SPANKEY SSH - PAM

ACCÈS ET AUTHENTIFICATION LINUX CENTRALISÉS

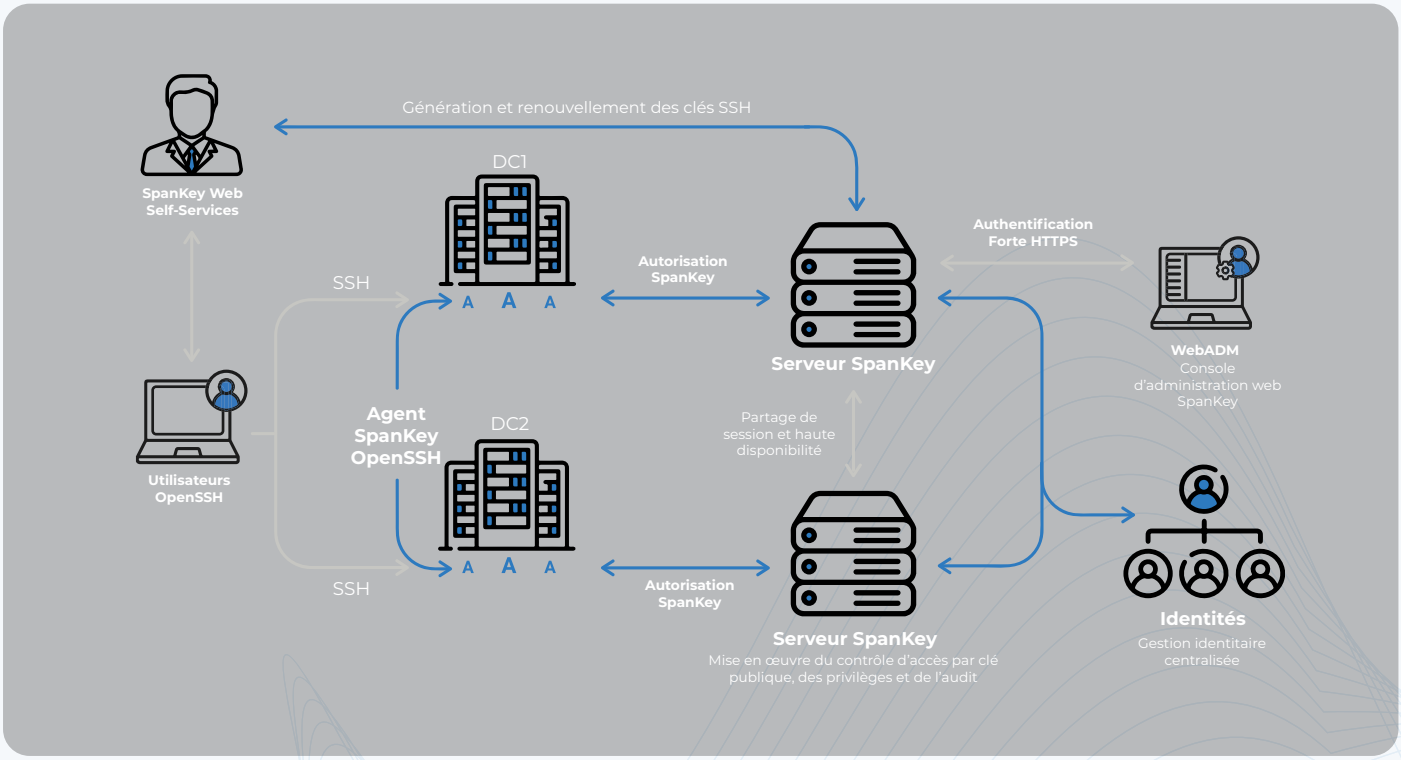
LA MEILLEURE FAÇON DE GÉRER LES ACCES SSH

SpanKey simplifie et centralise la gestion des accès SSH et des privilèges SUDO sur les systèmes Linux. Il s'appuie sur les annuaires, tels qu'Active Directory, OpenLDAP, ainsi que sur des annuaires cloud comme Entra ID, Google Workspace...

Les clés SSH et leur cycle de vie sont gérés automatiquement. Les privilèges SUDO sont définis de manière centralisée, par utilisateur ou par groupe, avec un contrôle précis. Toutes les sessions SSH sont auditées et les logs centralisés. Avec SpanKey, simplifiez l'administration des accès, renforcez la sécurité de vos infrastructures et garantissez une traçabilité complète des sessions.

