SoftNAS™

#1 Best-Selling NAS in the Cloud

Powerful and Frictionless Storage Administration

Kerberos, LDAP, & NFSv4

Configuration Guide

Table of Contents

Overview

This document explains how to configure **NFSv4 Server** with **Kerberos** and **LDAP authentication**.
Using **Kerberos** and/or LDAP with NFSv4 enables use of NFSv4 while maintaining each user's and user group's security rights for files and folders.

The goal of this document is to describe how to setup a network to enable the following:

- User authentication is performed using a central **Kerberos** server (typically Active Directory)
- User information (UID/GID/home directories) is stored in a LDAP directory
- NFS automount information is stored in LDAP
- NFSv4 authentication using **Kerberos** is possible with support for legacy NFSv3 mounts.

Server Components

NFS server V4

A **Network File Server (NFS)** is a client/server application that allows all network users to access shared files stored on computers of different types. NFS provides access to shared files through an interface called the **Virtual File System (VFS)** that runs on top of **TCP/IP**. Users can manipulate shared files as if they were stored locally on the user's own hard disk.

Kerberos Authentication

Kerberos is a secure method for authenticating a request for a service in a computer network. **Kerberos** lets a user request an encrypted "ticket" from an authentication process that can then be used to request a particular service from a server. The user's password does not have to pass through the network.

LDAP Server

The Lightweight Directory Access Protocol (LDAP) is an application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network.

Note: **SoftNAS Cloud** does not support installation of Open LDAP servers on the **SoftNAS Cloud** server itself. To use LDAP, typically an LDAP server would already be running separately in a network environment, and **SoftNAS Cloud** would be configured to reference that LDAP server. Refer to the vendor's LDAP server documentation or Open LDAP configuration and setup information (not included with **SoftNAS Cloud**).

Kerberos Authentication

Kerberos is an industry-standard protocol with the ability to provide secure, mutual authentication in potentially insecure environments.

Prerequisites

Configuration Steps

Prerequisites

The following prerequisites are required for a successful **Kerberos** install:

- Server packages
- Time synchronization
- Host Names

Server Packages

To begin using **Kerberos**, the following packages should be installed in the **SoftNAS Cloud** server.

```
krb5-appl-servers
krb5-appl-clients
krb5-server
krb5-workstation
krb5-auth-dialog
krb5-devel-1.10.3
krb5-pkinit-openssl
krb5-server-ldap

 yum install krb###
### yum -y install krb5-pkinit-openssl krb5-server-ldap
```

Time Synchronization

All machines that will participate in **Kerberos** authentication must have a reliable, synchronized time source. If the difference in time between systems varies by more than a small amount (usually five minutes), systems will not be able to authenticate.
The following error will be displayed in this case, in a Red Hat Enterprise Linux 5 environment

```
kadmin: GSS-API (or kerberos) error while initializing kadmin interface
```

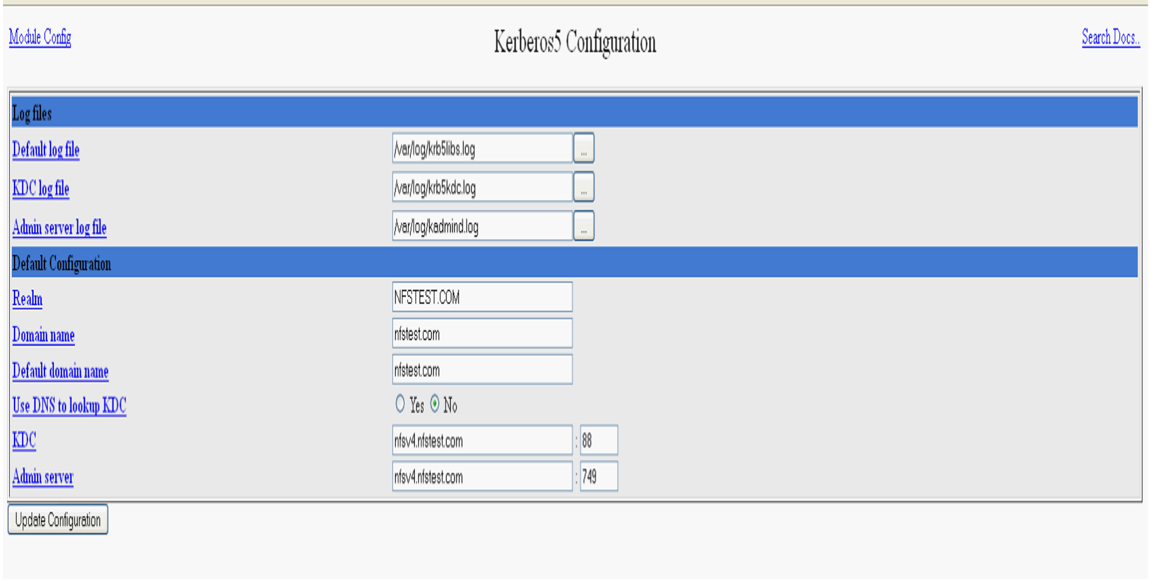
Resolution:

To resolve this error, it is necessary to ensure that the time between the client and the KDC is synchronized.

Host Names

All hosts must have their hostname set to the fully qualified hostname as reported by DNS. Both forward and reverse mapping must work properly. If the host name does not match the reverse DNS lookup, **Kerberos** authentication will fail.
To avoid this in the testing environment we have added the server name inside **`/etc/hosts`** file also in the clients hosts file.

```
10.185.147.225      nfsv4.nfstest.com   nfsv4 nfstest.com
```



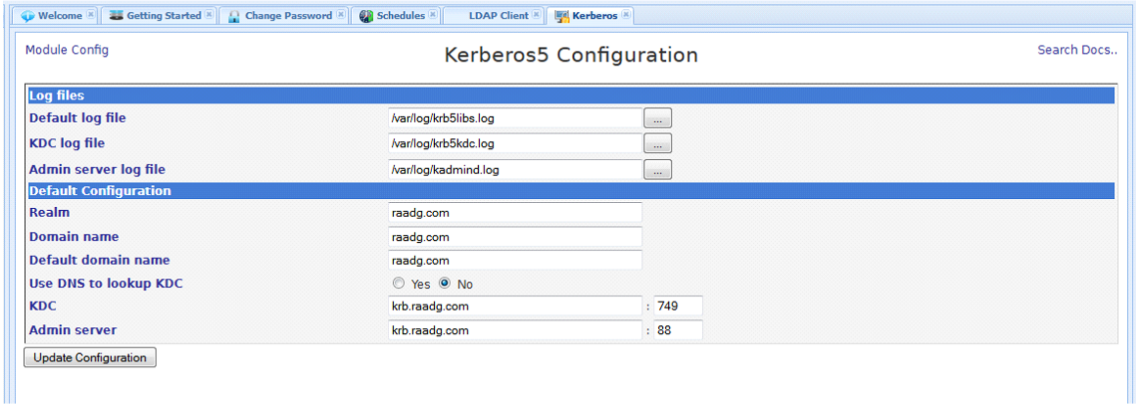
Module Config

Kerberos5 Configuration

Search Docs..

Log files	
Default log file	/var/log/krb5libs.log
KDC log file	/var/log/krb5kdc.log
Admin server log file	/var/log/kadmind.log
Default Configuration	
Realm	NFSTEST.COM
Domain name	nfstest.com
Default domain name	nfstest.com
Use DNS to lookup KDC	○ Yes ● No
KDC	nfsv4.nfstest.com : 88
Admin server	nfsv4.nfstest.com : 749

Update Configuration



Module Config

Kerberos5 Configuration

Search Docs..

