

Autenticación de Cherokee con OpenLDAP



Autor: Alejandro Esteban Durango López

Correo electrónico: alejiitodurango@misena.edu.co

Versión del documento: 1.1

Fecha de creación: 02/12/11

Última modificación:03/12/11

Índice de contenido

1.Licencia (BSD).....	1
2.Introducción	2
3.Instalación del servidor OpenLDAP.....	2
3.1 Búsqueda de paquetes.....	2
4.Configuración de OpenLDAP.....	2
4.1 Búsqueda del directorio	2
4.2 Modificar el archivo slapd.conf.....	3
4.3 Reiniciar el servicio OpenLDAP.....	4
4.4 Configurando el dominio.....	5
4.5 Agregar el archivo.ldif al sistema.....	5
4.6 Crear usuarios	5
5.Instalación del servidor web Cherokee.....	6
5.1 Búsqueda de paquetes.....	6
5.2 Configuración de Cherokee.....	8
5.2.1 Habilitar conexiones remotas.....	8
5.2.2 Ingresar al administrador de Cherokee.....	8
5.2.3 Activar la autenticación LDAP.....	9
5.2.4 Reiniciar el servidor.....	11
5.2.5 Pruebas.....	12
6.Revisiones.....	13
7.Conclusiones.....	13

1. Licencia (BSD)

Copyright (c) 2011, Alejandro Durango,

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the **OpenBSD Colombia** nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR

A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

2. Introducción

En este manual vamos a explicar como realizar la instalación y configuración básica del servidor OpenLDAP en OpenBSD y explicaremos la instalación y configuración del [servidor web cherokee](#) para que se autentique contra el servicio ldap.

3. Instalación del servidor OpenLDAP

El escenario de prueba lo realizaré en una maquina virtual de VirtualBox, pero funciona perfectamente en un entorno en producción. La versión del S.O. es OpenBSD 5.0/x86 (en su instalación por omisión).

3.1 Búsqueda de paquetes

Para empezar vamos al ftp donde se encuentran todos los paquetes oficiales de OpenBSD, el sitio principal es <ftp://ftp.openbsd.org/> allí buscamos los paquetes de acuerdo a nuestra versión, en este caso la buscamos en <ftp://ftp.openbsd.org/pub/OpenBSD/5.0/packages/i386/> el paquete que vamos a instalar se llama **openldap-server-2.4.24p0.tgz** que es la versión mas actualizada que se encuentra allí, cuando encontremos este paquete le vamos a dar clic derecho copiar dirección del vinculo.

Luego vamos ir a nuestro sistema OpenBSD y copiamos lo siguiente para instalar este paquete:

```
#pkg_add -v ftp://ftp.openbsd.org/pub/OpenBSD/5.0/packages/i386/openldap-server-2.4.25p0.tgz
```

Veremos algo así:

```
# pkg_add -v http://ftp.openbsd.org/pub/OpenBSD/5.0/packages/i386/openldap-server-2.4.25p0.tgz
openldap-server-2.4.25p0:db-4.6.21p4: ok
openldap-server-2.4.25p0:icu4c-4.8p0: ok
openldap-server-2.4.25p0:cyrus-sasl-2.1.23p7: ok
openldap-server-2.4.25p0:openldap-client-2.4.25: ok
openldap-server-2.4.25p0: ok
The following new rcscripts were installed: /etc/rc.d/saslauthd /etc/rc.d/slaped
See rc.d(8) for details.
#
```

4. Configuración de OpenLDAP

4.1 Búsqueda del directorio

Antes de explicar la configuración del servicio OpenLDAP es necesario que conozca el siguiente comando que le ayudará a depurar los errores del servicio. Cuando se le presenten problemas que no logre identificar, intente usar estos comandos:

```
# /etc/rc.d/slaped stop
# /usr/local/libexec/slaped -d 9 -u _openldap
```

Así el servicio OpenLDAP funcionará común y corriente pero adicional mostrará todos los errores que se produzcan durante el momento del arranque o ejecución. Al usar este comando tendrá que usar otra terminal mientras termina el proceso de depuración.

