BeyondTrust

SOLUTION BRIEF

Gestion des privilèges sur serveurs Unix & Linux : 15 cas d'usage

Ce guide a vocation à aider les admin IT et sécurité à comprendre rapidement comment BeyondTrust Endpoint Privilege Management for Unix & Linux et BeyondTrust Active Directory Bridge peuvent vous aider à faire évoluer progressivement votre gestion et votre sécurité des accès privilégiés et à éliminer la commande sudo, tout en centralisant l'administration, les audits et le reporting.

Table des matières

Introduction

Le principe du « moindre privilège » prévoit que tous les utilisateurs devraient avoir le juste niveau de droits d'accès et de privilèges nécessaires pour bien faire leur travail. Toutefois, de nombreuses fonctions élémentaires liées au système d'exploitation, à l'administration, aux applications et logiciels (ex. utilitaires de configuration) exigent plus que des privilèges de base. Par conséquent, les utilisateurs ont généralement besoin de privilèges élevés sous la forme d'identifiants root ou admin et de mots de passe. Pour compenser le risque de sécurité inhérent aux privilèges excessifs, les entreprises doivent revoir la nécessité de distribuer et maintenir des identifiants root et admin (ou tout simplement éviter de révéler les identifiants aux utilisateurs), sans impacter la productivité des utilisateurs ou administrateurs.

La solution BeyondTrust Endpoint Privilege Management permet aux équipes informatiques de mettre en place un contrôle granulaire des utilisateurs ayant accès aux serveurs Unix, Linux et Windows et de ce qu'ils sont en droit de faire avec cet accès. BeyondTrust permet aux entreprises de renforcer la sécurité système des serveurs tout en simplifiant le déploiement des solutions de gestion des accès privilégiés et en maintenant la productivité.

BeyondTrust Endpoint Privilege Management inclut les fonctionnalités suivantes :

- Scan, découverte, gestion et surveillance automatiques de l'accès aux mots de passe privilégiés root et admin, et aux clés SSH
- Elévation des commandes et délégation des privilèges avec des règles granulaires, ce qui renforce le contrôle sur ce que les utilisateurs Windows, Unix et Linux peuvent faire une fois connectés à un système
- Instauration de l'authentification unique SSO (single sign-on) et simplification des règles par la consolidation des comptes de plusieurs plateformes en un même jeu de règles de contrôle d'accès
- Plus grande visibilité sur les risques liés aux applications visées par l'élévation de privilèges
- Analyse, consignation, enregistrement et reporting des comportements liés aux mots de passe privilégiés, utilisateurs et comptes

Ce livre blanc expose plusieurs scénarios de gestion des privilèges sur les serveurs Unix/Linux, et détaille les fonctionnalités de Privilege Management for Unix & Linux et de BeyondTrust Active Directory Bridge (AD Bridge), qui font partie de la solution BeyondTrust Endpoint Privilege Management. Ces scénarios sont traités de façon progressive, des use cases les plus simples aux plus complexes.

Gestion des privilèges sur serveurs Unix & Linux : 15 cas d'usage

1. Ne plus avoir besoin de se connecter avec un compte root

De nombreux utilisateurs de systèmes et applications Unix et Linux emploient l'expression « j'ai besoin d'un accès root », ce qui signifie qu'ils ne peuvent effectuer leurs fonctions quotidiennes qu'au travers de l'utilisateur le plus puissant du système : « root ». Celui-ci est véritablement omnipotent : il n'y a quasiment rien qu'un utilisateur root ne puisse faire.

Permettre l'utilisation d'un compte root empêche de pouvoir auditer les actions d'un individu (puisque cela promeut le partage de compte) et interdit l'utilisation d'un mot de passe complexe et modifiable pour le compte root étant donné que plusieurs personnes doivent pouvoir utiliser le compte et profiter de ses privilèges à tout moment. Le recours au compte root et les pratiques comme celle du partage de compte accroissent le risque lié aux menaces de l'intérieur, dues à des comportements malveillants et accidentels, et aux menaces externes.

