Omavalvonta, asennus Ubuntu Server 14.04

Sami Hostikka

30.05.2014

Sisällys

Omavalvonnan tuotantoympäristön asennus on pyritty automatisoimaan. ***bootstrap.sh*** *skripti automatisoi Testshib testiversion asennuksen.*

1 Ubuntun päivittäminen

```
aptitude update
aptitude safe-upgrade
```

2 MySQL

- MySQL-palvelimen asennus

```
aptitude install mysql-server
```

- Konfiguroidaan MySQL

```
mysql_secure_installation

NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MySQL
      SERVERS IN PRODUCTION USE!  PLEASE READ EACH STEP CAREFULLY!


In order to log into MySQL to secure it, we'll need the current
password for the root user.  If you've just installed MySQL, and
you haven't set the root password yet, the password will be blank,
so you should just press enter here.

Enter current password for root (enter for none):
OK, successfully used password, moving on...

Setting the root password ensures that nobody can log into the MySQL
root user without the proper authorisation.

Set root password? [Y/n] y
New password:
Re-enter new password:
Password updated successfully!
Reloading privilege tables..
 ... Success!


By default, a MySQL installation has an anonymous user, allowing anyone
to log into MySQL without having to have a user account created for
them.  This is intended only for testing, and to make the installation
go a bit smoother.  You should remove them before moving into a
production environment.

Remove anonymous users? [Y/n] y
 ... Success!

Normally, root should only be allowed to connect from 'localhost'.  This
```

```
ensures that someone cannot guess at the root password from the network.

Disallow root login remotely? [Y/n] y
 ... Success!

By default, MySQL comes with a database named 'test' that anyone can
access.  This is also intended only for testing, and should be removed
before moving into a production environment.

Remove test database and access to it? [Y/n] y
 - Dropping test database...
 ... Success!
 - Removing privileges on test database...
 ... Success!

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

Reload privilege tables now? [Y/n] y
 ... Success!

Cleaning up...



All done!  If you've completed all of the above steps, your MySQL
installation should now be secure.

Thanks for using MySQL!
```

- Konfiguroidaan MySQL käyttämään UTF-8 merkistöä, `/etc/mysql/my.cnf`

  *Huomaa, esimerkkikonfiguraatio löytyy **configuration/etc/mysql** kansiosta*

```
[mysqld]
#...
collation-server = utf8_unicode_ci
init-connect='SET NAMES utf8'
character-set-server = utf8
```

- Kirjaudutaan MySQL-palvelimelle

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

- Lisätään omavalvonnalle oma tietokanta

```
mysql> create database omavalvonta;
```

- Lisätään Omavalvonnalle oma MySQL-käyttäjä

```
mysql> grant CREATE,INSERT,DELETE,UPDATE,SELECT on omavalvonta.* to
        omavalvonta@localhost;
```

- Määritetään käyttäjän omavalvonta salasana

```
mysql> set password for omavalvonta@localhost=password('salasana');
```

- Päivitetään käyttöoikeudet

```
mysql> flush privileges;
```

3 Apache

- Apachen asennus

```
aptitude install apache2
```

3.1 SSL-sertifikaatti

- Aktivoidaan Apchen uudelleenkirjoitus-moduuli

```
a2enmod rewrite
```

- Aktivoidaan Apachen SSL-moduuli

```
a2enmod ssl
```

- Tehdään SSL-sertifikaateille oma hakemisto

```
mkdir /etc/apache2/ssl
```

- Generoidaan itseallekirjoitettu sertifikaatti

```
openssl req -new -x509 -days 365 -nodes -out /etc/apache2/ssl/apache.pem -keyout
 /etc/apache2/ssl/apache.key

Generating a 1024 bit RSA private key
.....++++++
.......++++++
writing new private key to '/etc/apache2/ssl/apache.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:FI
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:HAMK Hameen ammattikorkea
Organizational Unit Name (eg, section) []:Tietohallinto
Common Name (eg, YOUR name) []:
Email Address []:
```

