



Une formation
Alphorm
com

Formation FortiManager *Installation et Configuration*



Mohamed Anass EDDIK



Une formation
Alphorm
com

Plan de la formation

Introduction

1. Introduction au FortiManager
2. Administrer et manager le FortiManager
3. Gérer les Devices
4. Déployer les règles de sécurité et les objets
5. Mettre en place le SD-WAN et la Security Fabric
6. Diagnostiquer et dépanner au niveau du FortiManager

Conclusion



Public concerné

Les administrateurs des pare-feux Fortigate
Les ingénieurs et administrateurs sécurité
Les ingénieurs de support

Une formation
Alphorm.com



Connaissances requises

Savoir comment configurer un Fortigate
Connaissance Réseau et Système
Technologies de la sécurité

Une formation
Alphorm.com



Formations pour les prérequis



Une formation
Alphorm.com





Présentation du Lab de travail



Mohamed Anass EDDIK

Une formation
Alphorm.com

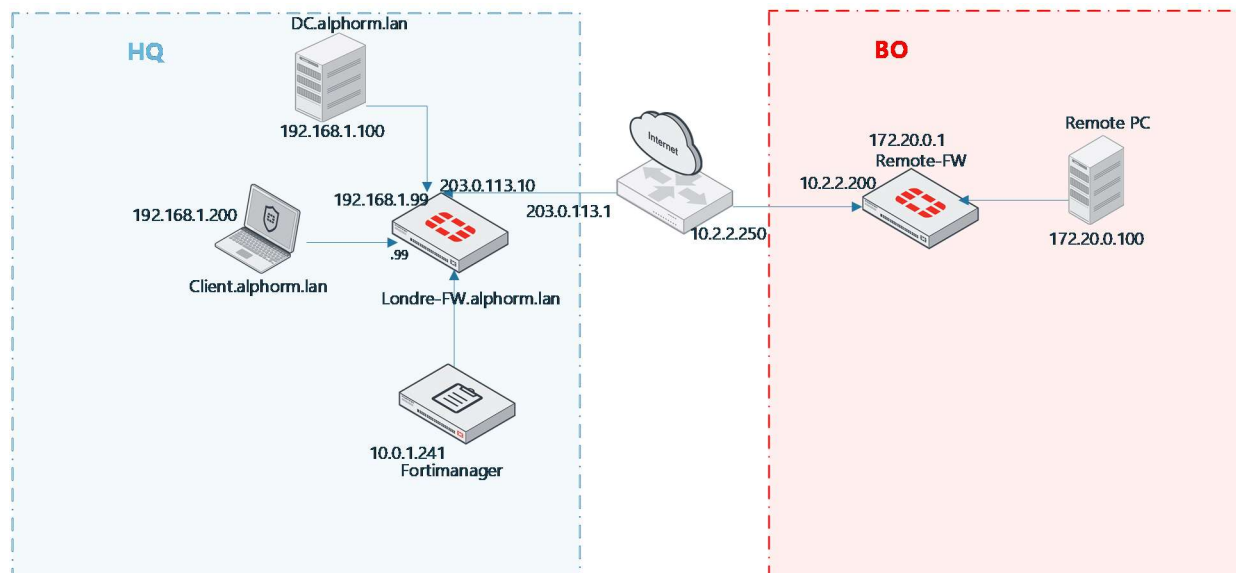


Plan

La topologie du LAB
Les prérequis du Lab

Une formation
Alphorm.com

La topologie du LAB



Les prérequis du Lab

Une machine avec 32Go de RAM
VMware Workstation/Fusion (ou ESXi)
Une VM FortiManager
Une ou deux VM Fortigate



Découvrir FortiManager



Mohamed Anass EDDIK



Plan

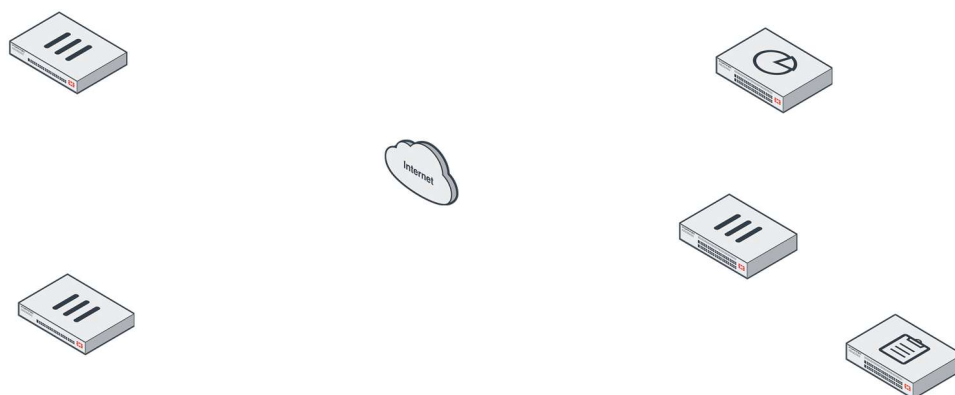
Qu'est ce que c'est FortiManager?

ADOMs

Panes manager

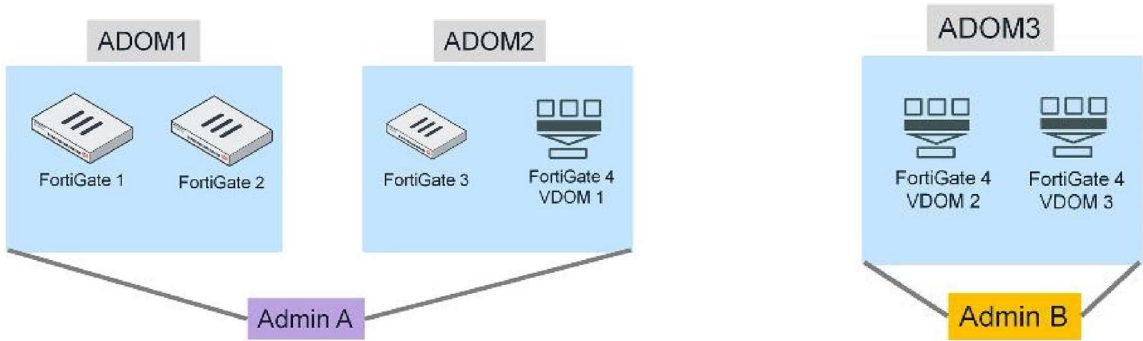
Une formation
Alphorm.com

Qu'est ce que c'est FortiManager?



