Traçabilité des administrateurs internes et externes : une garantie pour la conformité

Marc BALASKO – Ingénieur Avant-vente

WALLIX
TRACE, AUDIT & TRUST

Quelles normes ?

- Sécurité des données des titulaires de cartes bancaires

- Régulation des jeux en ligne

- Sécurité des données nominatives de santé

- Equilibrer sécurité et externalisation

Problématiques communes

Mot de passe

- PCI-DSS : 8.5.10 à 8.5.13

Mots de passe forts (7 caractères, alphanumériques) et archivés(4 derniers interdits , 6 échecs)

- Hébergement des données de santé à caractère personnel : P6 -> PSI 14 et 15

Présentation des critères suivants : Taille des mots de passe, complexité, expiration, historisation

- ARJEL

10 caractères minimum

Issus d'au moins 3 des 4 groupes de caractères suivants : minuscules, majuscules, spéciaux, chiffres

Ex : Wallix2011

Aperçu dans Wallix AdminBastion

Problématiques communes

Traçabilité des actions

- PCI-DSS : 10.2, 10.3

Toutes les actions des administrateurs sont enregistrées et consignées dans des journaux d'audit

- Hébergement des données de santé à caractère personnel : P6 -> 2.7

Présentation de la typologie des éléments tracés : Actions réalisées, comptes, etc..

