PROVEIT by rubycat DATASHEET

PAM/BASTION français
Certifié Visa de sécurité CSPN
par l'ANSSI

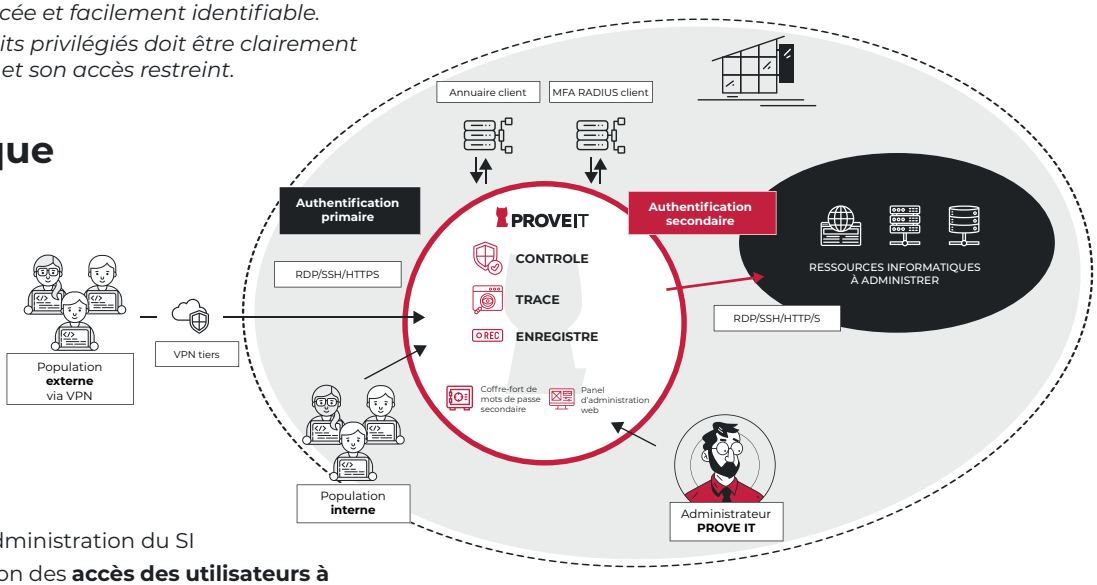
Une véritable politique de sécurité du SI inclut la **traçabilité** et le **contrôle des utilisateurs à privilèges**

Vos équipements critiques contiennent des **données** ou **applications sensibles** qu'il faut protéger pour garantir la continuité de votre activité, la pérennité de votre entreprise, mais aussi **la mise en conformité avec les normes et règlementations** (ISO 27001, RGPD, OSE,...) et **recommandations ANSSI** (Guide d'administration sécurisée du SI - partie 6.3).

Toute action sur un équipement critique doit impérativement être surveillée, tracée et facilement identifiable.

Toute personne à droits privilégiés doit être clairement identifiée et son accès restreint.

Schéma topologique



- **Point d'accès unique** pour l'administration du SI
- Portail fédérateur pour la gestion des **accès des utilisateurs à privilèges**
- Renforce la **sécurité des accès** avec notamment le **MFA** et le **coffre-fort d'identifiants secondaires** (gestion des secrets)
- Réduit le temps de **réponse à incidents**

	STANDARD	ADVANCED	ADVANCED CLUSTER
Contrôle des utilisateurs à privilèges et prestataires tiers	✓	✓	✓
Politique d'accès aux ressources critiques - RDP / SSH / HTTP/S	✓	✓	✓
Journalisation des connexions internes, externes et des opérations d'administration	✓	✓	✓
Coffre-fort sécurisé pour la gestion des comptes sensibles	✓	✓	✓
Enregistrement et archivage des sessions	✓	✓	✓
Visionnage en temps réel Re-visionnage pour analyse et action corrective	✓	✓	✓
Notifications avancées des évènements	✓	✓	✓
Politique de rétention configurable	✓	✓	✓
Segmentation des droits d'administration par profil : auditeurs / opérateurs / administrateurs	✗	✓	✓
API REST pour faciliter les opérations d'administration fréquentes	✗	✓	✓
Volumétrie supérieure à 40 sessions simultanées	✗	✗	✓
Haute-disponibilité	✗	✗	✓

La **licence PROVE IT** est basée sur le nombre de sessions simultanées ouvertes vers les ressources informatiques. Le nombre d'utilisateurs déclarés autorisés ainsi que le nombre de ressources déclarées sont illimités.