Log files	
Default log file	/var/log/krb5libs.log
KDC log file	/var/log/krb5kdc.log
Admin server log file	/var/log/kadmind.log
Default Configuration	
Realm	raadg.com
Domain name	raadg.com
Default domain name	raadg.com
Use DNS to lookup KDC	○ Yes ● No
KDC	krb.raadg.com : 749
Admin server	krb.raadg.com : 88

Update Configuration

The above snapshot is the **Kerberos** Configuration for the configuration files.

```
/etc/krb5.conf && /var/kerberos/krb5kdc/kdc.conf && /var/kerberos/krb5kdc/
kadm5.acl

1./etc/krb5.conf
==============
[logging]
default = FILE:/var/log/krb5libs.log
kdc = FILE:/var/log/krb5kdc.log
admin_server = FILE:/var/log/kadmind.log

[libdefaults]
 default_realm = NFSTEST.COM
 dns_lookup_realm = false
 dns_lookup_kdc = false
 clockskew = 120
 ticket_lifetime = 24h
 renew_lifetime = 7d
 forwardable = true

[realms]
 NFSTEST.COM = {
  kdc = nfsv4.nfstest.com:88
  admin_server = nfsv4.nfstest.com:749
  default_domain = nfstest.com
 }

[domain_realm]
 .nfstest.com = NFSTEST.COM
 nfstest.com = NFSTEST.COM

[appdefaults]
 pam = {
   debug = false
   ticket_lifetime = 36000
   renew_lifetime = 36000
   forwardable = true
   krb4_convert = false
 }
 kinit = {
   ticket_lifetime = 36000
   renew_lifetime = 36000
   forwardable = true
 }

2./var/kerberos/krb5kdc/kdc.conf
==========================
 [kdcdefaults]
 kdc_ports = 88
 kdc_tcp_ports = 88

[realms]
 NFSTEST.COM = {
  acl_file = /var/kerberos/krb5kdc/kadm5.acl
  dict_file = /usr/share/dict/words
  admin_keytab = /var/kerberos/krb5kdc/kadm5.keytab
  supported_enctypes = aes256-cts:normal aes128-cts:normal des3-hmac-
sha1:normal des-cbc-md5:normal des-cbc-crc:normal
 }


3./var/kerberos/krb5kdc/kadm5.acl
========================
 */admin@NFSTEST.COM */
```

Configuration Steps

After the **Prerequisites** have been met, continue with the following procedural steps:

1. Create the **Kerberos** database
2. Add administrative user
3. Create host principal for the KDC (nfsv4)
4. Setup the default policy
5. Add normal users
6. Perform firewall configuration

Create Kerberos Database

Create the database with the following command.

```
[root@nfsv4] kdb5_util create -s
```

The default password is **nf$Server.** After primary access, change the password as per typical security best practices.

Add the First Administrative User

If administering as root, the first user defined should be root/admin. The default realm is appended automatically, so the command to use is as follows.

```
[root@nfsv4] kadmin.local -q "addprinc root/admin"
```

The default password is **nf$Server.** After primary access, change the password as per typical security best practices.

Create a Host Principal for the KDC (nfsv4)

```
[root@nfsv4]# kadmin
  Authenticating as principal root/admin@nfsv4.nfstest.com with password.
  Password for root/admin@nfsv4.nfstest.com:
  kadmin: addprinc -randkey host/nfsv4.nfstest.com
  NOTICE: no policy specified for host/nfsv4.nfstest.com@nfstest.com;
assigning "default"
  Principal "host/nfsv4.nfstest.com@nfstest.com " created.
  kadmin: ktadd host/nfsv4.nfstest.com
```

Setup Default Policy

You will want to create the default password policy at this point. All new accounts will have this policy enforced.

```
[root@nfsv4] kadmin
  Authenticating as principal root/admin@nfstest.com with password.
  Password for root/admin@ nfstest.com:
  kadmin: add_policy -maxlife 180days -minlife 2days -minlength 8 -
minclasses 3 -history 10 default
```

Add a Normal User

```
[root@ec2-54-204-34-218 config]# kadmin.local -q "addprinc ahmed/users"
  Authenticating as principal root/admin@NFSTEST.COM with password.
  NOTICE: no policy specified for ahmed/users@NFSTEST.COM; assigning
"default"
  Enter password for principal "ahmed/users@NFSTEST.COM":
  Re-enter password for principal "ahmed/users@NFSTEST.COM":
  Principal "ahmed/users@NFSTEST.COM" created.
```

Firewall Configuration

Security best practices recommend using a firewall (e.g., **iptables**) to restrict access. For **Kerberos** to work, the following ports must be opened.

- Clients must be able to reach **all KDCs on UDP port 88** (for authentication).
- Clients must be able to reach the **primary KDC on TCP port 749** (for password management).
- The **primary KDC** must be able to reach the **secondary KDCs on TCP port 754** (for replication).

Open LDAP Server Configuration

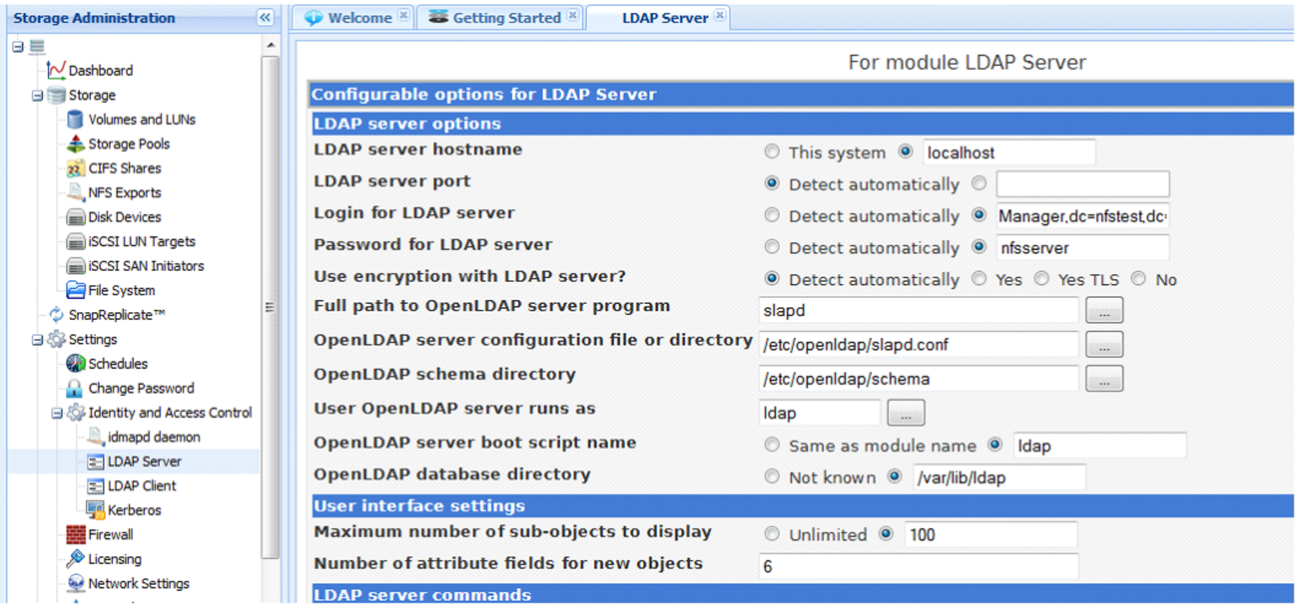
Initialize LDAP server and set up the configuration in the webmin-LDAP-server Module.

Build root DN for LDAP

1. Clear:

```
*rm -rf /var/lib/ldap/*
    *rm -rf /etc/openldap/slapd.d/*
    * cp /usr/share/openldap-servers/DB_CONFIG.example  /var/lib/ldap/
    * chown -R ldap.ldap /var/lib/ldap/
```

