FICHE TECHNIQUE

Active Roles

Gestion et sécurité pour Active Directory hybride et d'autres environnements.

Avantages

- Protège les données essentielles d'Active Directory et d'Azure Active Directory
- Réglemente les accès administratifs à l'aide du modèle de moindre privilège
- Suppression des limitations des outils natifs
- Automatise la création et la suppression des comptes utilisateurs/groupes
- Gère les comptes, notamment pour Exchange Online, Lync, SharePoint Online, Office 365, etc.
- Outil intuitif unique pour un environnement hybride
- Génère des rapports prêts pour l'audit
- Se déploie rapidement pour limiter les délais de rentabilité
- Sachez qui a effectué quelle modification et à quel moment
- Architecture modulaire pour répondre aux besoins actuels et futurs de l'activité
- Étend la gestion des identités centrée sur AD à de nombreux systèmes SaaS et non Windows

Présentation

Les difficultés liées à la gestion des comptes dans Active Directory (AD) et Azure AD sont nombreuses et variées. En outre, la sécurisation de ces systèmes critiques constitue souvent un véritable défi. Avec les outils natifs, la sécurité et la gestion de l'environnement AD hybride se révèlent inefficaces, fragmentées et sujettes aux erreurs.

Les entreprises actuelles évoluent à un rythme tel que les départements peinent à suivre les demandes de création, modification ou suppression des accès à l'environnement AD hybride. Ils sont en outre confrontés à des problèmes de sécurité tels que les salariés congédiés qui conservent un accès à une précieuse propriété intellectuelle. Ils doivent aussi répondre aux besoins de l'entreprise et satisfaire aux demandes de rapports des auditeurs. Ajoutez à cela la nécessité de contrôler précisément l'accès administrateur à Active Directory et Azure Active Directory, et faire face à l'explosion des applications non Windows et SaaS qui doivent également être gérées.

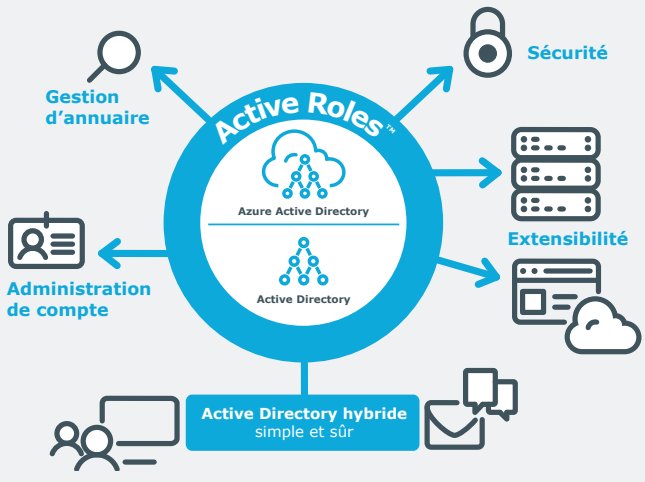
Heureusement, l'aide dont ils ont tant besoin vient d'arriver.
One Identity Active Roles permet d'automatiser ces tâches administratives fastidieuses et sujettes aux erreurs, et de résoudre les problèmes de sécurité. Active Roles automatise et unifie l'administration des comptes et des groupes tout en protégeant et sécurisant l'accès administrateur dont l'importance est cruciale.

Active Roles fournit des outils automatisés pour la gestion des comptes d'utilisateurs et de groupes de manière à palier les lacunes des outils Active Directory et Azure Active Directory natifs. Vous gagnez ainsi en efficacité et en précision, et réduisez le nombre d'interventions manuelles. Basé sur une architecture modulaire, Active Roles vous permet de répondre facilement aux besoins actuels et futurs de votre entreprise.

Fonctionnalités

Optimisé pour AD hybride

La solution Active Roles est optimisée pour répondre à la fois aux besoins des solutions AD locales et Azure AD dans un déploiement hybride. Elle propose une console centralisée, des workflows unifiés et une expérience d'administration homogène dans l'ensemble de votre environnement hybride. Elle élimine la nature fastidieuse, propice aux erreurs et limitée de l'utilisation de différents outils et de processus manuels.



Accès sécurisé

La solution Active Roles offre une gestion complète des comptes à privilèges pour Active Directory et Azure Active Directory. Avec la délégation, vous pouvez contrôler l'accès en utilisant un modèle basé sur le principe du moindre privilège. Basée sur des stratégies d'administration définies et leurs autorisations associées, elle génère des règles d'accès et les applique de façon stricte, éliminant ainsi les erreurs et les incohérences fréquentes avec les approches natives de la gestion d'AD hybride. 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.

