okta

Créer des portails en ligne pour vos clients et partenaires avec Okta

Analyse d'architecture

Okta France
Tour Égée - 9-11 Allée de l'Arche
92400
Courbevoie - France
paris@okta.com
01 85 64 08 80

Okta, l'identité d'entreprise clé en main

Okta est un service de gestion des identités en entreprise entièrement conçu dans le cloud et résolument axé sur la réussite des clients. Il permet aux équipes IT de gérer l'accès de toute personne à n'importe quelle application, via n'importe quel terminal. Que les personnes concernées soient des collaborateurs, des partenaires ou des clients, et que les applications soient on-premise, dans le cloud ou sur un mobile, Okta aide les départements IT à renforcer la sécurité, à optimiser la productivité et à garantir la conformité.

Portails clients et partenaires : vue d'ensemble et problématiques

Les entreprises utilisent des portails pour gérer l'accès aux applications web destinées à leurs clients et partenaires. Pour créer ces portails, les administrateurs fédèrent généralement plusieurs applications et services web exécutés en arrière-plan afin de former une solution complète.

Par exemple, un fabricant d'imprimantes peut réserver une partie de son site web, accessible à ses clients, au retour de marchandises, au suivi des livraisons et au recyclage des cartouches vides. Côté clients, ce portail doit ressembler à l'application web de l'entreprise pour l'ensemble de ces tâches. Mais en arrière-plan, les administrateurs utilisent plusieurs applications pour gérer ces tâches : un CRM pour gérer les informations des comptes clients, une application d'assistance client pour les tickets d'incident et un système propriétaire d'expédition pour traiter les retours (voir figure 1). Certaines de ces applications peuvent être dans le cloud et d'autres, on-premise.

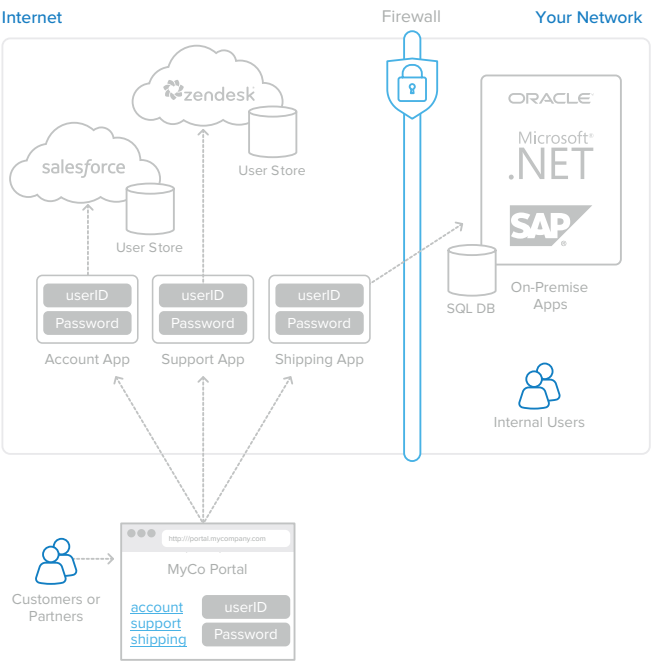

Figure 1 : Portail externe piloté par différentes applications web exécutées en arrière-plan.

L'approche composite illustrée figure 1 pose néanmoins plusieurs problèmes :

- **L'expérience client n'est pas fluide : plusieurs connexions sont souvent nécessaires pour accéder aux différentes parties du portail.**
- **Les utilisateurs doivent s'enregistrer séparément pour chaque partie, ce qui complique l'expérience.**
- **La multiplication des référentiels d'utilisateurs indépendants rend la gestion IT difficile.**

Ces problèmes sont complexes, longs et potentiellement coûteux à résoudre en développant des logiciels personnalisés. Le service de gestion des identités d'Okta apporte une solution en permettant aux entreprises de ne présenter qu'une seule application web parfaitement intégrée à leurs clients et partenaires, qui peuvent l'exploiter avec un jeu d'identifiants unique (voir figure 2). L'enregistrement centralisé peut être automatisé, et les utilisateurs s'identifient une fois pour toutes. Okta simplifie en outre le provisioning et le déprovisioning des utilisateurs dans les applications cibles. Au moment de la connexion, les clients et les partenaires peuvent être dirigés vers une page de destination commune et accéder aux applications autorisées sans obstacle supplémentaire.

