubicaciones geográficas, centros de datos o la nube.
- **Control de la API:** las empresas necesitan una forma de controlar el carácter operativo ampliado de cómo se publican las API a distintos partners y desarrolladores, así como de realizar un seguimiento de ello, mediante características de políticas como la medición, los acuerdos de nivel de servicio, la disponibilidad y el rendimiento.
- **Flexibilidad de implementación:** las soluciones de gestión de API deberían integrarse con la infraestructura existente de la empresa.
- **Capacitación de desarrolladores y creación de una comunidad:** las empresas necesitan una forma de atraer a los desarrolladores, gestionarlos y ayudarlos a sacar el máximo partido a las interfaces de programación de aplicaciones publicadas.
- **Rentabilización de la API:** en el caso de algunas empresas, la publicación de las API no es suficiente. Las interfaces de programación de aplicaciones también representan una nueva oportunidad de generar ingresos y, además, existen distintas soluciones de gestión de API que permiten rentabilizarlas en distintos niveles.

En el caso de las empresas, la necesidad de abordar estos requisitos funcionales no admite discusión. Sin embargo, con estos requisitos funcionales, las empresas esperarán que la solución de gestión de API brinde ciertas características operativas que resulten útiles para su propia experiencia de TI.

- **Seguridad de la solución:** dado que las soluciones de gestión de API se implementan en la zona desmilitarizada (DMZ), las empresas también requerirán soluciones de API de TI sólidas que satisfagan una serie de requisitos de seguridad, desde la protección contra la infiltración hasta la conformidad con la industria de las tarjetas de pago, pasando por los Estándares Federales de Procesamiento de la Información y la compatibilidad con el módulo de seguridad de hardware para la seguridad clave de la API.
- **Capacidad de gestión de la solución:** las empresas disponen de entornos de desarrollo, pruebas y producción que se extienden por varias ubicaciones geográficas, centros de datos y nubes, lo que significa que una solución de gestión de API debe ajustarse a sus estilos y procesos de desarrollo específicos.
- **Fiabilidad de la solución:** las empresas que publican las interfaces de programación de aplicaciones de forma comercial esperan un tiempo de actividad del 99,999 %, o incluso mayor, y no pueden permitirse interrupciones. ¿Qué características presenta una solución sólida y disponible?

En este libro blanco se detallan estos distintos requisitos funcionales y operativos con el fin de que los gestores de TI, administradores web y arquitectos empresariales dispongan de la información clave para elegir una solución de gestión de API.

Requisitos funcionales de la solución de gestión de API

Seguridad de la API

Es frecuente que las funciones de seguridad resulten primordiales para los compradores potenciales que buscan una solución de gestión de API; sobre todo cuando el cliente es una empresa que desea proteger información crucial publicada mediante una API independiente de estándares como el protocolo de acceso a objetos simples (SOAP), la transferencia de estado representacional (REST) o JavaScript Object Notation (JSON). Los aspectos de seguridad de la API comienzan con el control de acceso. En el caso de las interfaces de programación de aplicaciones orientadas al exterior de la empresa, significa tener la capacidad de:

- aceptar distintos tipos de credenciales de autenticación.
- emitir distintos tipos de credenciales para los desarrolladores.
- admitir distintos esquemas de autorización de recursos, incluidos los federados como el protocolo Open Authorization (OAuth), OpenID Connect y el lenguaje de marcado para confirmaciones de seguridad (SAML).

En el caso de las empresas consolidadas, a este reto se le añade la dificultad de la integración con la infraestructura de identidades existente. Por tanto, el objetivo global de estas empresas es lograr flexibilidad e integración. La política debería aceptar distintos tipos de tókenes de acceso e incluso permitir moverse entre diferentes claves de API de desarrolladores; todo ello sin alterar el código. La solución debería admitir una amplia variedad de esquemas de Open Authorization, dado que son los estándares para la seguridad móvil y las interfaces de programación de aplicaciones. También debería gestionar distintos estilos de Open Authorization, como un código de autentificación de mensajes en clave-hash (HMAC), y combinaciones con estándares empresariales, como el lenguaje de marcado para confirmaciones de seguridad (SAML). Desde luego, la solución de gestión de API también debe funcionar con las inversiones de identidad preexistentes de empresas como CA, IBM, Oracle y RSA.

No obstante, el control de acceso no lo es todo en cuanto a seguridad de las API. Las interfaces de programación de aplicaciones abren una ventana programática a sus datos, por lo que una solución de gestión de API de tipo empresarial deberá proporcionar al arquitecto de la empresa o administrador de seguridad un exhaustivo control sobre los datos que se publican, el modo en que se mantiene la confidencialidad de la información y la forma en que su transmisión puede protegerse frente a la interceptación o la alteración.

