Centreon

Installation 22.10 sur CentOS 8

Pré requis

- CentOS 8
- 4 vcpu
- 4 Go de RAM

Installation

Paquets

Exécuter en tant que root

```
curl -L -s
https://raw.githubusercontent.com/centreon/centreon/22.10.x/centreon/unatten
ded.sh | sh
```

Noter le mot de passe mariaDB généré de façon aléatoire en fin d'installation.

Configuration générale

- Se connecter à l'interface web http://adresse_IP
- Suivre les indications au fur et à mesure Post installation

Passage en https

Générer un certificat autosigné

- Installer les paquets

```
dnf install mod_ssl mod_security openssl
```

- Générer un certificat autosigné

```
openssl genrsa -out ca.key 2048
openssl req -new -key ca.key -out ca.csr
openssl x509 -req -days 365 -in ca.csr -signkey ca.key -out ca.crt
```

```
mv ca.crt /etc/pki/tls/certs
mv ca.key ca.csr /etc/pki/tls/private
```

- Mettre à jour le fichier /etc/httpd/conf.d/ssl.conf

```
SSLCertificateFile /etc/pki/tls/certs/ca.crt
SSLCertificateKeyFile /etc/pki/tls/private/ca.key
```

- Redémarrer le service

```
systemctl restart httpd
```

Certificat Let's Encrypt

- Installer les paquets

```
dnf install certbot python3-certbot-apache mod_ssl
```

- Générer le certificat

```
certbot --apache -d <url> certonly
```

- Désactiver les fichiers de configuration

```
cd /etc/httpd/conf.d
mv welcome.conf welcome.conf.inhib
mv userdir.conf userdir.conf.inhib
mv autoindex.conf autoindex.conf.inhib
mv 10-centreon.conf 10-centreon.conf.inhib
```

- Interdire l'accès par défaut

Créer un fichier deny-all.conf

```
<VirtualHost _default_:80>
        ServerName xxx.xxx.xxx.xxx

        ErrorLog /var/log/httpd/error.log
        CustomLog /var/log/httpd/access.log combined

        <Directory />
                Deny from all
        </Directory>
</VirtualHost>

<VirtualHost _default_:443>
        ServerName xxx.xxx.xxx.xxx

        ErrorLog /var/log/httpd/error.log
        CustomLog /var/log/httpd/access.log combined
```

```
        SSLEngine on
        SSLCertificateFile
/etc/letsencrypt/live/url_du_site/fullchain.pem
        SSLCertificateKeyFile /etc/letsencrypt/live/url_du_site/privkey.pem

        <Directory />
                Deny from all
        </Directory>
</VirtualHost>
```

- Récupérer le fichier exemple de Centreon

```
cp /usr/share/centreon/examples/centreon.apache.https.conf /etc/httpd/conf.d
```

- Modifier les 2 lignes

```
    SSLCertificateFile    /etc/letsencrypt/live/url_du_site/fullchain.pem
    SSLCertificateKeyFile /etc/letsencrypt/live/url_du_site/privkey.pem
```

- Redémarrer le service

```
systemctl restart httpd
```

Sécurisation

Voir § Sécurisation du serveur

Haut de page

Installation ova pour VMWare

Création VM

Modification de la VM

- Créer la VM à partir du fichier OVA télécharger sur le site Centreon
- Ajouter une interface réseau
- Modifier éventuellement les paramètres de la VM avant de la démarrer

Modification de l'OS

- Se connecter avec utilisateur root, password centreon
- Changer le clavier en azerty : Changement clavier
- Modifier le mot de passe
- Configurer l'adresse IP : Configuration IP

- Changer le hostname

```
hostnamectl set-hostname nom_du_serveur
```

- Définir le fuseau horaire

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

- Définir le fuseau horaire pour PHP dans le fichier /etc/opt/rh/rh-php73/php.d/50-centreon.ini
- Prise en compte en redémarrant le service :

```
systemctl restart rh-php73-php-fpm
```

- Mise à jour du partitionnement de la base Centreon

```
su - centreon
/opt/rh/rh-php73/root/bin/php /usr/share/centreon/cron/centreon-
partitioning.php
exit
```

- Redémarrage des services centreon

```
systemctl restart cbd centengine gorgoned
```

Mise à jour de l'OS

```
yum update --nogpgcheck
```

Haut de page

Interface Centreon

Connexion

- Aller sur l'url http://ip_address/centreon
- Se connecter avec admin/<mot_de_passe>

