LIVRE BLANC

Mieux ensemble : booster Active Directory avec One Identity Active Roles en 10 étapes

À propos de ce document

Ce document vous propose de corriger et d'éviter les problèmes de comptes d'utilisateurs dans AD en 10 étapes. Ces étapes font appel aux fonctionnalités AD natives et à une technologie de workflow courante, comme Microsoft SharePoint. Ainsi, l'implémentation des recommandations du présent document demande peu d'efforts d'apprentissage.

Toutefois, même si vous tenez compte de toutes les recommandations de ce document, si vous ne disposez pas des outils supplémentaires nécessaires pour gérer et automatiser vos processus, la plupart des tâches administratives et des confirmations manuelles restent l'apanage de vos responsables métiers, chargés des RH et équipes informatiques.

Bonne nouvelle : vous pouvez franchir quasiment tous ces obstacles grâce à One Identity Active Roles by Quest. Active Roles offre une multitude de fonctionnalités vous permettant de ne plus dépendre des utilisateurs finaux, des responsables ni des RH. Poursuivez votre lecture pour découvrir comment Active Roles facilite chacune de ces 10 étapes.

Présentation

Microsoft Active Directory (AD) et Azure AD (AAD) permettent de structurer et de normaliser les modes de gestion et de stockage des données d'identité et de compte. One Identity Active Roles apporte des capacités d'agilité, de sécurité, de rapidité et d'unité à la gestion d'AD/Azure AD. Lorsqu'ils utilisent Active Roles et AD/AAD conjointement, les administrateurs IT disposent d'une solution capable d'améliorer significativement la sécurité et l'efficacité de leurs environnements AD tout en limitant leur vulnérabilité. Prenons une métaphore : imaginez une puissante voiture de sport en version de production à laquelle on ajoute des suspensions de course et un turbo, mais aussi un tableau de bord et un système de surveillance des performances améliorés reliés au Cloud, tout en la protégeant à l'aide d'une clé à accès distant à la fois programmable et hautement sécurisée.

En exposition, le véhicule fait déjà forte impression, mais après être sorti sur le marché et réétudié, vous pouvez lancer une nouvelle version améliorée et ainsi gérer tous types de circonstances, y compris des changements considérables et des menaces. Le véhicule est alors plus rapide, plus sûr, braque mieux que jamais, demande moins d'entretien et consomme moins de carburant. Vous amortissez rapidement votre investissement supplémentaire et vous vous préparez à faire des voyages que vous n'envisagiez pas auparavant. Et c'est beaucoup mieux.

C'est la même chose avec Active Roles et One Identity Active Roles. Ils fonctionnent mieux ensemble.

Si vous êtes comme 95 % des entreprises du classement Fortune 1000, vous disposez déjà de la voiture d'exposition – au quotidien, Microsoft Active Directory est un peu comme votre chauffeur ; il provisionne et déprovisionne les autorisations des utilisateurs. Mais le monde bouge vite et les ressources gérées par AD et Azure AD (mais aussi AD LDS) ne cessent de se diversifier. Par ailleurs, d'autres tendances viennent obscurcir la gestion d'AD/AAD, notamment la sécurité des identités, la migration vers le Cloud et le rôle majeur d'AD/AAD dans la gestion des accès privilégiés. Récemment, avec l'implémentation de l'architecture de sécurité Zero-Trust (à moindres privilèges) pour éviter et limiter les dommages consécutifs à une violation, est né le besoin de développer et d'améliorer les fonctionnalités natives d'AD/AAD. C'est là où One Identity Active Roles peut automatiser et booster les services AD/AAD.

Dans ce document, nous vous expliquons comment nettoyer les données de vos comptes d'utilisateurs Microsoft AD/AAD en 10 étapes. Ce processus est primordial pour gagner en efficacité et en sécurité. Nous décomposerons chacune des dix étapes et vous expliquerons en détail quelle est leur importance et quel est le rôle que joue One Identity Active Roles au sein de ces étapes. Nombre d'entre elles font appel au bon sens, comme la suppression des comptes non utilisés et la révocation des accès à certaines applications et ressources, mais comme nous le savons tous, dans le feu de l'action, il est difficile de prioriser les tâches manuelles de maintenance des comptes lorsque se présentent des situations critiques en lien avec la technologie et les données. Découvrez comment One Identity Active Roles vous permet d'automatiser et de sécuriser ces tâches et comment, lorsque vous l'utilisez en parallèle de One Identity CertAccess, vous pouvez vous assurer que les processus de certification, d'autorisation et d'approbation sont respectés et documentés.

Active Roles offre une multitude de fonctionnalités vous permettant de ne plus dépendre des utilisateurs finaux, des responsables ni des RH.

Ces 10 étapes font appel aux fonctionnalités AD natives et à une technologie de workflow courante, comme Microsoft SharePoint. Ainsi, l'implémentation des recommandations du présent document demande peu d'efforts d'apprentissage.

Toutefois, même si vous tenez compte de toutes les recommandations de ce document, si vous ne disposez pas des outils supplémentaires nécessaires pour gérer et automatiser vos processus, la plupart des tâches administratives et des confirmations manuelles restent l'apanage de vos responsables métiers, chargés des RH et équipes informatiques.

Bonne nouvelle : vous pouvez franchir quasiment tous ces obstacles grâce à One Identity Active Roles by Quest. Active Roles offre une multitude de fonctionnalités vous permettant de ne plus dépendre des utilisateurs finaux, des responsables ni des RH.

Poursuivez votre lecture pour découvrir comment et pourquoi Active Directory et One Identity Active Roles sont plus performants utilisés ensemble.

Active Directory, outil essentiel dans le contrôle des risques et la mise en conformité

Pour la plupart des organisations, Active Directory (AD) est au cœur de la gestion des accès et des identités. Par conséquent, il s'agit probablement de la technologie la plus importante du réseau. De plus en plus de systèmes et d'applications dépendent d'AD et d'Azure Active Directory (AAD) pour gérer l'authentification, les stratégies, les droits et les configurations. Si AD n'est pas sécurisé, rien ne l'est.

Comptes d'utilisateurs : enjeu de sécurité crucial, maintenance difficile

La sécurisation d'Active Directory/Azure AD est essentielle dans le contrôle des risques et la mise en conformité. Néanmoins, c'est un défi que de veiller à la clarté, à l'organisation et à la sécurité d'AD, tout particulièrement en matière de comptes d'utilisateurs.

Les comptes d'utilisateurs sont à la base de l'authentification et de l'accès au réseau, aux systèmes et aux applications. Leur maintenance est difficile sans outil adéquat permettant de prendre en charge le suivi de l'ensemble des autorisations d'un utilisateur sur plusieurs plates-formes. Un compte d'utilisateur est créé à chaque nouveau recrutement. Au fil de l'évolution des missions et des tâches de l'utilisateur, son compte AD est mis à jour (poste, service et numéro de téléphone, par exemple), y compris lorsqu'il rejoint et quitte des groupes. Enfin, lorsque l'utilisateur quitte l'organisation, les droits d'accès au compte doivent être supprimés en bonne et due forme.

