ONE IDENTITY

Cornell figure au tableau d'honneur de la sécurité Active Directory

La solution Active Roles de One Identity aide l'université de Cornell à sécuriser un environnement AD distribué, hétérogène et fragmenté.

Pays : **États-Unis**

Effectifs : **Corps enseignant : 1 679 | Personnel administratif : 8 000**

Étudiants : **23 000**

Secteur : **Enseignement supérieur**

Site Web : **www.cornell.edu/about/**

Enjeux

- Assurer la cohérence dans un environnement AD hautement distribué et hétérogène
- Protéger les données universitaires contre les attaques visant AD
- Éliminer les erreurs humaines et toute utilisation abusive des informations d'identification des administrateurs AD

Résultats

- Mise en œuvre du modèle de délégation complexe souhaité pour les administrateurs AD
- Authentification et autorisation simplifiées sous Unix/Linux, basées sur les tâches administratives gérées par AD
- Élimination du risque d'accès administrateur illimité sur l'ensemble des domaines AD sans entraver les activités informatiques

Solutions

- Sécurité Active Directory

Produits

- Active Roles by One Identity

Dans l'enseignement supérieur, les risques sont omniprésents. Compte tenu de la multitude d'informations personnelles, de données financières et de propriétés intellectuelles qu'elles détiennent, les universités constituent des cibles de choix pour les pirates. De plus, le fait qu'une grande partie de la charge de travail informatique dans les établissements d'enseignement supérieur soit gérée par des étudiants, des prestataires et du personnel temporaire au sein de réseaux très dispersés et peu contrôlés ne fait qu'aggraver la situation. Heureusement, l'université de Cornell a trouvé une solution à ces enjeux de longue date.

« L'une de nos principales préoccupations en matière de sécurité est la compromission de nos domaines Active Directory, déclare Muhammad Arif, Gestion des identités, CIT de l'université de Cornell. Nous ne pouvons pas nous permettre les conséquences d'une telle violation, qu'il s'agisse du vol de données sensibles ou de l'atteinte à la réputation de l'Université. Nous avions auparavant un environnement très décentralisé, composé de plus d'une centaine de domaines Active Directory (AD) totalement indépendants, indique Muhammad Arif. Ces domaines ne faisaient l'objet d'aucune supervision, qu'il s'agisse de leur configuration, de la mise en œuvre des paramètres de sécurité ou des mécanismes d'authentification et des droits d'accès accordés. Tous ces facteurs exposaient les données et la réputation de l'université à des risques importants. Nous n'avions aucune visibilité sur le niveau de sécurité de ces domaines ni sur les activités du service informatique. »

L'un des principaux enjeux liés à la sécurité d'AD réside dans les limites des outils natifs. Le compte d'administrateur AD est généralement partagé entre tous les membres du personnel informatique nécessitant ces privilèges. Les autorisations reposent généralement sur le principe du tout ou rien, sans responsabilité individuelle quant aux actions réalisées avec des droits d'administration. De plus, des tâches telles que la délégation des droits, leur élévation temporaire ou encore la duplication des stratégies entre domaines sont extrêmement complexes, voire impossibles à mettre en œuvre.

« Avec un environnement Active Directory aussi largement réparti et un si grand nombre d'administrateurs répartis dans plusieurs services, nous avions besoin d'un moyen de déléguer les droits d'accès pour gérer les objets AD, signale Muhammad Arif. De plus, nous avions besoin d'octroyer aux administrateurs d'autres services la capacité de "sous-déléguer" les droits d'accès. Ce modèle de délégation nécessitait de contrôler correctement la dénomination des objets dans AD, ainsi que l'audit des actions effectuées avec des droits d'administrateur. » L'Université a estimé que le moyen le plus efficace de répondre aux enjeux de sécurité posés par son environnement AD était de se doter d'un logiciel commercial prêt à l'emploi et capable d'enrichir les fonctionnalités natives des outils AD en offrant le niveau de précision et de contrôle nécessaire pour réduire les risques et renforcer la sécurité. « Nous recherchions une solution qui réponde à nos besoins, qui soit aboutie et qui ait fait ses preuves auprès de clients dont les environnements présentaient des défis et des complexités similaires aux nôtres, explique Muhammad Arif. Nous recherchions également un fournisseur capable d'offrir un excellent service d'assistance sur lequel nous pourrions compter en cas de besoin. »

> **Active Roles offrait d'emblée plusieurs fonctionnalités clés, notamment la délégation et la sous-délégation, l'application des conventions de dénomination, l'historique des modifications et l'application des politiques relatives aux objets AD.**
>
> *Muhammad Arif, Gestion des identités, CIT, Université de Cornell*

> **Avec Active Roles en place, nous avons planifié un bon modèle de gestion des délégations, des normes de dénomination, de la structure des unités organisationnelles et de l'accès à AD pour plusieurs centaines d'administrateurs… Et ce modèle fonctionne actuellement depuis près d'une décennie.**
>
> *Muhammad Arif, Gestion des identités, CIT, Université de Cornell*

