DOCUMENTAÇÃO TÉCNICA | DEZEMBRO DE 2016

Escolhendo a solução certa de gerenciamento de APIs para o usuário corporativo

ca technologies

A oportunidade da API

A API (Application Programming Interface - Interface de Programação de Aplicativos) pode ser um conceito antigo, mas está passando por uma transformação à medida que um número cada vez maior de organizações, orientadas por requisitos de dispositivos móveis e da nuvem, está abrindo seus ativos de informações para desenvolvedores externos. Ao expor os dados a seus desenvolvedores por meio das APIs, empresas como eBay, Expedia e Salesforce estão obtendo sucesso com as vendas em novos mercados. De acordo com o ProgrammableWeb.com, o número de APIs abertas que são oferecidas publicamente pela internet já ultrapassa 16.000; em 2005, eram apenas 32[1].

Abrir as APIs para os desenvolvedores externos permite que muitas startups de tecnologia se tornem plataformas, fomentando comunidades de desenvolvedores vinculadas a seus principais recursos de dados ou aplicativos. Isso se converte em novo alcance (pense no rápido crescimento do Twitter), em receita (pense no AppExchange da Salesforce.com) ou em retenção do usuário final (pense no Facebook).

O uso de APIs para compartilhar informações e funcionalidades com desenvolvedores externos não se limita às startups de tecnologia. Um número maior de empresas, orientadas pelas iniciativas de nuvem, dispositivo móvel e integração de parceiros, está usando APIs para se posicionar no centro de um ecossistema de desenvolvedores e, ao fazer isso, está impulsionando novas possibilidades de alcance, receita e retenção em torno de seus ativos de informações. No entanto, diferentemente de muitas startups, as empresas devem abordar a publicação de APIs com muito cuidado, pois há muita coisa em jogo, incluindo a reputação, a regulamentação e as necessidades simultâneas de clientes, parceiros, funcionários e acionistas.

O desafio do gerenciamento de APIs corporativas

A publicação de APIs em uma comunidade de desenvolvedores externos, seja pública ou de parceiros, traz vários desafios e riscos para a empresa. Como você protege os ativos de informações que está expondo contra abusos ou ataques? Como você fornece suas APIs como serviços confiáveis e sem o downtime que pode afetar os usuários das APIs? Como você controla o acesso e o uso de suas APIs de maneira consistente e orientada a diretivas? Como as APIs trazem lucros para você? Como você ajuda os desenvolvedores a detectar suas APIs e autogerenciar seu acesso? Essas perguntas, igualmente relevantes para startups e empresas, são mais críticas e urgentes para organizações de TI corporativas. Não somente porque as empresas não podem se arriscar com os danos à reputação que podem resultar de uma estratégia precipitada de gerenciamento de APIs, mas também devido às salvaguardas e aos processos de TI deliberados que precisam ser mantidos.

Mas não importa que tipo de API uma empresa deseja expor, ela precisará de uma solução de gerenciamento de APIs que possa atender a algumas áreas funcionais básicas:

- **Segurança das APIs** — as empresas não podem arcar com o uso incorreto ou o abuso de suas informações, nem com a exposição de algum recurso de aplicativo por uma API.
- **Gerenciamento do ciclo de vida das APIs** — as empresas precisam de uma forma de garantir que as atualizações das APIs não sejam interrompidas quando elas forem atualizadas/mudarem de versão ou forem movidas entre ambientes, locais geográficos, datacenters e para a nuvem.
- **Governança das APIs** — por meio de características de diretiva, como medição, SLAs, disponibilidade e desempenho, as empresas precisam de uma forma de controlar e rastrear a natureza operacional mais ampla de como as APIs são expostas a diferentes parceiros e desenvolvedores.
- **Flexibilidade de implantação** — as soluções de gerenciamento de APIs devem integrar-se à infraestrutura que já existe na empresa.
- **Capacitação de desenvolvedores e criação de comunidades** — as empresas precisam de uma forma de integrar os desenvolvedores, gerenciá-los e auxiliá-los no máximo aproveitamento das APIs expostas.
- **Monetização de APIs** — para algumas empresas, publicar APIs não é o suficiente. As APIs também representam uma nova oportunidade de receita, e as diferentes soluções de gerenciamento de APIs possibilitam a monetização em níveis diferentes.

