



Une formation
Alphorm.com

Formation FortiAnalyzer *Installation et Configuration*



Mohamed Anass EDDIK



Une formation
Alphorm.com

Plan de la formation

Introduction

1. Introduction au FortiAnalyzer
2. Administrer et manager le FortiAnalyzer
3. Enregistrer les équipements et communication
4. Logging
5. Rapports

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

FortiAnalyzer

Installation et configuration

Formations pour les prérequis



Une formation
Alphorm.com



FortiAnalyzer

Installation et configuration

Une formation
Alphorm.com

Présentation du Lab de travail



Mohamed Anass EDDIK

FortiAnalyzer

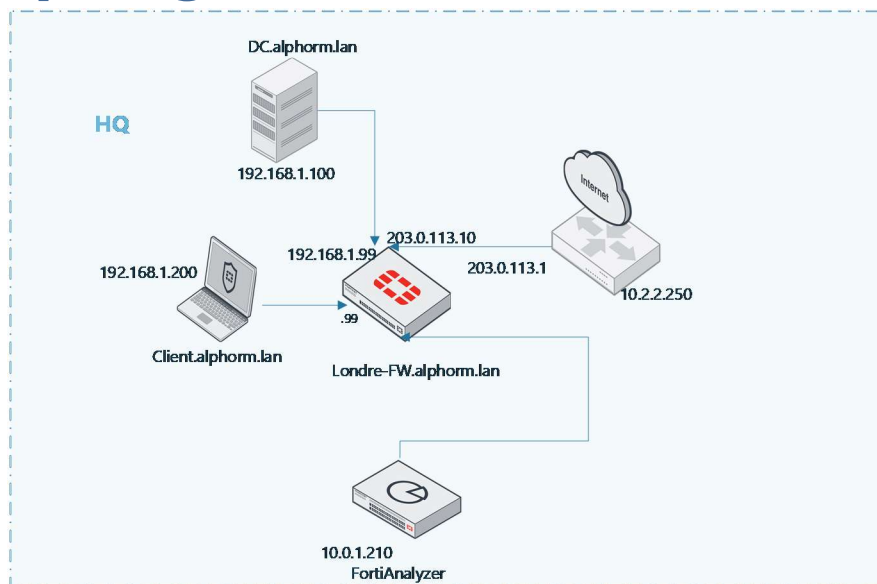
Installation et configuration

Une formation
Alphorm.com

Plan

La topologie du LAB
Les prérequis du Lab

La topologie du LAB



Les prérequis du Lab

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



Découvrir FortiAnalyzer



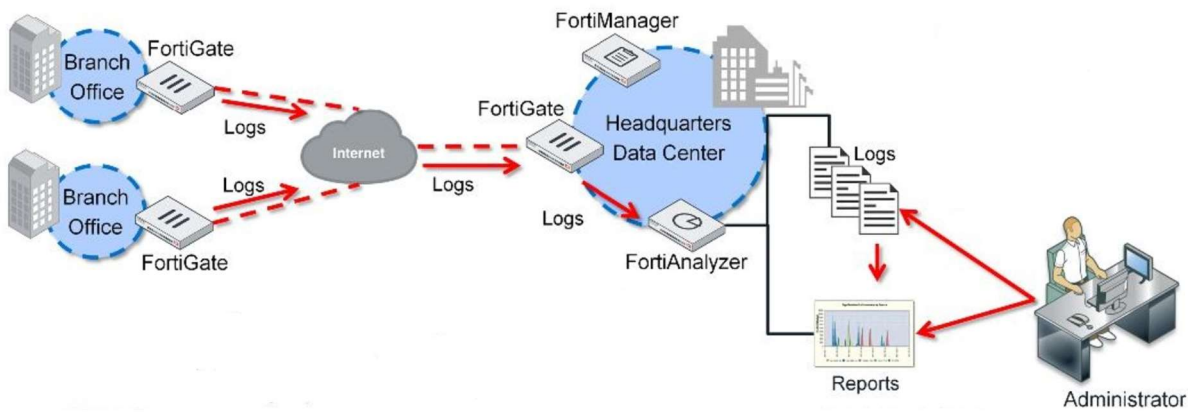
Mohamed Anass EDDIK



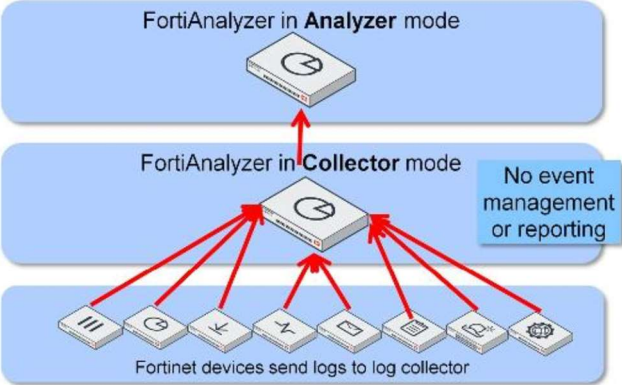
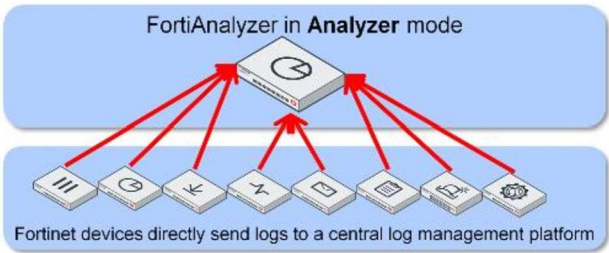
Plan