Une formation
Alphorm.com

ADOMs

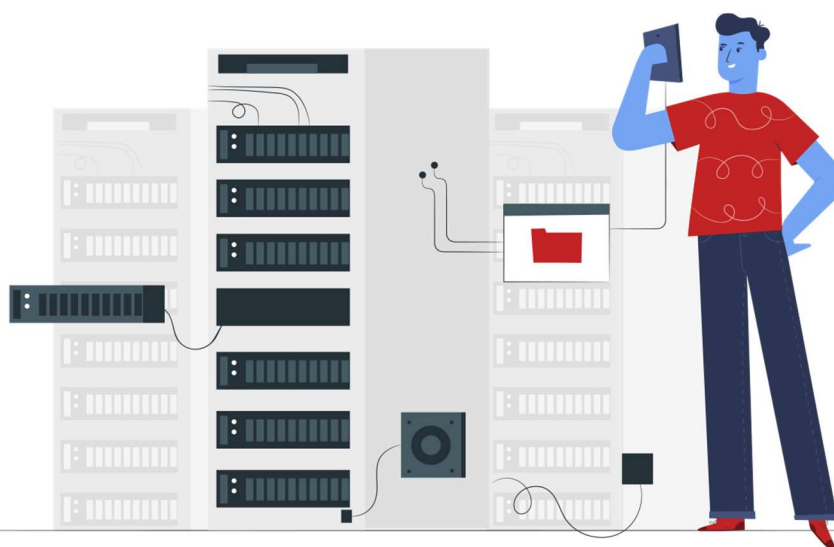


Panes manager





Démo



Une formation
Alphorm.com



Commencer avec le FortiManager



Mohamed Anass EDDIK

Une formation
Alphorm.com

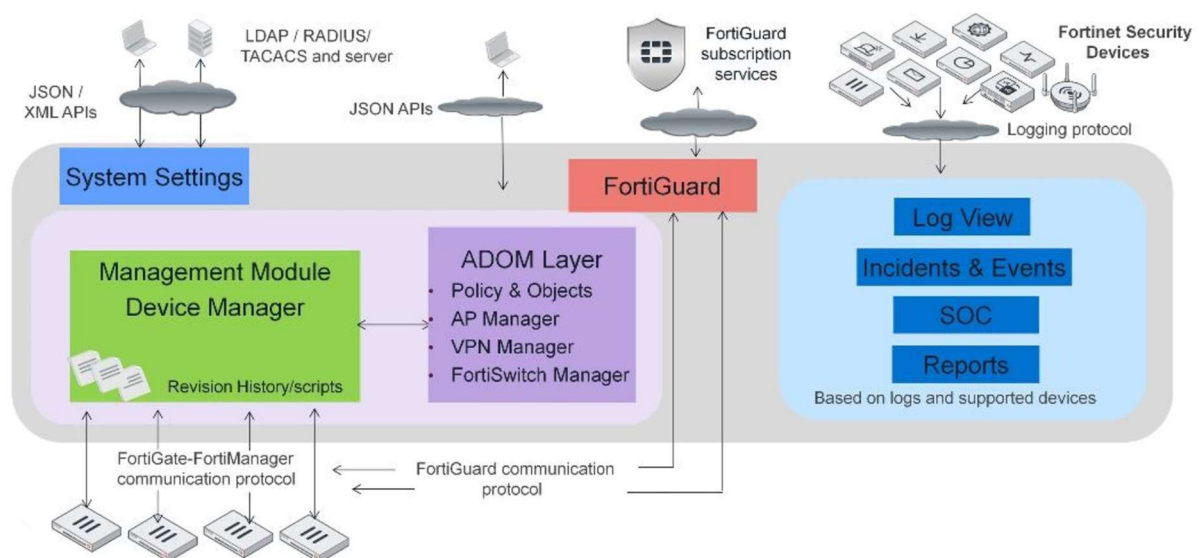


Plan

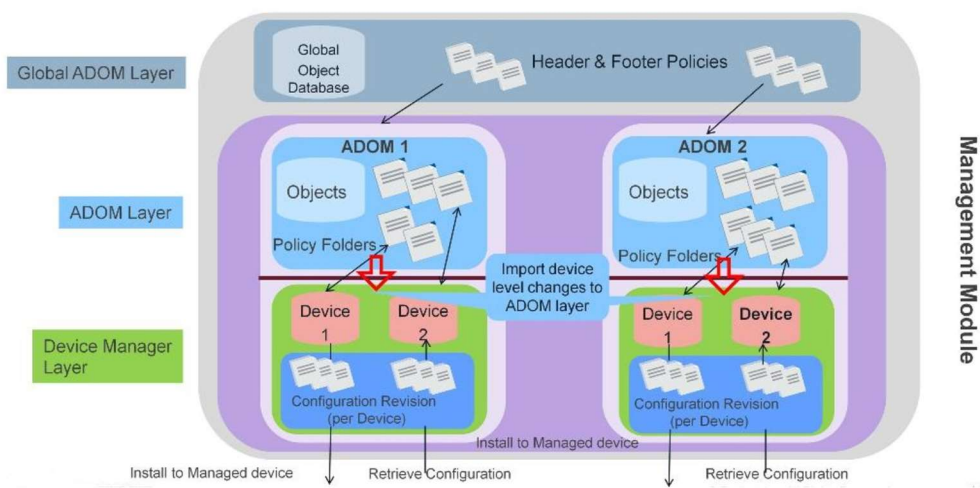
Découvrir les flux internes
Management des modules
Cycle de vie pour le management
d'un équipement

