NoCatBOX HOWTO v1.4
NoCatAuth + Gateway Installation on the same machine

Toni dlF. Diaz
toni@blyx.com
September 2003

ChangeLog:

1.0 Initial release (12/9/2003)
1.1 Added `chmod +x throttle.fw` (15/9/2003)
1.2 Added NoCat Gateway stats note. (3/10/2003)
1.3 Added MySQL user repository configuration. (8/10/2003)
1.4 Added managing groups and OpenLDAP user repository configuration. (23/10/2003)

Description:

NoCatAuth is a software written in perl that allows control of the access in a net through a captive portal. This captive portal is used to control the access to type 802.11 networks, is formed by a gateway and a authentication service. Allows three kind of access, two authenticated: Owner and Member and one without authentication needed: Guest.

Imagine you enter a large building (Internet) trough the door (Gateway) and the porter (NoCatAuth) ask you for accreditation, there are three kind of people (Users) that access the building, the visitors (Guest), the workers (Member) and the managers (Owner). The visitors can only move inside the building by walking, the workers only can use the electric stairs and the managers can do what they want and use the lift. We are going to install in a similar machine with linux “a door with a door man“.

This manual is written for NoCatAuth version 0.82 and is being developed actively by Rober Flickenger and Schuyler Erle, the project web is http://nocat.net.

Objectives:

The objective of this document is to install in the same machine a gateway and an autentication service after an HostAP wireless access point has been installed. This HostAP can be for a local network or for your wireless community. The authentication service can however be installed in another machine on the network.

All software and configuration files used are available through the following link: http://blyx.com/public/wireless/nocatbox/ in addition some configuration files are available in the appendix of this document.

For a better understanding of the way NoCatAuth works, we strongly recommend the reading of the following documents:

http://lists.nocat.net/pipermail/nocat/2002-July/001791.html (english)
http://blyx.com/public/wireless/wifi-auth.pdf (spanish)

The linux distribution used for the development of this manual is RedHat Linux 9 and kernel 2.4.21.

In order to obtain the correct operation of NoCatAuth, it is necessary to have installed a certain software.

Requirements:

-Kernel 2.4.X with iptables:

There is a kernel configuration example in the etc/ directory, inside the NoCatAuth-0.82.tar.gz package.

-HostAP-0.0.X:

For installation and adequate running of HostAP I recommend these manuals:
http://madridwireless.net/docs/hostap/ap-hostap-1.1.pdf (spanish)
http://www.blyx.com/more.php?id=18_0_1_0_M4 (spanish)
http://www.blyx.com/more.php?id=22_0_1_0_M4 (english)

-Apache web server 1.3.27 + mod_ssl

If you do not have experience installating Apache with mod_ssl try with
http://www.apachetoolbox.com

-Perl version equal or upper to 5.6 (to see the version: #perl -v):

NoCatAuth is written in Perl this is why some modules are needed for an adequate operation, the required modules depend, most of them, on the authentication method used. In this manual we will use a file with users and passwords, so these perl modules will be needed:

```
Digest-MD5
Net-Netmask
```

All the available modules for perl are in the following url:
http://www.cpan.org/modules/01modules.index.html
Nevertheless the modules can be installed as .deb or .rpm packages depending on the distribution.

-DHCP 3.0 of ISC (configuration file in the Appendix).

-DNS server in the same machine or in the same net.

Is recommended but no mandatory to have DNS cache in the local machine.

GnuPG installation:

GnuPG is used to sign the queries between the gateway and the authentication service:

Install gnupg-1.2.3.tar.bz2,

```
# tar zxvf gnupg-1.2.3.tar.bz2
# cd gnupg-1.2.3
# ./configure
# make
# make install
```

You can also install it by packages from the adequate distribution.

