



Une formation
Alphorm.com

Formation WALLIX BASTION *Le Guide du Débutant*



Mohamed Anass EDDIK



Une formation
Alphorm.com

Plan de la formation

Introduction

1. Introduction Wallix Bastion
2. Gérer les sessions
3. Gérer les sessions d'audit
4. S'authentifier avec un certificat X509
5. Configurer les options avancées

Conclusion



Public concerné

Les ingénieurs et administrateurs sécurité
Personne qui prépare la certification WCP
Les gens qui veulent découvrir le monde de
traçabilité

Une formation
Alphorm.com



Connaissances requises

Protocoles SSH, RDP, Linux
Compétences systèmes et réseau
Technologies de la sécurité

Une formation
Alphorm.com



Présentation du Lab de travail



Mohamed Anass EDDIK

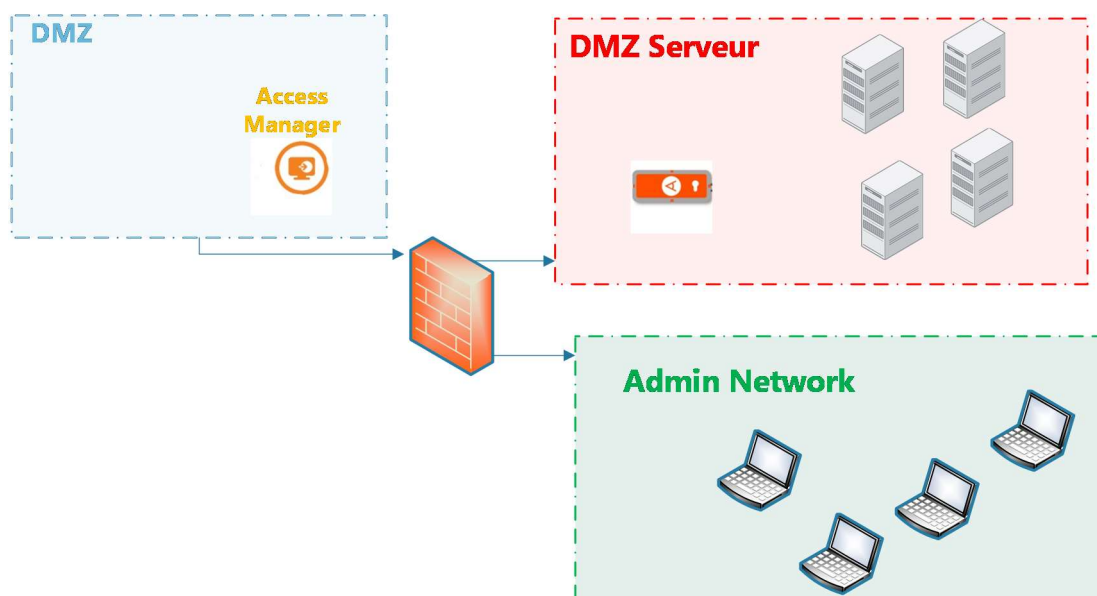


Plan

La topologie du LAB
Les prérequis du Lab

Une formation
Alphorm.com

La topologie du LAB





Les prérequis du Lab

Une machine avec 16Go de RAM
VMware Workstation/Fusion (ou ESXi)
Une VM Wallix Bastion
Une VM Windows
Une VM Linux

Une formation
Alphorm.com





Une formation
Alphorm.com

Découvrir Wallix Bastion



Mohamed Anass EDDIK



Une formation
Alphorm.com

Plan

C'est quoi Wallix Bastion ?
Les Plateformes
Différents scénarios
d'architecture



Wallix Bastion ?

