Conexión de Asterisk con openLDAP

Sumario

Conexión Asterisk con openldap.

Co propósito de manter a información dos usuarios/as nun directorio, evitando deste xeito a duplicación de datos conectaremos Asterisk con un servidor openldap, donde se almacenará basicamente a información que doutro xeito estaría nos ficheiros de configuracion Asterisk *sip.conf* e *extensions.conf*.

Configuración ldap.

Instalaremos un servidor openldap no mesmo servidor onde corre Asterisk.

```
yum install openldap openldap-clients openldap-servers
```

Configuramos o servidor ldap cuns datos de exemplo para asterisk.

slapd.conf

Editamos o ficheiro */etc/openldap/slapd.conf*

```
#
# See slapd.conf(5) for details on configuration options.
# This file should NOT be world readable.
#
include         /etc/openldap/schema/core.schema
include         /etc/openldap/schema/cosine.schema
include         /etc/openldap/schema/inetorgperson.schema
include         /etc/openldap/schema/nis.schema

# Allow LDAPv2 client connections.  This is NOT the default.
allow bind_v2

# Do not enable referrals until AFTER you have a working directory
# service AND an understanding of referrals.
#referral       ldap://root.openldap.org

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

# Load dynamic backend modules:
# modulepath    /usr/lib/openldap

# modules available in openldap-servers-overlays RPM package:
# moduleload accesslog.la
# moduleload auditlog.la
# moduleload denyop.la
# moduleload dyngroup.la
# moduleload dynlist.la
# moduleload lastmod.la
# moduleload pcache.la
# moduleload ppolicy.la
# moduleload refint.la
# moduleload retcode.la
```

```
# moduleload rwm.la
# moduleload smbk5pwd.la
# moduleload syncprov.la
# moduleload translucent.la
# moduleload unique.la
# moduleload valsort.la

# modules available in openldap-servers-sql RPM package:
# moduleload back_sql.la

# The next three lines allow use of TLS for encrypting connections using a
# dummy test certificate which you can generate by changing to
# /etc/pki/tls/certs, running "make slapd.pem", and fixing permissions on
# slapd.pem so that the ldap user or group can read it.  Your client software
# may balk at self-signed certificates, however.
# TLSCACertificateFile /etc/pki/tls/certs/ca-bundle.crt
# TLSCertificateFile /etc/pki/tls/certs/slapd.pem
# TLSCertificateKeyFile /etc/pki/tls/certs/slapd.pem

# Sample security restrictions
#       Require integrity protection (prevent hijacking)
#       Require 112-bit (3DES or better) encryption for updates
#       Require 63-bit encryption for simple bind
# security ssf=1 update_ssf=112 simple_bind=64

# Sample access control policy:
#       Root DSE: allow anyone to read it
#       Subschema (sub)entry DSE: allow anyone to read it
#       Other DSEs:
#               Allow self write access
#               Allow authenticated users read access
#               Allow anonymous users to authenticate
#       Directives needed to implement policy:
# access to dn.base="" by * read
# access to dn.base="cn=Subschema" by * read
# access to *
#       by self write
#       by users read
#       by anonymous auth
#
# if no access controls are present, the default policy
# allows anyone and everyone to read anything but restricts
# updates to rootdn.  (e.g., "access to * by * read")
#
# rootdn can always read and write EVERYTHING!

#######################################################################
# ldbm and/or bdb database definitions
#######################################################################

database        bdb
suffix          "dc=my-domain,dc=com"
rootdn          "cn=Manager,dc=my-domain,dc=com"
# Cleartext passwords, especially for the rootdn, should
# be avoided.  See slappasswd(8) and slapd.conf(5) for details.
# Use of strong authentication encouraged.
# rootpw                secret
# rootpw                {crypt}ijFYNcSNctBYg

# The database directory MUST exist prior to running slapd AND
# should only be accessible by the slapd and slap tools.
# Mode 700 recommended.
directory       /var/lib/ldap

# Indices to maintain for this database
index objectClass                       eq,pres
index ou,cn,mail,surname,givenname      eq,pres,sub
index uidNumber,gidNumber,loginShell    eq,pres
index uid,memberUid                     eq,pres,sub
index nisMapName,nisMapEntry            eq,pres,sub

# Replicas of this database
#replogfile /var/lib/ldap/openldap-master-replog
```

```
#replica host=ldap-1.example.com:389 starttls=critical
#     bindmethod=sasl saslmech=GSSAPI
#     authcId=host/ldap-master.example.com@EXAMPLE.COM
```

