Guía de Instalación PKIUDB

Antes de la instalación

- Si se utilizara Mandrake 9.1 se necesita instalar los siguientes paquetes:
  - Apache
  - OpenLdap
  - make
  - gcc
  - mod_perl
  - mod_ssl
  - gettext

- Instalar OpenSSL en ambas computadoras RA y CA, en nuestro caso fue una sola computadora.

  - Bajar el archivo ***openssl-0.9.7b.tar.gz*** de www.openssl.org

  - Descomprimir el archivo: ***tar xvf openssl-0.9.7b.tar.gz***

    De preferencia tienes que estar ubicado en tu directorio HOME y estar como superusuario (*root*).

  - Compilación e Instalación de OpenSSL.

    cd openssl-0.9.7b
    ./config
    make
    make test
    make install

    Para hacer uso de esta nueva instalación debes usar la siguiente ruta ***/usr/local/ssl***

- Preparar MySQL

  - Verificar si MySQL esta corriendo: ***/usr/init.d/mysql status***
  - Cargar el MySQL Monitor, digitando ***mysql*** y enter

    mysql>*create database openca;*
    mysql>*grant all privileges on openca.* to openca@localhost identified by "mysqlopenca";*

- Bajar el archivo ***openca-0.9.1-1.tar.gz*** de www.openca.org

- Crear el directorio para los archivos del servidor web: ***mkdir /srv/ca***

- Descomprimir el archivo: ***tar xvf openca-0.9.1-1.tar.gz***

De preferencia tienes que estar ubicado en tu directorio HOME y estar como superusuario (*root*).

Instalación de CA

Configuración del software

cd openca-0.9.1-1

./configure --prefix=/srv/ca /
--with-web-host=ca.pkiudb.edu.sv /
--with-httpd-host=ca.pkiudb.edu.sv /
--with-httpd-user=apache /
--with-httpd-group=nogroup /
--with-dist-user=adonis /
--with-dist-group=openca /
--with-ca-organization=pkiudb.edu /
--with-ca-locality=soyapango /
--with-ca-country=sv /
--with-service-mail-account=adonis@pkiudb.edu.sv /
--with-openssl-prefix=/usr/local/ssl /
--with-sendmail="/usr/sbin/sendmail -t" /
--with-hierarchy-level=ca /
--enable-dbi /
--with-db-type=mysql /
--with-db-name=openca /
--with-db-host=localhost /
--with-db-port=3306 /
--with-db-user=openca /
--with-db-passwd=mysqlopenca /
--with-ldap-host=ca.pkiudb.edu.sv /
--with-ldap-root="cn=Manager,ou=Internet,o=pkiudb.edu,c=sv" /
--with-ldap-root-pwd=ldappasswd

Compilación e Instalación

make ca
make install-ca

Configuración del servidor apache

Se utilizo ***http2.conf*** para crear el Virtual Host, el cual se encuentra en la siguiente ruta ***/etc/httpd/conf/***

```
<VirtualHost ca.pkiudb.edu.sv>
    ServerAdmin adonis@ca.pkiudb.edu.sv
    DocumentRoot /srv/ca/apache/htdocs
    ServerName ca.pkiudb.edu.sv
    SetEnvIf User-Agent ".*MSIE.*" \
            nokeepalive ssl-unclean-shutdown \
            downgrade-1.0 force-response-1.0
    CustomLog /var/log/httpd/ssl_response_log \
    "%t%h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"
    <Directory "/srv/ca/apache/htdocs">
            Options Indexes FollowSymlinks MultiViews
            AllowOverride None
            Order allow,deny
            Allow from all
    </Directory>
    ScriptAlias /cgi-bin/ "/srv/ca/apache/cgi-bin/"
    <Directory "/srv/ca/apache/cgi-bin">
            AllowOverride None
            Options None
            Order allow,deny
            Allow from all
    </Directory>
</VirtualHost>
```

Instalación de RA

- Crear el directorio para los archivos del servidor web: ***mkdir /srv/ra***

- Cargar el MySQL Monitor, digitando ***mysql*** y enter

  mysql>*create database openca;*
  mysql>*grant all privileges on openca.* to openca@localhost identified by "mysqlopenca";*