Solution de contrôle et de traçabilité
des administrateurs vers des serveurs

Protocoles supportés :

SSH

Telnet, Rlogin

RDPet VNC

RAW TCP/IP

Une formation
Alphorm.com

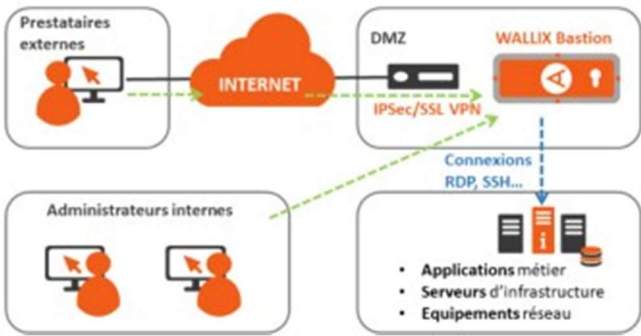


Les Plateformes

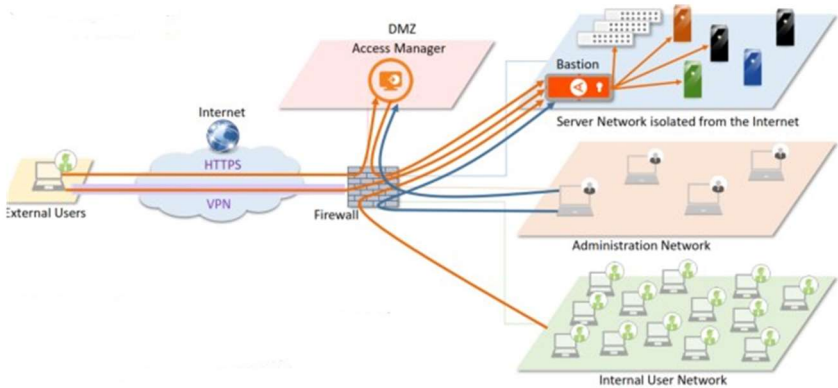


Une formation
Alphorm.com

Différents scénarios d'architecture

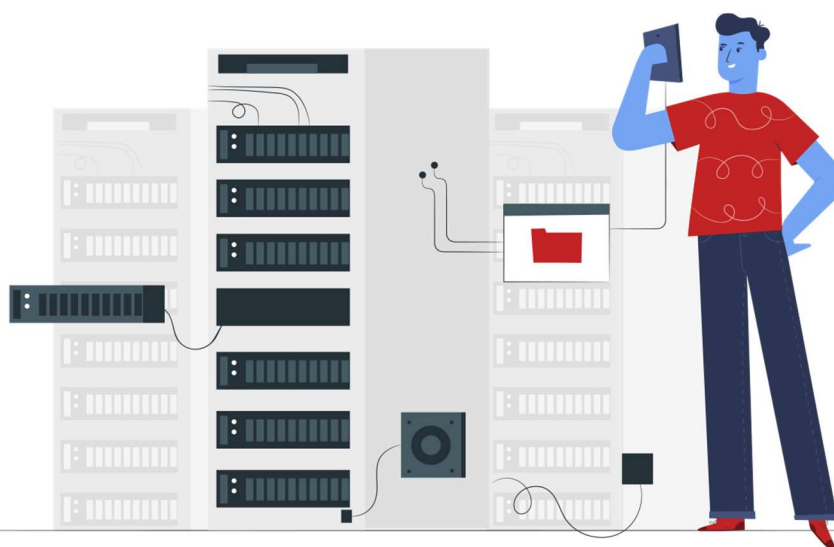


Différents scénarios d'architecture





Démo



Une formation
Alphorm.com



Installer Wallix Bastion



Mohamed Anass EDDIK

Une formation
Alphorm.com



Une formation
Alphorm.com

Plan

Configuration par défaut Arborescence accès SSH



Une formation
Alphorm.com

Configuration par défaut

Configuration par défaut du réseau :

Eth0 : 192.168.10.5/24

GW : 192.168.10.1

SSH administration port : 2242

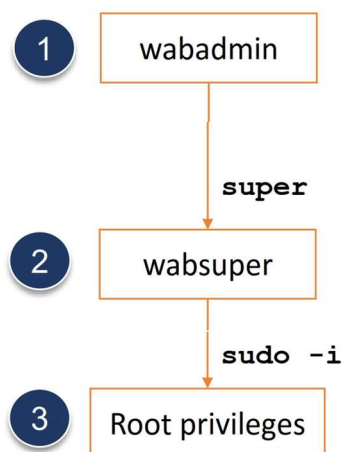
Utilisateurs système:

