WALLIX
CYBERSECURITY SIMPLIFIED

WALLIX ACADEMY

Formations certifiantes à distance

SECURE
YOUR DIGITAL
FUTURE

WALLIX ACADEMY

Formations certifiantes à distance

Pour bénéficier de notre formation à distance,
vous devrez utiliser Microsoft Teams.

La plateforme WALLIX Training LABs vous permet de suivre tous les LAB de formation indépendamment. Pour cela, la plateforme comprend 4 machines virtuelles préconfigurées: contrôleur de domaine (Windows 2016), serveur Windows 2016, serveur Linux et WALLIX Bastion.

Configuration minimum requise :

- 8GB de Ram ou plus
- Processeur I5
- 40 Go d'espace disque disponible
- Dans la première étape de la formation, nous configurerons cette plateforme.
- Les droits d'administrateur sur votre ordinateur sont obligatoires pour installer et configurer correctement tous ces outils.

Préparez les machines virtuelles du laboratoire :

Téléchargez et installez Virtual Box
https://www.virtualbox.org/wiki/Downloads
- Platform package
- Virtual Box Extension Package

L'accès aux machines virtuelles du laboratoire
vous sera communiqué au moment de votre inscription.

WALLIX
CYBERSECURITY SIMPLIFIED

SECURE
YOUR DIGITAL
FUTURE

WALLIX CERTIFIED PROFESSIONAL / **WCP**

Cette formation est destinée aux ingénieurs et techniciens des clients finaux et partenaires revendeurs de WALLIX qui souhaitent maîtriser la configuration, le déploiement et l'administration de la solution WALLIX Bastion.

PRÉREQUIS :

Le stagiaire doit être familiarisé avec **les protocoles SSH, RDP, le concept de proxy et les environnements Linux. Des compétences systèmes, réseaux et infrastructures** permettront au stagiaire de s'approprier plus vite le Bastion.

DESCRIPTION :

Cette formation technique de 3 jours permet de découvrir et de prendre en main notre solution WALLIX Bastion. Elle offre les moyens nécessaires d'appréhender les concepts et les fonctionnalités de base pour un déploiement dans une architecture classique. Alternant théorie et pratique, elle se base sur une participation active du stagiaire qui devra configurer et administrer le bastion dans une plateforme de LAB pour devenir complètement autonome. En fin de formation, le stagiaire devra passer un examen sous la forme d'un QCM. **Un score minimum de 70% est requis pour obtenir la certification WALLIX Certified Professional (WCP).**

Le stagiaire certifié recevra un diplôme attestant du statut **WALLIX Certified Professional (WCP).**

Contenu de la formation :

I. Formations et certifications	• Mise à jour de la version du Bastion
II. Entreprise et produits	• Restaurer une version précédente du Bastion
• L'entreprise WALLIX	• Installer/désinstaller un hotfix
• Produits et services	• Supervision et logs
• Licences et support	• Configuration d'un serveur mail et activation des notifications
III. Installation et prise en main du Bastion	• Les composants et les services principaux du Bastion
• Installation d'une appliance WALLIX Bastion	**IV. WALLIX Session Manager**
• La localisation dans un réseau	• Concepts globaux
• La configuration initiale	• Ajouter un utilisateur primaire (authentification locale)
• Première connexion	• Ajouter un groupe primaire
• Modification du mot de passe ADMIN	• Ajouter un équipement
• Installation de la licence	• Ajouter un compte secondaire (compte d'équipement
• Configuration réseau	• Ajouter un groupe de ressources
• Configuration du fuseau horaire et des serveurs NTP	• Ajouter une autorisation
• Ajouter un administrateur du Bastion	• Connexion à un serveur RDP
• Sauvegarde de la configuration	• Connexion à un serveur SSH
• Restauration de la configuration	• Modification du message d'avertissement
• Sauvegarde d'une version du Bastion	• Ajouter une application

