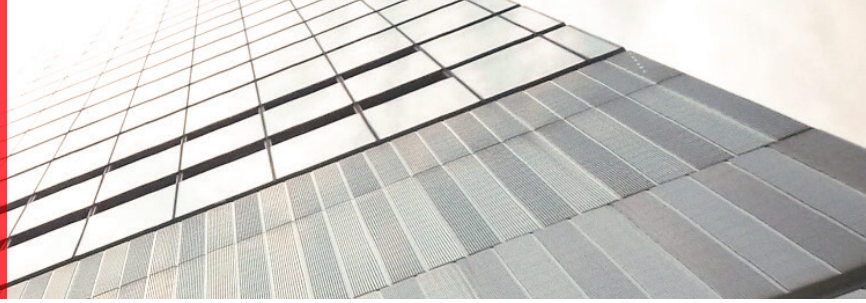
Centrify
ZERO TRUST PRIVILEGE



# Services d'élévation des privilèges de Centrify

## Appliquer le principe de moindre privilège pour réduire la surface d'attaque

**Cela fait quelques années que les cybercriminels ne se contentent plus de « pirater » pour voler des données : ils se connectent tout simplement aux systèmes grâce aux identifiants à privilèges faibles, dérobés ou compromis. Une fois connectés, ils profitent du fait que beaucoup d'entreprises allouent des privilèges trop importants à leurs utilisateurs administratifs. Cela permet aux cybercriminels de pénétrer plus en profondeur et de se déplacer latéralement à travers le réseau, en quête de plus de comptes et d'identifiants à privilèges pour accéder à l'infrastructure la plus critique et aux données les plus sensibles d'une entreprise. La solution Zero Trust Privilege octroie uniquement les privilèges adaptés de manière temporaire pour limiter les mouvements latéraux au sein du réseau.**

### Zone de danger : trop de privilèges

Le principe de moindre privilège est plus répandu que vous ne le croyez. Pensez aux accès physiques de votre bureau : des utilisateurs de divers niveaux ont des droits d'accès différents, et pour avoir accès à certains endroits, vous devez formuler une demande qui doit être acceptée. Ce concept est très répandu en matière de sécurité physique et le même raisonnement vaut pour la sécurité logicielle, notamment lors de l'octroi d'accès granulaires basés sur le rôle aux ressources à privilèges.

Le principe de moindre privilège devrait également être appliqué pour limiter les mouvements latéraux au sein du réseau. C'est ainsi que procèdent souvent les cybercriminels pour accéder aux données sensibles : ils commencent à un endroit, puis ils se déplacent latéralement jusqu'à trouver ce qu'ils recherchent. Si nous limitons les éléments auxquels ils peuvent accéder, nous pouvons mettre fin aux mouvements latéraux. De la même manière, personne ne devrait disposer d'une clé ou d'un badge unique donnant accès à l'ensemble du système. Il faut éviter d'utiliser le compte racine sur un serveur car il fournit un accès trop important et il n'est pas attribué à l'utilisateur réel, que nous appellerons « Bob ». Bob devrait plutôt se connecter directement au système cible avec ses propres droits qui lui permettent de redémarrer uniquement un certain ensemble de serveurs. S'il a besoin de modifier la configuration ou d'accéder à un système cible différent, il devra alors émettre une demande d'accès pour une période précise. Les accès peuvent être attribués automatiquement ou via des services tels que ServiceNow® ou SailPoint Technologies®. De plus, une authentification multifacteur (MFA) peut être demandée. Une fois qu'il a terminé, Bob retrouvera ses privilèges de base.

### Appliquer le principe de moindre privilège pour réduire la surface d'attaque

Le service d'élévation des privilèges de Centrify limite l'exposition aux risques de cyberattaques causées par des individus ayant un niveau de privilège trop important. Les clients peuvent ainsi mettre en œuvre les meilleures pratiques et accorder des accès à privilèges temporaires et adaptés, ce qui limitera les préjudices potentiels causés par les intrusions.

#### ÉLÉVATION DES PRIVILÈGES

Sécurisez et gérez des privilèges précis sur les systèmes Windows, Linux et UNIX afin de limiter les préjudices potentiels liés aux intrusions. Permettez aux utilisateurs de se connecter sous leur propre identité pour établir une responsabilité et élevez les privilèges selon leur rôle au sein de l'organisation.

