okta

Les huit principes de la gestion des accès à une infrastructure moderne

Okta France
Paris

paris@okta.com
01 85 64 08 80

Introduction

Les ressources qui composent votre infrastructure font partie des biens les plus sensibles et les plus précieux de votre réseau d'entreprise. Dès lors, le contrôle des accès aux serveurs et aux bases de données, qu'ils se trouvent dans le cloud ou sur site, est la priorité absolue des services IT et des équipes de sécurité. Si les méthodes traditionnelles mettent essentiellement l'accent sur la « protection des clés », les failles de sécurité dues au vol d'identifiants d'administration se succèdent malgré tout, année après année. Il est temps de passer à autre chose.

Ce livre blanc se penche sur les principales difficultés rencontrées pour sécuriser l'accès à l'infrastructure, et explique pourquoi nous devons revoir l'approche de notre secteur. À partir du modèle Zero Trust de Forrester, nous avons développé une méthodologie d'accès à l'infrastructure, qui repose sur huit principes indispensables à un environnement plus sécurisé et adapté à l'ère du cloud.

Les méthodes classiques manquent d'efficacité

Avec les identifiants statiques, la possession est la seule et unique règle ; il n'y a aucun lien direct avec identité

Les identifiants posent un sérieux problème, commun à tous les systèmes à base de mots de passe ou de clés, soit la majorité des systèmes actuels. Le principal obstacle à la sécurité de l'infrastructure réside dans le mécanisme de délivrance d'identifiants utilisés pour se connecter aux serveurs. N'importe quel utilisateur muni d'une clé ou d'un mot de passe de connexion valable peut en effet accéder au système, quel que soit le moyen employé pour se procurer cette information. Les identifiants dérobés deviennent alors un sésame entre les mains des pirates. De nombreux produits et pratiques ont vu le jour pour tenter de résoudre ce problème. Ces solutions consistent pour l'essentiel à protéger les informations d'identification par une couche de gestion afin d'empêcher le vol, la perte ou l'usage abusif. Même si elles constituent un progrès par rapport à l'autogestion, elles partent toujours du principe que c'est l'identifiant qui détient la clé d'accès au système, et non l'utilisateur.

Problèmes posés par les solutions classiques :

- **Identifiants statiques.** Même si les informations d'identification sont protégées par une couche de gestion, leurs propriétés intrinsèques demeurent inchangées. Plusieurs utilisateurs peuvent avoir le même identifiant, et l'identité ne fait l'objet d'aucune garantie ni d'aucun suivi.

Le problème des identifiants serveur

Caractère statique : Une fois générée, une clé est immuable. Cette propriété cryptographique ne la rend pas plus sûre pour autant. En effet, les informations d'identification sont souvent perdues, dérobées ou utilisées à mauvais escient.

Provisioning manuel : La suppression d'une clé (en cas de départ ou de mutation d'un collaborateur, par exemple) est un processus manuel. L'administrateur doit savoir à quel utilisateur correspondent les différents serveurs et les clés. Mais comment peut-il être sûr d'avoir totalement révoqué les droits d'accès d'une personne ?

Absence de lien avec l'identité : Même si l'exemple d'Alice et Bob prouve l'intérêt d'une infrastructure à clé privée (PKI), une clé privée n'est en revanche associée à aucun profil d'identité. La possession est la seule et unique règle, et n'importe qui peut s'approprier une clé.

Partage entre les systèmes : La divulgation des identifiants est en tout point identique à celle des mots de passe, mais les enjeux sont plus importants. Lorsque vous ajoutez une clé à un système, vous ne faites que cumuler des privilèges. Mais savez-vous combien il existe de clés donnant accès au système ?

- **Pénibilité d'utilisation.** Ces produits sont connus pour alourdir les opérations, surtout dans les environnements cloud élastiques extrêmement automatisés. Ils peuvent ainsi être un frein à l'automatisation, ce qui ralentit l'adoption d'une infrastructure cloud.
- **Expérience utilisateur médiocre.** Les processus hors bande de vérification des informations d'identification sont fastidieux pour les administrateurs système et connus pour leur lenteur. Gênés dans leur travail, les utilisateurs se tournent vers d'autres solutions, ce qui rend les contrôles de sécurité inefficaces.

En finir avec les clés grâce au Zero Trust

Le modèle de sécurité Zero Trust modifie notre approche de la sécurisation du réseau d'entreprise. L'accès ne relève pas d'une décision binaire exclusivement basée sur le réseau. Il s'inscrit dans une démarche contextuelle tenant compte d'informations dynamiques sur l'utilisateur, l'appareil, le réseau et le lieu. La méthode est simple : toujours vérifier avant de faire confiance.