Une formation
Alphorm.com

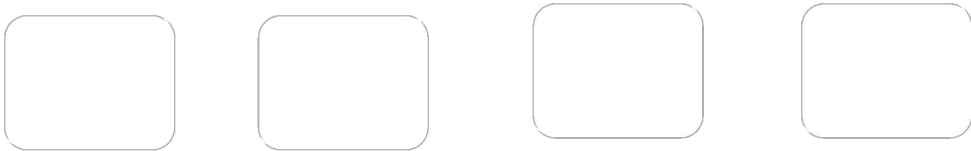
Découvrir les flux interne



Management des modules

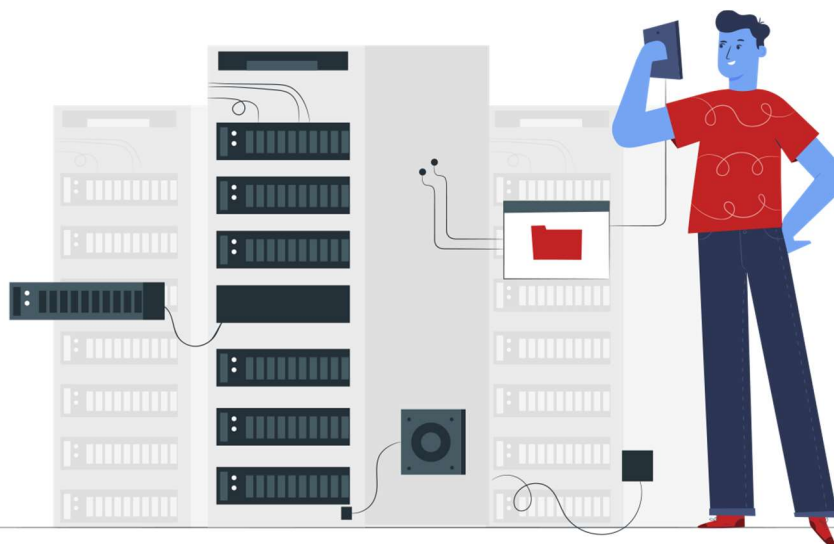


Cycle de vie pour le management d'un équipement





Démo



Une formation
Alphorm.com



Installer FortiManager



Mohamed Anass EDDIK

Une formation
Alphorm.com



Plan

Les ports de FortiManager
Configuration par défaut
Les cas d'usage



Les ports de FortiManager

Functionality	Port(s)
Destination Ports	
Remote management of a FortiGate device	TCP 541 (IPv4), TCP 542 (IPv6)
Firmware image download	TCP 443
Antivirus, IPS, Web Filtering, Antispam updates from FortiManager to FortiGuard Distribution Servers	TCP 443
DNS lookup	UDP 53
Syslog	UDP 514
Listening Ports	
FortiGuard Antivirus and IPS update push	UDP 9443
FortiGuard Antivirus or IPS update request from a FortiGate device	TCP 8890
FortiGuard Antispam or Web Filtering rating lookup from a FortiClient or FortiGate	UDP 53 or 8888
Web Services (a.k.a XML API)	TCP 8080
Web GUI and JSON API	TCP 443
Antivirus and IPS updates for FortiClient	TCP 80
HA heartbeat or synchronization (FortiManager HA cluster)	TCP 5199
Two FortiManagers configured in cascade mode	
FortiManagers in cascade mode both listening and destination ports	TCP 8891, 8900 and 8901



Configuration par default

Port1 interface IP : **192.168.1.99/24**

Ping, HTTP,HTTPS,SSH sont activé par défaut

Login : **admin**

Mot de passe : **(vide)**

Une formation
Alphorm
com



Les cas d'usage

Vente en détail

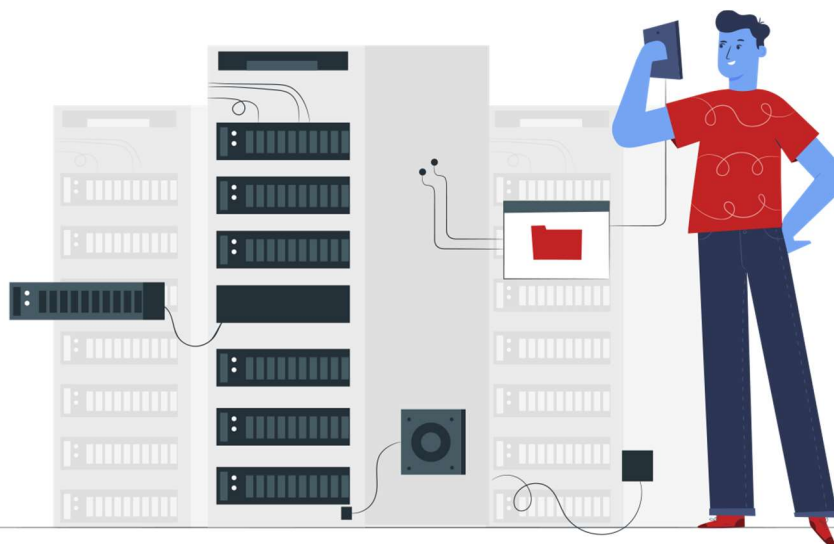
MSSP

Exigences pour différentes organisations

Une formation
Alphorm
com



Démo



Une formation
Alphorm.com



Configurer les ADOMs



Mohamed Anass EDDIK

Une formation
Alphorm.com



Plan

Les Modes ADOM

Les versions des ADOMs et les upgrades

Migration des ADOMs

Une formation
Alphorm.com



Les Modes ADOM

Mode Normal

- ADOM lecture/écriture
- Tous les changements peuvent se faire depuis le mode
- Les équipements manager sont automatiquement mis à jour

Mode Backup

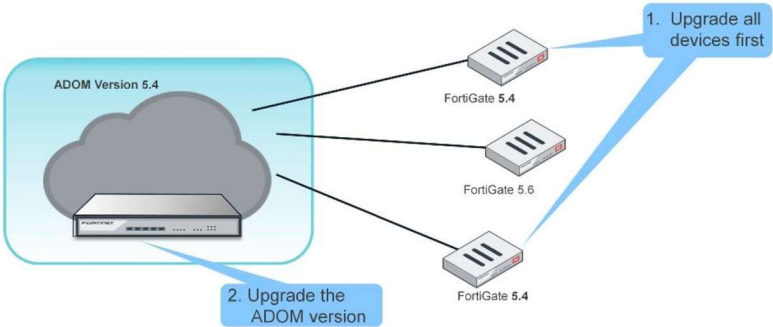
- ADOM lecture seule
- Juste le script qui permet les changements sur les équipements
- Peut faire les changements directement sur les équipements