WALLIX
CYBERSECURITY SIMPLIFIED

WALLIX CERTIFIED PROFESSIONAL / **WCP**

• Ajouter un scénario SSH	• Changement de mot de passe côté administrateur
• Prérequis	• Bris de glace
• Ajouter un utilisateur primaire (authentification externe)	• L'audit du Password Manager
• Importer des utilisateurs primaires depuis un serveur LDAP/AD	• Le process d'approbation pour le Password Manager
• Ajouter un compte secondaire (domaine global)	**VII. WALLIX Access Manager**
• Le process d'approbation pour le Session Manager	• Concepts globaux
• Les Profiles utilisateurs	• Installation du server MySQL
• Import/export	• Installation du WALLIX Access Manager
• Gestion de la HA	• La configuration par défaut
V. Session Audit	• Ajouter une organisation
• Sessions courantes	• Ajouter un Bastion à une organisation
• L'historique des sessions	• Ajouter un utilisateur primaire à une organisation
• L'historique des approbations	• Politique de mot de passe d'une organisation
• L'historique des comptes	• Personnaliser la charte graphique de l'interface web
• L'historique des authentifications	• Se connecter à une organisation
• Les statistiques des connexions	• Se connecter à un serveur en RDP
• Les logs d'audit	• Se connecter à une application
• Les paramètres d'enregistrement des sessions	• Se connecter à un serveur en SSH
• Gestion des enregistrements de sessions	• Accéder au mot de passe des comptes
VI. WALLIX Password Manager	• L'audit de session depuis l'Access Manag
• Concepts globaux	• Administrer le WALIX Access Manager
• Ajouter une politique d'emprunt	**VIII. La haute disponibilité WALLIX**
• Configurer la politique d'emprunt dans un compte secondaire	• LA HA Bastion WALLIX
• Ajouter un compte PM dans le groupe de ressources	• La réplication HA WALLIX
• Activer l'emprunt de MDP dans une autorisation	**IX. Centre de support client WALLIX**
• L'emprunt de mot de passe côté utilisateur	• Avant d'ouvrir un ticket support
• Ajouter une politique de changement de mot de passe	• Ouvrir un ticket support
• Les plugins de changement de mot de passe	
• Activer le changement de MDP dans un compte secondaire	
• Activer le changement de MDP et configurer la politique de changement de mot de passe dans un domaine local/global	
• Activer le changement de mot de passe à la libération	

SECURE
YOUR DIGITAL
FUTURE

WALLIX CERTIFIED EXPERT / **WCE**

Cette formation est destinée aux ingénieurs des partenaires revendeurs de WALLIX qui souhaitent offrir des services professionnels aux clients finaux pour des déploiements avancés de la solution WALLIX Bastion.

PRÉ-REQUIS / COMPÉTENCES :

Le stagiaire doit être certifié **WCP (WALLIX CERTIFIED PROFESSIONAL).** Il doit également être familiarisé avec **la ligne de commande GNU/Linux. Des connaissances en scripting** faciliteront le suivi de cette formation.

DESCRIPTION:

Cette formation technique de 2 jours présente les notions avancées des solutions WALLIX pour pouvoir fournir des services professionnels à des clients finaux. Fondée sur la mise en pratique des configurations avancées du Bastion (architecture actif/actif, provisioning automatique, plan de reprise d'activité, etc.), la formation permet d'acquérir les connaissances et les compétences nécessaires pour des déploiements spécifiques et/ou à large échelle dans des environnements complexes. Un examen sous la forme d'un QCM doit être passé par le stagiaire en fin de formation et il devra avoir un score de 70% pour obtenir le diplôme attestant du statut **WALLIX Certified Expert (WCE).**

I. Authentifications Avancées	• Sécuriser l'identifiant/mot de passe utilisés par l'application AutoIt
• Bastion - LDAP/AD Authentification explicite	• Le script WAB5IELogon
• Bastion – Radius Authentification explicite	**III. Les paramètres des proxies**
• Bastion – Kerberos Authentification explicite	• Concepts globaux
• Bastion – Kerberos Authentification transparente	• Politique de connexion RDP
• Bastion – Certificat X509 Authentification transparente	• Les paramètres globaux du proxy RDP
• Access Manager – LDAP Authentification explicite	• Les paramètres globaux du proxy RDP sesman
• Access Manager – Certificate X509 Authentification transparente	• Changer le certificat autosigné du proxy RDP
• Access Manager – SAML (Security assertion markup language) Authentification explicite	• Politique de connexion SSH
II. Applications avancées	• Les paramètres globaux du proxy SSH
• Rappel : Les applications dans WALLIX Session Manager	• Politique de connexion TELNET
• Les clusters	• Politique de connexion VNC
• Le langage de scripting AutoIt	• Les paramètres globaux du proxy VNC
• Télécharger et installer l'application AutoIt	**IV. Password Manager Avancés**
• Écrire un script AutoIt *.au3	• Rappel : WALLIX Password Manager
• Compiler un script pour générer une application AutoIt *.exe	• WAAPM : WALLIX Application to Application Password Manager
• Télécharger l'application AutoIt sur le serveur tolt *.exe	•Le Bastion comme Vault Externe (à partir de V6.1)
• Ajouter une application AutoIt sur le Bastion	

WALLIX
CYBERSECURITY SIMPLIFIED

WALLIX CERTIFIED EXPERT / **WCE**

V. REST API	• Les méthodes de l'API REST du Bastion
• Concept global	• Consulter les ressources avec l'API REST
• L'API REST du Bastion	• Ajouter une ressource avec l'API REST
• L'authentification sur l'API REST du Bastion	• Modifier une ressource avec l'API REST
• Déconnexion de l'API REST du Bastion	• Supprimer une ressource avec l'API REST

A propos de WALLIX

Editeur de logiciels de cyber sécurité, WALLIX Group est le spécialiste Européen de la gouvernance des comptes à privilèges. Répondant à l'évolution réglementaire et aux enjeux de cybersécurité qui touchent l'ensemble des entreprises, les solutions WALLIX protègent des cybermenaces, vols et fuites de données liés aux identifiants volés et aux privilèges détournés.

WWW.WALLIX.COM

WALLIX
CYBERSECURITY SIMPLIFIED