okta

Les avantages de la migration d'ADFS vers Okta

Okta France
Paris

paris@okta.com
01 85 64 08 80

L’authentification unique, un projet complexe à mettre en œuvre

Le taux d’adoption des applications cloud a grimpé en flèche ces dernières années, et des solutions telles que Salesforce.com, Box ou Office 365 ont désormais leur place dans l’environnement d’entreprise. Dès lors, de nombreuses organisations ont adopté, ou envisagent d’adopter, des politiques destinées à régir ces applications cloud.

Pour permettre à leurs utilisateurs d’accéder facilement à toutes les applications cloud et web sans devoir s’authentifier sur chacune d’elles, un grand nombre d’entreprises cherchent à mettre en place un système d’authentification unique, ou Single Sign-On (SSO). Leur objectif est de connecter l’ensemble de leurs applications cloud à une source unique et fiable, qui bien souvent n’est autre que Microsoft Active Directory. Elles sont nombreuses à conclure que la solution SSO idéale pour une authentification reposant sur l’AD est Active Directory Federation Services (ADFS), tout simplement parce que ce sont deux produits signés Microsoft.

Or, toutes les solutions d’intégration à Active Directory ne se valent pas, loin de là. Les équipes informatiques qui envisagent d’adopter ADFS doivent étudier tous les aspects de son implémentation en tant que solution SSO. Certes, la licence d’ADFS est gratuite, mais il existe divers coûts cachés comme la configuration, le support en continu et le matériel. De plus, il est important de prendre en considération les atouts que procure une solution complète de gestion des identités : provisioning, gestion des accès contextualisée pour les terminaux mobiles, centralisation du reporting, sans oublier la prise en charge préintégrée des milliers d’applications utilisées en entreprise à l’heure actuelle.

Ce livre blanc présente les principales caractéristiques d’une intégration Active Directory et d’un déploiement SSO réussis. Il détaille en outre les avantages d’une migration depuis une implémentation ADFS on-premise vers la solution avancée et 100 % cloud d’Okta.

Éléments essentiels d’une solution SSO efficace

La mise en place d’une solution d’authentification unique exige de tenir compte d’un très grand nombre d’éléments. Il est donc conseillé de s’attacher aux aspects essentiels, critiques pour la réussite du projet. Certains pourraient sembler insignifiants au départ, mais risquent de donner lieu à des problèmes significatifs à mesure que l’entreprise se développera et adoptera de nouvelles applications.

- **Intégration d’Active Directory**
  Si votre entreprise utilise Active Directory, votre solution SSO doit vous permettre d’en tirer parti pour que les applications cloud prenant en charge l’authentification unique soient toujours synchronisées avec ce service.

- **Intégration et prise en charge des applications**
  Lorsque vous envisagez d’implémenter une solution à l’échelle de l’entreprise, vous devez toujours tenir compte de sa capacité à prendre en charge l’ensemble des applications, actuelles et futures. Peut-être devez-vous intégrer seulement une ou deux applications cloud aujourd’hui, mais quelle sera la stratégie de votre entreprise à plus long terme ? En effet, à mesure que vos applications montent en charge, leurs exigences de configuration peuvent évoluer, obligeant l’administrateur à gérer chacune d’elles individuellement. Les fastidieuses opérations nécessaires pour les configurer une à une peuvent alors peser lourdement sur le budget et la charge de travail de l’équipe IT.

- **Haute disponibilité**
  Chaque arrêt qu'impose le déploiement d'une solution SSO se traduit par une immobilisation des utilisateurs. Certes, cet arrêt peut être planifié, mais il arrive qu'il soit inattendu. Il faut que le service SSO et le support associé soient suffisamment agiles pour fonctionner en continu, y compris lorsque le fournisseur modifie la configuration des applications.

  Qu'elle soit causée par vos serveurs ou par des modifications au niveau de l'application, toute indisponibilité entraîne une baisse de productivité et un ralentissement de l'activité dans son ensemble.