Une formation
Alphorm.com



Les versions des ADOMs et les upgrades

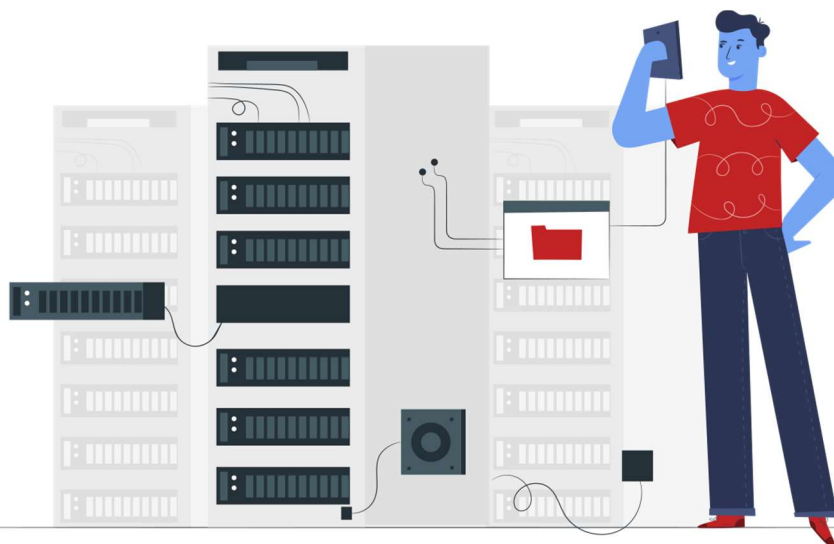
ADOM Version	Forti OS Version			
	5.4	5.6	6.0	6.2
5.4	Yes	Yes	No	No
5.6	No	Yes	Yes	No
6.0	No	No	Yes	No
6.2	No	No	Yes	Yes



Migration des ADOMs



Démo



Une formation
Alphorm.com



Administrer les comptes



Mohamed Anass EDDIK

Une formation
Alphorm.com



Plan

Les profils d'accès Workspace Mode



Les profils d'accès

Nom du profil	Permissions des Admin
Package_User	Accès en lecture/écriture vers les règles et les objets Lecture seule vers le système et autres permissions
Restricted_User	Pas de permission vers système Accès seul vers tous les équipements
Standard_User	Pas de permission vers système Accès en lecture/écriture vers tous les équipements
Super_User	Accès total à tout



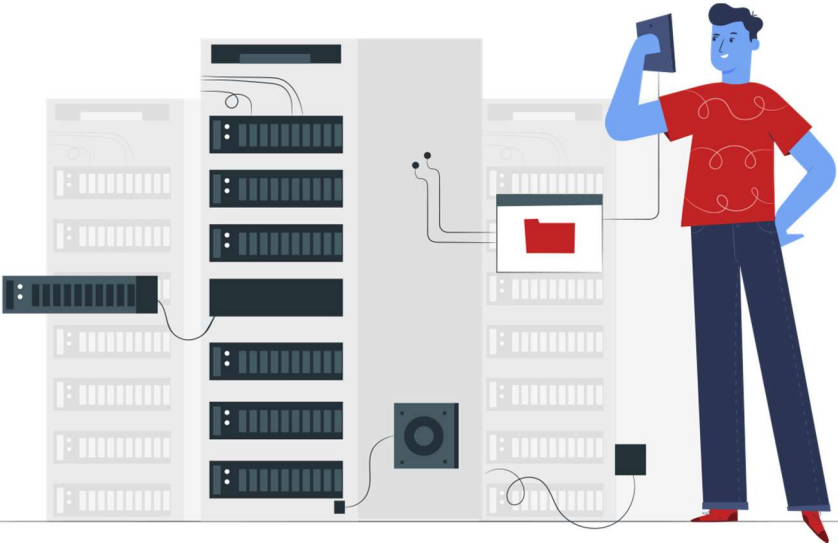
Workspace Mode

Une formation
Alphorm.com



Démo

Une formation
Alphorm.com





Une formation
Alphorm.com

Créer des Sauvegardes et monitorer les événements



Mohamed Anass EDDIK



Une formation
Alphorm.com

Enregistrer les devices



Mohamed Anass EDDIK



Les méthodes d'enregistrement

Wizard

L'administrateur Fortimanager utilise l'assistant d'enregistrement de l'appareil pour enregistrer l'appareil

Si l'appareil est pris en charge et que les détails sont corrects, Fortimanager enregistre l'appareil

Demande depuis un équipement supporté

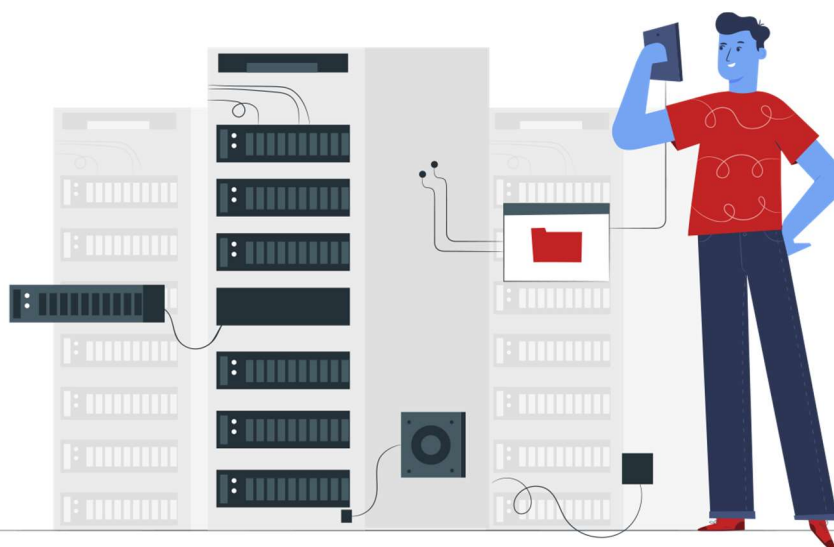
L'administrateur de l'appareil pris en charge, demande l'enregistrement

