

Solution Privileged Access Suite for Unix

Simplifiez la sécurité et l'administration des systèmes UNIX et satisfaites aux exigences de conformité

Avantages

- Simplifie l'administration des accès et des identités à travers divers environnements
- Consolide la gestion des identités UNIX dans Active Directory
- Applique l'accès du moindre privilège
- Fonctionnalités de délégation UNIX flexibles
- Contrôle complet à partir d'une même console
- Répondez facilement aux exigences de conformité et d'audit pour l'ensemble de votre environnement UNIX
- Gestion centralisée des stratégies sur les serveurs UNIX/Linux

Configuration système requise

Pour consulter la liste complète des exigences système, visitez oneidentity.com/privileged-access-suite-for-unix

Les systèmes UNIX (notamment Linux et Mac OS), par nature, font face à des défis distincts lorsqu'il s'agit de sécurité et d'administration. Comme les systèmes natifs basés sur UNIX ne sont pas liés les uns aux autres, chaque serveur ou chaque instance de système d'exploitation doit avoir sa propre source d'authentification et d'autorisation, notamment l'autorisation superutilisateur par le biais du compte root.

En l'absence de moyens de gestion efficace des identités à travers les systèmes UNIX et non UNIX ainsi que de contrôle et d'audit de l'utilisation du compte root, les organisations se retrouvent avec une gestion inefficace et très incohérente ce qui pourrait entraîner des failles de sécurité potentiellement catastrophiques.

La solution Privileged Access Suite for UNIX, de la gamme de produits One Identity, résout ces problèmes intrinsèques de sécurité et d'administration des systèmes basés sur UNIX tout en facilitant l'application des exigences

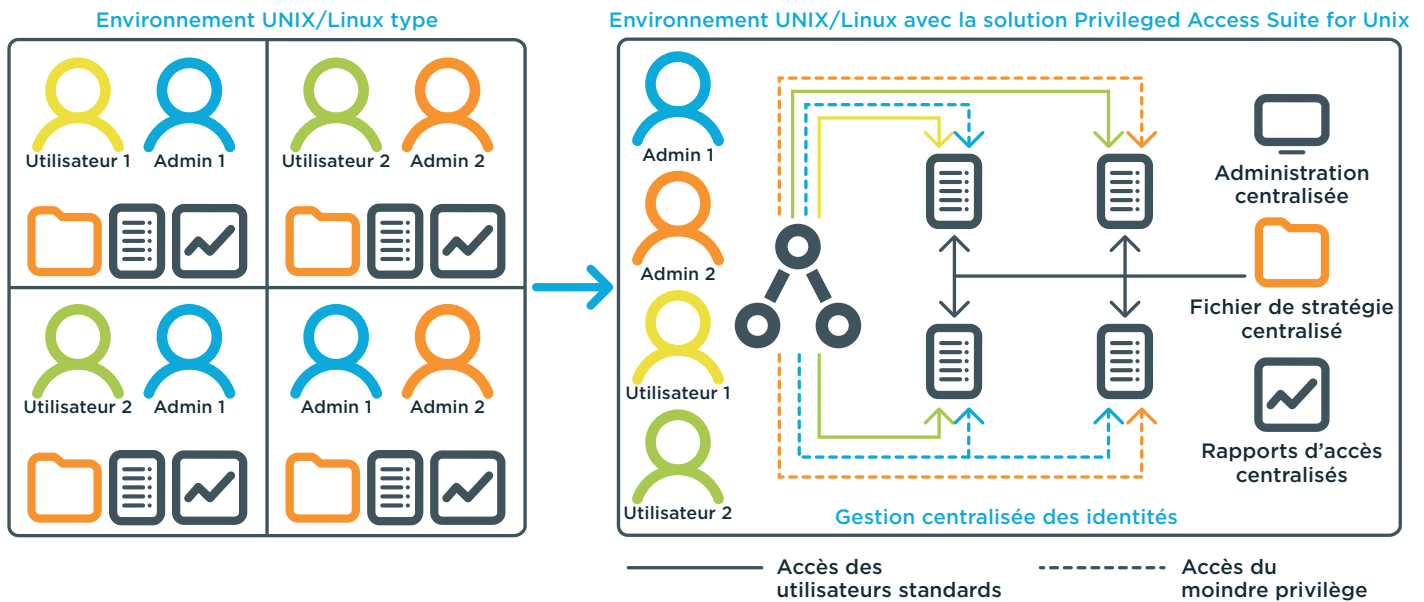


Figure 1 : La solution Privileged Access Suite for Unix unifie et consolide les identités tout en fournissant des responsabilités individuelles et un accès du moindre privilège basé sur un fichier de stratégie unique ainsi que des rapports centralisés sur l'ensemble de votre environnement UNIX/Linux.

de conformité. Elle unifie et consolide les identités, attribue des responsabilités individuelles et permet de centraliser les rapports d'accès utilisateur et administrateur à UNIX.

