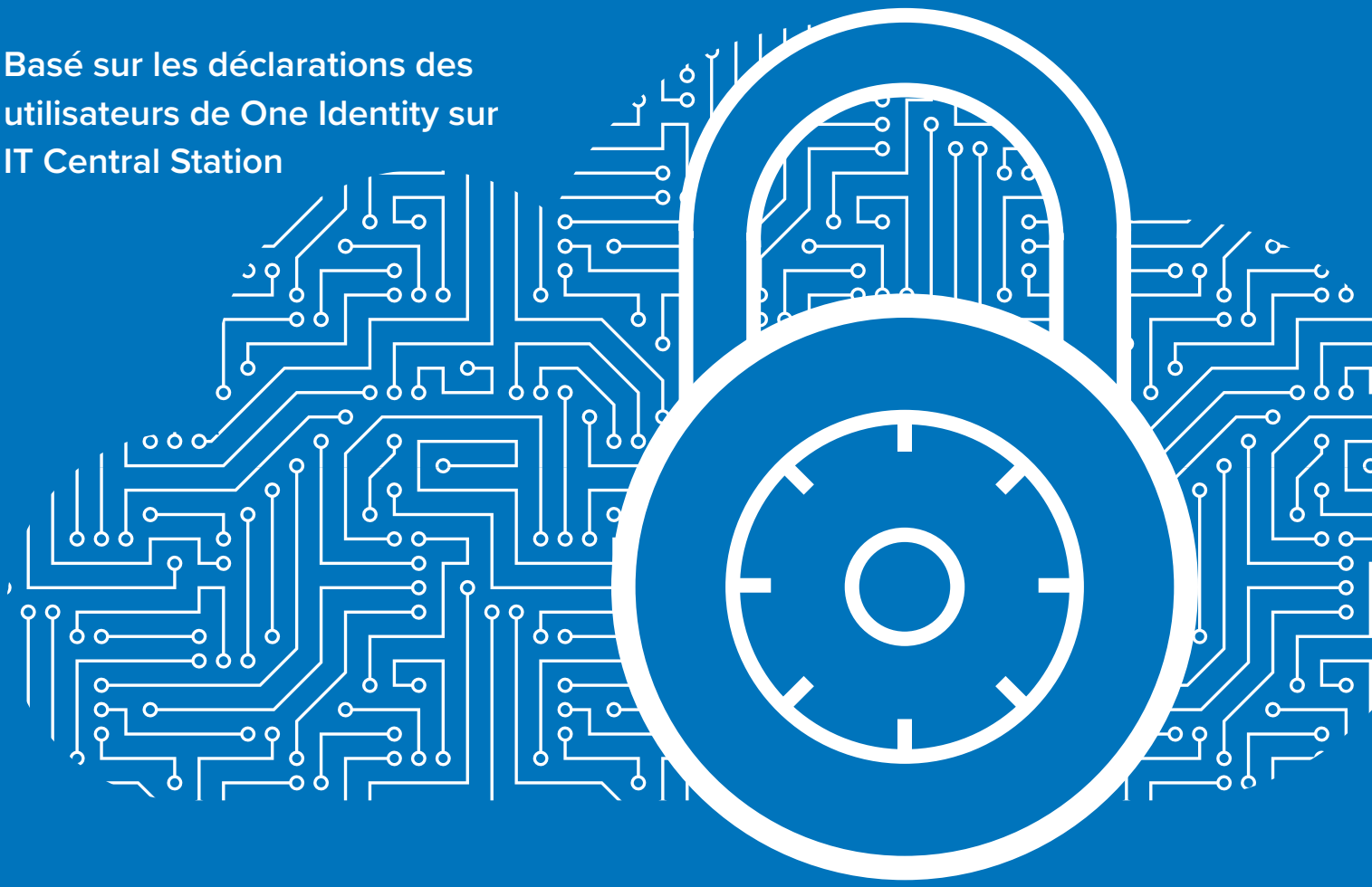
Rapport PeerPaper™ 2021

10 bonnes pratiques pour gérer et sécuriser Microsoft Active Directory dans un monde informatique en mouvement

Basé sur les déclarations des utilisateurs de One Identity sur IT Central Station



IT Central Station
Unbiased reviews from the tech community

CSO
FROM IDG

RÉSUMÉ

La plupart des programmes de gestion des accès et des identités (IAM, Identity and Access Management) reposent sur Microsoft Active Directory (AD) et Azure AD (AAD) en toute confiance. Néanmoins, alors que les environnements d'IAM migrent vers le Cloud, se modernisent et adoptent le concept de gouvernance, les responsables informatiques sont tenus de pallier les carences de sécurité et d'efficacité natives d'AD. C'est pourquoi ils recherchent des solutions pour démultiplier les fonctions d'AD qui sont parfois insuffisantes. Des entreprises de premier plan définissent des approches concrètes pour sécuriser et gérer les environnements AD hybrides au fur et à mesure que la gouvernance des identités et des comptes évolue avec l'adoption du Cloud, entre autres. À travers cette revue, nous vous proposons une plongée dans ces nouvelles bonnes pratiques basées sur les expériences réelles des utilisateurs de la solution One Identity Active Roles – selon leurs déclarations sur IT Central Station.