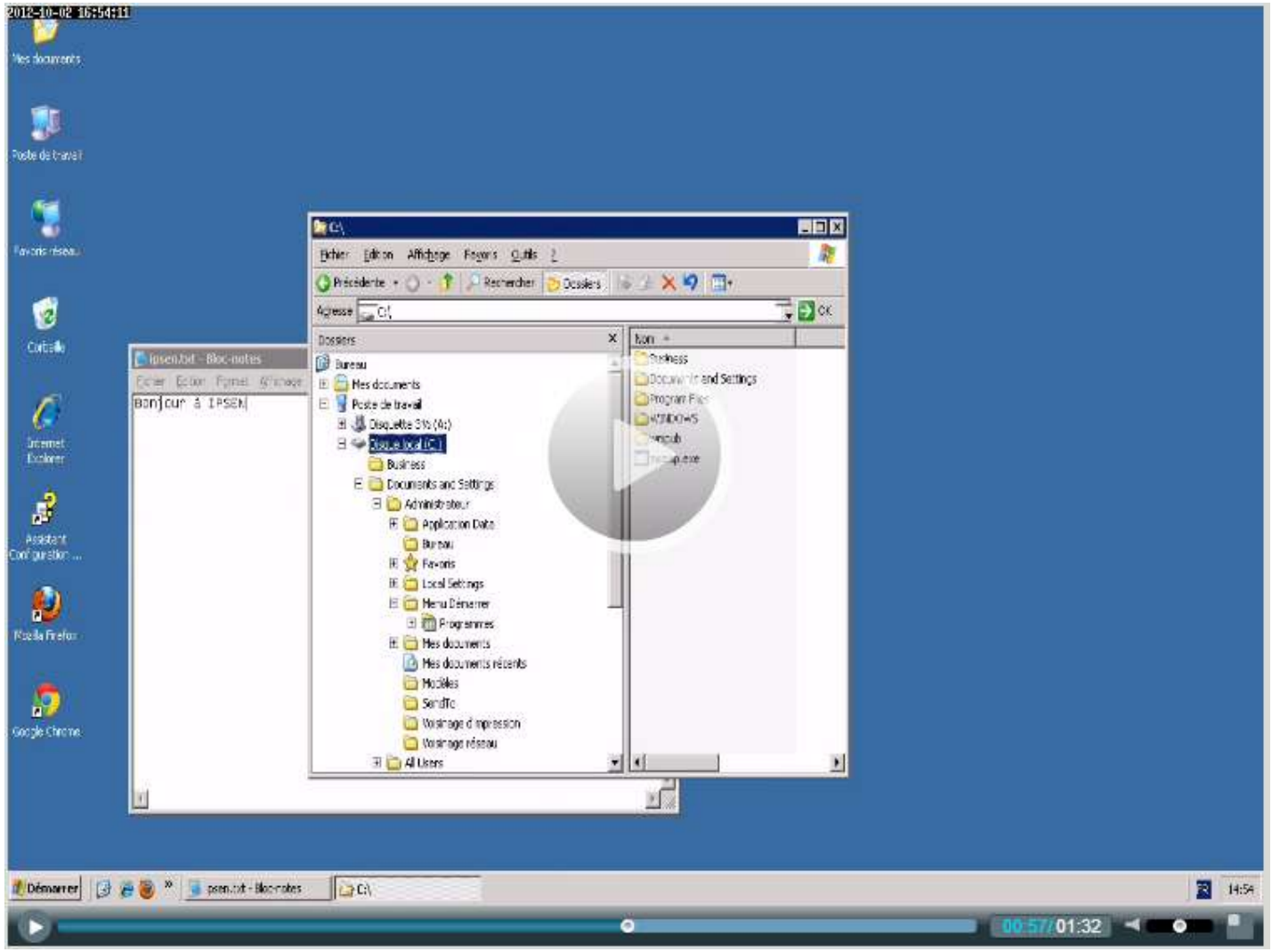
- ARJEL : 5.7.2.a

Préciser les contrôles sur les sous-traitants

Traces activées et consolidées pour retrouver l'exécutant d'une action

Aperçu dans Wallix AdminBastion

Aperçu dans Wallix AdminBastion



Problématiques communes

Authentification

- PCI-DSS : 10.3

Toutes les tentatives d'authentification sont logguées (succès/échec)

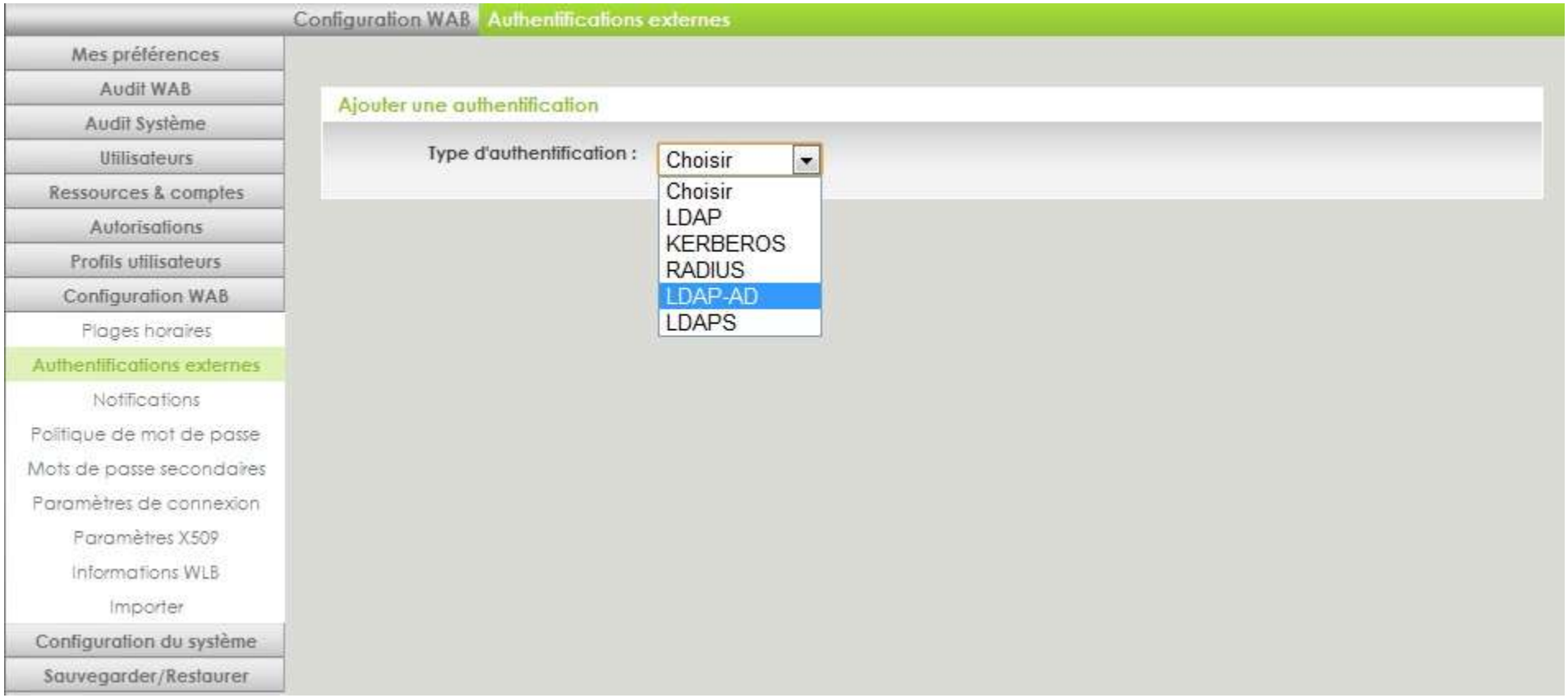
- Hébergement des données de santé à caractère personnel : P6 -> 2.7