Login : wabadmin, password : SecureWabAdmin

Login : wabsuper, password devrait être défini



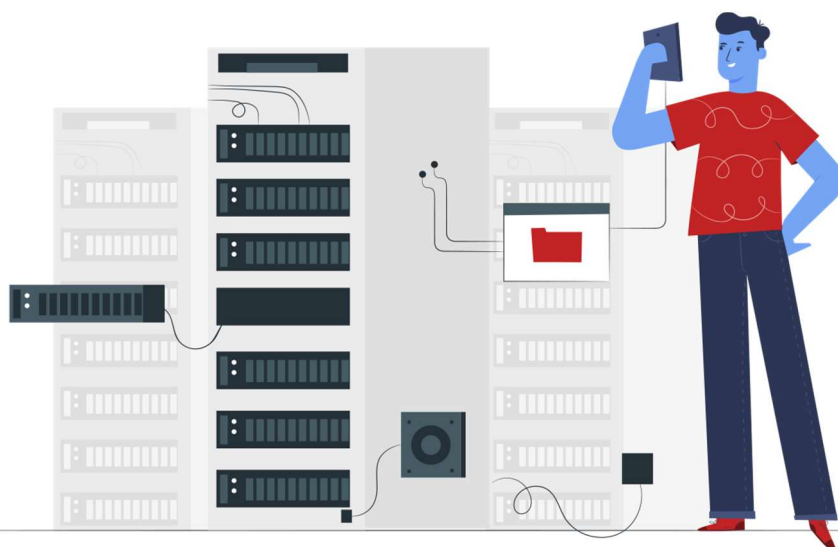
Arborescence accès SSH



Une formation
Alphorm.com



Démo



Une formation
Alphorm.com



Une formation
Alphorm.com

Prendre la main



Mohamed Anass EDDIK



Une formation
Alphorm.com

Plan

Ports de communication
Restauration du compte
Admin

Ports de communication

Depuis Wallix Bastion

SSH : 22 RDP : 3389 HTTP/HTTPS : 80/443
SMTP : 25 SMTPS : 465 SMTP+STARTTLS : 587
NTP : 123 • DNS : 53 Syslog : 514
Authentification externe Kerberos : 88
Authentification externe LDAP : 389
Authentification externe LDAP sur SSL : 636
Authentification externe RADIUS : 1812
Authentification externe TACACS+ : 49
Stockage réseau NFS : 2049
Stockage réseau CIFS : 445
SMB pour la gestion de mots de passe : 139 | 445

Vers Wallix Bastion

Proxy SSH/SFTP/TELNET/RLOGIN : 22
Proxy RDP/VNC : 3389
Interface CLI d'administration de
WALLIX Bastion (console SSHADMIN)
: 2242
Interface Web d'administration de
WALLIX Bastion (GUI) : 443



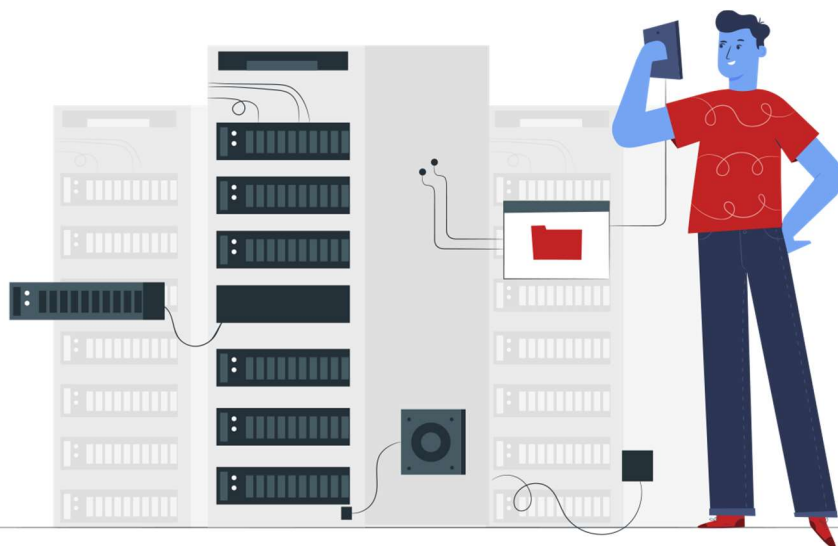
Restauration du compte Admin

```
root@wb-training:~# WABRestoreDefaultAdmin
```