PROVE IT se décline en : STANDARD - ADVANCED - CLUSTER

Mode d'achat

2 modes d'achat disponibles :
- Licence perpétuelle - contrat annuel de maintenance à souscrire en supplément.
- Souscription - licence à durée déterminée avec maintenance incluse.

Pour vous accompagner, nous disposons d'un **réseau d'intégrateurs certifiés** sur la solution. Contactez-nous.

PROVE IT est disponible via différentes **centrales d'achat** (UGAP - marché multi-éditeurs, CAIH - marché ELODI, RESAH/SIPERREC,...).

Certification et label

- Visa de sécurité - CSPN par l'ANSSI (2018)
- Label France Cybersecurity
- Médaille d'Or - Trophée de la Sécurité à Paris en 2018

Mise en conformité : réglementations - recommandations - normes

PROVE IT est un élément fort de votre mise en conformité :

RGPD - ISO27001 - CNIL - ANSSI - HDS - TISAX - NIS & NIS2 - ...

Documentation et support

Un support éditeur en France dédié - Le contrat de maintenance intègre la mise à disposition des mises à jour mineures et majeures ainsi qu'une veille de vulnérabilité.

Documentation disponible en anglais et en français dans la solution.

Caractéristiques techniques

POC
Licence POC gratuite sur demande
Environnement
VMWare ESXi 5+
Microsoft Hyper-V 2008+
QEMU/KVM
Livraison et déploiement
Livraison de la solution via une image ISO basée sur Ubuntu 20.04 LTS
Fourniture de prérequis pour dimensionner la VM
Ex : 10 sessions = 4CPU, 3Go RAM, 110Go d'espace stockage pour 60j de rétention
Installation en moins d'une heure
Se positionne en rupture protocolaire, coupure des flux d'administration
Peut fonctionner en totale autonomie – environnement cloisonné
Sans agent / non invasive
Disponible en version STANDALONE *(STANDARD / ADVANCED)* ou CLUSTER
Possibilité d'automatiser le provisionning en ligne de commande – ANSIBLE
Utilitaires compatibles (liste non-exhaustive)
MRemoteNG
MobaXterm
Putty
Portails Web – tels que RDWeb (Microsoft)

MSTSC
Version minimale RDP : v8
Version minimale SSH : v2
Version minimale navigateur web : Chrome 103, Edge 103, Firefox 100
Topologie
Se positionne derrière un VPN tiers pour les accès distants
Interface réseau : gestion de plusieurs interfaces réseau avec possibilité de dédier une des interfaces pour le SSH de maintenance, le WebAdmin et l'API REST
Sauvegarde et migration
Automatique – en local sur la VM
Possibilité d'import / export des sauvegardes
Script de migration disponible pour passer des versions STANDARD et ADVANCED vers la version CLUSTER
Vie de la solution
Mise à jour régulières disponibles :
- Mineures : tous les mois environ
- Majeures : tous les 16 mois environ
Autonomie dans la mise à jour de l'OS Ubuntu
Documentations : guides d'administration, d'utilisateur et d'installation, notices d'intégration – incluses dans le WebAdmin – actualisées à chaque version