Présentation de la typologie des éléments tracés : Authentification (succès/échec)

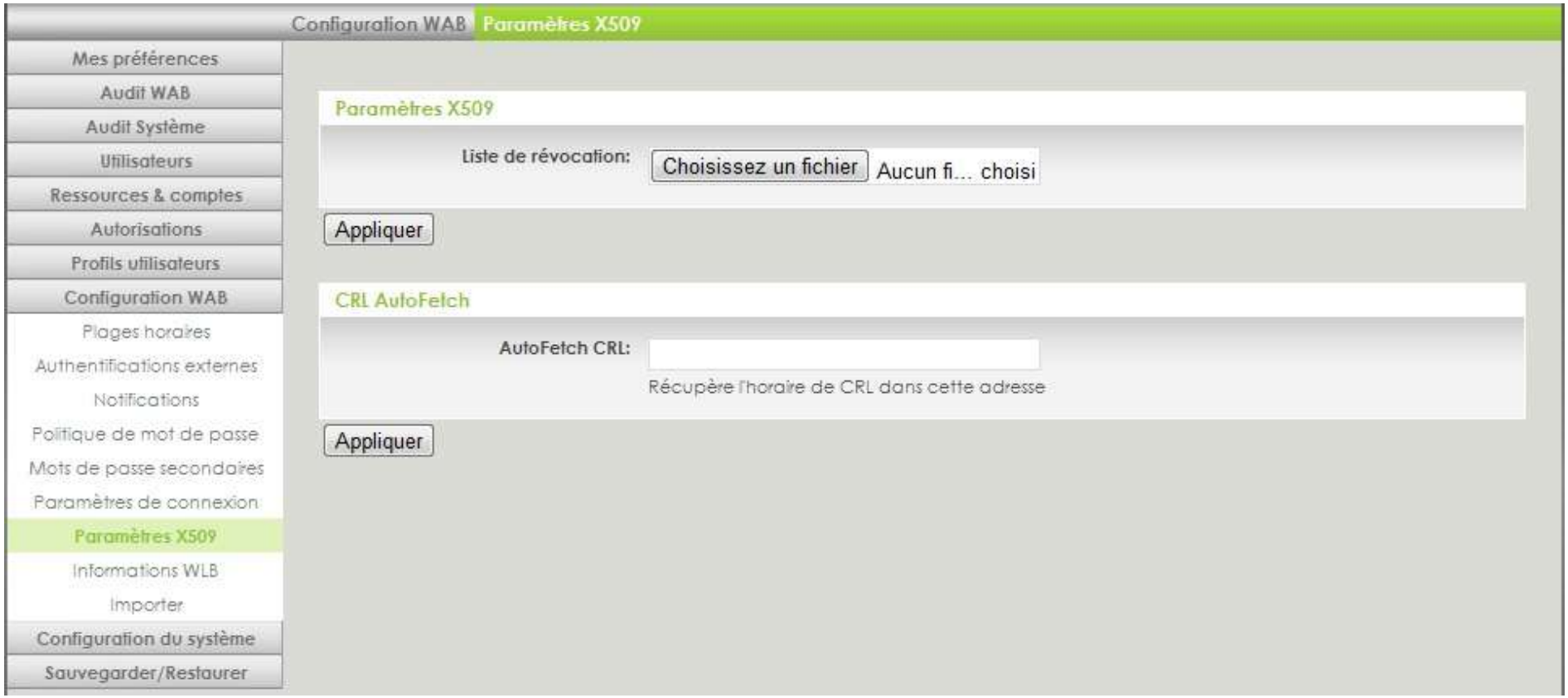
- ARJEL : 5.7.3.e.1

Authentification via certificat X509 V3

Aperçu dans Wallix AdminBastion



Aperçu dans Wallix AdminBastion



Aperçu dans Wallix AdminBastion

Maîtriser les risques d'infogérance

ANSSI Agence nationale de la sécurité des systèmes d'information

- Risques inhérents aux interventions distantes :2.2.2
  - Mots de passe par défaut ou faibles
  - Absence de traçabilité des actions
  - Possibilité d'effacer les traces a posteriori