Ce processus paraît simple et clair. Toutefois, dans de nombreuses organisations, on compte un grand nombre de comptes d'utilisateurs dont les autorisations sont inappropriées ou obsolètes, et qui ne respectent pas les stratégies de sécurité de l'organisation. Qui plus est, ils exposent l'organisation à des risques de sécurité.

La cause première de ces problèmes ? De mauvaises pratiques de gestion du cycle de vie des comptes d'utilisateurs. En règle générale, les organisations font confiance aux utilisateurs finaux, aux responsables et aux RH pour reconnaître les évènements qui affectent le compte AD d'un utilisateur. Ces personnes très affairées sont ensuite censées informer leur équipe informatique – elle aussi surchargée – qu'AD doit être mis à jour pour refléter les modifications des comptes d'utilisateurs. Lorsqu'une organisation s'appuie uniquement sur des processus manuels, ces changements sont trop souvent ignorés, ce qui donne naissance à des comptes fantômes et à des autorisations inappropriées susceptibles d'être prises pour cible par les pirates souhaitant causer des ravages sur l'organisation.

Améliorer l'agilité, la sécurité et les performances d'Active Directory en 10 étapes

Étape 1 : effectuer l'analyse régulière des comptes

Le moyen le plus efficace pour maintenir un environnement AD/AAD propre et sûr consiste à vérifier régulièrement les comptes d'utilisateurs. En vérifiant les propriétés d'un compte avant un audit, vous pouvez détecter et corriger de nombreux points avant que les auditeurs ne les soulèvent.

Dresser la liste des comptes d'utilisateurs en toute simplicité

Il fut un temps où récupérer la liste des comptes d'utilisateurs n'était pas chose aisée. Désormais, il s'agit simplement d'exécuter un script Windows PowerShell et d'importer les résultats dans Microsoft Excel. Ce script (Output-ADUsersAsCSV) est disponible à l'adresse http://www.ultimatewindowssecurity.com/ tools/Output-ADUsersAsCSV. Il se présente sous la forme d'une feuille de calcul semblable à l'exemple ci-dessous.

	A	B	C	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
1	Distinguished Name	Display Name	SAM ID	Description	Office	Phone	E-mail Address	Job Title	Dept	Org	Company	Manager	Can user change password ?	Does password expire?	Is account disabled?	Account Expiration Date	Last Log-on Date	Has user ever logged on?
2	CN=Administrator,CN=Users,DC=mt		Administrat	Built-in account for administering the computer/domain									Yes	Yes	No		10/13/12	Yes
3	CN=Guest,CN=Users,DC=mtg,DC=lo		Guest	Built-in account for guest access to the computer/domain									Yes	No	Yes			No
4	CN=krbtgt,CN=Users,DC=mtg,DC=lo		krbtgt	Key Distribution Center Service Account									Yes	Yes	Yes			No

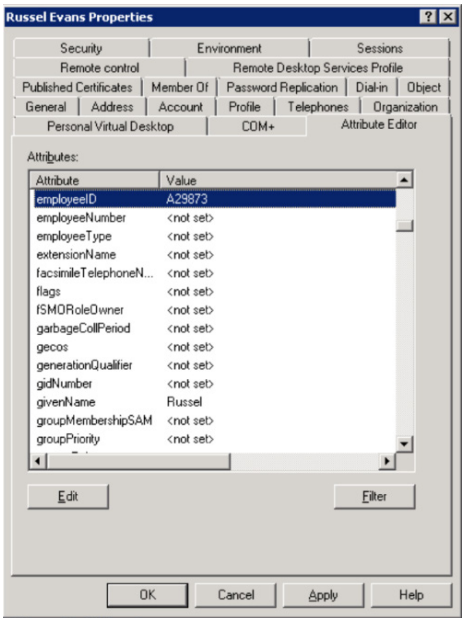
Filtrer la feuille de calcul à la recherche des comptes non conformes

Grâce au script et à la feuille de calcul que vous obtenez, vous pouvez appliquer des filtres aux différentes propriétés des utilisateurs afin de repérer les comptes non conformes. Commencez par identifier les comptes qui présentent des problèmes faciles à détecter, notamment ceux dont les mots de passe n'expirent jamais. Ensuite, appliquez des critères de filtrage à d'autres colonnes, comme sur l'ID SAM ou la description, pour éliminer les services, les applications et les autres comptes qui font exception.

Ces problèmes sont faciles à corriger avant d'accueillir les auditeurs et vous permettront de réduire le nombre de risques détectés lors de votre audit. Autre problème de taille à traiter : les comptes dormants. Nous reviendrons sur ce sujet plus tard ; une étape y est dédiée dans ce document.

D'autres problèmes sont à noter, notamment les comptes qui n'auraient jamais dû être créés ou qui n'ont pas été provisionnés selon les conventions de dénomination ou d'autres contrôles de création de compte.

Prenons un exemple : les conventions de dénomination d'Acme Corp exigent que tous les comptes des utilisateurs finaux commencent par 'u-', les comptes des administrateurs par 'p-' (pour privilège) et les comptes de service par 's-'. Tout d'abord, filtrez tous les comptes qui commencent par ces préfixes pour identifier les comptes restants, potentiellement douteux. Il se peut que certains des comptes restants soient des exceptions légitimes ; nous y reviendrons dans une étape suivante. Mais pour la plupart, ces comptes sont mystérieux et doivent faire l'objet d'une enquête pour déterminer leur rôle et leur état.



Plusieurs méthodes vous permettent d'associer des comptes AD aux entrées des collaborateurs : (1) Utiliser l'attribut ID de collaborateur ou Numéro de collaborateur dans AD ; (2) Via l'onglet Éditeur d'attributs, comme illustré dans la figure ci-dessus ;

(3) En saisissant l'ID collaborateur dans le champ Description ou Notes ; (4) En intégrant le numéro de collaborateur dans le nom de connexion.

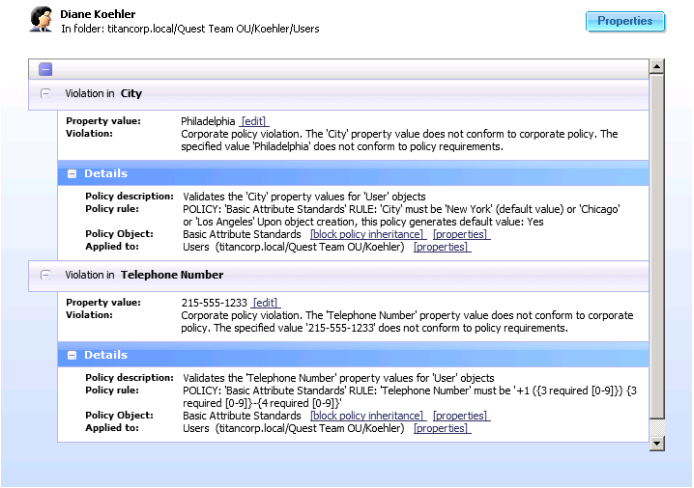
Il est tout à fait recommandé de réaliser cette étape avant un audit. Mais c'est tous les mois que vous devriez y penser pour veiller au bon fonctionnement d'AD. Après tout, votre mission ne consiste pas uniquement à passer des audits ; l'objectif doit être d'assurer la sécurité et l'organisation d'AD à tout moment.

