LIVRE BLANC | DÉCEMBRE 2016

Choisir la solution de gestion des API adéquate pour l'utilisateur en entreprise

ca technologies

Les API : une opportunité

Le concept d'API (interface de programmation d'applications) n'est certes pas neuf, mais il est actuellement en pleine mutation : poussées par les exigences de la mobilité et du Cloud, de plus en plus d'entreprises ouvrent en effet leurs ressources informatiques aux développeurs externes. En exposant leurs données aux développeurs via les API, des sociétés comme eBay, Expedia et Salesforce réalisent d'excellentes ventes sur de nouveaux marchés. D'après le site ProgrammableWeb.com, le nombre d'API ouvertes proposées publiquement sur Internet dépasse à présent les 16 000, contre seulement 32 en 2005[1].

L'ouverture d'API aux développeurs externes permet à un grand nombre de start-up technologiques de se convertir en plates-formes, car elle donne naissance à des communautés de développeurs liées à leurs données fondamentales ou à leurs ressources d'applications. Cela se traduit par une explosion de l'audience (il suffit de penser à la croissance exceptionnelle de Twitter), une progression des revenus (le meilleur exemple étant sans doute la plate-forme AppExchange de Salesforce.com) ou une fidélisation des utilisateurs (Facebook).

Il n'y a toutefois pas que les start-up technologiques qui ont recours aux API pour partager des informations et des fonctionnalités avec les développeurs externes : de plus en plus d'entreprises, poussées par les avancées du Cloud et des technologies mobiles, ainsi que les projets d'intégration avec leurs partenaires, les mettent à profit pour se positionner au centre d'un écosystème de développeurs et, ce faisant, conférer à leurs ressources informatiques la possibilité de toucher un plus large public, accroître leurs revenus ou fidéliser leurs utilisateurs. Cependant, contrairement à beaucoup de start-up, les entreprises classiques doivent aborder avec une grande prudence la publication des API, car elles risquent gros, que ce soit pour leur réputation ou en matière de réglementation et de gestion des besoins simultanés de leurs clients, partenaires, employés et actionnaires.

Bien gérer ses API : le défi des entreprises

Publier ses API auprès d'une communauté de développeurs externes, qu'il s'agisse de partenaires ou du grand public, fait apparaître une série de défis et de risques pour l'entreprise. Comment protéger des abus ou des attaques les informations que vous exposez ? Comment faire de vos API des services fiables sans risque d'interruption susceptible d'affecter les utilisateurs ? Comment réglementer l'accès aux API et leur utilisation de manière cohérente et conforme aux règles définies ? Comment gagner de l'argent grâce à vos API ? Comment aider les développeurs à les découvrir et à gérer eux-mêmes leurs accès ? Si ces questions sont pertinentes aussi bien pour les start-up que pour les grandes entreprises, elles sont considérablement plus pressantes pour les organisations IT de ces dernières. Et pas seulement parce que les entreprises ne peuvent pas se permettre les atteintes à leur réputation que ne manquerait pas de causer une stratégie de gestion des API bâclée, mais également du fait de garde-fous et de processus IT à préserver.

Quel que soit le type d'API qu'une entreprise souhaite exposer, elle devra adopter une solution de gestion des API capable de prendre en charge certaines fonctions de base :

- **Sécurité des API :** les entreprises ne peuvent pas tolérer le moindre emploi abusif de leurs données ou des ressources applicatives qu'elles exposent.
- **Gestion du cycle de vie des API :** les entreprises doivent pouvoir faire en sorte que leurs API restent fonctionnelles en dépit des mises à niveau et changements de version, d'environnement, de région, de data center ou de service Cloud.
- **Gouvernance des API :** par le biais des caractéristiques de règle telles que les mesures, les accords sur les niveaux de service (SLA), la disponibilité et les performances, les entreprises recherchent un moyen de contrôler et de suivre selon une vaste perspective opérationnelle la façon dont les API sont exposées aux différents partenaires et développeurs.
- **Flexibilité du déploiement :** les solutions de gestion des API doivent s'intégrer aux infrastructures existantes de l'entreprise.
- **Outils pour développeurs et mise en place d'une communauté :** les entreprises ont besoin d'un moyen d'attirer les développeurs, de les gérer et de les aider à tirer le meilleur parti possible des API exposées.
- **Monétisation des API :** pour certaines entreprises, publier des API ne suffit pas. Les API constituent également une source potentielle de nouveaux revenus, et les différentes solutions de gestion des API en permettent la monétisation à différents degrés.