Configuration

- Cliquer sur la tête en haut à droite
- Cliquer sur « Edit Profile »

Language

fr_FR

Timezone/Location

Europe/Paris

Mot de passe

Changer le mot de passe par défaut

Démarrage

Interface web

- A partir de l'interface cliquer en haut à gauche sur « Collecteurs » puis « Configurer les collecteurs »
- Sélectionner « Central » puis choisir « Exporter la configuration »
- Cocher « Déplacer les fichiers générés » et « Redémarrer l'ordonnanceur »

Console

- collect process

```
systemctl restart cbd centengine
```

- task manager

```
systemctl restart gorgoned
```

- passive monitoring

```
systemctl start snmptrapd centreontrapd
```

- Pour monitorer le serveur lancer le démon SNMP

```
systemctl start snmpd
```

Plugin packs

- Cliquer sur « Configuration / Gestionnaire de connecteurs de supervision »
- Choisir les plugin à installer en passant la souris au-dessus et en cliquant sur le +
- Une fois le plugin installé une coche verte apparait sur le plugin

SNMP

Il faut installer un serveur SNMP sur les serveur à superviser via SNMP (notamment les plugins Linux de base pour CPU, RAM, ...)

Installation

```
dnf install net-snmp net-snmp-libs net-snmp-utils
systemctl start snmpd
systemctl enable snmpd
```

Configuration

Utilisation

Titre

Goupes d'hôtes

Configuration > Hôtes > Groupes d'hôtes

Hôtes

Configuration > Hôtes > Hôtes

Haut de page

Sécurisation du serveur

Mots de passe

Modifier les mots de passe pour les utilisateurs :

- root
- centreon
- centreon-engine
- centreon-broker
- centreon-gorgone

SE Linux

Activation

Pour activer SE Linux en mode permissif modifier le fichier /etc/selinux/config

```
SELINUX=permissive
SELINUXTYPE=targeted
```

Puis redémarrage du serveur :

```
shutdown -r now
```

Installation packages centreon SE Linux

```
dnf install centreon-common-selinux centreon-web-selinux centreon-broker-selinux centreon-engine-selinux centreon-gorgoned-selinux centreon-plugins-selinux
```

Vérifier l'installation :

```
semodule -l | grep centreon
   centreon-broker 0.0.6
   centreon-common 0.0.11
   centreon-engine 0.0.10
   centreon-gorgoned       0.0.4
   centreon-plugins        0.0.2
   centreon-web    0.0.8
```

Accès fichiers

```
chown centreon:centreon /etc/centreon/conf.pm
chmod 660 /etc/centreon/conf.pm
chown apache:apache /etc/centreon/centreon.conf.php
chmod 660 /etc/centreon/centreon.conf.php
```

MariaDB

Exécuter le script de sécurisation proposé par MariaDB et répondre aux questions

```
mysql_secure_installation
```

firewalld

Installation

```
dnf install firewalld
systemctl start firewalld
systemctl enable firewalld
```

configuration

```
# For default protocols
firewall-cmd --zone=public --add-service=ssh --permanent
firewall-cmd --zone=public --add-service=http --permanent
firewall-cmd --zone=public --add-service=https --permanent
firewall-cmd --zone=public --add-service=snmp --permanent
firewall-cmd --zone=public --add-service=snmptrap --permanent
# Centreon Gorgone
firewall-cmd --zone=public --add-port=5556/tcp --permanent
# Centreon Broker
firewall-cmd --zone=public --add-port=5669/tcp --permanent
firewall-cmd --reload
```

Vérification

```
firewall-cmd --list-all
```

Fail2ban

Installation

```
dnf install python3-inotify epel-release fail2ban fail2ban-systemd
```

Mise à jour policy SE Linux

```
dnf update -y selinux-policy*
```

Configuration

Copier le fichier :

```
cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
```

Editer le fichier /etc/fail2ban/jail.local et ajouter la dernière ligne à la section [centreon]

```
port    = http,https
logpath = /var/log/centreon/login.log
backend  = pyinotify
```

Activation

Editer le fichier /etc/fail2ban/jail.d/custom.conf pour y ajoouter les lignes suivantes :

```
[centreon]
enabled = true
findtime = 10m
bantime = 10m
maxretry = 3
```

- maxretry : nombre d'échec d'authentification avant de bannir l'adresse
- bantime : durée du banissement
- findtime : intervalle pour chercher les échecs d'authentification

Redémarrer et activer le service :

```
systemctl restart fail2ban
systemctl enable fail2ban
```

> Il faut avoir essayé de se connecter au moins une fois pour que le fichier /var/log/centreon/login.log existe sinon le service ne démarre pas.