Notez que cette étape vise à détecter certains problèmes et à y régir, mais qu'elle n'a aucune vocation préventive ni proactive. Votre objectif doit être d'éviter que des problèmes ne surviennent. L'étape 2 est un premier pas qui vous permettra de réaliser cet objectif.

Contribution d'Active Roles

Active Roles vous donne la possibilité de comparer les normes que vous appliquez aux objets AD (c'est-à-dire les règles) à vos objets AD réels. Les résultats de cette comparaison (appelée une demande de vérification de stratégie) vous parviennent en quelques clics à l'écran ou par l'intermédiaire de rapports planifiés régulièrement. Cette fonctionnalité peut aider une organisation à mettre de l'ordre.

Avec un investissement administratif relativement faible pour la création de règles, vous pouvez enfin commencer à reprendre le contrôle.



Active Roles vous donne la capacité de comparer les normes que vous appliquez aux objets AD (c'est-à-dire les règles) à vos objets AD réels.

Étape 2 : associer les comptes aux données sur les collaborateurs

Pour assurer la propreté et la sécurité des comptes AD, un moyen fondamental consiste à associer tous les comptes à un utilisateur réel. Ce processus concerne aussi les comptes non humains, comme ceux qui sont créés pour des services et des applications, et sera détaillé ultérieurement à l'étape 7. Commençons par nous concentrer sur les comptes qui sont créés pour des personnes, y compris les utilisateurs finaux, les sous-traitants, les administrateurs et autres.

Le plus important est d'associer le compte d'un collaborateur à l'entrée principale correspondante dans votre système de gestion des RH.

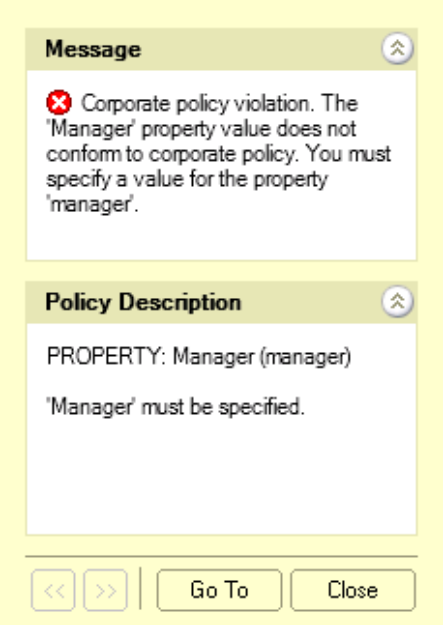
Ce couplage est crucial, car l'accès d'un collaborateur au réseau doit être attaché à son statut et son rôle au sein de l'organisation. Ainsi, c'est l'entrée maître du système de gestion des RH qui fait foi, car ce sont les données qui ont le plus de chance d'être à jour.

Lorsque le statut ou le rôle d'un collaborateur change, vous devez être en mesure de trouver ses comptes et de modifier son statut ou ses droits pour refléter ce changement. Il est primordial de documenter l'identifiant des collaborateurs dans les comptes AD. Bien sûr, vous devez également mettre en œuvre des procédures qui facilitent la réponse à ces évènements, mais nous y reviendrons dans une prochaine étape.

Lorsque le statut ou le rôle d'un collaborateur change, vous devez être en mesure de trouver ses comptes et de modifier son statut ou ses droits pour refléter ce changement. Il est primordial de documenter l'identifiant des collaborateurs dans les comptes AD. Bien sûr, vous devez également mettre en œuvre des procédures qui facilitent la réponse à ces évènements, mais nous y reviendrons dans une prochaine étape.

Contribution d'Active Roles

En appliquant des règles de création de comptes, Active Roles peut exiger que tous les comptes non humains soient créés avec une valeur Manager ou EmployeeID. Dans les faits, Active Roles peut gérer le provisionnement de comptes et le format de n'importe quel attribut.



Lorsqu'ils réussissent, les intrus (humains ou automatisés) créent souvent des comptes détournés pour s'assurer de conserver un accès continu et de masquer leur activité.

Étape 3 : surveiller les nouveaux comptes

Lors des audits informatiques d'AD, il est courant de trouver des comptes inutiles qui ne respectent pas les normes, y compris des comptes qui s'éloignent des conventions de dénomination de l'entreprise. Ce phénomène se produit lorsque les personnes autorisées à créer des comptes sont trop nombreuses dans le département IT. Nous y reviendrons dans une prochaine étape.

Les intrus créent souvent des comptes détournés

Lorsqu'ils réussissent, les intrus (humains ou automatisés) créent souvent des comptes détournés pour s'assurer de conserver un accès continu et de masquer leur activité. Flame, un récent logiciel malveillant armé, tentait spécifiquement de créer de tels comptes dès qu'il détectait qu'il s'exécutait sous l'autorité d'un administrateur de domaine.

Arrêtez-les dès qu'ils créent un compte

Voilà pourquoi la surveillance des nouveaux comptes est primordiale ; mais elle est aussi chronophage et n'aboutit pas toujours. Il est préférable d'identifier un compte non conforme lorsqu'il est créé :

- Identifiez qui a créé le compte.
- Cette personne fait-elle toujours partie de l'entreprise ?
- Pourquoi le compte a-t-il été créé ?

Comment surveiller et vérifier les nouveaux comptes

Deux méthodes s'offrent à vous pour surveiller les nouveaux comptes et répondre aux difficultés :

- Surveillez les logs de sécurité du contrôleur de domaine AD à la recherche de l'ID d'évènement 4720 (vous devez activer la sous-catégorie d'audit Gestion des comptes d'utilisateurs).
- Exécutez le script Output-ADUsersAsCSV et triez la colonne Date de création.