2. In **SoftNAS StorageCenter**, **configure Webmin LDAP module** as shown in the screenshot below:



For module LDAP Server

Configurable options for LDAP Server

LDAP server options

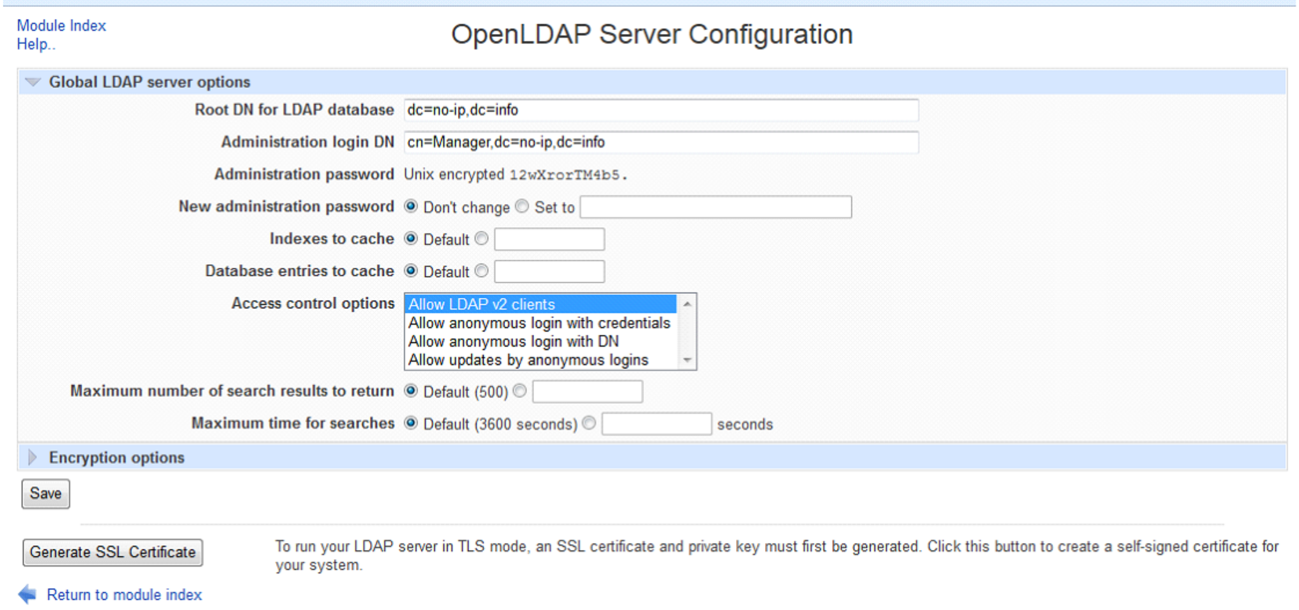
LDAP server hostname	○ This system ● localhost
LDAP server port	● Detect automatically ○
Login for LDAP server	○ Detect automatically ● Manager,dc=nfstest,dc
Password for LDAP server	○ Detect automatically ● nfsserver
Use encryption with LDAP server?	● Detect automatically ○ Yes ○ Yes TLS ○ No
Full path to OpenLDAP server program	slapd ...
OpenLDAP server configuration file or directory	/etc/openldap/slapd.conf ...
OpenLDAP schema directory	/etc/openldap/schema ...
User OpenLDAP server runs as	ldap ...
OpenLDAP server boot script name	○ Same as module name ● ldap
OpenLDAP database directory	○ Not known ● /var/lib/ldap

User interface settings

Maximum number of sub-objects to display	○ Unlimited ● 100
Number of attribute fields for new objects	6

LDAP server commands

3. Click **Save**. The openLDAP server configuration page is displayed.



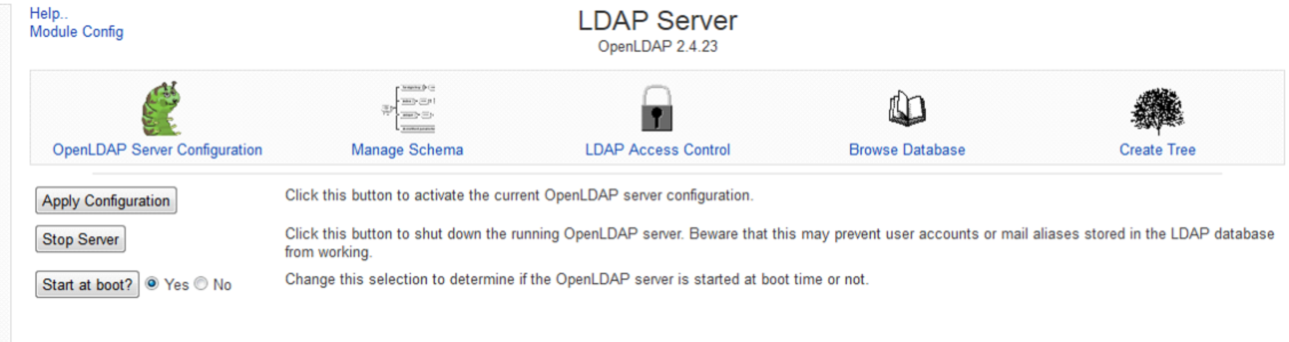
OpenLDAP Server Configuration

Global LDAP server options

Root DN for LDAP database	dc=no-ip,dc=info
Administration login DN	cn=Manager,dc=no-ip,dc=info
Administration password	Unix encrypted 12wXrorTM4b5.
New administration password	● Don't change ○ Set to
Indexes to cache	● Default ○
Database entries to cache	● Default ○
Access control options	Allow LDAP v2 clients Allow anonymous login with credentials Allow anonymous login with DN Allow updates by anonymous logins
Maximum number of search results to return	● Default (500) ○
Maximum time for searches	● Default (3600 seconds) ○ seconds

Encryption options

To run your LDAP server in TLS mode, an SSL certificate and private key must first be generated. Click this button to create a self-signed certificate for your system.



LDAP Server

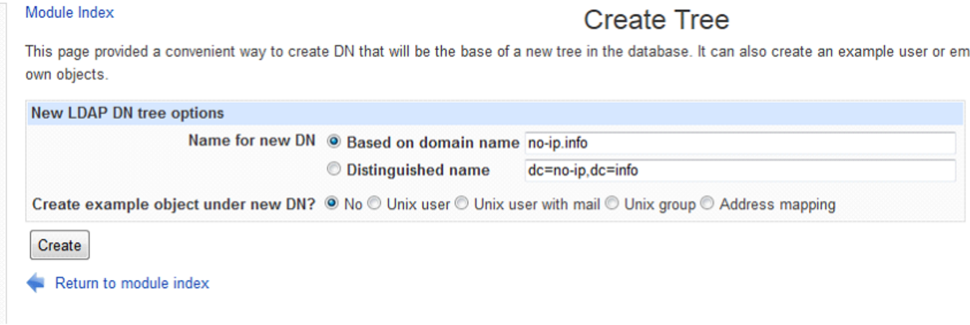
OpenLDAP 2.4.23

Apply Configuration — Click this button to activate the current OpenLDAP server configuration.

Stop Server — Click this button to shut down the running OpenLDAP server. Beware that this may prevent user accounts or mail aliases stored in the LDAP database from working.

Start at boot? ● Yes ○ No — Change this selection to determine if the OpenLDAP server is started at boot time or not.

Create Tree



Create Tree

This page provided a convenient way to create DN that will be the base of a new tree in the database. It can also create an example user or email alias under the tree, as a template for your own objects.

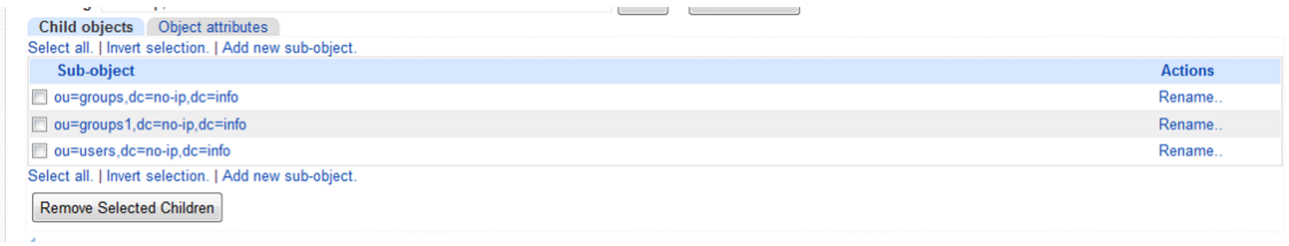
New LDAP DN tree options		
Name for new DN	● Based on domain name	no-ip.info
	○ Distinguished name	dc=no-ip,dc=info
Create example object under new DN?	● No ○ Unix user ○ Unix user with mail ○ Unix group ○ Address mapping	

Check the LDAP server to verify creation of `cn=Manger,dc=no-ip,dc=info.`

Create an Organization Unit

An Organization Unit holds Groups and Users.