Para arrancar el servicio de modo normal puede usar el comando:

```
# /etc/rc.d/slapd start
```

El archivo de configuración de openldap se encuentra en el siguiente directorio

```
#cd /etc/openldap
```

```
# pwd
```

```
/etc/openldap
```

```
# ls -la
```

```
total 28
```

```
drwxr-xr-x  3 root  wheel   512 Dec  2 01:19 .
drwxr-xr-x 24 root  wheel  2560 Dec  2 01:19 ..
-rw-r--r--  1 root  wheel   245 Dec  2 01:19 ldap.conf
drwxr-xr-x  2 root  wheel   512 Dec  2 01:19 schema
-rw-r----- 1 root  _openldap 2107 Dec  2 01:19 slapd.conf
#
```

Y el archivo de configuración es:

```
#vi slapd.conf
```

4.2 Modificar el archivo slapd.conf

Una vez ingresemos al directorio, vamos a modificar las siguientes líneas:

```
database      bdb
suffix        "dc=my-domain,dc=com"
rootdn        "cn=Manager,dc=my-domain,dc=com"
```

Y las cambiaremos por nuestra propia información:

```
#####
# BDB database definitions
#####
database      bdb
suffix        "dc=alejo,dc=durango,dc=2011,dc=com"
rootdn        "cn=admin,dc=alejo,dc=durango,dc=2011,dc=com"
# Cleartext passwords, especially for the rootdn, should
# be avoid.  See slappasswd(8) and slapd.conf(5) for details.
# Use of strong authentication encouraged.
rootpw        149822
# 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/openldap-data
# Indices to maintain
index objectClass eq
database monitor
```

Note que también agregamos en la última línea el monitoreo a nuestro backend.

Explicación:

suffix: Será nuestro dominio al estilo Ldap

rootdn: Usuario administrador del dominio

rootpw: Contraseña del usuario administrador del dominio (en este caso esta en texto plano), en caso de que quiera usar un hash puede leer la documentación del comando *slappasswd*.

database monitor: Permite habilitar el monitoreo a nuestro backedn BDB.

Ejemplo:

```
# slappasswd
New password:
Re-enter new password:
{SSHA}Av1JIImwDILsw7wm7VQ6E5OfS5jo3yh
#
```

4.3 Reiniciar el servicio OpenLDAP

Para probar que todo esta bien debemos reiniciar el servicio, lo hacemos con el siguiente comando:

```
#!/etc/rc.d/slapd restart
```

```
s lapd(ok)
s lapd(ok)
```

Es posible que por facilidad para nuestra configuración desemos trabajar con la nueva estructura de configuración de OpenLDAP, en ese caso necesitamos convertir el archivo *slapd.conf* a la estructura basada en directorios.

```
# pwd
/etc/openldap
# mkdir slapd.d
# slapttest -f slapd.conf -F slapd.d
config file testing succeeded
# chown -R _openldap:_openldap slapd.d
```

Observe que es necesario ponerle permisos al directorio para el usuario propietario del servicio OpenLDAP en ejecución.

De ahí en adelante podemos trabajar con la configuración del directorio *slapd.d*, pero debemos tener en cuenta que el servicio OpenLDAP evalúa primero si existe el archivo *slapd.conf* para luego ir al directorio, así que tendremos que eliminar o renombrar el archivo *slapd.conf* para usar nuestra nueva configuración. El directorio de configuración tiene una estructura similar a esta:

```
# pwd
/etc/openldap
# ls -l slapd.d/cn\=config
total 180
drwxr-x--- 2 root wheel  512 Dec  2 11:47 cn=schema
-rw----- 1 root wheel 79166 Dec  2 11:47 cn=schema.ldif
-rw----- 1 root wheel  525 Dec  2 11:47 olcDatabase={-1}frontend.ldif
```

```
-rw----- 1 root wheel 513 Dec 2 11:47 olcDatabase={0}config.ldif
-rw----- 1 root wheel 2261 Dec 2 11:47 olcDatabase={1}bdb.ldif
-rw----- 1 root wheel 465 Dec 2 11:47 olcDatabase={2}monitor.ldif
#
```