Lorsque vous vérifiez chaque compte, essayez de répondre au mieux aux questions suivantes :

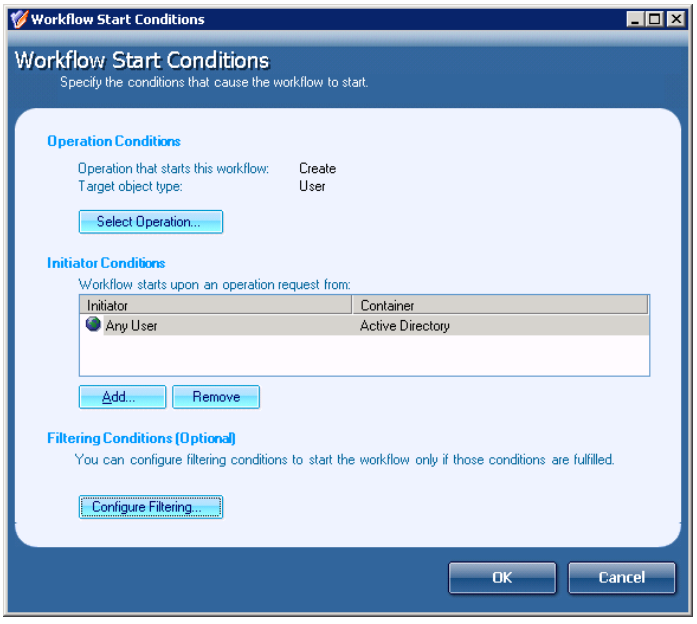
- Existe-t-il un ticket de travail ou d'autres documents corroborant ce compte ?
- Le compte répond-il aux conventions de dénomination établies ?
- Le compte respecte-t-il les autres normes et règles appliquées à la création de comptes dans l'organisation ?

```
ID d'évènement 4720 – Un compte d'utilisateur a été
créé

Objet :

      ID de sécurité : ACME-FR\administrator

      Nom du compte : administrator

      Domaine du compte : ACME-FR

         ID de connexion :

Nouveau compte 0x20f9d :

      ID de sécurité : ACME-FR\John.Locke

      Nom du compte : John.Locke

      Domaine du compte : ACME-FR

Attributs :

      Nom de compte SAM : John.Locke

      Nom d'affichage : John Locke

      Nom principal de l'utilisateur : John.Locke@
      acme-fr.local
```

S'il s'avère que le compte n'est pas autorisé ou qu'il n'est pas conforme, vous devez contacter la personne qui en est à l'origine. La première méthode présente l'avantage d'indiquer qui a créé le compte grâce à l'évènement 4720 du log de sécurité.

Contribution d'Active Roles

Active Roles joue le rôle de pare-feu virtuel autour d'Active Directory, en veillant à appliquer un modèle de moindres privilèges aux accès. Grâce à l'utilisation de workflows pour toutes les opérations, et notamment la création, la modification ou la suppression d'un compte dans le domaine, l'ensemble des processus qui sont généralement effectués manuellement peuvent être automatisés. Ainsi, toutes ces actions hautement importantes sont mises en œuvre immédiatement et intégralement, dans le respect des exigences de l'audit.



Étape 4 : automatiser la maintenance des comptes

Étapes de création d'un compte

Pour vous assurer que les nouveaux comptes sont créés conformément aux normes en place, automatisez les processus de création des comptes au maximum afin de limiter les potentielles erreurs humaines. La création d'un compte comprend les étapes suivantes :

1. Créer le compte dans AD
2. Définir les attributs d'identité (poste, numéros de téléphone, etc.)
3. Créer la boîte aux lettres du compte dans Microsoft Exchange/O365
4. Ajouter le compte à des groupes adaptés au rôle de l'utilisateur
5. Inscrire le compte AD auprès d'autres applications, le cas échéant

Automatisation avec les scripts PowerShell

Nombre de ces étapes peuvent être automatisées à l'aide de scripts PowerShell. Les scripts suivants permettent d'automatiser les étapes 1 à 4.

```
New-ADUser –Name 'randyjones'

–SamAccountName randyjones – AccountExpirationDate
01/01/2014

–GivenName 'Randy' –Surname

'Jones'

–DisplayName 'RandyJones' –Path
'CN=Users,DC=acme,DC=local' – EmployeeID '93299' –
OfficePhone

'27884' –Title 'CEO'

Enable-Mailbox –Identity acme\ randyjones –Database
Database01

Add-ADGroupMember Group1 acme\randyjones

Add-ADGroupMember Group2 acme\randyjones
```

Vous pouvez créer une version personnalisée de ce script pour les rôles qui présentent un fort taux de roulement dans votre organisation. Vous pouvez également l'améliorer pour accepter certaines entrées et créer le compte en fonction de critères définis au moment de l'exécution.

Contribution d'Active Roles

Active Roles offre de nombreuses interfaces, y compris PowerShell, l'écriture de scripts ADSI, le langage SPML, la norme SCIM, le MMC et le Web. Ces fonctionnalités sont importantes, car elles vous permettent d'appliquer des normes (c'est-à-dire des règles) à n'importe quelle opération CRUD sur un objet AD, quelle que soit l'interface. Grâce à cette couche de gestion, vous pouvez vous assurer que l'ensemble des activités de votre environnement AD sont entièrement sous le contrôle de vos normes. Le non-respect de ces normes peut entraîner une violation autorisée (qui peut être déclarée) ou une réponse d'erreur, selon votre choix.

Étape 5 : traiter les utilisateurs

ayant quitté l'organisation et les changements de rôles

Pour les organisations qui utilisent des outils de gestion d'AD classiques, les comptes d'utilisateurs fantômes ou orphelins constituent une source de risque continue. Sans automatisation et/ou source unique d'informations sur les identités et les autorisations, vous risquez de conserver des personnes qui n'ont plus aucun rapport avec l'organisation dans vos données d'identité. Il est capital que les responsables de la mise à jour des statuts (le chargé des RH ou le responsable informatique) soient informés dès que quelqu'un quitte l'organisation ou change de rôle.

La recherche de comptes dormants ne résout pas ce problème

Bien que cela semble simple, les organisations ont souvent des difficultés à désactiver les comptes d'utilisateurs ou à modifier les droits en cas de changement du statut de l'utilisateur. Lorsqu'un audit questionne la désactivation des comptes des utilisateurs ayant quitté l'organisation, la réponse est souvent la même : en général, l'organisation part en quête des comptes dormants en recherchant ceux qui n'ont pas fait l'objet d'une connexion récente. Cette approche est défaillante, car lorsqu'une personne ne travaille plus dans l'entreprise et continue d'accéder au réseau, son compte n'apparaît pas comme dormant et il ne figure pas dans le rapport correspondant.

La recherche de comptes dormants permet de traiter les symptômes sans s'attaquer à la cause du problème. En adoptant une approche qui tient compte de l'intégralité du cycle de vie d'un compte AD, du recrutement au départ en passant par toutes les étapes intermédiaires, ce problème peut être éliminé.

Le même raisonnement peut être appliqué aux données redondantes. Cette étape est toute aussi importante que la création d'entrées précises. Si vous ne purgez pas les données redondantes et inutiles, vous encombrez votre environnement AD avec des données désordonnées.

Méthodes efficaces pour gérer les utilisateurs ayant quitté l'organisation et les changements de rôles

Les trois points suivants présentent des méthodes pour traiter les changements de statuts efficacement, par ordre de préférence descendant :

- La plupart des organisations disposent de processus clairement définis, qu'elles appliquent rigoureusement, afin de supprimer l'accès physique d'un utilisateur au bâtiment ; il suffit d'intégrer la désactivation du compte AD à ce processus.
- Si votre application de RH inclut un workflow, automatisez-le de sorte que les administrateurs reçoivent un e-mail automatiquement lorsqu'un utilisateur quitte l'organisation, change de rôle ou passe sous l'autorité d'un autre responsable.
- La majorité des applications de RH vous permettent de planifier la création automatique de rapports : planifiez un rapport journalier sur les départs de collaborateurs et les changements de postes et envoyez-le aux administrateurs de comptes.