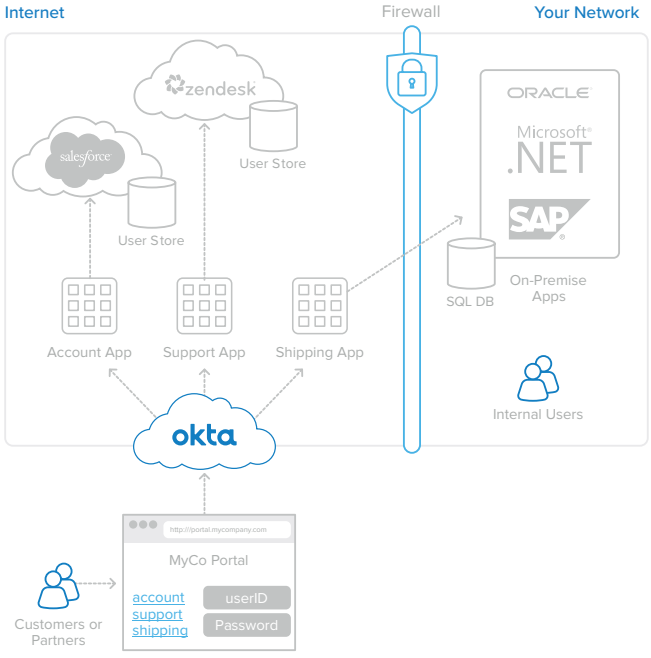

Figure 2 : Portail client simplifié et optimisé avec Okta.

Avec Okta, les entreprises peuvent automatiser rapidement toutes les fonctionnalités de gestion des utilisateurs du portail et offrir une expérience fluide à leurs clients et partenaires, avec un service 100 % à la demande, sécurisé et hautement disponible.

Automatisation de la gestion des identités d'un portail avec Okta

Okta propose de nombreuses fonctionnalités pour répondre aux besoins de gestion des utilisateurs, d'authentification unique (SSO) et de reporting des portails clients et partenaires.

Flexibilité d'un référentiel d'identités cloud

Le service d'Okta comprend un référentiel d'utilisateurs cloud natif permettant de centraliser les identités des clients, des partenaires et des collaborateurs. Ce référentiel peut être utilisé avec ou sans les annuaires externes. Ainsi, les profils utilisateurs et les propriétés correspondantes peuvent émaner d'Okta et y être gérés, ou être administrés depuis différentes sources externes.

Prenons l'exemple d'un groupe de collaborateurs internes, dont les identités seraient gérées dans Active Directory ou LDAP, et qui aurait besoin d'accéder au portail de son entreprise. Okta pourrait se servir d'Active Directory ou de LDAP pour authentifier les employés qui accèdent aux applications du portail, tandis que les comptes utilisateurs des clients et partenaires pourraient être gérés en mode natif dans Okta, ce qui éviterait d'avoir à utiliser un annuaire supplémentaire. Cela dit, Okta peut également gérer les comptes clients et partenaires dans un annuaire d'entreprise existant.

Enregistrement et gestion automatisés des utilisateurs d'applications

Avec Okta, les utilisateurs d'un portail n'ont besoin de s'inscrire qu'une seule fois. Grâce à ses fonctionnalités de gestion des utilisateurs, les comptes sont en effet automatiquement créés dans chaque application web exécutée en arrière-plan.

Pour ajouter des utilisateurs au système, Okta prend en charge l'enregistrement initial de différentes manières :

- **Utilisation de l'interface d'administration Okta**
- **Importation en masse depuis un fichier CSV ou un annuaire externe**
- **Utilisation par programmation des API de gestion des utilisateurs RESTful d'Okta**

Les API RESTful d'Okta peuvent être utilisées avec un formulaire d'enregistrement d'utilisateur personnalisé pour un provisioning entièrement en libre-service, ou assurer la gestion des workflows d'approbation nécessaires.