Privilege Management for Unix & Linux instaure un modèle de délégation du moindre privilège qui permet d'éliminer ou de restreindre fortement l'utilisation du compte root, sans perturber les workflows utilisateur. Avec la solution BeyondTrust, vous pouvez permettre aux utilisateurs d'exécuter une commande à un niveau de privilège supérieur dicté par votre politique centralisée. Le fait de supprimer la nécessité d'une connexion root permet au compte de l'utilisateur root d'avoir des contrôles de sécurité renforcés ou d'être basculé vers un système de gestion des mots de passe, comme BeyondTrust Password Safe.

2. Mettre en conformité le compte root

Les admins les plus expérimentés peuvent, de temps à autre, avoir légitimement besoin d'utiliser le compte root selon les types de changements à apporter au niveau système, ou simplement du fait de la nature ad-hoc des commandes à exécuter.

Toutefois, l'équipe de conformité doit impérativement surveiller TOUTE l'activité et générer des rapports portant sur toutes les actions effectuées. Pour autoriser l'accès des administrateurs système à un compte hautement privilégié, les équipes de conformité ont besoin des bons outils et processus pour pouvoir identifier qui a utilisé le compte root, quand et quels changements ont été apportés. De plus, il est impératif que les logs ne puissent être modifiés.

Privilege Management for Unix & Linux permet l'élévation de comptes utilisateur nommés au niveau root avec enregistrement de toute la session, ce qui crée un enregistrement des activités infalsifiable et centralisé, avec à la clé la visibilité sur ce que chaque administrateur système a réalisé.

3. Quand sudo ne suffit plus

Sudo existe depuis longtemps, mais avec la multiplication du nombre des systèmes et des utilisateurs, son administration devient excessivement chronophage. Ajoutez à cela les limitations imposées aux contrôles dans Sudo et l'on comprend que les

systèmes semblent dangereusement exposés à un nombre croissant de menaces de sécurité internes et externes.

La gestion des règles dans Privilege Management for Unix & Linux est bien plus flexible et permet de créer des règles plus granulaires au niveau des commandes et des systèmes. Privilege Management for Unix & Linux renforce la sécurité de plusieurs façons, notamment en dissociant les données des règles et des logs du poste de travail de l'utilisateur ou du serveur, et en utilisant la technologie la plus moderne et efficace de chiffrement des données stockées et en transit.

4. Contrôler les autorisations et accès aux systèmes de fichiers

Pour les systèmes de fichiers, il est possible de définir des autorisations individuelles au niveau fichier ou dossier (lecture, écriture, exécution, etc.). Mais comme ces autorisations sont très statiques par nature, il faut les configurer pour chaque hôte. Des risques se posent aussi quand on autorise l'accès de comptes hautement privilégiés (comme root) à un serveur ou un poste de travail, car un compte ayant ce niveau des privilèges peut facilement manipuler les autorisations et les réglages de propriété au moyen de commandes comme « chmod » et « chown ». Ainsi, autoriser l'accès illimité d'un compte à des fichiers et des données constitue un risque majeur.

Privilege Management for Unix & Linux règle le problème en autorisant l'application de paramètres de sécurité runtime, contrôlés de façon centralisée, qui protègent les informations les plus critiques des comptes les plus privilégiés. Les règles Advanced Control and Audit (ACA) de Privilege Management for Unix & Linux peuvent s'appliquer de façon dynamique, permettant l'instauration pendant une durée donnée de règles d'autorisation d'accès aux systèmes de fichiers, ou n'autorisant l'accès que dans certaines conditions, comme en présence d'une authentification bifactorielle ou de la référence valide d'un incident recensé dans le système de gestion des incidents.

Ainsi, les entreprises peuvent autoriser un accès de niveau « root » complet et dans le même temps bloquer l'accès de l'utilisateur root aux fichiers utilisateur stockés dans '/home', ou autoriser l'exécution de scripts, sans possibilité de les lire ni de les modifier.

