wallix academy

WALLIX ACADEMY
FORMATIONS CERTIFIANTES

Qualiopi
processus certifié

La certification qualité a été délivrée
au titre de la catégorie d'action suivante :
ACTIONS DE FORMATION

A propos de WALLIX

Éditeur de logiciels de solutions de cybersécurité, le groupe WALLIX est un spécialiste européen de la gouvernance des comptes à privilèges. En réponse aux récentes évolutions réglementaires (NIS/GDPR en Europe et OVI en France) et aux menaces de cybersécurité qui touchent aujourd'hui toutes les entreprises, nos solutions aident les utilisateurs à protéger leurs actifs informatiques critiques : données, serveurs, terminaux et objets connectés.

Qualiopi
processus certifié

La certification qualité a été délivrée au titre de la catégorie d'action suivante :
ACTIONS DE FORMATION

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**

SECURE
YOUR DIGITAL
FUTURE

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.

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.

Une offre de e-learning est en développement.

	PAM (P)	MFA (A)	EPM (E)	IDaaS (I)	PAM-OT (OT)
Disponibilités des formations certifiantes WALLIX	**WALLIX Bastion AM**	**WALLIX Authentificator**	**WALLIX BestSafe**	**WALLIX Trustelem**	**WALLIX PAM4OT**
Certification training **WALLIX Certified Administrator - WCA**	●				
Certification training **WALLIX Certified Professional - WCP**	●		●		
Certification training en ligne **WALLIX Certified Professional - e-WCP**	●	●		●	●
Certification training **WALLIX Certified Expert - WCE**	●				
WALLIX PAM4ALL	●	●	●		

Nos formations sont disponibles en différents formats :

- **En présentiel dans vos locaux** : 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/services-et-support/academie-wallix/
Inscrivez-vous à une formation en envoyant un email* à :
academy@wallix.com

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

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

wallix

Privileged Access Management

wallix CERTIFIED PAM

WALLIX PAM

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

SECURE
YOUR DIGITAL
FUTURE

WALLIX CERTIFIED ADMINISTRATOR / **WCA-P**

WALLIX PAM

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.

PREREQUIS :

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.

Une maîtrise de l'anglais technique est nécessaire.

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. Elle fournit les moyens nécessaires pour comprendre les concepts et fonctionnalités de base pour sa maintenance et son administration de base. Elle repose sur une participation active du stagiaire qui aura la possibilité d'interagir avec notre formateur au cours de la session de formation.

La formation est dispensée en français. Les contenus des supports de formation sont en anglais.

EVALUATION :

Le formateur évalue la progression pédagogique du stagiaire tout au long de la formation au moyen de questions à l'oral, de QCM, et de travaux pratiques. Au démarrage de la formation, le stagiaire complète un pré-test.
A la fin de la formation, le stagiaire devra passer un examen sous la forme d'un QCM.

Un score de 70% est requis pour obtenir la certification WALLIX Certified Administrator PAM-Bastion (WCA-P).

wallix

SECURE
YOUR DIGITAL
FUTURE

CONTENU DE LA FORMATION

I. INTRODUCTION

WALLIX & Portfolio Présentation
Introduction au PAM

II. WALLIX BASTION SESSION MANAGER

Architecture WALLIX en général (Bastion, Access Manager)
Concepts globaux
Profils et rôles
Gestion des cibles
Gestion des comptes secondaires
Gestion des autorisations
Gestion de la Checkout policy
Gestion des applications
Session probe

III. WALLIX BASTION PASSWORD MANAGER

Configuration de la Checkout policy
Configuration de politique de changement de mot de passe
Autres méthodes de changement de mot de passe
Mécanisme de Bris de glace

IV. APPROBATION & AUDIT

Approbations
Audit

V. CONFIGURATION ÉTENDUE

SIEM/SNMP
CSV
Authentification externe
Access Manager
Audit depuis l'Access Manager

VI. MAINTENANCE

Services logins des administrateurs/utilisateurs
Commandes CLI
Gestion des Updates/Upgrades
Installer/Désinstaller un hotfix

VII. SUPPORT & DÉPANNAGE

Produit et licence
Ressources WALLIX
Fichiers de logs
Support Customer Success : ouvrir un ticket

wallix

SECURE
YOUR DIGITAL
FUTURE

WALLIX CERTIFIED PROFESSIONAL / **WCP-P**

WALLIX PAM

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

PREREQUIS :

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 la maîtrise de l'installation, configuration et déploiement de la solution Bastion.