NOTRE ENTREPRISE

Éditeur européen spécialisé dans la gestion des identités et des accès (IAM) et l'authentification multi-facteurs (MFA), RCDevs Security propose des solutions de sécurité modulaires et flexibles, disponibles en mode on-premise ou SaaS. Reconnue pour la fiabilité de ses logiciels et un haut niveau de satisfaction client, RCDevs accompagne aussi bien les PME que les grandes entreprises, tous secteurs confondus, à travers le monde.



Architecture Spankey

LES PROBLÉMATIQUES

La gestion des identités et des accès est essentielle en cybersécurité pour contrôler et tracer l'accès aux ressources numériques. Pourtant, la gestion des accès privilégiés via SSH reste un point faible. Ce protocole est couramment utilisé par les administrateurs pour se connecter à distance aux serveurs UNIX/Linux, exécuter des commandes ou transférer des fichiers.

Il s'appuie principalement sur des paires de clés publiques/privées. Bien plus sûres que les mots de passe, ces clés, sans gestion centralisée, sont souvent dupliquées, mal révoquées et peuvent échapper aux audits, entraînant une perte de contrôle des accès.

Ce manque de visibilité crée une faille majeure : une clé inconnue peut ouvrir un accès sensible sans laisser de trace claire de l'utilisateur.

LA RÉPONSE DE SPANKEY

SpanKey sécurise les accès SSH en s'appuyant sur toutes les sources d'identités configurées via WebADM, qu'il s'agisse de LDAP/AD, Entra ID, PingOne ou autres, pour un contrôle centralisé et unifié des utilisateurs.

Les points clés

➔ Intégration avec toutes les sources d'identités via WebADM (LDAP/AD, Entra ID, PingOne, etc.) pour un contrôle centralisé et unifié.

➔ Automatisation complète du cycle de vie des clés SSH : création, distribution et révocation, sans intervention manuelle.

➔ Gestion centralisée des privilèges SUDO limitant les actions sensibles aux utilisateurs autorisés.

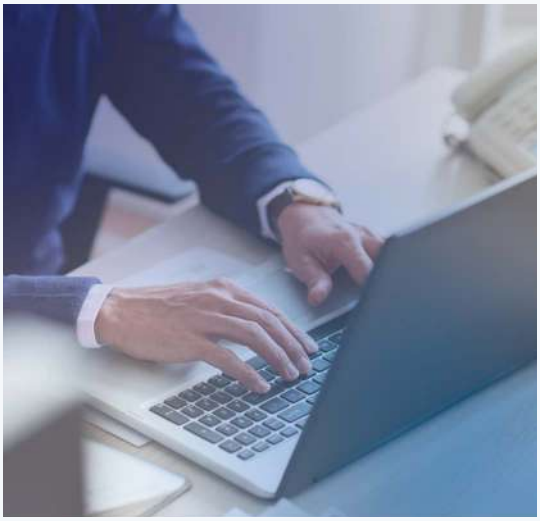
➔ Politiques d'accès flexibles et centralisées, appliquées en temps réel par l'agent SpanKey pour autoriser ou bloquer les connexions.

➔ Enregistrement et audit de toutes les connexions SSH, garantissant la conformité aux exigences IAM. Ainsi, SpanKey garantit des accès SSH sécurisés, contrôlés et pleinement intégrés à votre système global de gestion des identités.

PROVISIONNEMENTS AUTOMATISÉS

SpanKey automatise entièrement le provisionnement et la déprovision des accès et des clés SSH, en s'appuyant sur vos sources d'identités intégrées, qu'elles proviennent d annuaires d'entreprise ou de solutions IAM cloud.

La gestion dynamique par groupes d'utilisateurs déclenche automatiquement la création ou la révocation des autorisations sur les clients SpanKey. La distribution des clés SSH publiques, des règles SUDO et des configurations Auditd est centralisée et automatisée, garantissant une conformité immédiate et sans intervention manuelle.
La gestion automatique des cycles de vie des clés SSH garantit leur expiration et le renouvellement conformément aux exigences réglementaires et aux politiques internes.



AUDIT & TRAÇABILITÉ

Audit avancé
→ SpanKey déclenche automatiquement les règles d'audit dès la connexion, en enregistrant toutes les activités SSH, y compris les transferts SCP et SFTP.