5. Contrôler les accès au script et auditer les actions y étant réalisées

Les administrateurs Unix et Linux utilisent régulièrement des scripts nécessaires au quotidien pour la gestion et l'administration des systèmes. Nombre de ces scripts doivent être exécutés par un utilisateur privilégié, de type « root », ou appeler des fonctions qui exigent elles-mêmes de hauts niveaux de privilège. Il est indispensable d'utiliser une solution de moindre privilège pour l'attribution de droits ayant été elevés aux utilisateurs en ayant besoin. La meilleure façon jusqu'ici d'auditer l'activité de ces utilisateurs était d'enregistrer les sessions (« record stdin et stdout ») ou d'enregistrer tout ce que l'utilisateur tapait et tout ce qu'il voyait à l'écran. Le problème avec cette approche d'enregistrement des actions, c'est que consigner le fait que quelqu'un a tapé 'update.sh' sur la ligne de commande n'offre aucun moyen de savoir quelles actions ont été exécutées dans le script, quelles données ont pu être affectées, ni comment le système a pu être manipulé.

Avec Privilege Management for Unix & Linux et ses fonctions Advanced Control and Audit (ACA), les scripts peuvent être contrôlés plus étroitement (exécutés et lus, mais pas modifiés, même par un accès root), mais les entreprises peuvent aussi consigner et enregistrer toutes les requêtes réalisées au niveau du système, quelle que soit leur source, en cours de session.

Ainsi, des actions, comme l'exécution d'un script, peuvent être enregistrées avec chaque appel commandé par le script (lecture, écriture, exécution, etc.). En plus de consigner toutes les activités des scripts, Privilege Management for Unix & Linux permet de contrôler des actions individuelles dans le script et d'autoriser ou de bloquer les actions sans interrompre le traitement du script.

6. Contrôler les accès au niveau du système

Les outils traditionnels visant la mise en place du moindre privilège, comme sudo, contrôlent ce que l'utilisateur tape sur la ligne de commande et non ce que le système s'efforce de traiter. Les règles définies dans ces outils portent sur la saisie de l'utilisateur et non sur ce que le système fait. Mais dans la plupart des systèmes d'exploitation modernes, ces deux actions peuvent être très différentes. Par exemple, sous Windows, il est simple de créer un raccourci vers, disons, « notepad.exe », et de nommer ce raccourci « My Fav Text Editor.lnk ». Si la règle dans l'entreprise est d'empêcher quelqu'un de cliquer sur une icône nommée Notepad.exe, que se passe-t-il si quelqu'un clique sur le raccourci nouvellement créé ?

On retrouve le même genre de scénario dans Unix et Linux, systèmes d'exploitation à ligne de commande, où les règles de sécurité portent surtout sur ce que l'utilisateur tape à l'invite de commande. Le problème est que les raccourcis (liens symboliques et en dur) peuvent servir à appeler du code binaire (exécutables) et des scripts, ou des fichiers de référence. De plus, le code binaire (exécutables) peut être renommé pour contourner les règles de sécurité. Imaginez que quelqu'un renomme le code binaire 'shutdown' en 'ping'. Sudo pourrait bloquer la commande d'arrêt mais « ping » pourrait passer. Un administrateur sournois pourrait exécuter 'sudo ping' et le système s'arrêterait purement et simplement sans que quiconque puisse imaginer ce qu'il s'est réellement passé.

Les règles Advanced Control and Audit (ACA) de Privilege Management for Unix & Linux permettent de placer des contrôles d'une seule ligne autour de fichiers et de dossiers, ce qui permet de viser des fichiers individuels et des dossiers correspondant à un modèle de nommage ou d'appliquer à des dossiers entiers avec leurs sous-dossiers. Ces contrôles permettent de définir des autorisations granulaires pour chaque cible, mais surtout, ACA opère au niveau système et non au niveau de la ligne de commande. Quel que soit le nom de la commande 'shutdown', '/usr/sbin/shutdown' directement, un lien hard ou soft vers '/usr/sbin/shutdown' ou une copie renommée de la commande d'arrêt, ACA est suffisamment intelligent pour bloquer l'exécution de la commande émise.

7. Consolider les logs d'événements, le reporting et l'analytique

Du fait de leur nature même, basée sur des lignes de commandes, les systèmes Unix et Linux ne favorisent pas le reporting. Toutefois, ce dernier est essentiel, surtout pour les investigations post-mortem sur les logs ou la détection d'anomalies.