Centralized log Repository
Modes d'opération FortiAnalyzer

Centralized log Repository



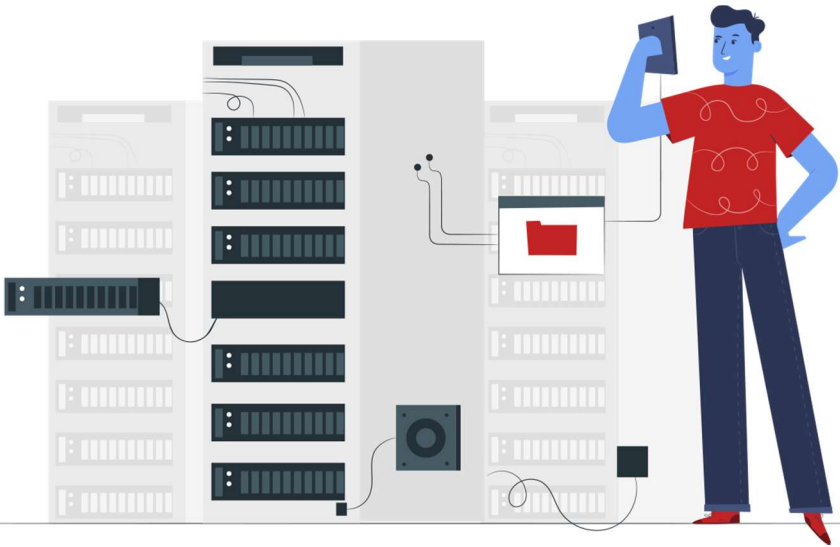
Modes d'opération FortiAnalyzer



Une formation
Alphorm.com



Démo



Une formation
Alphorm.com



Initier la configuration



Mohamed Anass EDDIK

Une formation
Alphorm.com



Configuration par défaut

Admin <none>

Port1 192.168.1.99/24 https,ssh

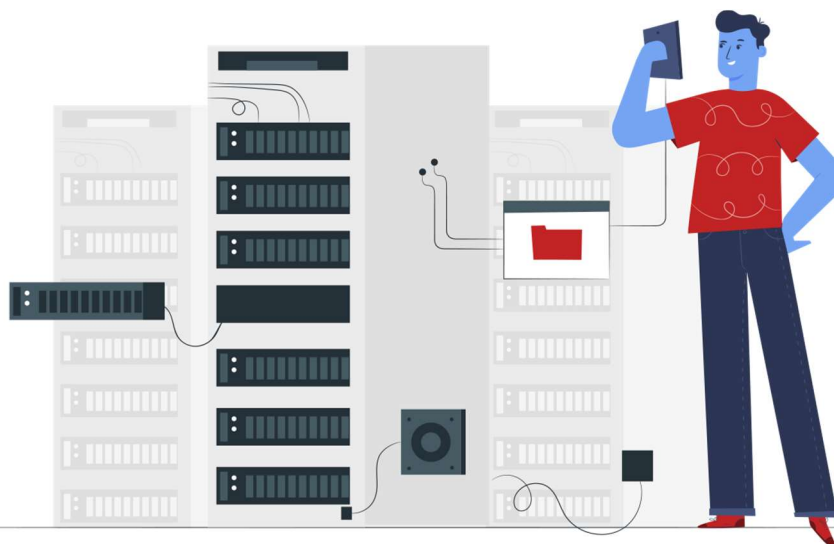
Une formation
Alphorm.com

FortiAnalyzer

Installation et configuration

Une formation
Alphorm.com

Démo



FortiAnalyzer

Installation et configuration

Une formation
Alphorm.com

Sauvegarde externe



Mohamed Anass EDDIK



Contrôler l'accès vers le FortiAnalyzer



Mohamed Anass EDDIK

Une formation
Alphorm.com



Plan

Profils d'administration
Authentification Externe

Une formation
Alphorm.com



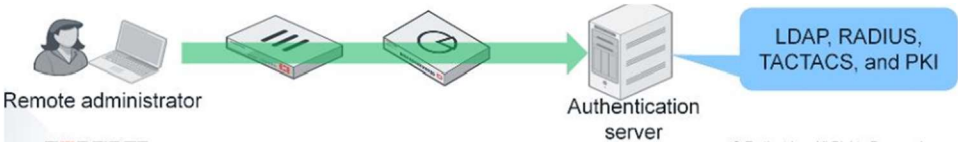
Profils d'administration

Nom du Profil	Privilège d'administration
Super_User	• Tous les privilège système activés • Tous les privilège système activés
Standard_User	• Pas de privilège système activés • Acces R/W pour tous les privilèges équipements
Restricted_user	• Pas de privilège système activés • Acces ead-only pour tous les privilèges équipements