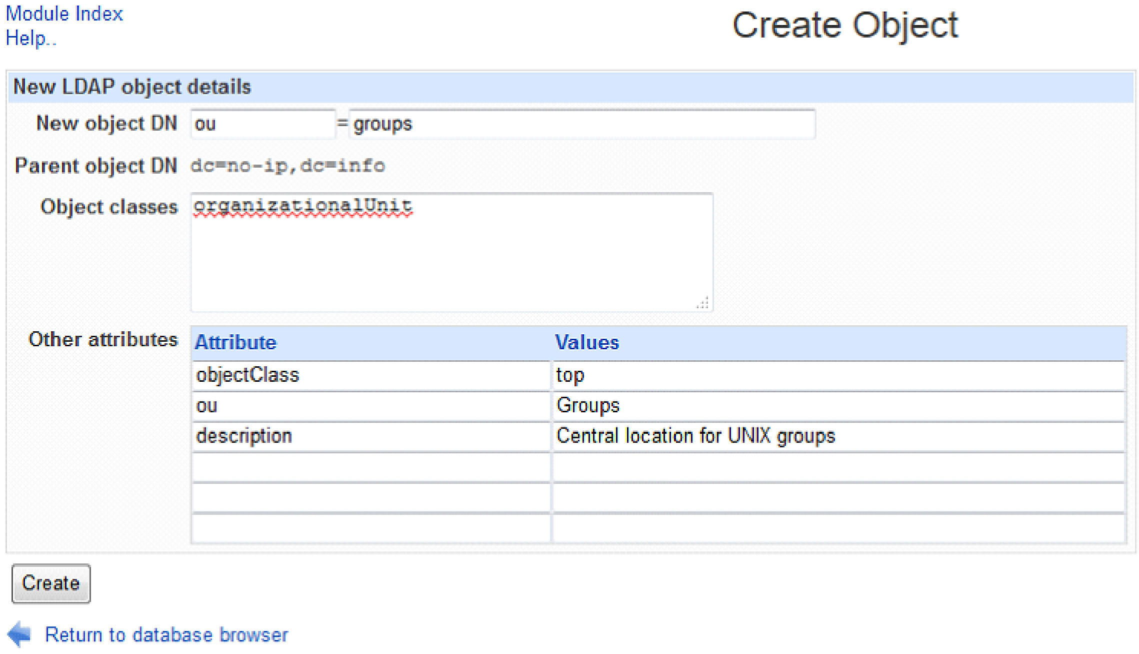
Click **Browse Database**.



	Sub-object	Actions
□	ou=groups,dc=no-ip,dc=info	Rename..
□	ou=groups1,dc=no-ip,dc=info	Rename..
□	ou=users,dc=no-ip,dc=info	Rename..

Create Objects

Click on **Add new sub-object** to create Groups and Users objects for LDAP users and Groups



Create Object

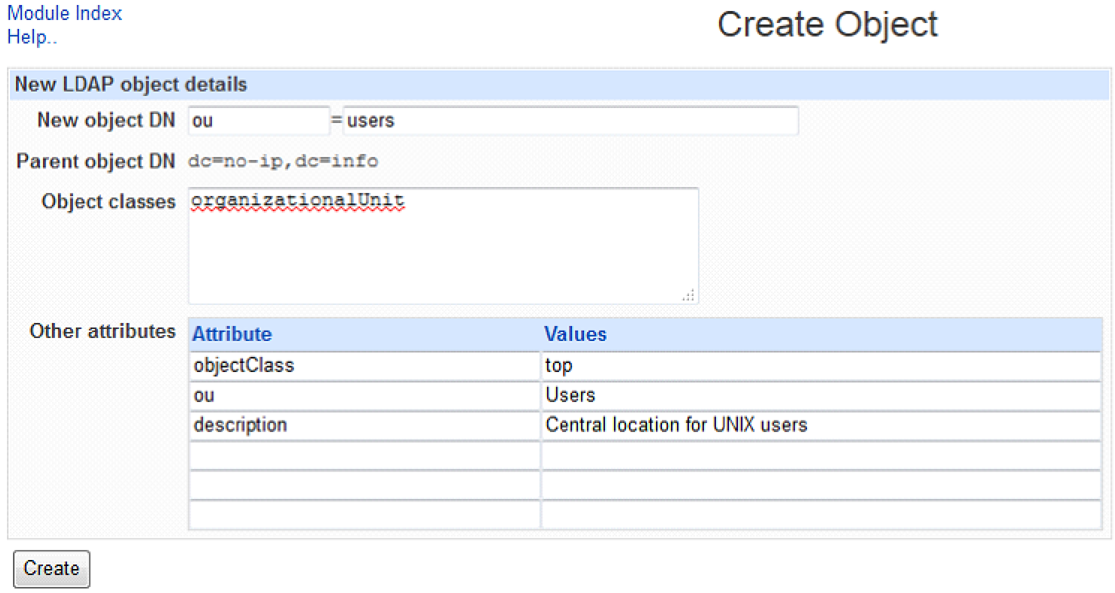
New LDAP object details

New object DN	ou = groups
Parent object DN	dc=no-ip,dc=info
Object classes	organizationalUnit

Other attributes

Attribute	Values
objectClass	top
ou	Groups
description	Central location for UNIX groups

For Users



Create Object

New LDAP object details

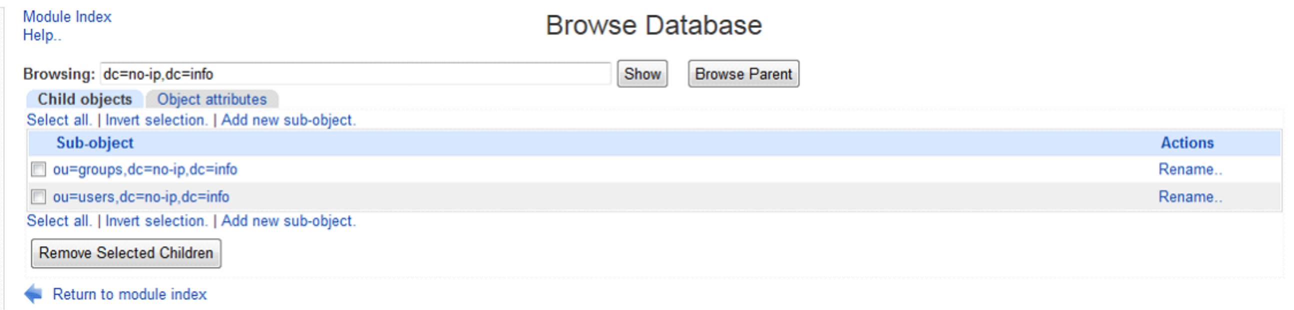
New object DN	ou = users
Parent object DN	dc=no-ip,dc=info
Object classes	organizationalUnit

Other attributes

Attribute	Values
objectClass	top
ou	Users
description	Central location for UNIX users

Review Settings

After the above steps have been successfully completed, the environment should be similar to the screencap below.



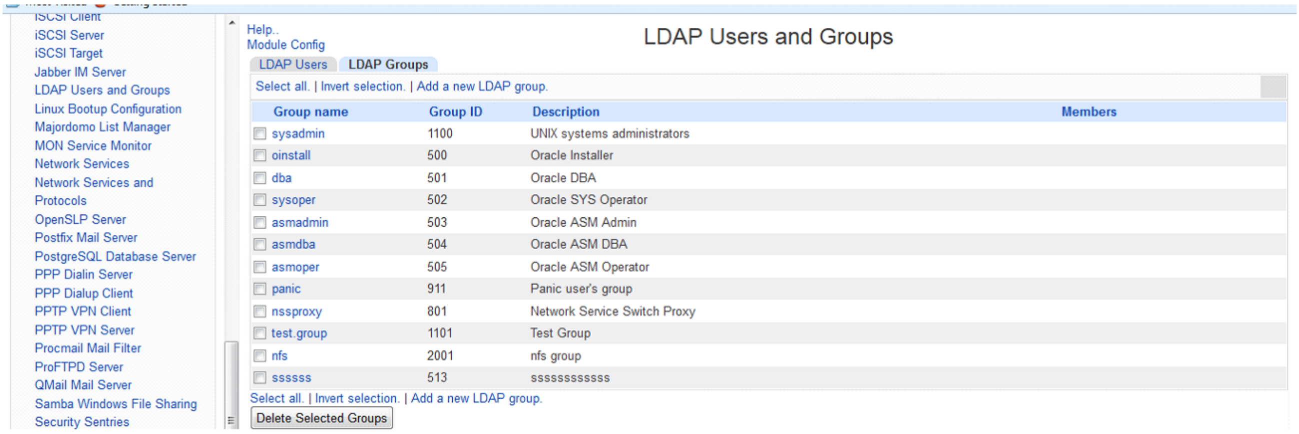
Browse Database

Browsing: dc=no-ip,dc=info

Sub-object	Actions
□ ou=groups,dc=no-ip,dc=info	Rename..
□ ou=users,dc=no-ip,dc=info	Rename..