Une maîtrise de l'anglais technique est nécessaire.

DESCRIPTION :

Cette formation technique de 3 jours permet de découvrir et de prendre en main la solution WALLIX Bastion. Elle offre les moyens nécessaires d'appréhender les concepts et 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.

La formation est dispensée en français. Les contenus des supports de formation sont en anglais.

EVALUATION :

Le formateur évalue la progression pédagogique du stagiaire tout au long de la formation au moyen de questions à l'oral, de QCM, et de travaux pratiques. Au démarrage de la formation, le stagiaire complète un pré-test.
A la fin de la formation, le stagiaire devra passer un examen sous la forme d'un QCM.

Un score de 70% est requis pour obtenir la certification WALLIX Certified Professional PAM-BASTION (WCP-P).

wallix

SECURE
YOUR DIGITAL
FUTURE

CONTENU DE LA FORMATION

I. FORMATION ET CERTIFICATION

Objectifs de la formation
Agenda indicatif
Présentation de la plateforme Academy
Examen de certification

II. ENTREPRISE ET PRODUITS

L'entreprise WALLIX
Les solutions de WALLIX

III. INSTALLATION ET GESTION DU BASTION

Installation du WALLIX Bastion appliance
Le Bastion dans l'infrastructure
Configuration initiale
Première connexion
Changement du mot de passe admin
Installation de la licence
Configuration du réseau
Configuration de la time zone du serveur NTP
Ajout d'un administrateur du Bastion
Back up de la configuration
Restauration de la configuration
Back up de la version du Bastion
Mise à jour de la version du Bastion
Retour à la version précédente du Bastion
Installer/désinstaller un hotfix
Monitoring et logs
Configurer un serveur mail et active les notifications
Composants principaux et services du Bastion
- Lab 1 : Installing and handling the WALLIX Bastion

IV. WALLIX SESSION MANAGER

Concepts globaux
Gérer les utilisations primaires (authentification locale)
Gérer les groupes d'utilisateurs primaires
Gérer les cibles
Gérer les comptes secondaires de cibles (compte de domaine local)
Ajouter un groupe de cibles
Ajouter une autorisation
Se connecter à un serveur en utilisant le protocole RDP
Se connecter à un serveur en utilisant le protocole SSH
Changer le message d'avertissement
- Lab 2.1 : RDP and SSH connections

Gérer les applications

wallix

AppDriver
- o Lab 2.2 : Application

Gérer un startup scenario SSH
- o Lab 2.3 : SSH startup scenario

Gérer les utilisateurs primaires avec une authentification externe
- o Lab 2.4 : External authentication

Gérer les comptes secondaires : compte de domaine global
- o Lab 2.5 Global domain account

Import/export
Discovery
- o Lab 2.6 : Discovery

Politique de connexion RDP et Session Probe
- o Lab 2.7 : Session Probe

V. WALLIX PASSWORD MANAGER

Concepts globaux
Gérer la Checkout policy
Ajouter un compte pour password management
Activer le password checkout dans l'autorisation
Password Checkout – côté utilisateur
- o Lab 3.1 : Password checkout

Ajouter une politique de changement de mot de passe
Plugins de changement de mots de passe
Gérer la politique de changement de mot de passe
Activer le changement de mot de passe pour un compte secondaire
Changement de mot de passe au check-in
Changement de mot de passe- vue administrateur
Mécanisme de bris de glace
Politique de mot de passe local
- o Lab 3.2 : Password change

VI. APPROBATIONS ET AUDIT

Profil approbateur et process d'approbation pour le session manager
Profil approbateur et process d'approbation pour le password manager
- o Lab 4.1 : Approval workflow