Vous y gagnez, car la désactivation de comptes et l'actualisation du statut des autorisations sont obligatoires pour respecter les exigences légales et professionnelles. Quel que soit votre processus, la direction doit comprendre son importance et les responsabilités doivent être clairement définies.

Contribution d'Active Roles

Active Roles propose des fonctionnalités de workflow qui permettent de déclencher des tâches ou des ensembles de processus dès que l'annuaire fait l'objet d'une modification. Ces processus concernent notamment les règles de clôture de compte grâce auxquelles votre organisation peut déterminer exactement ce qu'advient du compte d'un utilisateur lorsque son contrat est terminé.

Vous pouvez, par exemple, choisir de désactiver le compte, de déplacer l'emplacement de l'unité organisationnelle, de brouiller le mot de passe et d'altérer le nom de connexion, de renommer le compte avec des variables opérationnelles, d'affecter des délégués aux dossiers de messagerie et de base, etc.

Qui plus est, Active Roles peut retirer l'utilisateur de tous les groupes de sécurité, réattribuer l'annuaire de base d'un utilisateur, libérer des licences O365 attribuées et bien plus. Notez que ces règles peuvent être déclenchées manuellement, automatiquement ou de manière programmatique.

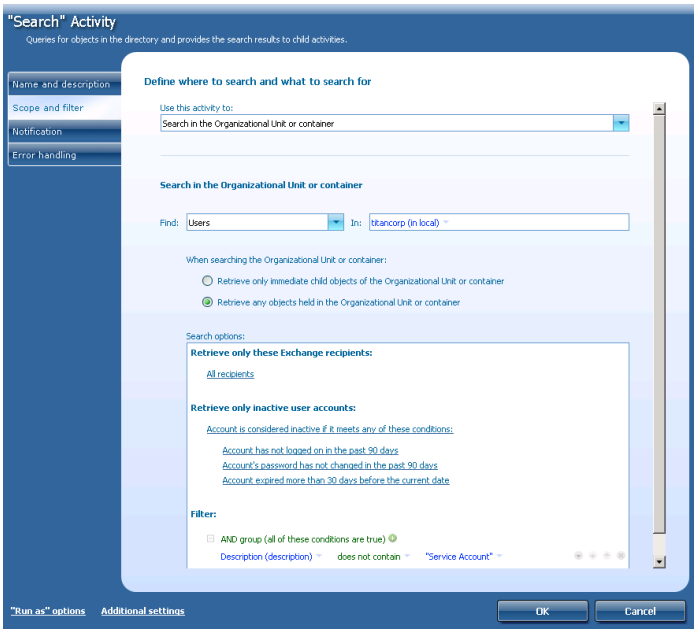
Étape 6 : traiter les comptes dormants

L'étape suivante consiste à vérifier régulièrement la présence de comptes dormants (c'est-à-dire les comptes d'utilisateurs qui n'ont pas fait l'objet d'une connexion récente). À nouveau, nous vous rappelons que cette étape ne peut pas remplacer l'étape 5.

Trouver les comptes dormants n'est pas difficile

Avant Windows 2003, trouver les comptes dormants n'était pas simple. Grâce à l'attribut lastLogonTimestamp (horodatage de la dernière connexion), c'est désormais chose aisée. Cette réplication (tous les sept jours) vous permet d'interroger les contrôleurs de domaine et de connaître le moment de la dernière connexion, ce qui facilite l'identification des utilisateurs dormants.

L'attribut LastLogonTimestamp est exposé par la commande Get-ADUser avec la propriété LastLogonDate, comme illustré



avec le script OutputADUsersAsCSV à l'étape 1. Avec ce script, vous n'avez qu'à trier la colonne Dernière connexion par ordre décroissant afin d'identifier facilement les comptes qui n'ont pas fait l'objet d'une connexion récente.

Vous devez également vérifier les comptes d'utilisateurs qui n'ont jamais fait l'objet d'une connexion. Dans les feuilles de calcul générées par le script Output-ADUsersAsCSV, ces comptes apparaissent dans les lignes associées à une colonne Dernière connexion vierge.

Contribution d'Active Roles

Active Roles automatise les processus d'identification et de gestion des comptes dormants, y compris les étapes de classification, de détection et de correction. Voilà qui facilite le processus de nettoyage des comptes. Si vous utilisez cette fonctionnalité en parallèle de règles adéquates sur la gestion du cycle de vie des comptes (comme le déprovisionnement), non seulement vous pouvez résoudre les problèmes existants, mais vous pouvez éviter de futures difficultés.

Étape 7 : gérer les comptes non humains

Tous les comptes n'appartiennent pas directement à une personne. Par exemple, de nombreuses applications ont besoin d'un ou de plusieurs comptes afin de connecter les services. Ces comptes disposent souvent d'accès privilégiés aux serveurs et aux données. C'est pourquoi ils doivent être sécurisés.

Pourquoi les comptes bénéficiant de privilèges élevés présentent des risques

Néanmoins, il est difficile d'effectuer le suivi des comptes dédiés aux applications et à d'autres services non humains. Lors des audits informatiques, il n'est pas rare de découvrir des comptes privilégiés qui présentent des risques pour les raisons suivantes :

- Personne ne sait avec exactitude quel est l'objet du compte ou quelles sont les raisons de son existence
- Malgré le départ d'un grand nombre d'administrateurs, le mot de passe du compte n'a pas été mis à jour, par peur de nuire à une application présente sur le réseau
- Le compte est autorisé à se connecter de manière interactive.
    - Les comptes non humains ne doivent pas avoir l'autorisation de se connecter de manière interactive – sur la console ou via un bureau à distance – afin d'éviter que les administrateurs (qui connaissent le mot de passe du compte) ne se connectent anonymement à ce compte sans rendre de comptes à titre individuel

Identifier les comptes non humains

Pour gérer les comptes non humains, la première étape consiste à identifier tous les comptes de ce type. Pour y parvenir, vous pouvez utiliser un préfixe dans la convention de dénomination du nom de connexion, en plaçant ces comptes dans une unité organisationnelle dédiée aux comptes non humains ou en les identifiant comme tels grâce à un autre attribut dans AD.

Documenter l'objet et le propriétaire de chaque compte

Ensuite, vous devez documenter l'objet du compte et les systèmes sur lesquels il est utilisé dans les champs Description ou Notes du compte.

Désignez un propriétaire pour chaque compte non humain et reportez ces informations dans AD. Le propriétaire peut être le compte d'utilisateur d'un individu, mais il est généralement préférable de sélectionner un groupe qui corresponde à l'équipe responsable de l'application ou de la technologie qui utilise le compte. Le propriétaire peut également figurer dans le champ Description ou Notes.