WALLIX
BASTION

Le Guide du Débutant

Démo



Une formation
Alphorm.com

WALLIX
BASTION

Le Guide du Débutant

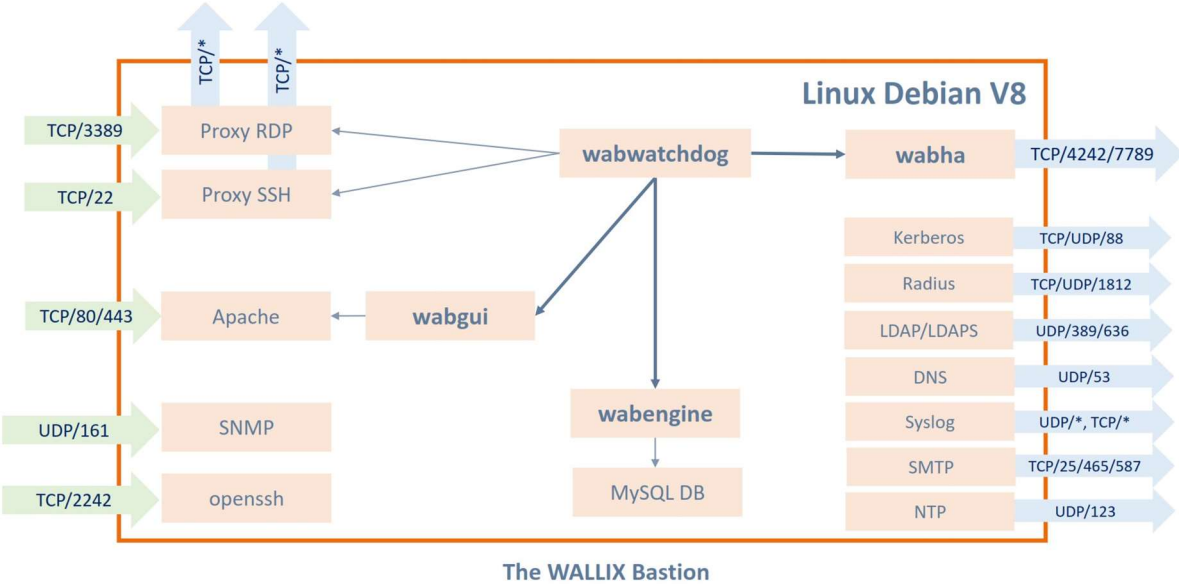
Initier la Configuration



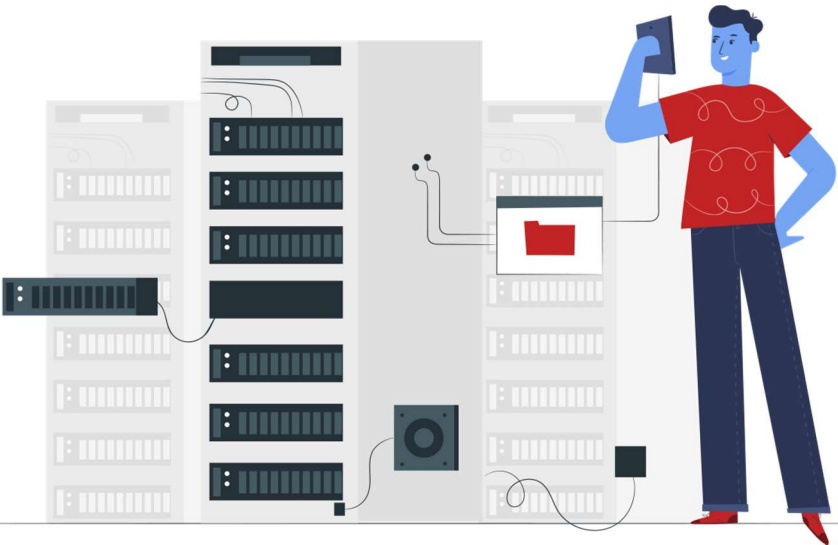
Mohamed Anass EDDIK

Une formation
Alphorm.com

Composant et services de Bastion



Démo





Ajouter des utilisateurs et groupes d'utilisateurs



Mohamed Anass EDDIK

Une formation
Alphorm.com



Déclarer les domaines et les ressources



Mohamed Anass EDDIK

Une formation
Alphorm.com



Plan

Domaine ?
Ressources ?

Une formation
Alphorm.com

Domaine ?