4.4 Configurando el dominio

Lo que hicimos en el punto 4.2 fue definir cual es el usuario administrador del dominio pero aun no tenemos el dominio para trabajar en ldap, para agregar un nuevo dominio tenemos que crear un archivo ldif (puede tener cualquier nombre) que contenga la información básica.

```
#cd /etc/openldap
#vi archivo.ldif
```

Al archivo se le debe agregar la siguiente información, recuerde que esta información debe estar relacionada con la que se configuró en el punto 4.2.

```
dn: dc=alejo,dc=durango,dc=2011,dc=com
objectClass: top
objectclass: organization
objectclass: dcObject
dc: alejo
o: Dominio de Alejandro
```

4.5 Agregar el archivo.ldif al sistema

Después de crear el archivo ldif debemos agregarlo al ldap lo hacemos con el siguiente comando, recuerde que esta línea cambia según su propio RootDN.

```
#ldapadd -x -D "cn=admin,dc=alejo,dc=Durango,dc=2011,dc=com" -W -f archivo.ldif
```

Una vez ingresada la contraseña del administrador nos debe agregar el dominio al servidor OpenLDAP, si todo salió bien nos debe mostrar lo siguiente:

```
Enter LDAP Password:
adding new entry "dc=alejo,dc=durango,dc=2011,dc=com"
```

Si se presenta algún error, por favor verifique la estructura del archivo .ldif o verifique la línea de comando introducida.

4.6 Crear usuarios

Ahora vamos a crear los usuarios que se van a autenticar en el servidor cherokee, para hacerlo más fácil administraremos el servidor OpenLDAP desde una herramienta gráfica multiplataforma que se llama [Apache Directory Studio](#) o podemos usar [PHPMyLdapAdmin](#), [JXplorer](#) que también son herramientas libres que nos permite administrar el servicio de una forma mas sencilla.

Primero tenemos que crear una unidad organizacional (OU) que va a contener los usuarios del que queremos autenticar, en este caso la voy a llamar **user** y le agregaremos los siguientes atributos:

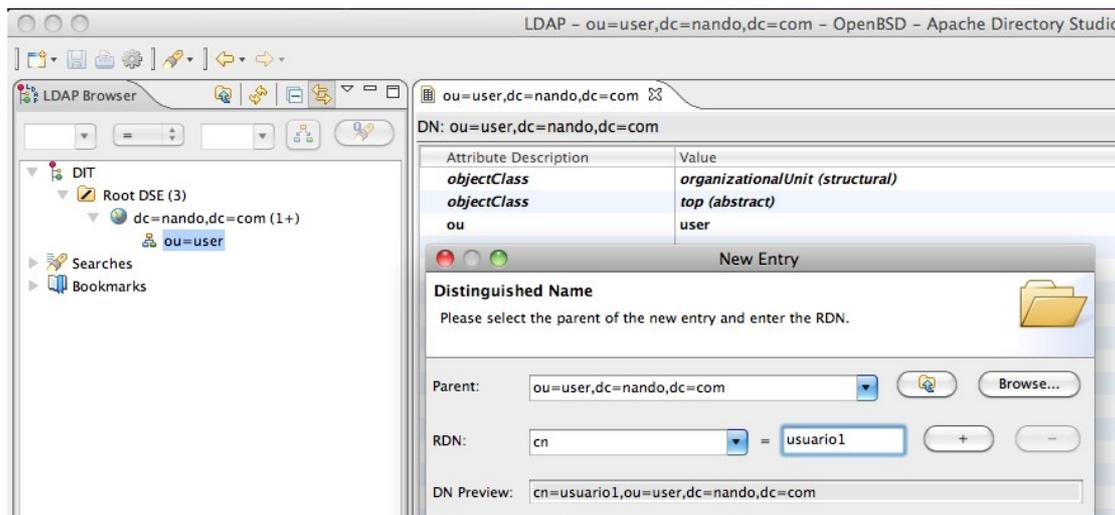
objectClass	organizationalUnit (structural)
objectClass	top (abstract)
ou	user

