

WALLIX ACADEMY

Formations certifiantes



WALLIX ACADEMY

Formations certifiantes

La WALLIX Academy a pour vocation de former partenaires et clients utilisateurs aux produits WALLIX et de créer et animer une communauté de certifiés, membres du Club des certifiés WALLIX.

WALLIX propose 3 niveaux de formations, Administrateur, Professionnel et Expert, pour l'ensemble de ses clients et partenaires de WALLIX. Suivre ces formations permettra à vos équipes de maîtriser les différents aspects techniques et fonctionnels des solutions WALLIX.

	PAM (P)	IDaaS (I)	EPM (E)
Disponibilités des formations certifiantes WALLIX	WALLIX Bastion	WALLIX Trustelem	WALLIX BestSafe
Formation à la certification WALLIX Certified Administrator - WCA	●		
Formation à la certification WALLIX Certified Professional - WCP	●	●	●
Formation à la certification WALLIX Certified Expert - WCE	●		

Nos formations sont disponibles en différents formats :

- **En présentiel** : inter or intra-entreprise, avec un maximum de 6 stagiaires.
- **A distance** : L'utilisation de Microsoft Teams est nécessaire. Veuillez vérifier les prérequis techniques demandés pour chaque formation technique.

Retrouvez les dates de formation sur

<https://www.wallix.com/fr/wallix-academy/>

Inscrivez-vous à une formation en envoyant un email* à :

academy@wallix.com

*Avec vos coordonnées complètes et les dates de formation choisies.

WALLIX est organisme de formation enregistré sous le numéro 11 75 51538 75. Cet enregistrement ne vaut pas agrément de l'Etat.

Privileged Access Management



PAM

WALLIX
CYBERSECURITY SIMPLIFIED

CERTIFIED

BASTION
2020

WALLIX Bastion

- WALLIX CERTIFIED ADMINISTRATOR / **WCA-P**
- WALLIX CERTIFIED PROFESSIONAL / **WCP-P**
- WALLIX CERTIFIED EXPERT / **WCE-P**

WALLIX CERTIFIED ADMINISTRATOR / **WCA-P** **PAM - BASTION**

Cette formation s'adresse aux ingénieurs et techniciens des utilisateurs finaux WALLIX et des partenaires revendeurs qui souhaitent comprendre notre solution WALLIX Bastion et être en mesure de la gérer au quotidien.

PRÉREQUIS :

Le stagiaire doit être familiarisé avec **SSH, RDP, les concepts de proxy et les environnements Linux**. Les **compétences en systèmes, réseaux et infrastructures** permettront au stagiaire d'acquérir plus rapidement le WALLIX Bastion. Cette formation se concentre sur les tâches d'administration de la solution Bastion et ne traite pas de son installation et de son déploiement.

DESCRIPTION :

Cette formation technique d'une journée vous permet de comprendre la solution WALLIX Bastion et d'être en mesure de la gérer au quotidien. Il fournit les moyens nécessaires pour comprendre les concepts et fonctionnalités de base pour sa maintenance et son administration de base. Il repose sur une participation active du stagiaire qui aura la possibilité d'interagir avec notre formateur au cours de la session de formation. À la fin de la formation, le stagiaire devra passer un test QCM. **Un score de 70% est requis pour obtenir la certification WALLIX Certified Administrator - Bastion (WCA-P).**

Contenu de la formation :

I. GÉNÉRALITÉS	V. CONFIGURATION ÉTENDUE
• Les solutions WALLIX	• Politiques de connexion
• Présentation du PAM	• Configuration options
II. LA SOLUTION WALLIX BASTION	- Désactivation de session probe
• Architecture WALLIX en général (Gestionnaire d'accès WALLIX, Bastions, HA)	- Activation des scénarios SSH
• Intégration possible (SNMP, SIEM)	• Transformation du coffre-fort
• Cas d'utilisation simple avec tous les composants / questions	• Intégration d'applications
III. WALLIX BASTION SESSION MANAGEMENT CONFIGURATION DE BASE	VI. MAINTENANCE ET SUPPORT
• Menus d'administration	• Fichiers logs (wabsysinfo), détails des logs
• Menus des auditeurs et des approbateurs	• Services - Utilisateurs administrateurs / connexions
• Configuration de base (ajout / suppression de ressources / utilisateurs) provisionning GUI	• Gestion des mises à jour / mises à niveau
• Configuration de base (ajout / suppression de ressources / utilisateurs) CSV / API	- Trouvez et parcourez les release notes (compatibilités et chemin de migration, procédure de mise à jour)
IV. WALLIX BASTION PASSWORD GESTION & CONFIGURATION DE BASE	- Présentation des logiques de release (LTS, intermédiaire, correctifs)
• Configuration de la gestion des MDP	VII. DÉPANNAGE
• Procédure Breaking glass	• Exemples
	• Ressources WALLIX (portail de support, base de connaissances, documentation et téléchargement)