Audit de session
Session en cours
Historique de session
Historique d'un compte
Historique d'approbation
Historique d'authentification
Statistiques de connexion
Audit du password manager
Paramètres des enregistrement de sessions
Gestion des enregistrements de sessions
Commandes CLI
Politique de rétention
- o Lab 4.2 : Session audit

VII. WALLIX ACCESS MANAGER

Concepts globaux
Installer l'Access Manager en appliance
Configuration par défaut
Gestion des organisations
Gérer les Bastions sur l'Access Manager
Gérer les utilisateurs primaires locaux
Gérer les utilisateurs primaires avec une authentification externe (LDAP)
Ajouter une domaine Bastion
Politique de mot de passe des organisations
Personnaliser le template des organisations
Connexion aux organisations
Connexion à un serveur en utilisant le protocole RDP
Connexion à une application
Connexion à un serveur en utilisant le protocole SSH
Accéder au mot de passe d'un compte
Audit de sessions depuis l'Access Manager
Gérer les paramètres de l'Access Manager
Mettre à jour l'Access Manager

- Lab 5 : Configuring the Access Manager

VIII. HAUTE DISPONIBILITE WALLIX

Concepts globaux
La solution WALLIX Bastion HA
WALLIX Bastion HA (WABHA)
La réplication WALLIX Bastion HA

- Lab 6 : Replication

IX. CENTRE DE SUPPORT CLIENT WALLIX

Avant d'ouvrir un ticket
Ouvrir un ticket

SECURE
YOUR DIGITAL
FUTURE

WALLIX CERTIFIED e-PROFESSIONAL / **eWCP-P**

WALLIX PAM

Cette formation à distance s'adresse aux ingénieurs et techniciens des utilisateurs finaux WALLIX et des partenaires revendeurs de WALLIX qui souhaitent maîtriser la configuration, le déploiement et l'administration de la solution WALLIX.

PREREQUIS :

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 la maîtrise de l'installation, configuration et déploiement de la solution Bastion.

Une maîtrise de l'anglais technique est nécessaire.

Pour bénéficier de cette 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 **5 machines virtuelles préconfigurées** : contrôleur de domaine (Windows 2016), serveur Windows 2016, serveur Linux, WALLIX Bastion et Access Manager.

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

SECURE
YOUR DIGITAL
FUTURE

WALLIX CERTIFIED e-PROFESSIONAL / **eWCP-P**

WALLIX PAM

DESCRIPTION :

Cette formation technique en ligne d'une durée estimée 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.

La formation est dispensée en français. Les contenus des supports de formation sont en anglais.

EVALUATION :

Au démarrage de la formation, le stagiaire complète un pré-test.
Des tests en ligne sont effectués à la fin de chaque chapitre.
A la fin de la formation, le stagiaire devra passer un examen sous la forme d'un QCM

Un score de 70% est requis pour obtenir la certification WALLIX Certified e-Professional PAM BASTION (eWCP-P).

wallix

SECURE
YOUR DIGITAL
FUTURE

CONTENU DE LA FORMATION

0. LABS ENVIRONMENTS

Lab 0: Platform Presentation

- o Lab 0 : Virtual Box Configuration

I. PRODUCT

Wallix Bastion&Access Manager

II. INSTALLING AND HANDING WALLIX BASTION

01 Prerequisites
02 Initial Configuration Command Lines
03 Initial Configuration WEB
04 Backup And Restoration
05 Updating Bastion
06 Monitoring Logs And System Administration
07 Main Components

- o Lab 1 : Installing and handling the WALLIX Bastion

III. WALLIX SESSION MANAGER

00 Global concepts Custom Profiles
01 Manage user primary account
02 Manage devices
03 Manage authorizations

- o Lab 2.1: RDP and SSH connections

04 Manage applications

- o Lab 2.2: Applications

05 Manage SSH Startup Scenario

- o Lab 2.3: Startup scenario

06 Manage Primary User With External Authentication

- o Lab 2.4: External authentication

07 Manage Secondary Account Global Domain

- o Lab 2.5: Global Domain Account

08 Import Export
09 Session Probe

- o Lab 2.6: Discovery
- o Lab 2.7: Session Probe

IV. WALLIX PASSWORD MANAGER

01 Password visualization

- o Lab 3.1: Password checkout

02 Password change

- o Lab 3.2: Password change

03 BreakGlass Scenario And Local Password Policy

wallix

SECURE
YOUR DIGITAL
FUTURE

wallix

SECURE
YOUR DIGITAL
FUTURE

WALLIX CERTIFIED EXPERT / **WCE-P**

WALLIX PAM

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.