Pour les entreprises, ces exigences fonctionnelles constituent le strict minimum. Au-delà de celles-ci, elles s'attendent généralement à ce que leur solution de gestion des API dispose de certaines caractéristiques opérationnelles en phase avec leurs besoins informatiques propres.

- **Sécurisation de la solution :** les solutions de gestion des API étant déployées en zone démilitarisée (DMZ), les entreprises ont besoin qu'elles soient robustes et capables de répondre à toute une série d'exigences de sécurité, de la protection contre la pénétration à la conformité PCI en passant par la prise en charge des normes FIPS ou encore celle des modules HSM pour la sécurisation des clés d'API.
- **Facilité de gestion de la solution :** les entreprises actuelles possèdent des environnements de développement, de test et de production qui s'étendent sur des zones géographiques, des data centers et des Clouds distincts, avec pour conséquence que la solution de gestion des API doit impérativement s'adapter à leurs processus et styles de développement spécifiques.
- **Fiabilité de la solution :** les entreprises qui publient des API commercialement exigent une disponibilité de « cinq neuf » (99,999 %), voire supérieure, et ne peuvent pas se permettre des interruptions de service. Quelles sont les caractéristiques d'une solution robuste et à haute disponibilité ?

Ce livre blanc passe en revue les exigences fonctionnelles et opérationnelles précitées afin de proposer aux responsables informatiques, aux administrateurs Web et aux architectes d'entreprise les informations essentielles dont ils ont besoin pour choisir en toute connaissance de cause une solution de gestion des API adaptée.

Exigences fonctionnelles relatives aux solutions de gestion des API

Sécurité des API

Lorsqu'un acheteur potentiel recherche une solution de gestion des API, les fonctions ayant trait à la sécurité constituent souvent la préoccupation numéro un, en particulier dans le cas des entreprises désireuses de protéger des informations vitales exposées via une API indépendante de normes telles que SOAP, REST ou JSON. La sécurité des API commence par le contrôle des accès. Pour les API exposées à l'extérieur, cela suppose les possibilités suivantes :

- Acceptation de différents types d'information d'identification pour l'authentification
- Octroi de différents types d'information d'identification aux développeurs
- Prise en charge de différents modèles d'autorisation des ressources, y compris des modèles fédérés tels qu'OAuth, OpenID Connect et SAML

Pour les entreprises, ce défi est encore compliqué par la nécessité d'intégrer la solution choisie à l'infrastructure existante en matière d'identification. L'objectif global est donc d'allier flexibilité et intégration. Idéalement, il devrait être possible de prendre en charge différents type de jetons d'accès et même de passer d'un type de clé d'API pour développeurs à l'autre sans qu'il soit nécessaire de toucher au code. La solution sélectionnée doit être à même de gérer une grande diversité de modèles OAuth étant donné l'importance croissante de cette norme dans le domaine des API et de la sécurité mobile, mais également différents styles d'authentification OAuth tels qu'un code d'authentification de message haché (HMAC) ou les systèmes combinés à des normes telles que le langage SAML (Security Assertion Markup Language). Bien entendu, la solution de gestion des API doit également fonctionner avec les investissements déjà consentis par l'entreprise en matière d'identification, notamment auprès de fournisseurs tels qu'Oracle, IBM, CA Technologies ou RSA.

La sécurité des API ne s'arrête toutefois pas au contrôle des accès. Les API jouent le rôle d'une fenêtre de programmation sur vos données, raison pour laquelle toute solution de gestion d'API pour entreprise digne de ce nom doit offrir aux architectes d'entreprise ou aux administrateurs de sécurité un contrôle précis sur le choix des données exposées, sur la manière dont leur confidentialité est préservée et sur leur protection contre l'interception ou la falsification lors de leur transmission.

En outre, la sécurité des API repose à la fois sur l'intégrité de l'API elle-même et sur celle de la fonctionnalité/des données que celle-ci expose, imposant aux entreprises de garantir que les API ne sont pas la cible d'attaques, de déni de service ou d'utilisation abusive. Une solution de gestion des API de qualité doit offrir à son administrateur toutes sortes de possibilités de protection contre les menaces et assurer la disponibilité et la fiabilité des API et des communications qu'elles autorisent.