Luego dentro de esta OU vamos a crear los usuarios que como mínimo deben tener los siguientes atributos: *cn*, *sn*, *userPassword*. El atributo *cn* será el que usaremos como filtro para que cherokee pueda encontrar los usuarios y validarlos.

objectClass	organizationalPerson (structural)
objectClass	person (structural)
objectClass	top (abstract)
cn	user1
sn	user1
userPassword	SSHA hashed password

En este punto podemos crear todos los usuarios que hagan falta siguiendo el mismo procedimiento.

Un ejemplo:



5. Instalación del servidor web Cherokee

Actualmente hay paquetes disponibles para OpenBSD 5.0, sin embargo la versión de cherokee que encontramos no es la mas actualizada. En este momento se encuentran actualizando el port de cherokee a la nueva versión, esperemos que para la nueva release tengamos la última versión disponible. Recuerde que si desea tener la última versión puede estar pendiente de los cambios que ocurren en la versión current de OpenBSD y aplicar los parches manualmente.

5.1 Búsqueda de paquetes

Como lo dije antes, tenemos que ir al ftp donde están los paquetes <ftp://ftp.openbsd.org/>, allí buscamos los paquetes de acuerdo a nuestra versión y arquitectura en este caso la buscamos en <ftp://ftp.openbsd.org/pub/OpenBSD/5.0/packages/i386/> el paquete que vamos a instalar se llama **cherokee-ldap-1.0.14p3.tgz** esta versión de cherokee viene con la funcionalidad de poderse autenticar con el servicio ldap realizando una configuración muy sencilla, a este paquete le vamos a dar clic derecho copiar dirección del vinculo.

Luego vamos ir a nuestro sistema OpenBSD y copiamos lo siguiente para instalar este paquete:

```
#pkg_add -v ftp://ftp.openbsd.org/pub/OpenBSD/5.0/packages/i386/cherokee-ldap-1.0.14p3.tgz
```

Veremos algo así:

```
# pkg_add -v ftp://mirror.team-cymru.org/pub/OpenBSD/5.0/packages/i386/cheroke>
cherokee-ldap-1.0.14p3:spawn-fcgi-1.6.3p0: ok
cherokee-ldap-1.0.14p3:png-1.5.4: ok
cherokee-ldap-1.0.14p3:libart-2.3.21: ok
cherokee-ldap-1.0.14p3:rrdtool-1.2.30p3: ok
cherokee-ldap-1.0.14p3:libxml-2.7.8p2: ok
cherokee-ldap-1.0.14p3:femail-0.97p1: ok
cherokee-ldap-1.0.14p3:femail-chroot-0.97p3: ok
cherokee-ldap-1.0.14p3:php-5.2.17p5|***** i 79%
```

Es posible que tu sistema instale mas o menos dependencias, dependiendo de lo que hayas seleccionado al inicio de la instalación del sistema operativo y de otras utilidades básicas que hayas instalado, tales como: *bash, nano, wget, etc.*