Authentification Externe

LDAP,RADIUS,TACACS+,and PKI

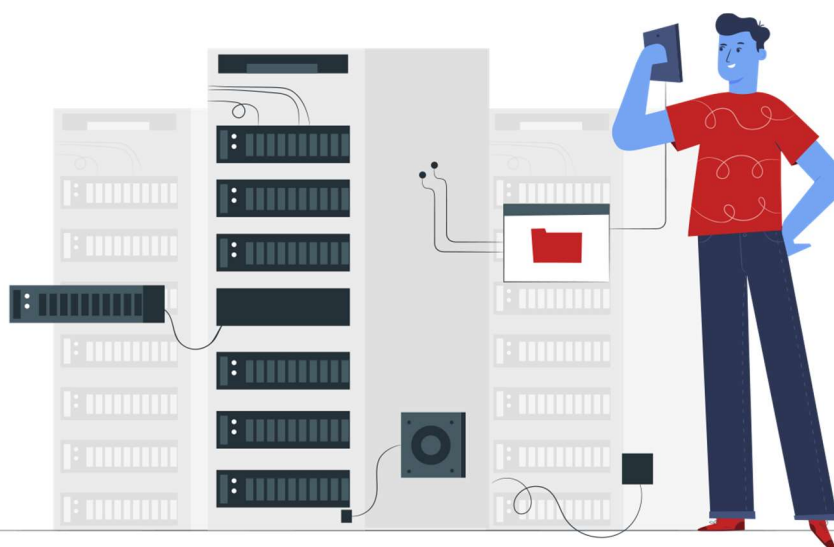


FortiAnalyzer

Installation et configuration

Une formation
Alphorm.com

Démo



FortiAnalyzer

Installation et configuration

Une formation
Alphorm.com

Configurer les ADOM et RAID



Mohamed Anass EDDIK



Plan

Mode ADOM
Types RAID

Une formation
Alphorm.com



Mode ADOM

Normal : il ne peut pas assigner les VDOMs du Fortigate depuis un seul équipement à plusieurs ADOMs du FortiAnalyzer

Avancé : pour assigner les VDOMs du Fortigate depuis un seul équipement vers plusieurs ADOMs du FortiAnalyzer

Une formation
Alphorm.com

FortiAnalyzer

Installation et configuration

Types RAID

RAID Basique a deux types d'opérations :

1. Mirroring
2. Striping

RAID Minimum est une miroir de 2 disques

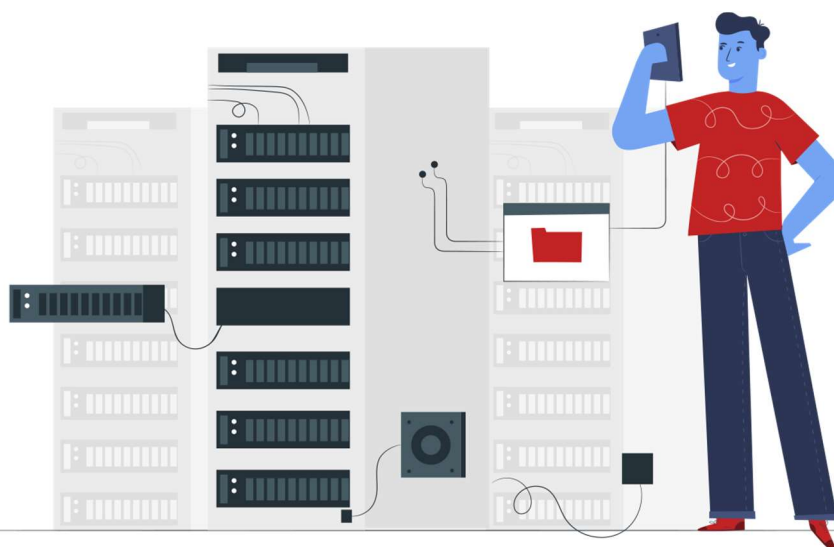
Pas toutes les versions RAID ont les mêmes
fonctionnement

Une formation
Alphorm.com

FortiAnalyzer

Installation et configuration

Démo



Une formation
Alphorm.com



Enregistrer et manager les équipements



Mohamed Anass EDDIK

Une formation
Alphorm.com



Plan

Méthodes d'enregistrement des
équipements

Quels logs sont collectés ?

Une formation
Alphorm.com



Méthodes d'enregistrement des équipements

Méthode 1 :

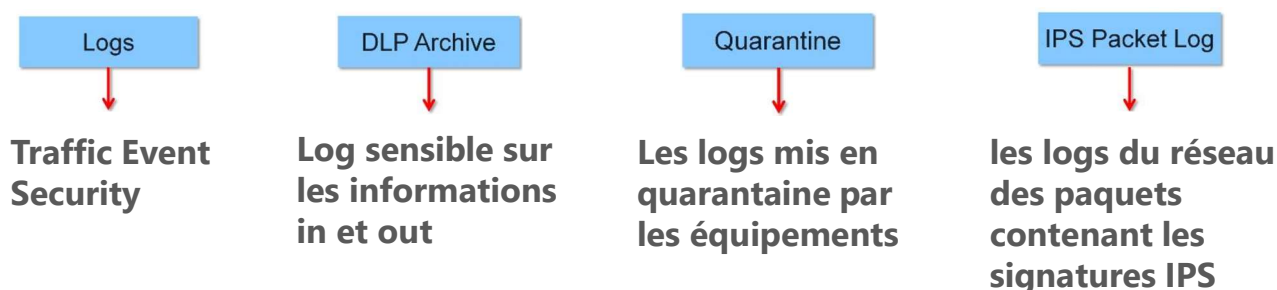
Demande depuis l'équipement (Fortigate)

