Eset Protect sur Debian Buster

Pour les besoins, je crée une VM avec 2Go de Ram et 4Go de Swap.

(Fix Me!) Encore à réaliser dans ce document:

- ~~Certificats pour l'interface Web~~
- Intégration active-directory

Installation

Installation MySQL

1. Faire une mise à jour du système

```
apt update
apt dist-upgrade
```

2. Installer deux parquets nécessaires

```
apt install gnupg lsb-release
```

3. Télécharger la source de paquets pour MySQL

```
wget https://dev.mysql.com/get/mysql-apt-config_0.8.14-1_all.deb
```

4. Installer le paquet

```
dpkg -i mysql-apt-config_0.8.14-1_all.deb
```

⇒Laisser le choix sur la version ***8.0*** et faire OK

5. Mettre à jour les dépots et installer mysql-server ainsi que d'autres paquets nécessaires à Eset SMC.

```
apt update
apt-get install xvfb cifs-utils libqtwebkit4 snmp mysql-server
odbcinst1debian2 libodbc1
```

Introduisez le mot de passe pour MySQL, puis à l'écran suivant, choisir la sécurité renforcée.

6. Au cas où on souhaiterait faire l'intégration avec l'active directory, ces paquets sont aussi nécessaires

```
apt install samba  ldap-utils libsasl2-modules-gssapi-mit krb5-user
```

7. Editer le fichier de configuration de MySQL

```
nano /etc/mysql/my.cnf
```

et ajouter les lignes suivantes

```
[mysqld]
log_bin_trust_function_creators=1
max_allowed_packet=33M
innodb_log_file_size=100M
innodb_log_files_in_group=2
```

8. Créer une base de donnée era_db et un utilisateur eset

```
mysql -u root -p
```

Une fois mysql client ouvert, collez les lignes suivantes

```
CREATE DATABASE era_db;
CREATE USER eset@localhost IDENTIFIED BY 'mot-de-passe-sql';
GRANT ALL PRIVILEGES ON era_db.* TO eset@localhost;
flush privileges;
quit
```

9. Redémarrer MySQL

```
service mysql restart
```

Installation myodbc

1. Télécharger la dernière version 8 disponible (info)

```
wget -qO- https://downloads.mysql.com/archives/get/p/10/file/mysql-
connector-odbc-8.0.17-linux-debian10-x86-64bit.tar.gz | tar xvzg -
```

2. Copier les fichiers

```
cd mysql-connector-odbc...
cp bin/* /usr/bin
cp lib/* /usr/lib/x86_64-linux-gnu/odbc/
```

3. Editer le fichier odbcinst.ici

```
nano /etc/odbcinst.ini
```

Avec ce contenu:

```
[MySQL]
Description = ODBC for MySQL
Driver = /usr/lib/x86_64-linux-gnu/odbc/libmyodbc8w.so
```

```
Setup = /usr/lib/x86_64-linux-gnu/odbc/libodbcmyS.so
FileUsage = 1
```

4. Procéder à l'installation

```
odbcinst -i -d -f /etc/odbcinst.ini
```

5. Faire un lien symbolique pour le socket

```
ln -s /var/run/mysqld/mysqld.sock /tmp/mysql.sock
```

Installation Eset SMC

1. Télécharger le programme d'install

```
wget
https://download.eset.com/com/eset/apps/business/era/server/linux/latest/server-linux-x86_64.sh
```

2. le rendre exécutable

```
chmod +x server-linux-x86_64.sh
```

3. Lancer le programme d'installation en changeant les données pour refléter votre situation

```
./server-linux-x86_64.sh --skip-license --db-type="MySQL Server" --db-driver="MySQL" \
--db-hostname=localhost --db-port=3306 --server-root-password="pwd-web-interface" \
--db-user-username="eset" --db-user-password="mot-de-passe-sql" \
--cert-hostname="srv-av.makeitsimple.lan" --cert-auth-common-name="srv-av.makeitsimple.lan" \
--cert-organization="makeITsimple" --cert-locality="BE" \
--ad-server="**ACTIVE DIRECTORY SERVER**" --ad-user-name="Administrator" --ad-user-password="**DOMAIN PASSWORD**"
```

La dernière ligne concerne l'intégration à l'Active Directory, l'omettre si pas d'application. Plus de détails sur les paramètres ici.