Depuis près de 20 ans, la solution Active Roles de One Identity répond aux besoins en matière d'administration et de sécurité d'AD de plus de 3 500 organisations, telles que l'université de Cornell. Elle dépasse les limites des outils natifs grâce à l'automatisation, aux workflows, aux processus de validation et à la centralisation des tâches d'administration des comptes Active Directory, telles que la création de comptes et la gestion des groupes. De plus, le modèle d'accès basé sur les rôles d'Active Roles permet aux organisations de mettre en œuvre une sécurité basée sur le principe des moindres privilèges pour les administrateurs grâce à de nombreuses options de sécurité flexibles, telles que les groupes temporaires et les workflows basés sur des modèles. « Active Roles offrait d'emblée plusieurs fonctionnalités clés, notamment la délégation et la sous-délégation, l'application des conventions de dénomination, l'historique des modifications et l'application des politiques relatives aux objets AD, ajoute Muhammad Arif. Cette solution offrait une plus grande souplesse grâce à la personnalisation aisée de l'interface Web et à la prise en charge des interfaces de programmation que nous utilisons, notamment VBScript, PowerShell et SPML. Ses fonctionnalités de personnalisation nous ont permis de configurer les droits d'accès de manière à ce que les administrateurs puissent uniquement consulter et modifier leurs unités organisationnelles dans Active Directory. »

Grâce à Active Roles, l'Université peut gérer ses différents environnements AD avec la certitude absolue que rien ne peut se produire en dehors du cadre défini par la stratégie en vigueur (et de nombreuses opérations peuvent désormais s'effectuer sans aucune intervention du service informatique). De plus, les administrateurs ne disposent que des autorisations nécessaires pour accomplir leurs tâches, ni plus ni moins. Toutes leurs actions sont contrôlées, suivies et peuvent même être annulées si nécessaire.

ONE IDENTITY

« Avec Active Roles en place, nous avons planifié un bon modèle de gestion des délégations, des normes de dénomination, de la structure des unités organisationnelles et de l'accès à AD pour plusieurs centaines d'administrateurs, déclare Muhammad Arif. Et ce modèle fonctionne actuellement depuis près d'une décennie. Nous avons également pu intégrer de nouvelles fonctionnalités grâce aux scripts, aux attributs virtuels et à la personnalisation Web afin de répondre à de nouvelles exigences. Grâce à Active Roles, je pense que la confiance dans la capacité de notre équipe informatique centrale à fournir un service fiable a augmenté, sans parler de la réduction des risques et de l'augmentation correspondante de la sécurité. » Muhammad Arif, Gestion des identités, CIT, Université de Cornell.

L'un des principaux avantages d'Active Roles de One Identity réside dans sa capacité à dépasser les limites d'AD. La solution prend également en charge Entra ID (et tout ce que cela implique) et peut être étendue aux systèmes Unix/Linux via une passerelle Active Directory, telle que One Identity Authentication Services, ainsi qu'à un grand nombre d'applications Web via la norme SCIM. « Comme nous sommes un établissement d'enseignement et de recherche, de nombreux enseignants, membres du personnel et étudiants utilisent des systèmes Linux comme outil de travail principal, déclare Muhammad Arif. Une fois qu'AD est devenu le fournisseur principal en matière d'authentification et d'autorisation, nous avons dû trouver un moyen d'intégrer les systèmes Linux à AD pour ces fonctions. Nous utilisons Active Roles pour publier automatiquement des attributs Unix à partir des objets "Utilisateur" et "Groupe" d'AD. Cela permet aux administrateurs de service d'activer des comptes utilisateurs en tant que "comptes Unix" au sein d'Active Roles, ce qui signifie qu'ils peuvent intervenir eux-mêmes sans avoir à démarcher le service informatique central pour activer des comptes Unix individuels en fonction des besoins. Grâce à Active Roles, je pense que la confiance dans la capacité de notre organisation informatique centrale à fournir un service fiable a augmenté, sans parler de la réduction des risques et de l'augmentation correspondante de la sécurité », conclut Muhammad Arif.

> **Grâce à Active Roles, je pense que la confiance dans la capacité de notre organisation informatique centrale à fournir un service fiable a augmenté, sans parler de la réduction des risques et de l'augmentation correspondante de la sécurité.**
>
> *Muhammad Arif, Gestion des identités, CIT, Université de Cornell*

À propos de One Identity

One Identity offre aux entreprises du monde entier une sécurité des identités fiable pour protéger toutes les identités, humaines et informatiques. Avec des options de déploiement et des conditions d'abonnement flexibles, allant de l'autogestion à la gestion complète, nos solutions s'intègrent directement sur la structure d'identité d'une organisation pour renforcer le périmètre d'identité, réduire le risque de violation et maintenir la gouvernance et la conformité à l'échelle. Basée à Cork, en Irlande, et bénéficiant de la confiance de 80 entreprises de la liste Fortune 100, One Identity est l'un des principaux fournisseurs de solutions intégrées de gouvernance et administration des identités (IGA) et de gestion des accès à privilèges (PAM) pour une sécurité des identités sans compromis. Pour en savoir plus, visitez : www.oneidentity.com.

CaseStudy-Cornell-University-PG-FR-WL-105183

ONE IDENTITY