SUJET TFE

CONCEPTION ET IMPLEMENTATION D'UN SYSTEME DE SURVEILLANCE ET D'ALERTE EXTERNE D'UNE INFRASTRUCTURE RESEAU MODULAIRE

Objectifs

Mettre en place une solution permettant de faciliter une intervention en temps réel sur les défaillances d'un système réseau.

Contraintes

Les différentes problématiques liées à l'infogérance dans un réseau de nos jours nécessitent de mieux prendre des dispositions afin de toujours avoir un état de son réseau et de le rendre le plus disponible possible ceci pour diverses raisons.

But

Dans le souci de mieux gérer et contrôler l'activité de notre infrastructure, notre but sera de le réaliser tout en tenant compte des différentes mesures suivantes à savoir : les mesures de performances, les mesures de disponibilité et les mesures d'intégrité.

Il sera donc question pour nous d'être informer ou d'être notifier en temps réel des possibles cas de problèmes, d'activité interrompu et de l'état de notre réseau qui peut être dû à une coupure d'électricité, coupure d'internet etc.

Cahier des charges

Ce travail se déroulera en deux parties.

PREMIERE PARTIE

Dans cette partie nous mettrons en place l'ossature (machines et services) dont on aura besoin.

- Une **VM (VMWare) Debian** configurée et fonctionnel plus un script .sh pour tout réinstaller :

  - Apache
    - PHP 7.2
    - SSL (Let's Encrypt)
  - MySQL Server
    - Initialisée par un script SQL
      - Si possible créer des variables pour les MDP des utilisateurs
    - Backup automatique vers le NAS
    - Cible de réplication pour la DB en docker de Zabbix Server et Proxy
    - Voir si possible de répliquer en temps réel sur une DB OVH
    - **PostgreSQL** pour remplacer MySQL, Utile ? à déterminer
      - Initialisée par un script SQL
      - Si possible créer des variables pour les MDP des utilisateurs
    - Backup automatique vers le NAS
    - Cible de réplication pour la DB en docker de Zabbix Server et Proxy
  - MongoDB
    - Peu servir pour la gestion des fichiers Backup ? (à dterminer si utile)
      - pfSense
      - Images disque VM et physique

    Avantage/inconvénient : MongoDB **VS** MySQL
  - Nextcould
    - Vhost Apache
  - Gitea
    - Rediriger par un vhost Apache
  - TeaSpeak with YouTube-dl

- sharelatex (Docker)
  - Rediriger par un vhost Apache
- OpenLDAP
- Zabbix-agent

- Pouvoir implémenter l'équivalent de la VM Debian en Docker avec volumes et variables : l'idéal serait d'avoir la VM construite plus haut dans un environnement docker

Docker car le but est de passer un maximum des services sous docker

A cet effet ces trois solutions s'offrent à nous.

- VSphere Integrated Containers
  - Configuration
  - Docker-compose ?
  - Fonctionnement
  - Point positifs / négatifs
- VMWare Photon OS
  - Configuration
  - Docker-compose ?
  - Fonctionnement
  - Point positifs / négatifs
- GUI (Portainer,)
  - Quelles sont celle disponible ?
  - Point positifs / négatifs
  - Fonctionnement
    - Possibilité de modification manuelle ?
    - Compatible docker compose ?
    - Gestion volume et variable ?
  - Chemin personnaliser pour les volumes ?
  -

Une étude approfondie définira quel outil sera le mieux adapter pour notre travail.

- **Monitoring** : nous définirons

- Un serveur externe au réseau (cloud, amis,… à déterminer) pour monitorer les services important . Dans la situation envisager ce dernier sera en failover avec un autre serveur situer à l'intérieure du réseau (à déterminer si utile).

- Serveur sous Docker avec volumes et variables
  - DB aussi sous docker
    - Réplication en réel sur la principale

        - Backup journalier sur le NAS
    - Notification par mail et sur Discord
- Un server local sous Debian (plus script pour installation et config) et en Docker (+DB local) avec volumes et variables,
    - Notification par mail et Discord
    - Zabbix Proxy

DEUXIEME PARTIE

Dans cette partie nous exploiterons l'ensemble des éléments à implémenter cités plus haut pour Pouvoir monitorer :

- pfSense :
    - Utilisation cpu/ram, hdd
    - Statistique réseau : trafic en sur chaque interface (+/- temps réel, trafic écouler sur la journée, la semaine, le mois, total) plus éventuellement par protocoles
    - Logs pare-feu (20 derniers au moins)
    - Etat des dynDNS, des services, des interfaces
    - Client connecter sur les LANs, VPN et leurs IP/MAC
- VMWare ESXI :
    - Utilisation cpu/ram, hdd
    - Température du cpu, hdd
    - Etats des VM (On/Off)
        - Utilisation cpu/ram, hdd
- Docker :
    - Etats des contenaire (On/Off)
    - Utilisation cpu/ram, hdd
- Linux :
    - Utilisation cpu/ram, hdd
    - Etats des services importants
        - SSH
        - MySQL
        - TeamSpeak/Teaspeak
            - Etat de chaque server (On/Off)
            - Nombre de client connecter/par server
        - VOIP (Asterisk)
        - Git (Gitea)
        - Web (Apache/Nginix)
        - Docker-engine

- LDAP

- Windows Server :
  - Utilisation cpu/ram, hdd
  - Etats des services importants
    - AD
    - DNS
    - DHCP
- Réseau
  - Wifi
    - Etat du contrôleur Unifi
      - Reprendre les infos du contrôleur
      - Client connecter par SSID
      - Etats des APs
      - Logs (20 derniers au moins)
  - Switch (Cisco SG500-28P)
    - Etats
    - Ports
      - Statut
      - POE
- Nas (Synology et Qnap)
  - Etats (On/Off)
  - Utilisation cpu/ram, hdd
  - Température du cpu, hdd
  - Etats des RAID, évènement SMART
  - Infos réseau /interface
    - Etats
    - Trafic (+/- temps réel, trafic écouler sur la journée, la semaine, le mois, total)
  - Utilisateurs connectés
  - Logs (20 derniers au moins)
  - Etats de services
    - Docker/VM
      - Etats (On/Off)
      - Utilisation cpu/ram, hdd
    - SMB
    - HTTP(S), SSH
    - Rsync
      - Date et heures du dernier backup
      - Infos backup (réusis, raté > log)