



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



- Sécurité des données des titulaires de cartes bancaires



- Régulation des jeux en ligne



- Sécurité des données nominatives de santé



- Equilibrer sécurité et externalisation

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

- Audit WAB
- Audit Système
- Utilisateurs
- Ressources & comptes
- Autorisations
- Profils utilisateurs
- Configuration WAB
- Plages horaires
- Authentications externes
- Notifications
- Politique de mot de passe**
- Mots de passe secondaires
- Paramètres de connexion
- Paramètres X509
- Informations WLB
- Importer
- Configuration du système
- Sauvegarder/Restaurer

Politique de mot de passe

Expiration du mot de passe	0	en jours. 0 signifie aucune expiration.
Échéance avant le premier avertissement	0	en jours. 0 signifie aucun avertissement.
Taille minimale du mot de passe	6	
Nombre maximum d'echecs d'authentifications par utilisateur	0	0 signifie aucun contrôle
Nombre minimal de caractères spéciaux	0	
Nombre minimal de lettres en majuscules	0	
Nombre minimal de caractères numériques	0	
Nombre de derniers mots de passe à rejeter	4	
L'identifiant et le mot de passe peuvent être identiques	Non	

Modifier

Charger la clé publique gpg

Télécharger Mots de passe interdits...

- password
- pass
- 123456
- azerty
- qwerty
- wxcvbn
- zxcvbn

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

Audit WAB Historique des connexions

Mes préférences

Audit WAB

Connexions courantes

Historique des connexions

Historique des authentifications

Statistiques sur les connexions

Audit Système

Utilisateurs

Ressources & comptes

Autorisations

Profil utilisateurs

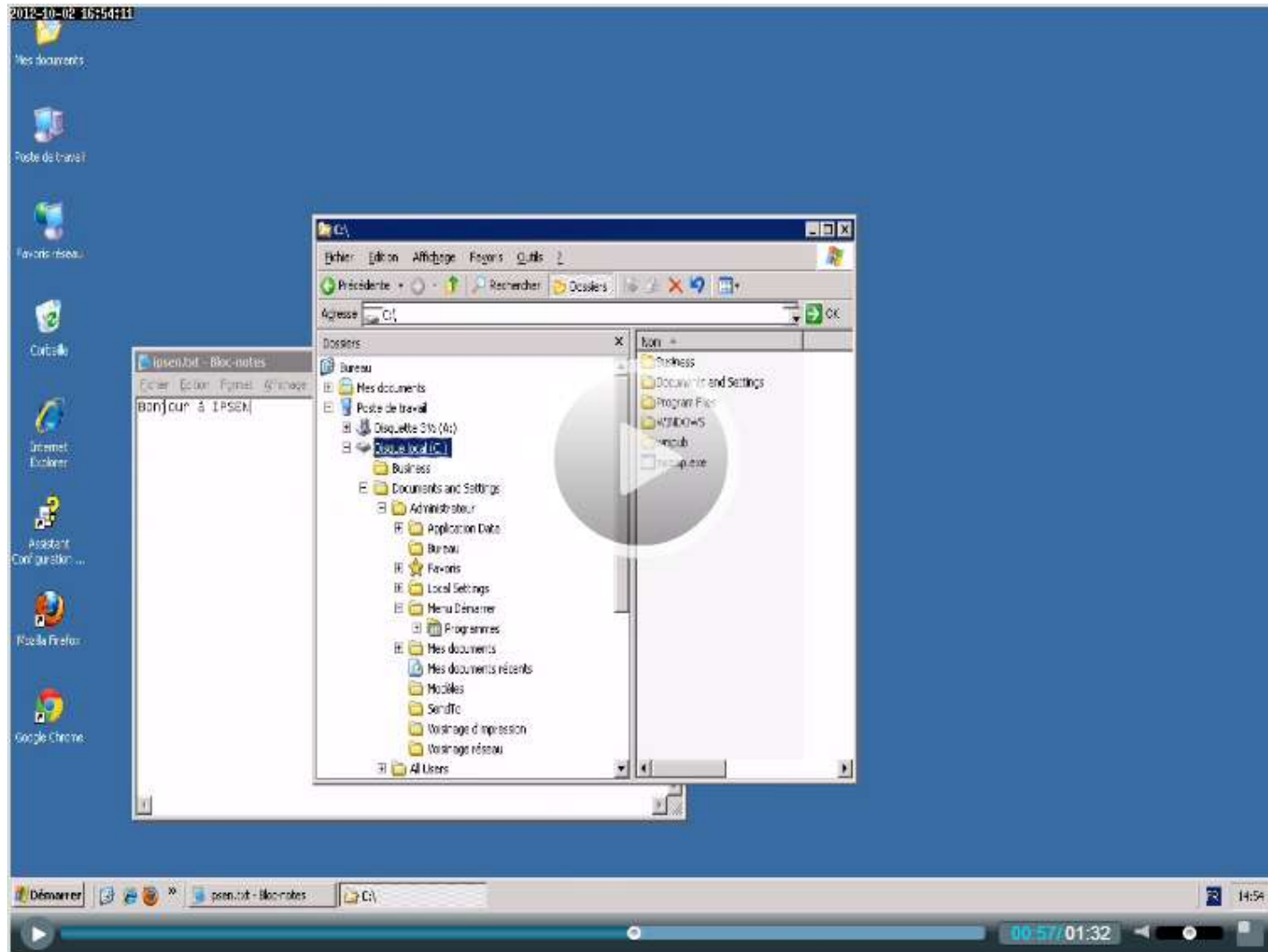
Configuration WAB

Configuration du système

Sauvegarder/Restaurer

Filter de recherche

	Utilisateur	Compte@équipement	Protocole src	Protocole dest	Début	Fin	Durée	Stat	
	mbu@10.10.4.109	test@win2k3-nd	RDP	RDP	2011-09-08 16:49:06	2011-09-08 17:05:38	0:16:32	✓	Télécharger le fichier csv
	mbu@10.10.4.109	test@win2k3-nd	RDP	RDP	2011-09-08 16:51:02	2011-09-08 16:51:07	0:00:05	✓	
	mbu@10.10.4.109	test@win2k3-nd	RDP	RDP	2011-09-08 16:50:11	2011-09-08 16:50:24	0:00:13	✓	
	mbu@10.10.4.109	test@win2k3-nd	RDP	RDP	2011-09-08 16:48:30	2011-09-08 16:48:56	0:00:26	✓	
	mbu@10.10.4.109	test@win2k3-nd	RDP	RDP	2011-09-08 16:41:50	2011-09-08 16:41:51	0:00:01	✓	
	mbu@10.10.4.109	test@win2k3-nd	RDP	RDP	2011-09-08 16:41:50	2011-09-08 16:41:51	0:00:01	✓	