Automatisation de l'administration des comptes

La solution Active Roles automatise une grande variété de tâches, notamment :

- La création de comptes d'utilisateurs et de groupes dans AD et AAD
- L'extension des tâches d'administration de comptes basées sur AD/AAD aux systèmes non-Windows et aux applications SaaS.
- La création de boîtes aux lettres Exchange et Exchange Online
- Le remplissage de groupes dans AD et AAD
- L'attribution des ressources dans Windows

Ce logiciel automatise également la réaffectation et la suppression des droits d'accès des utilisateurs dans AD, AAD et dans les systèmes associés à AD (notamment le déprovisioning des utilisateurs et des groupes). Il garantit 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 l'ensemble des systèmes et applications concernés de l'environnement AD/AAD hybride, tout comme dans les systèmes joints à AD comme Unix, Linux et Mac OS X, ainsi qu'un ensemble varié et croissant d'applications SaaS populaires via la solution One Identity Starling Connect.

Gestion quotidienne de l'annuaire

La solution Active Roles facilite la gestion des éléments suivants pour les environnements locaux et Azure AD :

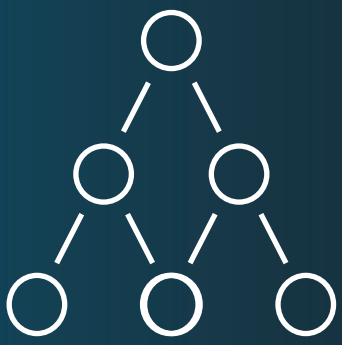
- Les destinataires d'Exchange, notamment l'attribution des boîtes de messagerie/OCS, la création, le déplacement, les suppressions, les autorisations et les listes de distribution
- Les groupes
- Les ordinateurs, notamment les partages, imprimantes, utilisateurs locaux et groupes
- Active Directory et Azure Active Directory

La solution Active Roles possède des interfaces intuitives qui optimisent les tâches quotidiennes d'administration et d'assistance de l'environnement AD/AAD hybride à l'aide d'un composant logiciel enfichable MMC et d'une interface Web.

Elle prend également en charge les options de personnalisation les plus courantes et populaires telles que PowerShell pour assurer le maximum de flexibilité et la possibilité d'utiliser Active Roles de la manière la plus avantageuse pour votre entreprise.

Extension de la portée de l'administration

La solution Active Roles prend en charge le standard SCIM qui permet d'inclure toute application SaaS compatible SCIM (via One Identity Starling Connect) dans les fonctionnalités d'administration de groupes et de comptes basée sur AD d'Active Roles.



Lorsque l'accès d'un utilisateur doit être modifié ou supprimé, les mises à jour se font automatiquement dans AD, AAD, Exchange Online, SharePoint Online, OCS, Skype Entreprise et Windows, tout comme dans les systèmes joints à AD comme Unix, Linux, Mac OS X et les applications SaaS.

Gestion des groupes et des utilisateurs dans un environnement hébergé

Synchronisez des clients de domaine AD avec un domaine AD hôte dans des environnements hébergés. La solution Active Roles permet de gérer des comptes d'utilisateurs et de groupes du domaine client au domaine hébergé en synchronisant les attributs et mots de passe. Utilisez des connecteurs prêts à l'emploi pour synchroniser vos comptes AD locaux avec Microsoft Office 365, Lync Online/ Skype Entreprise et SharePoint Online.

Consolidation des points de gestion par intégration

La solution Active Roles complète votre stratégie de gestion des accès et des identités et vos technologies existantes. Elle simplifie et consolide les points de gestion en assurant une intégration aisée avec de nombreux produits One Identity, notamment Identity Manager, Safeguard, Authentication Services, Password Manager et ChangeAuditor. Elle automatise et étend également les fonctionnalités de PowerShell, d'ADSI, de SPML et des interfaces Web personnalisables.

La solution Active Roles inclut toutes les technologies de synchronisation nécessaires pour gérer et sécuriser :

- Lync/Skype Enterprise
- Exchange
- One Drive
- SharePoint
- AD LDS
- Office 365 (y compris les rôles et les groupes)
- Azure AD
- Microsoft SQL Server
- OLE DB (MS Access)
- Fichiers plats

À propos de One Identity

One Identity, une entité Quest Software, aide les entreprises à mettre en place une stratégie de sécurité centrée sur l'identité. Grâce à notre portefeuille unique d'offres de gestion des identités et des accès, y compris de gestion des accès privilégiés et de gouvernance des identités, toutes augmentée par une stratégie de Cloud hybride, One Identity aide les entreprises à réaliser leur potentiel sans être entravées par la sécurité et tout en étant protégées contre les menaces. One Identity fait preuve de son engagement inégalé dans la réussite à long terme de ses clients. Plus de 7 500 entreprises à travers le monde font confiance aux solutions One Identity pour gérer plus de 125 millions d'identités, améliorant leur agilité et leur efficacité tout en sécurisant l'accès à leurs systèmes de données dans les environnements sur site, hybrides ou Cloud. Pour tout complément d'information, consultez le site www.oneidentity.com

Datasheet_2019_ActiveRoles74_US_RS_42104