L'administrateur FortiManager accepte (ou refuse) la demande

Une formation
Alphorm.com



Démo



Une formation
Alphorm.com



Paramétrer les niveaux des devices



Mohamed Anass EDDIK

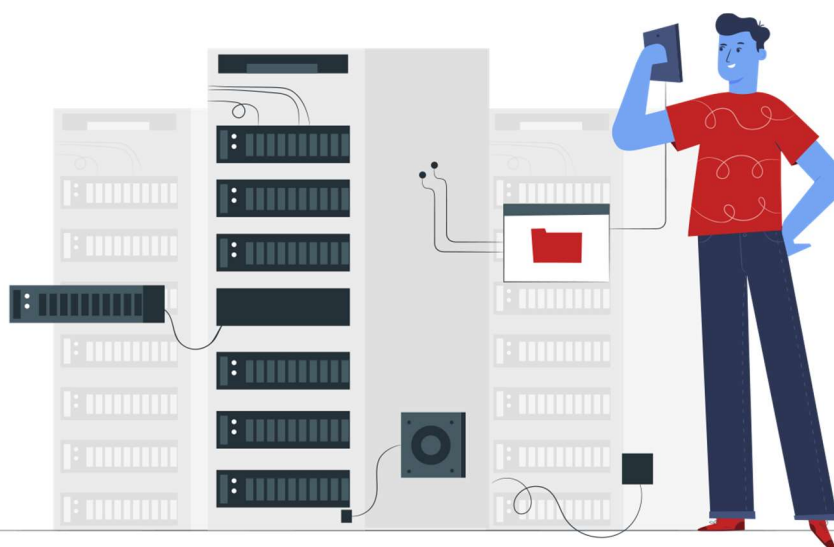
Une formation
Alphorm.com

État de l'appareil géré

Une formation
Alphorm.com



Démo



Une formation
Alphorm.com



Configurer les Devices Groups



Mohamed Anass EDDIK

Une formation
Alphorm.com



Plan

Scripts

Interaction Fortigate-Fortimanager

Une formation
Alphorm.com



Scripts

Peut apporter de nombreuses modifications à de nombreux appareils gérés

Aide à simplifier les changements de configuration en vrac et à maintenir la cohérence

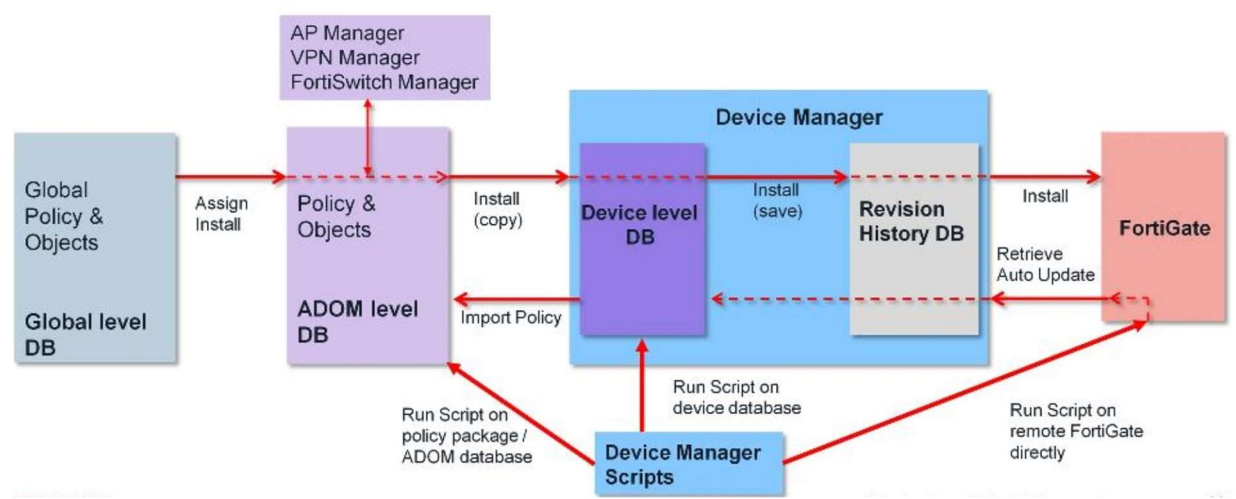
Deux types de scripts :