TABLE DES MATIÈRES

INTRODUCTION

La sécurité est une préoccupation de premier plan pour tous les RSSI et les responsables informatiques. Par conséquent, la mise en place d'un cadre sûr et maîtrisé pour la gestion des accès et des identités (IAM, Identity and Access Management) est un pilier essentiel des stratégies de cybersécurité. En effet, les cadres de sécurité courants, comme ceux édités par le NIST, considèrent que c'est à travers un contrôle efficace de l'identité des utilisateurs et de leurs privilèges d'accès qu'un grand nombre de contre-mesures peuvent être appliquées. Dans ce domaine, Microsoft Active Directory (AD) et Azure AD (AAD) restent au cœur de la plupart des programmes d'IAM.

Toutefois, les responsables de la sécurité rencontrent parfois des difficultés avec AD, car l'environnement informatique se transforme pour devenir hybride et de plus en plus complexe. Ils cherchent à accroître les fonctionnalités limitées et inefficaces des outils AD natifs. Des solutions innovantes ont émergé à travers des approches concrètes, permettant de prolonger la viabilité d'AD à mesure que la gouvernance des identités évolue avec l'adoption progressive du Cloud.

Sauf mention contraire, l'ensemble des sociétés figurant dans ce document comptent plus de 10 000 salariés.

Gestion des accès et des identités dans un monde de sécurité et d'informatique changeant

Alors que les organisations déplacent leurs ressources multimédias vers le Cloud et modernisent leurs opérations, elles se trouvent confrontées à de nouveaux défis d'IAM. Les cas d'utilisation de One Identity Active Roles montrent comment les gestionnaires d'identités adaptent l'IAM au Cloud. Par exemple, un responsable informatique des services de sécurité d'une firme d'aéronautique et de défense utilise Active Roles pour ses services Active Directory locaux. Néanmoins, les serveurs eux-mêmes sont hébergés dans Azure.

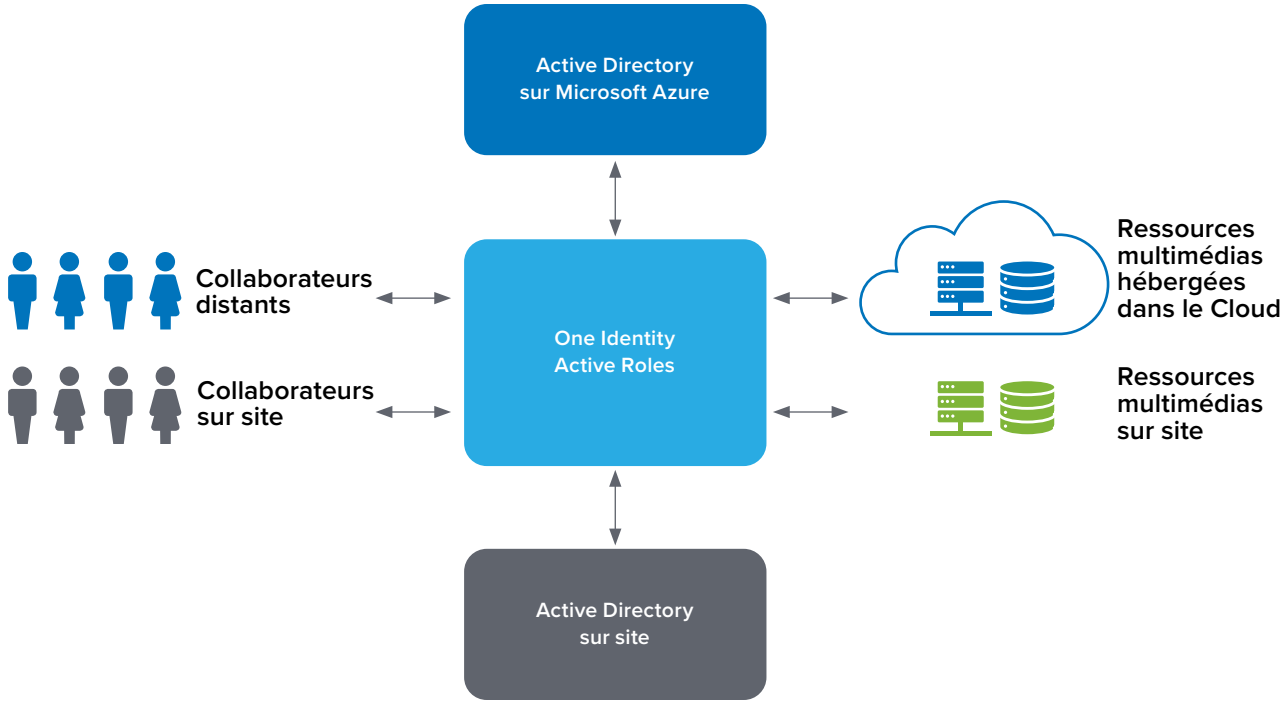


Figure 1 – La migration vers le Cloud entraîne la nécessité de centraliser l'IAM afin de gérer l'accès aux ressources multimédia, peu importe où elles sont hébergées.

