REPORTE OFICIAL | DICIEMBRE DE 2016

Elija la solución correcta de administración de API para el usuario empresarial

ca technologies

La oportunidad de API

La interfaz de programación de aplicaciones (API) puede ser un concepto viejo, pero está atravesando un proceso de transformación debido a que, impulsadas por requisitos móviles y de nube, más organizaciones están exponiendo sus recursos de información a desarrolladores externos. Al exponer los datos mediante API a los desarrolladores, empresas como eBay, Expedia y Salesforce logran con éxito alcanzar ventas en mercados nuevos. Según ProgrammableWeb.com, el número de API abiertas que se ofrecen públicamente por Internet excede ahora las 16 000 (de tan solo 32 en 2005)[1].

Exponer las API a desarrolladores externos permite que muchas iniciativas tecnológicas se conviertan en plataformas al promover las comunidades de desarrolladores vinculadas a los recursos de aplicaciones o los datos centrales. Esto se traduce en un nuevo alcance (piense en el crecimiento rápido de Twitter), ingresos (piense en AppExchange de Salesforce.com) o retención de usuarios finales (piense en Facebook).

El uso de API para compartir información y funcionalidades con desarrolladores externos no se limita a iniciativas tecnológicas. Más empresas, impulsadas por iniciativas móviles, de nube y de integración de socios de negocios, utilizan las API para lograr ubicarse en el centro de un ecosistema de desarrolladores y, al hacerlo, impulsar un nuevo alcance, ingresos y posibilidades de retención en torno a los activos de información. Sin embargo, a diferencia de muchas iniciativas, las empresas deben enfocarse en la publicidad de API con mucho cuidado, ya que tienen mucho en la línea, incluidas la reputación, la regulación y las necesidades simultaneas de clientes, socios, empleados y accionistas.

El reto de administración de API empresariales

Publicar las API a una comunidad de desarrolladores externos, ya sea pública o de socios de negocios, genera muchos retos y riesgos para la empresa. ¿Cómo protege los activos de información que expone contra abusos o ataques? ¿Cómo entrega las API como servicios confiables sin tiempo de inactividad que pueda generar un impacto sobre los usuarios de las API? ¿Cómo gestiona el acceso y el uso de las API de forma coherente y de acuerdo con las políticas? ¿Cómo genera ingresos a partir de las API? ¿Cómo ayuda a los desarrolladores a descubrir las API y autoadministrar su acceso? Estas preguntas relevantes para las iniciativas y las empresas por igual, son más acuciantes y urgentes para las organizaciones de TI empresarial. No solo porque las empresas no pueden permitirse el daño de la reputación que pueda surgir de una estrategia de administración de API apresurada, sino también por los amparos y procesos deliberados de TI que se deben mantener.

Sin importar qué tipo de API desean exponer, se requerirá una solución de administración de API que pueda abordar algunas áreas funcionales básicas:

- **Seguridad de API:** las empresas no pueden permitir el uso incorrecto o el abuso de la información ni de ningún recurso de aplicación expuesto por una API.
- **Administración del ciclo de vida de las API:** las empresas necesitan una manera de garantizar que las actualizaciones de las API no se interrumpan cuando actualicen las API o creen nuevas versiones de estas, o se muevan por diferentes entornos, geografías, centros de datos y la nube.
- **Gobernabilidad de las API:** mediante las características de la política, como medición, SLA, disponibilidad y desempeño, las empresas necesitan una manera de controlar y rastrear el carácter operativo más amplio de cómo las API se exponen a diferentes socios y desarrolladores.
- **Flexibilidad en la implementación:** las soluciones de administración de API se deben integrar con la infraestructura existente de la empresa.
- **Desarrollo de una comunidad y habilitación de desarrolladores:** las empresas necesitan una forma de incorporar desarrolladores, administrarlos y ayudarlos a aprovechar al máximo las API expuestas.
- **Monetización de API:** para algunas empresas, publicar API no es suficiente. Las API también representan una nueva oportunidad de ingresos y las diferentes soluciones de administración de API permiten la monetización en diferentes grados.