Además, la seguridad de las API se basa en la integridad tanto de la propia API como de los datos y funcionalidades que hace públicos, lo que requiere la capacidad de garantizar que las interfaces de programación de aplicaciones no se ven comprometidas por ataques, denegaciones de servicio o usos indebidos. Una buena solución de gestión de API facilitará al operador abundantes controles de protección frente a amenazas, que garantizarán la disponibilidad y la fiabilidad de la API y de las comunicaciones que habilita.

Gestión del ciclo de vida de la API

Las interfaces de programación de aplicaciones no se crean de forma aislada. Al igual que cualquier funcionalidad de aplicaciones, estas requieren sus propios ciclos de vida de desarrollo, incluidas las fases de diseño, codificación, prueba e implementación. Ello requiere la posibilidad de realizar el seguimiento de los cambios de una API en todo el ciclo de vida del desarrollo, con independencia de si el proceso de desarrollo sigue un enfoque ágil o en cascada. Por este motivo, toda solución de gestión de API debe contar con flujos de trabajo completamente funcionales con estos fines:

- Planificación y diseño de interfaces de programación de aplicaciones con estándares del sector
- Integración y protección integrales de las interfaces de programación de aplicaciones
- Pruebas, implementación y adaptación de versiones y reversiones
- Gestión y control de la utilización de las API, incluidos informes y análisis

Una solución de gestión de API completamente funcional debería ser capaz de admitir simultáneamente varias versiones en el proceso de producción, para dar cabida a clientes más antiguos o a distintas tecnologías de acceso, como el protocolo de acceso a objetos simples (SOAP), la transferencia de estado representacional (REST) o JavaScript Object Notation (JSON). Un marco de trabajo de gestión del ciclo de vida que solo pueda albergar desarrollos localizados no logrará satisfacer las necesidades de las empresas más modernas. Tanto la nube pública como la privada están cobrando una creciente importancia. Esto significa que las empresas precisan de una solución de gestión de API que pueda abarcar las fases de prueba y producción en la nube, así como que permita aislar a los desarrolladores de estas API de las particularidades de la topología y las idiosincrasias de las redes.

Control de la API

El control es un término amplio que a menudo se emplea para reflejar una gran variedad de requisitos de gestión, de procesos y de visibilidad, y define los términos y condiciones bajo los cuales una API se publica a uno o más consumidores. Aunque la idea de control engloba los conceptos de seguridad y ciclo de vida, también articula varios requisitos de los acuerdos de nivel de servicio, de monitorización y de generación de informes. Además, en el caso de las soluciones de gestión de API, este concepto resulta relevante para el imperativo más general de habilitar términos y condiciones diferenciados con el fin de compartir datos y funcionalidades de las interfaces de programación de aplicaciones con distintos consumidores en función de sus identidades, capacidades, niveles de suscripción u otros contextos transaccionales que puedan establecerse en la política.

El control eficaz de la API gira en torno a la flexibilidad. La tecnología para controlar la forma en que se comparten las interfaces de programación de aplicaciones debería seguir las preferencias y los procesos de la empresa, y no al revés. Esto significa que la solución de gestión de API se debería poder configurar en función de cualquier tipo de acuerdo de nivel de servicio, seguridad, registro u otra clase de control que recurra a una política. La política es la clave de la flexibilidad y garantiza la coherencia de una implementación a otra. Las soluciones de gestión de API que restringen las capacidades de los administradores a la realización de controles de forma general sin un IDE de políticas completo limitan el alcance del control y el modo en que se puede controlar.

Flexibilidad de implementación

La mayoría de las empresas cuentan con una infraestructura diseñada para complementar la manera de llevar a cabo su trabajo. A medida que una empresa avanza hacia una solución de gestión de API, debería evaluar las soluciones que se conectan a su entorno existente. Los equipos responsables de la arquitectura deberían ser capaces de gestionar esta solución como una extensión de su infraestructura, en lugar de como un entorno independiente. Para obtener más información sobre este nivel de integración, lea el resumen de la solución, "An Architect's Guide for Extending Your ESB/SOA Environment to Mobile, Cloud, and IoT".

Capacitación de desarrolladores y creación de una comunidad

El control de una API le garantiza al editor de la publicación un control coherente; sin embargo, si no se da a conocer esa interfaz a los desarrolladores externos ni pueden utilizarla fácilmente, el editor se arriesga a que no se le dé el uso. Por ese motivo, las soluciones de gestión de API más modernas trascienden las funciones de control como la seguridad, el ciclo de vida y el propio control a fin de ofrecer una funcionalidad que ayude a los editores a presentar la información de sus interfaces de programación de aplicaciones a los desarrolladores externos, lo que a menudo se lleva a cabo mediante portales para desarrolladores. Este tipo de portales brindan un espacio de interacción único que permite que los desarrolladores se registren y obtengan una cuenta, soliciten una clave de acceso a la API, sepan qué interfaces se encuentran disponibles y consulten código de ejemplo.

