ManageEngine
Key Manager Plus

FICHE TECHNIQUE

Solution Web de gestion des clés SSH et des certificats SSL pour les entreprises.

Qu'est ce que ça fait?

Key Manager Plus de ManageEngine est une solution Web de gestion des clés et des certificats qui aide les entreprises à découvrir, consolider, créer, déployer, auditer et suivre les cycles de vie de SSH (Secure Socket Shell) et certificats SSL/TLS (Secure Sockets Layer/Transport Layer Security). Il offre une visibilité et un contrôle complets sur les environnements SSH et SSL et aide les administrateurs à prendre le contrôle total des identités numériques pour prévenir les violations et les problèmes de conformité.

Pourquoi c'est important?

La protection des données en transit a toujours été un défi majeur pour les administrateurs de la sécurité informatique. Les clés SSH aident les organisations à garantir la sécurité de l'accès administratif à distance et du transfert de données, mais elles présentent également des défis uniques.

Habituellement, les clés SSH ne sont ni surveillées ni gérées, ce qui rend les organisations vulnérables cyber-attaques. En l'absence d'un système automatisé, obtenir la liste de toutes les clés utilisées, trouver et restreindre les privilèges d'accès et assurer une rotation périodique est une tâche herculéenne.

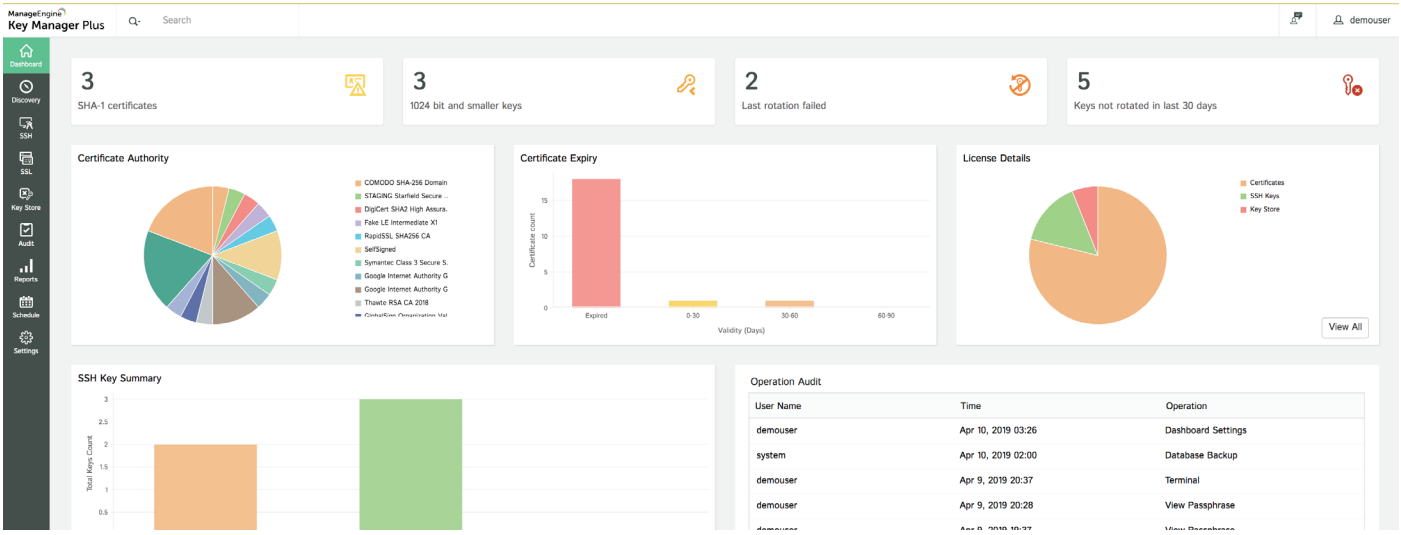
De même, la gestion d'un environnement SSL/TLS peut être intimidante, en particulier lorsque les organisations utilisent un grand nombre de certificats SSL émis par différentes autorités de certification avec des périodes de validité différentes. Les certificats SSL, lorsqu'ils ne sont pas gérés, peuvent expirer de manière inattendue, ou les certificats SSL non valide/non autorisés pourraient être utilisés. Les deux scénarios peuvent entraîner des interruptions de service ou afficher des messages d'erreur qui nuisent à la crédibilité de votre marque et, dans les cas extrêmes, entraîner des failles de sécurité.