BeyondTrust règle ce problème avec l'intégration entre Privilege Management for Unix & Linux et la plateforme centrale, BeyondInsight. Privilege Management for Unix & Linux envoie les données des logs d'événements à BeyondInsight afin qu'elles soient représentées sur le tableau de bord (essentiellement qui, quoi, où et quand). Ces données peuvent être présentées dans des rapports faciles à lire, avec accès au cube de données pour les besoins de reporting sur mesure. Ces données peuvent être corrélées avec d'autres via la fonction Auditor de BeyondInsight pour la détection et le reporting d'anomalies. Cette intégration simplifie et accélère la lisibilité du reporting d'événements Unix et Linux de sorte que les parties prenantes puissent avoir une vision plus claire de leurs risques privilégiés.

8. Forensics (post-mortem) : le temps presse

On peut vite se retrouver submergé à consigner toute l'activité utilisateur Unix/Linux. En cas d'investigation légale (forensics), les entreprises peuvent aisément perdre du temps et mobiliser excessivement leur personnel.

Avec Privilege Management for Unix & Linux, il est possible de nommer dynamiquement les journaux d'événements, de les conserver de façon centralisée et d'en contrôler l'accès via la console centrale BeyondInsight. Privilege Management for Unix & Linux utilise SOLR pour indexer toutes les sessions enregistrées, toutes les informations étant accessibles par ligne de commande ou via l'API REST.

9. Enregistrer les sessions (tout ce qui est saisi est vu)

Le moindre privilège est un idéal pour la plupart des organisations de sécurité, mais parfois vous devez juste activer une commande privilégiée, comme une commande shell root. Un audit strict est un moyen efficace de laisser les personnes honnêtes rester honnêtes. Pour des admins de confiance, une commande root complète ne pose aucun problème du moment que l'activité de l'admin est enregistrée de façon inviolable. Ce niveau de supervision aide à s'assurer que les admins n'abusent pas de leurs droits, tout en aidant une entreprise à se mettre en conformité au niveau des accès privilégiés.

Une simple ligne dans les règles de Privilege Management for Unix & Linux suffit à déclencher l'enregistrement de toute une session, qui est ensuite nommée dynamiquement et indexée automatiquement via SOLR. Cette fonctionnalité permet de voir la session de nombreuses façons différentes : par lecture interactive, lecture style vidéo, affichage de la transcription de session, affichage de l'historique des commandes, ou via une recherche dans un index. Cette fonctionnalité permet d'effectuer des recherches rapidement, de façon à mieux gérer le risque.

10. Gérer les mots de passe et mettre en place le principe du « moindre privilège »

Pour qu'une solution de gestion des mots de passe fonctionne, il faut un compte de second niveau (compte fonctionnel) pour que le gestionnaire de mots de passe puisse exécuter les modifications de mot de passe, si jamais celui du compte géré devait être désynchronisé ou inconnu du coffre-fort. C'est aussi vrai pour toute application qui aurait besoin de privilèges supérieurs, comme les outils d'analyse, l'administration à distance automatisée, etc. Ces comptes créent un risque au niveau du système cible du fait du niveau de privilège attribué par le gestionnaire de mots de passe utilisateur.

En installant Privilege Management for Unix & Linux avec BeyondTrust Password Safe et en ajoutant une règle simple, tout compte utilisateur (même avec des droits extrêmement limités sur le système cible) peut se voir attribuer les privilèges demandés par Password Safe pour fonctionner. C'est la garantie de niveaux supérieurs de sécurité et de conformité en éliminant les comptes avec privilèges dont les comptes fonctionnels ont généralement besoin, tout en réduisant la surface d'attaque de l'hôte concerné.

11. Intégration de Privileged Password Management avec Command Execution

Parfois, les administrateurs doivent effectuer une action sur un système hôte cible qui exige l'utilisation d'un compte/mot de passe, qui ne réside pas nécessairement sur l'hôte lui-même. En exécutant une commande via Privilege Management for Unix & Linux, ex. pbrun sqlplus, Privilege Management for Unix & Linux peut extraire les identifiants d'une solution de stockage de mots de passe pour exécuter la commande voulue. Cette intégration fait en sorte que les entreprises peuvent non seulement contrôler leurs identifiants privilégiés, mais aussi permettre un contrôle très granulaire des commandes sur les systèmes cibles une fois l'identifiant récupéré.