Un portal de desarrolladores de API orientado al uso empresarial debería:

- ofrecer API móviles y fácilmente accesibles (incluso para Open Authorization y OpenID Connect).
- proporcionar informes y análisis a los operadores.
- facilitar la gestión de relaciones de la empresa.

Puesto que cada empresa llevará a cabo la publicación de las API con distintas experiencias y prioridades, un enfoque de portal de API universal no resultará más atractivo que un marco de trabajo de control, ciclo de vida y seguridad de API también único. Es por eso por lo que muchas empresas querrán estudiar la posibilidad de contar con un portal de API que se pueda descomponer. Esto podría traducirse en un portal de marca blanca que se pueda personalizar para adaptarlo a una estrategia de captación de desarrolladores en particular o en un portal de API que se pueda utilizar como componentes específicos mediante un portal empresarial de desarrolladores preexistente. De nuevo, la flexibilidad es la clave.

Rentabilización de la API

El concepto de rentabilización está relacionado con la idea de la capacitación de los desarrolladores. Mientras muchas empresas se interesarán en favorecer la adopción mediante el acceso gratuito a sus interfaces de programación de aplicaciones para dispositivos móviles y la Web; otras, en cambio, se plantearán ofrecer opciones de pago según el uso para los niveles de acceso superiores. De nuevo, nos encontramos con que no existe un único camino a la hora de abordar la cuestión de la rentabilización. Aquí se ofrecen varias opciones:

- Un modelo freemium en el que el uso hasta un determinado umbral de transmisión de datos o solicitudes de clientes sea gratuito
- Pago por niveles específicos de garantía de servicios o por trato prioritario con relación a otros usuarios que utilicen la versión gratuita
- Oferta de información o funcionalidades de mayor calidad que no se encuentren disponibles para aquellos clientes que no paguen

Con independencia del enfoque adoptado, la solución de gestión de API debería ser lo suficientemente sofisticada como para brindar flexibilidad a la empresa en cuanto al modo de establecer sus criterios de ingresos. La solución debería ser capaz de:

- capturar una variedad de estadísticas de uso para crear una base para la medición del consumo
- ofrecer prestaciones avanzadas de acuerdo de nivel de servicio y del tipo de este para permitir la jerarquización por prioridad del tráfico
- crear interfaces de programación de aplicaciones virtuales únicamente de pago que se puedan aislar para clientes que paguen, sin codificación

Requisitos operativos de la solución de gestión de API

Seguridad de la solución

Puesto que una solución de gestión de API será con frecuencia el único elemento tecnológico que separe a las API de las empresas del mundo exterior, el nivel de seguridad que la solución puede conferir será tan elevado como el de la propia solución. Si la solución se pone en riesgo, cualquier tipo de seguridad que se haya volcado en las API quedará igualmente expuesta a los riesgos. Por consiguiente, las empresas que estudian las soluciones de gestión de API deberían considerar la seguridad de la solución como un factor de vital importancia.

Estas soluciones funcionarán como intermediarias entre el mundo exterior y las interfaces de programación de aplicaciones internas, lo que significa que el rasgo más importante que se evalúa con frecuencia es si la propia solución puede quedar expuesta a algún peligro. Ello dependerá del tipo de prueba de infiltración a la que se haya sometido la solución, del grado de restricción del acceso a la solución y de si ha superado las evaluaciones de vulnerabilidad más importantes. Se deben tener en cuenta las soluciones validadas por la Security Technical Implementation Guide (STIG, Guía de implementación técnica de seguridad), la certificación Payment Card Industry Data Security Standard (PCI DSS, Estándar de seguridad de datos para la industria de las tarjetas de pago) para las soluciones que vayan a utilizar información de tarjetas de crédito, la conformidad con los Federal Information Processing Standard (FIPS, Estándares federales de procesamiento de la información) y la certificación de Common Criteria (Criterios comunes) para aquellas soluciones que requieran cumplir estándares superiores de seguridad gubernamentales.

Si se persiguen propósitos más prácticos, las empresas buscarán frecuentemente soluciones de gestión de API basadas en servidores proxy que les permitan gestionar la intermediación de las solicitudes externas a una API interna. Las puertas de enlace de API basadas en intermediarios ofrecen la ventaja de eliminar puntos internos de control y aislamiento, lo que simplifica la certificación y la administración de la seguridad, como en el caso del cortafuegos de una red. Puede que algunas también proporcionen compatibilidad con el módulo de seguridad de hardware (HSM) integrada para cifrar claves de API. Además, puesto que, en muchos casos, las claves de API constituyen la primera línea de defensa de autenticación frente a las infracciones, la protección de esas claves contra los ladrones mediante el cifrado representa una estrategia prudente.