Par conséquent, les entreprises ont besoin d'une solution capable de centraliser et d'automatiser la gestion de ces identités numériques et de contrer l'utilisation abusive des privilèges causée par des clés d'utilisation inappropriées et certificats.

Avantages

- Bénéficiez d'une visibilité complète de toutes les clés SSH et certificats SSL présents dans votre organisation, et réalisez un contrôle centralisé.
- Supprimez les relations d'approbation clé publique-utilisateur existantes et générez de nouvelles paires de clés. Déployez les nouvelles clés publiques auprès des utilisateurs en bloc et appliquez la rotation périodique directement à partir de Key Manager Plus.
- Obtenez des certificats SSL auprès d'autorités de certification de confiance pour vos sites Web publics via un flux de travail de demande de certificat sans tracas.
- Gérez de bout en bout le cycle de vie des certificats grâce à un déploiement centralisé, des analyses de vulnérabilité et des notifications récurrentes lorsque les certificats sont sur le point d'expire.
- Accédez instantanément à des pistes d'audit en temps réel inviolables et à des rapports complets sur toutes les opérations effectuées autour de la gestion des clés et des certificats.

Tableau de bord centralisé offrant une vue d'ensemble des opérations liées à SSL/SSH en un coup d'œil.



Principales caractéristiques

Gestion des certificats SSL

Découverte de certificat SSL/TLS
Découvrez tous les certificats SSL/TLS déployés dans votre réseau et ajoutez-les à un inventaire sécurisé et centralisé.

Workflow de demande de certificat
Générez des CSR instantanément; demandez et acquérez des certificats d'autorité de certification publics via un workflow de demande de certificat sans tracas.

Déploiement centralisé
Centralisez le déploiement des certificats nouvellement acquis sur leurs serveurs d'extrémité respectifs.

Analyse de vulnérabilité SSL
Identifiez et corrigez les configurations SSL vulnérables et les chiffrements faibles, et remplacez tous les certificats révoqués.

Intégration Active Directory
Intégrez, importez et gérez facilement les certificats mappés aux comptes d'utilisateurs dans Active Directory.

Marquage de certificat SHA-1
Identifiez et remplacez les certificats qui utilisent la fonction de hachage SHA-1 obsolète.

Alertes d'expiration
Éliminez les temps d'arrêt de service en recevant des notifications périodiques personnalisables sur les certificats sur le point d'expirer.

Gestion des certificats SSL

Découverte de clé SSH
Découvrez toutes les clés SSH de votre réseau et ajoutez-les à un référentiel sécurisé et centralisé.

Création et déploiement de clés
Créez de nouvelles paires de clés SSH; associez-les aux utilisateurs en masse et déployez-les sur systèmes cibles.

Rotation périodique des clés
Créez des tâches planifiées pour faire pivoter automatiquement les clés SSH à des intervalles de temps périodiques afin d'éviter toute utilisation abusive des privilèges.

Cartographie utilisateur-clé
Créez des tâches planifiées pour faire pivoter automatiquement les clés SSH à des intervalles de temps périodiques afin d'éviter toute utilisation abusive des privilèges.

Reprise d’activité
Planifiez des sauvegardes de l'ensemble de votre base de données à intervalles réguliers à des fins de reprise d’activité.

Audit et rapports
Établissez un mécanisme d'audit infalsifiable et obtenez un accès instantané à des rapports complets sur toutes les activités des utilisateurs.

Exigences matérielles

Le tableau ci-dessous explique les capacités matérielles minimales que votre serveur d'applications Key Manager Plus doit posséder pour une installation et une exécution réussies.