Al finalizar el proceso de instalación de cherokee, te deberías encontrar con algo similar a lo que vemos en el siguiente pantallazo, recuerda ejecutar los comandos recomendados por las utilidades php, python y otros.

```
cherokee-ldap-1.0.14p3:cherokee-1.0.14p6: ok
cherokee-ldap-1.0.14p3: ok
The following new rcscripts were installed: /etc/rc.d/cherokee
See rc.d(8) for details.
--- +cherokee-1.0.14p6 -----
To complete the installation, you need to configure cherokee. As root:

    # /usr/local/sbin/cherokee-admin -b[IP] -p[PORT]

(by default it will bind to 127.0.0.1 on port 9090).
--- +femail-chroot-0.97p3 -----
By default, femail will use `localhost' for smtp host. Make sure to
review FAQ Section 10.16 discussing name resolution with httpd(8)'s
default chroot(2).

Additionally, one may create a custom femail.conf; see femail(8).

If you're using femail with PHP inside a chroot jail, be aware that
PHP's built-in "mail" function uses popen(), which requires /bin/sh.
--- +php-5.2.17p5 -----
To enable the php-5.2 module please create a symbolic
link from /var/www/conf/modules.sample/php-5.2.conf
to /var/www/conf/modules/php.conf.

ln -s /var/www/conf/modules.sample/php-5.2.conf \
    /var/www/conf/modules/php.conf

The recommended php configuration has been installed
to /etc/php-5.2.ini.
--- +python-2.7.1p9 -----
If you want to use this package as your default system python, as root
create symbolic links like so (overwriting any previous default):
ln -sf /usr/local/bin/python2.7 /usr/local/bin/python
ln -sf /usr/local/bin/python2.7-2to3 /usr/local/bin/2to3
ln -sf /usr/local/bin/python2.7-config /usr/local/bin/python-config
ln -sf /usr/local/bin/pydoc2.7 /usr/local/bin/pydoc
#
```

Como se recomienda en el proceso de instalación debemos ejecutar los comandos de enlaces simbólicos que hacen que los binarios apunten a las rutas estándar.

```
# ln -s /var/www/conf/modules.sample/php-5.2.conf \  
> /var/www/conf/modules/php.conf  
# ln -sf /usr/local/bin/python2.7 /usr/local/bin/python  
# ln -sf /usr/local/bin/python2.7-2to3 /usr/local/bin/2to3  
# ln -sf /usr/local/bin/python2.7-config /usr/local/bin/python-config  
# ln -sf /usr/local/bin/pydoc2.7 /usr/local/bin/pydoc
```

5.2 Configuración de Cherokee

La administración de cherokee la vamos a hacer desde el administrador web que trae incorporado este paquete.

5.2.1 Habilitar conexiones remotas

Por defecto el administrador web de cherokee solo acepta conexiones locales, lo primero que vamos a hacer es activar las conexiones remotas esto lo hacemos con el siguiente comando:

```
#cherokee-admin -b192.168.10.29
```

La dirección IP que se agrega en el comando es la dirección por la que se va a escuchar el servicio, si el comando se ejecutó correctamente debe mostrar algo parecido a esto:

```
# Cherokee Web Server 1.0.14 (Aug 16 2011): Listening on port 192.168.10.29:9090,  
TLS disabled, IPv6 enabled, using kqueue, 4096 fds system limit, max. 2041  
connections, caching I/O, 5 threads, 408 connections per thread, standard  
scheduling policy
```

Login:

User: admin

One-time Password: **pQxSfGJKxs143wxO**

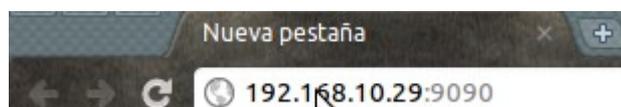
Web Interface:

URL: <http://192.168.10.29:9090/>

Nota: El password que nos dan varía cada vez que ejecutas este comando.

5.2.2 Ingresar al administrador de Cherokee

- Para ingresar al administrador gráfico de cherokee basta con digitar el URL que nos dieron en el punto anterior en el navegador



- Después digitamos el usuario y la contraseña que también nos dieron en el punto anterior

El servidor 192.168.10.29:9090 en Cherokee-admin requiere un nombre de usuario y una contraseña.

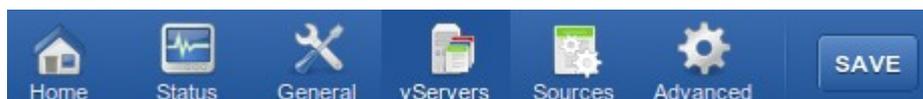
Nombre de usuario:

Contraseña:

- Si estos datos son correctos nos debe aparecer esto:

5.2.3 Activar la autenticación LDAP

- Para activar la autenticación en el ldap primero vamos a dar clic en *vservers* que se encuentra en esquina superior derecha de la ventana.