Capacidad de gestión de la solución

A diferencia de las empresas nuevas habituales, que pueden llevar todo su sitio web de producción desde una única instancia de Amazon o desde un proveedor alojado pequeño, las empresas consolidadas suelen contar con una serie variada de entornos de desarrollo y producción, como:

- Equipos de desarrolladores distribuidos por el mundo
- Entornos de producción que se expanden por centros de datos de todo el mundo
- Sistemas de recuperación ante desastres basados en la nube

Por lo tanto, la capacidad de gestión será centralizada, sea cual sea la decisión final. Algunas de las consideraciones que tendrán prioridad respecto a otras funciones serán la forma de gestionar los clústeres de las puertas de enlace de la API, la manera de equilibrar la carga geográficamente, el modo de trabajar en un entorno de centro de datos desasistido y la manera de gestionar las cargas máximas. Una vez más, no todas las soluciones de gestión de API están diseñadas para atender a las necesidades específicas de la empresa; por ello, y antes de emprender un camino determinado, se debería tener precaución a la hora de analizar la compatibilidad de cada una de las soluciones con aspectos como la gestión de clústeres, la conmutación por error, la resistencia a las cargas, la recuperación ante desastres y otros factores de gestión operativos.

Fiabilidad de la solución

Una vez que la empresa decida poner en marcha un programa de publicación de API, se convertirá en el acto en un proveedor de servicios para los usuarios de su API, que confiarán en la empresa y esperarán una disponibilidad continua del servicio. En este sentido, las empresas otorgarán inevitablemente una importancia considerable a la fiabilidad en el momento de elegir la solución de gestión de API. La empresa buscará soluciones en las que la redundancia se encuentre incorporada y el riesgo de inactividad se haya eliminado o minimizado hasta el extremo. Las empresas que buscan soluciones de gestión de API puede que prefieran considerar aquellas que puedan:

- implementarse in situ, en la nube o mediante una solución híbrida (una puerta de enlace de API in situ y un portal de desarrolladores en la nube)
- ofrecer redundancia completa, con independencia del modelo de implementación
- integrarse en la infraestructura existente
- cumplir los requisitos de seguridad

Conclusiones

Dado que no hay dos empresas que presenten necesidades o entornos exactamente idénticos, nunca existirá una solución de gestión de API que sirva para todas. Sin embargo, todas las empresas comparten la necesidad común de disfrutar de un funcionamiento y una capacidad funcional excelentes. En la mayoría de los casos de empresas que se animan a comenzar a publicar interfaces de programación de aplicaciones de manera externa, esto se traducirá en el deseo de una solución de gestión de API flexible y basada en políticas que pueda satisfacer el riguroso nivel de producción de un proveedor de servicios de clase de tono de marcación. En el plano funcional, se requerirá una solución de gestión de API que pueda cumplir una serie de prerrequisitos de seguridad, adaptarse a los ciclos de vida de desarrollo habituales, controlarse mediante políticas, favorecer la incorporación y la capacitación de desarrolladores, y respaldar la opción de rentabilización. En el plano operativo, la solución de gestión de API debería ser segura, fiable y sencilla de gestionar.

Uso de investigación independiente para ayudarle a elegir una solución de gestión de API

Varias de las empresas analistas principales cubren la tecnología de gestión de API y publican informes en los que se comparan distribuidores para ayudar a las empresas a elegir las mejores soluciones para sus estrategias digitales. Los sitios de opiniones sobre el sector de la TI, como IT Central Station, también pueden ser una fuente de información excelente para las comparaciones de distribuidores y las reseñas de los clientes.

Para obtener copias gratuitas de los informes de comparación de distribuidores de los principales analistas y ver lo que opinan los usuarios de CA API Management, visite: **ca.com/es/products/api-management/why-ca-api-management.html**.

Contacto con CA Technologies

Estamos encantados de recibir sus preguntas y comentarios.

Para obtener más información, visite **ca.com/es/api**.

Comuníquese con CA Technologies en ca.com/es

CA Technologies (NASDAQ: CA) crea un software que impulsa la transformación de las empresas y les permite aprovechar las oportunidades que brinda la economía de las aplicaciones. El software se encuentra en el núcleo de cada empresa, sea cual sea su sector. Desde la planificación hasta la gestión y la seguridad, pasando por el desarrollo, CA colabora con empresas de todo el mundo para cambiar la forma en que vivimos, realizamos transacciones y nos comunicamos, ya sea a través de la nube pública, la nube privada, plataformas móviles y entornos de mainframe y distribuidos. Para obtener más información, visite **ca.com/es**.

1 Directorio de API de ProgrammableWeb, diciembre de 2016 www.programmableweb.com/apis/directory.

CS200-241661_1216