Le parlement britannique optimise la gestion d'Active Directory (AD)

UK Parliament Digital Service

Avec Active Roles, le PDS simplifie la gestion d'Active Directory tout en améliorant la sécurité et libérant du temps pour la migration Cloud hybride

Client :

Parliamentary Digital Service (PDS, service numérique parlementaire)

Secteur d'activité :

Secteur public - Gouvernment

Pays :

Royaume-Uni

Site Internet :

www.parliament.uk

Défi

- Gestion inefficace des JML (Joiners, Movers, Leavers : nouvelles recrues, changements de poste, départs) se traduisant en heures perdues chaque mois
- Augmentation des risques avec le contrôle manuel de la PAM (gestion des accès à privilèges)
- Absence de prise en charge du Cloud hybride

Solution

- One Identity Active Roles

Libère du temps afin de se consacrer aux projets de migration stratégiques

Automatise les processus JML et de PAM pour renforcer la protection, l'efficacité et la sécurité

Traite les complexités liées aux licences pour les conférences Zoom pendant la pandémie

Dirige la migration vers Active Directory et l'intégration à Azure Active Directory

Le PDS (Parliamentary Digital Service, service numérique parlementaire) sert la chambre des communes britannique, la chambre des Lords ainsi que le personnel parlementaire. Doté de nombreuses missions, le PDS soutient l'équipe informatique, gère le réseau parlementaire, développe des applications et se prépare aux besoins technologiques à venir. Il gère également le site web et les réseaux sociaux du parlement.

Alors que des foules de touristes se pressent autour du parlement britannique, les foules de criminels hors du réseau parlementaire sont d'autant plus impressionnantes. « Les menaces de sécurité sont constantes », explique Cherry O'Donnell, responsable de la gestion des accès et des identités au PDS. « Nous sommes une cible majeure ; la sécurité du réseau est ainsi une priorité absolue ».

Gestion de multiples changements

Maintenir la sécurité d'un réseau tout en gérant rigoureusement les accès n'est pas une mince affaire. Cela représente un défi pour PDS en raison du nombre et de la diversité des comptes dans Active Directory (AD).

Il existe des comptes pour les membres du parlement (députés) et leur personnel ainsi que pour les Lords et leurs collaborateurs. Ensuite, il y a plus de 2 000 salariés parlementaires titulaires et des comptes qui devront être créés ou supprimés pour les 100 à 200 personnes qui rejoignent ou quittent le réseau chaque mois. De plus, les groupes AD devront être mis à jour pour de nombreux utilisateurs du réseau qui changent de poste au sein du parlement. Enfin, parmi les groupes AD, on trouve les comptes à privilèges que PDS doit contrôler afin que les administrateurs puissent accéder au matériel, notamment les serveurs, pour des tâches d'application de correctifs par exemple.

> Avec One Identity Active Roles nous disposons d'**une vue limpide** des **permissions** à tout moment ainsi que dans le passé. Nous ne laissons **pas de place à l'erreur**. »
>
> Cherry O'Donnell, responsable de la gestion des accès et des identités du PDS

Des tâches chronophages

Que ce soit pour gérer les JML (nouvelles recrues, changements de poste et départs) ou contrôler la PAM (gestion des accès à privilèges), le travail au sein d'AD était majoritairement manuel. Cela consommait de nombreuses heures chaque mois que l'équipe du PDS aurait pu utiliser sur des projets stratégiques. L'absence d'automatisation entraînait un risque accru d'erreur humaine et augmentait la possibilité à une personne d'accéder à des données non autorisées. En outre, l'ancienne solution de gestion des accès n'était pas optimisée pour Azure AD dans une solution hybride constituée d'AD local et dans le Cloud.

« Les heures que nous économisons nous permettent d'accélérer d'autres initiatives comme l'adoption de nouvelles plateformes pour Active Roles 7.4 ».