- **Provisioning des utilisateurs et des applications cloud**
  Le provisioning implique la création, l'actualisation et la suppression de l'accès à une application ou à d'autres ressources. Il faut en moyenne une demi-heure à un administrateur IT pour traiter chaque demande de provisioning ou de déprovisioning. Il faut ajouter à cela les appels passés au service d'assistance pour réinitialiser les mots de passe et configurer les différents terminaux des collaborateurs. En automatisant le provisioning et la gestion du cycle de vie des utilisateurs, la direction peut faire gagner un temps précieux à l'équipe informatique et aux autres départements, et leur éviter bien des désagréments.

- **Gestion des accès contextualisée pour les terminaux mobiles**
  La mobilité pourrait bien être le prochain levier de productivité de votre équipe, mais vous considérez peut-être l'aspect de la sécurité comme un frein. Votre solution SSO doit donc s'intégrer avec la solution de gestion des terminaux mobiles (MDM, Mobile Device Management) que vous utilisez déjà. Elle doit vous permettre de définir des politiques afin d'empêcher les terminaux non gérés d'accéder aux applications et aux données. Et pour plus de sécurité, elle devra prendre en charge l'authentification multifacteur (MFA).

- **Consolidation efficace des domaines**
  En cas de fusion-acquisition, les entreprises et leurs ressources sont intégrées à des degrés divers, ce qui peut constituer un défi au moment de consolider les domaines, les outils et les stratégies en matière de sécurité. L'adoption d'une approche cloud moderne de l'authentification unique peut accélérer et simplifier ce processus.

- **Journalisation et reporting**
  De nombreux organismes de réglementation exigent des pistes d'audit indiquant notamment à quels systèmes et applications les utilisateurs ont (ou ont eu) accès. De même, l'équipe informatique doit fournir des informations détaillées sur le déprovisioning des applications pour les collaborateurs qui quittent l'entreprise. La solution SSO idéale doit pouvoir collecter les informations d'usage pour permettre aux administrateurs IT de satisfaire rapidement les exigences de l'entreprise et du secteur en matière de rapports de conformité.

Utilisation d'Active Directory Federation Services (ADFS) comme solution SSO

Pour étendre les fonctionnalités d'identification d'Active Directory aux applications cloud à l'extérieur du pare-feu, les clients se tournent vers Microsoft Active Directory Federation Services (ADFS). Il s'agit d'une solution « gratuite », mais dont le fonctionnement exige divers composants matériels, des logiciels Microsoft supplémentaires et de nombreuses opérations de configuration et de maintenance. Les entreprises qui l'utilisent pour assurer une authentification unique sont confrontées à des exigences de configuration complexes et à une dépendance vis-à-vis d'autres ressources pour satisfaire les exigences minimales d'une solution SSO.

Composants d'ADFS

Si vous envisagez d'utiliser ADFS comme solution SSO, il est essentiel d'appréhender l'ensemble de ses composants sous-jacents. ADFS est constitué de trois composants : le serveur ADFS, le proxy FSP (Federation Service Proxy) installé entre la batterie de serveurs ADFS et les applications externes, et la base de données de configuration ADFS.[1]

ADFS a été développé en tant que toolkit, c'est-à-dire une fonctionnalité de Windows Server, et non comme une solution de bout en bout répondant aux besoins de l'authentification unique. S'ils peuvent faire preuve de flexibilité, les toolkits nécessitent toutefois de nombreux aménagements pour aboutir à une solution complète. Cela représente une charge de travail supplémentaire pour l'équipe IT.

En effet, il faut consacrer à chaque composant ADFS un développement personnalisé et un certain nombre d'opérations administratives pour comprendre, configurer et actualiser les connexions SSO vers les applications cloud cibles ; cela complique toute montée en capacité destinée à prendre en charge un grand nombre d'applications.