Une analyste d'affaires senior à l'Université George Washington utilise Active Roles afin de gérer plusieurs aspects d'AD, y compris la fonction centrale de création de comptes. « Nous exposons les propriétés des groupes d'utilisateurs Azure AD natifs afin de contribuer à l'amélioration de la prise en charge. Nous provisionnons et déprovisionnons des applications, et nous créons les rapports nécessaires. » explique-t-elle. La figure 1 correspond à une architecture de référence simple qui illustre la façon dont les ressources multimédia et les instances AD sont désormais distribuées entre hébergement dans le Cloud et sur site.

Problèmes avec AD et les autres systèmes existants

Le passage vers des solutions d'IAM augmentées (comme Active Roles) est motivé par les problèmes auxquels font face les utilisateurs d'AD et d'autres systèmes existants, mais aussi par le besoin combler les lacunes des outils AD natifs. Un responsable technique de la sécurité chez Liberty Global, un opérateur de télécommunications, déclare : « Si nous avons opté pour cette solution [Active Roles] – et cette décision remonte à 10 ou 15 ans – c'est en raison de la délégation Active Directory. Nous ne pouvions pas autoriser tous les utilisateurs à accéder de façon native à nos instances Active Directory. Nous avons pensé à utiliser la solution Microsoft, car c'est un outil gratuit et intégré dont nous sommes déjà équipés. Mais après avoir dépassé une certaine taille, nous nous sommes rendu compte qu'il ne suffisait plus. Les fonctionnalités de gestion AD et AAD de cette solution sont vraiment performantes. Elles sont bien meilleures que les outils natifs. »

Le responsable de la sécurité des informations d'une entreprise manufacturière de plus de 5 000 salariés déclare : « Initialement, nous utilisions les outils natifs Microsoft. Nous sommes passés à Active Roles, car les outils natifs Microsoft permettaient uniquement de gérer les composants clés sans offrir toutes les fonctions nécessaires au provisioning, au déprovisioning, au contrôle des accès basé sur les rôles et à l'historique des modifications. Microsoft ne propose pas l'approche de proxy permettant de gérer Active Directory de manière centralisée. Avec Microsoft, Active Directory est distribué par nature, tandis qu'Active Roles centralise les éléments. »

« Avant Active Roles, nous utilisions une solution de rédaction de scripts en interne », raconte un responsable informatique senior du Conseil scolaire du district de Toronto. « Nous avons changé de solution pour bénéficier d'une meilleure prise en charge, mais aussi pour mettre un terme à la rédaction manuelle et répétée de scripts pour les builds, parfois obsolètes et incompatibles. Ainsi, nous disposons d'un produit d'avenir pour lequel nous bénéficions d'un support adapté. En comparaison, nous n'utilisons quasiment pas les outils Microsoft natifs ; les connecteurs pour la fédération des utilisateurs et la synchronisation avec d'autres solutions sont non-existants. »

Pour l'analyste d'affaires senior de l'Université George Washington, Active Roles a permis à son équipe d'éliminer Oracle Identity Manager (OIM). Elle raconte : « Malheureusement, OIM a été mis en place il y a environ neuf ans, mais il s'est avéré que son cycle de vie était trop long pour intégrer des applications et passer au provisioning basé sur les rôles. C'est pourquoi nous ne sommes jamais allés au-delà de la phase initiale. Nous avons collecté toutes les informations de ce système et nous avons créé, si je puis dire, une toute nouvelle instance Active Roles pour les gérer. Nous devions redémarrer OIM dès que nous avions un problème. Ce n'est plus le cas aujourd'hui depuis que nous sommes passés à Active Roles. Nous n'avons enregistré aucun ticket pour redémarrage en plus d'un an, depuis que nous avons migré. »

Nous avons changé de solution pour bénéficier d'une meilleure prise en charge, mais aussi pour mettre un terme à la rédaction manuelle et répétée de scripts pour les builds, parfois obsolètes et incompatibles.

Renforcer la sécurité avec une meilleure gestion des accès et des identités

Une solution d'IAM plus performante – c'est-à-dire plus sûre, plus facile à gérer et plus efficace – est un élément clé pour améliorer la posture de sécurité globale d'une organisation et établir une approche solide envers la gouvernance et l'administration AD/AAD. Toutefois, la mise en œuvre de cette idée n'est pas toujours simple. Nous avons dégagé dix recommandations d'IAM pour développer une approche plus robuste, sûre et efficace. La solution d'IAM doit être en mesure d'empêcher les utilisateurs d'effectuer des modifications non autorisées. Il se peut que le fardeau administratif soit élevé ; les utilisateurs privilégient ainsi des solutions d'automatisation ainsi que l'intégration à d'autres systèmes. Par ailleurs, la délégation du contrôle est un aspect essentiel dans une solution d'IAM efficace. Idéalement, les solutions d'IAM doivent également permettre d'adopter un modèle de moindres privilèges pour le contrôle des accès, ouvrant la voie à la sécurité Zero-Trust (zéro confiance).