Domaine global

Un domaine global représente une entité de gestion regroupant une multitude de comptes cibles pouvant être utilisés pour l'authentification sur **une multitude** d'équipements

L'avantage significatif de cette entité réside dans le déploiement et la synchronisation du changement de mot de passe en une seule fois sur tous les comptes des équipements associés au domaine

Domaine local

Un domaine local représente une entité de gestion regroupant une multitude de comptes cibles pouvant être utilisés pour l'authentification sur **un seul et unique** équipement



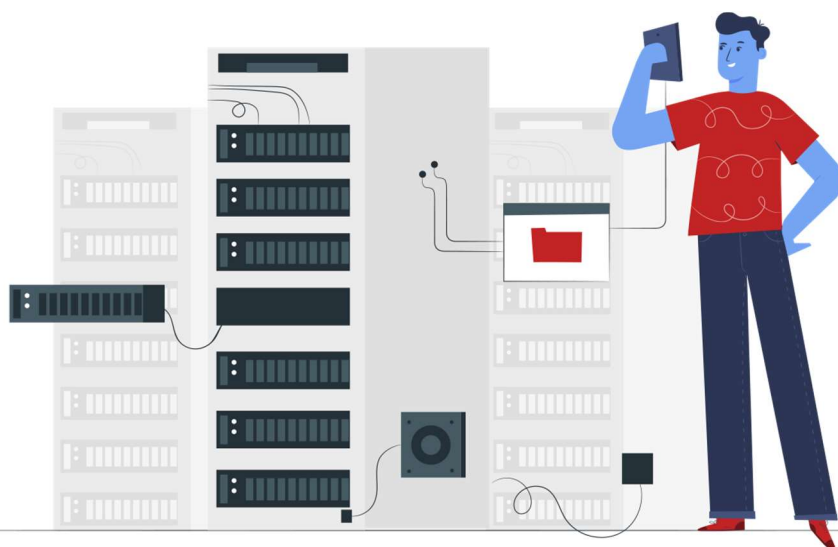
Ressources ?

Domaine
Equipements
Applications
Comptes

Une formation
Alphorm.com



Démo



Une formation
Alphorm.com



Créer les autorisations vers les ressources



Mohamed Anass EDDIK

Une formation
Alphorm.com



Se Connecter en RDP



Mohamed Anass EDDIK

Une formation
Alphorm.com

Options spécifiques au RDP

RDP_CLIPBOARD_UP : autorise le transfert de données via le presse-papier depuis le client vers la session RDP

RDP_CLIPBOARD_DOWN : autorise le transfert de données via le presse-papier depuis la session vers le client RDP

RDP_CLIPBOARD_FILE : autorise le transfert de fichiers avec la fonction copier/coller via le presse-papier

RDP_PRINTER : autorise l'utilisation d'imprimantes locales lors de la session à distance

RDP_COM_PORT : autorise l'utilisation de ports locaux série et parallèle lors de la session à distance

RDP_DRIVE : autorise l'utilisation de disques locaux lors de la session à distance

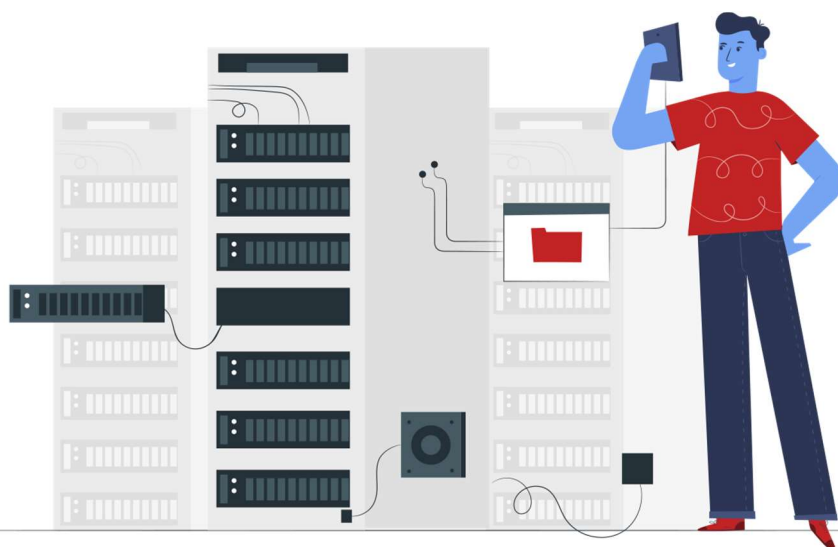
RDP_SMARTCARD : autorise l'utilisation des cartes à puce locales lors de la session à distance