Para as empresas, atender a esses requisitos funcionais não é algo negociável. No entanto, em conjunto com esses requisitos funcionais, uma empresa espera que sua solução de gerenciamento de APIs apresente determinadas características operacionais que sejam relevantes para sua experiência exclusiva de TI.

- **Segurança da solução** — uma vez que as soluções de gerenciamento de APIs são implantadas na "DMZ (Demilitarized Zone - Zona Desmilitarizada)", as empresas também precisarão de soluções de APIs robustas de nível de TI que possam atender a vários requisitos de segurança, incluindo proteção de penetração, conformidade com o PCI e suporte à FIPS e ao HSM para segurança de chaves de APIs.
- **Capacidade de gerenciamento da solução** — as empresas têm ambientes de desenvolvimento, teste e produção que englobam locais geográficos, datacenters e nuvens, o que significa que uma solução de gerenciamento de APIs deve se ajustar a processos e estilos de desenvolvimento específicos.
- **Confiabilidade da solução** — as empresas que publicam APIs comercialmente esperam que o tempo de atividade seja de 99,999% ou até maior e não podem arcar com interrupções. Quais são as características de uma solução robusta e disponível?

Esta documentação técnica examina esses diferentes requisitos funcionais e operacionais, de modo a fornecer aos gerentes de TI, gerentes da web e arquitetos corporativos informações importantes para a escolha de uma solução de gerenciamento de APIs.

Requisitos funcionais da solução de gerenciamento de APIs

Segurança das APIs

Para os compradores em potencial que estão em busca de uma solução de gerenciamento de APIs, os recursos de segurança muitas vezes são uma prioridade, principalmente quando o comprador é uma empresa que pretende proteger informações vitais expostas por meio de uma API independente de padrões, como SOAP, REST ou JSON. As preocupações com a segurança da API começam com o controle de acesso. Para APIs voltadas aos usuários externos, isso significa ter a capacidade de:

- Aceitar diferentes tipos de credenciais para autenticação
- Emitir diferentes tipos de credenciais para desenvolvedores
- Oferecer suporte a diferentes esquemas de autorização de recursos, incluindo os federados, como OAuth, OpenID Connect e SAML

Para as empresas, esse desafio inclui a necessidade de integrar-se à infraestrutura de identidades existente. Portanto, a meta dominante é atingir flexibilidade e integração. Na diretiva, deve haver uma capacidade de oferecer suporte a diferentes tipos de tokens de acesso e, até mesmo, passar de um tipo de chave de API de desenvolvedor para outro, sem modificar códigos. A solução deve ser capaz de oferecer suporte a uma ampla gama de esquemas OAuth, já que esses são os padrões das APIs e da segurança móvel, e também de lidar com uma variedade de estilos OAuth, como HMAC (Hash-based Message Authentication Code) e de combinações com padrões corporativos, como a SAML (Security Assertion Markup Language). Obviamente, a solução de gerenciamento de APIs também precisa trabalhar com investimentos em identidade preexistentes de empresas como CA, IBM, Oracle e RSA.

No entanto, a segurança das APIs não se restringe ao controle de acesso. As APIs fornecem a janela programática de seus dados, motivo pelo qual uma solução de gerenciamento de APIs de nível corporativo precisará fornecer ao arquiteto corporativo ou administrador de segurança controle refinado sobre quais dados serão expostos, como essas informações serão mantidas em sigilo e como sua transmissão pode ser assegurada contra interceptação ou falsificação.

Além disso, a segurança das APIs se baseia na integridade da API e nos dados/na funcionalidade que ela expõe, o que exige a capacidade de garantir que as APIs não sejam comprometidas por ataques, negações de serviço ou uso incorreto. Uma boa solução de gerenciamento de APIs fornecerá a seu operador vários controles de proteção contra ameaças que garantirão a disponibilidade e a fidelidade da API e das comunicações que ela possibilita.