L'initiative BeyondCorp de Google, exemple particulièrement réussi de déploiement Zero Trust, repose sur les principes suivants :

- **La connexion depuis un réseau spécifique ne doit pas déterminer les services accessibles.**
- **L'accès aux services est accordé en fonction de l'identité et du terminal de l'utilisateur.**
- **L'accès aux services doit être entièrement authentifié, autorisé et crypté.**

BeyondCorp a totalement bouleversé l'organisation de Google. Toutes les sociétés ne sont pas prêtes à faire face à de tels changements. C'est pourquoi Okta recommande une approche progressive. Le premier cas d'usage du Zero Trust doit être l'accès à l'infrastructure. Il ne concerne qu'une poignée de techniciens capables de gérer les changements d'architecture et de procédure, et nos clients se sont félicités de l'avoir implémenté.

Les huit principes de la gestion des accès à une infrastructure moderne

Aujourd'hui, toutes les entreprises, quelle que soit leur taille, devraient avoir accès à une meilleure architecture basée sur l'identité. Okta Identity Cloud est une plateforme de base spécialement conçue pour cette méthodologie, idéalement complétée par le produit Advanced Server Access.

Pour réorganiser l'accès à l'infrastructure, il est indispensable de rompre avec les méthodes et produits classiques. Chez Okta, nous avons aidé nos clients à mettre en place cette nouvelle méthodologie sur des déploiements d'infrastructure à grande échelle, avec des résultats significatifs et mesurables. De cette expérience concrète, nous avons retenu huit principes formant une architecture cohérente, adaptée à n'importe quelle entreprise moderne. Chacun de ces principes, axé sur les résultats, se concentre sur les besoins réels des entreprises et ce qu'elles attendent de leurs solutions de gestion des identités et des accès.

1 Automatisation des opérations manuelles

Le provisioning des contrôles d'accès est automatiquement assuré par la gestion des configurations

Les méthodes traditionnelles de gestion des accès peuvent être extrêmement lourdes. Avec l'essor des services cloud, elles montrent des signes de vieillissement. Prenons l'exemple d'un administrateur serveur qui quitte son entreprise. La désactivation de l'ensemble de ses comptes et identifiants est un véritable défi. C'est en optant pour l'automatisation, à n'importe quel niveau d'échelle et d'élasticité, que les entreprises tirent le meilleur parti de l'infrastructure cloud. Les produits de sécurité peuvent toutefois freiner l'adoption du cloud, car ils sont rarement compatibles avec l'automatisation.

Face à la multiplication des outils et processus DevOps, les contrôles de sécurité doivent changer de cap pour rester en phase avec les équipes en charge du développement et des opérations, qui créent et déploient l'« infrastructure as code ». Si l'infrastructure est correctement mise en place, les équipes peuvent configurer les environnements une fois pour toutes, puis passer le relais à l'automatisation. La configuration est essentielle, et mieux vaut qu'elle ait lieu dans un environnement de test. Une fois ce travail de préparation accompli, la mise à l'échelle peut s'opérer efficacement.

Point à retenir

Tout ce qui touche à Okta se présente sous forme d'API. L'adhésion, le provisioning et la configuration peuvent être entièrement automatisés, ce qui rend la solution incroyablement facile à utiliser.

S’agissant des contrôles d’accès, les comptes d’utilisateur et de groupe présents sur la machine sont automatisés. Les règles d’accès correspondantes sont alors appliquées lors du processus d’autorisation. Tout changement de statut d’un utilisateur, d’appartenance à un groupe ou de spécification d’une règle doit être enregistré en quasi-temps réel, pour que chaque demande puisse être évaluée sur la base des informations les plus récentes. Si un administrateur serveur quitte l’entreprise, le système d’enregistrement doit déclencher une série de workflows qui lui interdisent immédiatement tout accès.

2 Abandon des clés statiques au profit d’identifiants éphémères

Le champ d’application et la durée des identifiants de connexion sont limités pour n’autoriser qu’une seule utilisation

Le transfert des contrôles d’accès de la couche réseau vers la couche applicative, où des informations contextuelles plus dynamiques permettent de prendre de meilleures décisions, est l’un des principes de base du Zero Trust. Cette méthode rompt ainsi avec le schéma des politiques d’accès purement binaires de type « sur le réseau/en dehors du réseau ». Supposons à présent que vous vous donniez tout ce mal pour recueillir des informations contextuelles et les appliquer en temps réel dans le seul but de fournir à l’utilisateur un identifiant statique partagé. Ce serait du gaspillage. Pour adhérer à la politique d’accès définie, le mécanisme de délivrance d’identifiants doit être parfaitement adapté.