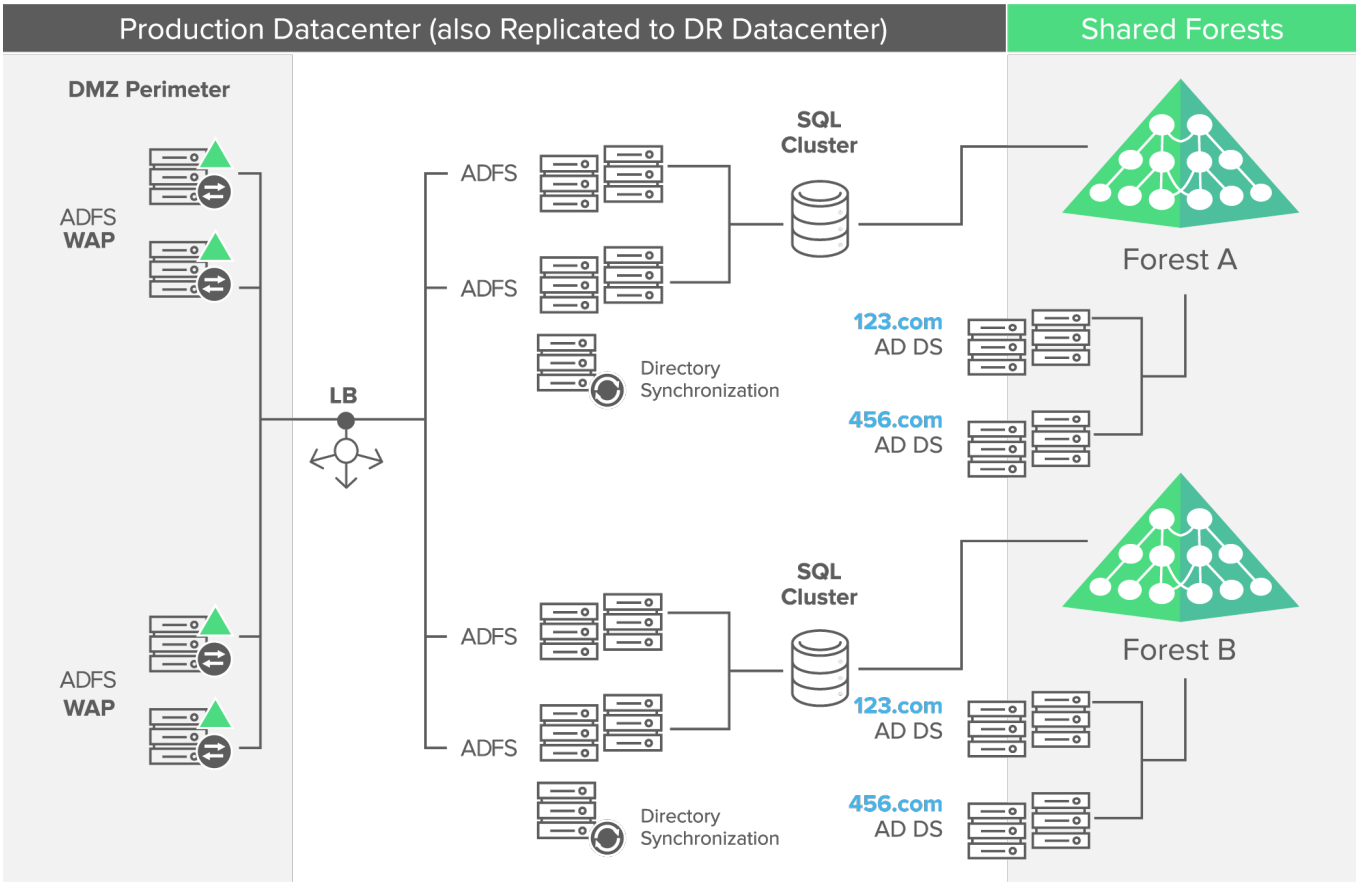

Figure 1. ADFS exige une infrastructure complexe on-premise pour s'intégrer avec Active Directory.

[1] Base de données SQL ou interne Windows

Personnalisation d'ADFS

La configuration d'ADFS comme solution SSO impose de définir des politiques d'authentification des utilisateurs et d'autorisation d'accès, mais aussi de générer des règles de revendication pour permettre l'authentification sur chaque application cloud. Ces diverses tâches nécessitent l'établissement de relations d'approbation entre ADFS et les applications cibles à l'aide d'un certificat SSL valide, rattaché au service ADFS. Dans un environnement de test, un certificat autosigné suffit, mais un certificat signé par un tiers est requis pour les environnements de production. Une fois ces relations d'approbation établies, des règles de revendication doivent être générées pour l'authentification sur l'application cloud cible. Auparavant, les administrateurs devaient rechercher manuellement les règles de revendication associées à chaque application, mais la situation s'est améliorée avec les modèles de politique de contrôle d'accès introduits dans ADFS 2016.

