Déploiement de la solution Supervision CheckMK

Ershad Ramezani

Table des matières

Introduction

OcciTech est une entreprise qui fournit des services d'infrastructure et d'hébergement dans la région Occitanie.

Suite à un audit, il a été décidé de changer la solution de surveillance actuelle basée sur Nagios pour une solution similaire technique afin de conserver les compétences acquises.

La demande

Durant ce projet, dans un premier temps, nous devons prendre en main une solution et construire une maquette représentative de l'infra à superviser.

Dans la première partie de votre étude, on se limitera au parc du Datacenter **OcciTech**, situé à Montpellier qui est constitué de serveurs sous Linux hébergeant des applications Web et des SGBDR[1], serveurs Sous Windows, switchs et routeurs Cisco.

Pour tous les serveurs, on surveillera les ressources communes comme :

- Joignable par Ping
- RAM (avertissement si RAM restant entre 20% et 10%, critique en dessous de 10%)
- Espace disque (avertissement si espace disque restant entre 20% et 10%, critique en dessous de 10%)
- Utilisation CPU (avertissement si CPU restant entre 20% et 10%, critique en dessous de 10%)

En plus de ces composants de base, sur les serveurs on supervisera le fonctionnement du service installé (apache, IIS, MySQL, MariaDB, SQL Server etc.).

Pour optimiser la méthode de supervision, les nœuds seront regroupés par groupes. Nous allons concevoir une maquette comportant les différents éléments à superviser, proposer une méthode qui facilitera leur supervision et intégrer facilement les nouveaux éléments le plus simplement possible.

La solution proposée : Checkmk

Checkmk est un outil créé pour surveiller les éléments de l'informatique tels que les serveurs, les applications, les réseaux, les infrastructures cloud, les conteneurs, les bases de données et les capteurs environnementaux.

Checkmk est un meilleur remplacement pour Nagios car il permet une migration facile depuis Nagios et offre de nombreux autres avantages :

- Il est simple et rapide à installer sur différentes plateformes ou dans un conteneur Docker.
- Il permet de transférer facilement tous les objets de surveillance Nagios existants, comme les hôtes, les groupes d'hôtes et les utilisateurs, vers Checkmk.
- La fonction de découverte automatique, disponible uniquement dans la version payante, détecte automatiquement les services et propose des métriques et des seuils adaptés.
- Les plug-ins Nagios existants peuvent également être facilement migrés vers Checkmk.
- La surveillance peut être étendue à des centaines de sites et des millions d'appareils, tous gérables depuis un emplacement central.

Schéma de projet

Nous allons commencer par la création d'un laboratoire qui présentera le datacenter de la société OcciTech. Ce labo comprendra :

- **Équipements réseau :** un routeur/pare-feu standard et un commutateur Cisco 3750
- **Serveurs virtuels :** le serveur Checkmk, Windows server 2016 (Active Directory et DHCP), Linux Debian (Serveur web Apache et MariaDB)

[1] Un système de gestion de BD relationnelles (SGBDR) est un logiciel standard qui repose sur les principes du modèle relationnel.

Ensuite, nous allons explorer les diverses options offertes par Checkmk pour optimiser la surveillance du réseau de l'entreprise, comme le regroupement des nœuds, des seuil d'alertes, des notifications par e-mail, etc.

Sur mon serveur Windows, j'ai créé :

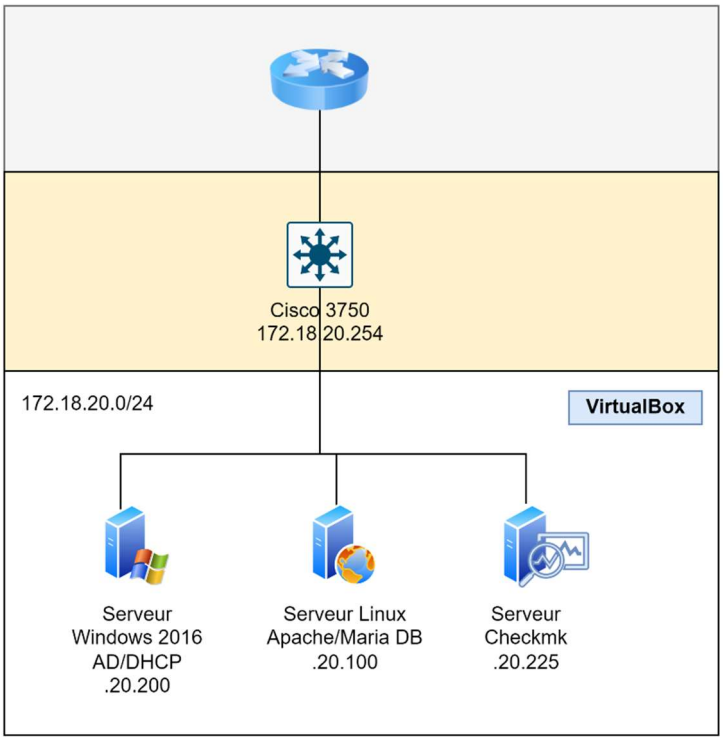
- Un domaine AD nommé occitech.local
- Un domaine DNS pour occitech.local avec un enregistrement pour le site web occitech.local
- Un serveur DHCP avec une plage d'adresses IP allant de 172.18.20.1 à 172.18.20.20