Méthode 2 :

Enregistrement d'équipement via l'assistant

Une formation
Alphorm.com

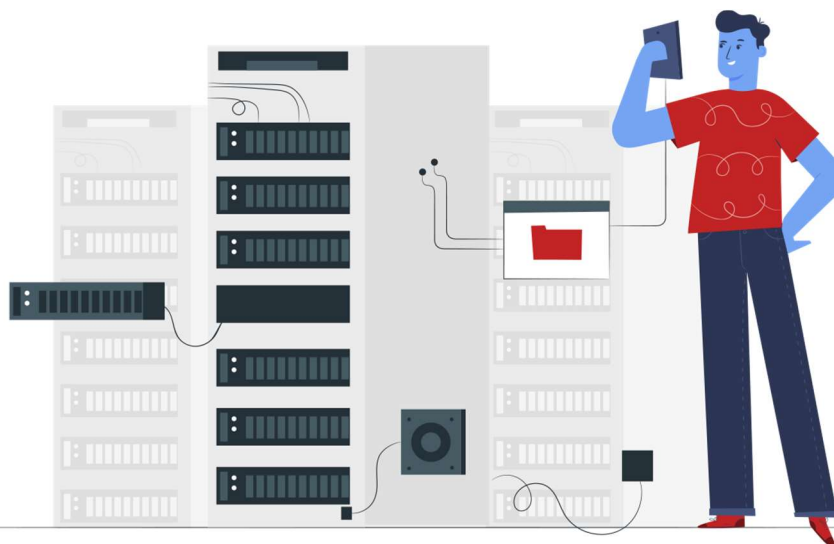
Quels logs sont collectés ?