Il est possible que les règles de chaque application évoluent au fil du temps, invalidant votre intégration SSO. Vous devez donc opérer un suivi de ces changements et actualiser les politiques de contrôle d'accès en conséquence.

Une fois que vous avez constitué l'infrastructure ADFS et développé les règles de demande adaptées à chaque application cloud cible, vous devez encore déterminer combien d'utilisateurs se serviront de l'authentification unique pour y accéder. La plupart du temps, Azure Active Directory est utilisé à cet effet.

Authentification unique et provisioning

Si votre entreprise prévoit d'utiliser ADFS et de passer d'une application aujourd'hui à cinq ou six dans les trois ans à venir, vous devrez configurer chaque nouvelle application manuellement. Préparez-vous également à effectuer une maintenance régulière afin de vous assurer que chaque application reste connectée aux réseaux et à l'infrastructure de l'entreprise. Si le coût peut sembler raisonnable dans un premier temps, le nombre d'heures de travail nécessaires à chaque nouvelle application ne baissera pas, faute d'économie d'échelle.

Pour ajouter une application au système SSO à partir d'Active Directory via ADFS, il faut répliquer chaque utilisateur dans Azure Active Directory. Cette opération nécessite des licences Microsoft Enterprise Mobility + Security, la solution de Microsoft de gestion des identités et des accès sur Azure Active Directory.

Le provisioning et la gestion du cycle de vie avec ADFS exigent l'achat et la configuration d'un outil supplémentaire : Microsoft Identity Manager (anciennement Forefront Identity Manager).

Avantages de la migration d'ADFS vers Okta

Si vous avez déjà déployé ADFS dans votre entreprise, mais que vous souhaitez prendre en charge un plus grand nombre d'applications cloud et de fonctionnalités, la solution d'Okta vous offre plusieurs avantages :

Simplicité

Les fondateurs d'Okta ont étudié les fonctionnalités d'ADFS et en ont intégré les meilleurs aspects au sein d'une plateforme cloud évolutive. Okta gère l'intégralité du déploiement et de la disponibilité du service, tout en offrant une fiabilité supérieure aux infrastructures de fédération des identités on-premise, lourdes et complexes.

Ce service intégré de gestion des identités a été conçu pour permettre aux utilisateurs de se connecter en toute sécurité à leurs applications et ce, en tout lieu, à tout moment et sur n'importe quel terminal.