#### GESTION DÉLÉGUÉE DES RÔLES À PRIVILÈGES ET DES POLITIQUES

La centralisation des rôles, droits et stratégies en matière de privilèges facilite la gestion des environnements hétérogènes (UNIX, Linux et Windows). Les stratégies sont stockées dans Active Directory, à l'écart d'autres objets communs pour prendre en charge la délégation vers les administrateurs de serveurs et la séparation des fonctions des administrateurs Active Directory, évitant ainsi que les administrateurs de serveurs ne manipulent des objets AD qu'ils ne devraient pas. Ces actions sont réalisées sans modifier le schéma d'Active Directory.

#### AUTHENTIFICATION MULTIFACTEUR LORS DE L'ÉLÉVATION DES PRIVILÈGES

L'authentification multifacteur lors de la connexion est une excellente mesure, notamment pour les administrateurs. Toutefois, l'authentification multifacteur devrait également être appliquée lors de l'élévation des privilèges à des fins de protection contre les acteurs malveillants. Assurez-vous que seuls les humains autorisés peuvent exécuter des commandes à privilèges au moyen d'une MFA préalable.

#### AFFECTATION TEMPORAIRE DES RÔLES

Minimisez les risques pour la sécurité en permettant aux administrateurs de demander systématiquement un nouveau rôle afin d'obtenir les droits adaptés à leurs missions. Les demandes d'accès pour les rôles à privilèges permettent aux organisations d'accorder des privilèges et des rôles temporaires ou durables au moyen d'un modèle souple et adapté, conforme aux besoins professionnels variables.

## Accorder uniquement les privilèges requis sur Windows, Linux et Unix

Réduisez le risque d'attaque résultant d'individus ayant trop de privilèges et de l'utilisation habituelle de comptes à privilèges partagés. Appliquer le principe du moindre privilège limite les préjudices potentiels liés aux intrusions. Par conséquent, le service d'élévation des privilèges précis et souple de Centrify permet à vos utilisateurs d'effectuer leur travail, réduit les risques et facilite la mise en œuvre du principe de moindres privilèges temporaires, dont les contrôles d'accès sont basés sur le rôle.

- Les contrôles d'accès basés sur le rôle facilitent l'application du principe de moindre privilège. technologie brevetée de gestion de Zones de Centrify fournit des contrôles d'accès hautement granulaires et basés sur le rôle qui facilitent l'application d'un modèle de moindre privilège sur les systèmes Windows, Linux et UNIX.
- Sécurisez vos systèmes Windows, Linux et UNIX en contrôlant entièrement les accès. Contrairement aux outils décentralisés à but unique comme sudo, Centrify vous permet de configurer des privilèges dynamiques pour que les utilisateurs puissent uniquement élever leurs privilèges à des moments précis, pendant une période donnée et sur certains serveurs uniquement. Vous pouvez également isoler les serveurs en fonction de la durée et des relations de confiance pour renforcer la sécurité des données sensibles. Cela permet de limiter encore plus les mouvements latéraux.
- Centrify fournit un ensemble d'outils puissants pour simplifier l'application et la gestion du principe de moindre privilège.

## Simplifier la gestion des environnements hétérogènes

La centralisation des rôles, droits et stratégies en matière de privilèges facilite la gestion des environnements hétérogènes (UNIX, Linux et Windows). Les stratégies des services Zero Trust Privilege de Centrify sont stockées dans Active Directory, à l'écart des autres objets communs pour prendre en charge la délégation vers les administrateurs de serveurs et la séparation des fonctions des administrateurs Active Directory, évitant ainsi que les administrateurs de serveurs ne manipulent des objets AD qu'ils ne devraient pas. De plus, Centrify offre un modèle de stratégie hiérarchique conçu pour supporter la gestion ordinaire en entreprise des contrôles centralisés pyramidaux. Les rôles et droits communs sont gérés de manière centralisée tout en prenant en charge les délégations départementales, basées sur le rôle ou sur l'ordinateur vers les équipes administratives subordonnées pour les attributions de droits sur les systèmes.

- Un modèle de stratégie structuré et robuste pour Windows, Linux et UNIX garantit la conformité des systèmes et la réduction des frais de maintenance.
- Gérer à la fois les stratégies Windows, Linux et UNIX dans Active Directory permet d'adopter une approche consistante envers la sécurité des accès à privilèges et de créer une séparation des fonctions efficace entre les propriétaires de stratégies et les administrateurs de systèmes. Cette approche homogène des environnements hétérogènes permet de raccourcir la durée des audits et de faciliter la conformité.