WALLIX CERTIFIED PROFESSIONAL / **WCP-P**

PAM - BASTION

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 - Bastion (WCP-P).**

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

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 CERTIFIED PROFESSIONAL / **WCP-P**

PAM - BASTION

• 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 Profils utilisateurs	• Installation du serveur 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 WALLIX 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	

WALLIX CERTIFIED EXPERT / WCE-P PAM - BASTION

Cette formation est destinée aux ingénieurs des partenaires revendeurs WALLIX et aux utilisateurs finaux qui souhaitent réaliser des déploiements avancés de la solution WALLIX Bastion.

PRÉ-REQUIS / COMPÉTENCES :

Le stagiaire doit être certifié **WALLIX Certified Professional - Bastion (WCP-P)**. 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 - Bastion (WCE-P)**.

Contenu de la formation :

I. Authentifications Avancées	• Sécuriser l'identifiant/mot de passe utilisés par l'application Autolt
• 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 Autolt	• Les paramètres globaux du proxy VNC
• Télécharger et installer l'application Autolt	IV. Password Manager Avancés
• Écrire un script Autolt *.au3	• Rappel : WALLIX Password Manager
• Compiler un script pour générer une application Autolt *.exe	• WAAPM : WALLIX Application to Application Password Manager
• Télécharger l'application Autolt sur le serveur tolt *.exe	• Le Bastion comme Vault Externe (à partir de V6.1)
• Ajouter une application Autolt sur le Bastion	

WALLIX CERTIFIED EXPERT / **WCE-P**

PAM - BASTION

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

Formations à distance PAM - BASTION : Prérequis techniques

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.

Nos formations sont accessibles aux personnes en situation de handicap. Pour plus d'informations ou cas de besoin d'un aménagement particulier de la formation, merci de contacter notre référent handicap à l'adresse suivante : academy@wallix.com

IDaaS



IDaaS

WALLIX
CYBERSECURITY SIMPLIFIED

CERTIFIED

TRUSTELEM
2020

WALLIX Trustelem

• WALLIX CERTIFIED PROFESSIONAL / **WCP-I**

WALLIX CERTIFIED PROFESSIONAL / WCP-I IDaaS - TRUSTELEM

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

PRÉREQUIS :

Le stagiaire doit être familiarisé avec les objets **Active Directory** et les environnements **Microsoft**. Des compétences **systèmes, réseaux et infrastructures** permettront au stagiaire de s'approprier plus vite WALLIX Trustelem.

DESCRIPTION :

Cette formation technique d'une journée vous permet de découvrir et administrer notre solution WALLIX Trustelem. Elle permet de comprendre les concepts et fonctionnalités nécessaires au déploiement dans une architecture classique. Alternant théorie et pratique, elle est basée sur la participation active du stagiaire qui devra configurer et administrer la solution à travers notre 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 Trustelem Certified Professional (WCP-I) certification.**

Contenu de la formation :