Pour réduire le risque lié aux informations d’identification, mieux vaut limiter leur valeur que de les protéger par un plan de gestion. Un identifiant dont la durée et le champ d’application sont limités n’a en soi aucune valeur, en dehors de ce délai et de ce périmètre.

Les technologies modernes offrent davantage de souplesse en termes de délivrance des identifiants, dont ils permettent de contrôler l’étendue et la durée. Pour créer des identifiants de connexion à la demande parfaitement conformes avec la politique d’accès, privilégiez une architecture de certificats client. Le champ d’application est le contexte environnant — un utilisateur se servant d’un appareil pour accéder à un serveur. Le certificat n’est créé qu’une fois l’utilisateur authentifié et autorisé, et son délai d’expiration est tellement court qu’il ne peut être employé qu’une seule fois.

Point à retenir

L'exploitation de l'infrastructure PKI de bout en bout pour assurer l'authentification des certificats client est loin d'être une tâche anodine. Okta la simplifie grâce à Advanced Server Access, qui pilote en arrière-plan une autorité de certification programmable. Les serveurs reposant sur Okta sont configurés pour approuver les certificats signés, qui sont remis aux utilisateurs sur demande.

3 Abandon des comptes partagés au profit des identités des utilisateurs

Les comptes système sont directement attribuables à une source utilisateur via un fournisseur d'identités

Avec les produits de gestion des accès classiques, l'administrateur système a des privilèges spécifiques. L'utilisation de comptes partagés verrouillés individuellement est une pratique courante. Le but est de respecter le principe du moindre privilège et de limiter les activités possibles pour un utilisateur sur chaque système. Si les résultats obtenus en suivant ce principe cadrent parfaitement avec le modèle Zero Trust, l'utilisation de comptes séparés est en revanche contraire à la notion de périmètre constitué par les individus.

Les politiques d'accès contextualisées définissent de manière explicite les utilisateurs auxquels l'accès doit être accordé ou refusé. Pour que ces politiques puissent être appliquées efficacement, les contrôles d'accès doivent être directement liés à une identité au sein de votre système d'enregistrement, ce qui évite d'utiliser des comptes partagés.

Ce modèle ne peut être mis en place qu'avec une couche d'identités robuste, répercutée sur les systèmes en aval via l'automatisation. Les comptes présents sur la machine sont directement liés à ceux du fournisseur d'identités, et les changements sont automatiquement enregistrés.

Point à retenir

Convaincu de l'intérêt des contrôles d'accès basés sur l'identité, Okta étend les workflows d'authentification directement depuis le compte de l'utilisateur, dont le provisioning est ensuite assuré en aval des serveurs. Toutes les activités sont attribuables à l'utilisateur, ce qui permet d'obtenir un journal d'audit clair et cohérent.

4 Abandon du principe d'élévation des privilèges au profit de contrôles d'accès basés sur les rôles

Les autorisations de niveau système font partie des fonctions du rôle de l'utilisateur et sont accordées lors de l'authentification initiale

Les comptes partagés, qui délèguent des privilèges pour des activités spécifiques sur la machine, font office de « rails de guidage » pour les chemins et commandes système. Autre forme d'application du principe du moindre privilège, ce modèle d'élévation est une pratique très courante. Avec cette approche, l'application des règles pose problème. En effet, dans la mesure où le plan de gestion se trouve en local sur le système, il peut être extrêmement difficile de savoir avec précision quels utilisateurs doivent avoir tel ou tel droit sur une machine donnée. La gestion de listes blanches et de listes noires est fastidieuse et difficile à suivre, quel que soit le niveau d'échelle.

Point à retenir

Okta simplifie le respect des politiques en offrant un point de contrôle central où l'appartenance aux groupes est transmise aux serveurs en aval. La constitution de listes blanches et de listes noires au niveau des commandes devient alors une fonction directe du rôle de l'utilisateur, et la politique est gérée au niveau de la couche d'accès.

