Instalar LDAP 389-DS en CentOS 7

 # hostnamectl
Static hostname: pavilion.cadilinea.lan

 # vi /etc/hosts

```
...
192.168.100.107  pavilion.cadilinea.lan pavilion
```

 # firewall-cmd --permanent --add-port=389/tcp
success
 # firewall-cmd --permanent --add-port=636/tcp
success
 # firewall-cmd --permanent --add-port=9830/tcp
success
 # firewall-cmd --reload
success
 # firewall-cmd --list-ports
9830/tcp 389/tcp 636/tcp

 # vi /etc/sysctl.conf

```
...
net.ipv4.tcp_keepalive_time = 300
net.ipv4.ip_local_port_range = 1024 65000
fs.file-max = 64000
```

 # sysctl --system

```
...
* Applying /etc/sysctl.conf ...
net.ipv4.tcp_keepalive_time = 300
net.ipv4.ip_local_port_range = 1024 65000
fs.file-max = 64000
```

 # vi /etc/security/limits.conf

```
...
*     soft  nofile      8192
*     hard  nofile      8192
```

 # vi /etc/profile

```
...
ulimit -n 8192
```

 # vi /etc/pam.d/login

```
...
session     required /lib/security/pam_limits.so
```

```
# useradd ldapadmin
# passwd ldapadmin

# yum install 389-ds-base openldap-clients
# yum localinstall ftp://rpmfind.net/linux/epel/testing/7/x86_64/i/idm-console-framework-1.1.14-1.el7.noarch.rpm
```

```
# yum localinstall ftp://rpmfind.net/linux/epel/testing/7/x86_64/3/389-adminutil-1.1.22-1.el7.x86_64.rpm

# yum localinstall ftp://rpmfind.net/linux/epel/testing/7/x86_64/3/389-admin-1.1.42-1.el7.x86_64.rpm

# yum localinstall ftp://rpmfind.net/linux/epel/testing/7/x86_64/3/389-admin-console-1.1.10-1.el7.noarch.rpm

# yum localinstall ftp://rpmfind.net/linux/epel/testing/7/x86_64/3/389-console-1.1.9-1.el7.noarch.rpm

# yum localinstall ftp://rpmfind.net/linux/epel/testing/7/x86_64/3/389-ds-console-1.2.12-1.el7.noarch.rpm

# yum localinstall ftp://rpmfind.net/linux/epel/testing/7/x86_64/3/389-admin-console-doc-1.1.10-1.el7.noarch.rpm

# yum localinstall ftp://rpmfind.net/linux/epel/testing/7/x86_64/3/389-adminutil-devel-1.1.22-1.el7.x86_64.rpm

# yum localinstall ftp://rpmfind.net/linux/epel/testing/7/x86_64/3/389-ds-console-doc-1.2.12-1.el7.noarch.rpm


# setup-ds-admin.pl

==============================================================================
This program will set up the 389 Directory and Administration Servers.

It is recommended that you have "root" privilege to set up the software.
Tips for using this program:
  - Press "Enter" to choose the default and go to the next screen
  - Type "Control-B" then "Enter" to go back to the previous screen
  - Type "Control-C" to cancel the setup program

Would you like to continue with set up? [yes]: y

==============================================================================
Your system has been scanned for potential problems, missing patches,
etc.  The following output is a report of the items found that need to
be addressed before running this software in a production
environment.

389 Directory Server system tuning analysis version 23-FEBRUARY-2012.

NOTICE : System is x86_64-unknown-linux3.10.0-327.4.5.el7.x86_64 (4 processors).

Would you like to continue? [yes]: y

==============================================================================
Choose a setup type:

   1. Express
       Allows you to quickly set up the servers using the most
       common options and pre-defined defaults. Useful for quick
       evaluation of the products.

   2. Typical
       Allows you to specify common defaults and options.
```

```
   3. Custom
       Allows you to specify more advanced options. This is
       recommended for experienced server administrators only.

To accept the default shown in brackets, press the Enter key.

Choose a setup type [2]:

===============================================================================
Enter the fully qualified domain name of the computer
on which you're setting up server software. Using the form
<hostname>.<domainname>
Example: eros.example.com.

To accept the default shown in brackets, press the Enter key.

Warning: This step may take a few minutes if your DNS servers
can not be reached or if DNS is not configured correctly.  If
you would rather not wait, hit Ctrl-C and run this program again
with the following command line option to specify the hostname:

    General.FullMachineName=your.hostname.domain.name

Computer name [pavilion.cadilinea.lan]:

===============================================================================
The servers must run as a specific user in a specific group.
It is strongly recommended that this user should have no privileges
on the computer (i.e. a non-root user).  The setup procedure
will give this user/group some permissions in specific paths/files
to perform server-specific operations.

If you have not yet created a user and group for the servers,
create this user and group using your native operating
system utilities.

System User [nobody]: ldapadmin
System Group [nobody]: ldapadmin

===============================================================================
Server information is stored in the configuration directory server.
This information is used by the console and administration server to
configure and manage your servers.  If you have already set up a
configuration directory server, you should register any servers you
set up or create with the configuration server.  To do so, the
following information about the configuration server is required: the
fully qualified host name of the form