Cherry O'Donnell, responsable de la gestion des accès et des identités du PDS

Le PDS a engagé One Identity pour l'aider à renforcer la gestion et la sécurité d'une infrastructure AD hybride. L'organisation possédait une version antérieure de One Identity Active Roles et elle souhaitait optimiser sa solution pour profiter des innovations récentes du produit. Épaulé par l'équipe de One Identity, le PDS a débuté le processus d'amélioration en remplaçant des milliers de lignes Shell de ligne de commande et de langage de script avec Active Roles en utilisant les modules PowerShell et les workflows Active Roles. « Un conseiller One Identity travaille avec nous », remarque Mme O'Donnell. « Nous avons tous travaillé très dur sur ce projet et nous avons atteint nos objectifs. »

Plusieurs heures par mois d'économie pour la gestion des accès

La gestion des JML dans AD est désormais entièrement automatisée, ce qui permet à l'équipe de gestion des accès et des identités de récupérer un temps précieux. Mme O'Donnell affirme que « les heures que nous économisons nous permettent d'accélérer d'autres initiatives comme l'adoption de nouvelles plateformes pour Active Roles7.4. En ayant récupéré des heures de travail, nous pouvons désormais réaliser d'importantes tâches comme l'analyse des menaces. Je me demande même comment nous trouvions le temps de faire les choses par le passé ». Il n'y a plus d'échanges d'e-mails demandant l'accès au compte d'une personne qui commence ou pour supprimer le compte d'une personne quittant l'organisation. Les intégrations avec les ressources humaines permettent de partager les données des JML avec Active Roles. Les comptes sont ainsi activés ou supprimés automatiquement. « L'accès aux services de base comme les e-mails ou OneDrive sont en place dès l'arrivée du collaborateur. Les salariés nous appellent pour configurer leur mot de passe et ils sont prêts » ajoute Mme O'Donnell.

Rendre les accès à privilèges fluides et sécurisés

Le PDS a également automatisé la PAM, avec des limites de temps désormais appliquées pour l'accès aux serveurs pour des tâches telles que l'application de correctifs. « Dès que le temps imparti pour une tâche est écoulé, Active Roles supprime automatiquement la permission », indique Mme O'Donnell. « Il n'y a aucun risque que quelqu'un oublie de la faire. » Le PDS passe à un modèle Zero-Trust

où chaque action administrative est authentifiée de manière unique. Pour le moment, la PAM reste simple. Les administrateurs demandent les permissions via un portail Web avec des menus défilant. Active Roles génère la permission sauf si la tâche est si confidentielle qu'elle doit être autorisée par Mme O'Donnell ou un autre membre-cadre du PDS.

Dès que la permission est octroyée, des e-mails sont envoyés à l'équipe de cybersécurité et à l'équipe de gestion des accès et des identités du PDS afin d'assurer la visibilité de toute élévation de permissions. De plus, Active Roles génère des enregistrements d'accès pour consultation par les auditeurs si nécessaire. « Avec One Identity Active Roles nous disposons d'une vue limpide des permissions à tout moment ainsi que dans le passé », explique Mme O'Donnell. « Nous ne laissons pas de place à l'erreur. »

Offrir une réponse forte à la pandémie

Avec Active Roles, le PDS a également permis au parlement britannique de répondre de manière efficace à la pandémie. Les membres du parlement et les ministres du gouvernement utilisent les communications vidéo Zoom pour leurs discussions et débats. Cependant, comme le parlement britannique possède un nombre fixe de licences Zoom, le PDS doit gérer rigoureusement les accès. « Nous créons actuellement un formulaire web optimisé par Active Roles," explique Mme O'Donnell. « Le formulaire indiquera le nom et la date de la discussion ou du débat et Active Roles ajoutera ensuite le membre du parlement ou le ministre au groupe AD Zoom. L'accès est révoqué automatiquement à la fin de la journée. »

La gestion des accès entièrement dans le Cloud

L'équipe du PDS est ravie d'adopter Active Roles 7.4. « C'est du pur Cloud », explique Mme O'Donnell. « Nous pourrons créer un utilisateur dans le Cloud et lui donner accès à SharePoint et à OneDrive à travers un même workflow. C'est une solution véritablement centralisée ». D'après Mme O'Donnell, les améliorations de la version 7.4 reflètent l'orientation client de One Identity. « La technologie nous offre de nouvelles possibilités tout en créant de nouveaux risques », poursuit-elle. « One Identity fournit les outils permettant de tirer profit du meilleur tout en nous protégeant des menaces. C'est la tranquillité assurée. »

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. Notre vaste portefeuille intégré d'offres de gestion des identités comprend la gestion des comptes, la gouvernance et l'administration des identités, ainsi que la gestion des accès à privilèges. En savoir plus sur le site OneIdentity.com