INTÉGRATION D'ANNUAIRES AVEC OKTA

Analyse d'architecture

Okta France
Paris

paris@okta.com
01 85 64 08 80

Annuaires utilisateurs et cloud - Vue d'ensemble

Dans la plupart des entreprises, les annuaires de type Microsoft Active Directory (AD) ou Lightweight Directory Access Protocol (LDAP) tels que SunOne ou Oracle Internet Directory jouent un rôle essentiel dans la coordination des politiques de gestion des identités et des accès. L'annuaire Active Directory ou LDAP fait généralement office de « source fiable » pour les identités des utilisateurs et permet de contrôler l'accès aux ressources on-premise : réseaux, serveurs de fichiers, applications web, etc. (voir figure 1). Lorsque des applications on-premise sont intégrées avec Active Directory ou LDAP, les utilisateurs bénéficient d'une expérience optimale : ils se connectent une fois à leur domaine et ont ensuite accès à toutes les ressources dont ils ont besoin. Les administrateurs, quant à eux, savent précisément qui a accès à quoi. Ce modèle est très répandu car il convient bien aux architectures basées sur un réseau local (où les applications sont mises à disposition à partir d'équipements protégés par un pare-feu). Mais comme nous allons vous l'expliquer, cette approche trouve actuellement ses limites au vu de l'adoption massive du cloud — un changement de paradigme qui exige le recours à une nouvelle solution.

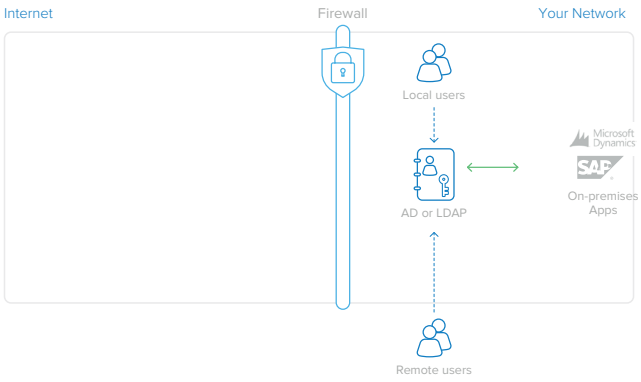

Figure 1 : Gestion des identités des utilisateurs d'applications on-premise via Active Directory ou LDAP

La multiplication des annuaires utilisateurs indépendants est l'une des conséquences de la migration vers les applications cloud : celles-ci sont généralement déployées séparément, et chacune possède sa propre base de données d'identifiants (voir figure 2). Si l'on se limite à une ou deux applications, les désagréments sont mineurs, mais face au succès croissant des applications cloud, les administrateurs ont bien du mal à gérer des annuaires utilisateurs toujours plus nombreux. Et le problème ne fait que s'aggraver. Chaque nouvelle application s'accompagne d'une multitude de mots de passe utilisateurs, et les administrateurs perdent rapidement le contrôle des accès. Pire encore, en cas de départ d'un collaborateur, la plupart des entreprises peinent à identifier avec précision les comptes à désactiver et ne disposent pas des fonctionnalités d'audit nécessaires pour assurer le déprovisioning en temps voulu.

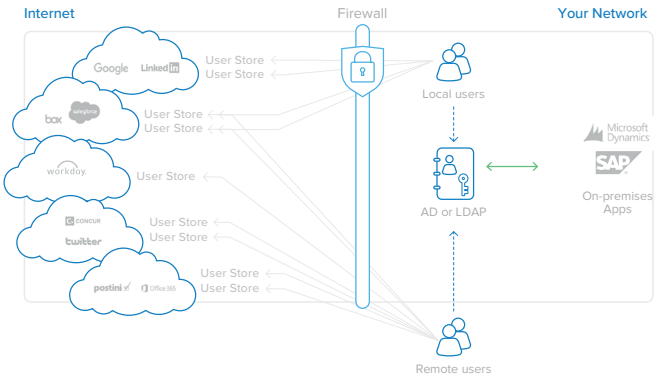

Figure 2 : Multiplication des annuaires utilisateurs consécutive à l'adoption d'applications cloud

Face au problème de la multiplication des annuaires utilisateurs indépendants, l'une des solutions consiste à intégrer toutes les applications cloud dans un magasin d'identités partagé (voir figure 3). Les annuaires utilisateurs Active Directory ou LDAP, capables d'assurer la gestion des identités à la fois pour les applications on-premise et cloud, sont de loin les options les plus pratiques. Certains fournisseurs d'applications cloud proposent des API ou des toolkits qui permettent de connecter les référentiels d'identités de leurs applications à Active

Directory ou LDAP. Toutefois, l'intégration via des API nécessite un développement personnalisé. Or, les toolkits sont tous différents et exigent souvent d'importants investissements en configuration, équipement (matériel nécessaire pour exécuter le logiciel connecteur) et maintenance, car les applications évoluent au fil de temps. Plus le nombre d'applications cloud augmente, plus ce modèle d'intégration au cas par cas avec Active Directory ou LDAP est inabordable. Or, les entreprises ont constamment besoin de nouvelles applications.