<hostname>.<domainname>(e.g. hostname.example.com), the port number
(default 389), the suffix, the DN and password of a user having
permission to write the configuration information, usually the
configuration directory administrator, and if you are using security
(TLS/SSL).  If you are using TLS/SSL, specify the TLS/SSL (LDAPS) port
number (default 636) instead of the regular LDAP port number, and
provide the CA certificate (in PEM/ASCII format).

If you do not yet have a configuration directory server, enter 'No' to
be prompted to set up one.

Do you want to register this software with an existing
configuration directory server? [no]:
```

```
==============================================================================
Please enter the administrator ID for the configuration directory
server.  This is the ID typically used to log in to the console.  You
will also be prompted for the password.

Configuration directory server
administrator ID [admin]:
Password:
Password (confirm):

==============================================================================
The information stored in the configuration directory server can be
separated into different Administration Domains.  If you are managing
multiple software releases at the same time, or managing information
about multiple domains, you may use the Administration Domain to keep
them separate.

If you are not using administrative domains, press Enter to select the
default.  Otherwise, enter some descriptive, unique name for the
administration domain, such as the name of the organization
responsible for managing the domain.

Administration Domain [cadilinea.lan]:

==============================================================================
The standard directory server network port number is 389.  However, if
you are not logged as the superuser, or port 389 is in use, the
default value will be a random unused port number greater than 1024.
If you want to use port 389, make sure that you are logged in as the
superuser, that port 389 is not in use.

Directory server network port [389]:

==============================================================================
Each instance of a directory server requires a unique identifier.
This identifier is used to name the various
instance specific files and directories in the file system,
as well as for other uses as a server instance identifier.

Directory server identifier [pavilion]:

==============================================================================
The suffix is the root of your directory tree.  The suffix must be a valid DN.
It is recommended that you use the dc=domaincomponent suffix convention.
For example, if your domain is example.com,
you should use dc=example,dc=com for your suffix.
Setup will create this initial suffix for you,
but you may have more than one suffix.
Use the directory server utilities to create additional suffixes.

Suffix [dc=cadilinea, dc=lan]:

==============================================================================
Certain directory server operations require an administrative user.
This user is referred to as the Directory Manager and typically has a
bind Distinguished Name (DN) of cn=Directory Manager.
You will also be prompted for the password for this user.  The password must
be at least 8 characters long, and contain no spaces.
Press Control-B or type the word "back", then Enter to back up and start over.
```

```
Directory Manager DN [cn=Directory Manager]:
Password:
Password (confirm):

==============================================================================
The Administration Server is separate from any of your web or application
servers since it listens to a different port and access to it is
restricted.

Pick a port number between 1024 and 65535 to run your Administration
Server on. You should NOT use a port number which you plan to
run a web or application server on, rather, select a number which you
will remember and which will not be used for anything else.

Administration port [9830]:

==============================================================================
The interactive phase is complete.  The script will now set up your
servers.  Enter No or go Back if you want to change something.

Are you ready to set up your servers? [yes]:
Creating directory server . . .
Your new DS instance 'pavilion' was successfully created.
Creating the configuration directory server . . .
Beginning Admin Server creation . . .
Creating Admin Server files and directories . . .
Updating adm.conf . . .
Updating admpw . . .
Registering admin server with the configuration directory server . . .
Updating adm.conf with information from configuration directory server . . .
Updating the configuration for the httpd engine . . .
Starting admin server . . .
The admin server was successfully started.
Admin server was successfully created, configured, and started.
Exiting . . .
Log file is '/tmp/setupeck01n.log'

# systemctl enable dirsrv.target
Created symlink from /etc/systemd/system/multi-user.target.wants/dirsrv.target
to /usr/lib/systemd/system/dirsrv.target.

# systemctl enable dirsrv-admin
Created symlink from /etc/systemd/system/multi-user.target.wants/dirsrv-
admin.service to /usr/lib/systemd/system/dirsrv-admin.service.

# systemctl start dirsrv.target

# systemctl start dirsrv-admin

(Tambien:   start-dirsrv    y      start-ds-admin
            stop-dirsrv    stop-ds-admin)
```