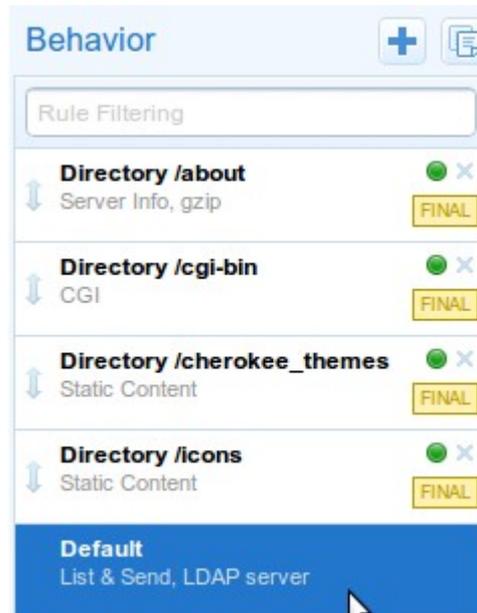
- Luego debemos dar clic sobre rule *management*.

Match	Handler	Auth	Root	Secure	Enc	Exp	Timeou	Shapin	Log	Final	Enable
Directory /about	Server Info				✓				✓	✓	✓
Directory /cgi-bin	CGI		✓						✓	✓	✓
Directory /cherokee themes	Static Content		✓						✓	✓	✓
Directory /icons	Static Content		✓						✓	✓	✓
Default	List & Send	LDAP s							✓	✓	✓

- Luego damos clic sobre *security*



- luego damos clic en **default** que se encuentra al lado derecho de la ventana



- Después en **Validation Mechanism** seleccionamos la opción de **LDAP server**

Authentication

Validation Mechanism

LDAP server ▼

Which, if any, will be the authentication method.

- Después se nos habilitarán unas opciones debajo de esta, que son:

- Método de autenticación, lo dejamos **basic**

Methods

Basic ▼

Allowed HTTP Authentication methods.

- Mensaje de bienvenida, ponemos el que deseemos

Realm

secret

Name associated with the protected resource.

- Usuario, no hay necesidad de ponerlo (solo si queremos filtrar algunos usuarios)

Users

Optional

User filter. List of allowed users.

- Dirección IP donde se encuentra el servidor OpenLDAP, en este caso como están en la misma maquina los dos servicios colocamos **localhost**

Server

localhost

LDAP server IP address.

- Puerto por el que esta escuchando el servidor ldap, ponemos el que trae por defecto

- Usuario administrador del dominio, *el rootdn del punto 4.2*

Bind Domain

cn=admin,dc=alejo,dc=durango,dc=2011,dc

Domain sent during the LDAP authentication operation. Optional.

- Contraseña del usuario administrador, *el rootpw del punto 4.2*

Bind Password

149822

Password to authenticate in the LDAP server.

- Dominio base, *el suffix del punto 4.2*

Base Domain

dc=alejo,dc=durango,dc=2011,dc=com

Domain sent during the LDAP authentication operation. Optional.

- Filtro para buscar a los usuarios

(Ver http://www.cherokee-project.com/doc/modules_validators_ldap.html)

Filter

cn=\${user}

Object filter. It can be empty.

- Los demás los dejamos como están

Use TLS

Enabled

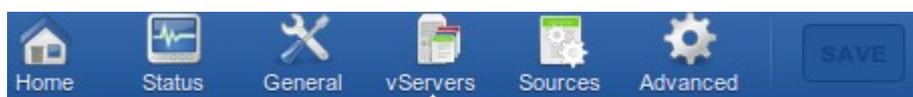
Enable to use secure connections between the web and LDAP servers.