Para las empresas, abordar estos requisitos funcionales no es negociable. Sin embargo, junto con estos requisitos funcionales, una empresa espera que su solución de administración de API entregue ciertas características operativas relevantes a su experiencia única de TI.

- **Seguridad de soluciones:** debido a que las soluciones de administración de API se implementan en la "zona desmilitarizada" (DMZ), las empresas también necesitarán soluciones de API de nivel de TI sólidas que puedan cumplir con una gama de requisitos de seguridad, desde la protección contra la infiltración hasta el cumplimiento de las normas del sector de las tarjetas de pago (PCI), el cumplimiento del estándar de procesamiento de información federal (FIPS) y el respaldo del módulo de seguridad de hardware (HSM) para la seguridad clave de las API.
- **Capacidad de administración de soluciones:** las empresas poseen entornos de desarrollo, prueba y producción que abarcan geografías, centros de datos y nubes, lo que significa que una solución de administración de API debe adaptarse a sus procesos y estilos de desarrollo específicos.
- **Confiabilidad en la solución:** las empresas que publican API comercialmente esperan cinco nueves de disponibilidad, si no más, y no pueden admitir interrupciones. ¿Cuáles son las características de una solución sólida y disponible?

En este reporte oficial se examinan los diferentes requisitos funcionales y operativos para ofrecer a los administradores de TI, los administradores web y los arquitectos empresariales información clave para seleccionar una solución de administración de API.

Requisitos funcionales de una solución de administración de API

Seguridad de API

Para los posibles compradores que buscan una solución de administración de API, las funciones de seguridad a menudo son prioridad, en particular, cuando el comprador es una empresa que busca proteger información vital expuesta a través de una API independiente de estándares, como SOAP, REST o JSON. Las preocupaciones de seguridad de las API comienzan con el control de acceso. Para las API externas, esto significa tener la capacidad de realizar lo siguiente:

- Aceptar diferentes tipos de credenciales para la autenticación
- Emitir diversos tipos de credenciales para los desarrolladores
- Admitir diferentes esquemas de autorización de recursos, incluidos los federados, como OAuth, OpenID Connect y SAML

Para las empresas, este reto se agrava por la necesidad de integración con la infraestructura de identidades existente. Por lo tanto, el objetivo general es lograr flexibilidad e integración. En cuanto a las políticas, debe haber capacidad para admitir diferentes tipos de token de acceso e incluso para moverse de un tipo de clave de API de desarrollador a otro, sin tocar el código. La solución debe poder admitir una amplia gama de esquemas de OAuth, dado que estos son los estándares para la seguridad móvil y las API, pero también manejar una variedad de estilos de OAuth, como el código de autenticación de mensajes basado en hash (HMAC), y combinaciones con estándares empresariales, como lenguaje de marcado para confirmaciones de seguridad (SAML). Por supuesto, la solución de administración de API también necesita funcionar con inversiones de identidades preexistentes de empresas como CA, IBM, Oracle y RSA.

Sin embargo, la seguridad de las API no se limita al control del acceso. Las API proporcionan una ventana programática a sus datos, por ese motivo, una solución de administración de API de nivel empresarial necesitará ofrecer al arquitecto de la empresa o al administrador de seguridad un control detallado de qué datos se exponen, cómo se mantiene confidencial esta información y cómo se puede garantizar que no haya intercepción o alteraciones de su transmisión.

Además, la seguridad de API se basa en la integridad tanto de la API como de los datos/la funcionalidad que expone, lo que requiere una capacidad para garantizar que las API no están comprometidas por un ataque, una denegación de servicio o un mal uso. Una buena solución de administración de API equipará a su operador con una gran cantidad de controles de protección contra amenazas que asegurarán la disponibilidad y fidelidad de las API y las comunicaciones que permiten.