Create Groups and Users elements

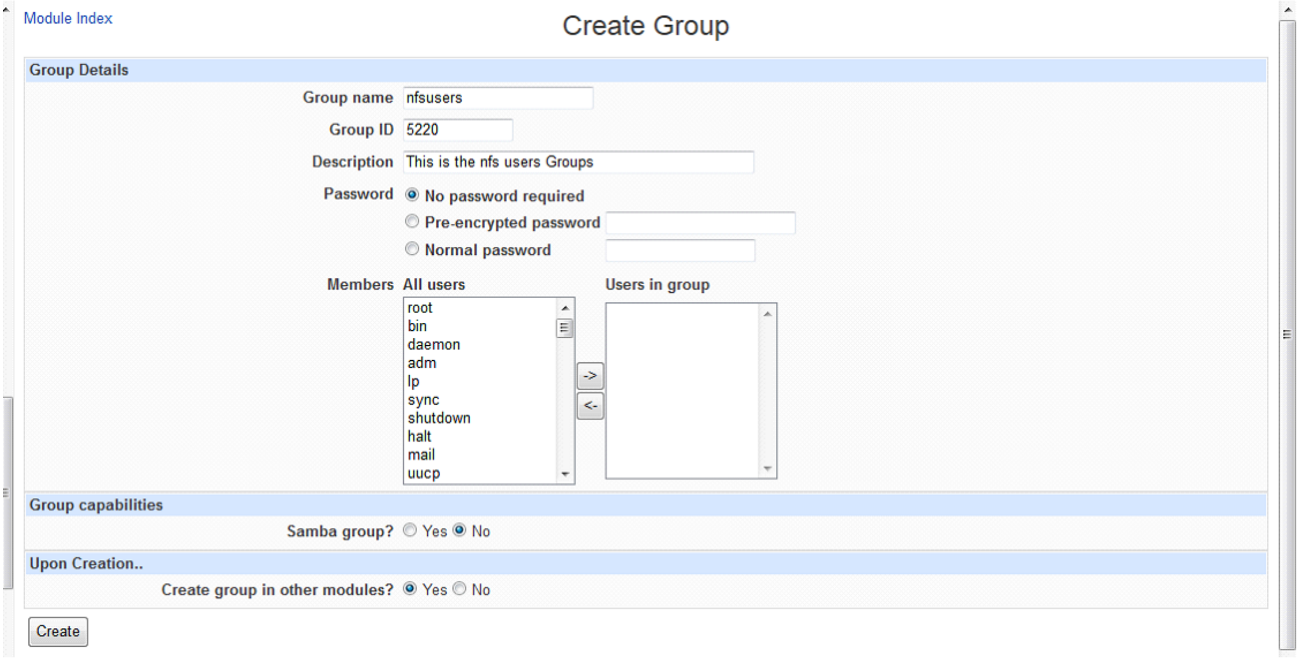
Click on **LDAP Users and Groups** in the left Panel.



LDAP Users and Groups

Group name	Group ID	Description	Members
□ sysadmin	1100	UNIX systems administrators	
□ oinstall	500	Oracle Installer	
□ dba	501	Oracle DBA	
□ sysoper	502	Oracle SYS Operator	
□ asmadmin	503	Oracle ASM Admin	
□ asmdba	504	Oracle ASM DBA	
□ asmoper	505	Oracle ASM Operator	
□ panic	911	Panic user's group	
□ nssproxy	801	Network Service Switch Proxy	
□ test.group	1101	Test Group	
□ nfs	2001	nfs group	
□ ssssss	513	ssssssssssss	

Add New LDAP Group



Create Group

Group Details

Group name: nfsusers

Group ID: 5220

Description: This is the nfs users Groups

Password: ● No password required ○ Pre-encrypted password ○ Normal password

Members: All users: root, bin, daemon, adm, lp, sync, shutdown, halt, mail, uucp — Users in group: (empty)

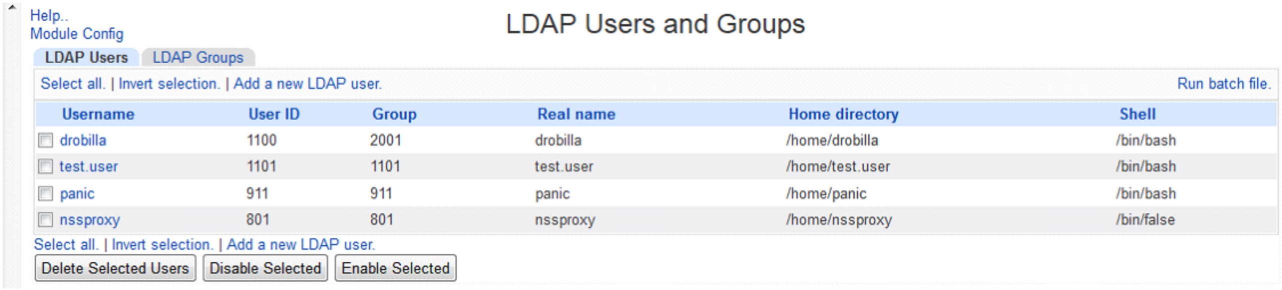
Group capabilities

Samba group? ○ Yes ● No

Upon Creation..

Create group in other modules? ● Yes ○ No

Add New User to NFSusers



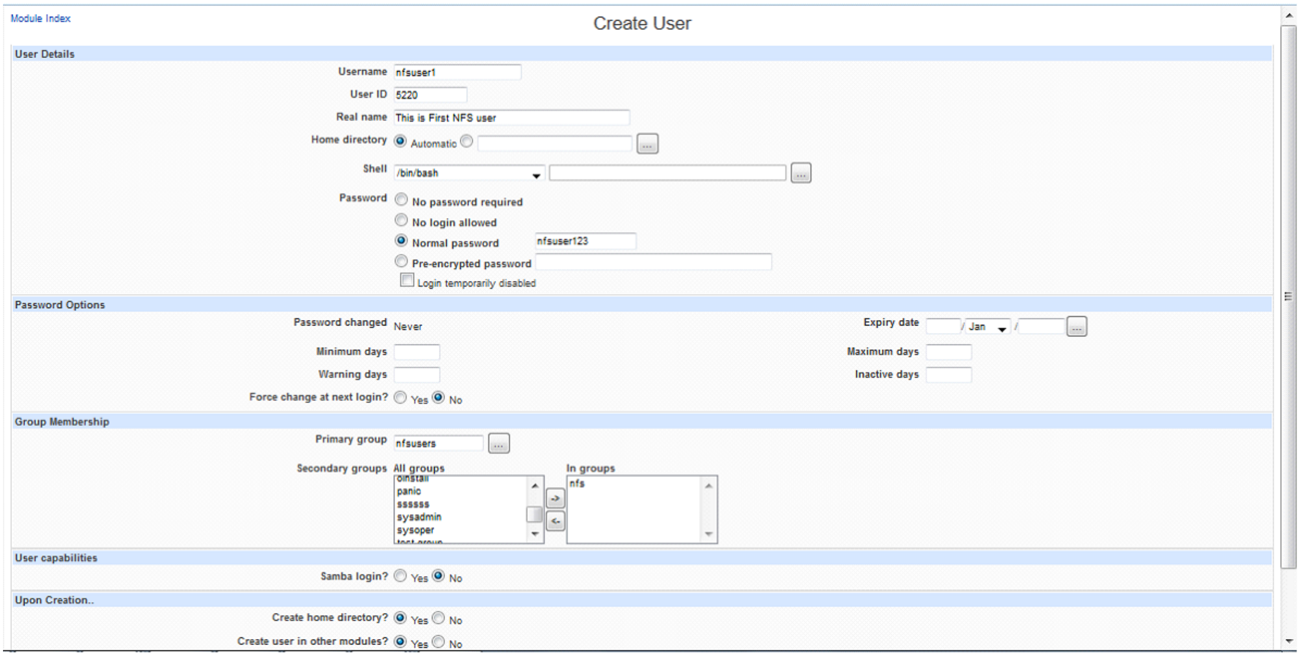
Help..
Module Config

LDAP Users and Groups

LDAP Users
LDAP Groups
Select all. | Invert selection. | Add a new LDAP user.
Run batch file.