Gestion du cycle de vie des API

Les API ne fonctionnent pas en vase clos : comme toute autre fonctionnalité applicative, elles ont leur propre cycle de développement, allant de la conception au déploiement en passant par l'écriture du code et les tests. Il est donc nécessaire de pouvoir assurer le suivi des modifications tout au long de ce cycle de développement, que celui-ci se fasse selon l'approche en cascade ou selon les méthodes Agile. C'est pourquoi une solution de gestion des API doit disposer de workflows parfaitement fonctionnels pour réaliser les opérations suivantes :

- Planification et conception des API à l'aide des normes sectorielles
- Intégration et sécurisation des API de bout en bout
- Test, déploiement et prise en charge des changements de version et des retours à un état antérieur
- Gestion et supervision de l'utilisation des API, y compris des rapports et des fonctionnalités analytiques

Pour être pleinement fonctionnelle, une solution de gestion des API doit également être en mesure de gérer simultanément plusieurs versions en production, que ce soit pour prendre en charge les clients plus anciens ou pour gérer différentes technologies d'accès, comme le protocole SOAP (Simple Object Access Protocol), la méthode REST (Representational State Transfer) ou le protocole JSON (JavaScript® Object Notification). Un cadre de gestion du cycle de vie qui n'administre que le développement localisé ne peut pas répondre aux besoins des entreprises modernes. Le Cloud, tant public que privé, est en croissance permanente. Cela implique pour les entreprises de disposer d'une solution de gestion des API qui couvre les tests et la production dans le Cloud, et qui puisse isoler les développeurs d'API des fluctuations en matière de topologie et de caractéristiques réseau.

Gouvernance des API

Le terme de « gouvernance » est souvent utilisé pour désigner de manière très large différentes exigences en termes de gestion, de processus et de visibilité, ainsi que les conditions générales selon lesquelles une API est exposée auprès d'un ou de plusieurs utilisateurs. Bien que la notion de gouvernance inclue celles de sécurité et de cycle de vie, elle comprend également certaines exigences relatives aux SLA, à la supervision et au reporting. En outre, dans le cas des solutions de gestion des API, elle a trait à l'impératif plus global consistant à proposer des modalités d'exposition des données ou des fonctionnalités différentes en fonction de l'identité des consommateurs, de leurs capacités, de leur type d'abonnement ou de tout autre contexte transactionnel pouvant être défini au sein d'une règle.

Pour être efficace, la gouvernance des API doit avant tout être flexible : la technologie utilisée pour contrôler les modalités de partage des API doit dépendre des préférences et des processus de l'entreprise, et non l'inverse. Par conséquent, la solution de gestion des API doit être configurable et pouvoir s'adapter à tout SLA, à toute mesure de sécurité, à tout processus de journalisation ou à tout autre contrôle par le biais d'une règle. Les règles sont en effet au cœur de la flexibilité : ce sont elles qui garantissent la cohérence du résultat final d'une implémentation à l'autre. Lorsqu'elles restreignent les administrateurs à des contrôles imprécis sans environnement de développement gérant pleinement les règles, les solutions de gestion des API limitent les possibilités de contrôle.

Flexibilité de déploiement

La majorité des entreprises disposent d'une infrastructure existante, conçue en fonction de la façon dont elles gèrent leur activité métier. Lorsqu'une entreprise envisage d'adopter une solution de gestion des API, elle doit étudier des solutions qui s'adapteront à son environnement existant. Les équipes d'architecture doivent pouvoir gérer cette solution en tant qu'extension de leurs propres infrastructures, plutôt que comme un environnement distinct. Pour plus d'informations sur ce niveau d'intégration, reportez-vous au dossier solution intitulé « Guide d'architecture pour l'extension de votre environnement ESB/SOA aux modèles mobile, Cloud et IoT ».

Outils pour développeurs et mise en place d'une communauté

La gouvernance des API garantit un contrôle homogène pour l'éditeur, mais si les développeurs extérieurs ne peuvent pas découvrir et utiliser facilement les API, le risque est grand qu'elles restent inutilisées. C'est pour cette raison que la plupart des solutions modernes de gestion des API vont au-delà des fonctions telles que la sécurité, la gestion du cycle de vie et la gouvernance, et proposent des fonctionnalités destinées à aider les éditeurs à faire découvrir leurs API aux développeurs externes, le plus souvent via un portail spécialisé. Offrant un point d'interaction unique, ce type de portail permet aux développeurs de se créer un compte, de demander une clé d'API, de découvrir quelles sont les API disponibles et de consulter des exemples de code.