PREREQUIS :

Le stagiaire **doit être certifié WCP-P ou e-WCP** (WALLIX CERTIFIED PROFESSIONAL PAM BASTION/WALLIX CERTIFIED e-PROFESSIONAL PAM BASTION).
Il doit également **être familiarisé avec les lignes de commande GNU/Linux**.

Des connaissances en scripting faciliteront le suivi de cette formation.

Cette formation se concentre sur la maîtrise de l'installation, configuration et déploiement de la solution Bastion.

Une maîtrise de l'anglais technique est nécessaire.

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.

La formation est dispensée en français. Les contenus des supports de formation sont en anglais.

EVALUATION :

Le formateur évalue la progression pédagogique du stagiaire tout au long de la formation au moyen de questions à l'oral, de QCM, et de travaux pratiques. Au démarrage de la formation, le stagiaire complète un pré-test.
A la fin de la formation, le stagiaire devra passer un examen sous la forme d'un QCM.

Un score de 70% est requis pour obtenir la certification WALLIX Certified Expert PAM - BASTION (WCE-P).

wallix

SECURE
YOUR DIGITAL
FUTURE

CONTENU DE LA FORMATION

I. AUTHENTIFICATION AVANCEE

Méthodes d'authentification avancée sur le Bastion
Authentification explicite Bastion :

- LDAP/AD
- PINGID
- Radius
- Kerberos

Authentification transparente Bastion :

- certificat X509
- Kerberos

Authentification 2 facteurs Bastion (2FA)
Méthodes d'authentification de l'Access Manager
Authentification explicite Access Manager LDAP
Authentification transparente Access Manager - X509
Authentification explicite Access Manager - SAML
(Security assertion markup language)

- o Lab 1: Check configuration of the WALLIX Bastion
- o Lab 2.0: Advanced Authentications
  X509 Authentication
- o Lab 2.1: Advanced Authentications
  Transparent authentication Kerberos

II. APPLICATIONS AVANCEES

Rappels : Applications dans WALLIX session manager
Clusters
AppDriver
Languade de scripting AutoIt
Télécharger et installer l'application AutoIt
Ecrire un script AutoIt *.au3
Compiler le script et générer l'application AutoIt *.exe
Uploader l'application AutoIt application sur le serveur
Ajouter une application AutoIt sur le Bastion
Sécuriser les credentials utilisés par les applications Autoit

- o Lab 3: Advanced Applications

III. PARAMETRES DES PROXIES

Concepts Globaux
Politique de connexion RDP
Paramètres globaux du Proxy RDP
Paramètres globaux du Proxy RDP sesman
Changer le certificat autosigné du proxy RDP
Politique de connexion SSH
Paramètres globaux du Proxy SSH
Politique de connexion TELNET

wallix

III. PARAMETRES DES PROXIES (SUITE)

Politique de connexion VNC
Paramètres globaux du Proxy VNC
- Lab 4: Proxy Parameters

IV. PASSWORD MANAGER AVANCE

Rappel : WALLIX Password Manager
WAAPM : WALLIX Application to Application Password Manager
Bastion en tant que Vault externe
- Lab 5: Advanced Password Manager

V. API REST WALLIX BASTION

Concept global
API REST WALLIX Bastion
API REST authentication sur le Bastion
Logout de l'API REST du Bastion
Les méthodes de l'API REST du Bastion
Les codes de réponse de l'API REST du Bastion
Parcourir les ressources de l'API REST du Bastion
Ajouter une ressource avec l'API REST du Bastion
Modifier une ressource avec l'API REST du Bastion
Supprimer une ressource avec l'API REST du Bastion
- Lab 6: API REST WALLIX Bastion

Authentification Multi-Facteurs pour PAM

wallix
CERTIFIED
MFA

WALLIX MFA pour PAM

- WALLIX CERTIFIED e-PROFESSIONAL / **eWCP-A**

SECURE
YOUR DIGITAL
FUTURE

WALLIX CERTIFIED e-PROFESSIONAL / **eWCP-A**

WALLIX MFA

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 Authenticator.