Sur mon serveur linux, j'ai mis en place :

- Un serveur MariaDB avec une base de données intitulée "occitech"
- Un serveur Apache2 avec un site web https://occitech.local (le protocole https est activé avec un certificat auto-signé)

Il est simple de trouver les tutoriels pour configurer ces services sur internet.

Remarque : Tous les ports réseau sont configurés en mode pont pour permettre une communication avec le commutateur et l'ensemble du réseau.



Installation du Checkmk

Choisir une édition

Avant de commencer à installer Checkmk, il faut choisir quelle édition nous voulons utiliser parmi les différentes options qui sont proposées :

- La version gratuite de Checkmk, appelée Checkmk Raw Edition (CRE), est entièrement open-source et utilise Nagios comme base pour surveiller des environnements complexes.
- La Checkmk Enterprise Standard Edition (CEE) est destinée aux utilisateurs professionnels et offre des fonctionnalités supplémentaires par rapport à la version Raw.
- La Checkmk Enterprise Free Edition (CFE) est idéale pour tester la version Standard sans engagement ou pour surveiller jusqu'à 25 hôtes. Cette version gratuite inclut toutes les fonctionnalités de la version standard et est illimitée pendant les 30 premiers jours. Nous avons choisi cette édition pour notre laboratoire.

Choisir la méthode d'installation

Le serveur Checkmk a besoin d'un système d'exploitation Linux pour fonctionner. Il existe quatre options disponibles qui sont installées de façons différentes.

- L'installation de Checkmk est courante sur un **serveur Linux**, qu'il soit en physique ou en virtuel. Les systèmes d'exploitation compatibles sont Debian/Ubuntu, CentOS/Red Hat et SUSE.
- Il est possible d'utiliser **l'Appliance virtuelle Checkmk virt1**, qui est une machine virtuelle avec un format OVA, pouvant être utilisée sur des hyperviseurs tels que VirtualBox ou VMware ESXi.
- Pour une utilisation physique, il est possible d'utiliser une **application préinstallée** et prête à l'emploi directement sur un appareil à installer dans notre datacenter.
- Les éditions Raw et Enterprise sont disponibles avec des images de conteneur (**Docker**) prêtes à l'utilisation.

Nous allons installer Checkmk sur un serveur linux Ubuntu 22.04 virtualisé sur VirtualBox.

Installation sur Ubuntu

Préparer le serveur linux

Suivez ce lien pour installer une machine Ubuntu 22.04 sur VirtualBox :

https://www.how2shout.com/linux/how-to-install-ubuntu-22-04-server-on-virtualbox/

Nous allons mettre en place une configuration de pont d'accès réseau pour connecter notre serveur au reste du réseau, y compris le commutateur.

Vérifiez l'heure et la date avec la commande *date*. Configurez le *time zone* si besoin avec la commande suivante :

```
sudo timedatectl set-timezone Europe/Paris
```

Configurez l'adresse IP en statique en créant ce fichier :

```
sudo vim /etc/netplan/01-netcfg.yaml
```

Avec ce contenu :

```
network:
  version: 2
  renderer: networkd
  ethernets:
    enp0s3:
      addresses:
        - 172.18.20.225/24
      nameservers:
        addresses: [172.18.20.200]
      routes:
        - to: default
          via: 172.18.20.254
```

Utilisez la commande sudo netplan apply pour appliquer la nouvelle configuration d'adresse IP

Il est important de noter que le serveur DNS mentionné dans ce fichier est celui qui se trouve sur le serveur AD local. Cela est crucial si l'on souhaite ajouter les noms de nos serveurs et services (web, AD, ftp, etc.) plutôt que leurs adresses IP lors de l'ajout des hôtes dans Checkmk.