Dans le cadre du processus de création d'utilisateurs, Okta peut en outre transformer le format des noms d'utilisateur afin de garantir le respect des exigences de différentes applications cloud en la matière. Par exemple, si une partie du portail d'une entreprise repose sur la plateforme Salesforce.com, il est possible qu'un client ou un partenaire cherchant à s'inscrire sur ce portail possède déjà un compte Salesforce.com (sophie@client.com, par exemple). Dans ce cas, il lui serait normalement interdit de créer un autre compte ou de s'inscrire. Okta résoudrait ce problème en appliquant une transformation pour cette utilisatrice, dont le provisioning donnerait sophie@okta.client.com afin d'éviter tout conflit d'espace de noms d'utilisateur avec Salesforce.com.

Mais Okta va encore plus loin : les propriétés utilisateurs spécifiques d'une application, comme l'appartenance à un groupe, le rôle ou le profil, peuvent également être définies selon des règles associées au profil utilisateur Okta. Les attributs de ce profil peuvent même être transmis aux applications exécutées en arrière-plan dans le cadre du processus de provisioning.

Accès à toutes les applications web ou cloud par authentification unique (SSO)

Okta crée une expérience fluide en permettant aux utilisateurs d'accéder par authentification unique (SSO) à toutes les applications web qui composent le portail d'une entreprise. Les utilisateurs s'authentifient une fois pour toutes et ont ainsi accès aux différentes parties du portail sans avoir à ressaisir leurs identifiants.

Pour permettre l'authentification SSO dans toutes les applications, Okta doit tout d'abord établir une session authentifiée avec le navigateur de l'utilisateur. Une fois cette session établie, le service peut authentifier l'utilisateur dans n'importe quelle application connectée selon les règles de contrôle d'accès définies dans Okta. La session Okta initiale peut essentiellement être établie de deux manières :

- **à l'aide de la page de destination « Mes Applications » d'Okta ;**
- **via une connexion SAML établie par un fournisseur de services à un portail existant.**

La page de destination « Mes Applications » d'Okta permet de lancer facilement les applications attribuées. Cette option est couramment utilisée en l'absence de portail centralisé et lorsque les besoins de personnalisation sont mineurs. Lorsqu'une connexion SAML est établie par un fournisseur de services :

1. **L'utilisateur se connecte à un portail centralisé, http://support.ABC.com.**
2. **S'il ne s'est pas encore identifié, il est redirigé vers une page de connexion Okta parallèlement à l'exécution d'une requête SAML, puis renvoyé vers le portail avec une réponse SAML après avoir saisi ses nom d'utilisateur et mot de passe.**
3. **La réponse SAML connecte automatiquement l'utilisateur au portail.**

4. **L'utilisateur dispose à présent d'une session de portail et d'une session Okta qui lui permettent d'être automatiquement authentifié dans les applications qui lui ont été attribuées. Pour en savoir plus, voir figure 3.**

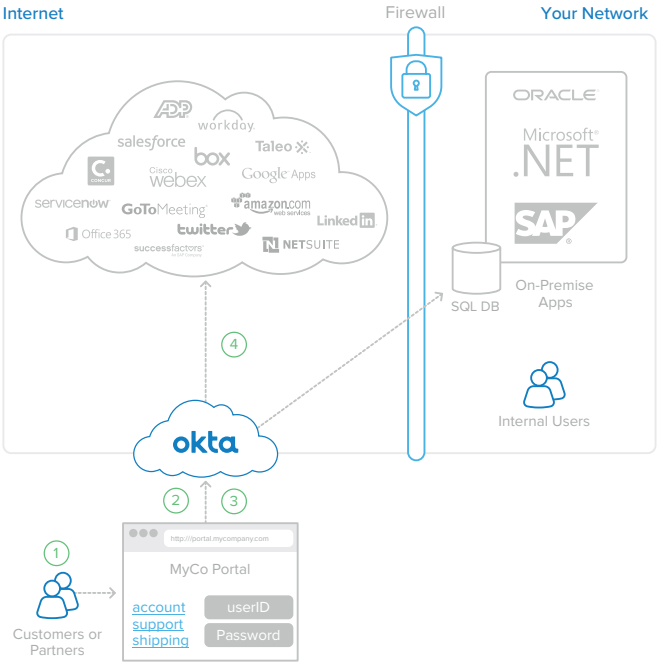

Figure 3 : Authentification pour toutes les applications via une connexion SAML établie par un fournisseur de services.