4. Démarrer le service et vérifier son statut

```
service eraserver start
service eraserver status
```

- Effacer l'historique afin que les mots de passe ne trainent pas trop

```
history -c
```

Installation Eset ERA (Interface graphique)

1. Installer Tomcat et Openjdk

```
apt-get install openjdk-11-jdk tomcat9
```

2. Télécharger ERA sur le site d'Eset

```
wget
https://download.eset.com/com/eset/apps/business/era/webconsole/latest/
era.war -P /var/lib/tomcat9/webapps/
```

~~- Copier le fichier au bon endroit <code bash>cp era.war /var/lib/tomcat9/webapps/</code>~~

1. Redémarrer le service et vérifier son statut

```
service tomcat9 restart
service tomcat9 status
```

Configuration TLS

1. Créer une clé et un certificat pour le serveur eset
2. Fusionner le CA & le certificat ensemble

```
cat makeitsimple-ca.crt srv-eset.makeitsimple.lan.crt >
/tmp/fullchain.crt
```

3. Créer un fichier pkcs12

```
openssl pkcs12 -export -inkey srv-eset.makeitsimple.lan.key -in
fullchain.crt \
-out /tmp/srv-eset.makeitsimple.lan.p12 -name srv-eset -password
pass:**temppass**
```

Remplacez temppass par un mot de passe qui servira à protéger le fichier p12

4. Ajouter ce fichier P12 dans une base de clés keytool

```
keytool -importkeystore -deststorepass eset-era-c3rt -destkeypass eset-
era-c3rt \
-destkeystore /opt/eset/keystore -srckeystore srv-
eset.makeitsimple.lan.p12 \
-srcstoretype PKCS12 -srcstorepass temppass -alias srv-eset -noprompt
```

   - eset-era-c3rt sera le mot de passe pour accéder à notre keytool
   - temppass est le mot de passe que vous avez défini dans le point précédent
5. Editer le fichier de config de Tomcat

```
nano /var/lib/tomcat9/conf/server.xml
```

et ajouter ceci après <Service name="Catalina">

```
<Connector protocol="org.apache.coyote.http11.Http11NioProtocol"
port="8443" maxThreads="200" scheme="https" secure="true"
SSLEnabled="true" keystoreFile="/opt/eset/keystore" keystorePass="eset-
era-c3rt" clientAuth="false" sslProtocol="TLS"/>
```

6. Redémarrer Tomcat

```
service tomcat9 restart
```

Vous pouvez voir les logs de Tomcat si vous avez des soucis

```
cat /var/log/tomcat9/catalina.*.log
```

Configuration TLS (seconde version)

1. Créer une clé et un certificat pour le serveur eset
2. Editer le fichier de config de Tomcat

```
nano /var/lib/tomcat9/conf/server.xml
```

et ajouter ceci après <Service name="Catalina">

```
<Connector port="8443"
protocol="org.apache.coyote.http11.Http11AprProtocol"  maxThreads="150"
SSLEnabled="true" >
        <UpgradeProtocol
className="org.apache.coyote.http2.Http2Protocol" />
        <SSLHostConfig>
            <Certificate certificateKeyFile="/opt/eset/srv-
eset.makeitsimple.lan.pem"
                         certificateFile="/opt/eset/srv-
eset.makeitsimple.lan.crt"type="RSA" />
        </SSLHostConfig>
    </Connector>
```

3. Redémarrer Tomcat

```
service tomcat9 restart
```

Vous pouvez voir les logs de Tomcat si vous avez des soucis

```
cat /var/log/tomcat9/catalina.*.log
```

Ouvrir l'interface utilisateur

Se rendre sur :

- Sans certificat: http://fqdn:8080/era
- Avec certificat: https://fqdn:8443/era

Installer l'agent Linux version facile et sans besoin de certificat

1. Télécharger l'agent

```
wget https://download.eset.com/com/eset/apps/business/era/agent/latest/agent-linux-x86_64.sh
```

2. Le rendre exécutable

```
chmod +x agent-linux-x86_64.sh
```

3.
```
./agent-linux-x86_64.sh --skip-license --hostname=srv-eset.makeitsimple.lan --port=2222 --webconsole-password=motdepasseinterfaceweb
```

Sources

- Installation
  - https://help.eset.com/esmc_install/71/en-US/installation.html?installation_linux.html
  - https://help.eset.com/esmc_install/71/en-US/component_installation_server_linux.html
  - https://help.eset.com/esmc_install/71/en-US/odbc_configuration.html
  - https://help.eset.com/esmc_install/71/en-US/mysql_configuration.html
  - https://dev.mysql.com/doc/connector-odbc/en/connector-odbc-installation-binary-unix-tarball.html
- SSL/TLS
  - https://www.kassianoff.fr/blog/fr/eset-remote-administrator-installation-sous-ubuntu-lts
  - https://chrisjrob.com/2015/11/17/install-eset-remote-administrator-on-ubuntu/