Installer le paquet Checkmk

Suivez ce lien pour télécharger et installer la dernière version du paquet Checkmk sur un Ubuntu 22.04.

```
https://checkmk.com/download
```

Téléchargez le fichier *.deb* avec cette commande :

```
sudo wget https://download.checkmk.com/checkmk/2.1.0p14/check-mk-free-2.1.0p14_0.jammy_amd64.deb
```

Mettre à jour la liste des miroirs et mettre à niveau le système :

```
sudo apt update && sudo apt upgrade
```

Installez maintenant le paquet qui comprend toutes ses dépendances avec cette commande :

```
sudo apt install ./check-mk-free-2.1.0p14_0.jammy_amd64.deb
```

Vérifiez la version avec cette commande. Cela permettra si l'installation est finie avec succès :

```
omd version
```

Vous allez avoir cette réponse dans le terminal :

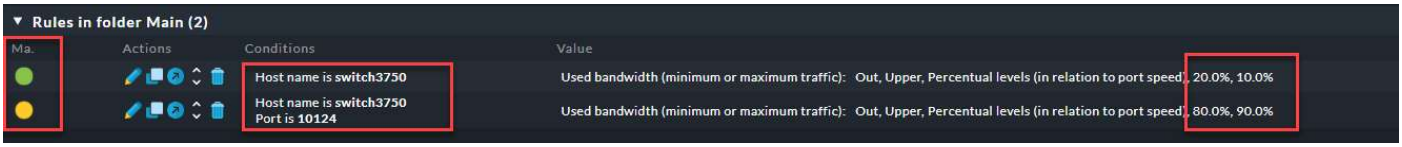
```
OMD - Open Monitoring Distribution Version 2.1.0p14.cfe
```

Utilisez la commande *omd* pour créer un nouveau site Checkmk. Vous pouvez choisir votre propre nom, dans cet exemple nous avons nommé le site « *test_site » :*

La version complète est disponible aussi mais protéger par un mot de passe.

Merci de me contacter par email :

Ershad.ra@gmail.com



La deuxième règle étant de couleur jaune, cela signifie qu'elle est liée à un service, mais n'est pas en vigueur car une autre règle ayant une priorité plus élevée est en cours d'application.

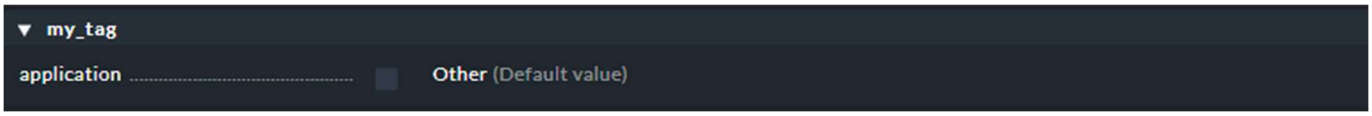
Configurer des balises d'hôte (host tags)

Les règles sont limitées aux hôtes en fonction de la présence ou non de balises d'hôte spécifiques.

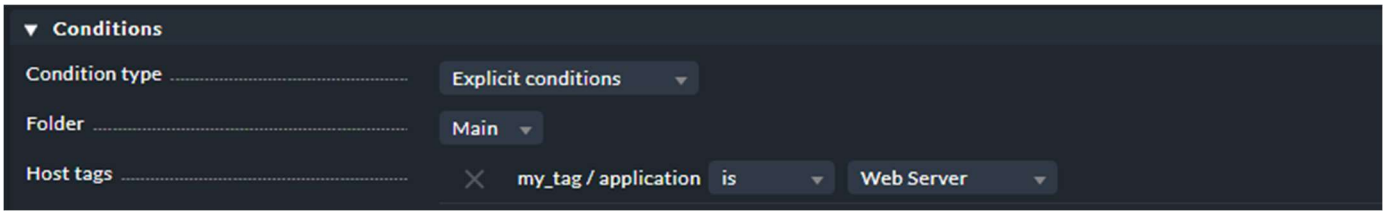
Pour illustrer, imaginons qu'on souhaite créer des balises pour les différents services disponibles sur notre réseau. Pour ce faire, il suffit d'accéder à l'onglet "setup/hosts/tags/add tag group" et de créer un groupe de balises intitulé "application". On peut ensuite ajouter un sujet, ici "my_tag", et y inclure 3 balises distinctes :

Sauvegardez les modifications et appliquez les changements :

Retournez à la liste des hôtes (setup/hosts/hosts) et modifiez la configuration d'un hôte en attribuant la catégorie "Web servers" :