1. Réduire les modifications non autorisées pour limiter les risques

Dans le cadre du contrôle des accès et des identités, les modifications non autorisées sont une source d'exposition aux risques, car des utilisateurs inconnus peuvent accéder à des données sans que les administrateurs ne le sachent. En s'ajoutant à AD, Active Roles contribue à limiter l'impact de tels comportements. Comme l'explique le responsable de la sécurité des informations pour une entreprise manufacturière : « Étant donné que nous pouvons supprimer les droits d'administration principaux, nous recensons moins de modifications non contrôlées. De fait, nous observons globalement une meilleure disponibilité du service et moins de détections lors des audits. » Et d'ajouter : « C'est incontestable, la solution Active Roles réduit les risques auxquels s'expose notre organisation. Les risques ont été réduits de manière considérable, car nous évitons de modifier la sécurité native d'Active Directory et nous contrôlons les accès en fonction de rôles afin de gérer Active Directory directement via l'application. »

> **Nous avons choisi d'adopter cette solution, car nous avions besoin de verrouiller le système et de le rendre plus sûr.**

Le responsable technique de la sécurité chez Liberty Global met le sujet en perspective lorsqu'il déclare : « Le retour sur investissement d'Active Roles est observable dans l'atténuation des risques, notamment l'élimination du risque d'accès non autorisé et du risque de polluer Active Directory. » Il poursuit : « En revanche, nous prenons le risque que des personnes obtiennent un accès qu'elles ne devraient pas avoir. Il se peut que plusieurs comptes soient créés pour un même but. »

« Les choses se sont améliorées, car nous ne voyons plus de 'modifications sauvages' apportées à AD sans que nous le sachions » remarque un analyste des identités senior pour une entreprise fabriquant des biens de consommation. « Les utilisateurs remplissent les mêmes missions, mais nous pouvons désormais nous assurer qu'ils ne modifient rien par inadvertance. Auparavant, les utilisateurs pouvaient mettre à jour AD directement. Nous limitons désormais ce risque en utilisant Active Roles comme intermédiaire. Nous avons choisi d'adopter cette solution, car nous avions besoin de verrouiller le système et de le rendre plus sûr. »

2. Intégrer l'IAM aux systèmes de sécurité

L'IAM est un domaine de l'informatique et de la sécurité qui prend tout son sens lorsqu'il peut s'intégrer facilement avec les autres systèmes de l'organisation. Par exemple, pour le responsable de la sécurité des informations pour une entreprise manufacturière, cela signifie qu'il peut utiliser Active Roles pour provisionner des objets Active Directory. En même temps, il l'utilise pour se connecter, via le service de synchronisation Active Roles, à un système de RH afin de provisionner ou de déprovisionner les collaborateurs. Il raconte : « En général, nous l'utilisons pour provisionner tous les objets – groupes de sécurité et objets informatiques – de manière déléguée. Le serveur Active Roles permet de modifier la sécurité d'Active Directory afin de déléguer l'accès à différentes équipes informatiques pour le provisioning, sans toucher à la sécurité existante d'Active Directory. »

> **...nous l'utilisons pour provisionner tous les objets – groupes de sécurité et objets informatiques – de manière déléguée.**

Le responsable informatique de la société aéronautique utilise l'interface PowerShell d'Active Roles pour laisser d'autres parties de son environnement et d'autres applications (susceptibles de communiquer avec Active Roles) effectuer des modifications au sein d'Active Directory à l'aide des commandes PowerShell. Il note : « Nous pouvons appliquer les mêmes principes que nos droits de sécurité afin qu'ils soient obligés d'utiliser Active Roles, réduisant ainsi les risques du point de vue de la sécurité. »

3. Déléguer pour renforcer la sécurité

Les membres d'IT Central Station ont parlé de leur préférence : ils souhaitent être en mesure de déléguer les accès aux processus AD. Par exemple, BeClever IT Solutions, une entreprise de services technologiques, travaille avec un client qui rencontre des problèmes d'autorisations et de délégation. Dans cette entreprise, de nombreux utilisateurs doivent mener des activités d'administration dans AD. Ce phénomène est problématique eu égard aux potentielles erreurs qu'ils peuvent commettre. Désormais, avec Active Roles, ils peuvent se passer d'administrateurs de domaine et conserver leurs utilisateurs habituels. Ils peuvent pré-remplir certains champs avec des valeurs données.