- Cli
- Tcl

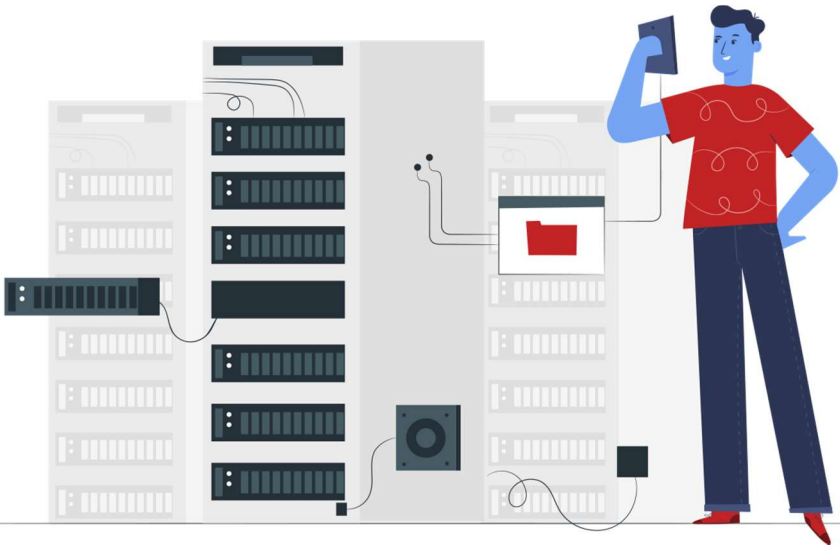
Les scripts sont activés par défaut

Une formation
Alphorm.com

Interaction Fortigate-FortiManager



Démo





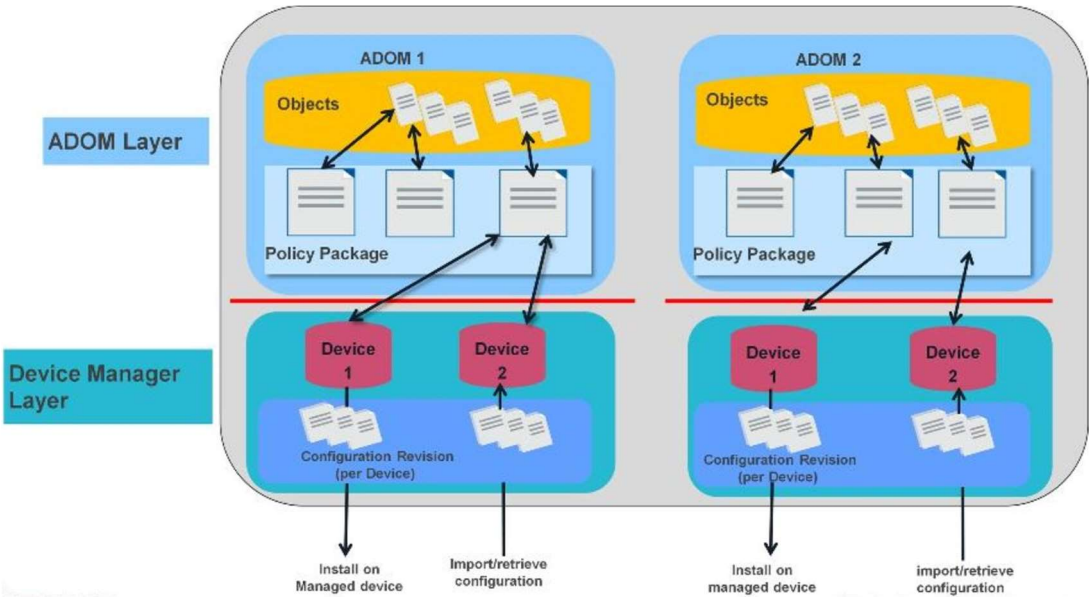
Manager les règles de sécurité et les objets



Mohamed Anass EDDIK

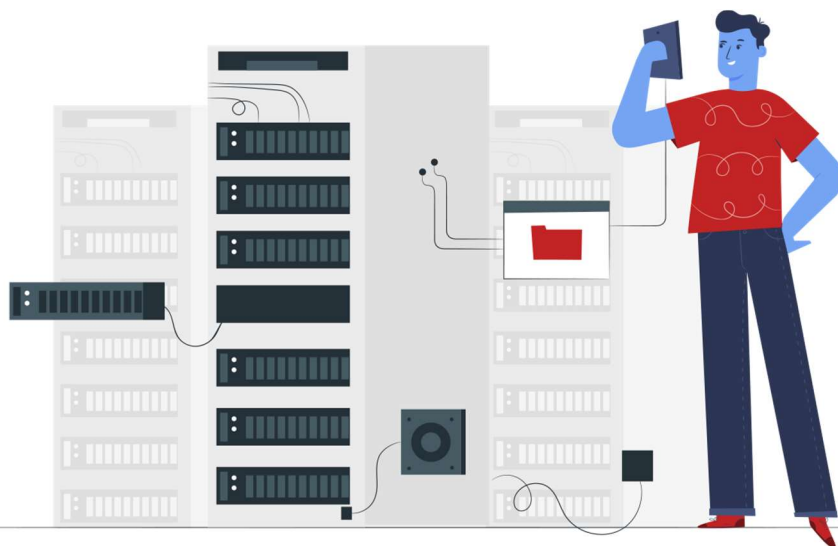
Une formation
Alphorm.com

Policy Workflow





Démo



Une formation
Alphorm.com



Utiliser le Wizard



Mohamed Anass EDDIK

Une formation
Alphorm.com



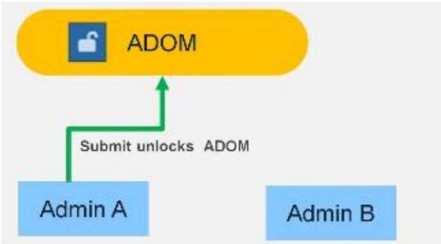
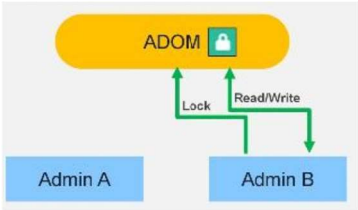
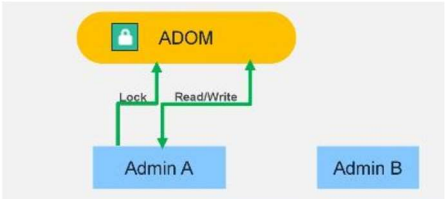
Configurer le workflow mode



Mohamed Anass EDDIK

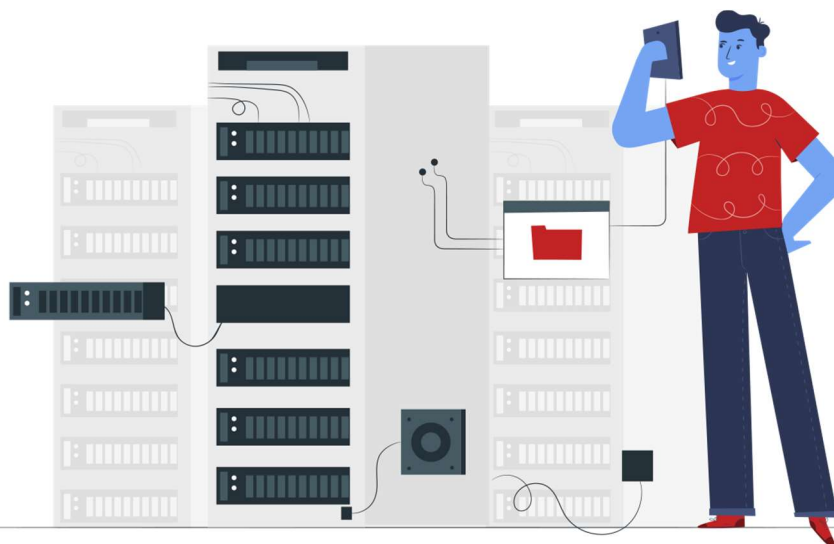
Une formation
Alphorm.com

Comment utiliser le mode Workflow





Démo



Une formation
Alphorm.com



Configurer le SD-WAN



Mohamed Anass EDDIK

Une formation
Alphorm.com



Plan

Prérequis SD-WAN

Partager les politiques et les objets

Une formation
Alphorm.com



Prérequis SD-WAN

Prérequis Fortigate

- Au moins 2 membres sur les interfaces
- Les interfaces ne doivent pas être reclusées par un autre élément de configuration
- Supports aggregate, VLAN, IPSEC interfaces
- Une seule interface SD-WAN par VDOM