Taille de l'organisation	Processeur	RAM	Disque dur
Petite (Moins de 500 clés *)	Dual Core/Core 2 Duo or plus	4 Go	• 300 Mo pour le produit • 10 Go pour la base de données
Moyenne (500-1000 clés *)	Quad Core ou plus	8 Go	• 500 Mo pour le produit • 20 Go pour la base de données
Grande (> 1000 clés *)	Octa Core ou plus	16 Go	• 1 Go pour le produit • 30 Go pour la base de donnée

* Le terme «clés» fait référence au nombre de clés privées SSH plus le nombre de certificats SSL/TLS plus toute clé numérique gérée à l'aide de Key Manager Plus.

Logiciels requis

Systèmes d'exploitation

Windows

- Windows 10
- Windows 8
- Windows 7
- Windows Vista
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008
- Windows Server 2003
- Windows 2000 Server / Professional

Linux

(Key Manager Plus fonctionne généralement bien avec toutes les versions de Linux)

- Ubuntu 9.x and above
- CentOS 4.4 & above
- Red Hat Linux 9.0
- Red Hat Enterprise Linux 5.3, 5.4, 5.5

Remarque: Key Manager Plus peut également être exécuté sur les machines virtuelles de tous les systèmes d'exploitation ci-dessus.

Bases de données prises en charge

- PostgreSQL 9.2.4 - livré avec le produit.
- Prend en charge MS SQL Server 2008 et plus (le serveur SQL doit être installé dans Windows 2008 Server ou plus).

Navigateurs pris en charge

Le client HTML nécessite que l'un des navigateurs suivants soit installé sur le serveur d'applications.

- IE 9 et plus (sous Windows)
- Chrome et Firefox (sous Windows, Linux et Mac)

Logiciels prérequis

Aucune installation de logiciel préalable n'est requise pour utiliser Key Manager Plus. Il vous suffit de disposer des exigences matérielles et logicielles mentionnées ci-dessus, ainsi que d'un serveur de messagerie externe (serveur SMTP) pour envoyer des notifications par e-mail aux utilisateurs.

En dehors de cela, vous devez également disposer des fonctionnalités suivantes si vous prévoyez d'utiliser les opérations de découverte SSH et SSL dans Key Manager Plus.

- Un compte de service disposant de droits d'administrateur de domaine sur le serveur Key Manager Plus et sur les systèmes cibles que vous souhaitez gérer.
- Framework Microsoft .NET.

Gestion des certificats SSL

Découverte SSL prise en charge	Intégration CA
Certificats d'utilisateurs AD Certificats dans Microsoft Certificate Store Certificats émis par l'autorité de certification Microsoft Certificats de serveur SMTP Certificats d'équilibrage de charge Certificats hébergés dans AWS — ACM et IAM Certificats auto-signés	Let's Encrypt Microsoft CA GoDaddy Sectigo Symantec Thawte GeoTrust RapidSSL DigiCert

Algorithme de clé privée	Longueur de la clé privée (bit)a	Algorithme de signature
RSA DSA EC	1024 2048 4096	SHA256 SHA384 SHA512

Type de fichier de clés	Détection de vulnérabilité SSL
JKS PKCS12	État de révocation du certificat: CRL, OCSP Heartbleed POODLE Suites de chiffrement faibles

Gestion des clés SSH

Type de clé SSH	Longueur de clé SSH (bit)	Algorithme de signature
RSA DSA ECDSA ED25519	1024 2048 4096	SHA256 SHA384 SHA512

Autres spécifications

Méthodes d'authentification	Versions SSH, SSL/TLS prises en charge
Local (nom d'utilisateur et mot de passe) Active Directory RADIUS	SSH-2 SSL 3.0 TLS 1.0 TLS 1.1 TLS 1.2

Key Manager Plus nous permet de rester au top des certificats SSL pour tous nos sites Web. Avec Key Manager Plus, nous sommes en mesure de surveiller les certificats qui arrivent à expiration et de déployer de nouveaux certificats en temps opportun.

Ken Odibe
Consultant senior en infrastructure cloud,
Sapphire Systems

Planifier une démo personnalisée

Obtenir un devis

Zoho Corporation
4141 Hacienda Drive,
Pleasanton, CA 94588
Téléphone: +1-925-924-9500

ManageEngine
Key Manager Plus