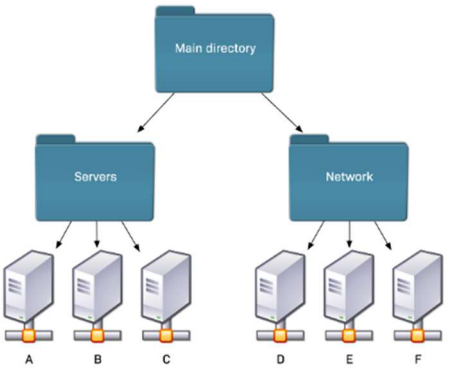


Puis allez dans une règle, par exemple CPU load (*setup/service monitoring rules*), et définissez sa *conditions* par des balises. Désormais cette règle sera appliquée seulement aux hôtes qui ont la balise *Web Server* :



Dossiers et héritage

Checkmk utilise une structure hiérarchique de dossiers pour gérer les hôtes. En créant cette arborescence, vous pouvez bénéficier de l'héritage des attributs.

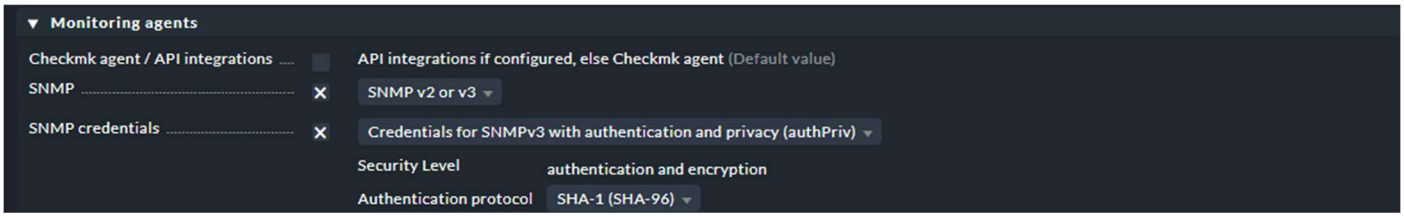


Crée un dossier depuis *setup/hosts/add folder*

Ajoutez des hôtes dans ces dossiers

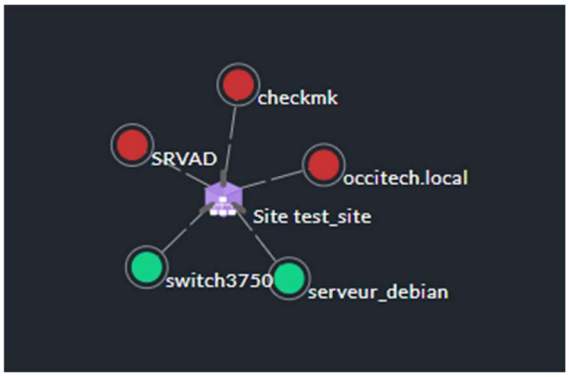
Allez dans la configuration de dossier :

En configurant un dossier, toutes les modifications apportées seront appliquées à tous les hôtes qui se trouvent dans ce dossier. Par exemple, on peut ajouter un tag ou configurer le type d'agent pour tous les hôtes simultanément. Il est également possible de définir l'agent SNMP v3 pour tous les switches en définissant les identifiants sur un dossier plutôt que de le faire individuellement pour chaque switch.



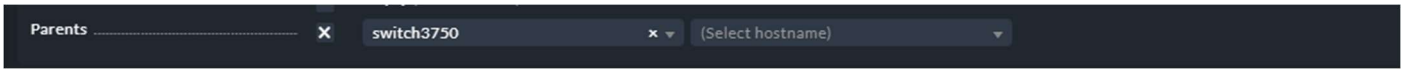
Topologie du réseau

Cet outil permet de déterminer les objets parent et de limiter les notifications inutiles. A titre d'exemple, dans notre laboratoire, nous avons un commutateur et plusieurs serveurs qui sont tous reliés directement au serveur Checkmk.



Si les serveurs sont connectés à un switch et que le trafic doit passer par ce dernier pour atteindre Checkmk, le switch jouera le rôle de parent. En cas de panne de ce switch, Checkmk sera conscient que les autres commutateurs ou serveurs connectés à celui-ci ne sont pas accessibles, et la situation sera considérée comme UNKNOWN plutôt que DOWN. Il ne déclenchera donc pas de notification pour ces équipements.

Pour définir la configuration parents, allez dans les paramétrage d'un hôte et la section Basic Settings :



J'ai relié le switch 3750 en tant que parent du serveur Debian. Voici la nouvelle topologie :

Maintenant, je vais mettre le switch hors tension pour vérifier l'impact sur la topologie réseau. (Note: Au lieu de mettre le switch hors tension, nous pouvons également modifier l'adresse IP dans la configuration de l'hôte pour obtenir le même résultat).