NocatAuth-0.82 installation and configuration:

```
# tar zxvf NoCatAuth-0.82.tar.gz
# cd NoCatAuth-0.82
# mkdir /usr/local/nocat
# make PREFIX=/usr/local/nocat/gateway gateway
# make PREFIX=/usr/local/nocat authserv
# make PREFIX=/usr/local/nocat pgpkey
# cp /usr/local/nocat/trustedkeys.gpg /usr/local/nocat/gateway/pgp
# chown -R nobody:nobody /usr/local/nocat/pgp
```

Change nobody:nobody to the user:group used by your Apache web server.

```
# mv authserv-nocat.conf /usr/local/nocat/nocat.conf
# mv gw-nocat.conf /usr/local/nocat/gateway/nocat.conf
```

**Be careful with the configurations because the configuration file for the authentication service and for the gateway are called nocat.conf but each one content and function is different.

Edit /usr/local/nocat/nocat.conf and change the following parameters:

`LocalGateway`	`wlan0_ip` (example: 192.168.0.246)
`LocalNetwork`	`wlan0_network` (example: 192.168.0.0/24)

Edit /usr/local/nocat/gateway/nocat.conf and change the following parameters:

`AuthServiceAddr`	`eth0_ip` (example: 10.10.21.246)
`LocalNetwork`	`eth0_network` (example: 10.10.21.0/24)
`DNSAddr`	`dns_ip` (example: 10.10.21.20)
`Owners`	`your-user-name` (example: toni)

If you choose to install a DNS server in your NoCatBox remember you have to comment the DNSAddr line in the configuration file /usr/local/nocat/gateway/nocat.conf and add the appropriate line in /etc/resolv.conf.

Edit /usr/local/nocat/gateway/bin/throttle.fw and adjust the following directives as per your preferences and internet connection. This is the configuration I use for an ADSL 256/128 line:

```
TOTAL_DOWN=256kbit
TOTAL_UP=128kbit

OWNER_DOWN=256kbit     # fw mark 1
OWNER_UP=128kbit
OWNER_OPTIONS=""

COOP_DOWN=128kbit      # fw mark 2
COOP_UP=64kbit
COOP_OPTIONS=""

PUBLIC_DOWN=32kbit     # fw mark 3
PUBLIC_UP=32kbit
```

So that throttle.fw has effect:

```
# chmod +x usr/local/nocat/gateway/bin/throttle.fw
```

The firewall NoCatAuth configuration is located in /usr/local/nocat/gateway/nocat.conf specifically in these directives:

```
IncludePorts
ExcludePorts
```

By default NoCatAuth only excludes access to port 25 of each client.

Additional configurations:

DHCP 3.0 server of ISC configuration:

Install the dhcp server and copy dhcpd.conf in the /etc directory, then edit the starting script /etc/init.d/dhcpd and add wlan0 to the following line, inside the start section:

```
daemon /usr/sbin/dhcpd wlan0 ${DHCPDARGS}
```

Apache web server for SSL use configuration:

Copy nocat-apache-ssl.conf named ssl.conf in the Apache configuration directory and modify the SSLCertificateFile and SSLCertificateKeyFile directives path to point to server.crt and server.key respectively.

Probably you will have to modify in ssl.conf & the log file (CustomLog) path as well.

Edit httpd.conf (an example of httpd.conf) and add in the end of the Apache configuration file this line:

```
Include conf/ssl.conf
```

Copy NoCatAuth-0.82/etc/authserv.conf in the /usr/local/nocat/etc/ directory.

Starting scripts configuration:

```
# cp run-nocatbox  a /etc/rc.d/init.d/
# chmod +x /etc/rc.d/init.d/run-nocatbox
```

Running our NoCatBox:

Start the web server:

```
# {apache-path}/bin/apachectl startssl
```

Start NoCatAuth and the dhcp server with the run_nocatbox script:

```
# /etc/rc.d/init.d/run_nocatbox start
```

To see your NoCat Gateway stats open your web browser and type:

```
http://localhost:5280/status
```

Users administration:

Create the Owner account as we have indicated in /usr/local/nocat/gateway/nocat.conf:

```
# /usr/local/nocat/bin/admintool -c your-user-name password
```

To add a Member user and Members group (for member class is needed to add user to group):