I. ENTREPRISE ET PRODUIT	VI. GESTION DES ACCÈS À WALLIX TRUSTELEM
• WALLIX et ses Produits	• L'interface de Gestion des Accès
• Trustelem	• Définition des Règles d'Accès
II. LA SOLUTION WALLIX TRUSTELEM	VII. EXPÉRIENCE UTILISATEUR SUR WALLIX TRUSTELEM
• Gestion de l'Identité et des Accès	• Authentification intégrée à Windows
• Accès Utilisateurs	• Authentification à l'aide de Certificats
III. PRÉSENTATION DE L'INTERFACE D'ADMINISTRATION WALLIX TRUSTELEM	• Réinitialisation du Mot de Passe Active Directory par l'Utilisateur
• Trois Principales Etapes	VIII. SUIVI DE LA SOUSCRIPTION WALLIX TRUSTELEM
• Présentation des Différents Onglets	• Logs
IV. GESTION DES UTILISATEURS DE WALLIX TRUSTELEM	• Alertes
• Utilisateurs créés dans WALLIX Trustelem	• Sessions
• Utilisateurs issus d'Azure AD	• Tableaux de bord
• Utilisateurs issus de GSuite	IX. INTRODUCTION RAPIDE AUX APIS
• Utilisateurs issus d'Active Directory	• Présentation des Principales Fonctionnalités
V. GESTION DES APPLICATIONS DE WALLIX TRUSTELEM	X. PLANIFIER UN PROJET SSO
• Modèles Génériques	• Présentation des principales étapes à suivre
• Applications Pré-intégrées	

Nos formations sont accessibles aux personnes en situation de handicap. Pour plus d'informations ou cas de besoin d'un aménagement particulier de la formation, merci de contacter notre référent handicap à l'adresse suivante : academy@wallix.com

Endpoint Privilege Management



WALLIX Bestsafe

- WALLIX CERTIFIED PROFESSIONAL / **WCP-E**

WALLIX CERTIFIED PROFESSIONAL / WCP-E EPM - BESTSAFE

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

PRÉREQUIS :

Le stagiaire doit être familiarisé avec les objets **Active Directory**, les outils **MMC** et les environnements **Microsoft**. Des **compétences systèmes, réseaux et infrastructures** permettront au stagiaire de s'approprier plus vite **WALLIX BestSafe**.

DESCRIPTION :

Cette formation technique de 2 jours vous permet de découvrir et administrer notre solution **WALLIX BestSafe**. Elle permet de comprendre les concepts et fonctionnalités nécessaires au déploiement dans une architecture classique. Alternant théorie et pratique, elle est basée sur la participation active du stagiaire qui devra configurer et administrer la solution à travers notre 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 BestSafe CERTIFIED PROFESSIONAL (WCP-E).**

Contenu de la formation :

I. ENTREPRISE ET PRODUIT	• Flags de Règles
• WALLIX et ses Produits	• Héritage des règles
• Comment BestSafe peut vous aider à réduire votre surface d'attaque	V. CONFIGURATION AVANCÉE DE WALLIX BESTSAFE
• Rappels sur les principaux concepts Active Directory	• Onglet Général
• Rappels sur le contexte de sécurité d'un processus	• Sécurité des Postes Utilisateurs
II. LA SOLUTION WALLIX BESTSAFE	• Actions d'Urgence
• POLP (Principle of Least Privilege)	• Statistiques
• Architecture de WALLIX BestSafe	• Règles Interdites
• Architecture réseau de WALLIX BestSafe	• Administrateurs de Règles
III. INSTALLATION DE WALLIX BESTSAFE	VI. MAINTENANCE & SUPPORT
• Prérequis et modifications de l'AD	• Analyse des Logs BestSafe
• Installation/ Réinstallation/ Mise à jour de la Console d'Administration	• Vérification des Règles
• Installation/ Réinstallation/ Mise à jour du Client	VII. CONFIGURATION DES RÈGLES DE RANSOMWARE ET DES RÈGLES DE SÉCURITÉ
• Activation de la licence	• Gestion des membres des Groupes Locaux à Privilège – Règles de Sécurité
IV. CONFIGURATION DES RÈGLES DE PRIVILÈGE DE WALLIX BESTSAFE	• Activation des Règles de Sécurité
• Gérer le contexte de sécurité d'un process Windows – Les règles de privilège	• Gestion des Règles de Sécurité
• Règles de Privilège - Restricted / Blocked / Administrator / Lignes de commande / Filtrer par Groupes / Juste à temps – Validité des règles / Filtrage des règles par OS	• Règles de Ransomware
• Gestion des Privilèges / Processus Parents	• Gestion des Mots de Passe des Comptes Locaux

Nos formations sont accessibles aux personnes en situation de handicap. Pour plus d'informations ou cas de besoin d'un aménagement particulier de la formation, merci de contacter notre référent handicap à l'adresse suivante : academy@wallix.com

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