Administración del ciclo de vida de una API

Las API no se desarrollan en un vacío. Como cualquier funcionalidad de aplicaciones, las API demandan su propio ciclo de vida de desarrollo, desde el diseño hasta la codificación, la prueba y la implementación. Esto requiere una capacidad de rastrear cambios a una API durante el ciclo de vida del desarrollo, ya sea que el proceso de desarrollo siga una estrategia en cascada o una estrategia ágil. Es por eso que una solución de administración de API tiene que tener flujos de trabajo completamente funcionales para lo siguiente:

- Planificar y diseñar API usando los estándares del sector
- Integrar y asegurar API de manera integral
- Probar, implementar y adoptar las versiones y reversiones
- Administrar y monitorear la utilización de API, incluidos los reportes y análisis

Una solución de administración de API debe poder acomodar diversas versiones en producción simultáneamente, ya sea para adaptar viejos clientes o diferentes tecnologías de acceso, como protocolo de acceso a objetos simples (SOAP), transferencia de estado representacional (REST) y notificación de objeto de JavaScript® (JSON). Un marco de administración del ciclo de vida que solo puede dar cabida a un desarrollo localizado no cumplirá con las necesidades de las empresas más modernas. La nube, tanto la pública como la privada, está ganando importancia. Lo que significa que las empresas necesitan una solución de administración de API que pueda abarcar las pruebas y la producción en la nube, así como también la capacidad de aislar a los desarrolladores de API de los altibajos de las idiosincrasias de la red y la topología.

Gobernabilidad de las API

La gobernabilidad es un término amplio usado a menudo para capturar una amplia gama de requisitos de administración, procesos y visibilidad; además, define los términos y condiciones en virtud de los cuales una API se expone a uno o más consumidores. Si bien gobernabilidad abarca los conceptos de seguridad y ciclo de vida, también articula diversos requisitos de SLA, monitoreo y reportes. Además, en el caso de las soluciones de administración de API, la gobernabilidad es relevante para lo más imperativo que es permitir distintos términos y condiciones para el intercambio de funcionalidades y datos de API entre distintos consumidores según su identidad, capacidad, nivel de suscripción u otro contexto transaccional que se pueda definir en la política.

La gobernabilidad eficaz de las API gira en torno a la flexibilidad. La tecnología para controlar cómo las API se comparten debe seguir las preferencias y los procesos de la empresa, y no al revés. Esto significa que una solución de administración de API debe poder configurarse en torno a cualquier SLA, seguridad, registro u otro control mediante política. La política es el centro de la flexibilidad y garantiza la coherencia de una implementación a la otra. Las soluciones de administración de API que restringen a los administradores a los controles generales sin IDE de política total limitan lo que se puede gestionar y la forma en que se puede controlar.

Flexibilidad de implementación

La mayoría de las empresas tienen una infraestructura existente diseñada para complementar la manera en que hacemos negocios. A medida que las empresas se acercan a la solución de administración de API, deben evaluar las soluciones que encajan en su entorno existente. Los equipos de arquitectura deben poder administrar esta solución como una extensión de su infraestructura en lugar de como un entorno separado. Para obtener más información sobre este nivel de integración, lea el resumen sobre la solución, "La guía del arquitecto para extender su entorno ESB/SOA a móvil, nube e IoT".

Desarrollo de comunidades y habilitación de desarrolladores

Gestionar una API le asegura al publicador un control consistente, pero si los desarrolladores externos no pueden descubrir y consumir fácilmente esa API, el publicador corre el riesgo de que esta no sea utilizada. Debido a esto, las soluciones de administración de API más modernas van más allá de las características de control, como seguridad, ciclo de vida y gobernabilidad, para proporcionar una funcionalidad que ayude a los publicadores a exponer información sobre sus API a los desarrolladores externos, a menudo a través de portales de desarrolladores. Un portal de desarrolladores que proporciona un único punto de interacción permite que el desarrollador se registre en una cuenta, solicite una clave de acceso de API, descubra qué API están disponibles y vea un código de ejemplo.