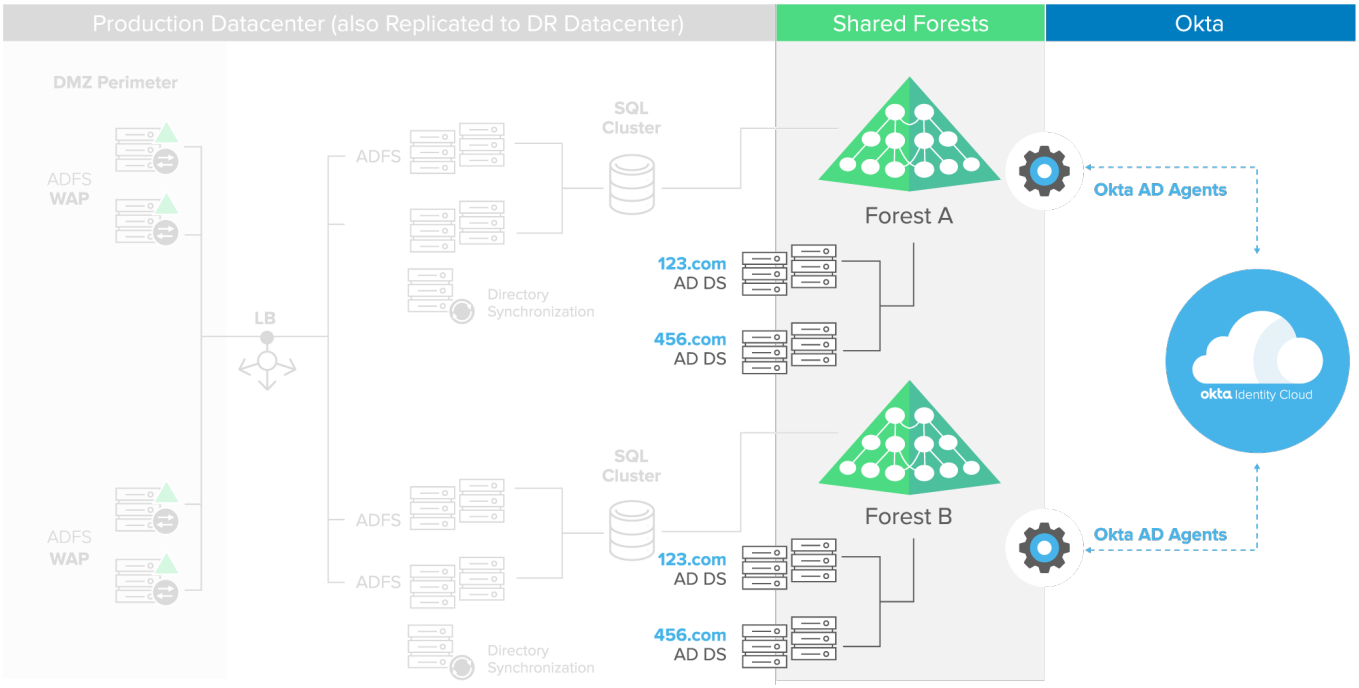

Figure 2. Les agents Active Directory légers et la plateforme cloud d'Okta assurent une intégration sécurisée à l'infrastructure Active Directory en place

Intégration d'Active Directory

La plateforme cloud d'Okta est une offre 100 % à la demande qui assure une intégration sécurisée avec votre infrastructure Active Directory en place.

Le service principal d'Okta est une solution multitenant dotée d'un agent Active Directory qui s'installe en local, sans nécessiter l'achat ni la gestion d'une appliance ou d'un serveur quelconque. L'agent léger d'Okta établit une connexion sécurisée, exclusivement sortante, via HTTPS, sans nécessiter de modification du pare-feu. Une fois qu'Okta a authentifié l'utilisateur sur l'application cloud, l'agent n'intervient plus. Tout le trafic se déroule entre l'utilisateur et l'application.

Okta prend en charge la délégation d'authentification, le provisioning et le déprovisioning, la synchronisation d'annuaire et la gestion des mots de passe Active Directory. Dès que des modifications se produisent au niveau d'Active Directory ou d'Okta, elles sont synchronisées de manière incrémentielle. Par exemple, lorsqu'un administrateur désactive un utilisateur dans Okta Universal Directory, cela entraîne instantanément la désactivation de cet utilisateur dans Active Directory.

Authentification unique avec intégration simple d'applications

Okta Integration Network est un vaste catalogue d'applications, infrastructures et terminaux préintégrés, à usage professionnel et personnel. Les utilisateurs finaux se connectent à un portail d'applications centralisé pour accéder facilement à celles qui leur ont été attribuées. Comme illustré sur la figure 3, la plateforme cloud intégrée d'Okta permet de déployer bien plus rapidement l'authentification unique depuis Active Directory, l'authentification fédérée et les intégrations applicatives étroites.