 # systemctl status dirsrv.target

● dirsrv.target - 389 Directory Server
  Loaded: loaded (/usr/lib/systemd/system/dirsrv.target; enabled; vendor preset: disabled)
  Active: active since dom 2016-02-07 21:17:40 CET; 1min 49s ago

feb 07 21:17:40 pavilion.cadilinea.lan systemd[1]: Reached target 389 Directory Server.
feb 07 21:17:40 pavilion.cadilinea.lan systemd[1]: Starting 389 Directory Server.

 # systemctl status dirsrv-admin

```
● dirsrv-admin.service - 389 Administration Server.
   Loaded: loaded (/usr/lib/systemd/system/dirsrv-admin.service; enabled; vendor preset: disabled)
   Active: active (running) since dom 2016-02-07 21:14:33 CET; 5min ago
 Main PID: 5156 (httpd)
   CGroup: /system.slice/dirsrv-admin.service
           ├─5156 /usr/sbin/httpd -k start -f /etc/dirsrv/admin-serv/httpd.conf
           ├─5158 /usr/sbin/httpd -k start -f /etc/dirsrv/admin-serv/httpd.conf
           └─5159 /usr/sbin/httpd -k start -f /etc/dirsrv/admin-serv/httpd.conf

feb 07 21:14:33 pavilion.cadilinea.lan systemd[1]: Starting 389 Administration Server....
feb 07 21:14:33 pavilion.cadilinea.lan systemd[1]: PID file /var/run/dirsrv/admin-serv.pid not
readable (yet?) after start.
feb 07 21:14:33 pavilion.cadilinea.lan systemd[1]: Started 389 Administration Server..
feb 07 21:18:34 pavilion.cadilinea.lan systemd[1]: Started 389 Administration Server..
```

 # ldapsearch -x -b "dc=cadilinea,dc=lan"

```
# extended LDIF
#
# LDAPv3
# base <dc=cadilinea,dc=lan> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# cadilinea.lan
dn: dc=cadilinea,dc=lan
objectClass: top
objectClass: domain
dc: cadilinea

# Directory Administrators, cadilinea.lan
dn: cn=Directory Administrators,dc=cadilinea,dc=lan
objectClass: top
objectClass: groupofuniquenames
cn: Directory Administrators
uniqueMember: cn=Directory Manager

# Groups, cadilinea.lan
dn: ou=Groups,dc=cadilinea,dc=lan
objectClass: top
objectClass: organizationalunit
ou: Groups

# People, cadilinea.lan
dn: ou=People,dc=cadilinea,dc=lan
objectClass: top
objectClass: organizationalunit
ou: People
```