12. Centraliser la gestion des règles Sudo

Même pour les utilisateurs les plus aguerris d'un outil de moindre privilège, il y aura toujours quelques machines ayant accès à sudo. Avec autant d'itérations différentes du fichier de règles des utilisateurs de sudo utilisées par différents groupes au sein de l'entreprise, la nécessité de contrôler et suivre les modifications apportées à chaque fichier devient rapidement ingérable. Quasiment tous les utilisateurs de sudo peinent à gérer correctement les fichiers de règles sudo individuels créés sur chaque hôte Unix ou Linux.

Des outils de synchronisation manuelle et des solutions LDAP/de base de données développées en interne peuvent sembler séduisants de prime abord, mais les contrôles de fiabilité, de complexité et de sécurité finissent par réduire l'efficacité de ces configurations, provoquant souvent plus de problèmes qu'ils n'en résolvent. Il n'existe pas de moyen efficace d'annuler les modifications apportées à un ou plusieurs fichiers d'utilisateurs sudo, ni de revenir à un point donné de temps/version d'un fichier de règles.

Privilege Management for Unix & Linux permet de centraliser rapidement un ou plusieurs fichiers d'utilisateur sudo, facilitant la gestion des changements et le contrôle de version. Les changements de règles peuvent être validés avant d'apporter les modifications en direct dans le fichier, ou être comparés avec les différences mises en évidence entre deux versions du fichier d'un utilisateur sudo. La fonctionnalité d'annulation/récupération (roll-back/roll-forward) permet de basculer rapidement entre deux versions enregistrées du fichier sudo gérées par PMUL pour Sudo. Il est possible de regrouper les hôtes se connectant ou de les faire tourner dans un environnement hybride un à un plus hôtes groupés. Ceci permet un accès simple et contrôlé à des fichiers sudo spécifiques sur ou plusieurs serveurs centralisés, selon le groupe de l'hôte qui fait la demande.

13. Stocker de façon centralisée les données d'audit Sudo

Utiliser sudo revient à placer des données de fichiers journaux en différents endroits de différents systèmes. Selon la version d'Unix ou Linux, les données des événements

sont enregistrées dans différents fichiers syslog et également mélangées avec d'autres données d'événements système. Il faut impérativement un meilleur moyen de déplacer et de stocker les données des fichiers journaux sudo et des sessions sudo.

Privilege Management for Unix & Linux établit une connexion réseau sécurisée à un serveur centralisé qui stocke les données d'événements et de sessions (chiffrées au besoin) en un lieu sûr et centralisé à mesure que les données des fichiers journaux sont écrites, ce qui évite tout risque de modification des fichiers journaux et accélère l'analyse des logs et les investigations au besoin.

14. Consolider les comptes et annuaires

Quand des utilisateurs et des administrateurs ont besoin d'avoir accès à un système, il convient de créer un compte sur chaque hôte pour autoriser l'accès au système de l'utilisateur. Ces comptes utilisateur sont souvent associés à des droits excessifs et l'on omet souvent de faire le ménage quand un salarié change de poste ou quitte l'entreprise. Les entreprises doivent donc trouver le moyen de réduire le nombre de comptes créés, de contrôler à quel serveur ces comptes consolidés peuvent se connecter et d'exercer un contrôle sur les droits que détient l'utilisateur authentifié.

BeyondTrust Active Directory Bridge (AD Bridge), couplé à Privilege Management for Unix & Linux, gère la consolidation des comptes avec les droits d'accès système consolidés et un système de moindre privilège pour contrôler les droits des utilisateurs, post-authentification. L'appartenance d'un utilisateur à un groupe Active Directory permet de contrôler à quels serveurs l'utilisateur peut avoir accès, tandis qu'une politique de règles centralisée permettra de contrôler et auditer les activités d'un utilisateur lors de chaque session authentifiée.