	mbu@10.10.4.192	test@debian32	SSH	SSH_SHELL_SESSION	2011-09-08 16:32:00	2011-09-08 16:32:03	0:00:03	✓	



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

Configuration WAB **Authentifications externes**

Mes préférences

Audit WAB

Audit Système

Utilisateurs

Ressources & comptes

Autorisations

Profils utilisateurs

Configuration WAB

Plages horaires

Authentifications externes

Notifications

Politique de mot de passe

Mots de passe secondaires

Paramètres de connexion

Paramètres X509

Informations WLB

Importer

Configuration du système

Sauvegarder/Restaurer

Ajouter une authentification

Type d'authentification :

- Choisir
- Choisir
- LDAP
- KERBEROS
- RADIUS
- LDAP-AD**
- LDAPS

Configuration WAB Paramètres X509

- Mes préférences
- Audit WAB
- Audit Système
- Utilisateurs
- Ressources & comptes
- Autorisations
- Profils utilisateurs
- Configuration WAB
 - Plages horaires
 - Authentifications externes
 - Notifications
 - Politique de mot de passe
 - Mots de passe secondaires
 - Paramètres de connexion
 - Paramètres X509**
 - Informations WLB
 - Importer
- Configuration du système
- Sauvegarder/Restaurer


Paramètres X509

Liste de révocation: Aucun fi... choisi

CRL AutoFetch

AutoFetch CRL:

Récupère l'horaire de CRL dans cette adresse

Audit WAB	Filtre de recherche 			
	Date	Identifiant	IP source	Résultat
Connexions courantes				
Historique des connexions				
Historique des authentifications				
Statistiques sur les connexions				
Audit Système				
Utilisateurs				
Ressources & comptes				
Autorisations				
Profils utilisateurs				
Configuration WAB				
Configuration du système				
Sauvegarder/Restaurer				
	2011-09-08 17:47:35	mbu	10.10.4.109	DENIED
	2011-09-08 17:43:15	mbu	10.10.4.109	SUCCESS
	2011-09-08 17:42:07	mbu	10.10.4.109	SUCCESS
	2011-09-08 16:51:02	mbu	10.10.4.109	SUCCESS
	2011-09-08 16:50:08	mbu	10.10.4.109	SUCCESS
	2011-09-08 16:49:04	mbu	10.10.4.109	SUCCESS
	2011-09-08 16:48:28	mbu	10.10.4.109	SUCCESS
	2011-09-08 16:41:50	mbu	10.10.4.109	SUCCESS
	2011-09-08 16:31:59	mbu	10.10.4.192	SUCCESS
	2011-09-08 16:31:18	mbu	10.10.4.192	SUCCESS

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



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/>

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/>

ANSSI

Agence nationale de la
sécurité des systèmes
d'information



■ 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

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 ».