Gerenciamento do ciclo de vida das APIs

As APIs não são criadas de maneira isolada. Como qualquer funcionalidade de aplicativo, as APIs demandam seu próprio ciclo de vida de desenvolvimento, do design à codificação e do teste à implantação. Isso exige a capacidade de rastrear as alterações em uma API no ciclo de vida do desenvolvimento, não importando se o processo de desenvolvimento segue uma abordagem ágil ou em cascata. Por esse motivo, qualquer solução de gerenciamento de APIs precisará ter fluxos de trabalho totalmente funcionais para:

- Planejar e projetar APIs usando padrões do setor
- Integrar e proteger APIs de ponta a ponta
- Testar, implantar e acomodar controle de versão e reversões
- Gerenciar e monitorar a utilização das APIs, incluindo relatórios e análises

Uma solução de gerenciamento de APIs totalmente funcional também deve ser capaz de acomodar várias versões em produção simultaneamente, seja para acomodar clientes antigos ou diferentes tecnologias de acesso, como SOAP (Simple Object Access Protocol), REST (Representational State Transfer) e JSON (JavaScript® Object Notification). Uma estrutura de gerenciamento de ciclo de vida que pode apenas acomodar o desenvolvimento localizado não atenderá às necessidades da maioria das empresas modernas. A importância da nuvem, pública e privada, está aumentando. Isso significa que as empresas precisam de uma solução de gerenciamento de APIs que possa estender os testes e a produção para a nuvem e isolar os desenvolvedores de APIs dos imprevistos de idiossincrasias e topologias de rede.

Governança das APIs

Governança é um termo amplo frequentemente usado para capturar uma ampla gama de requisitos de gerenciamento, processo e visibilidade e define os termos e as condições sob os quais uma API é exposta a um ou mais consumidores. Embora a governança inclua conceitos de segurança e ciclo de vida, ela também articula vários requisitos de SLA, monitoramento e geração de relatórios. Além disso, no caso de soluções de gerenciamento de APIs, a governança é relevante para o imperativo mais amplo de permitir termos e condições diferenciados para compartilhamento de funcionalidade e dados de APIs com diferentes consumidores, com base na respectiva identidade, na capacidade, no nível de assinatura ou em outro contexto transacional que possa ser definido na diretiva.

Flexibilidade é o que torna a governança das APIs eficaz. A tecnologia para controlar como as APIs são compartilhadas deve seguir as preferências e os processos da empresa, não o contrário. Isso significa que uma solução de gerenciamento de APIs deve ser configurável para qualquer SLA, segurança, log ou outro controle que use diretivas. A diretiva é a parte essencial da flexibilidade e garante consistência de uma implementação para outra. As soluções de gerenciamento de APIs que restringem os administradores a controles não muito refinados sem um IDE de diretiva completa limitam o que pode ser controlado e como isso pode ser feito.

Flexibilidade de implantação

A maioria das empresas conta com uma infraestrutura existente projetada para complementar o modo como elas fazem negócios. À medida que a empresa passa a usar uma solução de gerenciamento de APIs, ela deve avaliar as soluções que se integram ao ambiente existente. As equipes de arquitetura devem conseguir gerenciar essa solução como uma extensão de sua infraestrutura, não como um ambiente separado. Para obter mais informações sobre esse nível de integração, leia o resumo da solução: "An Architect's Guide for Extending Your ESB/SOA Environment to Mobile, Cloud, and IoT".

Capacitação de desenvolvedores e criação de comunidades

Controlar uma API garante controle consistente para o editor, mas, se essa API não puder ser facilmente detectada e consumida por desenvolvedores externos, o editor correrá o risco de ela não ser utilizada. Por esse motivo, a maioria das soluções de gerenciamento de APIs modernas vai além dos recursos de controle, como segurança, ciclo de vida e governança, para fornecer funcionalidades que ajudem os editores a expor informações sobre suas APIs a desenvolvedores externos — muitas vezes por meio de portais de desenvolvedores. Fornecendo um único ponto de interação, um portal de desenvolvedores permite que um desenvolvedor se registre usando uma conta, solicite uma chave de acesso de API, detecte quais APIs estão disponíveis e veja exemplos de código.