Tout portail pour développeurs d'API axé sur l'utilisation en entreprise doit offrir les fonctionnalités suivantes :

- Des API mobiles facilement utilisables (y compris pour OAuth et OpenID Connect)
- Des outils de reporting et d'analyse pour les opérateurs
- Une gestion facile de la relation métier

Du fait que chaque entreprise aborde la publication d'API avec son propre bagage et ses propres priorités, un portail d'API doit pouvoir être personnalisé, au même titre qu'un cadre de gestion de la sécurité, de cycle de développement et de gouvernance. Par conséquent, les entreprises auront la plupart du temps intérêt à envisager un portail décomposable. Il peut s'agir d'un portail en marque blanche pouvant être personnalisé en fonction d'une stratégie d'engagement des développeurs donnée, ou bien d'un portail d'API pouvant être utilisé en tant que composant distinct, via un portail de développeurs d'entreprise préexistant. Une fois encore la flexibilité est le maître-mot.

Monétisation des API

Le concept de monétisation est lié à celui de mise à disposition d'outils pour les développeurs. Si les entreprises décident souvent de favoriser l'adoption de leurs API en accordant gratuitement l'accès à leurs déclinaisons Web et mobiles, par exemple, d'autres peuvent parfaitement décider de rendre payants les niveaux d'accès plus élevés (souvent selon le modèle du paiement à l'utilisation). Une fois encore, il n'existe pas qu'une seule bonne façon d'aborder la question de la monétisation. Voici quelques possibilités :

- Modèle « freemium » selon lequel l'utilisation est gratuite en dessous d'un certain seuil de transmission de données ou de demandes client
- Facturation de certains niveaux de garantie de service ou la priorité sur les utilisateurs de l'offre gratuite
- Fourniture d'informations ou de fonctionnalités auxquelles les utilisateurs de l'offre gratuite n'ont pas accès

Quelle que soit l'approche choisie, la solution de gestion des API doit être suffisamment élaborée pour permettre à l'entreprise de fixer ses critères de monétisation en toute flexibilité. La solution doit offrir les possibilités suivantes :

- Collecter un large éventail de statistiques qui serviront à mesurer l'utilisation
- Proposer des fonctionnalités avancées en matière de SLA et de catégories de services afin d'autoriser la hiérarchisation du trafic
- Créer des API payantes virtuelles séparées et réservées aux clients payants, sans nécessiter de codage

Exigences opérationnelles relatives aux solutions de gestion des API

Sécurité de la solution

La solution de gestion des API étant souvent le seul élément technologique séparant les API publiées par l'entreprise du monde extérieur, son niveau de sécurité détermine celui des API. Si la solution est elle-même compromise, toute mesure de sécurité censée protéger les API le sera également. Il est par conséquent recommandé aux entreprises qui recherchent une solution de gestion des API de considérer la sécurité de celle-ci comme une priorité absolue.

Étant donné que cette solution servira d'intermédiaire entre le monde extérieur et les API internes, son évaluation commence souvent par déterminer si la solution peut elle-même être compromise. Cela dépend du type de tests de pénétration qu'elle a subis, des restrictions d'accès qu'elle impose et des tests de vulnérabilité qu'elle a réussis. Il est recommandé de privilégier les solutions ayant passé le test STIG (Security Technical Implementation Guide), celles ayant reçu la certification PCI DSS (Payment Card Industry Data Security Standard) pour les solutions destinées à traiter des données de cartes de crédit, ou celles qui sont certifiées FIPS (Federal Information Processing Standard) et Common Criteria pour les solutions devant respecter des normes de sécurité gouvernementales plus strictes.

Pour la plupart des applications pratiques, les entreprises préfèreront les solutions de gestion des API qui font transiter les requêtes provenant de l'extérieur par une passerelle. Les passerelles d'API à intermédiaire ont l'avantage d'offrir des points de contrôle et d'isolation clairement définis, ce qui facilite l'administration et la certification de la sécurité (à l'instar des pare-feu sur les réseaux). Certaines prennent même en charge le chiffrement des clés d'API à l'aide de modules de sécurité matériels. Dans la mesure où ces clés constituent bien souvent la principale ligne de défense contre les abus, il est effectivement prudent de les protéger du vol en les chiffrant.

Facilité de gestion de la solution

Contrairement à la plupart des start-up, qui font généralement tourner l'intégralité de leur site Web de production sur une seule instance Amazon ou chez un petit fournisseur hébergé, les grandes entreprises possèdent souvent des environnements de développement et de production hétéroclites. Par exemple :

- Des équipes de développement dispersées dans plusieurs pays
- Des environnements de production répartis sur des data centers situés aux quatre coins du globe
- Des systèmes de reprise après sinistre basés sur le Cloud

Dans un tel contexte, les possibilités d'administration pèsent lourd dans la balance lorsqu'il est question de choisir une solution. Les considérations techniques, telles que la manière d'administrer un cluster de passerelles d'API, un data center entièrement automatisé ou l'équilibrage géographique des charges, ou encore la gestion des pics de charge, prévaudront sur d'autres fonctionnalités. Une fois de plus, toutes les solutions de gestion des API ne sont pas conçues pour répondre aux besoins des grandes entreprises. Avant de s'engager dans une voie, il est donc important de prendre soin d'évaluer les capacités de chaque solution en matière de gestion de clusters, de basculement, de répartition de charge, de reprise après sinistre et d'autres facteurs d'ordre opérationnel.