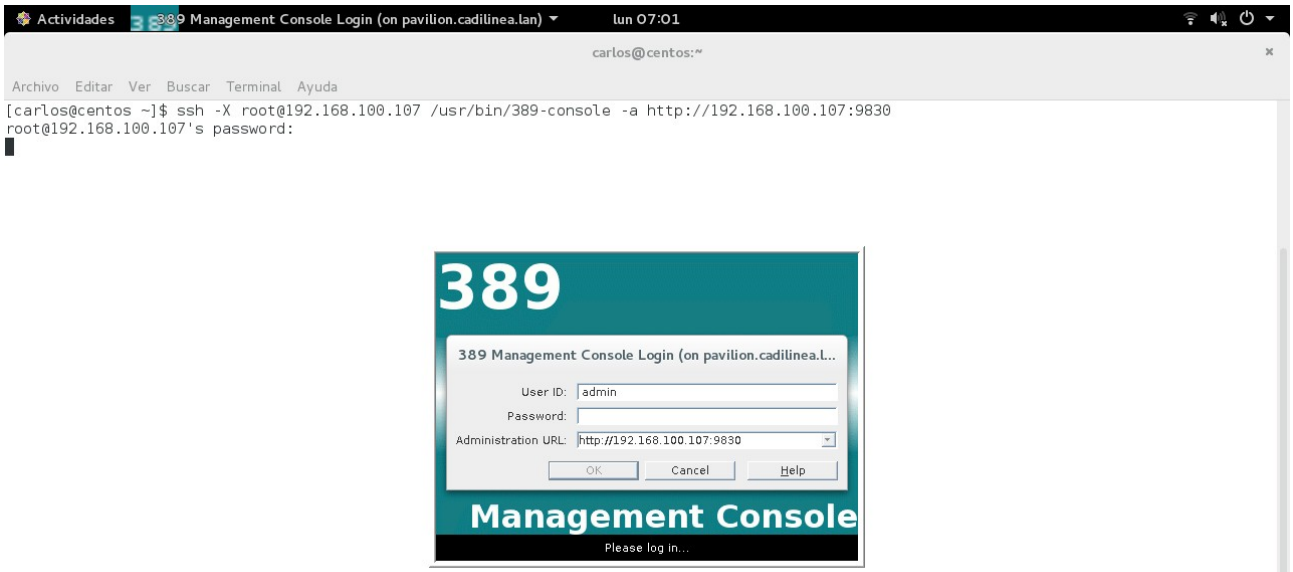
```
# Special Users, cadilinea.lan
dn: ou=Special Users,dc=cadilinea,dc=lan
objectClass: top
objectClass: organizationalUnit
ou: Special Users
description: Special Administrative Accounts

# Accounting Managers, Groups, cadilinea.lan
dn: cn=Accounting Managers,ou=Groups,dc=cadilinea,dc=lan
objectClass: top
objectClass: groupOfUniqueNames
cn: Accounting Managers
ou: groups
description: People who can manage accounting entries
uniqueMember: cn=Directory Manager

# HR Managers, Groups, cadilinea.lan
dn: cn=HR Managers,ou=Groups,dc=cadilinea,dc=lan
objectClass: top
objectClass: groupOfUniqueNames
cn: HR Managers
ou: groups
description: People who can manage HR entries
uniqueMember: cn=Directory Manager

# QA Managers, Groups, cadilinea.lan
dn: cn=QA Managers,ou=Groups,dc=cadilinea,dc=lan
objectClass: top
objectClass: groupOfUniqueNames
cn: QA Managers
ou: groups
description: People who can manage QA entries
uniqueMember: cn=Directory Manager

# PD Managers, Groups, cadilinea.lan
dn: cn=PD Managers,ou=Groups,dc=cadilinea,dc=lan
objectClass: top
objectClass: groupOfUniqueNames
cn: PD Managers
ou: groups
description: People who can manage engineer entries
uniqueMember: cn=Directory Manager

# search result
search: 2
result: 0 Success

# numResponses: 10
# numEntries: 9
```