Il déclare : « C'est fantastique pour eux, car certains salariés sont de simples techniciens informatiques peu qualifiés qui n'ont aucune connaissance des fonctions avancées d'AD. Cette solution nous permet d'éliminer des tâches informatiques fastidieuses lors du provisioning. » De même, le responsable de la sécurité des informations pour une entreprise manufacturière note : « Avec l'accès délégué à Active Directory, nous pouvons révoquer un grand nombre de droits d'administration. Nous pouvons davantage contrôler nos systèmes et évoluer dans un environnement plus sûr qu'auparavant. »

4. Adopter le modèle de moindres privilèges et la sécurité Zero-Trust

Certains utilisateurs d'Active Roles sur IT Central Station tirent profit de la solution pour implémenter un modèle de gestion des accès à moindres privilèges. Cette approche prend de l'ampleur, notamment avec la disparition du périmètre de sécurité traditionnel et le passage des organisations vers un modèle Zero-Trust. Comme le décrit le responsable informatique de la société aéronautique : « Nous nous penchons sur l'utilisation du modèle de moindres privilèges afin de ne conserver qu'un minimum de droits natifs Active Directory et ainsi limiter les potentiels problèmes. Lorsque moins de personnes disposent de droits natifs Active Directory, les difficultés que nous devons résoudre sont moins nombreuses. » La figure 2 est une représentation du modèle de moindres privilèges sous forme de cercles concentriques allant du moindre privilège à l'extérieur vers le privilège maximal à l'intérieur.

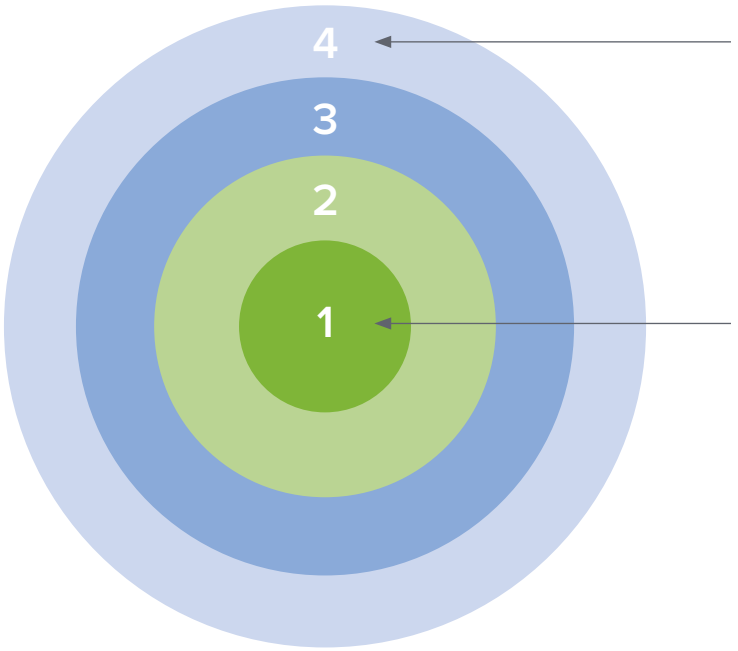
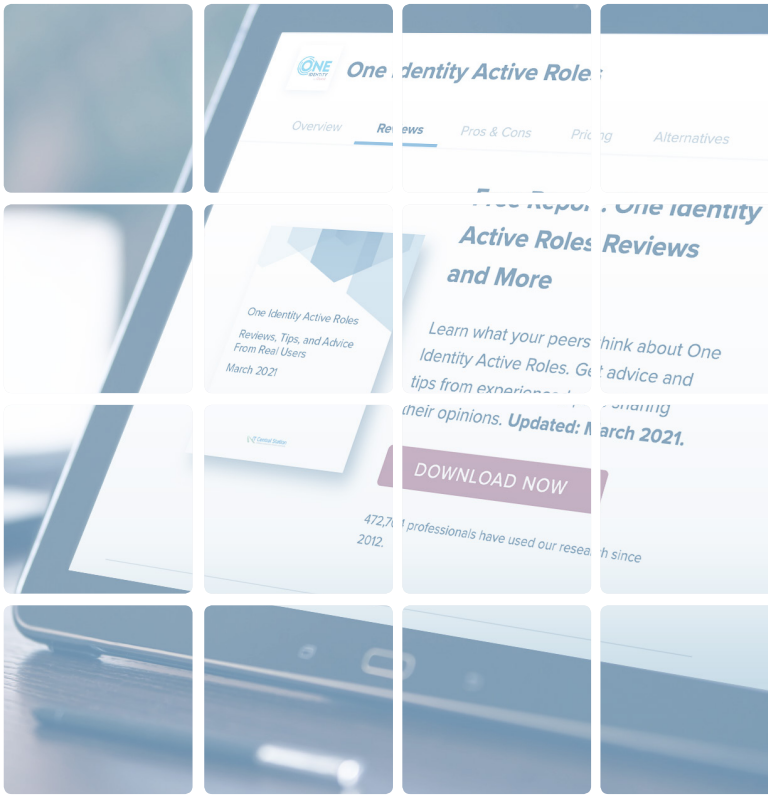


Figure 2 – Le modèle de moindres privilèges attribue aux utilisateurs le plus bas niveau d'accès par défaut. Lorsqu'il dispose d'autorisations spécifiques, un utilisateur peut bénéficier de privilèges plus élevés et accéder à davantage de zones sensibles dans l'infrastructure, à des données, etc.