FortiAnalyzer

Installation et configuration

Démo



Une formation
Alphorm.com

FortiAnalyzer

Installation et configuration

Gérer les problèmes de communication

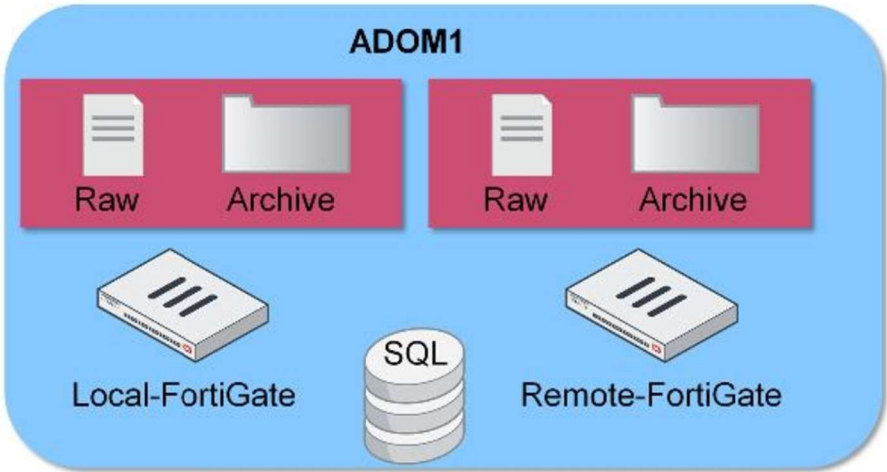


Mohamed Anass EDDIK

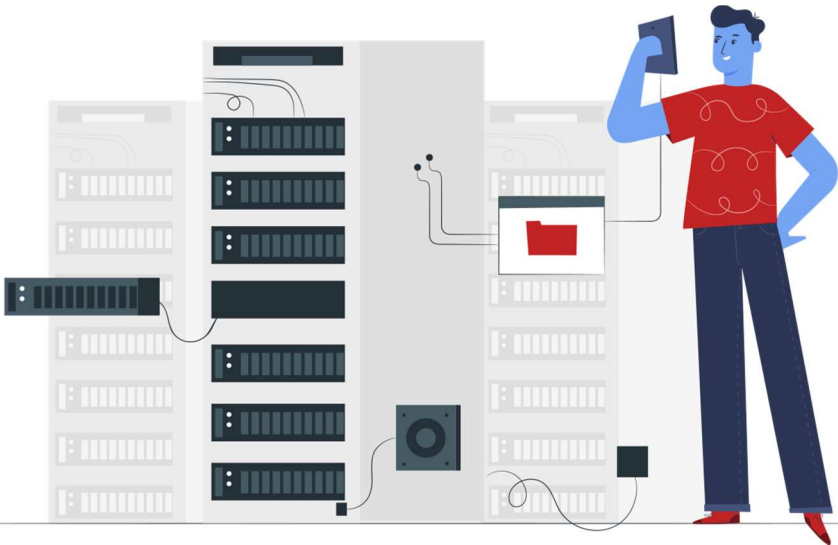
Une formation
Alphorm.com



Quota du disque



Démo



FortiAnalyzer

Installation et configuration

Une formation
Alphorm
com

Gérer les logs



Mohamed Anass EDDIK

FortiAnalyzer

Installation et configuration

Une formation
Alphorm
com

Plan

Types de log par équipement
Le workflow d'un fichier de log

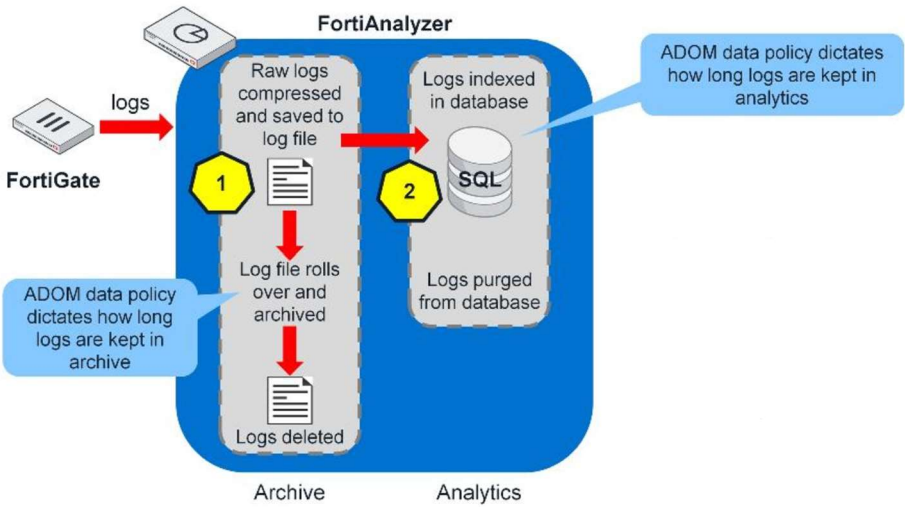


Types de log par équipement

Device	Log type
FortiGate	- Traffic [forward, local, sniffer] - Event [Endpoint, High Availability, System, User, Router, VPN, WAD, Wireless] - Security [Application Control, AntiVirus, Data Leak Prevention (DLP), Anti-Spam, Web Filter, Intrusion Prevention System (IPS), Anomaly (DOS-policy), WAF]
FortiCarrier	Traffic, Event
FortiCache	Traffic, Event, AntiVirus, Web Filter
FortiClient	Traffic, Event
FortiMail	History, Event, AntiVirus, Email Filter
FortiManager	Event
FortiSandbox	Malware, Network Alerts
FortiWeb	Event, Intrusion Prevention System (IPS), Traffic
Syslog	Generic