Active Roles automatise les processus d'identification et de gestion des comptes dormants, y compris les étapes de classification, de détection et de correction.

L'utilisation des comptes de services managés a été introduite avec Windows Server 2008 R2 (et par la suite les comptes de services managés de groupe) afin de gérer (modifier) automatiquement les mots de passe des comptes de services. En utilisant ces fonctionnalités, vous pouvez considérablement limiter le risque de compromission des comptes système.

Maintenance des mots de passe

Les comptes non humains posent une grande difficulté, notamment dans la maintenance des mots de passe. Le mot de passe d'un compte non humain doit être modifié dès qu'un administrateur (qui connaît le mot de passe) quitte l'organisation. À moins que les comptes ne soient correctement documentés, il est difficile de savoir quels étaient les comptes non humains auxquels un administrateur pouvait accéder. Toutefois, la modification du mot de passe d'un compte entraîne des risques. En effet, tous les services ou tâches planifiés qui sont exécutés grâce à ce compte, ou les applications qui stockent le mot de passe du compte, doivent être mis à jour, sans quoi ils échoueront à la prochaine tentative de démarrage ou de connexion.

Identifier les systèmes sur lesquels est utilisé un compte

Si vous tentez de nettoyer un ensemble de comptes non humains existant, vous pouvez identifier les systèmes sur lesquels un compte est utilisé en consultant le log de sécurité Windows. Si vous avez activé la sous-catégorie d'audit des opérations de ticket de service Kerberos dans l'objet de stratégie de groupe du contrôleur de domaine par défaut, vos contrôleurs de domaine consignent l'évènement avec l'ID 4769. En recherchant toutes les occurrences 4769 dans les logs de sécurité des contrôleurs de domaine qui sont associées au nom du compte de service concerné, vous pouvez générer une liste de tous les ordinateurs sur lesquels le compte est utilisé. Observez le champ Nom du service dans ces évènements. Associé à un évènement avec l'ID 4769, le champ Nom du service identifie l'ordinateur pour lequel le compte d'utilisateur demande à être authentifié.

Limiter les droits de connexion des comptes

non humains

La dernière étape pour sécuriser les comptes non humains consiste à limiter leurs droits de connexion sur les ordinateurs de tout le domaine. Cette démarche permet d'éviter que les comptes non humains ne fassent l'objet d'abus par des individus qui se connectent grâce au compte de manière interactive sur la console d'un ordinateur ou via un bureau à distance. Cette étape sert de barrière défensive en profondeur au cas où les mots de passe ne seraient pas modifiés au départ d'un administrateur. Dans Windows, cinq types de connexion permettent d'autoriser et de refuser des droits :

Pour vous connecter d'une certaine façon, vous devez disposer du droit Autoriser la connexion correspondant. Par ailleurs, si le droit Refuser la connexion vous a également été attribué, vous ne pouvez pas vous connecter, car le droit Refuser la connexion remplace le droit Autoriser la connexion. Vous pouvez trouver ces droits dans un objet de stratégie de groupe sous Ordinateur Settings\Windows Settings\

Security Settings\Local Policies\ User Right Assignments.

En règle générale, les comptes non humains doivent disposer uniquement du droit Ouvrir une session as a service. Il est recommandé d'interdire explicitement les droits de connexion interactive et depuis un bureau à distance afin d'éviter toute utilisation détournée du compte. Si vous ajoutez tous les comptes non humains à un groupe spécifique dans ce but, vous pouvez ensuite affecter à ce groupe les droits « Interdire l'ouverture d'une session locale » et « Interdire l'ouverture de sessions par les services Bureau à distance » dans un objet de stratégie de groupe (par exemple, Stratégie de domaine par défaut), qui sont appliqués à tous les ordinateurs du domaine.

Restez vigilant si vous interdisez le droit de connexion au réseau. Il se peut que l'application qui utilise le compte ait besoin d'accéder à des ressources sur d'autres réseaux.

Contribution d'Active Roles

Active Roles permet d'exiger et de confirmer (par l'intermédiaire de rapports de comparaison) que l'ensemble des comptes non humains sont configurés à l'aide de la convention de dénomination, des paramètres d'attribut, de l'emplacement d'objet et de l'appartenance à un groupe (en lien avec les objets de stratégie de groupe) qui respectent les normes de votre entreprise. De plus, vous pouvez activer des workflows si-alors afin d'appliquer l'approbation (progressive) à tous les comptes (de service) créés dans un emplacement d'unité organisationnelle donné et/ou pour ces comptes avec un préfixe spécifique, etc. Toutes ces actions sont entièrement auditées et associées à l'individu qui en est réellement responsable.

Étape 8 : contrôler les exceptions

Documenter les exceptions légitimes et approuvées

Le vieil adage dit que les règles sont faites pour être transgressées. Il existe bel et bien des exceptions légitimes aux normes appliquées aux comptes d'utilisateurs. Par exemple, il se peut que l'une de vos applications ait besoin d'un compte d'utilisateur dont le nom ne respecte pas votre convention de dénomination classique. Dans de telles situations, vous devez être en mesure de documenter les exceptions légitimes et approuvées. Pour y parvenir, le meilleur moyen consiste à utiliser des exceptions nommées en fonction de l'unité organisationnelle ou à signaler les comptes qui font exception dans le champ Description ou Notes.

Mais il ne suffit pas de signaler qu'un compte fait exception ; l'objet et le propriétaire du compte doivent également être documentés, comme le décrit l'étape 7.

Type de connexion	Droits de connexion
Interactive	Autoriser l'ouverture d'une session locale Interdire l'ouverture d'une session locale
Bureau à distance	Autoriser l'ouverture de session par les services Bureau à distance Interdire l'ouverture de session par les services Bureau à distance
Service	Ouvrir une session as a service Interdire l'ouverture de session as a service
Tâche planifiée	Ouvrir une session as a service Interdire l'ouverture de session as a service
Réseau (p. ex., accès à un dossier partagé)	Ouvrir une session en tant que tâche Interdire l'ouverture de session en tant que tâche
Chiffrement en transit RDP FIPS 140-2	Accéder à cet ordinateur à partir du réseau Interdire l'ouverture de session par les services Bureau à distance

Le vieil adage dit que les règles sont faites pour être transgressées. Il existe bel et bien des exceptions légitimes aux normes appliquées aux comptes d'utilisateurs.

Les exceptions ne doivent pas devenir monnaie courante

Attention toutefois aux implémentations AD dans lesquelles un grand pourcentage de comptes font exception. Le personnel peut prendre l'habitude de signaler qu'un compte fait exception dès qu'il ne trouve pas pratique de suivre les normes et procédures de maintenance des comptes. Le provisionnement des exceptions ne doit pas faire l'objet d'abus.

Contribution d'Active Roles

Active Roles permet de répondre aux exceptions et de les contrôler grâce à des règles qui garantissent que les comptes qui font exception sont autorisés uniquement dans certains emplacements. Lorsqu'une exception est créée dans un emplacement dédié, Active Roles assure que l'ensemble des normes de configuration obligatoires, des attributs ou d'autres contraintes stratégiques sont respectés et appliqués.