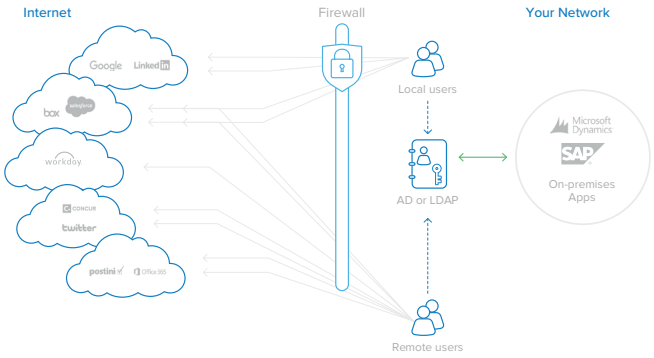

Figure 3 : L'intégration avec plusieurs applications cloud est coûteuse et difficile à gérer.

Obstacles aux intégrations Active Directory ou LDAP « maison »	Approche Okta
Disposez-vous des compétences requises pour développer ces intégrations ?	Avec Okta, les intégrations n'exigent aucune expérience en programmation ni en développement et s'opèrent en quelques minutes via une interface conviviale.
Comment allez-vous gérer les intégrations et les mettre à niveau ?	Okta collabore avec des éditeurs de logiciels, et suit au quotidien les modifications et mises à niveau des API afin de tirer parti des dernières fonctionnalités en date. Nous publions des mises à jour chaque semaine pour tenir compte de ces changements.
Comment surveillez-vous l'état des intégrations ?	Okta surveille et teste constamment les intégrations pour veiller à ce qu'elles fonctionnent comme prévu après les mises à niveau et le lancement de nouvelles versions.
Quel protocole utilisez-vous pour vous connecter à chaque application cloud ?	Inutile de connaître SAML, OAuth, SCIM ou d'autres protocoles d'intégration : Okta gère ces intégrations à votre place.
Que se passe-t-il en cas de panne du serveur qui exécute une intégration maison basée sur un toolkit ?	Okta active automatiquement la reprise après basculement avec une architecture d'agent redondant.
Comment intégrer une application cloud avec une configuration Active Directory ou LDAP à plusieurs domaines ?	Okta prend en charge plusieurs environnements de domaines Active Directory et/ou LDAP.
Quelles modifications du pare-feu sont nécessaires pour chaque intégration d'application cloud avec Active Directory ou LDAP ?	Avec Okta, aucune modification du pare-feu n'est nécessaire pour prendre en charge l'intégration Active Directory ou LDAP.

Le service cloud de gestion des identités et des accès d'Okta résout ces problèmes au moyen d'un point d'intégration unique, qui offre une solution hautement disponible pour la totalité des intégrations d'applications web et cloud avec Active Directory et LDAP. Okta élimine les inconvénients liés à la création et à la gestion de plusieurs intégrations d'annuaires on-premise.

Intégration d'annuaires avec Okta pour toutes les applications cloud

Okta propose une solution d'intégration d'annuaires simple et complète pour les applications web on-premise et cloud. Le service de gestion des identités et des accès à la demande d'Okta offre des fonctions d'authentification, de provisioning et déprovisioning d'utilisateurs, mais aussi d'analyse et reporting détaillés de l'utilisation des applications web on-premise et cloud. L'une des principales composantes de ce service est la fonctionnalité d'intégration d'annuaires d'Okta, très facile à configurer et conçue pour une haute disponibilité. Par ailleurs, Okta gère ces intégrations à votre place, avec des milliers d'applications prises en charge dans le réseau d'applications Okta (OAN).

Pour l'intégration Active Directory, Okta propose trois composants légers et sécurisés :

- **Agent Okta Active Directory :** agent léger qui peut être installé sur un serveur Windows et permet de se connecter aux annuaires Active Directory on-premise pour les demandes de provisioning, de déprovisioning et d'authentification des utilisateurs.
- **Application web Okta IWA (Integrated Windows Authentication) :** application web légère qui est installée sur un serveur IIS (Internet Information Services) et permet d'authentifier les utilisateurs de domaine via l'authentification Windows intégrée.
- **Agent Okta Active Directory Password Sync :** agent léger installé sur les contrôleurs de domaines, qui synchronise automatiquement les changements de mots de passe Active Directory, les envoie à Okta et les synchronise avec les applications dont les utilisateurs se servent.

Pour l'intégration LDAP, Okta propose un composant on-premise léger et sécurisé :

- **Agent Okta LDAP :** agent léger qui peut être installé sur un serveur Windows et permet de se connecter aux annuaires utilisateurs LDAP on-premise pour les demandes de provisioning, de déprovisioning et d'authentification.

Les agents Okta Active Directory/LDAP, l'application web Okta IWA et l'agent Okta Active Directory Password Sync peuvent être couplés au service cloud Okta lui-même pour former une architecture hautement disponible, facile à configurer et à gérer, et adaptée à de nombreux cas d'usage. Ce document fournit des détails supplémentaires sur cette architecture flexible.