Une formation
Alphorm.com

Le workflow d'un fichier de log

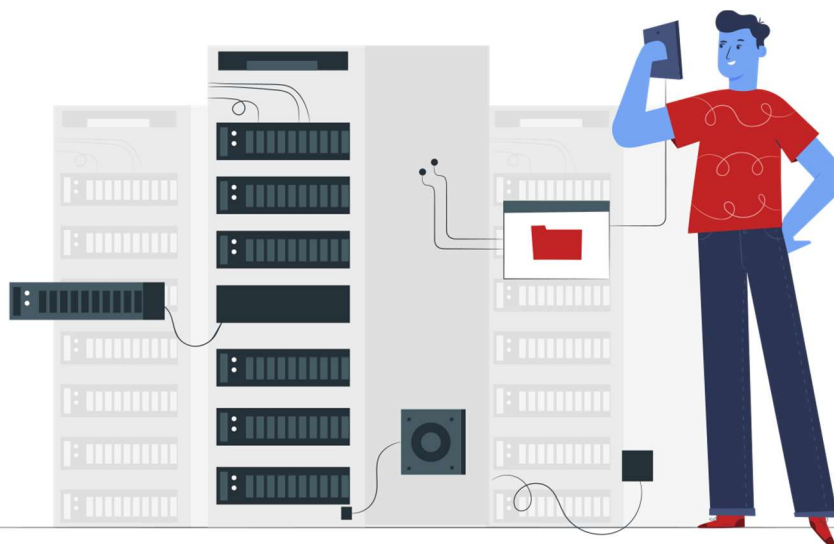


FortiAnalyzer

Installation et configuration

Une formation
Alphorm.com

Démo



FortiAnalyzer

Installation et configuration

Une formation
Alphorm.com

Diagnostiquer et gérer les logs



Mohamed Anass EDDIK



Une formation
Alphorm.com

Connaître les Types de Rapports



Mohamed Anass EDDIK



Une formation
Alphorm.com

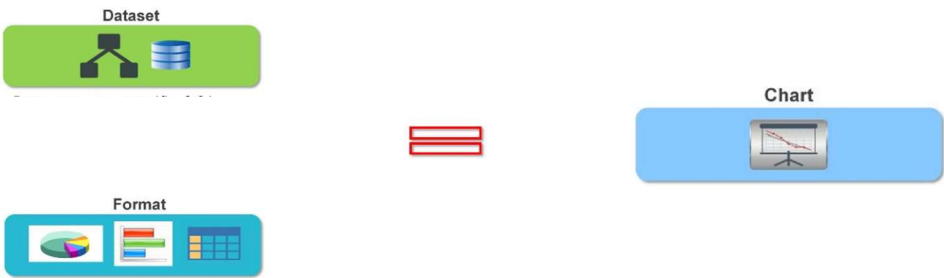
Plan

Les éléments qui composent
un rapport

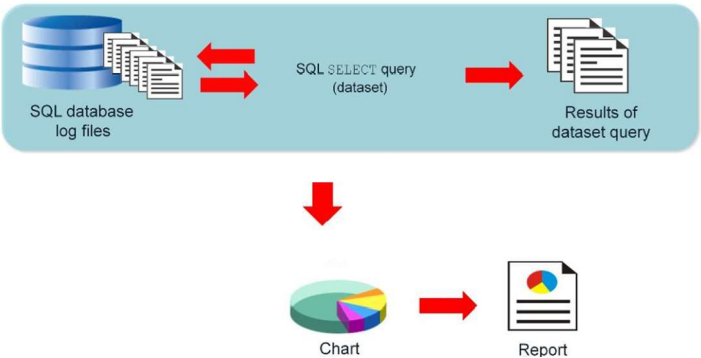
Rapport Workflow



Les éléments qui composent un rapport



Rapport Workflow

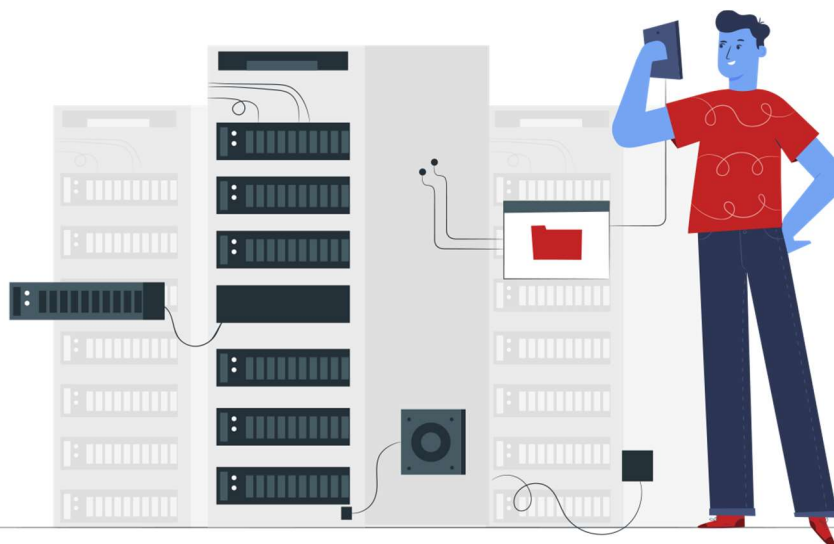


FortiAnalyzer

Installation et configuration

Une formation
Alphorm.com

Démo



FortiAnalyzer