Par ailleurs, vous pouvez employer des workflows d'approbation avec réaffectation hiérarchique pour les demandes de création (manuelle ou programmatique) associées à de nouvelles tentatives d'exceptions afin d'éviter que l'exception ne devienne la règle.

Étape 9 : contrôler l'autorité des administrateurs

Restreindre les personnes autorisées à créer des comptes

Si AD regorge souvent de comptes inutiles ou obscurs, c'est parce qu'un trop grand nombre de personnes sont autorisées à créer des comptes d'utilisateurs.

Afin d'appliquer des contrôles de sécurité à la création des comptes, qui sont des éléments cruciaux en matière de sécurité et de conformité, vous devez limiter le nombre de personnes qui sont autorisées à créer des comptes à quelques techniciens expérimentés.

Utiliser l'assistant Délégation de contrôle

AD prend en charge la stratégie de moindres privilèges en autorisant les administrateurs de domaine à déléguer certaines autorisations à des unités organisationnelles spécifiques. Lorsqu'elle est correctement implémentée, la fonctionnalité de délégation de contrôle d'AD permet aux collaborateurs de

Active Roles inclut plus de 300 modèles d'accès utilisés couramment, éprouvés et testés, qui font d'Active Roles l'un des outils les plus rapides pour se lancer et devenir opérationnel.

mener à bien leurs missions sans leur donner davantage de droits que ceux strictement nécessaires. Par exemple, plutôt que de faire passer les membres du centre d'assistance en administrateurs de domaine, vous pouvez accorder au groupe du centre d'assistance l'autorisation Réinitialiser le mot de passe sur l'unité organisationnelle qui contient vos comptes d'utilisateurs finaux.

Pour lancer l'assistant Délégation de contrôle, il vous suffit de cliquer avec le bouton droit de la souris sur l'unité organisationnelle souhaitée et de sélectionner « Délégation de contrôle ». La figure suivante illustre l'autorité Réinitialiser le mot de passe, déléguée au groupe du centre d'assistance.

Contribution d'Active Roles

Dans Active Roles, les « rôles » sont des modèles d'accès. Les modèles d'accès regroupent une sélection d'autorisations qui peuvent être très précises et s'appliquer à n'importe quel emplacement de votre infrastructure Active Directory. Il est même possible de les appliquer à des emplacements virtuels que vous pouvez personnaliser et maintenir de manière dynamique au sein de l'outil.

Les modèles d'accès regroupent plusieurs autorisations AD qui sont catégorisées par objectif cible et qui vous permettent de déléguer facilement des autorisations d'administration selon un modèle à moindres privilèges. Ces jeux d'autorisations peuvent être simples (comme avec l'autorisation Réinitialiser le mot de passe) ou détaillés, avec des autorisations en écriture/lecture/liste sur tout ou partie des attributs d'un objet AD. Active Roles inclut plus de 300 modèles d'accès utilisés couramment, éprouvés et testés, qui font d'Active Roles l'un des outils les plus rapides pour se lancer et devenir opérationnel – mais aussi pour générer un retour sur investissement. En outre, la création de modèles est simple et rapide.

Étape 10 : tirer profit de la technologie de workflow

Mieux vaut SharePoint que l'e-mail seul pour gérer les comptes

De nombreuses organisations essaient de traiter les demandes de nouveaux comptes, les cessations de contrat, les modifications de postes et d'autres types d'approbation sans autre outil que l'e-mail. Cette approche ne permet pas de respecter facilement les normes de gestion des comptes ni d'entrer en conformité. La technologie de workflow, telles les listes dans SharePoint, ne permettra jamais d'automatiser

entièrement la gestion des comptes, mais elle permet sans nul doute de l'améliorer. Par exemple, SharePoint est une technologie de workflow qui vous permet d'attribuer à des listes d'annonces une adresse e-mail qui transforme les e-mails entrants en nouveaux éléments de liste, et de déplacer tous les documents joints vers les pièces jointes de l'élément de la liste. Vous pouvez personnaliser la liste à l'aide de champs Statut afin de suivre les étapes du traitement de l'élément de la liste.

Exemple : utiliser SharePoint pour gérer les changements de comptes faisant suite à une cessation de contrat

Par exemple, vous pouvez utiliser une liste e-mail SharePoint pour organiser les notifications de cessation de contrat et documenter les points de conformité avec la procédure qui est appliquée aux utilisateurs sortants. Si vous utilisez l'option 2 ou 3 de l'étape 5, configurez l'application de RH de sorte qu'elle envoie ses e-mails à votre liste SharePoint, et ajoutez les colonnes Statut et Nom à la liste. Lorsque de nouvelles notifications ou rapports en lien avec une cessation de contrat apparaissent dans la liste, vous pouvez désactiver les comptes associées dans AD et modifier l'élément de la liste afin d'indiquer qu'il a été traité et quels comptes ont été désactivés au cours de la procédure. Vous pouvez même vous abonner à des alertes sur la liste afin d'être averti de la création d'éléments. Des listes similaires peuvent être créées pour les demandes de nouveaux comptes et les notifications de changement de poste. Dans tous les cas, vous devez tirer profit de la technologie de workflow afin de réduire le fardeau quotidien des administrateurs, mais aussi améliorer votre conformité.

Contribution d'Active Roles

L'architecture d'Active Roles permet d'appliquer des fonctionnalités de rapports et d'audit à toutes les opérations CRUD. Cela signifie que les rapports sont disponibles pour toutes les créations ou modifications de comptes, toutes les créations ou modifications de groupes et les déprovisionnements de comptes. En fait, tout ce qui se passe via Active Roles est audité.

Les rapports répondent à cinq questions incontournables (qui, quoi, quand, où et pourquoi) et peuvent être envoyés automatiquement aux auditeurs. En outre, les rapports sont accessibles en ligne via un portail Web.

Le corollaire de ce haut niveau d'audit est la possibilité d'annuler des actions en toute sécurité. Par exemple, un compte déprovisionné par erreur peut être restauré en quelques clics sans aucune interruption d'activité.

Maintenir un environnement AD propre et sûr automatiquement

Étendre et automatiser les fonctionnalités des outils natifs pour limiter les risques

Les 10 recommandations de ce document vous aideront à nettoyer les comptes d'utilisateurs de votre environnement AD, mais aussi à éviter que des problèmes ne se répètent. Toutefois, si vous vous contentez de suivre ces recommandations sans investir dans des outils supplémentaires, la plupart des tâches administratives et des confirmations manuelles reposeront sur l'équipe informatique, et vous continuerez de dépendre des utilisateurs finaux, des responsables et des chargés des RH pour être notifié des évènements importants du cycle de vie des utilisateurs.