La solution Privileged Access Suite for UNIX est une solution tout-en-un pour la sécurité UNIX qui associe les solutions de pont Microsoft® Active Directory® et de délégation des comptes root au sein d'une console unifiée afin d'offrir aux organisations une vue centralisée et une administration simplifiée des identités et des droits d'accès dans l'ensemble de leur environnement UNIX.

Pont Active Directory

La solution Privileged Access Suite for UNIX étend l'authentification et l'autorisation unifiées d'Active Directory (AD) aux systèmes UNIX, Linux et Mac OS au moyen d'un pont Active Directory. Authentication Services, la solution One Identity de pont Active Directory écarte le besoin d'une solution séparée d'authentification et d'autorisation des systèmes UNIX natifs en consolidant la gestion

des identités et des accès dans Microsoft Active Directory. Les systèmes UNIX deviennent des « citoyens à part entière » d'AD à travers un compte unique bien géré qui améliore l'efficacité de la gestion du cycle de vie de l'identité. Ce compte s'appuie sur la qualité d'authentification d'AD afin de permettre à UNIX d'utiliser l'authentification sécurisée Kerberos, ce qui améliore la sécurité.

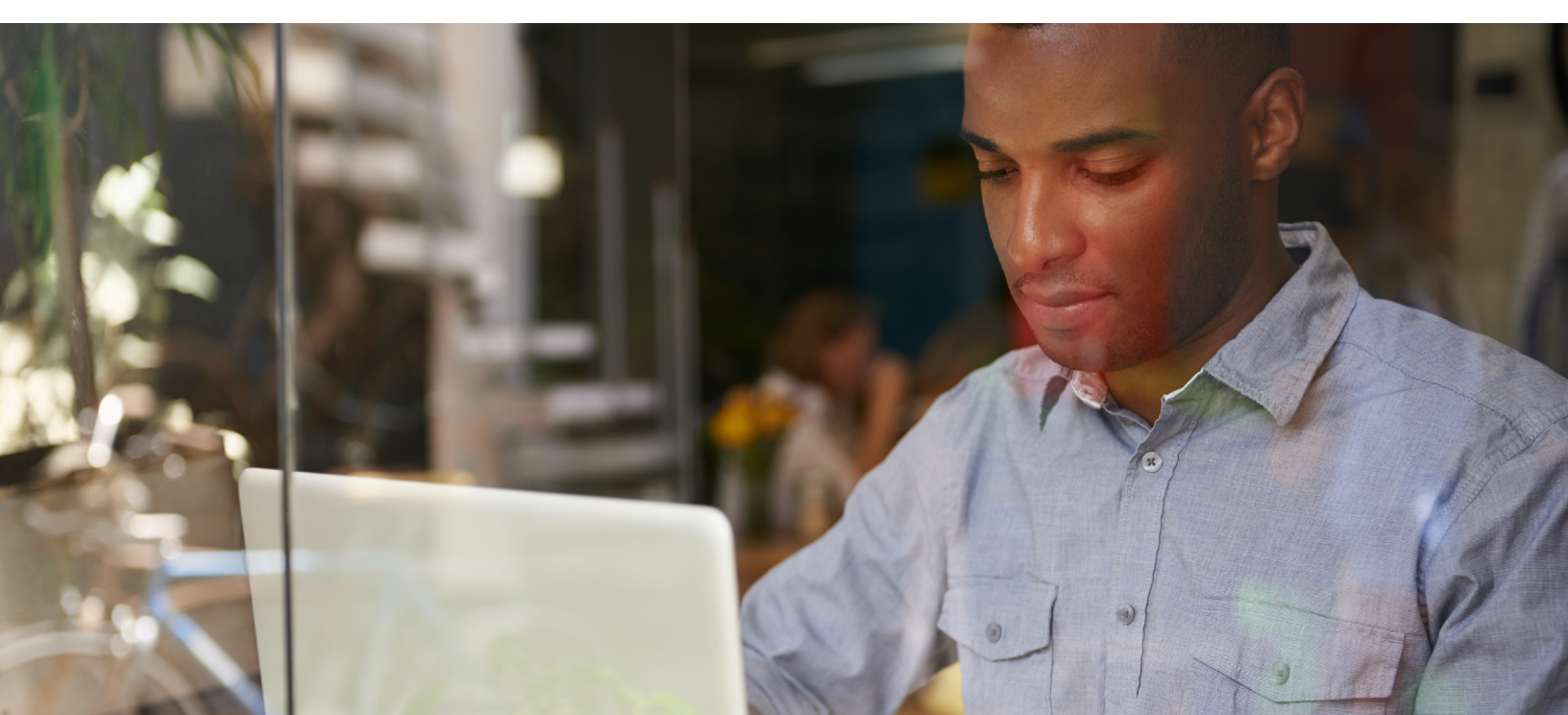
Délégation du compte root

Privileged Access Suite for UNIX offre deux possibilités différentes de délégation du compte root UNIX. La suite complète ou remplace sudo en fonction de vos besoins. Lorsque vous choisissez de compléter sudo avec le logiciel Privilege Manager for Sudo, vous conservez toutes les fonctionnalités de sudo qui vous sont familières tout en l'améliorant avec un serveur central de stratégies, une gestion centralisée, et les rapports centralisés sur les droits d'accès et les activités tels que l'enregistrement des frappes d'activités effectuées à travers sudo.

Si vous préférez remplacer sudo par le logiciel Privilege Manager for Unix, vous pourrez toujours déléguer les privilèges des comptes root UNIX selon des rapports centralisés des stratégies de droits d'accès, néanmoins vous bénéficierez de permissions plus granulaires et de la possibilité d'enregistrer les frappes pour toutes les activités d'un utilisateur dès qu'il se connecte et non uniquement les commandes dotées du préfixe « su ». En outre, cette option améliore la sécurité en limitant les shells et l'exécution des commandes d'hôtes distants tout en renforçant les binaires afin d'éliminer la possibilité d'utiliser des commandes qui obtiennent une élévation d'accès sans détection.

Fonctionnalités

Identités consolidées : simplifiez la gestion des identités en consolidant les comptes UNIX à l'aide d'un système d'accès basé sur les rôles géré de manière centralisée par le biais d'Active Directory (AD) et d'une seule identité AD.