PREREQUIS :

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

Une maîtrise de l'anglais technique est nécessaire.

Pour bénéficier de cette 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, tenant Trustelem MFA, WALLIX Bastion et Access Manager.

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

SECURE
YOUR DIGITAL
FUTURE

WALLIX CERTIFIED e-PROFESSIONAL / **eWCP-A**

WALLIX MFA

DESCRIPTION :

Cette formation technique d'une durée estimée d'une journée vous permet de découvrir et administrer notre solution WALLIX Authenticator. Elle permet de comprendre les concepts et fonctionnalités nécessaires au déploiement dans une architecture classique.

Alternant théorie et pratique, elle est basée sur des vidéos de démonstration permettant au stagiaire de configurer et administrer la solution à travers notre plateforme de LAB pour devenir complètement autonome.

Le contenu de la formation est en anglais, sous-titré anglais.

EVALUATION :

Au démarrage de la formation, le stagiaire complète un pré-test.
Des tests en ligne sont effectués à la fin de chaque chapitre.
A la fin de la formation, le stagiaire devra passer un un examen sous la forme d'un QCM.

Un score de 70% est requis pour obtenir la certification WALLIX Certified e-Professional AUTHENTICATOR (eWCP-A).

wallix

SECURE
YOUR DIGITAL
FUTURE

CONTENU DE LA FORMATION

I. INTRODUCTION

Introduce WALLIX & Products
WALLIX Authenticator

II. TRUSTELEM ADMINISTRATION INTERFACE PRESENTATION

Presentation of the different tabs

III. USERS MANAGEMENT

Users created in WALLIX Authenticator
Users from Active Directory
Manage Users
Manage Groups
Best practices
- o Lab 1: Synchronize an Active Directory with Trustelem

IV. APPLICATIONS MANAGEMENT

SAML-> Access Manager
LDAP/Radius Access Manager and Bastion

V. ACCESS MANAGEMENT

Access management interface
Access rules
Enrolment through campaigns
Manage Groups
Manual enrolment

VI. BASTION AND ACCESS MANAGER

Usual authentications
MFA for Active Directory users
- o Lab 2: Radius MFA for AD users on the Bastion

MFA for a local Bastion user
- o Lab 3: Radius MFA for a local Bastion user

MFA for Access Manager with account mapping
- o Lab 4: Radius MFA for AD users on the Access Manager

MFA for Access Manager without account mapping
- o Lab 5: SAML MFA for AD users on the Access Manager
- SAML MFA for external users on the Access Manager

SAML Bastion

wallix

VII. FOLLOW-UP OPERATIONS

Logs
Alerts
Sessions
Dashboard

VIII. ADVANCED FEATURES

Integrated Windows authentication
Authentication with certificates
Self service password reset
API

Endpoint Privilege Management

wallix
CERTIFIED
EPM

WALLIX EPM

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

SECURE
YOUR DIGITAL
FUTURE

WALLIX CERTIFIED PROFESSIONAL / **WCP-E**

WALLIX EPM

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.

PREREQUIS :

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

Une maîtrise de l'anglais technique est nécessaire.

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.

Les contenus des supports de formation sont en anglais.

EVALUATION :

Le formateur évalue la progression pédagogique du stagiaire tout au long de la formation au moyen de questions à l'oral, de QCM, et de travaux pratiques. Au démarrage de la formation, le stagiaire complète un pré-test.
A la fin de la formation, le stagiaire devra passer un examen sous la forme d'un QCM.