Les équipes informatiques d'un grand nombre d'organisations passent beaucoup trop de temps à créer et à clore des comptes d'utilisateurs dans AD. Les outils natifs sont inefficaces et chronophages. Avec les processus manuels qu'ils impliquent, les erreurs humaines potentielles augmentent et peuvent compromettre la sécurité et la stabilité de votre environnement Windows. De plus, de nombreuses organisations disposent de processus tout autant inefficaces mais entièrement séparés pour la création de comptes dans les systèmes hors de Windows, ce qui représente un fardeau administratif supplémentaire et introduit encore davantage de risques pour la sécurité.

Active Roles automatise la maintenance des comptes d'utilisateurs, limite le nombre de tâches et renforce la sécurité

Comme vous l'avez constaté dans la section « Contribution d'Active Roles » de chaque étape, Active Roles automatise la majorité des tâches de maintenance d'AD et offre tout un panel de fonctionnalités qui éliminent la dépendance aux utilisateurs finaux, aux responsables et aux chargés des RH. Active Roles vous aide à accomplir chacune des étapes figurant dans ce document.

Avec Active Roles, AD peut se synchroniser à des bases de données et des répertoires externes, y compris SharePoint Server, les applications métiers et bien d'autres. Sur la quasi-totalité des systèmes d'exploitation modernes, chaque système peut désormais bénéficier de la synchronisation d'identité bidirectionnelle sur site ou dans le Cloud. Cerise sur le gâteau : en s'intégrant à votre application de RH, la création de comptes d'identité peut être utilisée pour la gestion des accès automatisée.

Active Roles automatise la création et l'administration de comptes basés sur AD. Les utilisateurs sont affectés à des rôles professionnels qui sont mappés à leurs responsabilités afin de veiller à ce qu'ils disposent exactement des autorisations adéquates sur les ressources nécessaires – rien de plus et rien de moins. Les utilisateurs sont satisfaits, car ils ont accès aux ressources dont ils ont besoin pour mener à bien leurs missions ; les administrateurs sont aussi satisfaits, car ils gagnent du temps sur une multitude de tâches chronophages et fastidieuses qui sont désormais automatisées.

Active Roles fournit des fonctions préconfigurées de gestion des comptes individuels et de groupe, de sécurité stricte axée sur les rôles, d'administration quotidienne des identités et d'audit et de rapport intégrés pour les environnements centrés sur Windows.

Active Roles inclut les fonctionnalités suivantes :

- **Accès sécurisé** – Active Roles agit comme un pare-feu virtuel pour Active Directory, vous permettant de contrôler les accès à l'aide de la délégation, en utilisant un modèle à moindres privilèges. L'utilisation de politiques d'administration définies et des autorisations associées permet d'appliquer strictement les règles d'accès, éliminant ainsi les erreurs et les incohérences récurrentes dans les approches natives à la gestion d'AD. En outre, des procédures d'approbation robustes et personnalisées établissent un processus et une supervision informatiques conformes aux exigences de l'entreprise, avec des chaînes de responsabilité qui complètent la gestion automatisée des données d'annuaire.
- **Création de comptes automatisée** – Automatisez une multitude de tâches, notamment :
- La création de comptes d'utilisateurs et de groupes dans AD/AAD

- La création de boîtes aux lettres Exchange/Exchange Online
- L'affectation de membres à des groupes
- L'attribution des ressources dans Windows

Active Roles automatise également la réaffectation et la suppression des droits d'accès des utilisateurs dans AD/AAD et dans les systèmes associés à AD (notamment la cessation des utilisateurs et des groupes), garantissant ainsi l'efficacité et la sécurité du processus administratif pendant tout le cycle de vie des groupes et des utilisateurs. Lorsque l'accès d'un utilisateur doit être modifié ou supprimé, les mises à jour se font automatiquement dans AD, Exchange, SharePoint, OCS, Lync et Windows, tout comme dans les systèmes joints à AD comme UNIX, Linux et Mac OS X.

- **Gestion quotidienne de l'annuaire –** Vous permet de gérer facilement l'ensemble des éléments suivants :
- Les destinataires d'Exchange/Exchange Online, notamment l'attribution des boîtes de messagerie/OCS, la création, le déplacement, les suppressions, les autorisations et les listes de distribution
- Les groupes
- Les ordinateurs, notamment les partages, imprimantes, utilisateurs locaux et groupes
- Active Directory, notamment les services AD LDS
- Inclut également une interface intuitive qui améliore les tâches quotidiennes d'administration et les opérations d'assistance par le biais d'un composant logiciel enfichable (CLE) MMC et d'une interface Web.
- **Gestion des groupes et des utilisateurs dans un environnement hébergé –** Active Roles fonctionne dans un environnement hébergé dans lequel les comptes d'un domaine client AD sont synchronisés avec un domaine AD hébergé. La solution permet de gérer des comptes d'utilisateurs et de groupes du domaine client vers le domaine hébergé en synchronisant les attributs et mots de passe. Utilisez des connecteurs prêts à l'emploi pour synchroniser vos comptes AD locaux avec d'autres plates-formes et applications. Tirez profit d'une gamme croissante de plus de 30 connecteurs (https://www.cloud.oneidentity.com/products/connect/connectors) afin de multiplier les services et les applications basés sur le Cloud, comme Salesforce, G-Suite et ServiceNow via One Identity Starling Connect.
- **Consolidation des points de gestion avec l'intégration –** Active Roles complète votre stratégie de gestion des accès et des identités et vos technologies existantes. La solution permet d'étendre toutes les fonctionnalités, de simplifier et de consolider les points de gestion en assurant une intégration aisée avec de nombreux produits One Identity, notamment Identity Manager, Privileged Password Manager, Desktop Virtualization, Authentication Services, Defender, Password Manager et Quest Change Auditor. Elle automatise et étend également les fonctionnalités de PowerShell, d'ADSI, de SPML et des interfaces Web personnalisables.

Performances, agilité et sécurité en 10 étapes

Étape 1 : effectuer l'analyse régulière des comptes

Étape 2 : associer les comptes aux données sur les collaborateurs

Étape 3 : surveiller les nouveaux comptes

Étape 4 : automatiser la maintenance des comptes

Étape 5 : traiter les utilisateurs ayant quitté l'organisation et les changements de rôles

Étape 6 : traiter les comptes dormants

Étape 7 : gérer les comptes non humains

Étape 8 : contrôler les exceptions

Étape 9 : contrôler l'autorité des administrateurs

Étape 10 : tirer profit de la technologie de workflow

Ces 10 étapes vous permettent de nettoyer vos données AD/Azure AD, ce qui est un élément critique pour les performances et la sécurité. One Identity Active Roles vous aide à mettre en œuvre ces étapes et à maintenir la précision et la pertinence de vos données à l'avenir. Prenez cette voiture d'exposition, donnez-lui des données propres et profitez des performances, de la rapidité et de l'ergonomie que vous offre Active Roles dans votre stratégie AD/AAD.

Microsoft Active Directory et One Identity Active Roles : mieux ensemble

À propos de One Identity

One Identity, une entité Quest, aide les organisations 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 organisations 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

Whitepaper_2021_MicrosoftBetterTogetherwithOIDActiveRoles_PG-FR-WL-67415