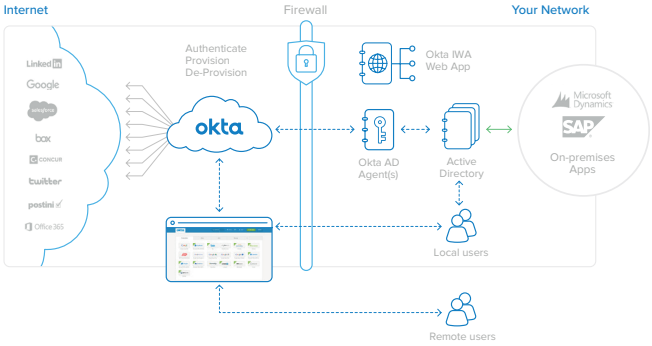

Figure 4 : Architecture Okta pour Active Directory : une seule intégration pour la totalité des applications web

La solution Okta d'intégration d'annuaires offre les fonctionnalités suivantes :

- **Installation et configuration simples et sécurisées**
- **Provisioning en temps réel**
- **Synchronisation intelligente des utilisateurs**
- **Provisioning JIT (Just in time)**
- **Délégation d'authentification efficace**
- **Authentification unique (SSO) sur postes de travail (Active Directory uniquement)**
- **Prise en charge de la réinitialisation des mots de passe en libre-service (Active Directory uniquement)**
- **Provisioning piloté par les groupes de sécurité**
- **Déprovisioning automatisé en un clic**
- **Accès par authentification unique (SSO) aux applications authentifiées**

Installation et configuration simples et sécurisées

Avec Okta, l'activation de l'intégration d'annuaires est un processus simple, piloté par un assistant. D'un simple clic dans la console d'administration Okta, vous pouvez télécharger l'agent Okta Active Directory ou LDAP et l'installer sur un serveur Windows ayant accès à votre contrôleur de domaine. Les agents Okta s'exécutent sur un autre serveur que celui du contrôleur de domaine.