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

Provisionnement :

- 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.**

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



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 connaître le login/mot de passe d'accès à la console Web cible : ils s'authentifieront uniquement avec leurs identifiants WAB

Démonstration

Annexe

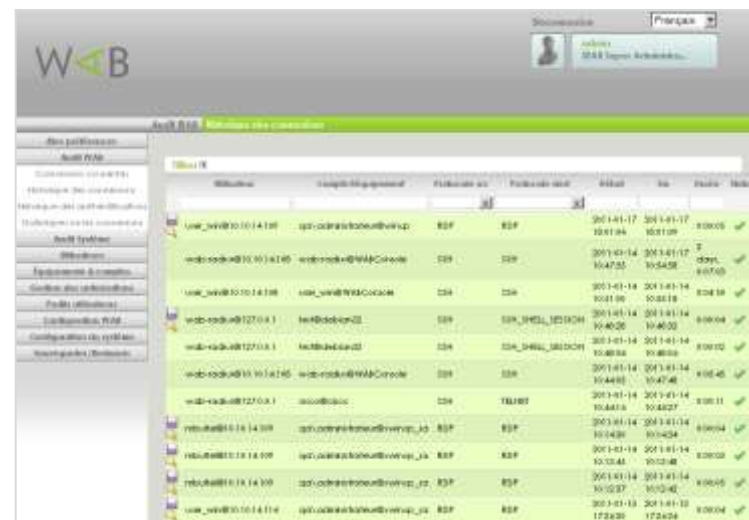
Rappel fonctionnalités WAB

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.



Utilisateur	Appareil/Équipement	Protocole de	Protocole vers	État	De	Jusqu'à	Statut
user_wab@10.14.10	ip2.admin@bastion@wsp	RDP	RDP	10.14.17	10.14.17	10.14.17	0000 ✓
wab-cod@10.10.116	wab-cod@WABCircle	SSH	SSH	10.47.35	10.47.35	10.14.17	0001 ✓
user_wab@10.14.10	user_wab@WABCircle	SSH	SSH	10.11.14	10.11.14	10.14.14	0002 ✓
wab-cod@127.0.1	10.40.00	SSH	SSH, SHEL, SUDO	10.40.00	10.40.00	10.14.14	0003 ✓
wab-cod@127.0.1	10.40.00	SSH	SSH, SHEL, SUDO	10.40.00	10.40.00	10.14.14	0004 ✓
wab-cod@10.10.116	wab-cod@WABCircle	SSH	SSH	10.44.15	10.44.15	10.14.14	0005 ✓
wab-cod@127.0.1	10.44.15	SSH	SSH	10.44.15	10.44.15	10.14.14	0006 ✓
rsbak@10.14.10	ip2.admin@bastion@wsp_10	RDP	RDP	10.14.36	10.14.36	10.14.14	0007 ✓
rsbak@10.14.10	ip2.admin@bastion@wsp_11	RDP	RDP	10.14.37	10.14.37	10.14.14	0008 ✓
rsbak@10.14.10	ip2.admin@bastion@wsp_12	RDP	RDP	10.14.38	10.14.38	10.14.14	0009 ✓
user_wab@10.14.10	ip2.admin@bastion@wsp_13	RDP	RDP	17.24.26	17.24.26	10.14.14	0010 ✓

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).



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

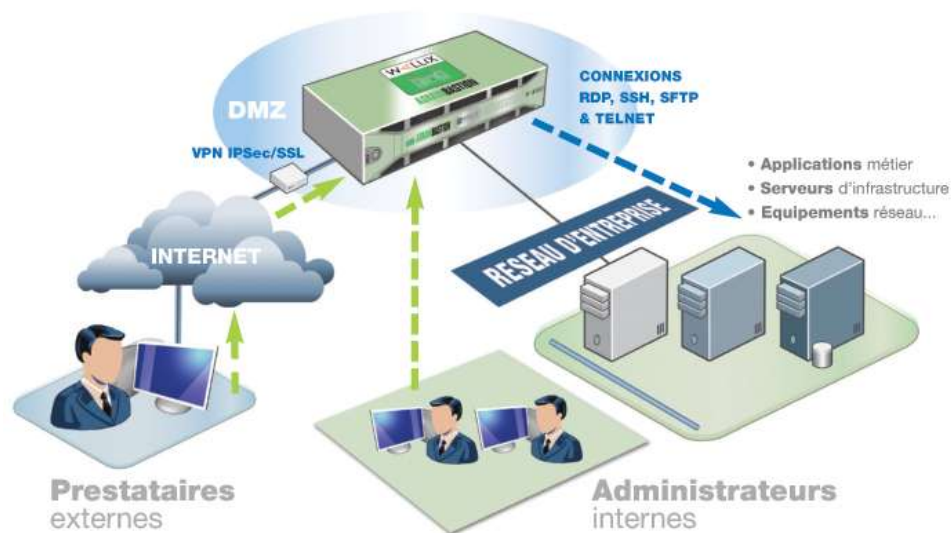
Ces règles se basent sur des critères tels que l'adresse IP, l'identifiant, les plages horaires, les protocoles ou le type de session SSH (X11, Shell, Remote exec, etc.)



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.



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 chaîne 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