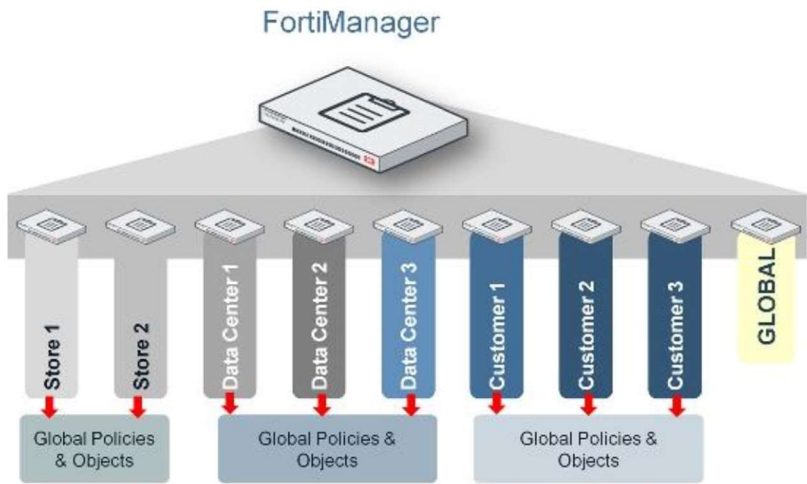
Prérequis FortiManager

- Activer le SD-WAN central management

Une formation
Alphorm.com



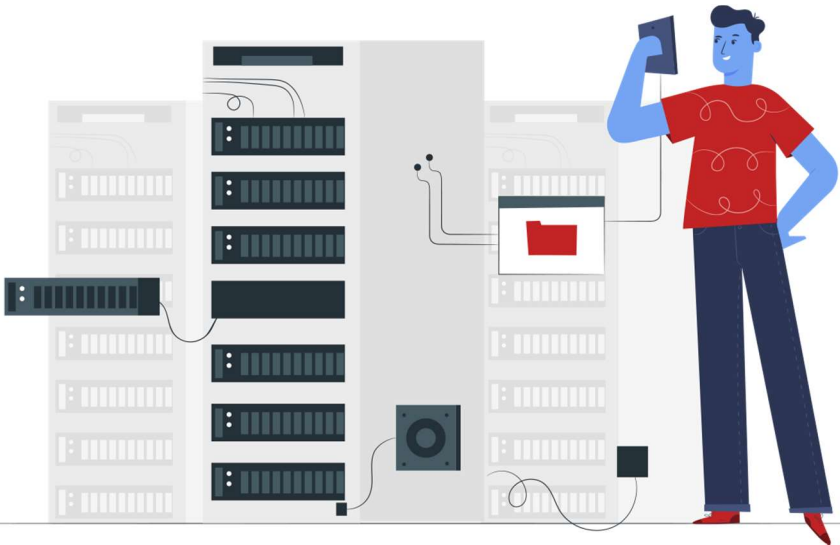
Partager les politiques et les objets



Une formation
Alphorm.com



Démo



Une formation
Alphorm.com



Une formation
Alphorm.com

Intégrer la Security Fabric



Mohamed Anass EDDIK



Une formation
Alphorm.com

Connaitre les différents scénarios de déploiement



Mohamed Anass EDDIK



Plan

FortiManager derrière le NAT

Fortigate derrière un NAT

Les deux équipements derrière un NAT

Une formation
Alphorm
com



FortiManager derrière le NAT

Une formation
Alphorm
com



Fortigate derrière un NAT

Une formation
Alphorm
com

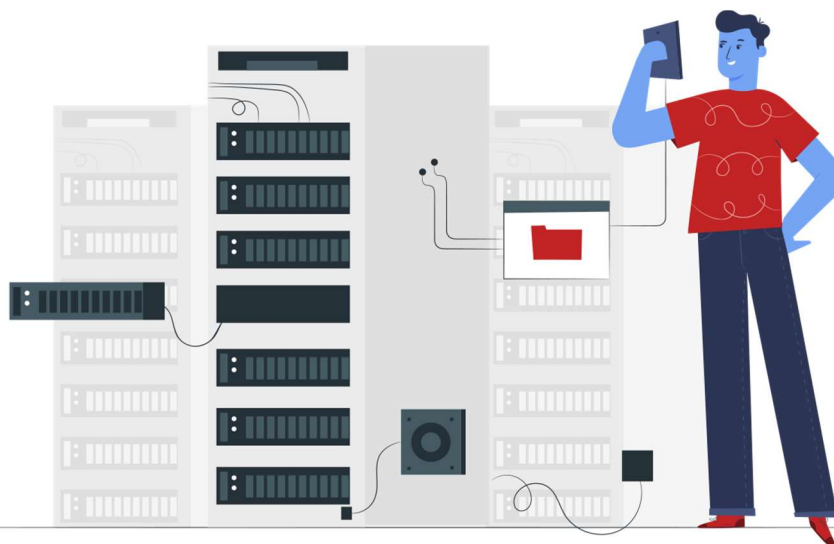


Les deux équipements derrière un NAT

Une formation
Alphorm
com



Démo



Une formation
Alphorm.com



Diagnostiquer et dépanner



Mohamed Anass EDDIK

Une formation
Alphorm.com



Intégrité de DataBase

Effectuez toujours un arrêt gracieux avant d'éteindre
Activer le verrouillage ADOM pour éviter les conflits de configuration lorsque plusieurs administrateurs exécutent des actions

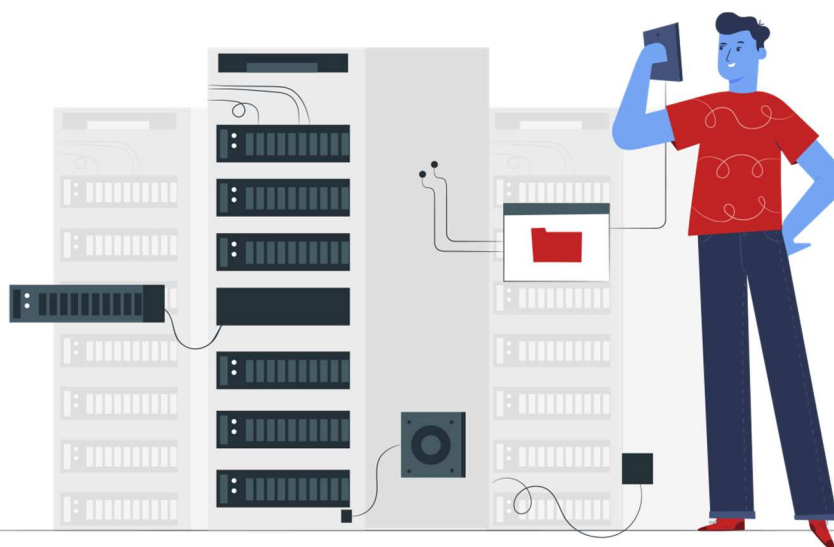
Avant d'effectuer la mise à niveau du firmware, assurez-vous que tous les administrateurs sont déconnectés