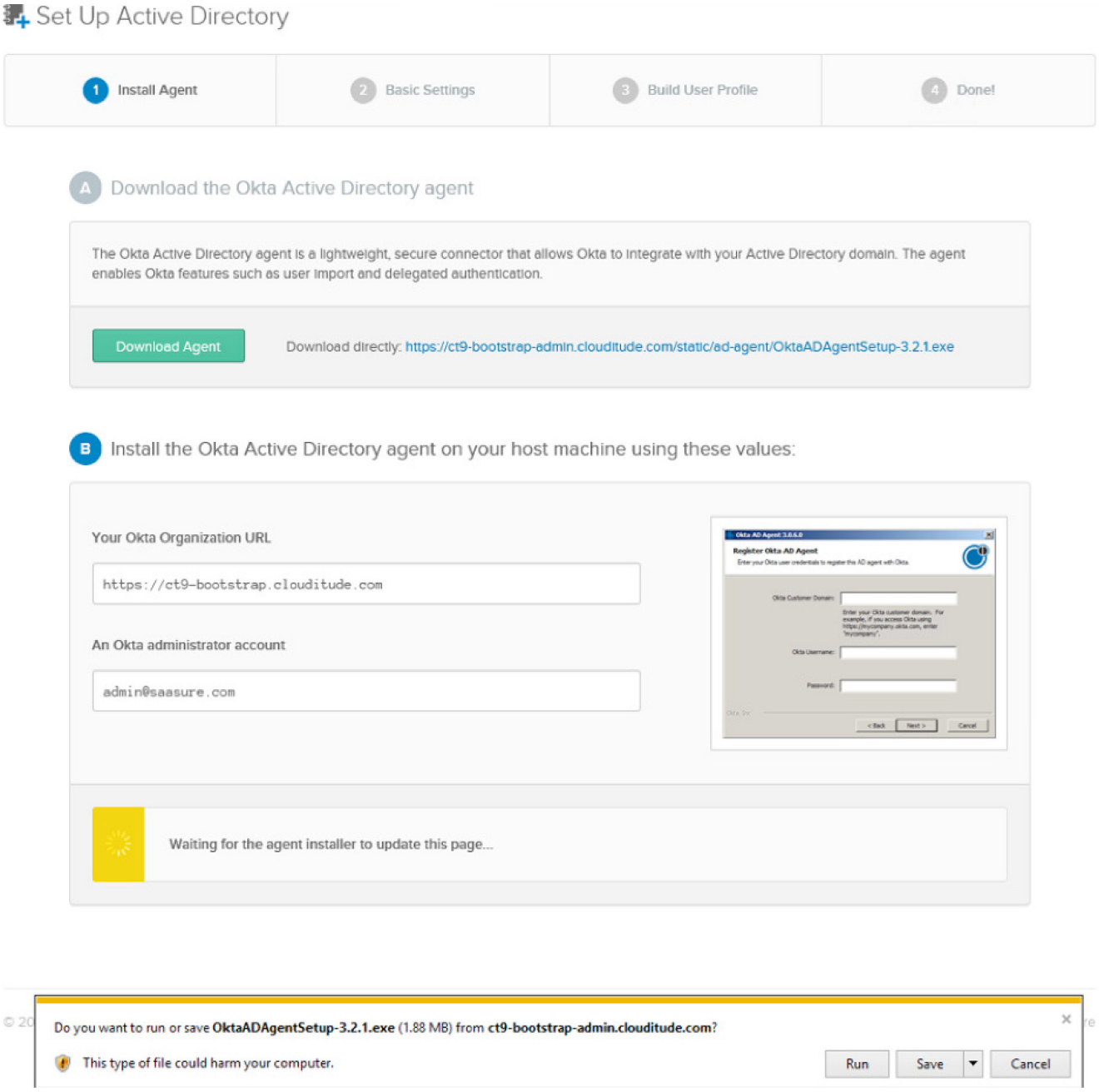

Figure 5 : Processus d'installation pour Active Directory

Lors de l'installation, il suffit de saisir votre URL Okta et vos identifiants d'administrateur Active Directory, et l'agent Okta Active Directory crée un compte d'intégration à faibles privilèges en lecture seule, puis établit une connexion sécurisée avec votre instance Okta. Il n'est pas nécessaire de configurer le réseau ou le pare-feu.

L'agent Okta Active Directory se connecte au service cloud d'Okta via une connexion SSL au port de sortie 443. Cette connexion est renouvelée toutes les 30 secondes pour garantir la compatibilité avec tous les pare-feux ou autres dispositifs de sécurité existants. En règle générale, si un utilisateur peut se connecter à un système à l'aide de ses identifiants Active Directory et accéder à Internet depuis un navigateur, l'agent Okta Active Directory fonctionne correctement et ne nécessite aucune modification du pare-feu.

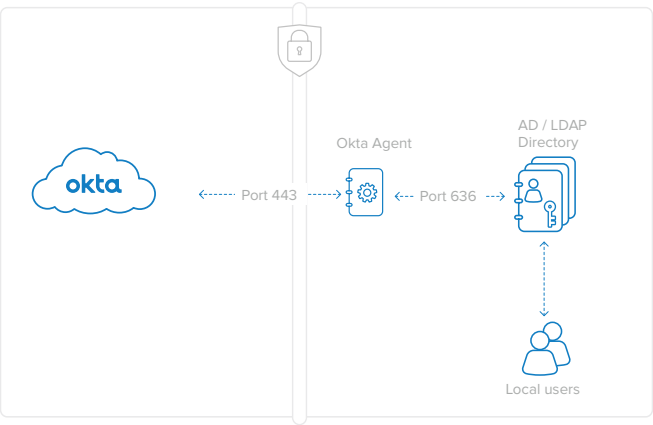

Figure 6 : L'agent Okta se connecte au port 443 pour Active Directory (connexion SSL cryptée) et au port 636 pour LDAP. Aucune modification du pare-feu n'est nécessaire.

La communication avec les agents Okta Active Directory/LDAP est sécurisée par une authentification SSL et mutuelle :

- **Connexion des agents Okta Active Directory/LDAP au service Okta :** l'agent authentifie le service en validant le certificat SSL du serveur Okta pour monentreprise.okta.com. Le service authentifie l'agent à l'aide d'un jeton de sécurité fourni à ce dernier lors de l'enregistrement. Pour générer le jeton de sécurité, le processus d'enregistrement a besoin des identifiants de l'administrateur Okta. Ce jeton est propre à chaque agent et peut être révoqué à tout moment.
- **Connexion de l'agent Okta au serveur contrôleur de domaine ou au serveur LDAP** : l'agent s'authentifie auprès du contrôleur de domaine à l'aide du compte d'intégration à faibles privilèges en lecture seule créé lors de son installation.

Synchronisation en temps réel

Les entreprises ne doivent pas craindre les incohérences d'informations de profil entre leur annuaire utilisateurs et Okta qui risqueraient d'apparaître lors d'importations planifiées. En effet, grâce à la synchronisation en temps réel, Okta actualise les profils à chaque connexion, en toute transparence. Ainsi, que vous changiez les informations de profil d'une personne ou d'un groupe, vos utilisateurs sont actualisés dans Okta tout au long de la journée.

La procédure d'activation de la synchronisation en temps réel est la suivante :

1. **Téléchargez et installez l'agent qui convient.**
2. **Importez les unités d'organisation et les groupes (sans les attributs de membre).**
3. **Définissez les préférences de sélection et de noms d'utilisateur des unités d'organisation (OU - Organization Unit). Remarque : le menu déroulant de planification des importations indique « Never » (Jamais).**
4. **Par défaut, la délégation d'authentification et le provisioning JIT (Just in time) sont activés.**
5. **Le provisioning JIT des utilisateurs peut débuter sans importation préalable, et ceux-ci deviennent immédiatement des utilisateurs Okta.**
6. **À chaque demande de délégation d'authentification ou de provisioning JIT, les appartenances aux groupes sont importées en même temps que le profil complet de l'utilisateur.**

7. **Les utilisateurs sont intégralement mis à jour lors de chaque connexion et de manière asynchrone.**

Les administrateurs peuvent modifier les unités d'organisation, de même que les données de profil des utilisateurs et des groupes dans Active Directory, et les utilisateurs seront mis à jour.