Maîtriser les risques d'infogérance

ANSSI Agence nationale de la sécurité des systèmes d'information

- Recommandations:2.2.3
  - Dispositifs techniques de sécurité : filtrage des accès réseau, droits d'accès
  - Traçabilité des actions
- Mise en œuvre d'une passerelle sécurisée:2.2.4
  - Authentifier la machine distante et la personne en charge du support
  - Assurer une traçabilité de confiance des actions effectuées
  - Audit de la passerelle sécurisée

http://www.ssi.gouv.fr/fr/bonnes-pratiques/

Maîtriser les risques d'infogérance

ANSSI Agence nationale de la sécurité des systèmes d'information

- Certification de Sécurité de Premier Niveau (CSPN)
  - WAB a été audité par un cabinet indépendant
  - Réponse aux exigences des SI sensibles (Ministères, Armées)

http://www.ssi.gouv.fr/fr/certification-qualification/cspn/

Conclusion

- Wallix AdminBastion 3.1

  - Plate-forme sécurisée et intégrée de traçabilité et de contrôle d'accès
  - Réponse aux exigences normatives nationales et internationales
  - D'autres normes sont couvertes : ISO 27001, HIPAA, Solvency II, Basel III, etc
  - Les normes évoluent en permanence, le WAB aussi

- Sources

  - www.pcisecuritystandards.org
  - www.esante.gouv.fr
  - www.arjel.fr
  - www.ssi.gouv.fr

Nouveautés
WAB 3.1

Visualisation temps réel SSH/RDP

Permet à un administrateur du WAB de visualiser les sessions RDP & SSH actives sur le WAB

Interruption possible de la session en cas d'actions « inappropriées » de la part de l'utilisateur.

Répond aux contraintes réglementaires du type « 4 yeux ».

Provisionning via Services Web

Autorise le « provisionning » du WAB via des services Web de type SOAP

Provisionning :

-des utilisateurs
- des comptes
- des équipements cibles
- des droits d'accès …

Ces informations peuvent être synchronisées automatiquement entre une solution centrale de type IAM et un WAB

Ce qui permet **une diminution drastique du TCO du WAB.**

Améliorations des performances

Connexions RDP/TSE

Hausse de 200% du nombre maximal de connexions RDP simultanées enregistrées

Division par 4 de la volumétrie de l'enregistrement d'une connexion RDP

Support du chiffrement TLS/SSL de bout en bout

Autres nouveautés

Authentification secondaire par clé SSH

Permet au WAB de relayer vers un équipement cible (ex : serveurs Unix/Linux) les informations contenues dans la clé privée SSH d'un utilisateur.

Ainsi, il est possible de mettre en place un WAB dans une infrastructure existante d'authentification par clés SSH.

Support de l'authentification secondaire par formulaire HTML

Permet d'utiliser le mode SSO du WAB en cas de connexions vers des consoles d'administration Web utilisant l'authentification par formulaire HTML.

Ainsi, les utilisateurs n'auront plus à connaitre le login/mot de passe d'accès à la console Web cible : ils s'authentifieront uniquement avec leurs identifiants WAB

WallixAdminBastion

Démonstration

Annexe

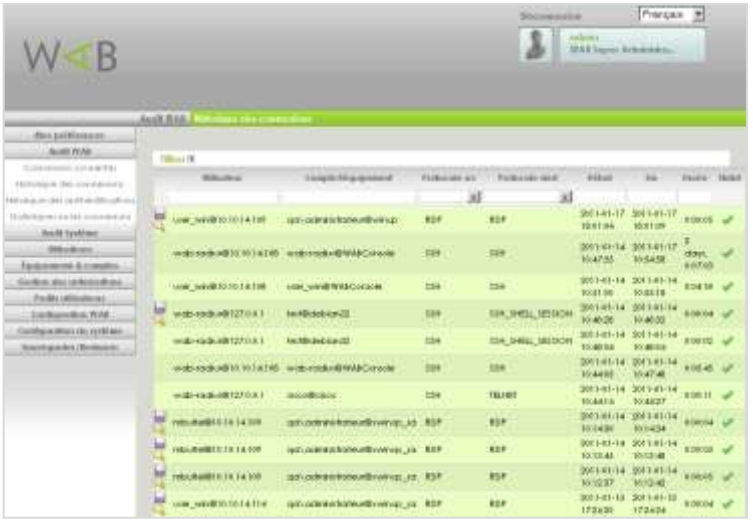
Rappel fonctionnalités WAB

Traçabilité

Vous savez qui fait quoi, quand, où et comment.

Wallix AdminBastion
permet la traçabilité des connexions
et des actions menées par les équipes IT
et les prestataires sur les équipements
administrés.