Autre avantage, AD Bridge permet aux utilisateurs de se connecter aux systèmes Unix, Linux ou Mac via leurs identifiants et mots de passe Active Directory (AD), sans autre synchronisation d'infrastructure ou de mot de passe.

Résultat : migration facilitée de plusieurs mécanismes d'authentification, identités et annuaires en une seule infrastructure basée sur Active Directory pour tous les systèmes et les utilisateurs. Ce contrôle centralisé accélère l'accueil et le départ des utilisateurs.

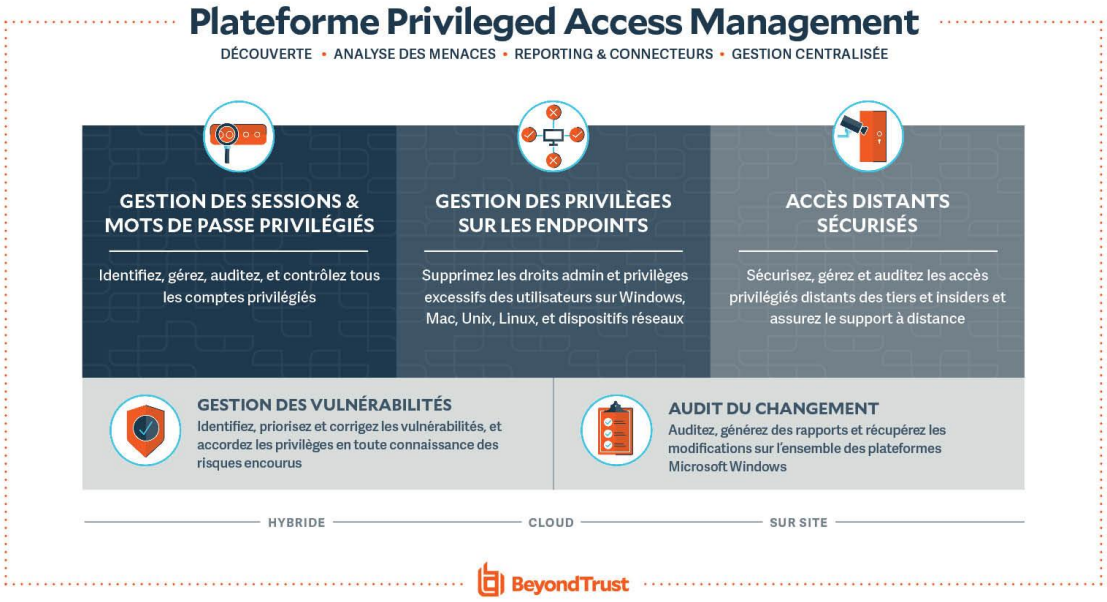
15. Etendre les règles de groupe aux systèmes non-Windows

Certaines entreprises choisissent de gérer de façon centralisée leurs systèmes Windows, Unix et Linux pour plus de sécurité, d'efficacité et de conformité, mais elles peinent parfois à appliquer uniformément les règles de configuration dans toute l'entreprise.

BeyondTrust Active Directory Bridge (AD Bridge), couplée avec Privilege Management for Unix & Linux, aide à uniformiser la configuration sur l'ensemble de l'entreprise par l'extension des outils de gestion natifs Group Policy à des paramètres Group Policy spécifiques pour Unix, Linux et Mac. Cette fonctionnalité facilite la conformité avec les réglementations SOX, PCI, HIPAA, etc. sur tous les systèmes en remplaçant NIS par une infrastructure Active Directory.

Plateforme Privileged Access Management de BeyondTrust

Privilege Management for Unix & Linux et Active Directory Bridge (AD Bridge) font partie des solutions BeyondTrust de Endpoint Privilege Management et s'intègrent avec d'autres solutions de gestion des accès privilégiés de la plateforme BeyondTrust Privileged Access Management, solution intégrée offrant contrôle et visibilité sur tous les comptes et utilisateurs privilégiés.



Prochaines étapes

Ce document présente des scénarios courants de délégation de privilèges et d'élévation de commandes basés sur des règles pour les serveurs Unix et Linux. Pour savoir comment BeyondTrust peut vous aider, visitez www.beyondtrust.com/endpoint-privilege-management.