Un score de 70% est requis pour obtenir la certification WALLIX Certified Professional EPM BestSafe (WCP-E).

wallix

SECURE
YOUR DIGITAL
FUTURE

CONTENU DE LA FORMATION

0. INTRODUCTION

Présentation WALLIX

I. GENERALITES

Introduction à BestSafe – Généralités
Sécurité de l'OS Windows
Concepts généraux d'Active Directory
Contexte de sécurité d'un process
Architecture BestSafe
Pré-requis réseaux BestSafe

II. INSTALLATION DE BESTSAFE

Configuration Active Directory
Installation de la console admin BestSafe (MMC)
- o Lab 1: Prepare AD for BestSafe – Auto Step by Step Wizard

Activation de la licence BestSafe
Installation de la console admin BestSafe (MMC)
- o Lab 2: BestSafe MMC admin console setup
- o Lab 2.1: BestSafe License Activation – Online
- o Lab 2.2: Windows BestSafe agent setup

III. REGLES DE PRIVILEGES

Types de règles
- o Lab 3: Privilege Rules Types

Lignes de commandes
Filtrage par utilisateur/groupe
- o Lab 4: Privilege Rules - Command Line
- o Lab 4.1: Command Line / Groups
- o Lab 4.2: General Properties – Rule Validity
- o Lab 4.3: Privileges
- o Lab 4.4: Privileges Rules - Exceptions
- o Lab 4.5: Hashes

Propriétés
- o Lab 5: Privilege Rules – Parent Processes

Héritage/Précédence
- o Lab 6: Privileges Rules - Flags
- o Lab 6.1: Inheritance & Precedence
- o Lab 6.2: Block Inheritance

IV. PARAMETRAGES GLOBAUX

Onglet DC
Onglet Configuration
- o Lab 7: Global settings

Règles de type Interdites
- o Lab 8: Forbidden Tab

wallix

IV. PARAMETRAGES GLOBAUX (SUITE)

Actions d'urgence

- o Lab 9: Emergency Tab

RBAC – Profiles utilisateurs

- o Lab 10: RBAC

V. REGLES DE MONITORING

Objectif

Niveau

Champs

- o Lab 11: Monitoring rules

VI. RANSOMWARE

Règles de Ransonware

Fonctionnalité de l'API Hooking de WALLIX BestSafe

Gestion des règles de ransomware

Lignes de commande

Groupes/Utilisateurs

Flags

Propriétés

- o Lab 12: Ransomware
- o Lab 12.1: Verify BestSafe Rules

IV. REGLES DE SECURITE

Règles de sécurités

Activer les règles de sécurité

Gestion des règles de sécurité

Menu contextuel

- o Lab 13: Security Rules

V. GESTION D'EQUIPEMENT

Fichier d'auto-login

Fichier d'élévation

- o Lab 14: Monitoring rules

Gestion de mot de passe

- o Lab 15: Local Password Management

Protection de répertoires

Remote Computer Control

VI. LOGS

Logs

Structure

Entête des champs

Partie variable

Exemples de logs

IDaaS

WALLIX IDaaS

• WALLIX CERTIFIED e-PROFESSIONAL / **eWCP-I**

SECURE
YOUR DIGITAL
FUTURE

WALLIX CERTIFIED e-PROFESSIONAL / **eWCP-I**

WALLIX IDaaS

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.

PREREQUIS :

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

Une maîtrise de l'anglais technique est nécessaire.

Pour bénéficier de cette 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, tenant IDaaS, WALLIX Bastion et Access Manager.

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

SECURE
YOUR DIGITAL
FUTURE

WALLIX CERTIFIED e-PROFESSIONAL / **eWCP-I**

WALLIX IDaaS

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.

Les contenus des supports de formation sont en anglais.

EVALUATION :

Au démarrage de la formation, le stagiaire complète un pré-test.
Des tests en ligne sont à la fin de chaque chapitre.
A la fin de la formation, le stagiaire devra passer un examen sous la forme d'un QCM.