Modificaremos as seguintes liñas:

Engadimos a seguinte liña a lista de includes, co esquema LDAP necesario para Asterisk.

```
include       /etc/openldap/schema/asterisk.schema
```

Previamente debemos copiar o ficheiro asterisk.schema o directorio schema de openldap

```
[root@hercules scripts]# cp usr/src/asterisk/asterisk-1.6.1.0/contrib/scripts/asterisk.schema /etc/openldap/schema/
```

Modificamos a liñas

```
suffix          "dc=iessanclemente,dc=net"
rootdn          "cn=Manager,dc=iessanclemente,dc=net"
...
rootpw          {SSHA}p1aUQtijsSqpYnsMjaJgyPrV58RYngkc
...
directory       /var/lib/ldap/iessanclemente-ldap
```

O password do *rootdn* obtémolo usando a ferramenta

```
[root@hercules openldap]# slappasswd
New password:
Re-enter new password:
{SSHA}p1aUQtijsSqpYnsMjaJgyPrV58RYngkc
[root@hercules openldap]#
```

Tamén temos que crear o directorio */var/lib/ldap/iessanclemente-net* que conterá a base de datos LDAP. Faremos este directorio pertencente o usuario ldap:ldap cos permisos 700 tal e como se indica no ficheiro s*lapd.conf* Para que surtan efecto estes cambios rearrancamos o servidor ldap.

```
[root@hercules ldap]# /etc/init.d/ldap restart
```

Neste punto só nos queda cargar algúns datos de exemplo na base de datos LDAP. Faremos isto mediante ficheiros ldiff. A continuación detallamos os datos de exemplo que cargaremos, así como os ficheiros necesarios e os comandos ldap para facer a carga.

sippeers.ldif

```
dn: ou=sippeers,dc=iessanclemente,dc=net
ou: sippeers
objectClass: top
objectClass: organizationalUnit

dn: cn=Antonio Perez,ou=sippeers,dc=iessanclemente,dc=net
objectClass: top
objectClass: inetOrgPerson
objectClass: AsteriskSIPUser
cn: Antonio Perez
sn: Perez
AstAccountCallerID: 2001
AstAccountHost: dynamic
AstAccountRealmedPassword: {SSHA}9aenZD/V5WDUIQdDkd5llKejOQHN09sq
AstAccountContext: default

dn: cn=Maria Arias,ou=sippeers,dc=iessanclemente,dc=net
objectClass: top
objectClass: inetOrgPerson
objectClass: AsteriskSIPUser
cn: Maria Arias
sn: Arias
AstAccountCallerID: 2002
AstAccountHost: dynamic
AstAccountRealmedPassword: {SSHA}sCtnygqFBp8oxWEd61KZAE2XTcIiJ63G
AstAccountContext: default
```

Ficheiro ldiff para crear dous usuarios SIP (Antonio Perez e María Arias) coas extensións 2001 e 2002 respectivamente.