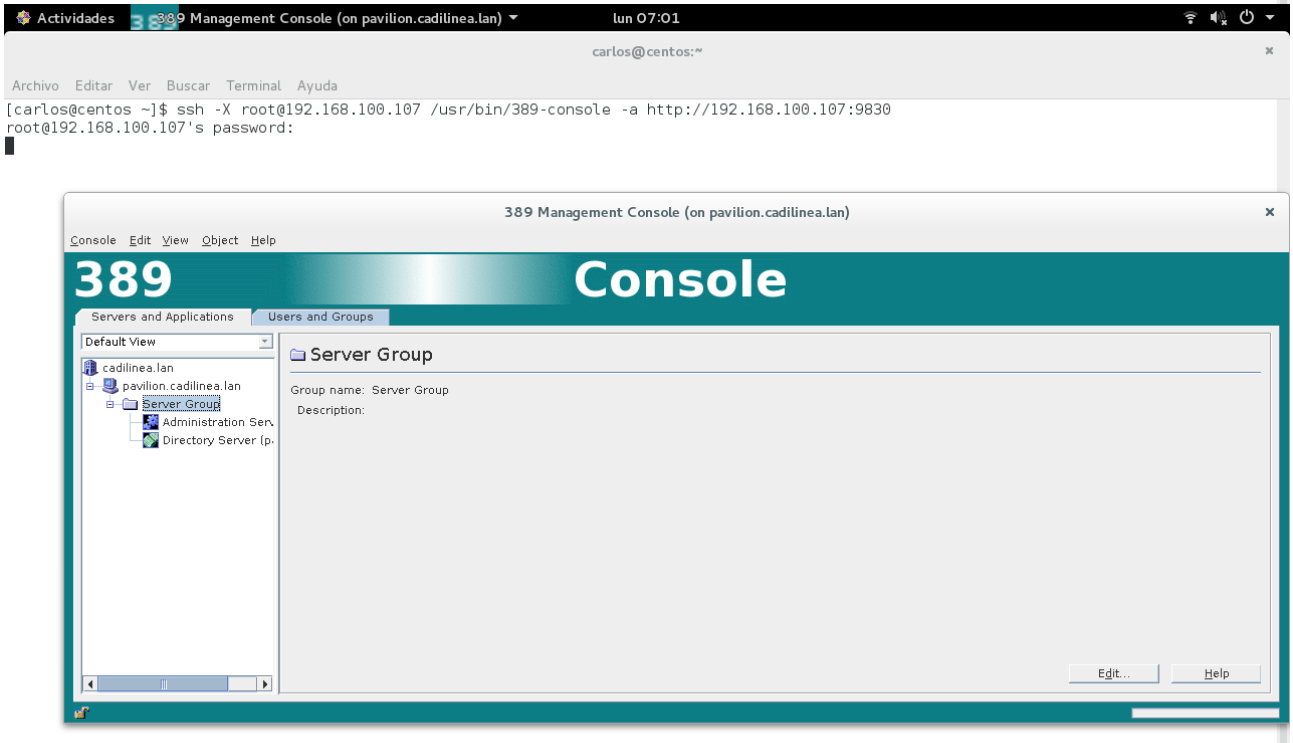
==> Ejecutar de forma LOCAL:

 # 389-console

==> Ejecutar de forma REMOTA:

 # ssh -X root@192.168.1.150 /usr/bin/389-console -a http://192.168.1.150:9830





Referencias:

http://directory.fedoraproject.org/
http://www.unixmen.com/install-and-configure-ldap-server-in-centos-7/