Un portal de desarrolladores de API focalizado en el uso empresarial debe cumplir con lo siguiente:

- Proporcionar API móviles fácilmente consumibles (incluso para OAuth y OpenID Connect)
- Proporcionar reportes y análisis para los operadores
- Habilitar fácilmente la administración de relaciones comerciales

Dado que diferentes empresas llegan a la publicación de las API con diversas experiencias y prioridades, una estrategia de portal de API universal será no más atractiva que un marco de gobernabilidad, ciclo de vida y seguridad de API universal. Por este motivo, muchas empresas desearán considerar un portal de API divisible. Esto podría significar un portal de etiqueta blanca que podría personalizarse para adaptarse a una estrategia de participación del desarrollador particular o un portal de API que se puede consumir como componentes discretos de un portal de desarrolladores empresariales preexistente. Nuevamente, la flexibilidad es lo esencial.

Monetización de API

El concepto de monetización está relacionado con la idea de habilitación del desarrollador. Si bien muchas empresas desean promover la adopción permitiendo el acceso libre a su Web y API móviles, otras desean ofrecer opciones de pago en función del uso para niveles de acceso superiores. Nuevamente, no existe una sola manera de abordar el problema de la monetización. Algunas opciones son las siguientes:

- Un modelo “freemium” donde el uso es gratuito debajo de cierto umbral de transmisión de datos o solicitudes de clientes.
- Cobro por niveles específicos de garantía de servicios o por prioridad sobre usuarios libres.
- Oferta de información o funcionalidades superiores no disponibles para clientes que no pagan.

Independientemente de la estrategia seleccionada, la solución de administración de API debe ser lo suficientemente sofisticada para ofrecer flexibilidad empresarial en cuanto a cómo se establecen los criterios de ingresos. La solución debe poder ser capaz de lo siguiente:

- Capturar una gama de estadísticas de uso para crear una base para medir el consumo
- Proporcionar capacidades avanzadas de SLA y clase de servicio para permitir la asignación de prioridades del tráfico
- Crear API virtuales pagas únicamente que se puedan aislar para los clientes que pagan, sin codificación

Requisitos operativos de una solución de administración de API

Seguridad de soluciones

Debido a que una solución de administración de API a menudo es la única pieza de tecnología que separa las API empresariales del mundo exterior, el nivel de seguridad que la solución puede atribuir a las API será tan sólido como la seguridad de la solución misma. Si la solución se ve comprometida, cualquier seguridad otorgada a las API se verá comprometida de un modo similar. Por lo tanto, las empresas que examinan las soluciones de administración de API deben considerar la seguridad de la solución como un punto absolutamente crítico.

Estas soluciones se interpondrán como intermediarias entre el mundo exterior y las API internas, lo que significa que la primera cualidad a menudo evaluada es si la solución misma puede quedar comprometida. Esto depende de a qué tipos de pruebas de inserción se sometió la solución, qué tan restringido es el acceso a la solución y si cumplió con las evaluaciones de vulnerabilidad clave. Se deben considerar las soluciones probadas por la guía de implementación técnica para la seguridad (STIG), la certificación del estándar relativo a la seguridad de los datos del sector de las tarjetas de pago (PCI DSS) para las soluciones que pasarán información de tarjetas de crédito, el cumplimiento del estándar de procesamiento de información federal (FIPS) y la certificación de criterios comunes para soluciones que requieren el cumplimiento de estándares de seguridad de gobernabilidad superiores.

Para propósitos más prácticos, las empresas buscan soluciones de administración de API basadas en proxy para el manejo de la intermediación de solicitudes externas de una API interna. Las puertas de enlace de API basadas en intermediarios ofrecen la ventaja de puntos de inserción claros de control y aislamiento, lo que simplifica la administración y certificación de seguridad (como con los firewall de red). Algunos también pueden ofrecer soporte de módulo de seguridad de hardware (HSM) incorporado para el cifrado de claves de API. Y en muchos escenarios, las claves de API son la línea principal de defensa de autenticación contra el abuso; por consiguiente, proteger esas claves contra robo a través del cifrado es una estrategia prudente.