Améliorer le processus de gestion des identités

Il est particulièrement important de renforcer la sécurité à l'aide d'un dispositif d'IAM plus performant. Mais quelles sont les conditions requises pour améliorer le processus de gestion des identités ? Les membres d'IT Central Station ont donné leur avis, soulignant l'importance d'un point de contrôle unifié, accompagné toutefois d'un contrôle granulaire. Il est primordial de gagner du temps, tout comme de disposer d'un processus d'intégration efficace. Il est également essentiel de pouvoir automatiser les workflows de gestion des identités à l'aide de stratégies et de modèles, en exploitant les groupes dynamiques pour un impact maximal.



5. Unifier la gestion à l'aide d'une interface unique

Les utilisateurs d'Active Roles, comme le responsable informatique de la société aéronautique, étaient ravis de pouvoir gérer plusieurs instances Active Directory à partir d'une seule console et de bénéficier d'une interface unique sur site. Il déclare : « Nous disposons de plusieurs environnements Active Directory. Nous pouvons les gérer et les surveiller d'un seul et même endroit. » L'analyste d'affaires senior de l'Université George Washington partage ce sentiment : « La flexibilité et l'extensibilité de cette plate-forme nous ont permis d'obtenir des résultats que nous n'espérions pas. Active Roles offre également une interface unique pour gérer AD et Azure AD. L'un des avantages que nous apprécions le plus est le fait d'avoir un accès complet depuis Active Roles si nous le souhaitons. »

Un membre du personnel chez Marriott Phoenix évoque également le problème du contrôle. Il explique : « Active Roles nous donne la possibilité de proposer un contrôle granulaire qui n'existe pas avec AD. Disposer d'un outil qui nous permet de gérer toutes les modifications apportées à AD à partir d'une seule interface est un véritable point fort. De plus, nous pouvons opérationnaliser les membres du centre d'assistance très rapidement, même s'ils ne disposent pas de solides connaissances techniques. »

6. Améliorer l'intégration et la gestion du cycle de vie des utilisateurs

Dans le cadre du cycle de vie des salariés, gérer les identités et les accès peut s'avérer chronophage, mais c'est aussi un point de vulnérabilité. Par exemple, les anciens salariés qui conservent leurs identifiants de connexion représentent une menace de sécurité. Pour limiter les risques associés, une solution d'IAM doit proposer des contrôles efficaces sur le cycle de vie des utilisateurs. Par exemple, le responsable de la sécurité des informations pour une entreprise manufacturière explique que sa solution lui permet d'automatiser le provisioning. Et d'ajouter : « Dans nos systèmes RH, nous automatisons la création, la clôture et la gestion continue de toute notre base de salariés. Nous comptons entre 5 000 et 6 000 salariés, tous ces processus sont entièrement automatisés et les équipes informatiques n'ont pas à intervenir. Nous gagnons de précieuses heures, probablement à hauteur de centaines d'heures par an. »

Cet utilisateur poursuit : « One Identity Active Roles a également amélioré la précision de notre processus d'intégration. En tant qu'entreprise, notre processus d'intégration des personnes est soumis aux audits prescrits par la loi Sarbanes-Oxley. Il y a dix ans en arrière, nous nous trouvions dans une situation telle que nous comptions des centaines de non-conformités. Aujourd'hui, nous n'en comptons pas une seule. » Le responsable informatique senior du Conseil scolaire du district de Toronto est du même avis : « Active Roles a amélioré la précision de notre processus d'intégration. Les erreurs sont moins nombreuses lors de la synchronisation. »

7. Automatiser les workflows de gestion des identités

Accorder une confiance excessive aux processus manuels pour administrer l'IAM s'avère à la fois inefficace et source d'erreurs. C'est pourquoi les administrateurs privilégient des solutions d'IAM qui permettent d'automatiser les processus de sécurité. D'après le responsable informatique de la société aéronautique, « avec l'utilisation automatisée d'Active Roles pour intégrer les nouveaux objets, créer des stratégies et des workflows, nous pouvons nous assurer que les données placées dans Active Directory lors de l'intégration de n'importe quel type d'objet sont précises et respectent nos normes. Nous évitons ainsi toute pollution, et nous rationalisons notre approche. »

> **Nous gagnons de précieuses heures, probablement à hauteur de centaines d'heures par an.**

Il poursuit : « Du point de vue de la gestion d'Active Directory, l'aspect le plus complexe auquel nous sommes confrontés, sans outil tel qu'Active Roles, est le contrôle du comportement des utilisateurs. Il se peut que j'installe ou que je configure un nouvel utilisateur d'une façon radicalement différente de la personne à côté de moi. Par exemple, sans produit tel qu'Active Roles, lorsqu'une personne se retrouve avec un ensemble de stratégies à suivre, il ne tient qu'à elle de les interpréter et de les respecter. Active Roles nous permet d'appliquer ces règles afin que les données injectées dans Active Directory soient propres et cohérentes. En disposant de données cohérentes, nous pouvons automatiser davantage d'actions et veiller à ce que les utilisateurs et les objets soient correctement configurés. »