RDP_AUDIO_OUTPUT : autorise la lecture audio lors de la session à distance



Démo

Une formation
Alphorm.com





Se Connecter en SSH



Mohamed Anass EDDIK

Une formation
Alphorm.com

Options spécifiques au SSH

SSH_SHELL_SESSION : autorise le démarrage des sessions shell

SSH_REMOTE_COMMAND : autorise l'exécution des commandes à distance

SSH_SCP_UP : autorise le transfert de fichiers vers l'équipement cible (transfert SCP depuis le client vers le serveur)

SSH_SCP_DOWN : autorise le transfert de fichiers depuis l'équipement cible (transfert SCP depuis le serveur vers le client)

SSH_X11 : autorise l'affichage d'applications X11 s'exécutant sur un équipement cible

SFTP_SESSION : autorise le transfert bi-directionnel de fichiers via SFTP (session SFTP)

SSH_DIRECT_TCPIP : autorise la redirection directe de port TCP/IP (depuis le client vers le serveur)

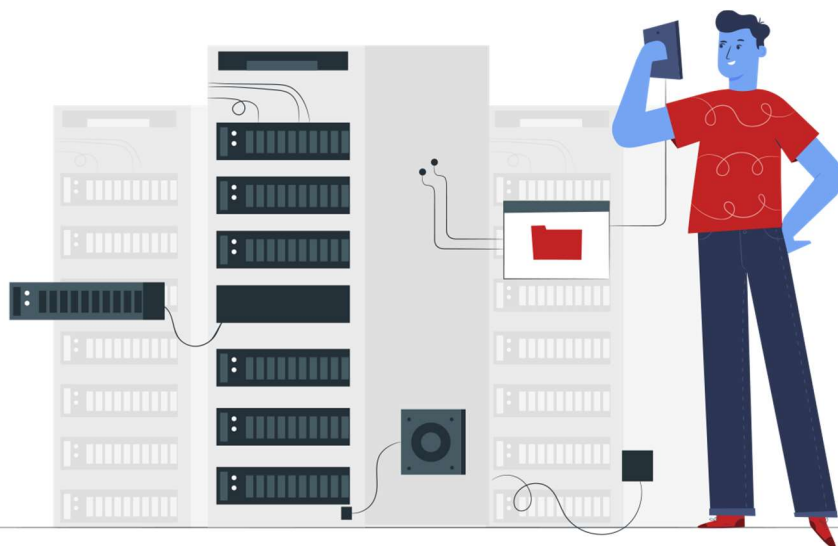
SSH_REVERSE_TCPIP : autorise la redirection inverse de port TCP/IP (depuis le serveur vers le client)

SSH_AUTH_AGENT : autorise le transfert d'authentification par agent (auth-agent multi-hops)

WALLIX
BASTION

Le Guide du Débutant

Démo



Une formation
Alphorm.com

WALLIX
BASTION

Le Guide du Débutant

Gérer les sessions courantes



Mohamed Anass EDDIK

Une formation
Alphorm.com



voir l'historique des sessions et d'authentifications



Mohamed Anass EDDIK

Une formation
Alphorm.com



Gérer les fichiers d'audit



Mohamed Anass EDDIK

Une formation
Alphorm.com



Configurer le certificat X509



Mohamed Anass EDDIK

Une formation
Alphorm.com



Plan

Prérequis
Etapas de configuration

Une formation
Alphorm.com



Une formation
Alphorm.com

Prérequis

Certificat au format PEM pour le serveur Web de WALLIX Bastion

Clé privée au format PEM correspondant à ce certificat du serveur

Clé publique de l'Autorité de Certification ayant délivré ce certificat du serveur. Il peut s'agir d'un certificat auto-signé ou délivré par une autorité reconnue