	Username	User ID	Group	Real name	Home directory	Shell
□	drobilla	1100	2001	drobilla	/home/drobilla	/bin/bash
□	test.user	1101	1101	test.user	/home/test.user	/bin/bash
□	panic	911	911	panic	/home/panic	/bin/bash
□	nssproxy	801	801	nssproxy	/home/nssproxy	/bin/false

Select all. | Invert selection. | Add a new LDAP user.
Delete Selected Users
Disable Selected
Enable Selected



Create User

User Details

Username: nfsuser1
User ID: 5220
Real name: This is First NFS user
Home directory: ● Automatic ○
Shell: /bin/bash
Password: ○ No password required
○ No login allowed
● Normal password nfsuser123
○ Pre-encrypted password
□ Login temporarily disabled

Password Options

Password changed: Never
Expiry date: / Jan /
Minimum days:
Maximum days:
Warning days:
Inactive days:
Force change at next login? ○ Yes ● No

Group Membership

Primary group: nfsusers
Secondary groups: All groups: oinstall, panic, ssssss, sysadmin, sysoper, test group
In groups: nfs

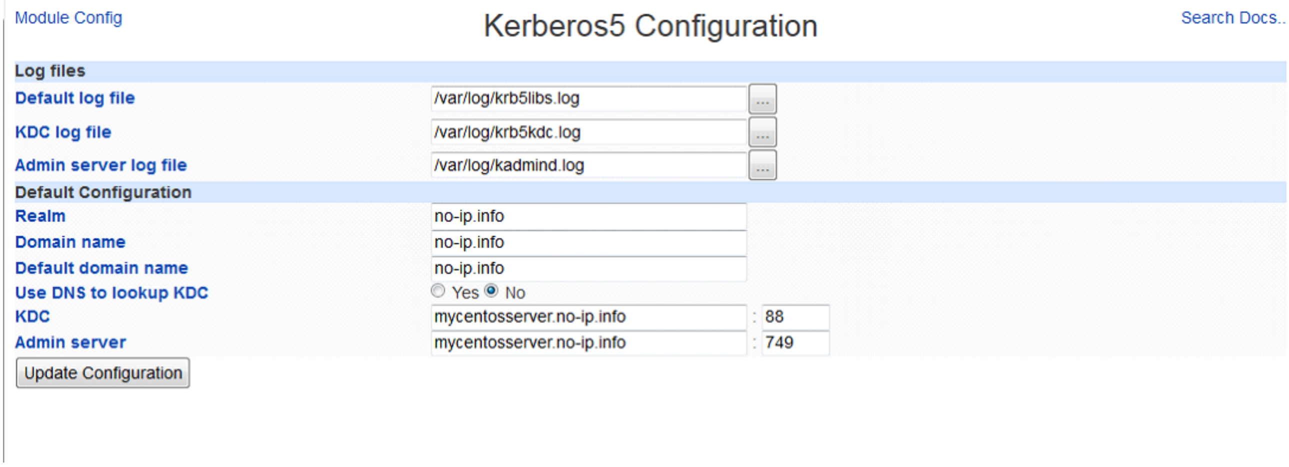
User capabilities

Samba login? ○ Yes ● No

Upon Creation..

Create home directory? ● Yes ○ No
Create user in other modules? ● Yes ○ No

Further Configuration



Kerberos5 Configuration

Log files

Default log file: /var/log/krb5libs.log
KDC log file: /var/log/krb5kdc.log
Admin server log file: /var/log/kadmind.log

Default Configuration

Realm: no-ip.info
Domain name: no-ip.info
Default domain name: no-ip.info
Use DNS to lookup KDC: ○ Yes ● No
KDC: mycentosserver.no-ip.info : 88
Admin server: mycentosserver.no-ip.info : 749

The LDAP server must be configured to use **Kerberos**. If the LDAP server is on the same machine as the **Kerberos KDC**, then everything is automatically set up; otherwise, perform the following configuration:

```
/etc/openlad/slapd.conf

access to attr=loginShell
        by dn.regex="uid=.*/admin,cn=GSSAPI,cn=auth" write
        by self write
        by * read
# Only the user can see their employeeNumber
access to attr=employeeNumber
```

```
        by dn.regex="uid=.*/admin,cn=GSSAPI,cn=auth" write
        by self read
        by * none
# Default read access for everything else
access to *
        by dn.regex="uid=.*/admin,cn=GSSAPI,cn=auth" write
        by * read
```

LDAP.conf

This file needs to be propagated to each host, including the LDAP servers. Only the following lines need to be present:

```
BASE    dc=no-ip,dc=info
URI     ldaps://mycentosserver.no-ip.info
```

This where all clients are going to point and look for an LDAP server.

Client Setup

Copy Files

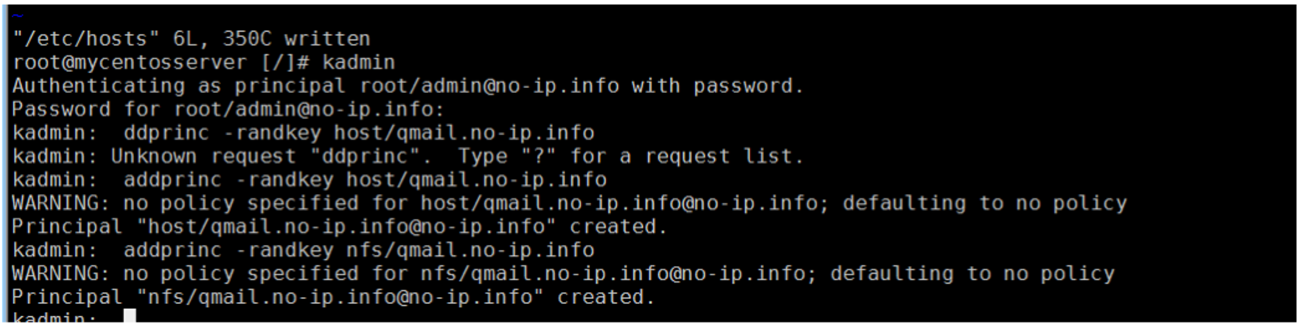
Copy the following files from the KDC or LDAP server.

```
/etc/krb5.conf
/etc/openldap/ldap.conf
/etc/openldap/cacerts/cacert.pem
```

Create Kerberos Principals

Run kadmin on the server and create the following principals. Replace **`qmail.no-ip.info`** with the fully qualified name of the client machine. If NFS is not in the network plan, adding the second principal is not crucial; however, if it is added at this point, it should not cause issues.

```
[root@mycentosserver]# kadmin
  Authenticating as principal root/admin@no-ip.info with password.
  Password for root/admin@no-ip.info:
  kadmin: addprinc -randkey host/qmail.no-ip.info
  kadmin: addprinc -randkey nfs/qmail.no-ip.info
```

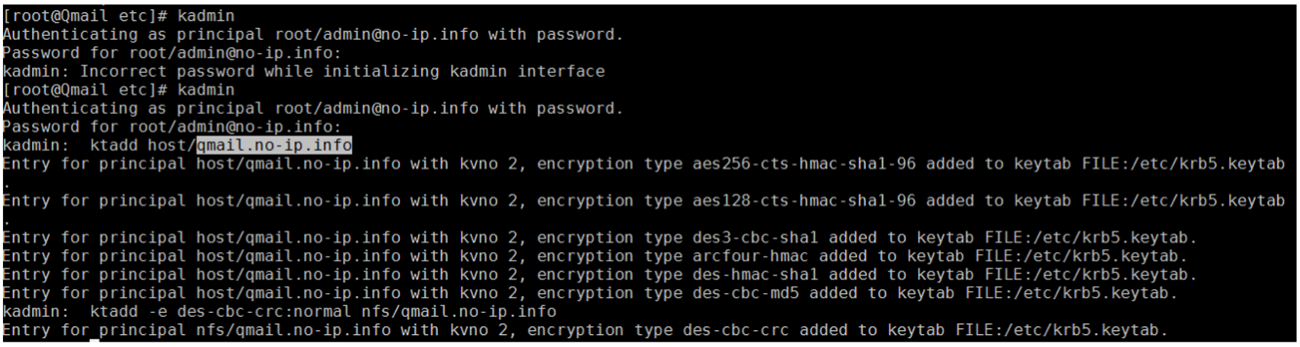


```
~
"/etc/hosts" 6L, 350C written
root@mycentosserver [/]# kadmin
Authenticating as principal root/admin@no-ip.info with password.
Password for root/admin@no-ip.info:
kadmin:  ddprinc -randkey host/qmail.no-ip.info
kadmin: Unknown request "ddprinc".  Type "?" for a request list.
kadmin:  addprinc -randkey host/qmail.no-ip.info
WARNING: no policy specified for host/qmail.no-ip.info@no-ip.info; defaulting to no policy
Principal "host/qmail.no-ip.info@no-ip.info" created.
kadmin:  addprinc -randkey nfs/qmail.no-ip.info
WARNING: no policy specified for nfs/qmail.no-ip.info@no-ip.info; defaulting to no policy
Principal "nfs/qmail.no-ip.info@no-ip.info" created.
kadmin:
```

Add Principal(s) to Keytab File

Note: Ensure accuracy when adding the principal(s) in the steps shown above. This specific method is critical for a successful installation.