Un score de 70% est requis pour obtenir la certification WALLIX Certified e-Professional IDaaS TRUSTELEM (eWCP-I).

wallix

SECURE
YOUR DIGITAL
FUTURE

CONTENU DE LA FORMATION

I. INTRODUCTION

- Introduce WALLIX & Products
- WALLIX Trustelem

II. TRAINING AND CERTIFICATION COURSES

- o Lab 0: SAML

III. TRUSTELEM ADMINISTRATION INTERFACE PRESENTATION

- Presentation of the different tabs

IV. USERS MANAGEMENT

- Add users
- Users from Azure Active Directory
- Users from GSuite
- Users from Active Directory
- Manage Users
- Manage Groups
- Best practices
  - o Lab 1: User Management

V. APPLICATIONS MANAGEMENT

- SAML or OpenID Connect
- Generic models
- Pre-integrated applications
- LDAP/Radius Access Manager and Bastion
  - o Lab 2.1: SAML
  - o Lab 2.2: LDAP AND RADIUS

VI. ACCESS MANAGEMENT

- Access management interface
- Access rules

VII. ADVANCED USER EXPERIENCE

- Integrated Windows Authentication
- Authentication with certificates
- Self-service password reset
  - o Lab 3: Advanced User Experience

VIII. FOLLOW-UP OPERATIONS

- Logs
- Alerts
- Sessions
- Dashboard
  - o Lab 4: Follow-up operations

wallix

SECURE
YOUR DIGITAL
FUTURE

IX. QUICK INTRODUCTION TO APIs
Main features presentation

X. DELEGATED ADMIN
Delegated Admin

XI. PROJECT PLANNING
Main steps to follow

wallix

PAM4ALL

WALLIX PAM4OT

• WALLIX CERTIFIED e-PROFESSIONAL / **eWCP-P-OT**

SECURE
YOUR DIGITAL
FUTURE

WALLIX CERTIFIED e-PROFESSIONAL / **eWCP-P-OT**

WALLIX PAM4OT

Cette formation est destinée aux ingénieurs et techniciens des clients finaux, travaillant dans le secteur de l'OT, et partenaires revendeurs de WALLIX, souhaitant vendre la solution PAM4OT.

PREREQUIS :

Le stagiaire **doit être au préalable certifié WCP-P ou e-WCP-P.** Des compétences **en systèmes, réseaux et infrastructures** permettront au stagiaire de s'approprier plus vite WALLIX PAM4OT.

Ce programme est conçu pour tous les professionnels ayant un profil technique et souhaitant être plus efficace et à l'aise dans la gestion de la solution de cybersécurité WALLIX PAM4OT.

Une maîtrise de l'anglais technique est nécessaire.

DESCRIPTION :

Cette formation technique en ligne d'une durée estimée d'une demi-journée vous permet de découvrir et de prendre le contrôle de la solution WALLIX PAM4OT.

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.

Les contenus des supports de formation sont en anglais.

EVALUATION :

Au démarrage de la formation, le stagiaire complète un pré-test.
Des tests en ligne sont effectués à la fin de chaque chapitre.
A la fin de la formation, le stagiaire devra passer un examen sous la forme d'un QCM.

Un score de 70% est requis pour obtenir la certification WALLIX Certified e-Professional PAM4OT (eWCP-P-OT).

wallix

SECURE
YOUR DIGITAL
FUTURE

CONTENU DE LA FORMATION

Introduction to the eWCP-P-OT Course Program

I. MODULE 1 E-WCP-P-OT PREREQUISITES

The e-WCP-P-OT Prerequisites

II. MODULE 2 DIGITAL ACCESS IN OT

Part 01 Discover the OT Universe:

1.1 What is OT?

1.2 Main Components, Equipment and Protocols

1.3 OT Context Understanding

Part 02 The Security Stakes of Identity & Access

III. MODULE 3 OT ISSUES AND SOLUTIONS

Introduction: Typical Users and Digital Access Issues

Part 01 How to manage Third-Party Access

Part 02 How to manage Industrial Protocols

Part 03 How to provide Secure Access while preserving Service Continuity

Part 04 How to secure File Transfer?

Part 05 How to allow a Secured Access to Critical Assets?

Part 06 How to trace and Audit for Incident Resolution and Regulatory Compliance

V. MODULE 4 PAM4OT ARCHITECTURES

Centralized Architecture

Decentralized Architecture

Hybrid Architecture

wallix

WWW.WALLIX.COM

wallix