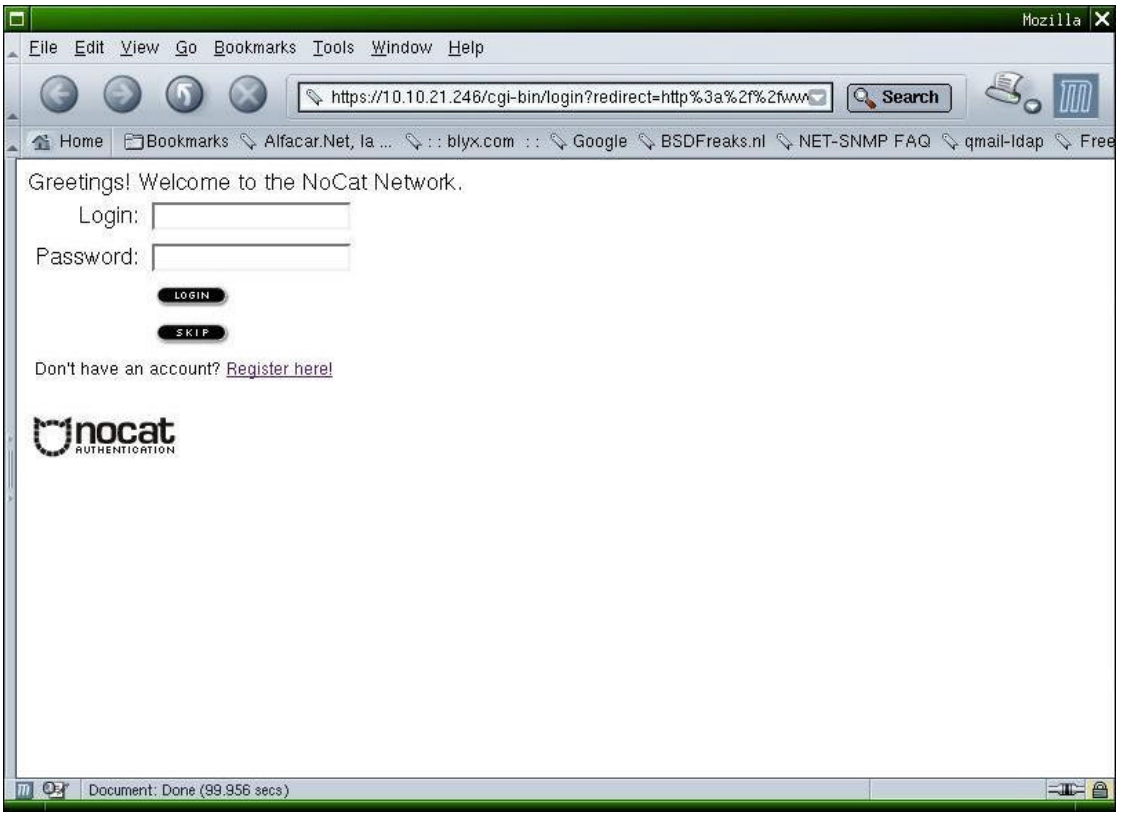
```
# /usr/local/nocat/bin/admintool -c user password
# /usr/local/nocat/bin/admintool -a user members
```

Any client that is not in a group will be considered in Public Class.

The Client side:

Configure the client to connect to our AP trough the wireless network, modify the network configuration to obtain IP address through dhcp. NoCatBox will assign an IP address, a DNS server and a gateway amongst other things.

Start your favourite navigator and try to go to some web sites. If everything is ok, you should be looking at a safe web page asking for our accreditation:

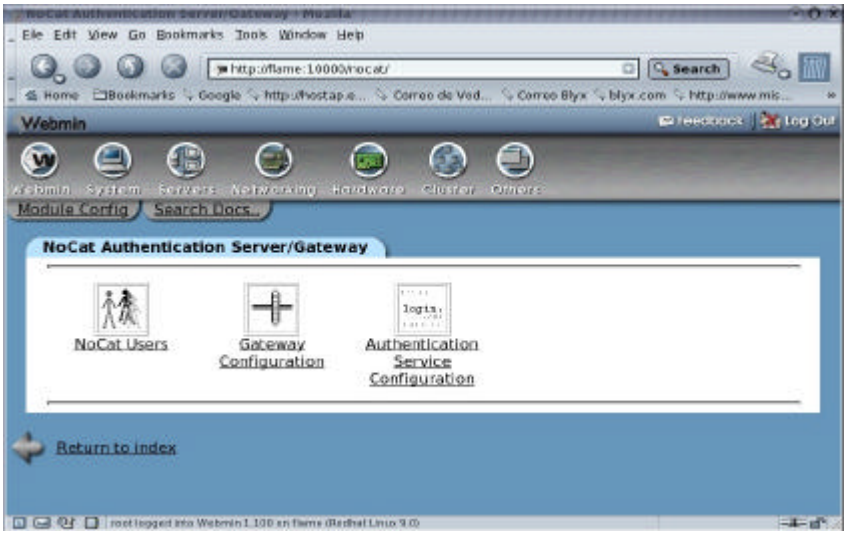


Enter the user and password we have supplied you with, add with the admintool utility and NoCatAuth automatically will readdress you to the web we had typed previously. We will then see a “popup“ window indicating our connection timeout:

While the client authentication takes place, in our gateway log (/usr/local/nocat/gateway/nocat.log) we can see:

```
[2003-09-10 01:38:31] Gateway running on port 5280.
[2003-09-10 01:38:41] Spawning child process 15682.
[2003-09-10 01:38:41] Connection to 192.168.0.246 from 192.168.0.120
[2003-09-10 01:38:41] Capturing  192.168.0.120  for http://www.google.com/
[2003-09-10 01:38:41] Notifying parent of Capture on peer 00:01:F4:EC:EF:22
[2003-09-10 01:38:41] Got notification Capture of peer 00:01:F4:EC:EF:22
[2003-09-10 01:38:41] Child process returned 1
[2003-09-10 01:39:00] Spawning child process 15685.
[2003-09-10 01:39:00] Connection to 192.168.0.246 from 192.168.0.246
[2003-09-10 01:39:00] Received notify 00:01:F4:EC:EF:22 from 192.168.0.246
gpgv: Firma creada el mié 10 sep 2003 01:39:00 CEST usando clave DSA ID 5931264A
gpgv: Firma correcta de "Toni Blyx <toni@blyx.com>"
[2003-09-10 01:39:00] Got auth msg Redirect     http://www.google.com/
Mac     00:01:F4:EC:EF:22
Action  Permit
User    toni
Mode    login
Timeout 600
Token   $1$92063757$EgD2gx5LOTeHfnvc4AjVb/
[2003-09-10 01:39:00] User  toni  permitted in class Owner
[2003-09-10 01:39:00] Notifying parent of Permit on peer 00:01:F4:EC:EF:22
[2003-09-10 01:39:00] Available MACs: 00:01:F4:EC:EF:22
[2003-09-10 01:39:00] Responding with:
User    toni
Token   $1$1$lpNwKF/E4m/s/FvggrZPX0
Timeout 600
[2003-09-10 01:39:00] Got notification Permit of peer 00:01:F4:EC:EF:22
[2003-09-10 01:39:00] Child process returned 1
```

For NoCatAuth configuration and administration via web, a webmin module can be used (http://www.webmin.com) available for NoCatAuth in the following URL ftp://ftp.sourceforge.net/pub/sourceforge/nocat-webmin/nocat-0.50.wbm :



NoCatAuth 0.82 + MySQL for users repository:

Needed Software:

Perl Modules:

```
Net::Netmask
perl-DBD-Mysql
perl-DBI y
MySQL Server Version > 3.23.4X
```

Running MySQL:

```
# /etc/init.d/mysqld start
Iniciando base de datos MySQL:                             [  OK  ]
Iniciando MySQL:                                           [  OK  ]
```

Assigning password to user root for MySQL Server:

```
# mysqladmin password your-password
```

Creating the nocat DB:

```
# mysqladmin create nocat -p
Enter password:
```

Adding the nocat DB structure to MySQL:

```
# mysql nocat < nocat.schema -p
Enter password:
```