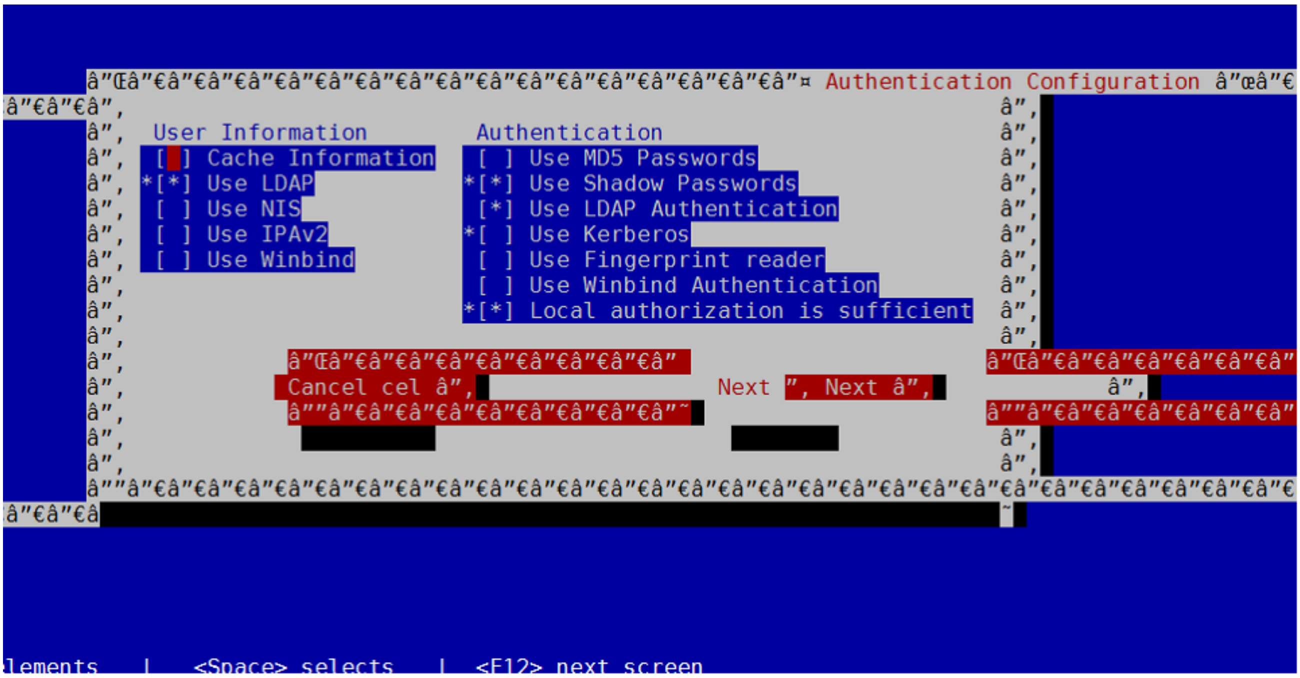
```
[root@qmail ~]# kadmin
  Authenticating as principal root/admin@no-ip.info with password.
  Password for root/admin@no-ip.info:
  kadmin: ktadd host/qmial.no-ip.info
  kadmin: ktadd -e des-cbc-crc:normal nfs/qmail.no-ip.info
```



```
[root@Qmail etc]# kadmin
Authenticating as principal root/admin@no-ip.info with password.
Password for root/admin@no-ip.info:
kadmin: Incorrect password while initializing kadmin interface
[root@Qmail etc]# kadmin
Authenticating as principal root/admin@no-ip.info with password.
Password for root/admin@no-ip.info:
kadmin:  ktadd host/qmail.no-ip.info
Entry for principal host/qmail.no-ip.info with kvno 2, encryption type aes256-cts-hmac-sha1-96 added to keytab FILE:/etc/krb5.keytab
.
Entry for principal host/qmail.no-ip.info with kvno 2, encryption type aes128-cts-hmac-sha1-96 added to keytab FILE:/etc/krb5.keytab
.
Entry for principal host/qmail.no-ip.info with kvno 2, encryption type des3-cbc-sha1 added to keytab FILE:/etc/krb5.keytab.
Entry for principal host/qmail.no-ip.info with kvno 2, encryption type arcfour-hmac added to keytab FILE:/etc/krb5.keytab.
Entry for principal host/qmail.no-ip.info with kvno 2, encryption type des-hmac-sha1 added to keytab FILE:/etc/krb5.keytab.
Entry for principal host/qmail.no-ip.info with kvno 2, encryption type des-cbc-md5 added to keytab FILE:/etc/krb5.keytab.
kadmin:  ktadd -e des-cbc-crc:normal nfs/qmail.no-ip.info
Entry for principal nfs/qmail.no-ip.info with kvno 2, encryption type des-cbc-crc added to keytab FILE:/etc/krb5.keytab.
```

Enable Authentication

Run the configuration tool by typing **authconfig** at the shell prompt. Check **Use LDAP** under **User Information** and **Use Kerberos** under **Authentication**.



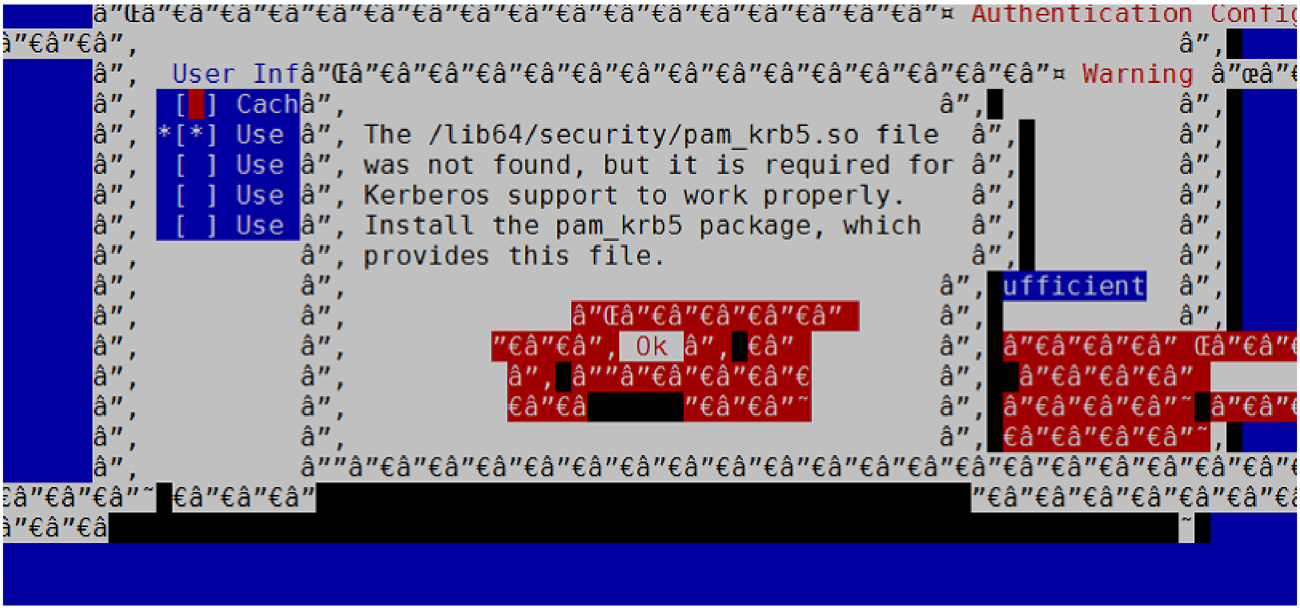
```
Authentication Configuration

 User Information              Authentication
 [ ] Cache Information         [ ] Use MD5 Passwords
*[*] Use LDAP                 *[*] Use Shadow Passwords
 [ ] Use NIS                   [*] Use LDAP Authentication
 [ ] Use IPAv2                *[ ] Use Kerberos
 [ ] Use Winbind               [ ] Use Fingerprint reader
                               [ ] Use Winbind Authentication
                              *[*] Local authorization is sufficient

        Cancel                      Next

lements   |   <Space> selects   |   <F12> next screen
```

This error message may pop up.