Plus vous pouvez extraire et appliquer de règles à partir de systèmes locaux, plus elles sont faciles à respecter via un point de contrôle central. Le passage à un système de contrôle d'accès basé sur l'identité implique l'octroi explicite d'autorisations au rôle de l'utilisateur, qui est susceptible d'évoluer. Prenons l'exemple d'un membre de l'équipe TechOps auxquels des privilèges « sudo » seraient accordés sur un serveur Linux, tandis qu'un membre de l'équipe DataScience ne serait autorisé qu'à exécuter des requêtes SQL en lecture seule sur un serveur de bases de données.

Avec cette approche, les rôles font partie des fonctions de l'utilisateur et de l'appartenance aux groupes dans le fournisseur d'identités. Une fois l'utilisateur connecté, les systèmes doivent pouvoir déterminer son rôle et lui accorder les autorisations locales correspondantes. Il s'agit d'une fonction d'automatisation, qui relève aussi du modèle d'autorisation du système local.

5 Abandon des interfaces d'annuaire au profit des comptes locaux

Le provisioning et le déprovisioning des comptes système ont lieu directement sur la machine

Les serveurs ont leurs propres systèmes de comptes et de fichiers locaux, et peuvent être difficiles à lier à un système d'enregistrement. Il n'est pas rare d'exécuter une interface d'annuaire sur la machine, qui est alors synchronisée avec un fournisseur d'identités sous-jacent. Sous Linux, un module PAM LDAP est utilisé à cet effet. La création et l'exécution de ces interfaces, qui tombent rapidement en panne à grande échelle, sont un vrai casse-tête. Le problème risque alors très vite de se déplacer pour se situer au niveau des systèmes distribués, à la cohérence incertaine.

Le provisioning direct des comptes locaux depuis le fournisseur d'identités constitue une approche plus efficace. Avec cette méthode, il est en effet inutile d'exécuter une interface d'annuaire sur la machine, ce qui permet d'établir un lien plus direct avec le principe du contrôle d'accès basé sur les rôles, où les autorisations système sont associées au compte local.

Les interfaces d'annuaire sont remplacées par un agent local ayant le contrôle des comptes locaux, et par une liaison directe avec le système d'enregistrement. Cet agent peut enregistrer les changements de statut d'utilisateur ou d'appartenance à un groupe, et créer, mettre à jour ou supprimer des comptes locaux en conséquence.

Point à retenir

Okta gère les comptes d'utilisateur et de groupe locaux présents sur une machine via un agent serveur, et automatise entièrement la gestion du cycle de vie des comptes utilisateurs. Si un utilisateur est désactivé dans Okta, son compte local est lui aussi instantanément désactivé. Vous n'avez donc pas à vous demander à quels serveurs l'utilisateur avait accès.

6 Abandon des réseaux VPN au profit des bastions

Les systèmes privés sont protégés via une architecture de bastions avec contrôles d'accès à la couche 7

La sécurisation des environnements d'infrastructure est traditionnellement un exercice de protection du réseau. À l'ère du cloud, le périmètre réseau a cependant été délaissé au profit du modèle Zero Trust. L'initiative BeyondCorp de Google, qui s'est traduite par l'abandon des réseaux VPN jusqu'alors utilisés par ses collaborateurs partout dans le monde, en est l'un des exemples les plus marquants.

Si la segmentation du réseau est une mesure de défense en profondeur vivement conseillée, elle doit néanmoins rester indépendante du mécanisme de contrôle des accès. L'utilisation de bastions légers est une approche cloud native plus efficace de la protection des ressources de l'infrastructure privée. Les utilisateurs s'authentifient sur ces hôtes, qu'ils franchissent pour atteindre le système cible. Correctement configurée, une architecture de bastions permet de se passer de réseau VPN, en étendant des workflows d'authentification fluide depuis n'importe quel emplacement.

La meilleure approche consiste à configurer des systèmes privés au niveau de la couche réseau afin d'accéder aux connexions entrantes via les hôtes bastions. Il faut ensuite déployer les bastions sur l'Internet public, généralement sous forme de groupe d'instances pour plus de disponibilité. Une fois l'utilisateur authentifié, plusieurs méthodes lui permettent d'atteindre le système cible, la redirection des ports étant l'une des plus répandues. Elle présente toutefois un risque dû au décryptage du trafic. Okta recommande de rediriger le trafic via le bastion, afin de préserver le canal crypté jusqu'au système cible.

Point à retenir

Les bastions occupent une place de choix aux yeux d'Okta, qui permet de configurer les machines cibles avec des hôtes bastions où l'authentification et le transport sont parfaitement fluides.