Now try if everyone it's ok on the DB:

```
# mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 16 to server version: 3.23.56

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql> show databases;
+----------+
| Database |
+----------+
| mysql    |
| nocat    |
| test     |
+----------+
3 rows in set (0.00 sec)

mysql> use nocat;
Database changed

mysql> show tables;
+-----------------+
| Tables_in_nocat |
+-----------------+
| eventlog        |
| hardware        |
| member          |
| network         |
| node            |
+-----------------+
5 rows in set (0.00 sec)

mysql> desc eventlog;
+----------+---------------------+------+-----+---------+----------------+
| Field    | Type                | Null | Key | Default | Extra          |
+----------+---------------------+------+-----+---------+----------------+
| id       | int(10) unsigned    |      | PRI | NULL    | auto_increment |
| class    | tinyint(3) unsigned |      |     | 0       |                |
| severity | tinyint(3) unsigned |      |     | 0       |                |
| event    | varchar(255)        | YES  |     | NULL    |                |
| created  | datetime            | YES  |     | NULL    |                |
```

```
+----------+--------------------+------+-----+---------+----------------+
5 rows in set (0.00 sec)

mysql> desc hardware;
+-------------+------------------+------+-----+---------+----------------+
| Field       | Type             | Null | Key | Default | Extra          |
+-------------+------------------+------+-----+---------+----------------+
| id          | int(10) unsigned |      | PRI | NULL    | auto_increment |
| mac         | varchar(17)      | YES  |     | NULL    |                |
| owner       | int(10) unsigned |      |     | 0       |                |
| description | varchar(255)     | YES  |     | NULL    |                |
| created     | datetime         | YES  |     | NULL    |                |
| modified    | timestamp(14)    | YES  |     | NULL    |                |
+-------------+------------------+------+-----+---------+----------------+
6 rows in set (0.00 sec)

mysql> desc member;
+-------------+---------------------+------+-----+---------+-------+
| Field       | Type                | Null | Key | Default | Extra |
+-------------+---------------------+------+-----+---------+-------+
| url         | varchar(255)        | YES  |     | NULL    |       |
| description | text                | YES  |     | NULL    |       |
| created     | datetime            | YES  |     | NULL    |       |
| modified    | timestamp(14)       | YES  |     | NULL    |       |
| status      | tinyint(3) unsigned | YES  |     | NULL    |       |
| login       | varchar(250)        |      | PRI |         |       |
| pass        | varchar(255)        |      |     |         |       |
| name        | varchar(255)        | YES  |     | NULL    |       |
+-------------+---------------------+------+-----+---------+-------+
8 rows in set (0.00 sec)

mysql> desc network;
+----------+--------------+------+-----+---------+-------+
| Field    | Type         | Null | Key | Default | Extra |
+----------+--------------+------+-----+---------+-------+
| login    | varchar(250) |      | PRI |         |       |
| network  | varchar(250) |      | PRI |         |       |
| admin    | char(1)      | YES  |     |         |       |
| created  | datetime     | YES  |     | NULL    |       |
| modified | timestamp(14)| YES  |     | NULL    |       |
+----------+--------------+------+-----+---------+-------+
5 rows in set (0.00 sec)

mysql> desc node;
+-----------+---------------------+------+-----+---------+----------------+
| Field     | Type                | Null | Key | Default | Extra          |
+-----------+---------------------+------+-----+---------+----------------+
| id        | int(10) unsigned    |      | PRI | NULL    | auto_increment |
| owner     | int(10) unsigned    |      |     | 0       |                |
| address   | varchar(255)        | YES  |     | NULL    |                |
| service   | tinyint(3) unsigned | YES  |     | NULL    |                |
| range     | tinyint(3) unsigned | YES  |     | NULL    |                |
| bandwidth | tinyint(3) unsigned | YES  |     | NULL    |                |
| created   | datetime            | YES  |     | NULL    |                |
| modified  | timestamp(14)       | YES  |     | NULL    |                |
| lat       | float               | YES  |     | NULL    |                |
| lon       | float               | YES  |     | NULL    |                |
+-----------+---------------------+------+-----+---------+----------------+
10 rows in set (0.01 sec)

mysql> exit
Bye
```