3.2 Proxy

- Aktivoidaan Apachen proxy-moduuli

```
a2enmod proxy
a2enmod proxy_http
```

3.3 Konfigurointi

- Lisätään omavalvonnalle vhost, `/etc/apache2/sites-enabled/omavalvonta.conf`

*Huomaa, esimerkkikonfiguraatio löytyy **configuration/etc/apache/sites-enabled** kansiosta*

```
LoadModule rewrite_module modules/mod_rewrite.so
LoadModule proxy_module modules/mod_proxy.so

<VirtualHost *:80>
  RewriteEngine On
  RewriteCond %{HTTPS} off
  RewriteRule .* https://%{SERVER_NAME}%{REQUEST_URI} [R,L]
</VirtualHost>

<VirtualHost *:443>
  # SSL
  SSLEngine On
  SSLCertificateFile /etc/apache2/ssl/apache.pem
  SSLCertificateKeyFile /etc/apache2/ssl/apache.key

  # Proxy
  ProxyPreserveHost On
  ProxyPass /Shibboleth.sso !
  ProxyPass / http://127.0.0.1:9000/
  ProxyPassReverse / http://127.0.0.1:9000/

        <Location />
                AuthType shibboleth
                ShibRequestSetting requireSession false
                ShibUseHeaders On
                Require shibboleth
        </Location>
</VirtualHost>
```

- Määritetään palvelimen nimi, `/etc/apache2/conf-enabled/fqdn.conf`

*Huomaa, esimerkkikonfiguraatio löytyy **configuration/etc/apache/conf-enabled** kansiosta*

```
ServerName example.com
```

4 Shibboleth

- Asennetaan Shibboleth service provider

```
aptitude install libapache2-mod-shib2
```

- Generoidaan Shibbolethille sertifikaatti

```
shib-keygen -y 3 -h example.com -e https://example.com/shibboleth
```

- Konfiguroidaan Shibboleth toimimaan Apachen kanssa, `/etc/apache2/conf.d/shib.conf`

  Huomaa, esimerkkikonfiguraatio löytyy ***configuration/etc/apache/conf.d*** *kansiosta*

```
LoadModule mod_shib /usr/lib/apache2/modules/mod_shib_22.so

UseCanonicalName On

<Location /Shibboleth.sso>
  SetHandler shib
</Location>
```

- Konfiguroi Shibboleth
- Käynnistetään Shibd daemon uudelleen

```
service shibd restart
```

- Käynnistetään Apache uudelleen

```
service  apache2 restart
```

5 Riippuvuudet

- Asennetaan JDK ja unzip

```
aptitude install openjdk-7-jdk openjdk-7-jre unzip
```

6 Omavalvonta

- Lisää omavalvonnalle käyttäjätunnus

```
useradd -m -s /bin/false omavalvonta
```

- Siirrä tietokanta palvelimelle
- Palauta tietokanta

```
mysql -u root -p omavalvonta < sql/db.sql
```

- Siirrä omavalvonta-1.0.zip palvelimelle
- Pura siirretty zip-tiedosto

```
unzip -d /home/omavalvonta omavalvonta-1.0.zip
```

- Anna omavalvonnalle suoritusoikeudet

```
chmod +x /home/omavalvonta/omavalvonta-1.0/bin/omavalvonta
```

- Aseta omavalvonta käyttäjä omavalvonnan tiedostojen omistajaksi

```
chown -R omavalvonta:omavalvonta /home/omavalvonta/omavalvonta-1.0
```

- Lisätään omavalvonnalle Upstart käynnistyskripti, `/etc/init/omavalvonta.conf`

*Huomaa, käynnistyskripti löytyy **configuration/etc/init** kansiosta*

```
# Usage:
#   start omavalvonta
#   stop omavalvonta
#   restart omavalvonta
#
# WARNING: This is still beta, I have not tested the respawning functionality, but it sh
#
# http://leon.radley.se

description "Omavalvonta"
author "Leon Radley <leon@radley.se>"
version "1.0"

env PROJECT=omavalvonta
env USER=omavalvonta
env GROUP=omavalvonta
env HOME=/home/omavalvonta
env PORT=9000
env ADDRESS=127.0.0.1
env CONFIG=production.conf
env EXTRA="-Duser.language=fi -Duser.country=FI -Duser.timezone=Europe/Helsinki"

start on runlevel [2345]
stop on runlevel [06]

respawn
respawn limit 10 5
umask 022
expect daemon

exec start-stop-daemon --pidfile ${HOME}/RUNNING_PID --chuid $USER:$GROUP --exec ${HOME}
```