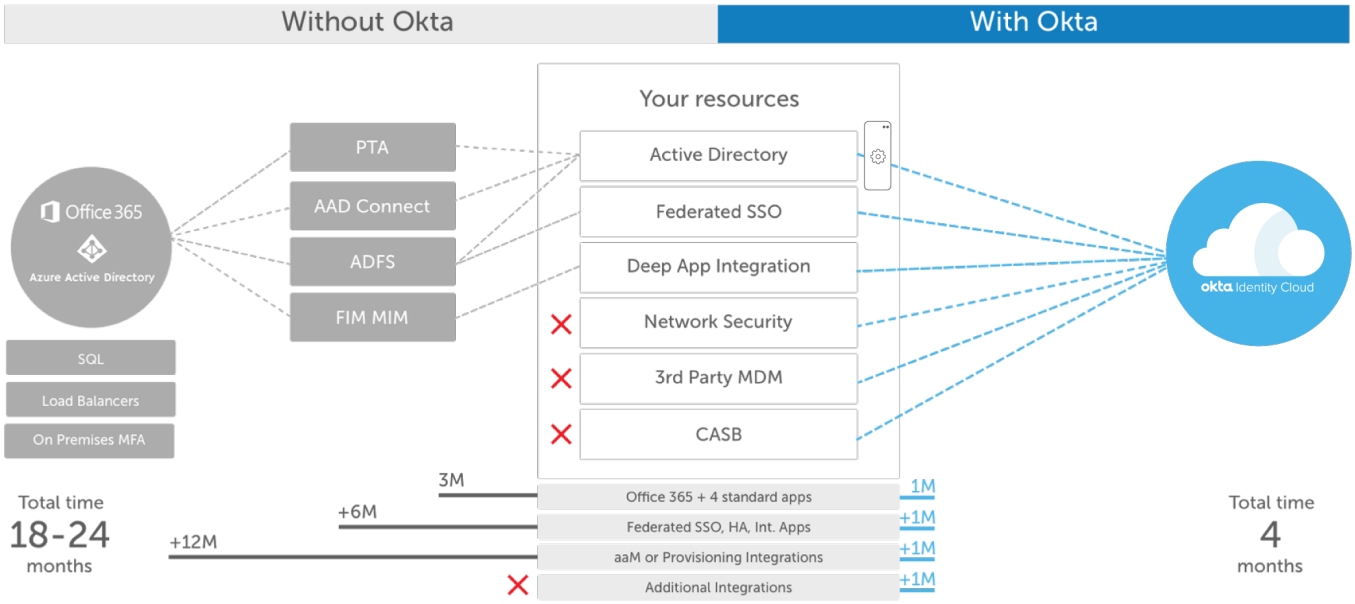

Figure 3. Okta simplifie et accélère l'authentification unique, le provisioning et l'intégration avec d'autres applications et services

Haute disponibilité

Une solution SSO ne devrait jamais être indisponible, même pour une maintenance planifiée. La plateforme cloud d'Okta est conçue pour assurer une disponibilité de 99,9 %, sans aucun arrêt planifié.[2] Multitenant, son architecture est redondante dans plusieurs zones de disponibilité et régions. Okta gère et supervise en permanence l'intégration des applications cloud, de sorte que vous ne devez pas vous soucier des modifications apportées aux applications sous-jacentes. Collaborateurs, partenaires et clients disposent ainsi d'un accès ininterrompu aux applications métier stratégiques.

Provisioning des utilisateurs et des applications

Okta prend en charge un système de gestion basé sur les groupes, capable de provisionner les utilisateurs sur un ensemble d'applications selon la fonction définie dans Active Directory. Si un collaborateur change de fonction dans l'entreprise, Okta actualise automatiquement les applications auxquelles il peut accéder conformément aux modifications apportées à son compte dans Active Directory. Lorsqu'il quitte l'entreprise, Okta détecte son changement de statut dans Active Directory et supprime automatiquement tous ses accès.

Okta offre un provisioning préintégré pour plus de 80 applications SaaS majeures. La plateforme permet le contrôle des identités et le provisioning d'utilisateurs à l'aide des attributs d'identité provenant de systèmes RH tels que Workday et SuccessFactors.

Gestion des accès contextualisée avec reconnaissance des terminaux

La gestion des accès contextualisée d'Okta réduit les risques en contrôlant la manière dont les utilisateurs et les terminaux accèdent aux ressources de l'entreprise. Grâce à des politiques associant l'authentification multifacteur adaptative et la fonctionnalité d'approbation Device Trust, Okta garantit que seuls les utilisateurs et les terminaux approuvés ont accès aux applications et données de l'entreprise. Okta vous donne les moyens d'exercer un contrôle d'accès granulaire sur des milliers d'applications, et les terminaux les plus courants. Grâce à l'authentification multifacteur adaptative d'Okta, l'administrateur peut choisir d'autoriser ou de refuser l'accès, d'imposer une authentification renforcée ou de limiter les droits d'accès d'un utilisateur à certaines applications. Ces décisions ne reposent pas simplement sur un mot de passe, une question de sécurité ou un jeton, mais sur l'identité de l'utilisateur, le réseau ou le pays depuis lequel il se connecte et le terminal qu'il utilise.