Enregistrement de session
→ La capture en temps réel du terminal permet la lecture graphique des sessions SSH depuis la console d'administration, facilitant l'analyse post-incident et la conformité.

Journalisation approfondie
→ Les commandes, processus et événements du système de fichiers peuvent être enregistrés en détail.

Intégration SIEM
→ Les journaux peuvent être automatiquement envoyés vers un SIEM pour une analyse centralisée, la corrélation d'événements et des alertes personnalisées.

CONTRÔLE D'ACCES CENTRALISÉ

SpanKey offre un contrôle d'accès centralisé et granulaire, permettant de définir précisément qui peut accéder à quelles ressources, à quel moment, et sous quelles conditions d'authentification, incluant la possibilité d'exiger une MFA OpenOTP pour renforcer la sécurité.

GESTION DES COMPTES PARTAGÉS

Contrôle des comptes partagés
→ SpanKey permet de contrôler et tracer l'accès aux comptes partagés locaux tels que root, mysql, ou autres.

Accès individuel
→ Les utilisateurs autorisés accèdent à ces comptes via leur clé SSH personnelle, assurant ainsi une traçabilité précise des actions réalisées.

Responsabilité
→ Chaque opération effectuée avec un compte partagé est donc rattachée à l'identité individuelle de l'utilisateur, renforçant la responsabilisation et la transparence des accès aux ressources critiques.

BACKUP MASTER KEY

La clé Backup / Master offre un accès d'urgence, permettant de se connecter à n'importe quel système et sous n'importe quel compte. Elle garantit une solution de secours en cas de perte ou d'indisponibilité des clés habituelles.

SELF-SERVICE D'ENRÔLEMENT DES CLÉS SSH

Auto-gestion des clés SSH
→ Le portail web self-service permet aux utilisateurs de gérer leurs clés SSH en toute autonomie.

Génération de clés
→ Les utilisateurs peuvent générer une nouvelle paire de clés (RSA, DSA ou ECC),

Importation de clés
→ Les utilisateurs peuvent importer manuellement une clé publique existante.

Révocation de clés
→ Les utilisateurs peuvent révoquer les clés obsolètes ou compromises.

Politiques de sécurité
→ Les politiques de sécurité peuvent imposer la taille et la durée de validité des clés, assurant ainsi une protection conforme aux standards de l'entreprise.

Renouvellement automatique
→ Lorsqu'une clé expire, un lien de renouvellement est automatiquement envoyé à l'utilisateur.

Conformité & nouvel enrôlement
→ Ce processus permet de se réinscrire facilement tout en restant conformes aux politiques de sécurité.

FONCTIONNALITÉ OFFLINE

La fonctionnalité Offline utilise un cache local sécurisé pour permettre aux clients SpanKey d'effectuer une authentification SSH, même sans connexion au serveur, garantissant ainsi un accès fiable et sécurisé en conditions dégradées.

AUTHENTIFICATION MULTI-FACTEURS & ÉCRAN DE VERROUILLAGE

Lorsqu'elle est couplée à OpenOTP, l'authentification SpanKey permet d'ajouter jusqu'à trois facteurs supplémentaires : le mot de passe du compte, un code OTP ou une notification Push, et une opération de badging. SpanKey prend également en charge les clés FIDO2 pour les connexions SSH, ainsi que toutes les méthodes d'authentification compatibles avec OpenOTP.

SpanKey intègre une fonctionnalité de verrouillage automatique du terminal SSH en cas d'inactivité. Lorsqu'un utilisateur reste inactif pendant une durée définie, la session se verrouille automatiquement et exige la saisie de son mot de passe pour reprendre l'accès.

MÉTHODES D'AUTHENTIFICATION

OpenOTP Token App
Push mobile
ou OTP token

PKI
Authentification basée
sur le certificat utilisateur

Magic Links
QRCode par Mail ou SMS
pour confirmer l'accès

YubiKey
YubiOTP, OATH-HOTP
& PIV

FIDO2
Authentification par
cryptographie à clé publique

Tokens Logiciels
OATH basé sur
l'événement et le temps

Tokens Physiques
OATH basé sur
l'événement et le temps

Méthodes Traditionnelles
OTP par SMS, par Mail & Mail
sécurisé ou liste imprimée