Um portal de desenvolvedores de APIs com foco no uso corporativo deve:

- Fornecer APIs móveis que possam ser facilmente consumidas (inclusive para OAuth e OpenID Connect)
- Fornecer análise e geração de relatórios para os operadores
- Possibilitar o gerenciamento simples das relações com o negócio

Uma vez que diferentes empresas chegarão à publicação de APIs com diferentes experiências e prioridades, uma abordagem genérica de portal de APIs não será mais atrativa do que uma estrutura genérica de segurança, ciclo de vida e governança de APIs. Esse é o motivo pelo qual muitas empresas talvez considerem um portal de APIs decomponível. Isso pode significar um portal terceirizado que possa ser personalizado para se adequar a uma determinada estratégia de envolvimento de desenvolvedores ou um portal de APIs que possa ser consumido como um componente distinto por um portal corporativo de desenvolvedores preexistente. Novamente, flexibilidade é o lema.

Monetização de APIs

O conceito de monetização está relacionado à ideia de capacitação do desenvolvedor. Embora muitas empresas queiram incentivar a adoção permitindo acesso gratuito a suas APIs móveis e da web, outras desejarão oferecer opções de pagamento conforme o uso para camadas mais altas de acesso. Como já foi dito, não há uma única maneira correta de abordar o problema da monetização. Algumas opções são:

- Utilizar um modelo "freemium" em que o uso abaixo de um determinado limite de transmissão de dados ou solicitações de cliente seja gratuito
- Cobrar por níveis específicos de garantia de serviço ou por prioridade sobre usuários gratuitos
- Oferecer informações premium ou funcionalidades não disponíveis a clientes não pagantes

Independentemente da abordagem escolhida, a solução de gerenciamento de APIs deve ser sofisticada o suficiente para proporcionar a uma empresa a flexibilidade no modo como ela define seus critérios de receita. A solução deve ser capaz de:

- Capturar uma ampla variedade de estatísticas de uso a fim de criar uma base para medição de consumo
- Fornecer recursos avançados de SLA e classe de serviço, permitindo priorização do tráfego
- Compor APIs virtuais disponibilizadas apenas mediante pagamento, que possam ser isoladas para clientes pagantes, sem codificação

Requisitos operacionais da solução de gerenciamento de APIs

Segurança da solução

Uma vez que a solução de gerenciamento de APIs muitas vezes será a única parte da tecnologia que separa APIs corporativas do mundo exterior, o nível de segurança que a solução pode conferir às APIs será tão forte quanto a segurança da solução em si. Se a solução for comprometida, qualquer segurança gerada nas APIs será comprometida de maneira semelhante. Portanto, as empresas que estão avaliando as soluções de gerenciamento de APIs devem tornar a segurança da solução uma questão da máxima importância.

Essas soluções atuarão como intermediárias entre o mundo exterior e as APIs internas. Isso significa que a primeira qualidade muitas vezes avaliada é se a solução em si será comprometida. Isso dependerá do tipo de teste de penetração pelo qual a solução passará, de quão restrito é o acesso à solução e se ela atendeu às principais avaliações de vulnerabilidade. É necessário considerar as soluções testadas pelo STIG (Security Technical Implementation Guide), a certificação PCI DSS (Payment Card Industry Data Security Standard) para soluções que passarão informações de cartão de crédito, a conformidade com o FIPS (Federal Information Processing Standard) e a certificação Common Criteria para soluções que precisam atender aos padrões mais elevados de segurança do governo.

Para a maioria das finalidades práticas, muitas vezes, as empresas buscarão soluções de gerenciamento de APIs que se baseiem em proxy para lidar com a intermediação de solicitações externas para uma API interna. Os gateways de APIs com base em intermediário oferecem a vantagem de pontos claros de controle e isolamento em linha, simplificando a certificação e administração da segurança (como acontece com os firewalls de rede). Alguns também podem oferecer suporte ao HSM (Hardware Security Module) integrado para criptografia de chaves de APIs. Em muitas situações, as chaves de APIs são a principal linha de defesa de autenticação contra abusos, portanto, proteger essas chaves contra roubo por meio de criptografia é uma estratégia prudente.