Une fois la session Okta établie, les utilisateurs peuvent être automatiquement authentifiés dans toutes les applications qui leur ont été attribuées, grâce à une intégration SSO personnalisée ou basée sur un catalogue. Ces intégrations SSO peuvent être fédérées (moyennant la prise en charge d'une norme de type SAML ou d'un autre protocole d'authentification fédérée propriétaire), ou bien utiliser le protocole SWA (Secure Web Authentication) d'Okta pour envoyer un formulaire sécurisé à la page de connexion de l'application.

Les applications disponibles dans le réseau d'applications d'Okta, qui sont pour la plupart des applications commerciales, sont préintégrées pour l'authentification SSO via le protocole SAML ou SWA. Ces intégrations, fournies dans le cadre du service Okta, sont constamment mises à jour.

Pour les applications personnalisées non disponibles dans le réseau d'applications d'Okta, Okta propose des toolkits d'intégration facilitant la prise en charge du protocole SAML, comme illustré figure 4. Ces toolkits SAML sont disponibles pour les applications .NET exécutées sous IIS, et sont compatibles avec l'authentification par formulaire et de nombreux autres langages, dont Java et PHP. Les entreprises peuvent également faire appel au protocole SWA d'Okta pour permettre l'authentification SSO dans ces applications.

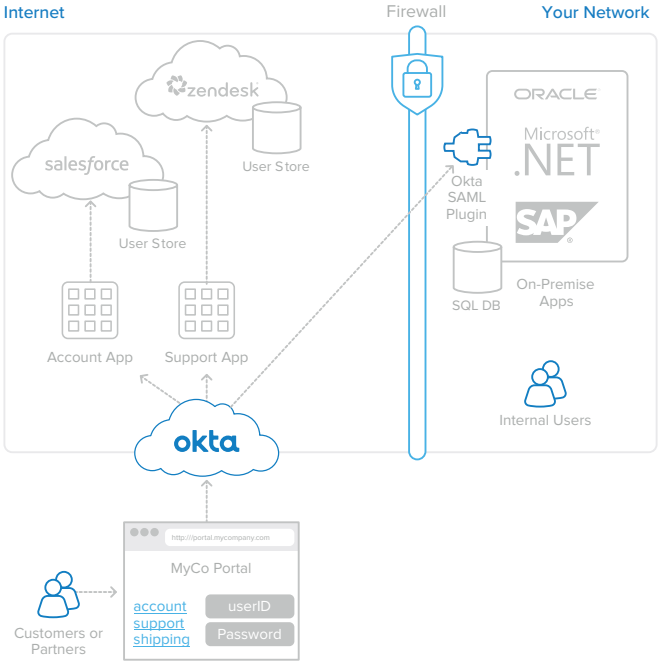

Figure 4 : Toolkits d'intégration SAML pour applications web on-premise.

La seule condition requise par le protocole SWA est le provisioning du compte utilisateur dans l'application cible, avec un mot de passe connu pouvant ensuite être stocké en toute sécurité dans le service Okta.

Intégration et authentification fédérée des portails tiers

Le « portail intégré » fait partie des configurations courantes. Dans ce cas, votre portail est incorporé dans une autre application exécutée par un tiers. Supposons que vous mettiez un portail de configuration de produits à la disposition de vos partenaires. L'un de vos distributeurs pourrait incorporer ce portail dans sa propre application de traitement des commandes, et proposer ainsi une solution plus complète. Okta facilite la tâche des collaborateurs du distributeur, qui n'ont besoin de s'identifier qu'une seule fois.

Pour ces portails intégrés, il faut aussi très souvent que les utilisateurs ayant accès au portail puissent se connecter facilement depuis le réseau de leur propre entreprise, sans avoir à saisir d'identifiants supplémentaires. Reprenons l'exemple précédent : les collaborateurs du distributeur s'authentifieraient chaque matin sur le réseau de leur entreprise ; ils pourraient ensuite accéder à l'outil de configuration de produits sans autres identifiants. Cet accès simplifié nécessiterait également le provisioning automatique de comptes pour les collaborateurs du distributeur.