Installation et configuration

Une formation
Alphorm.com

Personnaliser les rapports



Mohamed Anass EDDIK

FortiAnalyzer

Installation et configuration

Charts/Datasets prédéfinie

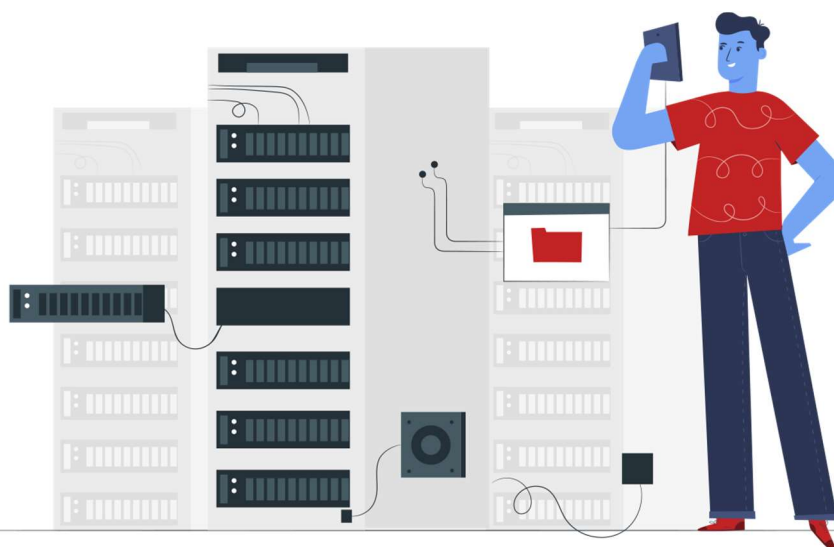
Par défaut, la librairie de graphique contient
plus de 300 Graphique
Par défaut, le librairie du Dataset contient
près de 400 datasets

Une formation
Alphorm.com

FortiAnalyzer

Installation et configuration

Démo



Une formation
Alphorm.com



Une formation
Alphorm.com

Gérer les rapports



Mohamed Anass EDDIK



Une formation
Alphorm.com

Conclusion



Mohamed Anass EDDIK



Bilan

Introduction au FortiAnalyzer

Administrer et manager le FortiAnalyzer

Enregistrer les équipements et
communication

Logging

Rapports

Une formation
Alphorm
com