Capacidade de gerenciamento da solução

Diferentemente de uma startup comum, que pode executar todo seu site de produção em uma única instância do Amazon ou em um provedor hospedado de pequeno porte, uma empresa normalmente terá ambientes de desenvolvimento e produção variados, tais como:

- Equipes de desenvolvedores distribuídas geograficamente
- Ambientes de produção que abrangem datacenters globais
- Sistemas de recuperação de falhas com base na nuvem

Portanto, a capacidade de gerenciamento será o ponto central de qualquer escolha. Considerações do tipo: como você gerencia clusters de gateways de APIs, como você equilibra a carga geograficamente, como você opera em um ambiente de datacenter que é desligado e como você lida com picos de carga terão prioridade sobre outros recursos. Mais uma vez, nem todas as soluções de gerenciamento de APIs são projetadas para atender às necessidades específicas da empresa. Sendo assim, antes de seguir por um determinado caminho, é preciso ter cuidado para avaliar como as várias soluções oferecem suporte ao gerenciamento de clusters, à tolerância a falhas, ao estouro de cargas, à recuperação de falhas e a outros fatores de gerenciamento operacional.

Confiabilidade da solução

Depois que uma empresa decidir embarcar em um programa de publicação de APIs, ela efetivamente se tornará um provedor de serviços para seus consumidores de APIs, que passarão a depender da empresa e esperarão que o tempo de atividade seja contínuo. Nesse contexto, inevitavelmente, uma empresa depositará uma importância considerável na confiabilidade ao selecionar sua solução de gerenciamento de APIs. A empresa buscará soluções em que a redundância seja integrada e o risco de downtime tenha sido extremamente minimizado ou até mesmo eliminado. As empresas que estão em busca de soluções de gerenciamento de APIs talvez considerem apenas aquelas que possam:

- Ser implantadas no local, na nuvem ou por meio de uma solução híbrida (gateway de APIs no local, portal de desenvolvedores na nuvem)
- Fornecer redundância completa, independentemente do modelo de implantação
- Integrar-se à infraestrutura existente
- Atender às exigências de segurança

Conclusões

Como duas empresas não têm exatamente as mesmas necessidades ou o mesmo ambiente, nunca haverá uma solução genérica de gerenciamento de APIs. No entanto, todas as empresas compartilham uma necessidade comum de excelência na operação e na capacidade funcional. Para a maioria das organizações que estão tentando iniciar a publicação de APIs externamente, isso se converterá no desejo de uma solução de gerenciamento de APIs flexível e orientada a diretivas que possa atender ao rigor da produção de um provedor de serviços de alto nível. Em termos funcionais, isso exigirá uma solução de gerenciamento de APIs que possa atender a uma variedade de pré-requisitos de segurança, acomodar ciclos de vida comuns de desenvolvimento, ser controlável por meio de diretivas, permitir a integração de desenvolvedores, estimular o envolvimento dos desenvolvedores e oferecer suporte à opção de monetização. Em termos operacionais, a solução de gerenciamento de APIs deverá ser segura, gerenciável e confiável.

Use pesquisas independentes para ajudá-lo a escolher a solução de gerenciamento de APIs

Grande parte das principais empresas analistas aborda a tecnologia de gerenciamento de APIs e publica relatórios que comparam fornecedores a fim de ajudar as empresas na escolha das melhores soluções para suas estratégias digitais. Sites de avaliação de TI, como o IT Central Station, também podem ser uma excelente fonte de informações para comparações de fornecedores e avaliações de clientes.

Para obter cópias gratuitas dos relatórios de comparação de fornecedores dos principais analistas e saber o que os clientes estão dizendo sobre o CA API Management, visite: **ca.com/us/products/api-management/why-ca-api-management.html**.

Entre em contato com a CA Technologies

Gostaríamos de receber suas dúvidas, seus comentários e seu feedback geral.

Para obter mais informações, visite **ca.com/api**.

Conecte-se à CA Technologies em ca.com/br

A CA Technologies (NASDAQ: CA) cria software que acelera a transformação das empresas e permite que elas aproveitem as oportunidades da economia dos aplicativos. O software está no cerne de todas as empresas, em todos os setores. Do planejamento ao desenvolvimento e do gerenciamento à segurança, a CA está trabalhando com empresas de todo o mundo para mudar a maneira como vivemos, fazemos negócios e nos comunicamos – usando dispositivos móveis, as nuvens privada e pública e os ambientes distribuídos e de mainframe. Obtenha mais informações em **ca.com/br**.

1 Diretório de APIs da ProgrammableWeb, dezembro de 2016, www.programmableweb.com/apis/directory

CS200-241661_1216