D'autres commentaires notables sur l'automatisation nous ont été rapportés :

- « Nous avons réussi à améliorer l'automatisation. Nous avions déjà automatisé nos systèmes, mais c'est encore mieux aujourd'hui. L'outil est capable d'extraire davantage de données de Trillium et SAP et de remplir Active Directory avec une certaine ouverture d'esprit. Deux techniciens sont chargés de ces activités. Pour chaque membre de l'équipe, Active Roles nous permet d'économiser 0,2 ETP. » – Responsable informatique senior du Conseil scolaire du district de Toronto

- « Nous avons éliminé des tâches qui ralentissaient notre service informatique, notamment avec certaines automatisations de workflows. Grâce au service de synchronisation Active Roles, nous pouvons traiter les données provenant des RH et mettre à jour automatiquement les attributs et les champs de données directement dans Active Directory, sans avoir à utiliser des procédures manuelles ni à importer les données de manière groupée. » – Responsable de la sécurité des informations pour une entreprise manufacturière de plus de 5 000 collaborateurs

- « Nous avons introduit le provisioning automatique basé sur les rôles pour la première fois grâce à Active Roles. Par ailleurs, en utilisant les workflows et les tâches programmées, nous avons pu automatiser un grand nombre de processus et les gérer de façon centralisée, mais aussi les utiliser pour contourner d'autres limitations de produits. Nous pouvons, entre autres, synchroniser des groupes plus vastes, de 50 000 membres et plus, sur Azure AD. » Analyste d'affaires à l'Université George Washington

8. Gagner du temps et améliorer l'efficacité

Lorsqu'elles bénéficient d'une solution d'IAM adaptée, les équipes informatiques et de sécurité peuvent gagner un temps précieux. C'est le cas pour l'analyste d'affaires senior de l'Université George Washington, qui a constaté qu'Active Roles permettait à son équipe de multiplier ses missions et d'être plus efficace. Le responsable technique de la sécurité chez Liberty Global partage une expérience comparable. En effet, la solution lui a permis d'éliminer de nombreuses tâches informatiques fastidieuses, tout particulièrement lorsque des salariés quittent l'entreprise.

Cet utilisateur explique « qu'Active Roles est capable de scripter dix ou quinze actions simultanément, toujours de la même manière. Avant, l'administrateur se retrouvait avec une liste de choses à faire, comme masquer la boîte de réception, désactiver l'utilisateur, supprimer des groupes, etc. Par ailleurs, l'historique des audits qui est conservé nous est particulièrement utile. Nous disposons d'un relevé des modifications apportées à un utilisateur, nous savons qui est à l'origine de ces modifications et quand elles ont été effectuées, ce qui nous aide beaucoup. Et comme nous externalisons désormais de nombreuses activités, nous sommes confrontés à une audience différente. Avec des outils de ce type, nous pouvons nous assurer que toutes les actions effectuées suivent un cadre bien défini, et que tous les utilisateurs font la même chose en même temps. »

La solution a permis à nos clients de gagner du temps en automatisant des tâches qui pouvaient prendre entre 30 et 45 minutes.

Certains utilisateurs ont réussi à quantifier le temps qu'ils ont gagné. Le directeur de la technologie pour BeClever IT Solutions révèle : « La solution a permis à nos clients de gagner du temps en automatisant des tâches qui pouvaient prendre de 30 à 45 minutes. » Le responsable informatique de la société aéronautique remarque que dans son organisation de 55 000 personnes, « les salariés rejoignent et quittent l'entreprise quotidiennement. » Dans cet environnement, « Active Roles nous dispense probablement d'au moins 500 requêtes par semaine. La solution a éliminé les tâches d'administration qui ralentissaient notre service informatique. Aujourd'hui, personne dans le service n'a à se soucier de mettre à jour le groupe lorsqu'une personne rejoint ou quitte l'entreprise. » L'analyste d'affaires senior de l'Université George Washington déclare : « Active Roles nous permet probablement de gagner au moins deux semaines sur chaque mois. Nous avons facilement réduit notre charge de travail de 50 %. »

9. Utiliser des stratégies et des modèles pour renforcer le contrôle basé sur les rôles

Les stratégies et les modèles basés sur les rôles permettent d'améliorer le contrôle des accès, de gagner du temps et de renforcer la précision de la gouvernance et de l'administration AD. Le membre du personnel chez Marriott Phoenix détaille : « Les modèles intégrés à Active Roles nous permettent de créer des groupes de sécurité sans avoir à les construire individuellement. L'outil simplifie énormément le processus et nous permet d'effectuer des vérifications plus facilement au cas où nous aurions besoin d'apporter des changements. » Du point de vue du responsable technique de la sécurité chez Liberty Global, « Active Roles offre la possibilité de mettre en place des stratégies et propose de nombreux exemples. » Il ajoute : « Nous pouvons utiliser des modèles d'accès, et les exemples proposés sont nombreux. L'outil propose même des workflows qui sont très puissants. »