Grâce à la **console d'administration du WAB**,
il est possible de suivre les connexions
en temps réel et d'en consulter le journal.



Enregistrement des sessions

En cas d'audit ou d'incident, vous pouvez visionner les sessions de travail de vos prestataires

Les actions effectuées sur les équipements cibles sont enregistrées en continu pour visionnage ultérieur

- au format vidéo pour les sessions graphiques Windows Terminal Server (RDP) & VNC
- au format texte pour les sessions en lignes de commande (SSH, Telnet).

WallixAdminBastion

Contrôle des accès

Vous contrôlez les accès de vos prestataires informatiques, qu'ils soient internes ou externes, les comptes à privilèges et les utilisateurs à risque.

Grâce à des règles simples et puissantes vous contrôlez les accès aux équipements

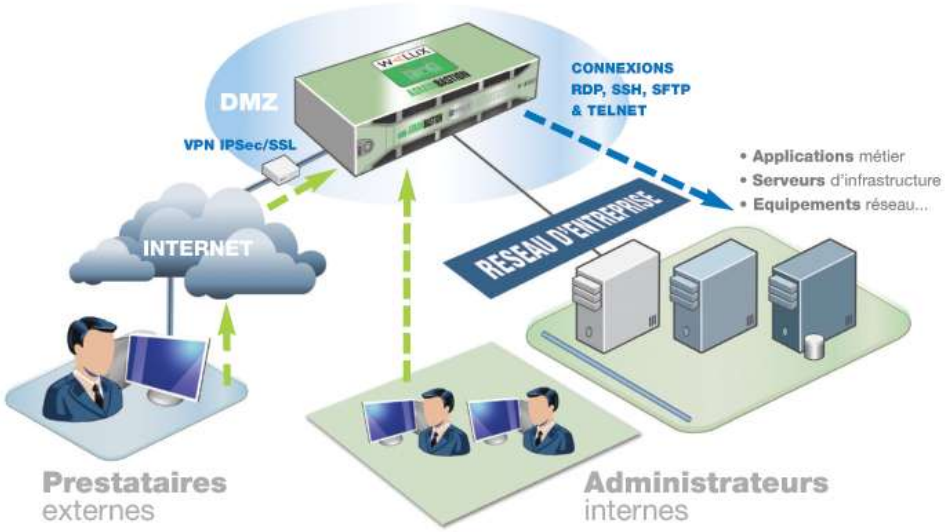
Ces règles se basent sur des critères tels que l'adresse IP, l'identifiant, les plages horaires, les protocoles ou le type de session SSH (X11, Shell, Remote exec, etc.)

Authentification unique

Chaque utilisateur se connecte au WAB avec un couple identifiant/mot de passe UNIQUE ou certificat pour accéder aux équipements cibles

Les mots de passe de ces équipements sont stockés dans le WAB et permettent d'automatiser l'ouverture de sessions.

Vous gérez facilement le turn-over de vos équipes IT, sans craindre de laisser l'accès à vos serveurs critiques à des personnes qui ne sont plus autorisées.



Autres fonctionnalités

Statistiques

Grâce à la fonction de reporting intégrée, les administrateurs du WAB peuvent consulter des graphiques et des statistiques sur l'activité du WAB

Analyse du flux SSH

Toutes les commandes entrées sont analysées en temps réel
avec envoi d'une alerte, voire coupure de la connexion SSH en cas de détection d'une chaine de caractères interdite.

Support certificats X509v3

L'authentification des utilisateurs internes et des prestataires externes peut s'effectuer **via un certificat électronique X509 V3**

Fonctionnement sans agent

WAB fonctionne sans agent spécifique, ni sur les équipements
administrés, ni sur les postes de travail, ce qui permet un déploiement rapide.

Contact

Marc BALASKO
Ingénieur avant-vente WAB

118, Rue de Tocqueville • 75017 PARIS
Tél. : +33 (0)1 70 36 37 52
Mob. : +33 (0)6 61 84 78 03
Fax : +33 (0) 1 43 87 68 38
email : marc.balasko@wallix.com

www.wallix.com

WALLIX FRANCE
http://www.wallix.fr
Email : sales@wallix.com
118, rue de Tocqueville - 75017 Paris
Tél. : +33 (0)1 53 42 12 90
Fax : +33 (0)1 43 87 68 38

WALLIX UK
http://www.wallix.com
Email: sales-emea@wallix.com

WALLIX USA
http://www.wallix.com
Email: sales-usa@wallix.com