Provisioning JIT (Just in time)

Avec la fonctionnalité de provisioning JIT d'Okta, le provisioning d'utilisateurs est extrêmement simple et rapide. Elle permet en effet aux administrateurs IT d'autoriser la création automatique de nouveaux utilisateurs dans Okta, sous réserve qu'ils figurent déjà dans Active Directory ou un annuaire utilisateurs LDAP.

Les administrateurs IT n'ont pas besoin de procéder à une importation initiale avant d'activer les utilisateurs, ce qui permet de gagner du temps lors de la configuration. Ensuite, les utilisateurs peuvent immédiatement se connecter à Okta en saisissant leurs identifiants d'annuaire (Active Directory ou LDAP) sur leur page de connexion. Les administrateurs ont une vue d'ensemble des profils utilisateurs, des groupes et des appartenances aux groupes dans l'onglet « People » (Collaborateurs).

Le processus de provisioning JIT est le suivant :

1. **Un utilisateur dont le provisioning n'a pas encore été réalisé dans le service Okta tente de se connecter à monentreprise.okta.com.**
2. **Okta et l'agent Okta vérifient les identifiants de l'utilisateur dans l'annuaire Active Directory ou LDAP.**
3. **Si l'utilisateur est actif dans Active Directory ou LDAP, un nouveau compte utilisateur est automatiquement créé dans Okta. Ce nouveau compte reprend les identifiants Active Directory ou LDAP existants de l'utilisateur.**
4. **Selon les attributs de groupe de sécurité définis au niveau de l'annuaire, le provisioning de l'utilisateur dans les applications web et cloud en aval est automatique via le service Okta.**

Le provisioning JIT permet aux administrateurs IT d'encourager l'adoption du service Okta et des applications cloud allouées, et de se servir des identifiants Active Directory ou LDAP que les utilisateurs connaissent déjà.

Délégation d'authentification simple d'utilisation

La solution Okta d'intégration d'annuaires permet de déléguer l'authentification des utilisateurs dans Okta à un domaine Active Directory ou LDAP on-premise. Autrement dit, les tentatives de connexion des utilisateurs à monentreprise.okta.com sont comparées à l'annuaire Active Directory ou LDAP à des fins d'authentification. Les utilisateurs peuvent ensuite se connecter facilement à Okta en indiquant leur identifiant Okta et leur mot de passe Active Directory ou LDAP.

Voici le détail de cette procédure :

1. **L'utilisateur saisit son identifiant et son mot de passe sur la page d'accueil des utilisateurs Okta. Cette page de connexion est protégée par un chiffrement SSL et une image de sécurité destinés à prévenir le phishing. Il est en outre possible d'activer l'authentification multifacteur (question de sécurité supplémentaire ou envoi d'un jeton logiciel sur smartphone).**
2. **L'identifiant et le mot de passe sont transmis à un agent Okta Active Directory ou LDAP exécuté derrière le pare-feu sur la connexion SSL établie lors de la configuration.**
3. **L'agent Okta Active Directory ou LDAP transmet ces informations d'identification au contrôleur de domaine Active Directory ou LDAP à des fins d'authentification.**
4. **Le contrôleur de domaine répond par oui ou par non, selon qu'il valide ou non l'identifiant et le mot de passe.**

5. **La réponse est communiquée au service Okta par l'agent Okta Active Directory ou LDAP. En cas de réponse affirmative, l'utilisateur est authentifié et redirigé vers la page d'accueil Mes Applications d'Okta.**

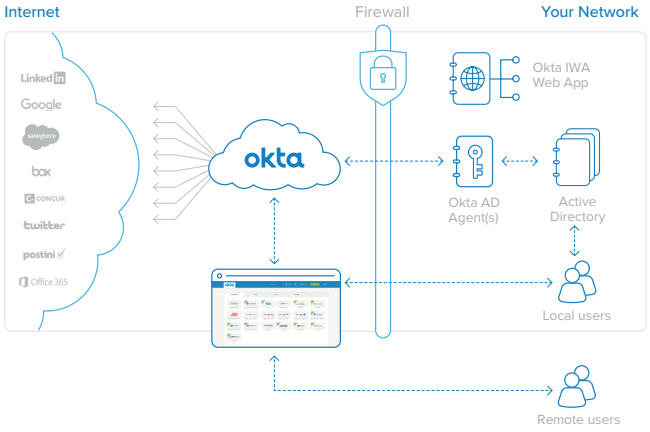

Figure 7 : Délégation de l'authentification à Active Directory

Pour l'utilisateur, la procédure de délégation de l'authentification à Active Directory ou à LDAP est simple :

1. **L'utilisateur se connecte à la page d'accueil Okta, puis lance l'application.**
2. **Okta recherche l'utilisateur dans un annuaire pour l'authentifier.**
3. **L'utilisateur se connecte aux applications cloud via la solution d'authentification unique (SSO) d'Okta.**

Dans la mesure où cette fonctionnalité régit l'accès des utilisateurs à Okta, l'architecture prend en charge plusieurs agents Okta Active Directory et/ou LDAP exécutés dans votre environnement à des fins de redondance. Si l'un des agents Okta Active Directory ou LDAP cesse de fonctionner ou perd sa connexion réseau, les demandes d'authentification sont automatiquement redirigées vers les autres agents Okta Active Directory ou LDAP.