Vérification

Pour voir le status courant de la règle centreon :

```
fail2ban-client status centreon
```

Sécurisation apache

Installation module SSL

```
yum install httpd24-mod_ssl httpd24-mod_security openssl
```

Passage en https

Sauvegarder le fichier de conf apache d'origine :

```
cp /opt/rh/httpd24/root/etc/httpd/conf.d/10-centreon.conf{,.orig}
```

Modifier le fichier de configuration apache /opt/rh/httpd24/root/etc/httpd/conf.d/10-centreon.conf en prenant en compte les fichiers certificats qui vont bien :

```
Alias /centreon/api /usr/share/centreon
Alias /centreon /usr/share/centreon/www/
```

```
<LocationMatch
^/centreon/(?!api/latest/|api/beta/|api/v[0-9]+/|api/v[0-9]+\.[0-9]+/)(.*\.p
hp(/.*)?)$>
    ProxyPassMatch fcgi://127.0.0.1:9042/usr/share/centreon/www/$1
</LocationMatch>

<LocationMatch
^/centreon/api/(latest/|beta/|v[0-9]+/|v[0-9]+\.[0-9]+/)(.*)$>
    ProxyPassMatch fcgi://127.0.0.1:9042/usr/share/centreon/api/index.php/$1
</LocationMatch>

ProxyTimeout 300

<VirtualHost *:80>
    RewriteEngine On
    RewriteCond %{HTTPS} off
    RewriteRule (.*) https://%{HTTP_HOST}%{REQUEST_URI}
</VirtualHost>

<VirtualHost *:443>
######################
# SSL configuration #
######################
    SSLEngine On
    SSLProtocol All -SSLv3 -SSLv2 -TLSv1 -TLSv1.1
    SSLCipherSuite ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-
SHA256:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:DHE-DSS-
AES256-GCM-SHA384:DHE-DSS-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-SHA:ECDHE-
ECDSA-AES128-SHA:ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-
RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:AES256-GCM-SHA384:AES128-
GCM-
SHA256:!aNULL:!eNULL:!LOW:!3DES:!MD5:!EXP:!PSK:!DSS:!RC4:!SEED:!ADH:!IDEA
    SSLHonorCipherOrder On
    SSLCompression Off
    SSLCertificateFile /etc/pki/tls/certs/localhost.crt
    SSLCertificateKeyFile /etc/pki/tls/private/localhost.key

    <Directory "/usr/share/centreon/www">
        DirectoryIndex index.php
        Options Indexes
        AllowOverride all
        Order allow,deny
        Allow from all
        Require all granted
        <IfModule mod_php5.c>
            php_admin_value engine Off
        </IfModule>

        FallbackResource /centreon/index.html

        AddType text/plain hbs
```

```
    </Directory>

    <Directory "/usr/share/centreon/api">
        Options Indexes
        AllowOverride all
        Order allow,deny
        Allow from all
        Require all granted
        <IfModule mod_php5.c>
            php_admin_value engine Off
        </IfModule>

        AddType text/plain hbs
    </Directory>
</VirtualHost>

RedirectMatch ^/$ /centreon
```

Secure flags et masquage signature apache

Ajouter les lignes suivantes :

```
Header set X-Frame-Options: "sameorigin"
Header always edit Set-Cookie ^(.*)$ $1;HttpOnly;Secure
ServerSignature Off
ServerTokens Prod
TraceEnable Off
```

Editer le fichier /etc/opt/rh/rh-php73/php.d/50-centreon.ini et vérifier que le paramètre **expose_php** est à off

```
max_execution_time = 300
session.use_strict_mode = 1
session.gc_maxlifetime = 7200
expose_php = Off
date.timezone = Europe/Paris
```

Masquer le répertoire /icons

Editer le fichier /opt/rh/httpd24/root/etc/httpd/conf.d/autoindex.conf et mettre en commentaire la ligne suivante en ajoutant un # en début de ligne :

```
21. Alias /icons/ "/opt/rh/httpd24/root/usr/share/httpd/icons/"
```