Fiabilité de la solution

Dès l'instant où une entreprise décide de se lancer dans un programme de publication d'API, elle devient en pratique un fournisseur de services pour ses utilisateurs d'API, qui compteront sur elle pour leur offrir une disponibilité en continu. Dans un tel contexte, il est inévitable que cette entreprise finisse par accorder une importante considérable à la fiabilité, ce qui fait de cette dernière un facteur essentiel à prendre en compte lors du choix de la solution de gestion des API. Il est conseillé aux entreprises de privilégier les solutions gérant directement la redondance et minimisant, voire éliminant complètement, le risque d'interruption. Il est donc recommandé aux entreprises de n'accorder de crédit qu'aux solutions de gestion des API qui offrent les atouts suivants :

- Possibilité de déploiement sur site, dans le Cloud ou via une solution hybride (passerelle d'API sur site, portail développeurs dans le Cloud)
- Redondance totale, quel que soit le modèle de déploiement
- Intégration à l'infrastructure existante
- Respect des exigences en matière de sécurité

Conclusions

Puisque chaque entreprise présente des besoins et des environnements uniques, il ne peut exister aucune solution universelle en matière de gestion des API. Cependant, toutes les entreprises ont en commun de rechercher l'excellence en matière de capacités fonctionnelles et opérationnelles. Pour la plupart des entreprises qui se lancent dans la publication d'API, cela se traduit par la volonté de disposer d'une solution de gestion flexible, obéissant à des règles strictes et à même de faire face aux rigueurs d'un environnement de production digne d'un opérateur de téléphonie. Sur le plan fonctionnel, elles auront besoin d'une solution capable de satisfaire à une série de prérequis en matière de sécurité et de s'adapter à des cycles de développement existants, dont la gouvernance peut s'effectuer au moyen de règles, en mesure d'attirer les développeurs, favorisant l'adoption par ceux-ci et offrant des possibilités de monétisation. Sur le plan opérationnel, la solution de gestion des API devra être sûre, fiable et offrir un maximum de possibilités d'administration.

Faites appel à un organisme de recherche indépendant pour vous aider à choisir la solution de gestion des API qui vous convient.

Plusieurs cabinets d'analystes de premier plan couvrent les technologies de gestion des API et publient des rapports à ce sujet, en comparant les différents fournisseurs, afin d'aider les entreprises à choisir la meilleure solution possible en fonction de leur stratégie numérique. Les sites d'évaluation IT tels que IT Central Station constituent également une excellente source d'informations pour consulter des comparatifs et des avis client.

Pour obtenir un exemplaire gratuit des comparatifs des meilleurs cabinets d'analystes et découvrir ce que les clients pensent de CA API Management, visitez le site : **www.ca.com/fr/products/api-management/why-ca-api-management.html**.

Contacter CA Technologies

Nous nous ferons un plaisir de répondre à vos questions, commentaires et remarques générales.

Pour plus d'informations, rendez-vous sur le site **ca.com/api**.

ca technologies

Restez connecté à CA Technologies sur ca.com/fr

CA Technologies (NASDAQ : CA) fournit les logiciels qui aident les entreprises à opérer leur transformation numérique. Dans tous les secteurs, les modèles économiques des entreprises sont redéfinis par les applications. Partout, une application sert d'interface entre une entreprise et un utilisateur. CA Technologies aide ces entreprises à saisir les opportunités créées par cette révolution numérique et à naviguer dans « l'Économie des applications ». Grâce à ses logiciels pour planifier, développer, gérer la performance et la sécurité des applications, CA Technologies aide ainsi ces entreprises à devenir plus productives, à offrir une meilleure qualité d'expérience à leurs utilisateurs, et leur ouvre de nouveaux relais de croissance et de compétitivité sur tous les environnements : mobile, Cloud, distribué ou mainframe. Pour plus d'informations, rendez-vous sur le site **ca.com/fr**.

1 Annuaire d'API ProgrammableWeb, décembre 2016, www.programmableweb.com/apis/directory

CS200-241661_1216