Avec ce mécanisme d'authentification, le mot de passe de l'utilisateur n'est jamais stocké dans le service Okta, et votre annuaire demeure la référence immédiate et optimale pour la validation des informations d'identification. L'annuaire Active Directory ou LDAP étant toujours utilisé pour l'authentification des utilisateurs, les changements de statut d'un utilisateur (modification du mot de passe ou désactivation, par exemple) sont immédiatement appliqués dans le service Okta.

Authentification unique (SSO) sur postes de travail

Okta prend en charge l'authentification unique (SSO) sur postes de travail, qui permet d'étendre les procédures de connexion au domaine Windows des utilisateurs locaux afin de leur octroyer l'accès à Okta et à leurs applications cloud. L'intégration Active Directory d'Okta utilise l'authentification Windows intégrée de Microsoft pour authentifier facilement dans Okta les utilisateurs déjà identifiés via leur connexion au domaine Windows. Il suffit de télécharger et d'installer l'application web Okta IWA et de configurer les plages d'adresses IP souhaitées.

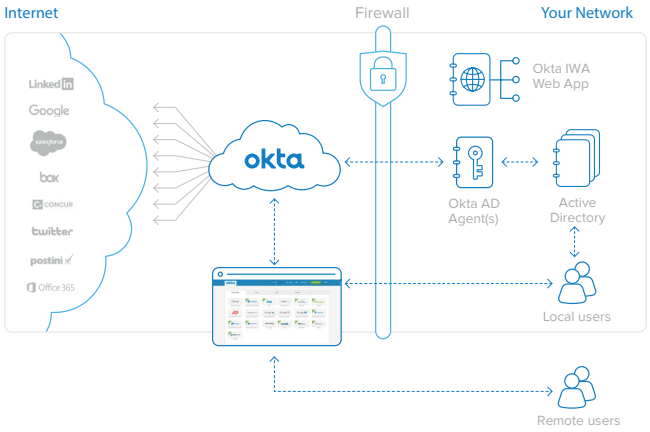

Figure 8 : Authentification unique (SSO) sur postes de travail avec l'application web Okta IWA (Integrated Windows Authentication)

Les étapes en arrière-plan de la procédure de connexion au service Okta par authentification unique (SSO) sur postes de travail (figure 9) sont les suivantes :

1. **L'utilisateur se connecte au site https://monentreprise.okta.com.**
2. **L'utilisateur est redirigé vers l'application web Okta IWA installée en local.**

3. **Cette dernière authentifie l'utilisateur via l'authentification Windows intégrée (Kerberos).**
4. **L'utilisateur est redirigé vers la page de connexion Okta avec des assertions signées par chiffrement contenant son identité Active Directory.**
5. **Le service Okta valide les assertions signées et renvoie directement l'utilisateur vers sa page d'accueil Okta.**

Toutes les étapes ci-dessus sont totalement transparentes pour l'utilisateur. Pour ce dernier, l'expérience est donc simple : il suffit de se connecter à https://monentreprise.okta.com pour accéder immédiatement à la page d'accueil des utilisateurs, qui contient des liens vers toutes les applications qui lui ont été attribuées. Autre possibilité : l'utilisateur clique sur un lien correspondant à une application donnée et est automatiquement identifié dans cette application. L'authentification dans Active Directory en arrière-plan est donc transparente pour l'utilisateur.

Enfin, les utilisateurs à distance ou absents du bureau retrouvent facilement leurs applications cloud et peuvent s'identifier sans mot de passe depuis la page d'accueil d'Okta.

Prise en charge de la réinitialisation des mots de passe en libre-service

Okta permet également aux utilisateurs de changer de mot de passe Active Directory. Lorsque leur mot de passe Active Directory arrive à expiration ou est réinitialisé, les utilisateurs sont automatiquement invités à le modifier lors de leur prochaine connexion à Okta. Les utilisateurs peuvent aussi modifier leur mot de passe Active Directory de façon proactive dans l'onglet de compte de leur page d'accueil Okta. Okta synchronise alors ces informations d'identification avec Active Directory.

Provisioning piloté par les groupes de sécurité

Le service Okta possède une fonction de groupe permettant de piloter le provisioning et l'affectation en masse d'applications aux utilisateurs d'Okta en fonction des groupes auxquels ils appartiennent. Okta permet en effet d'associer des groupes de sécurité Active Directory ou LDAP aux groupes Okta natifs et, par extension, d'allouer automatiquement des applications aux utilisateurs selon leur appartenance aux groupes de sécurité Active Directory ou LDAP.

Lorsque vous ajoutez un utilisateur à votre annuaire, vous pouvez le placer dans un groupe de sécurité. Lors de la synchronisation automatique avec Okta, cet utilisateur est ensuite ajouté, et le provisioning des comptes figurant dans les applications associées à ce groupe de sécurité est automatique. Par ailleurs, les paramètres spécifiques d'une application (rôles, profils, données utilisateur, etc.) sont automatiquement définis en fonction des règles en vigueur dans le service Okta. Par exemple, une règle peut être définie dans Okta afin d'assurer le provisioning d'un compte Salesforce.com pour les membres du groupe de sécurité Active Directory ou LDAP « Ventes » et pour ainsi leur donner accès à ce compte.