Authentification multifacteur pour ADFS

Les clients souhaitant continuer d'utiliser ADFS comme fournisseur d'identité pour certaines applications peuvent tout de même employer l'authentification multifacteur d'Okta. Ils bénéficieront ainsi d'une méthode d'authentification forte sans devoir se doter d'une infrastructure MFA supplémentaire on-premise.[3]

[2] https://www.okta.com/a-secure-reliable-service-you-can-trust/
[3] https://help.okta.com/en/prod/Content/Topics/integrations/adfs-okta-int.htm

Consolidation efficace des domaines

Grâce à Okta Universal Directory, les entreprises peuvent connecter un nombre illimité d'annuaires pour rendre leurs données disponibles sur le Web sans recourir à des approbations de forêts Active Directory, ni ouvrir de port sur leur pare-feu. Imaginons que votre environnement compte plusieurs domaines Active Directory : certains sont des domaines de confiance, d'autres non. Avec Okta, vous installez un agent Active Directory derrière le pare-feu (ou deux pour assurer une haute disponibilité intégrée) pour qu'il gère les annuaires depuis la console d'administration centralisée.

Journalisation et reporting

Le tableau de bord unifié d'Okta facilite la consultation du statut des utilisateurs, des accès et des applications, et permet de générer des rapports de conformité.

Toujours disponible et à jour

Nous avons mis au point Okta en tenant compte de la perspective de nos clients, et nous publions régulièrement des mises à jour ne nécessitant aucun arrêt de fonctionnement. Les utilisateurs finaux se connectent à un portail centralisé pour accéder aux applications qui leur ont été attribuées. Créer une solution de ce type avec ADFS nécessiterait des interventions manuelles en interne ou les services d'un sous-traitant, ce qui augmenterait les coûts.

Okta est une plateforme SaaS (Software-as-a-Service) qui offre à elle seule tous les avantages d'ADFS, ainsi que ceux des autres outils Microsoft nécessaires pour constituer une solution SSO complète.

Avantages financiers

Comme illustré sur la figure 4, ADFS entraîne différents coûts : installations matérielles et logicielles, maintenance, intégrations personnalisées, licences des machines virtuelles, et logiciels Enterprise Mobility + Security (EMS) et Microsoft Identity Manager (MIM). À cela s'ajoutent les éventuels coûts de perte de productivité, le temps d'effectuer l'installation et la mise en route.

L'installation, la maintenance et les intégrations personnalisées ont également un coût, même lorsqu'EMS est fourni gratuitement. Dans le cas des entreprises disposant déjà d'ADFS, il est possible qu'elles doivent encore payer les frais d'installation et de licence de MIM et d'EMS pour la prise en charge des fonctionnalités avancées.

Les frais de personnalisation très réduits et les coûts de licence limités d'Okta peuvent permettre aux entreprises une économie allant jusqu'à 60 % sur leur coût total de possession (TCO). Et comme l'intégration de nouvelles applications ne se répercute jamais sur le coût d'Okta, l'entreprise réalise des économies encore plus importantes à mesure qu'elle ajoute des applications cloud dans son infrastructure.