Making that nocat DB is property of the user *nocat* with password *nocatauth*:

```
# mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 17 to server version: 3.23.56

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql> grant all on nocat.* to nocat@localhost identified by 'nocatauth';
Query OK, 0 rows affected (0.04 sec)
```

```
mysql> flush privileges;
Query OK, 0 rows affected (0.00 sec)

mysql> quit
Bye
```

Verifying that we have granted the privileges to the user nocat (-ppassword is without space character):

```
# mysql -u nocat -pnocatauth
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 18 to server version: 3.23.56

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql> use nocat;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
+-----------------+
| Tables_in_nocat |
+-----------------+
| eventlog        |
| hardware        |
| member          |
| network         |
| node            |
+-----------------+
5 rows in set (0.00 sec)
```

We need to edit NoCatAuth configuration file (/usr/local/nocat/nocat.conf) to change authentication section:

```
##### Authservice authentication source.
#
# DataSource -- specifies what to authenticate against.
#   Possible values are DBI, Passwd, LDAP, RADIUS, PAM, Samba, IMAP, NIS.
#
DataSource      DBI
##
# Auth service database settings.
#
# If you select DataSource DBI, then Database, DB_User, and DB_Password
#   are required.
#
# Database is a DBI-style data source specification.
#
# For postgres support:
# Database      dbi:Pg:dbname=nocat
#
# For mysql support:

Database        dbi:mysql:database=nocat
DB_User         nocat
DB_Passwd       nocatauth
```

We add users to our new nocat data base with admintool NoCatAuth utility (probably you must read User Administration section of this document):

```
# /usr/local/nocat/bin/admintool -c toni password
```

Remembers that you must add users to the corresponding groups for the class members.

We verified that we have added the user correctly to members table:

```
# mysql -u nocat -pnocatauth
Welcome to the MySQL monitor.  Commands end with ; or \g.


Your MySQL connection id is 22 to server version: 3.23.56
```

```
Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql> use nocat;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> select * from member;
+------+-------------+---------+----------------+--------+---------+----------------------+------+
| url  | description | created | modified       | status | login   | pass                 | name |
+------+-------------+---------+----------------+--------+---------+----------------------+------+
| NULL | NULL        | NULL    | 20031007171235 |   NULL | toni    |pZIMzues3lYNIq8c4JIZug  | NULL |
+------+-------------+---------+----------------+--------+---------+----------------------+------+
1 rows in set (0.00 sec)

mysql> exit
Bye
```

Now we have available our user repository stored on MySQL Data Base Server.

NoCatAuth 0.82 + OpenLDAP for users repository:

Needed software:

```
OpenLDAP Server and clients (my version is 2.0.27-8)
```

Perl modules:

```
Net::LDAP
IO::Socket::SSL
```

Needed files are on http://blyx.com/public/wireless/nocatbox/

To install ldap modules from CPAN try with:

```
# perl -MCPAN -e shell
cpan> install Net::LDAP
cpan> install IO::Socket::SSL
```

If you have problems with CPAN try downloading from http://www.cpan.org

Changing our openldap configuration /etc/openldap/slapd.conf

```
suffix          "dc=blyx,dc=com"
rootdn          "cn=Manager,dc=blyx,dc=com"
rootpw          secret
loglevel 256
```

Make sure that inetorgperson.schema is included in slapd.conf

Add the next line to /etc/syslog.conf and you must to create ldap dir for logs:

```
local4.*                                                /var/log/ldap/ldap.log
# mkdir /var/log/ldap
```

Restart syslogd and run openldap:

```
# /etc/init.d/syslog restart
Desactivando el generador de logs del kernel:             [  OK  ]
Desactivando el generador de logs del sistema:            [  OK  ]
Iniciando logger del sistema:                             [  OK  ]
Iniciando el generador de logs del kernel:                [  OK  ]

# /etc/ini.d/ldap start
Iniciando slapd:                                          [  OK  ]
```