Résultat : en cas d'ajout d'un utilisateur dans votre annuaire, les tâches nécessaires pour lui permettre d'accéder à ses applications cloud et web s'exécutent automatiquement. Cette approche réduit considérablement les délais de provisioning des nouveaux collaborateurs et permet aux administrateurs IT de continuer à utiliser Active Directory ou LDAP comme point de départ de la gestion des accès.

Lorsqu'un utilisateur est affecté à un autre groupe de sécurité, la modification est détectée par l'agent Okta Active Directory ou LDAP et relayée au service Okta. Les règles d'affectation sont alors recalculées. Ces règles déclenchent l'attribution de nouvelles applications, la suppression d'affectations d'applications existantes ou la mise à jour des propriétés d'utilisateur dans les applications en aval.

Le processus d'affectation est exactement le même pour les applications nouvelles ou mises à jour. Les tâches de provisioning du compte, configuration de l'authentification unique (SSO) et mise à jour de la page d'accueil Mes Applications de l'utilisateur s'exécutent automatiquement. Le principe est le même pour les suppressions. Si un utilisateur se voit retirer l'accès à une application, il est immédiatement empêché d'utiliser l'authentification unique pour y accéder. Le compte de l'application est ensuite désactivé par le service Okta ou, si la désactivation ne peut pas s'opérer automatiquement, une tâche d'administration est créée. Cette tâche doit ensuite être supprimée une fois le compte désactivé manuellement. Toutes ces opérations peuvent s'exécuter automatiquement ou après confirmation par un administrateur Okta.

Déprovisioning en un clic

En général, la désactivation d'utilisateurs s'effectue depuis un référentiel d'identités d'entreprise standard, comme Active Directory ou LDAP. Avec la fonction de déprovisioning centralisé d'Okta, la désactivation d'un utilisateur de votre annuaire déclenche immédiatement un workflow de déprovisioning, afin d'empêcher efficacement les accès non autorisés à Okta et aux autres applications cloud. Le workflow génère une notification à l'intention des administrateurs et, le cas échéant, aide l'équipe IT à effectuer les tâches manuelles de déprovisioning associées à un utilisateur ou une application spécifique. Ce workflow sert en outre de piste d'audit ; dans Okta, la piste d'audit est entièrement enregistrée à des fins de reporting et de contrôle, ce qui permet de générer facilement des rapports de déprovisioning historiques par utilisateur ou par application.

Accès par authentification unique (SSO) aux applications authentifiées

La plupart des entreprises utilisent des applications web on-premise faciles à intégrer avec la solution d'authentification unique (SSO) d'Okta. Dans de nombreux cas, ces applications utilisent des données d'identification Active Directory ou LDAP pour l'authentification. Au lieu d'utiliser l'authentification Windows intégrée, elles demandent donc à l'utilisateur de saisir ses identifiants Active Directory ou LDAP lorsqu'il se connecte. Lorsque le service Okta est configuré pour déléguer l'authentification à Active Directory, la connexion à ces applications web internes peut là encore être automatisée.

Le processus d'activation de l'authentification SSO pour les applications web internes authentifiées par Active Directory ou LDAP, exécuté en arrière-plan et illustré figure 10, est le suivant :

1. **Okta est configuré pour déléguer l'authentification à Active Directory ou LDAP.**
2. **Le client utilise des applications on-premise authentifiées avec Active Directory ou LDAP.**
3. **L'utilisateur se connecte à Okta avec des identifiants Active Directory ou LDAP.**
4. **L'utilisateur accède aux applications 1 et 2 à technologie SWA à l'aide de ses identifiants Active Directory ou LDAP.**
5. **Les applications 1 et 2 authentifient l'utilisateur à l'aide d'Active Directory ou de LDAP.**

Okta peut se servir de son protocole SWA (Secure Web Authentication) pour connecter automatiquement les utilisateurs à ces applications web internes. Lorsqu'une application de ce type est configurée pour déléguer l'authentification à l'annuaire approprié (ce que fait également Okta), Okta enregistre le mot de passe Active Directory ou LDAP de l'utilisateur lors de la connexion et le lui attribue automatiquement dans les autres applications délégant l'authentification à Active

Directory ou LDAP. Il suffit donc à l'utilisateur de cliquer sur un lien pour accéder à ces applications et s'identifier automatiquement.

Okta synchronise les mots de passe Active Directory de manière sécurisée. Par conséquent, si le mot de passe change dans Active Directory, l'événement est enregistré lors de la connexion à Okta et le référentiel de mots de passe sécurisé de l'application concernée est immédiatement mis à jour, ce qui garantit la réussite de la tentative de connexion suivante.