## Demandes de rôle en libre-service pour des privilèges temporaires

Minimisez les risques pour la sécurité en permettant aux administrateurs de demander systématiquement un nouveau rôle afin d'obtenir les droits adaptés à leurs missions. Les demandes d'accès pour les rôles à privilèges permettent aux organisations d'accorder des privilèges et des rôles temporaires au moyen d'un modèle souple et adapté, conforme aux besoins professionnels variables.

- Autorisez les administrateurs à se connecter sous leur propre identité pour élever leurs privilèges en demandant systématiquement l'attribution d'un nouveau rôle et obtenir les droits nécessaires à leurs missions. Un système de demande libre-service facilite le processus de demande pour un rôle et une période spécifiques. En cas d'approbation, les droits seront retirés automatiquement dès l'expiration de la période définie.
- Minimisez la surface d'attaque en autorisant temporairement, pendant un délai précis, l'accès aux comptes et rôles à privilèges. Donnez aux administrateurs informatiques l'accès aux identifiants à privilèges, à une gestion à distance des sessions ou lorsqu'ils doivent temporairement modifier leur rôle dans le cadre de tâches administratives supplémentaires.
- Réduisez le risque d'intrusions en demandant une autorisation pour les utilisateurs informatiques qui doivent accéder aux systèmes avec des rôles à privilèges. Les utilisateurs des services informatiques de gestion des actifs ServiceNow® et de base de données de gestion des configurations (CMDB) ou des solutions de gouvernance et d'administration des identités SailPoint Technologies® peuvent demander à bénéficier de rôles à privilèges pour accéder à des serveurs spécifiques pendant une période donnée. Les autorisations sont accordées ou refusées à l'aide d'un processus de gestion basé sur le workflow.

## S'assurer que les commandes à privilèges sont bien lancées par le bon utilisateur à privilèges

L'exécution d'une commande à privilèges doit toujours être protégée des acteurs malveillants. Assurez-vous que seuls les humains autorisés ou les services et applications dotés des droits nécessaires peuvent réaliser une activité à privilèges. Centrify fournit une technologie basée sur l'hôte, qui ne peut pas être contournée, pour appliquer une authentification multifacteur lors des commandes à privilèges sur les serveurs Linux, UNIX et Windows.

- Que vous appliquiez une authentification multifacteur lors de la connexion au système ou au coffre-fort, ou lors de l'élévation des privilèges, l'intégration avec le service d'accès à privilèges de Centrify offre une authentification multifacteur consistante et facile à maintenir pour l'ensemble des accès à privilèges. Vous disposerez du plus large éventail d'authentifiants et d'une prise en charge directe des niveaux d'assurance 2 et 3 du NIST.
- Avec l'approche Zero Trust Privilege, vous devez toujours vérifier l'identité de l'émetteur de la demande d'accès à privilèges. La connexion des admins UNIX / Linux dans le but de vérifier le système n'est pas considérée comme à risque et ne devrait pas faire l'objet d'une authentification multifacteur. En revanche, une MFA devrait être nécessaire avant l'exécution des commandes à privilèges, en tirant parti des services d'authentification multifacteur centralisés de Centrify.
- Avec l'approche Zero Trust Privilege, vous devez toujours vérifier l'identité de l'émetteur de la demande d'accès à privilèges. Les administrateurs Windows ayant besoin d'exécuter des commandes à privilèges peuvent avoir à se soumettre à une authentification multifacteur, s'authentifier à nouveau en saisissant leur mot de passe AD ou valider leur identité à l'aide d'une carte à puce.

Nous avons pour mission de mettre fin à la cause principale d'intrusions : le détournement des identifiants à privilèges. Centrify renforce la protection de nos clients grâce à une approche Zero Trust Privilege adaptée au Cloud qui sécurise les accès aux infrastructures, DevOps, réseaux Cloud, conteneurs, projets big data et autres surfaces d'attaque des entreprises modernes. Pour en savoir plus, rendez-vous sur www.centrify.com.



Siège social aux États-Unis +1 (669) 444 5200
EMEA +44 (0) 1344 317950
Asie-Pacifique +61 1300 795 789
Brésil +55 11 3958 4876
Amérique latine +1 305 900 5354
sales@centrify.com

Centrify
ZERO TRUST PRIVILEGE