**Accès du moindre privilège :**

n'accordez aux administrateurs que les droits nécessaires pour l'exécution de leurs attributions tout en vous protégeant contre les risques liés à des accès trop étendus. Les administrateurs individuels ne reçoivent que les droits nécessaires pour remplir leurs responsabilités.

Gestion centralisée et

administration : appliquez des stratégies d'accès unifié et configurez-les de manière centralisée pour l'ensemble de votre environnement UNIX.

Rapports sudo :

créez facilement des rapports sur les droits d'accès sudo, ce qui résout l'un des aspects les plus complexes de la prise en charge de sudo dans une entreprise. Cela n'affecte en aucun cas la façon de travailler des utilisateurs. Aucune nouvelle formation n'est donc nécessaire. La création de rapports d'accès pour l'audit et la conformité a seulement été simplifiée.

Visibilité à 360 degrés :

apportez un contrôle et une visibilité intégrés de l'ensemble des activités UNIX/Linux avec une seule console. Obtenez facilement des informations sur l'auteur d'une stratégie d'accès, son contenu de cette dernière et quand elle a été appliquée. En outre, la solution Privileged Access Suite for Unix est la seule à fournir des rapports centralisés sur les droits d'accès individuels à travers sudo ainsi qu'une solution de délégation d'entreprise liée aux données d'un compte utilisateur dans AD.

Faites confiance, mais

vérifiez : elle fournit les responsabilités individuelles et la visibilité nécessaires au niveau des droits et des activités pour pouvoir répondre aux exigences de conformité et de sécurité. Les fonctionnalités d'audit couvrent les rapports sur les stratégies, les rapports sur les droits et leur historique, le suivi des modifications et le retour en arrière ainsi que l'enregistrement des frappes.

Authentification unique :

elle permet de bénéficier d'une véritable solution d'authentification unique pour l'ensemble des environnements UNIX, Linux et Mac OS ainsi que pour des applications basées sur les standards clés telles que SAP, Siebel etc.

Informations supplémentaires

Pour en savoir plus sur la solution Privileged Access Suite for UNIX, visitez oneidentity.com/privileged-access-suite-for-unix

À propos de One Identity

La gamme One Identity de solutions de gestion des accès et des identités (IAM) inclut une offre de solutions IAM concrètes de gouvernance des identités, de gestion des accès, et de gestion des comptes à privilèges axées sur l'entreprise, modulaires, intégrées et tournées vers l'avenir.

Pour en savoir plus, visitez OneIdentity.com