Une formation
Alphorm.com

Etales de configuration

Arrêter l'interface Web de WALLIX Bastion

Télécharger le certificat de l'AC (contenant sa clé publique) au format PEM

Télécharger la clé privée du serveur Web au format PEM

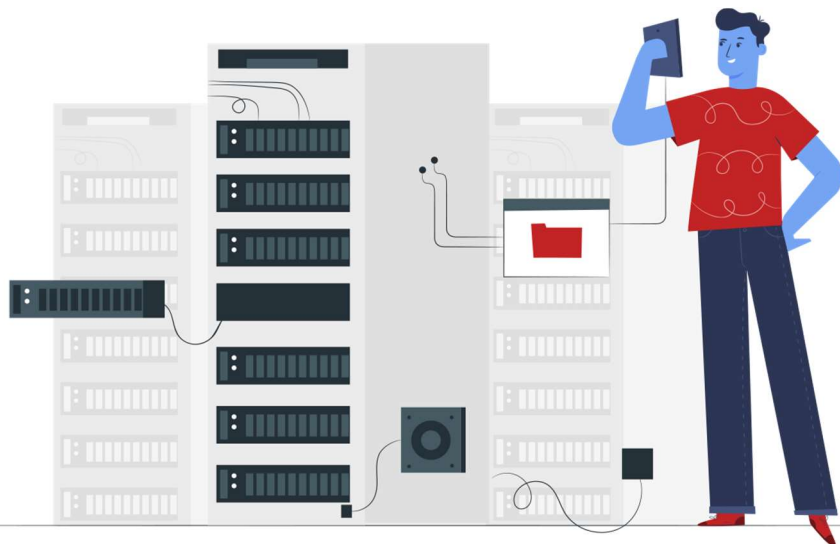
Télécharger le certificat du serveur Web (contenant sa clé publique) au format PEM

Redémarrer l'interface Web de WALLIX Bastion

WALLIX
BASTION

Le Guide du Débutant

Démo



Une formation
Alphorm.com

WALLIX
BASTION

Le Guide du Débutant

Authentifier un utilisateur



Mohamed Anass EDDIK

Une formation
Alphorm.com



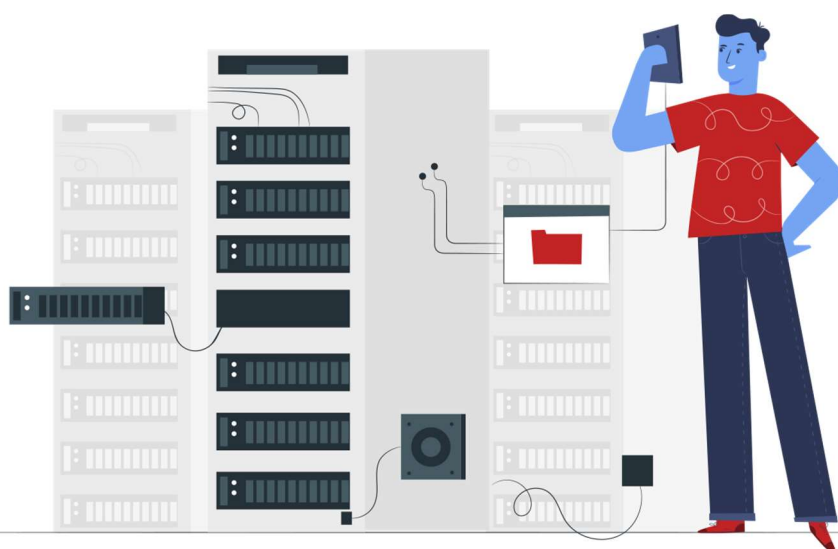
Processus de connexion

Une formation
Alphorm.com



Démo

Une formation
Alphorm.com





Une formation
Alphorm.com

Se connecter en SSH



Mohamed Anass EDDIK



Une formation
Alphorm.com

Réinitialiser les mots de passe système



Mohamed Anass EDDIK



Augmenter l'espace disque d'une VM



Mohamed Anass EDDIK

Une formation
Alphorm.com



Visualiser les enregistrements des vidéos



Mohamed Anass EDDIK

Une formation
Alphorm.com



Une formation
Alphorm.com

Conclusion



Mohamed Anass EDDIK



Une formation
Alphorm.com

Bilan

Introduction Wallix Bastion
Gérer les sessions
Gérer les sessions d'audit
S'authentifier avec un certificat X509
Configurer les options avancées