NB : Si vous ne pouvez pas résoudre une intégrité de données, vous pouvez réinitialiser le Fortimanager et restaurer sa configuration à partir d'une bonne sauvegarde

Une formation
Alphorm.com



Démo



Une formation
Alphorm.com



Une formation
Alphorm.com

Importer et installer



Mohamed Anass EDDIK



Une formation
Alphorm.com

Plan

Échec du rechargement
Résolution d'installation échouée



Échec du rechargement



Une formation
Alphorm.com



Résolution d'installation échouée

Si la version Fortigate n'est pas prise en charge par la version ADOM, ou Fortimanager ne prend pas en charge certaines fonctionnalités de Fortigate CLI, alors :

- Déplacer l'appareil Fortiagate pour prendre en charge ADOM ou utiliser le script pour résoudre le problème
- Installer à nouveau

Une formation
Alphorm.com



Résolution d'installation échouée

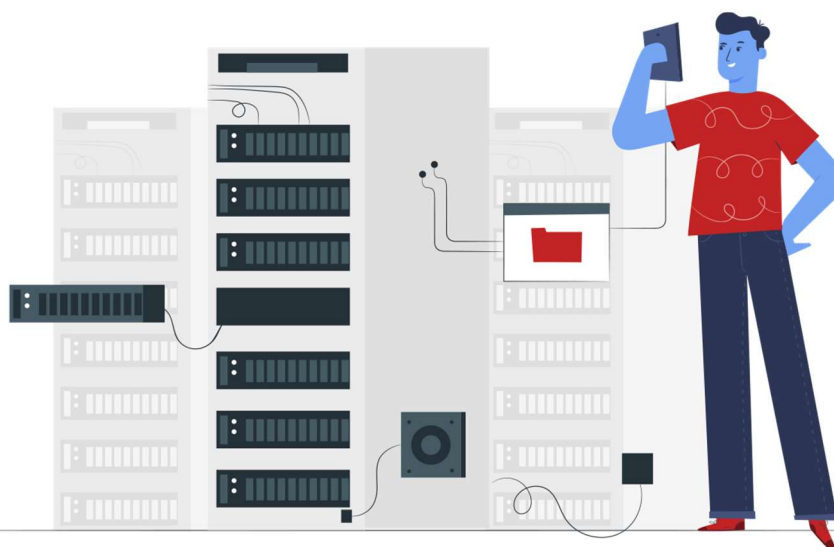
Pour résoudre les problèmes d'échec Install prendre ces étapes :

- Créez de nouveaux ADOM avec un firmware assorti sur Fortigate
- Déplacez Fortigate vers le nouvel ADOM
- Récupérez la configuration et le paquet de stratégie d'importation
- Recréez l'objet ou la stratégie et installez-le à nouveau

Une formation
Alphorm.com



Démo



Une formation
Alphorm.com



HA et Services Fortiguard



Mohamed Anass EDDIK

Une formation
Alphorm.com



Plan

High Availability
Synchronization HA
FortiManager comme un Fortiguard
Local

Une formation
Alphorm.com



High Availability

Tous les appareils Fortimanager en cluster doivent être le même modèle et le même firmware
Conçu pour un appareil principal et plusieurs périphériques secondaires
Soutient la redondance géographique
Chaque membre HA fonctionne de façon indépendante

Une formation
Alphorm.com



Synchronization HA

Ce qui est synchronisé?

Toutes les configurations de l'appareil
Toutes les révisions de configuration

Qu'est-ce qui n'est pas synchronisé ?

Paramètres de configuration pour : (Interface , routes ,HA, SNMP, log)
Fortiguard Fortiguard
Journaux locaux et journaux de console de message d'alerte (données)

Une formation
Alphorm.com



FortiManager comme un Fortiguard Local

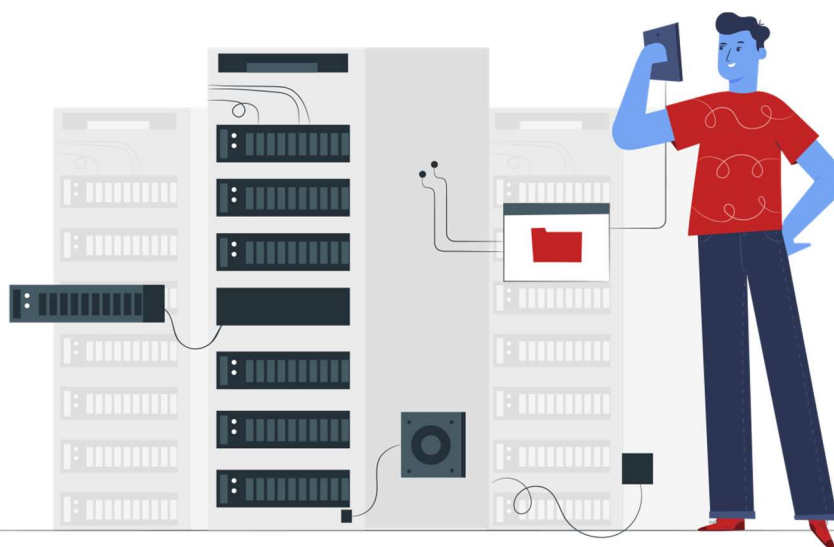
Donwload tous les antivirus, paquets IPS, filtres Web,
bases de données de filtres email sur le FortiManager

Réduit la charge de connexion Internet

Une formation
Alphorm.com



Démo



Une formation
Alphorm.com



Une formation
Alphorm.com

Conclusion



Mohamed Anass EDDIK



Une formation
Alphorm.com

Bilan

1. Introduction au FortiManager
2. Administrer et manager le FortiManager
3. Gérer les Devices
4. Déployer les règles de sécurité et les objets
5. Mettre en place le SD-WAN et la Security Fabric
6. Diagnostiquer et dépanner au niveau du FortiManager

