FICHE TECHNIQUE

Privileged Session Manager

Octroyez, contrôlez et enregistrez des droits d'accès privilégiés

Avantages

- Délégation des privilèges d'accès
- Nombre limité de tâches et de commandes Unix et Windows exécutées
- Connexion automatique
- Enregistrement, archivage et relecture des sessions pour répondre aux obligations d'audit

Privileged Session Manager est la solution idéale pour sécuriser l'accès des :

- Fournisseurs distants
- Consultants distants
- Développeurs distants
- Utilisateurs privilégiés en interne
- Développeurs (accédant aux environnements de production)
- Appels d'urgence

Si l'équipe informatique interne, les administrateurs système, les sous-traitants et les fournisseurs de services ont accès à des systèmes stratégiques de façon non contrôlée, les entreprises s'exposent à des risques majeurs, comme l'ont montré de récents incidents ayant fait les gros titres. Toutefois, pour répondre aux exigences de sécurité et de conformité, les entreprises ne peuvent pas se contenter de contrôler les droits d'accès des utilisateurs privilégiés. Elles doivent également surveiller les activités des utilisateurs de façon proactive et prendre des mesures lorsque leurs agissements sont inappropriés.

La solution Privileged Session Manager vous permet d'octroyer des droits d'accès privilégiés aux administrateurs, fournisseurs distants et utilisateurs à haut risque pour une période ou une session spécifique. Elle offre également des fonctionnalités d'enregistrement et de relecture de sessions complètes afin de satisfaire aux exigences d'audit et de conformité. Cette solution fournit un point de contrôle unique depuis lequel vous pouvez autoriser les connexions, limiter l'accès à certaines ressources, autoriser l'exécution de certaines commandes uniquement, visualiser les connexions actives, enregistrer toutes les activités, générer des alertes si

ONE IDENTITY™

des connexions excèdent la durée prédéfinie et rompre les connexions. Privileged Session Manager est un composant essentiel des produits de gestion des comptes à privilèges One Identity qui est déployé sur une appliance fiable et sécurisée.

Fonctionnalités

Accès contrôlé : une connexion via un navigateur Web sécurisé permet aux utilisateurs autorisés de demander une session pour accéder à des ressources spécifiques ou par le biais de comptes d'administration spécifiques. Chaque utilisateur peut voir uniquement les ressources spécifiques pour lesquelles il est autorisé à faire une demande d'accès. Pour renforcer le contrôle et assurer la conformité, vous pouvez configurer la connexion du workflow d'autorisation.

Accès proxy : Privileged Session Manager sert de proxy pour toutes les sessions d'accès aux ressources cibles. Comme les utilisateurs n'accèdent pas directement aux ressources, l'entreprise est protégée contre les virus, logiciels malveillants ou autres éléments dangereux qui peuvent être présents sur les systèmes des utilisateurs. Privileged Session Manager fait office de proxy et enregistre les pare-feu, routeurs, périphériques réseau, applications Web, Unix/Linux, AS/400, Windows, etc.

Contrôle des commandes : vous pouvez autoriser l'exécution de certaines commandes au cours d'une session en fonction de l'utilisateur qui accède aux ressources ou du système consulté. De plus, vous pouvez restreindre les commandes qu'un utilisateur est autorisé à exécuter au cours d'une session. Si l'utilisateur tente d'exécuter une commande interdite, vous pouvez automatiquement envoyer une notification à une personne spécifique ou annuler la commande, la connexion ou toute la session.

Audit, enregistrement et relecture de sessions complètes : toutes les activités d'une session sont enregistrées, c'est-à-dire toutes les actions qui ont lieu à l'écran, notamment les mouvements de la souris, les clics et les frappes, et peuvent être revisionnées à l'aide de commandes semblables à celles d'un enregistreur pour effectuer des analyses approfondies ou des contrôles de conformité. Seule l'activité actuelle est enregistrée et les enregistrements sont compressés pour limiter l'espace de stockage hors ligne requis, ce qui représente une capacité nettement inférieure à celle requise par d'autres solutions.

Revisionnage simple : les administrateurs peuvent facilement rechercher des événements spécifiques parmi les sessions et ajouter des signets afin de pouvoir revenir ultérieurement à un point précis d'une session.

Appliance sécurisée : l'appliance ne dispose pas de port de console ni d'interface au niveau de la console. Elle est uniquement accessible par le biais d'une interface Web sécurisée et basée sur les rôles. Elle assure ainsi une protection contre les attaques d'administrateurs hôtes et les modifications du système d'exploitation, des bases de données ou autres changements au niveau du système. L'appliance est également dotée d'un pare-feu interne qui protège contre les attaques réseau externes et offre des fonctions d'audit supplémentaires.

Workflow simple : les utilisateurs autorisés peuvent facilement sélectionner la ressource ou le compte qu'ils souhaitent consulter. Seuls les éléments pour lesquels ils sont autorisés à faire une demande d'accès apparaissent dans la liste. Le demandeur indique la durée prévue de la session, le motif de la demande et, si nécessaire, un numéro de ticket qui peut être intégré à un système de tickets existant.

Connexion automatique : vous pouvez associer Privileged Session Manager à Privileged Password Manager afin de configurer l'accès en vue d'une connexion automatique. La connexion automatique améliore la sécurité et la conformité, car les informations d'identification du compte ne sont jamais visibles par l'utilisateur.

La gestion des comptes à privilèges vue par One Identity

Les produits One Identity comprennent l'ensemble le plus complet de solutions de gestion des comptes à privilèges, spécialement conçues pour répondre aux besoins de toutes les entreprises. Outre les puissantes fonctions de gestion des sessions assurées par Privileged Session Manager, les produits One Identity fournissent un coffre-fort de mots de passe privilégiés exécuté sur la même appliance sécurisée. Les produits One Identity proposent également des solutions ciblées basées sur des agents et conçues pour la délégation granulaire des comptes root Unix et administrateur Active Directory ; des extensions pour que les commandes sudo open source répondent aux besoins des entreprises ; et l'enregistrement des frappes pour les activités root Unix. Toutes ces fonctions sont étroitement intégrées avec la solution de pont Active Directory leader du marché.

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

ONE IDENTITY™