10. Exploiter les groupes dynamiques pour réduire les risques et automatiser les mises à jour

« La fonction que je préfère dans Active Roles, c'est probablement celle des groupes dynamiques et le fait que les groupes dynamiques soient conçus à la volée et actualisés fréquemment. C'est capital pour nous », déclare le responsable informatique de la société aéronautique. Il ajoute : « Nous recevons des demandes régulières de l'entreprise ; il peut s'agir, par exemple d'une demande de création d'un groupe contenant tous les membres d'un service particulier, que ce soit au profit d'une liste de diffusion par e-mail, d'un groupe, pour sécuriser un serveur de fichiers, etc. Avec Active Roles, nous pouvons créer ce groupe et indiquer à Active Roles que tous les comptes utilisateur qui correspondent au critère donné doivent figurer dans le groupe. »

> **Nous n'avons pas à attendre que quelqu'un vérifie dans chacun des groupes si une personne est présente ou absente.**

Pour l'analyste d'affaires senior de l'Université George Washington, l'utilisation des groupes dynamiques permet de réduire les risques et de renforcer la sécurité en supprimant les comptes orphelins qui représentent une vulnérabilité de taille. Elle déclare : « Avec les groupes dynamiques, si une personne ne figure plus dans le flux en provenance du système RH, elle est immédiatement et automatiquement supprimée du groupe. Nous n'avons pas à attendre que quelqu'un vérifie dans chacun des groupes si une personne est présente ou absente. C'est une question qui entre dans les bonnes pratiques internes ; nous nous assurons de respecter les exigences de moindre accès. »

CONCLUSION

L'IAM constitue un défi grandissant à mesure que les environnements informatiques se complexifient et migrent, au moins en partie, vers le Cloud. Microsoft Active Directory reste un outil performant eu égard aux fonctions d'IAM de base. Mais en réalité, la gestion des identités et des contrôles d'accès crée un besoin nouveau ; celui de disposer de solutions automatisées et plus sophistiquées qui viennent en complément d'AD. Comme les utilisateurs de One Identity Active Roles l'ont expliqué dans leurs commentaires sur IT Central Station, une solution adaptée permet d'améliorer l'efficacité de l'IAM et de gagner du temps. Son utilisation peut entraîner la baisse du nombre de modifications non autorisées et le renforcement de la posture de sécurité de l'entreprise à travers la délégation, les groupes dynamiques, les stratégies et les modèles. De plus, un point de contrôle unifié génère des gains d'efficacité considérables. Enfin, les solutions comme Active Roles, capables de fonctionner dans le Cloud, sur site, mais aussi dans des environnements hybrides, offrent une base solide pour améliorer l'IAM en continu – et l'approche de sécurité globale d'une organisation – au fur et à mesure des évolutions de l'informatique et de la sécurité.

À PROPOS D'IT CENTRAL STATION

Avis d'utilisateurs, discussions franches, et plus encore pour les professionnels de la technologie d'entreprise.

Internet a radicalement bouleversé notre façon d'acheter. Nous nous tournons désormais vers des sites d'évaluation pour savoir ce que pensent d'autres utilisateurs réels avant d'acheter un appareil électronique, de réserver un hôtel, de consulter un médecin ou de choisir un restaurant. Mais dans le monde de la technologie d'entreprise, la plupart des informations que vous trouvez en ligne et dans votre boîte de réception proviennent de fournisseurs. Ce que vous voulez vraiment, c'est obtenir des informations objectives de la part d'autres utilisateurs. IT Central Station offre aux professionnels de la technologie une plate-forme communautaire leur permettant de partager des informations sur les solutions d'entreprise.

IT Central Station s'engage à offrir aux utilisateurs des informations de valeur, objectives et pertinentes. Nous validons tous les évaluateurs via un processus à triple authentification, et protégeons votre vie privée en vous offrant un environnement où vous pouvez poster anonymement et exprimer librement vos opinions. En conséquence, la communauté devient une ressource précieuse, vous garantissant l'accès aux bonnes informations et la mise en relation avec les bonnes personnes, chaque fois que vous en avez besoin.

www.itcentralstation.com

IT Central Station ne cautionne ni ne recommande aucun produit ou service. Les avis et opinions des évaluateurs cités dans ce document, les sites Web IT Central Station et les documents IT Central Station ne reflètent pas les opinions de IT Central Station.

À PROPOS DE ONE IDENTITY

One Identity, une entité Quest Software, aide les entreprises à mettre en place une stratégie de sécurité axée sur les identités, aussi bien sur site, dans le Cloud ou dans un environnement hybride. Avec notre vaste portefeuille intégré d'offres de gestion des identités, comprenant la gestion des comptes, l'administration et la gouvernance des identités, ainsi que la gestion des accès à privilèges, les entreprises peuvent réaliser tout leur potentiel et bénéficier d'une sécurité efficace grâce à une stratégie axée sur les identités, qui assure un accès adéquat à tous les types d'utilisateurs, tous les systèmes et toutes les données. En savoir plus sur le site OneIdentity.com.