Adding our ldap base tree:

```
# ldapadd -x -f basedn.ldif -D "cn=Manager,dc=blyx,dc=com" -W
```

If you want to store your user password in MD5 format:

```
# slappasswd -h {MD5} -s 123456
{MD5}4QrcOUm6Wau+VuBX8g+IPg==
```

You must to replace in toni.ldif file:
```
userPassword: 123456
```
with
```
userPassword: {MD5}4QrcOUm6Wau+VuBX8g+IPg==
```

Adding a new user to Organizational Unit usuarios:
```
# ldapadd -x -f toni.ldif -D "cn=Manager,dc=blyx,dc=com" -W
```

To see the user stored in ldap database:
```
# ldapsearch -x -h 10.10.21.246 -D "cn=Manager,dc=blyx,dc=com" -w secret –b "dc=blyx,dc=com"
'(uid=toni)'
```

Now we are going to change NocatAuth service configuration /usr/local/nocat/nocat.conf:

```
 DataSource               LDAP

 LDAP_Host              10.10.21.246 #(your ldapserver ip)
 LDAP_Base              ou=usuarios,dc=blyx,dc=com
 LDAP_Admin_User        cn=Manager,dc=blyx,dc=com
 LDAP_Admin_PW          secret
 LDAP_Hash_Passwords    No
 LDAP_Search_as_Admin   Yes
 LDAP_Filter            uid
```

NoCatAuth is unable to add users with admintool utility in LDAP yet, then you need to use ldapadd procedure to manage your users with LDAP.

To learn more about OpenLdap: http://www.openldap.org/doc

References:

http://nocat.net
http://www.aerocube.com
http://www.linuxjournal.com/article.php?sid=6887

Appendix:

NoCatBox starting script - /etc/rc.d/init.d/run-nocatbox

```
#!/bin/sh
#
# run-nocatbox
#
#       This script starts for our NoCatBox services
#

# Source networking configuration.
. /etc/sysconfig/network
. /etc/sysconfig/wireless_network

# Check that networking is up.
[ ${NETWORKING} = "no" ] && exit 0

[ -f /usr/local/nocat/gateway/bin/gateway ] || exit 0

# See how we were called.
case "$1" in
  start)
        # Start daemons.
        echo -n "Starting nocat gateway: "
        echo -n " Bringing up interface ${INTERFACE}"
        /sbin/ifconfig ${INTERFACE} up
        echo
        /sbin/ifconfig ${INTERFACE} ${IP} netmask ${NETMASK} broadcast ${BROADCAST}
        echo
        echo -n "Restarting dhcpd"
```

```
        /etc/rc.d/init.d/dhcpd restart
        echo
        echo -n "Starting gateway"
        # eth1
        /usr/local/nocat/gateway/bin/gateway
        echo
        ;;
  stop)
        # Stop daemons.
        echo -n "Shutting down nocat gateway "
        killall gateway
        echo
        ;;
  restart)
        $0 stop
        $0 start
        ;;
  *)
        echo "Usage: wireless_nocat {start|stop|restart}"
        exit 1
esac

exit 0
```

DHCP configuration file – /etc/dhcpd.conf:

```
ddns-update-style interim;
ignore client-updates;

subnet 192.168.0.0 netmask 255.255.255.0 {

# --- default gateway
        option routers                  192.168.0.246;
        option subnet-mask              255.255.255.0;

        option domain-name              "madridwireless.net";
        option domain-name-servers      10.10.21.20;

        option time-offset              -18000; # Eastern Standard Time

        range dynamic-bootp 192.168.0.101 192.168.0.120;
        default-lease-time 21600;
        max-lease-time 43200;
}
```

/etc/sysconfig/wireless_network file (RedHat):

```
INTERFACE=wlan0
IP=192.168.0.246
NETMASK=255.255.255.0
BROADCAST=192.168.0.255
```

For document corrections or additions: toni@blyx.com

For newer versions and Spanish version go to: http://blyx.com

Toni dlF. Díaz - toni@blyx.com
English translation: Javier Mateo & Toni dlF. Díaz