Tout cela est possible grâce à Okta, qui prend en charge les assertions SAML en entrée depuis un autre fournisseur d'identité ; celles-ci sont utilisées pour le provisioning des nouveaux comptes et l'octroi d'accès aux applications concernées qui alimentent le portail.

Dans l'exemple ci-dessus, les employés du distributeur s'identifieraient normalement sur le réseau de leur entreprise et, lors de leur première tentative d'accès au portail, ils seraient redirigés vers Okta à des fins d'authentification, via les assertions SAML de leur fournisseur d'identité (IdP).

S'il n'existe aucun compte, le provisioning des nouveaux comptes utilisateurs peut être automatique. Les autorisations des utilisateurs sont ensuite traitées, et le provisioning des comptes est assuré dans toutes les applications nécessaires qui alimentent le portail (dans le cas présent, l'outil de configuration de produits). Résultat : une expérience utilisateur fluide pour les collaborateurs du distributeur lorsqu'ils naviguent entre les applications de leur entreprise et le portail.

Une plateforme qui s'intègre avec les solutions de gestion des identités existantes

Okta peut aisément s'intégrer avec des applications créées sur mesure et des processus métier, mais aussi avec les solutions de gestion des identités existantes.

Des applications web peuvent devenir compatibles avec l'authentification SSO grâce à de simples modèles de code fournis par Okta dans plusieurs langages, dont Java, ASP.NET et PHP. Okta peut en outre s'intégrer avec une solution de gestion des identités on-premise existante.

Par exemple, moyennant une simple intégration entre Okta et une solution en place, Okta peut assurer l'authentification SSO et la gestion des utilisateurs de toutes les applications déjà intégrées dans cette solution. D'autres applications cloud et on-premise peuvent ensuite être intégrées directement avec Okta et l'ensemble des logiciels seront gérés au sein d'un unique framework cohérent.

Cette solution permet d'optimiser les investissements dans l'infrastructure en place afin d'accélérer l'implémentation, tout en offrant une expérience client fluide dans les anciennes applications comme dans les nouvelles, qu'elles soient on-premise ou dans le cloud.

Exemple : ABC S.A.S.

ABC S.A.S. a développé une série d'applications pour ses partenaires et ses clients. Ces applications sont les suivantes :

- **Un site de téléchargement conçu en PHP personnalisé**
- **Un site d'enregistrement des contrats créé dans Force.com à destination des partenaires**
- **Un site d'assistance reposant sur Jive et Zendesk**

ABC doit autoriser l'accès à ces différents sites via un identifiant et un mot de passe uniques. Les utilisateurs doivent s'inscrire une fois et avoir accès aux sites correspondant à leur profil. Les profils utilisateurs sont au nombre de trois : clients titulaires d'un contrat d'assistance ; clients dépourvus de contrat en cours de validité ; et revendeurs.

Les clients bénéficiant d'une assistance ont accès aux sites de téléchargement et de support technique, tandis que les clients sans contrat ont uniquement accès au site de téléchargement. Quant aux revendeurs, ils ont accès aux trois sites. Les clients, avec ou sans contrat, s'enregistrent eux-mêmes en remplissant un formulaire hébergé dans une partie non authentifiée du site d'assistance. Les partenaires sont, quant à eux, enregistrés par les responsables partenaires via un formulaire hébergé sur le portail des partenaires.

Conception de la solution avec Okta

Enregistrement et gestion des utilisateurs

Pour gérer l'enregistrement des utilisateurs et créer des comptes dans chacune de ces applications, Okta propose des fonctionnalités complètes de gestion des utilisateurs. Un utilisateur peut être créé via des API Okta appelées depuis le formulaire d'enregistrement des portails partenaires et d'assistance. Ces API permettent de définir des propriétés utilisateurs de base, comme les coordonnées et l'appartenance à des groupes. Imaginons que Jean Partenaire soit créé et ajouté à un groupe appelé « Partenaires ». L'appartenance au groupe Okta détermine les comptes à créer en aval dans les applications concernées. Dans le cas de Jean, les comptes pouvant être automatisés au moyen des fonctionnalités de provisioning d'utilisateurs d'Okta doivent être créés dans les quatre applications. Pour les applications et plateformes comme Zendesk et Force.com, cette opération est exécutée par le réseau d'applications d'Okta et ne nécessite aucune personnalisation du code, ni aucune configuration de la part de l'administrateur.