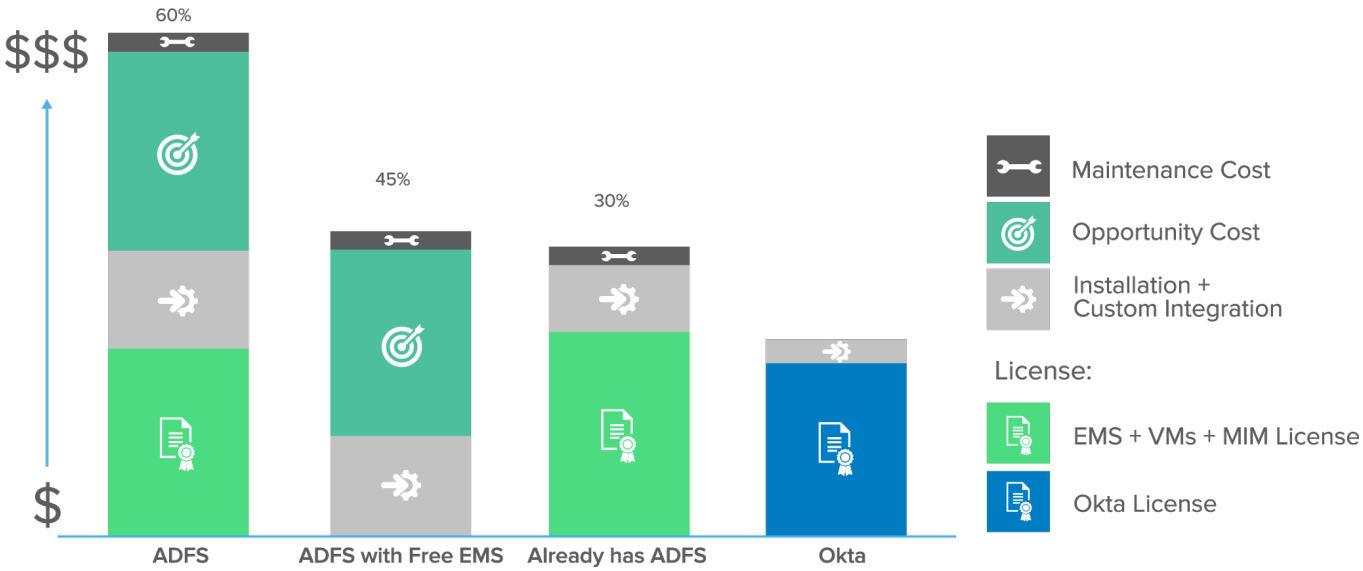

Figure 4. Coûts relatifs d'ADFS pour l'intégration d'une application.

Comparaison rapide entre Okta et ADFS

Caractéristiques	Approche Okta	Approche ADFS
Intégrations d'applications	Des milliers d'applications préintégrées Aucune nécessité de configurer et de gérer les intégrations d'applications	Les administrateurs IT créent et gèrent chaque intégration
Disponibilité	Solution multitenant à 100 % Toujours en service, sans temps d'arrêt Aucune modification de l'infrastructure AD requise	Implique des tâches de configuration, d'installation et de gestion Nécessite des mises à jour à mesure que les applications évoluent Disponibilité redondante Nécessite plusieurs serveurs (installation et basculement)
Gestion des accès et des utilisateurs	Contrôle des accès à toutes vos applications Association simplifiée de différents formats de nom d'utilisateur Ajout, modification et suppression simples de comptes utilisateurs et d'accès Importation directe depuis les groupes de sécurité Active Directory Configuration automatique pour toutes les applications intégrées	Obligation de créer et de gérer les attributs Active Directory personnalisés Nécessité d'apporter des modifications à chaque application Pas d'importation avec mise en correspondance des utilisateurs
Reporting	Tableau de bord avec statistiques globales sur l'état des utilisateurs et des applications Simplicité d'accès aux rapports sur les utilisateurs à des fins de conformité	Non disponible

Démarrer avec la version d'essai gratuite

Découvrez la simplicité d'implémentation d'Okta et commencez à déployer vos applications cloud en toute sécurité. Rendez-vous sur la page www.okta.com/freetrial pour accéder à la version d'essai gratuite.

Qui sommes-nous ?

Okta est un éditeur indépendant spécialisé dans la gestion et la protection des données d'identification, leader du secteur. La plateforme Okta Identity Cloud connecte et protège les collaborateurs des plus grandes entreprises au monde, en plus d'assurer une connexion sécurisée avec leurs partenaires, fournisseurs et clients. Grâce à son intégration avancée à plus de 6 500 applications, Okta Identity Cloud permet à n'importe quel utilisateur de se connecter facilement et en toute sécurité, tous terminaux confondus.

Des milliers de clients, dont 20th Century Fox, Adobe, Dish Networks, Experian, Flex, LinkedIn et News Corp, font confiance à Okta pour améliorer leur productivité, doper leur chiffre d'affaires et préserver leur sécurité.Grâce à Okta, ils peuvent accéder facilement et sans risque aux technologies dont ils ont besoin pour accomplir leurs missions stratégiques.

Pour en savoir plus, rendez-vous sur www.okta.com/fr