Documentation

CheckMK

Solution de supervision + Caddy

Eythan RONCIER-LEMEE
29/03/2026

Sommaire

1. Prérequis 2

1.1. Système & Matériel 2

1.2. Réseau 2

2. Installation du moteur Docker 2

2.1. Désinstallation des paquets conflictuels 2

2.2. Installation de Docker CE 2

2.3. Vérification de l'installation 2

3. Génération des certificats locaux 3

3.1. Installation & mise en place mkcert 3

3.2. Génération des certificats 3

4. Déploiement CheckMK & Caddy 4

4.1. Préparation de l'arborescence 4

4.2. Création du Caddyfile 4

4.3. Création du docker-compose.yml 4

4.4. Lancement du stack 5

5. Supervision : Installation et enregistrement de l'Agent 5

5.1. Lancement du stack ..... **Erreur ! Signet non défini.**

5.2. Lancement du stack ..... **Erreur ! Signet non défini.**

5.3. Lancement du stack ..... **Erreur ! Signet non défini.**

6. Ajout de l'hôte dans le panneau d'administration 6

7. Application des changements (Activation) 7

1. Prérequis

1.1. Système & Matériel

- **OS principal (Serveur de supervision) :** Debian 12 (Bookworm) ou Debian 13 (Trixie).
- **Ressources recommandées :** Minimum 4 Go de RAM et 2 vCPU
- **Navigateurs compatibles :** Google Chrome >= 131 ; Firefox >= 133 ; Microsoft Edge >= 131 ; Safari >= 18.1.
- **Seconde machine :** Une machine cible (Windows ou Linux) qui fera office de premier hôte à superviser.

1.2. Réseau

- Le serveur doit avoir une IP statique.
- Un enregistrement DNS local (ou une entrée dans le fichier hosts de votre poste client) pour résoudre le nom d'hote de la supervision vers l'IP du serveur Debian.

2. Installation du moteur Docker

2.1. Désinstallation des paquets conflictuels

Cette commande supprime proprement tout résidu d'anciennes installations Docker :

```
apt remove $(dpkg --get-selections docker.io docker-compose docker-doc podman-docker containerd runc | cut -f1)
```

2.2. Installation de Docker CE

Nous allons ajouter le dépôt officiel de Docker pour garantir d'avoir les dernières mises à jour de sécurité.

```
# 1. Mise à jour et installation des outils nécessaires
apt update
apt install -y ca-certificates curl

# 2. Création du dossier pour la clé GPG et téléchargement de celle-ci
install -m 0755 -d /etc/apt/keyrings
curl -fsSL https://download.docker.com/linux/debian/gpg -o /etc/apt/keyrings/docker.asc
chmod a+r /etc/apt/keyrings/docker.asc

# 3. Ajout du dépôt Docker aux sources APT
tee /etc/apt/sources.list.d/docker.sources <<EOF
Types: deb
URIs: https://download.docker.com/linux/debian
Suites: $(. /etc/os-release && echo "$VERSION_CODENAME")
Components: stable
Signed-By: /etc/apt/keyrings/docker.asc
EOF
```

```
# 4. Installation des composants Docker
apt update
apt install -y docker-ce docker-ce-cli containerd.io docker-buildx-plugin
docker-compose-plugin
```

2.3. Vérification de l'installation

Assurez-vous que le service est actif et démarre au boot :

```
systemctl enable --now docker
systemctl status docker
docker run --rm hello-world # Doit afficher "Hello from Docker!"
```

3. Génération des certificats locaux

3.1. Installation & mise en place mkcert

Puisque nous sommes sur un domaine local (`.lan`), Let's Encrypt ne peut pas fonctionner. `mkcert` permet de créer une Autorité de Certification (CA) locale pour générer des certificats valides.

```
mkdir -p /var/opt/certif
cd /var/opt/certif

# Téléchargement de mkcert
curl -sSL
https://github.com/FiloSottile/mkcert/releases/latest/download/mkcert-v1.4.4-
linux-amd64 -o /usr/local/bin/mkcert
chmod +x /usr/local/bin/mkcert

# Initialisation de l'autorité de certification locale
mkcert -install
```

3.2. Génération des certificats

Une fois l'installation et la mise de mkcert dans le dossier /bin/bash on va désormais générer nos certificats dans le dossier crée.

```
# Génération des certificats avec les noms exacts attendus par Caddy
mkcert -cert-file supervision.domain.lan.crt -key-file
supervision.domain.lan.key supervision.domain.lan

# Vérification de la présence des fichiers .crt et .key
ls -la
```

4. Déploiement CheckMK & Caddy

4.1. Préparation de l'arborescence

Nous allons déployer l'ensemble du stack via un seul fichier `docker-compose.yml`. Caddy gérera le HTTPS et redirigera le trafic vers le conteneur CheckMK.

```
mkdir -p /var/opt/checkmk
cd /var/opt/checkmk
```

4.2. Création du Caddyfile

Ce fichier indique à Caddy comment router le trafic et quels certificats utiliser. Créez-le fichier `/var/opt/checkmk/Caddyfile` :

```
Supervision.domain.lan {
    # Utilisation des certificats générés précédemment
    tls /certs/supervision.domain.lan.crt /certs/supervision.domain.lan.key
    # Redirection vers le port interne de CheckMK (5000)
    reverse_proxy checkmk:5000
}
```