Désactiver mod_security

Editer le fichier /opt/rh/httpd24/root/etc/httpd/conf.d/mod_security.conf et mettre en commentaire les 2 lignes suivantes :

```
29. SecRule MULTIPART_UNMATCHED_BOUNDARY "!@eq 0" \
30. "id:'200003',phase:2,t:none,log,deny,status:44,msg:'Multipart parser
    detected a possible unmatched boundary.'"
```

Prise en compte

Redémarrer les services php et apache :

```
systemctl restart rh-php73-php-fpm httpd24-httpd
```

Vérifier que le service apache a bien redémarré :

```
systemctl status httpd24-httpd
```

Activation http2

Installation module nghttp2

```
dnf install httpd24-nghttp2
```

Activation dans apache

Modifier le fichier de configuration apache /etc/httpd/conf.d/centreon.apache.https.conf

```
<VirtualHost *:443>
    Protocols h2 h2c http/1.1
    ...
</VirtualHost>
```

Modification configuration apache multi processeur

Modifier le fichier /etc/httpd/conf.modules.d/00-mpm.conf

Vérifier que le module mpm_prefork_module est en commentaire et que le module mpm_event_module est actif :

```
#LoadModule mpm_prefork_module modules/mod_mpm_prefork.so
```

```
LoadModule mpm_event_module modules/mod_mpm_event.so
```

Prise en compte

Redémarrer le service apache

```
systemctl restart httpd
```

Haut de page

Plugins

Scripts

Les plugins semblent se trouver maintenant sous /usr/lib/centreon/plugins et non plus sous /usr/lib/nagios/plugins.

Haut de page

Supervision

Serveur Linux

Debian/Ubuntu

- Installer les packages :

```
sudo apt-get install snmp snmpd snmp-mibs-downloader
```

- Autoriser le chargement des mibs en mettant en commentaire la ligne mibs du fichier de configuration /etc/snmp/snmp.conf

```
sudo sed -i 's/mibs :/# mibs :/g' /etc/snmp/snmp.conf
```

- Modifier le fichier /etc/snmp/snmpd.conf

```
rocommunity  public 127.0.01
rocommunity  public xxx.xxx.xxx.xxx
```

- Redémarrer le service

```
sudo systemctl restart snmpd
```

CentOS/Redhat

- Installer les packages :

```
sudo yum install net-snmp net-snmp-libs net-snmp-utils
```

- Modifier le fichier /etc/snmp/snmpd.conf

```
####
# First, map the community name "public" into a "security name"

#       sec.name  source          community
com2sec notConfigUser  <xxx.xxx.xxx.xxx>    public

####
# Second, map the security name into a group name:

#       groupName      securityModel securityName
group   notConfigGroup v1           notConfigUser
group   notConfigGroup v2c           notConfigUser

####
# Third, create a view for us to let the group have rights to:

# Make at least  snmpwalk -v 1 localhost -c public system fast again.
#       name           incl/excl     subtree         mask(optional)
view centreon included .1.3.6.1
view    systemview    included   .1.3.6.1.2.1.1
view    systemview    included   .1.3.6.1.2.1.25.1.1

####
# Finally, grant the group read-only access to the systemview view.

#       group          context sec.model sec.level prefix read   write
notif
access notConfigGroup    ""       any     noauth   exact centreon none
none
access  notConfigGroup ""      any       noauth    exact  systemview
none none
```

Centreon

Ajouter l'hôte dans Configuration / Hôtes / Hôtes et renseigner les informations

- nom, alias, adresse IP
- communauté et la version (v2c)

- serveur de supervision (Central)
- Fuseau horaire
- Commande de vérification base_centreon_ping
- Période de contrôle 24×7
- Dans l'onglet « Notification » indiquer « none » pour la période de notification

Aller dans Configuration / Hôtes / Groupes d'Hôtes

- Créer un groupe avec les serveurs Linux

Aller dans Configuration / Services / Services par Groupes d'Hôtes

- Créer des services liés au groupe précédent (OS-Linux-Cpu-SNMP, OS-Linux-Disk-Global-SNMP, OS-Linux-Memory-SNMP, Base-Ping-LAN)

Haut de page

Sources

Installation
Sécurisation plateforme
Plugin packs

Haut de page

From:
https://wiki.iot-acs.fr/ - **Wiki**

Permanent link:
https://wiki.iot-acs.fr/doku.php?id=all:bibles:linux:serveur:centreon

Last update: **2024/06/14 11:10**