Nous consulter pour toute autre configuration

Fonctionnalités

Général
Modes d'authentification sur le bastion et vers les équipements cibles
Annuaire interne (proveit-interne)
Annuaire externe : AD, AzureAD, OpenLDAP, LDAP – Synchrone / Asynchrone
Multi-facteurs - interfaçage avec solutions disposant d'un connecteur RADIUS (inWebo/STA/DUO/LinOTP/...)
Fail2Ban intégré et paramétrable (nb de tentatives sur une durée)
Compatibilité Kerberos / Protected Users / Restricted Admin (RDP)
Mode d'authentification vers les cibles :
- Propagation des identifiants primaires
- Utilisation des secrets du coffre-fort (clé SSH ou identifiant/mdp)
- Re-saisie manuelle par l'utilisateur
Royaumes
Gestion des scénarios d'authentification – serveur appelé – primaire et secondaire
Gestion des sessions : timeout inactivité – nb de sessions par utilisateur – par royaume
Licence
Par palier de 5 sessions
Jeton de burst – débrayer le nb de sessions de la licence en 1 clic
Parcours utilisateur
Accès Kiosque – affichage des différentes ressources avec accès ouverts à l'utilisateur
Accès Direct (traçabilité préservée) :
- Connexion directe à la ressource identifiée
- Connexion M2M
Cluster
Haute disponibilité
Répartition de charge – plus de 40 sessions
Hébergement sur le même LAN
Coffre-fort de mots de passe
Protégé via PASSPHRASE ou SECRET SHARING (partage de clés)
1 conteneur chiffré par secret
Chiffrement CHACHA20-POLY1305
API Admin (en version ADVANCED)
Automatisation des tâches d'administration fréquentes
Import en masse des ressources cibles (via template CSV)
Gestion des accès à privilèges – Gérer et maîtriser les accès à privilèges
Contrôle des accès
RBAC – Rôle Based Access Control
Politique d'accès activable / désactivable au clic
Filtre d'accès temporel : intervalle de date – date – fréquence – horaires
WebAdmin en HTTPS – administration de la plateforme
WebAdmin version ADVANCED – segmentation des droits d'administration par profil
Contrôle de session
Dissuasion – message d'avertissement d'enregistrement – personnalisable
SSH :
- Autoriser X11, SCP, SFTP, PTY, SHELL, exécution de commandes, enregistrer les frappes clavier de la session SHELL
- Contrôler les signaux POSIX pouvant être échangés dans le flux SSH
- Redirections – directes / inverses
RDP :
- NLA
- Autoriser les redirections disques, l'utilisation du presse-papier, les canaux dynamiques, utiliser le mode console
- Forcer le mode Restricted Admin
HTTP/S en mode natif – sans serveur de rebond
Tout autre protocole via serveur de rebond
Chiffrement
Protocole de chiffrement SSH : aes256-ctr,aes192-ctr,aes128-ctr
Protocole de chiffrement RDP : TLSv1.2-1.3 / ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-RSA-AES256-SHA
Protocole de chiffrement HTTPS : TLSv1.2-1.3 / ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305
Auditabilité – Visibilité sur les actions réalisées
Journalisation / Traçabilité et visibilité temps-réel
Visualisation en temps réel d'une session utilisateur par l'Administrateur PROVE IT
Clôture d'une session jugée illégitime par l'Administrateur PROVE IT
Recherche par nom de machine, protocole, date d'authentification...
Enregistrement des sessions sur l'ensemble des protocoles
Stockage sous format brut – optimisation de l'utilisation du CPU
Visualisation depuis le navigateur ou téléchargement des enregistrements en local
Vidéo : 1.5 Mo/minute/session active en moyenne
Durée de rétention des enregistrements et journaux paramétrable
Logs
Utilisateur : authentification
Administrateur PROVE IT : authentification, actions effectuées sur le WebAdmin
Notifications
Alerte en fonction d'un événement – ressource/utilisateur
Ex : connexion réussie à un service
Alerte système – dépassement de seuil, nb de sessions, volumétrie de stockage...
Notifications email
Via SMTP
Notifications syslog
Vers un concentrateur de logs externe – SIEM ou solution de supervision
SNMP
MIB Ubuntu

rubycat

control & trace

Editeur français de logiciels spécialisé dans la traçabilité et le contrôle d'accès au système d'information, RUBYCAT vous apporte son expertise en cybersécurité et expérience en sécurisation des accès pour vous aider à répondre de manière simple à une problématique majeure : le manque de visibilité sur les actions réalisées par les comptes à privilèges sur vos systèmes d'information.

RUBYCAT - Le Luthétium, 3 Square du Chêne Germain, 35 510 Cesson-Sévigné (Rennes)
Tél. : + 33 (0)2 99 30 21 11 – sales@rubycat.eu – www.rubycat.eu