- Lisätään konfigurointitiedosto `/home/omavalvonta/production.conf`, katso konfigurointi
- Käynnistä omavalvonta

```
service omavalvonta start
```

6.1 Konfigurointi

6.1.1 Esimerkkikonfiguraatio

*Huomaa, esimerkkikonfiguraatio löytyy **configuration/home/omavalvonta** kansiosta*

```
include "application.conf"

# Database configuration
# ~~~~~
db.default.url="jdbc:mysql://127.0.0.1/omavalvonta?characterEncoding=UTF-8"
db.default.user=omavalvonta
db.default.password="salasana"

# Shibboleth
# ~~~~~
# milliseconds
#shibboleth.session.maxAge=1800000
#shibboleth.login.url=/Shibboleth.sso/Login
#shibboleth.login.entityId=""
#shibboleth.logout.url=/Shibboleth.sso/Logout
#shibboleth.haka.logout.url=""
#shibboleth.adminRole=[Staff,Faculty]
#shibboleth.attribute.email=mail
#shibboleth.attribute.role=eduPersonPrimaryAffiliation
#shibboleth.attribute.firstName=givenName
#shibboleth.attribute.lastName=sn
#http://docs.oracle.com/javase/6/docs/api/java/lang/String.html#split(java.lang.String)
#shibboleth.separator=""
```

6.1.2 Konfigurointitiedoston sisältö

Muuttuja	Tarkoitus
db.default.url	Tietokannan JDBC url
db.default.user	Tietokannan käyttäjä
db.default.password	Tietokannan käyttäjän salasana
shibboleth.session.maxAge	Kirjautuneen käyttäjän session kesto millisekunteina
shibboleth.login.url	Shibboleth sp:n sisäänkirjautumisosoite
shibboleth.login.entityId	Shibboleth sp:n sisäänkirjautumisosoitteessa käytettävä entityID
shibboleth.logout.url	Shibboleth sp:n uloskirjautumisosoite
shibboleth.haka.logout.url	Haka logout osoite
shibboleth.adminRole	Lista rooleista, joilla on pääsy omavalvonnan ylläpitoon
shibboleth.attribute.email	Apachen request headereissa välittämän sähköposti atribuutin nimi
shibboleth.attribute.role	Apachen request headereissa välittämän rooli atribuutin nimi

Muuttuja	Tarkoitus
shibboleth.attribute.firstName	Apachen request headereissa välittämän etunimi atribuutin nimi
shibboleth.attribute.lastName	Apachen request headereissa välittämän sukunimi atribuutin nimi
shibboleth.separator	Regex, jolla erotetaan roolit, mikäli niitä on useita rooli atribuutissa

6.1.3 Konfiguraation oletusarvot

Muuttuja	Oletusarvo
db.default.url	
db.default.user	
db.default.password	
shibboleth.session.maxAge	1800000
shibboleth.login.url	/Shibboleth.sso/Login
shibboleth.login.entityId	
shibboleth.logout.url	/Shibboleth.sso/Logout
shibboleth.haka.logout.url	
shibboleth.adminRole	[Staff,Faculty]
shibboleth.attribute.email	mail
shibboleth.attribute.role	eduPersonPrimaryAffiliation
shibboleth.attribute.firstName	givenName
shibboleth.attribute.lastName	sn
shibboleth.attribute.roleRequired	false
shibboleth.attribute.firstNameRequired	false
shibboleth.attribute.lastNameRequired	false
shibboleth.separator	

6.1.4 Esimerkkejä

Muuttuja	Arvo
db.default.url	jdbc:mysql://127.0.0.1/omavalvonta?characterEncoding=UTF-8&useUnicode=true
db.default.user	omavalvonta
db.default.password	salasana
shibboleth.login.entityId	https://shibboleth.hamk.fi/shibboleth-hamk
shibboleth.haka.logout.url	https://shib-origin.tut.fi/SHIBLOGOUT
shibboleth.separator	`\\s*,\\s*`