Pour l'application PHP personnalisée, Okta peut émettre un appel via une simple interface de type REST afin d'informer l'application qu'un nouvel utilisateur doit être créé. Le développeur de l'application peut ensuite traiter l'appel REST et ajouter l'utilisateur à l'annuaire de cette même application.

Activation de l'authentification unique (SSO)

Pour activer l'authentification SSO entre ces différentes applications, il est nécessaire de connecter Okta à chacune d'elles. Pour Force.com, Jive et Zendesk, il suffit aux administrateurs de sélectionner les applications dans le réseau d'applications d'Okta en suivant un assistant à deux ou quatre étapes. Dans ces trois cas, le protocole SAML est le mécanisme SSO privilégié, mais les détails et la lourdeur des tâches nécessaires pour établir une relation de confiance et des liaisons entre les assertions sont épargnés à l'administrateur d'ABC.com, puisque c'est le service Okta qui s'en charge.

En ce qui concerne l'application PHP personnalisée, ABC.com peut se servir d'un modèle et d'un exemple de code PHP simples fournis par Okta et que les développeurs de l'entreprise peuvent intégrer dans la page de connexion de l'application. Une fois ce code incorporé, Okta peut activer automatiquement l'authentification SSO dans l'application de la même manière que pour Force.com et d'autres applications cloud. Pour activer l'authentification SSO, ABC.com peut également faire appel au protocole SWA d'Okta.

Automatisation de l'authentification SSO et de la gestion des utilisateurs du portail

Une fois l'authentification SSO et la gestion des utilisateurs activées dans les applications — que ce soit avec des intégrations sélectionnées dans le réseau d'applications d'Okta ou les bibliothèques SAML d'Okta — et une fois l'enregistrement des utilisateurs intégré via l'API de gestion REST d'Okta, le système est opérationnel.

Les utilisateurs peuvent s'inscrire une fois pour toutes, et leurs comptes seront créés dans toutes les applications nécessaires. Ils peuvent s'authentifier facilement dans une application et accéder à n'importe quelle autre application via des liens incorporés, sans être invités à saisir d'autres identifiants.

Par ailleurs, en cas de modification des propriétés utilisateurs (adresse e-mail, appartenance à des groupes, etc.), les propriétés mises à jour sont automatiquement répercutées dans les applications concernées. La solution est simple à mettre en œuvre, facile à gérer et offre une excellente expérience utilisateur.

Synthèse

Le service de gestion des identités et des accès d'Okta simplifie considérablement la création de portails web, que ce soit pour les clients ou les partenaires. Avec Okta, les entreprises peuvent :

- **présenter à leurs clients et partenaires une application web unique, parfaitement intégrée ;**
- **automatiser l'enregistrement, puis le provisioning et le déprovisioning des utilisateurs pour les applications cibles qui composent un portail ;**
- **proposer aux clients et partenaires une seule et même page de connexion, et leur permettre d'accéder aux applications autorisées sans obstacle supplémentaire ;**
- **éliminer les référentiel d'utilisateurs non synchronisés indépendants.**

Avec Okta, les entreprises peuvent automatiser rapidement toutes les fonctionnalités de gestion des utilisateurs d'un portail, avec un service 100 % à la demande, sécurisé et hautement disponible.

À propos d'Okta

Okta est la plateforme de gestion des connexions sécurisées entre les individus et les technologies. En mettant à profit la puissance du cloud, elle permet aux utilisateurs d'accéder à des applications à tout moment et depuis n'importe quel terminal, tout en assurant le respect de politiques de sécurité très strictes. La solution s'intègre directement avec les annuaires et systèmes de gestion des identités en place dans l'entreprise, ainsi qu'avec plus de 6 500 applications. Le service Okta s'exécutant sur une plateforme intégrée, il est possible de le déployer rapidement à grande échelle, moyennant un faible coût total de possession. Plus de 7 850 clients, dont Adobe, Allergan, Chiquita, LinkedIn, MGM Resorts International et Western Union, font confiance à Okta pour travailler plus rapidement, doper leur chiffre d'affaires et préserver leur sécurité.

Pour en savoir plus, consultez le site www.okta.com/fr ou suivez-nous sur www.okta.com/fr/blog.