7 Abandon des processus de vérification au profit de l'authentification unique (SSO)

Les workflows de connexion basés sur l'identité sont natifs pour le protocole de transport sous-jacent

Avec un modèle de compte partagé reposant sur des identifiants statiques, le workflow le plus répandu consiste à authentifier l'utilisateur, à vérifier l'identifiant partagé à utiliser, puis à s'en servir pour connecter l'utilisateur au système. Ce processus hors bande peut être long et fastidieux pour les administrateurs système, surtout en cas d'incident. De par leur profil très technique, ces professionnels ont alors tendance à contourner les contrôles de sécurité qui les empêchent de travailler.

L'authentification unique (SSO) est devenue monnaie courante pour accéder aux applications métier. Elle repose sur les mêmes principes et offre une expérience tout aussi fluide au niveau de la couche d'infrastructure.

Grâce aux ressources de l'infrastructure, cette méthode consiste à introduire des workflows d'authentification dans le protocole de transport sous-jacent. Lorsqu'un utilisateur se connecte à un serveur Linux via SSH, un workflow d'authentification soutenu par le fournisseur d'identités est initié. Si une politique d'authentification multifacteur a été définie, elle est intégrée au workflow.

Point à retenir

Okta a conçu le produit Advanced Server Access afin d'assurer une interface directe avec vos outils locaux, compatible avec les protocoles SSH et RDP pour les serveurs Linux et Windows respectivement. L'authentification et l'autorisation se déroulent en arrière-plan, garantissant ainsi un mode de contrôle d'accès plus sûr, sans compromettre l'expérience utilisateur.

8 Abandon des enregistrements de session au profit de journaux structurés

Les événements d'audit sont enregistrés dans des journaux structurés indexables et alertables

La criminalistique, dont la moindre tâche administrative exécutée sur un système doit être enregistrée pour une lecture ultérieure, est un exemple type d'activité soumise à des règles de conformité. Si l'accessibilité de ces informations présente des avantages en termes de sécurité, ils sont largement minorés par la lourdeur d'enregistrement, de stockage et de diffusion de ces données.

Du point de vue de la sécurité, les entreprises ont besoin de savoir avec précision qui a accès à tel ou tel système, depuis quel appareil et à quel moment — et ce qu'il se passe ensuite. Pour tirer des enseignements exploitables de ces données, il est préférable de les enregistrer et de les présenter sous forme de journal structuré via un enregistrement de session. Cette méthode permet en effet d'indexer et de rechercher rapidement des informations, et d'émettre des alertes.

Un tel niveau de fonctionnalités d'audit s'obtient essentiellement de deux manières : via une passerelle qui permet de rediriger l'ensemble du trafic, ou via un agent exécutant un processus d'enregistrement. L'une comme l'autre produisent des journaux structurés pouvant être remis à un service de journalisation ou SIEM pour un examen supplémentaire. Dans les deux cas, le traitement est asynchrone, afin de ne pas interférer avec la session utilisateur.

Point à retenir

Okta exécute un agent serveur léger sur chaque machine, afin d'enregistrer les activités de connexion sous forme d'écritures de journal pouvant être analysées via le tableau de bord ou un service de gestion des événements de sécurité (SIEM) tiers.

Qui sommes-nous ?

Okta est une solution de pointe qui aide les entreprises à gérer et sécuriser les identités de milliers de clients et de millions de collaborateurs. Notre approche extrêmement complète de la sécurité va des pratiques de recrutement à l'architecture et au développement du logiciel sur lequel repose Okta, sans oublier les stratégies et opérations de data center qui nous permettent d'offrir un service d'exception. Outre l'innovation produit et une approche reconnue de l'assistance client, la solution d'Okta s'appuie sur une équipe de cybersécurité hors pair, qui ne ménage pas ses efforts pour offrir la plateforme la plus sûre du marché aux utilisateurs et aux informations qui leur sont confiées.

Pour en savoir plus, consultez la page www.okta.com/education.

Nous utilisons des méthodes de gestion des clés de cryptage à la pointe de la technologie pour sécuriser les données clients. La protection de ces données est certifiée conforme aux réglementations les plus strictes : RGPD, FedRAMP, NIST SP 800-53, HIPAA et ISO 27001. L'entreprise protège les données utilisateur de multinationales comme ENGIE, Eurostar, Scottish Gas Networks et News Corp, mais aussi d'entreprises intervenant dans des secteurs ultra-réglementés, comme American Express, le ministère américain de la Justice et le Nasdaq.