extensions.ldif

```
dn: ou=extensions,dc=iessanclemente,dc=net
ou: extensions
objectClass: top
objectClass: organizationalUnit

dn: cn=2001,ou=extensions,dc=iessanclemente,dc=net
cn: 2001
objectClass: top
objectClass: device
objectClass: AsteriskExtension
AstContext: users
AstExtension: 2001
AstPriority: 1
AstApplication: Dial
AstApplicationData: SIP/antonio perez

dn: cn=2002,ou=extensions,dc=iessanclemente,dc=net
cn: 2002
objectClass: top
objectClass: device
objectClass: AsteriskExtension
AstContext: users
AstExtension: 2002
AstPriority: 1
AstApplication: Dial
AstApplicationData: SIP/maria arias
```

Ficheiro ldiff para crear 2 extensións 2001 e 2002 que utilizaremos para chamar aos dous usuarios anteriormente dados de alta.

eco-demo.ldif

```
dn: cn=600-1,ou=extensions,dc=iessanclemente,dc=net
cn: 600-1
objectClass: top
objectClass: device
objectClass: AsteriskExtension
AstContext: demo
AstExtension: 600
AstPriority: 1
AstApplication: Playback
AstApplicationData: demo-echotest

dn: cn=600-2,ou=extensions,dc=iessanclemente,dc=net
cn: 600-2
objectClass: top
objectClass: device
objectClass: AsteriskExtension
AstContext: demo
AstExtension: 600
AstPriority: 2
AstApplication: Echo


dn: cn=600-3,ou=extensions,dc=iessanclemente,dc=net
cn: 600-3
objectClass: top
objectClass: device
objectClass: AsteriskExtension
AstContext: demo
AstExtension: 600
AstPriority: 3
AstApplication: Playback
AstApplicationData: demo-echodone
```

Ficheiro ldiff co plan dunha proba de echo para a extenxión 600.

Carga dos datos de exemplo

A continuación cargamos en LDAP os anteriores ficheiros de configuración utilizando o comando ldapadd. Exemplo de carga das extensións.

```
[root@hercules ldap]# ldapadd -x -D "cn=Manager,dc=iessanclemente,dc=net" -W -f extensions.ldif
Enter LDAP Password:
```

Configuración Asterisk

Editamos o ficheiro */etc/asterisk/res_ldap.conf* e dentro da opción *[_general]* establecemos os seguintes parámetros

```
[_general]
;
; Specify one of either host and port OR url.  URL is preferred, as you can
; use more options.
host=127.0.0.1                                    ; LDAP host
port=389
url=ldap://localhost:389
protocol=3
basedn="dc=iessanclemente, dc=net"                ; Base DN
user="cn=Manager,dc=iessanclemente,dc=net"        ; Bind DN
pass=abc123.
```

Nos arpartados *host* e *url* establecemos o enderezo onde está instalado o servidor openldap. Neste caso está no mesmo servidor.

Editamos o ficheiro */etc/asterisk/extconfig.conf* e engadimos as seguintes liñas ao final

```
sipusers => ldap,"dc=iessanclemente,dc=net",sip
sippeers => ldap,"dc=iessanclemente,dc=net",sip
voicemail => ldap,"dc=iessanclemente,dc=net",voicemail
voicemail_data => ldap,"dc=iessanclemente,dc=net",voicemail
extensions => ldap,"dc=iessanclemente,dc=net",extensions
queues => ldap,"dc=iessanclemente,dc=net",queue
queue_members => ldap,"dc=iessanclemente,dc=net",queue_member
musiconhold => mysql,asterisk
queue_log => mysql,asterisk
meetme => ldap,"dc=iessanclemente,dc=net",meetme
```

Editamos o ficheiro */etc/asterisk/extensions.conf* para incluir as seguintes liñas

```
[users]
switch => Realtime/@

[demo]
switch => Realtime/@

[default]
include => users
include => demo
```

A versión 1.6 de Asterisk xa ven co módulo LDAP realtime interface, de todas maneiras comprobamos que este módulo está cargado no noso asterisk

```
hercules*CLI> module show like ldap
Module                     Description                        Use Count
res_config_ldap.so         LDAP realtime interface            0
1 modules loaded
hercules*CLI>
```