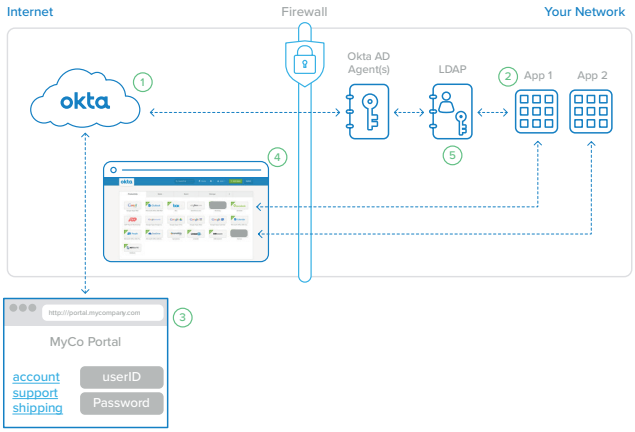

Figure 9 : Okta active l'authentification unique (SSO) pour les applications web internes authentifiées par LDAP.

Conclusion : Étendez votre annuaire au cloud grâce à Okta

Les entreprises délaissent de plus en plus les applications on-premise d'ancienne génération au profit de services cloud, avantageux en matière de fonctionnalités et de réduction des coûts. À l'heure actuelle, la question n'est pas de savoir si vous pouvez opérer cette transition, mais avec quelle rapidité vous pouvez la mettre en œuvre. L'une des principales difficultés de cette démarche consiste à gérer les identités selon des modalités cohérentes avec l'expérience et les attentes des utilisateurs et administrateurs. La réponse à ce problème consiste à lier Active Directory ou LDAP à ces services cloud, en déployant la solution cloud de gestion des identités d'Okta. Okta offre une solution de gestion des identités cloud à la fois flexible, hautement redondante et évolutive, sous la forme d'un service facile à configurer et pratiquement dépourvu de maintenance. Laissez Okta étendre votre utilisation d'Active Directory ou de LDAP à vos applications cloud — celles dont vous vous servez d'ores et déjà, comme celles dont vous aurez besoin à l'avenir.

L'agent Okta Active Directory en détail

L'agent Okta Active Directory est conçu pour monter en charge facilement et automatiquement. Par souci de redondance, il est possible de créer un cluster en installant l'agent Okta Active Directory sur plusieurs serveurs Windows ; le service Okta enregistre alors chacun de ces agents et leur associe automatiquement des commandes d'authentification et de gestion des utilisateurs. Si un agent perd sa connexion ou ne parvient pas à répondre aux commandes, il est retiré de la boucle, ce dont l'administrateur est informé par e-mail. En parallèle, l'agent tente de se reconnecter au service par le biais d'une interruption exponentielle renouvelée toutes les 60 secondes.

Configuration requise pour l'agent Okta Active Directory

Pour la prise en charge de l'agent Okta Active Directory, la configuration minimale requise est la suivante :

- **Windows Server 2003 R2 ou version ultérieure**
- **20 Mo de mémoire pour le service**
- **Compte de service Active Directory créé lors de l'installation de l'agent Okta Active Directory**

Nous recommandons néanmoins la configuration suivante :

- **256 Mo de mémoire pour le service**
- **Compte de service Active Directory dédié avec autorisations d'accès au domaine**
- **Serveur distinct de celui du contrôleur de domaine (pouvant être partagé)**

L’application web Okta IWA en détail

L’application web Okta IWA (Integrated Windows Authentication) est une application web IIS légère permettant d’activer l’authentification unique (SSO) sur postes de travail avec le service Okta. Elle s’installe dans le rôle Serveur Web de Windows Server 2008. Le programme d’installation configure le service IIS et tous les composants Windows.

Configuration requise pour l’application web Okta IWA

Pour la prise en charge de l’application web Okta IWA, la configuration requise est la suivante :

- **Rôle Serveur Web de Windows Server 2008**
- **50 Mo de mémoire**

L’agent Okta LDAP en détail

L’agent Okta LDAP est conçu pour monter en charge facilement et automatiquement. Par souci de redondance, il est possible de créer un cluster en installant des agents Okta LDAP sur plusieurs serveurs Windows. Le service Okta enregistre alors chacun de ces agents et leur attribue automatiquement des commandes d’authentification et de gestion des utilisateurs. Si un agent perd sa connexion ou ne parvient pas à répondre aux commandes, il est retiré de la boucle, ce dont l’administrateur est informé par e-mail. En parallèle, l’agent Okta LDAP tente de se reconnecter au service par le biais d’une interruption exponentielle renouvelée toutes les 60 secondes.

Configuration requise pour l’agent Okta LDAP

Pour la prise en charge de l’agent Okta LDAP, la configuration minimale requise est la suivante :

- **Windows Server 2003 R2 ou version ultérieure**
- **20 Mo de mémoire pour le service**
- **Compte de service LDAP créé lors de l’installation de l’agent Okta LDAP**

Nous recommandons néanmoins la configuration suivante :

- **256 Mo de mémoire pour le service**
- **Compte de service dédié avec autorisations d’accès au domaine**
- **Serveur distinct de celui du contrôleur de domaine (pouvant être partagé)**

L’agent Okta LDAP est compatible avec les principaux fournisseurs LDAP, notamment :

- **SunOne LDAP 5.2+, 6.*, 7.***
- **Oracle Internet Directory**
- **OpenLDAP**
- **OpenDJ**

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 7 950 clients, dont Adobe, Allergan, Chiquita, LinkedIn, MGM Resorts International et Western Union, font confiance à Okta pour travailler plus rapidement, booster 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/blog.