Capacidad de administración de soluciones

A diferencia de una empresa nueva típica, que puede ejecutar todo su sitio web de producción desde una sola instancia de Amazon o un pequeño proveedor alojado, una empresa generalmente tiene entornos de desarrollo y producción variados, tales como:

- Equipos de desarrolladores distribuidos geográficamente
- Entornos de producción que abarcan centros de datos globales
- Sistemas de recuperación de desastres basados en la nube

Por lo tanto, la capacidad de administración será central para cualquier decisión de selección. Las consideraciones como la forma de administrar clústeres de puertas de enlace de API, la forma de equilibrar la carga geográficamente, la manera de operar en un entorno de centro de datos y la manera de manejar cargas altas serán prioridad ante otras características. Nuevamente, no todas las soluciones de administración de API están diseñadas para satisfacer las necesidades específicas de la empresa, de modo que, antes de embarcarse en un camino particular, se debe tener cuidado al evaluar cómo las diversas soluciones admiten la administración de clústeres, la conmutación por error, el exceso de carga, la recuperación de desastres y otros factores de administración operativa.

Confiabilidad de la solución

Una vez que la empresa decide embarcarse en un programa de publicación de API, se convertirá efectivamente en un proveedor de servicios para sus consumidores de API quienes van a confiar en la empresa y esperan una disponibilidad continua. En este contexto e inevitablemente, una empresa tendrá una consideración particular por la confiabilidad al seleccionar la solución de administración de API. La empresa buscará soluciones donde se genera una redundancia y el riesgo de tiempo de inactividad se haya minimizado extremadamente o eliminado. Las empresas que buscan soluciones de administración de API deben considerar solo aquellas soluciones que pueden:

- Implementarse en instalaciones, en la nube o mediante una solución híbrida (puertas de enlace de API en las instalaciones, portal de desarrolladores en la nube)
- Proporcionar redundancia completa, independientemente del modelo de implementación
- Integrarse con su infraestructura existente
- Cumplir con los mandatos de seguridad

Conclusiones

Como no hay dos empresas con las mismas necesidades o el mismo entorno, nunca habrá una solución de administración de API con un tamaño que sirva para todas las empresas. Sin embargo, todas las empresas comparten una necesidad en común de excelencia en la operación y capacidad funcional. Para la mayoría de las organizaciones que intentan comenzar a publicar API externamente, esto se traduce en un deseo de una solución de administración de API flexible impulsada por políticas que pueda cumplir con el rigor de producción de un proveedor de servicio de clase de tono de marcación. Funcionalmente, se requiere una solución de administración de API que pueda cumplir con una variedad de requisitos previos de seguridad, adoptar ciclos de vida de desarrollo comunes, ser gobernable a través de políticas, permitir la incorporación de desarrolladores, promover la participación de desarrolladores y admitir la opción de monetización. Operativamente, la solución de administración de API debe ser segura, administrable y confiable.

Use la investigación independiente como ayuda para elegir una solución de administración de API

Varias de las principales firmas de análisis cubren la tecnología de administración de API y publican reportes que comparan los proveedores para ayudar a las empresas a elegir las mejores soluciones para sus estrategias digitales. Los sitios de revisión de TI, como la Estación central de TI, también pueden ser una excelente fuente de información para la comparación de proveedores y las revisiones de clientes.

Para obtener copias complementarias de los reportes de comparación de los principales proveedores analistas y ver qué están diciendo los clientes sobre CA API Management, visite: **ca.com/us/products/api-management/why-ca-api-management.html**.

Contáctese con CA Technologies

Recibimos cualquier pregunta, comentario y opinión general.

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

ca technologies

Comuníquese con CA Technologies en ca.com/ar

CA Technologies (NASDAQ: CA) crea un software que impulsa la transformación en las empresas y les permite aprovechar las oportunidades de la economía de la aplicación. El software es el centro de cada empresa, en cada sector. Desde la planificación hasta el desarrollo, pasando por la administración y la seguridad, CA trabaja con empresas en todo el mundo para cambiar el estilo de vida y la forma de realizar transacciones y comunicarse, mediante entornos móviles, de nubes públicas y privadas, de mainframe y distribuidos. Obtenga más información en **ca.com/ar**.

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