- **Configuración del software**

  cd openca-0.9.1-1

  ./configure --prefix=/srv/ra /
  --with-web-host=ra.pkiudb.edu.sv /
  --with-httpd-host=ra.pkiudb.edu.sv /
  --with-httpd-user=apache /
  --with-httpd-group=nogroup /
  --with-dist-user=adonis /
  --with-dist-group=openca /
  --with-ca-organization=pkiudb.edu /
  --with-ca-locality=soyapango /
  --with-ca-country=sv /
  --with-service-mail-account=adonis@pkiudb.edu.sv /
  --with-openssl-prefix=/usr/local/ssl /
  --with-sendmail="/usr/sbin/sendmail -t" /
  --with-hierarchy-level=ra /
  --enable-dbi /
  --with-db-type=mysql /
  --with-db-name=opencara /
  --with-db-host=localhost /
  --with-db-port=3306 /
  --with-db-user=openca /
  --with-db-passwd=mysqlopenca /
  --with-ldap-host=ra.pkiudb.edu.sv /
  --with-ldap-root="cn=Manager,ou=Internet,o=pkiudb.edu,c=sv" /
  --with-ldap-root-pwd=ldappasswd

- **Compilación e Instalación**

  make ext
  make install-ext

Configuración del servidor apache

Se utilizo ***http2.conf*** para crear el Virtual Host, el cual se encuentra en la siguiente ruta ***/etc/httpd/conf/***

```
<VirtualHost ra.pkiudb.edu.sv>
    ServerAdmin adonis@ca.pkiudb.edu.sv
    DocumentRoot /srv/ra/apache/htdocs
    ServerName ra.pkiudb.edu.sv
    SetEnvIf User-Agent ".*MSIE.*" \
            nokeepalive ssl-unclean-shutdown \
            downgrade-1.0 force-response-1.0
    SSLEngine on
    SSLCertificateFile /srv/ra/ssl.crt/server.pem
    SSLCertificateKeyFile /srv/ra/ssl.key/key.pem
    <Directory "/srv/ra/apache/htdocs/pub/">
            Options Indexes FollowSymlinks MultiViews
            AllowOverride None
            Order allow,deny
            Allow from all
    </Directory>
    <Directory "/srv/ra/apache/htdocs/ra/">
            Options Indexes FollowSymlinks MultiViews
            AllowOverride None
            Order allow,deny
            Allow from 192.168.10
    </Directory>
    <Directory "/srv/ra/apache/htdocs/ra_node/">
            Options Indexes FollowSymLinks MultiViews
            AllowOverride None
            Order allow,deny
            Allow from 192.168.10
    </Directory>
    <Directory "/srv/ra/apache/htdocs/ldap/">
            Options Indexes FollowSymLinks MultiViews
            AllowOverride None
            Order allow,deny
            Allow from 192.168.10
    </Directory>
    ScriptAlias /cgi-bin/ "/srv/ra/apache/cgi-bin/"
    <Directory "/srv/ra/apache/cgi-bin">
            AllowOverride None
            Options None
            Order allow,deny
            Allow from all
    </Directory>
</VirtualHost>
```

Configuración del Servidor LDAP

- Modificar el archivo /etc/openldap/slapd.conf

```
include     /etc/openldap/schema/core.schema
include     /etc/openldap/schema/cosine.schema
include     /etc/openldap/schema/inetorgperson.schema

pidfile     /var/run/slapd/slapd.pid
argsfile    /var/run/slapd/slapd.args

allow bind_v2

#######################################################################
# ldbm database definitions
#######################################################################

database bdb
suffix      "o=pkiudb.edu,c=sv"
rootdn      "cn=Manager,ou=Internet,o=pkiudb.edu,c=sv"

# Cleartext passwords, especially for the rootdn, should
# be avoided.  See slappasswd(8) and slapd.conf(5) for details.
# Use of strong authentication encouraged.

rootpw      "ldappasswd"
```

- Modificar el archivo: /srv/ra/OpenCA/etc/server/ldap.conf el cual tiene que estar acorde a la configuración anterior.

```
## Now the LDAP default base dn
basedn "o=pkiudb.edu, c=sv"

## Let's define the privileged Account Allowed to Modify the LDAP entries
ldaproot   "cn=Manager,ou=Internet,o=pkiudb.edu,c=sv"
ldappwd   "ldappasswd"
```

- Reiniciar el servicio de LDAP: ***/etc/init.d/ldap restart***