CA File

Optional

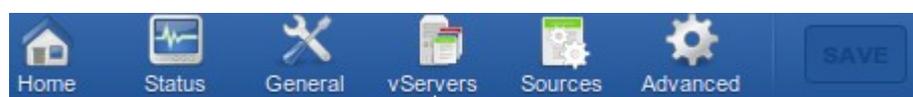
CA File for the TLS connections.

- Luego guardamos la configuración dando clic en **save** que se encuentra en la parte superior de la ventana.



5.2.4 Reiniciar el servidor

- Vamos iniciar el servidor cherokee para poder realizar pruebas, para iniciar el servidor vamos a dar clic en **home**



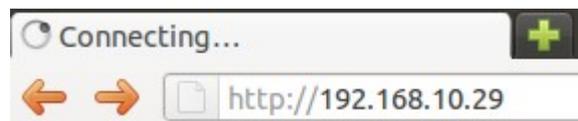
- Luego vamos a dar clic en **start server** para arrancar nuestro servidor.

Si todo salió bien, ya tendremos nuestro servidor Cherokee funcionando listo y configurado para validarse contra LDAP.

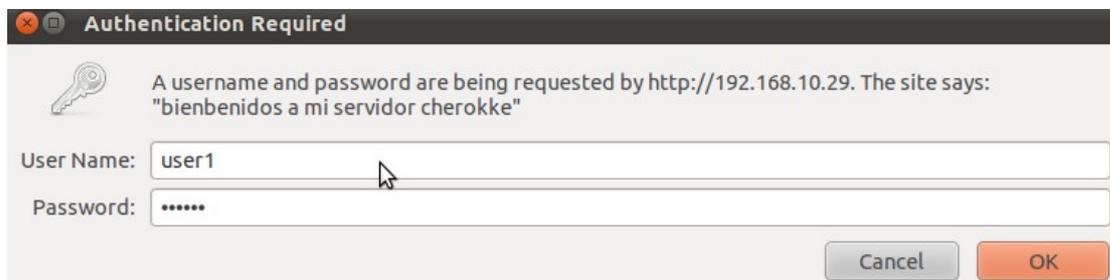
Server Information	Server is not Running	Start Server
Hostname	alejo.redsena.net	
Config File	/etc/cherokee/cherokee.conf	
Processors	2288 MHz, 1 Logical Processors, 1 Cores	4%
Memory	199MB	0.1GB Used, 0.1GB Free 57.0%

5.2.5 Pruebas

- Ya todo esta listo ahora solo falta hacer pruebas para ello vamos a nuestro navegador y digitamos la dirección ip de nuestro servidor (*sin el :9090*)



- Nos mostrara la siguiente ventana, donde digitaremos un usuario de los que creamos en el *punto 4.6* y usaremos su respectiva contraseña.



- Y si esta información es correcta nos debe mostrar la pagina de inicio de cherokee.



6. Revisiones

Nombre	Versión del Documento	Fecha	Comentarios
Fernando Quintero (@nonroot)	01/01/11	03/12/11	El comando para agregar el dominio estaba incorrecto, también agregué algunas explicaciones.

7. Conclusiones

- Es la primera vez que utilizo el sistema operativo OpenBSD, la motivación para crear este documento fue precisamente el interés en aprender los comandos y el funcionamiento básico del sistema operativo, este objetivo se logró.
- En el documento se puede apreciar que la configuración de los servicios de red es muy similar al sistema operativo Linux con el que estoy mas acostumbrado a trabajar, para realizar este documento no tuve muchos inconvenientes puesto que ya conocía la mayoría de los comandos.
- Podemos ver que Cherokee es un servidor web flexible y fácil de usar y que su entorno de administración gráfico, nos permite realizar procedimientos que en otros servidores podrían ser mas complejos.
- La plantilla usada para escribir el documento me presentó algunos problemas, la verdad descubrí que era mas fácil de usarla de lo que creía, antes de escribir un documento con la plantilla, deberíamos tomarnos el tiempo para entenderla.
- Le agradezco a Fernando Quintero (@nonroot), por el apoyo y revisión durante el proceso de elaboración de este documento.