4.3. Création du docker-compose.yml

Créez le fichier `/var/opt/checkmk/docker-compose.yml`

```
services:
  checkmk:
    image: "checkmk/check-mk-raw:2.4.0-latest"
    container_name: "supervision"
    ports:
      - "8000:8000" # Port requis pour la communication de l'agent (Agent
Receiver)
    environment:
      - CMK_PASSWORD=mypassword # À CHANGER : Mot de passe du compte
'cmkadmin'
      - TZ=Europe/Paris
    volumes:
      - supervision_data:/omd/sites
    tmpfs:
      # Optimisation : stocke les fichiers temporaires en RAM pour réduire
l'usure disque et améliorer les performances
      - /opt/omd/sites/cmk/tmp:uid=1000,gid=1000
    restart: always

  caddy:
    image: caddy:latest
    container_name: "caddy_proxy"
    ports:
```

```
      - "80:80"
      - "443:443"
    volumes:
      - /var/opt/certif:/certs:ro   # Montage des certificats en lecture seule
      - ./Caddyfile:/etc/caddy/Caddyfile:ro # Montage de la configuration
Caddy
    depends_on:
      - checkmk
    restart: always

volumes:
  supervision_data:
```

4.4. Lancement du stack

```
docker compose up -d
```

Vous pouvez maintenant accéder à l'interface via `https://supervision.domain.lan/cmk`. *(Identifiant par défaut : `cmkadmin` / Mot de passe : celui défini dans le compose).*

5. Supervision : Installation et enregistrement de l'Agent

Depuis la version 2.1, CheckMK utilise le "Agent Controller" qui chiffre les communications (TLS) entre l'agent et le serveur sur le port 8000. L'installation seule ne suffit plus, **il faut l'enregistrer**.

5.1. Récupération de l'agent

Depuis l'interface web (Panneau Admin) :

- Allez dans **Setup** (Configuration) > **Agents** > **Windows, Linux, Solaris, AIX**.
- Copiez le lien de téléchargement correspondant à votre OS (`.msi`, `.deb`, ou `.rpm`).

5.2. Déploiement sur Windows

- Téléchargez et double-cliquez sur l'installateur check_mk_agent.msi.
- Suivez les étapes (cochez l'installation propre si proposée).
- **Enregistrement TLS (Obligatoire) :** Ouvrez une invite de commande (CMD) **en mode Administrateur** et lancez :

```
"C:\Program Files (x86)\checkmk\service\cmk-agent-ctl.exe" register --hostname
NOM_DE_LA_MACHINE --server supervision.domain.lan --site cmk --user cmkadmin -
-password VOTRE_MOT_DE_PASSE_CMK
```

- Acceptez le certificat si on vous le demande. L'agent est maintenant prêt et sécurisé

5.3. Déploiement sur Linux (RPM & Debian based)

Sur la machine cible à superviser, téléchargez et installez l'agent :

```
# Exemple pour un paquet DEB.
# Remplacez l'URL par celle copiée depuis votre interface CheckMK
wget --no-check-certificate
https://bigbrother.eyrode.lan/cmk/check_mk/agents/check-mk-agent_2.4.0-
latest_all.deb

# Installation
dpkg -i check-mk-agent_2.4.0-latest_all.deb
# (Utilisez `rpm -ivh file.rpm` si vous êtes sur CentOS/RHEL/Rocky)

# Vérification que le service tourne
systemctl status cmk-agent-ctl-daemon.service
ss -pantul | grep 6556
```

Enregistrement TLS (Obligatoire) :

Exécutez la commande d'enregistrement pour lier l'agent au serveur (en remplaçant par vos valeurs) :

```
cmk-agent-ctl register \
    --server supervision.domain.lan \
    --site cmk \
    --user cmkadmin \
    --hostname NOM_DE_LA_MACHINE \
    --trust-cert
```

6. Ajout de l'hôte dans le panneau d'administration

Maintenant que l'agent est installé et enregistré, il faut déclarer la machine dans l'interface de CheckMK :

- Dans le menu de gauche, allez dans **Setup** > **Hosts** > **Hosts**.
- Cliquez sur **Add host**.
- **Hostname :** Entrez *exactement* le nom d'hôte (NOM_DE_LA_MACHINE) utilisé lors de la commande cmk-agent-ctl register.
- **IPv4 Address :** Cochez la case et entrez l'adresse IP de la machine cible.
- **Checkmk agent / API integrations :** Laissez sur API integrations if configured, else Checkmk agent (comportement par défaut).
- Cliquez sur **Save & go to service configuration**.
- CheckMK va scanner les services disponibles (CPU, RAM, Disques, Réseau...). Cliquez sur **Accept all** en haut de la page pour ajouter tous ces services à la supervision.

7. Application des changements (Activation)

Dans CheckMK, aucune modification n'est effective tant qu'elle n'est pas "activée".

- Cliquez sur le panneau jaune avec un point d'exclamation en haut à droite (qui indique "N changes").
- Cliquez sur le bouton **Activate on selected sites** pour pousser la configuration en production.
- Allez dans le menu **Monitor** > **All hosts** pour voir votre machine remonter ses métriques !