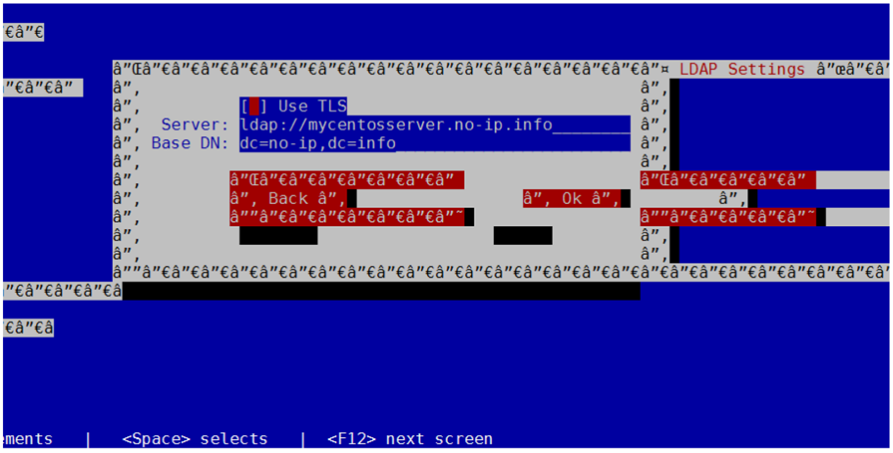
```
Authentication Config

 User Inf        Warning

 [ ] Cach
*[*] Use   The /lib64/security/pam_krb5.so file
 [ ] Use   was not found, but it is required for
 [ ] Use   Kerberos support to work properly.
 [ ] Use   Install the pam_krb5 package, which
           provides this file.
                                               ufficient

                  Ok
```

```
yum install  pam_krb5
```



```
€â”€
           â”Œâ”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”¤ LDAP Settings â”œâ”€â”€â
"€â"€â"    â",                                                   â",
           â",            [ ] Use TLS                            â",
           â",   Server: ldap://mycentosserver.no-ip.info_______ â",
           â",  Base DN: dc=no-ip,dc=info                        â",
           â",                                                   â",
           â",           â”Œâ”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€        â”Œâ”€â”€â”€â”€â”€â”€â”€â”€â”€
           â",           â", Back â",                 â", Ok â",          â",
           â",           â””â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”˜        â””â”€â”€â”€â”€â”€â”€â”€â”€â”€â”˜
           â",                                                   â",
           â",                                                   â",
           â””â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â
"€â"€â"€â
€â"€â

ments    |    <Space> selects    |   <F12> next screen
```

To view the contents, copy **`/etc/openldap/ldap`**.

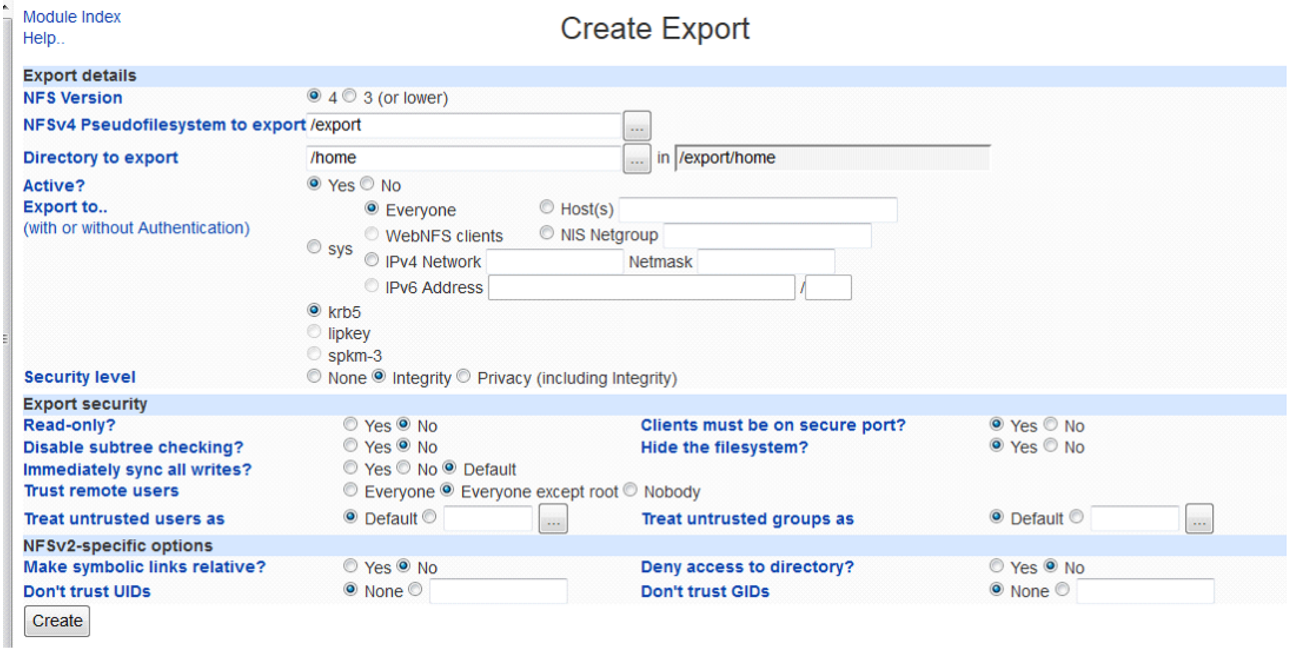
At this point the LDAP & **Kerberos** are configured to get information from LDAP and auth from **Kerberos.**

NFSv4 Configuration

Creating Exports

Share **/home** using **/export/home** to share all **LDAP_USER_HOMEDIR.**

Configure the exports as needed against the screencaps below:

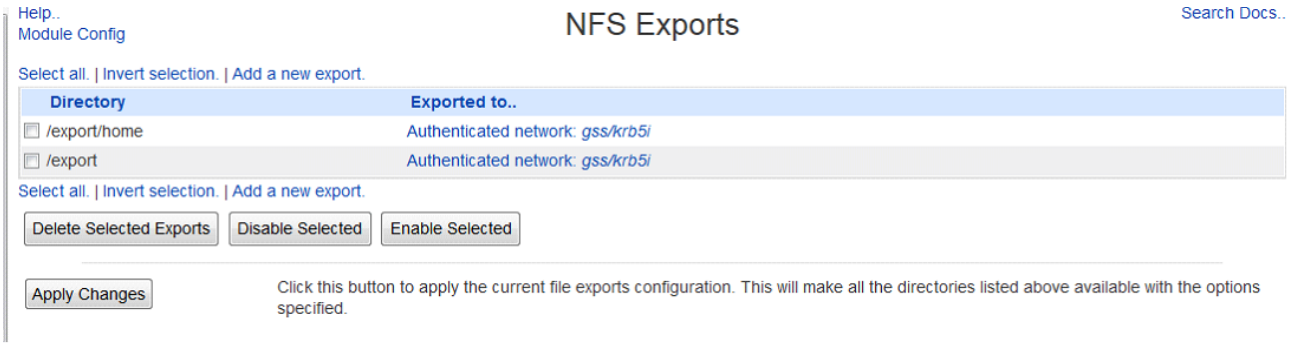


Module Index
Help..

Create Export

Export details			
NFS Version	● 4 ○ 3 (or lower)		
NFSv4 Pseudofilesystem to export	/export ...		
Directory to export	/home ... in /export/home		
Active?	● Yes ○ No		
Export to.. (with or without Authentication)	○ sys ● krb5 ○ lipkey ○ spkm-3	● Everyone ○ WebNFS clients ○ IPv4 Network Netmask ○ IPv6 Address /	○ Host(s) ○ NIS Netgroup
Security level	○ None ● Integrity ○ Privacy (including Integrity)		
Export security			
Read-only?	○ Yes ● No	Clients must be on secure port?	● Yes ○ No
Disable subtree checking?	○ Yes ● No	Hide the filesystem?	● Yes ○ No
Immediately sync all writes?	○ Yes ○ No ● Default		
Trust remote users	○ Everyone ● Everyone except root ○ Nobody		
Treat untrusted users as	● Default ○ ...	Treat untrusted groups as	● Default ○ ...
NFSv2-specific options			
Make symbolic links relative?	○ Yes ● No	Deny access to directory?	○ Yes ● No
Don't trust UIDs	● None ○	Don't trust GIDs	● None ○

NFS Exports



Help..
Module Config
Search Docs..

NFS Exports

Select all. | Invert selection. | Add a new export.

Directory	Exported to..
□ /export/home	Authenticated network: *gss/krb5i*
□ /export	Authenticated network: *gss/krb5i*

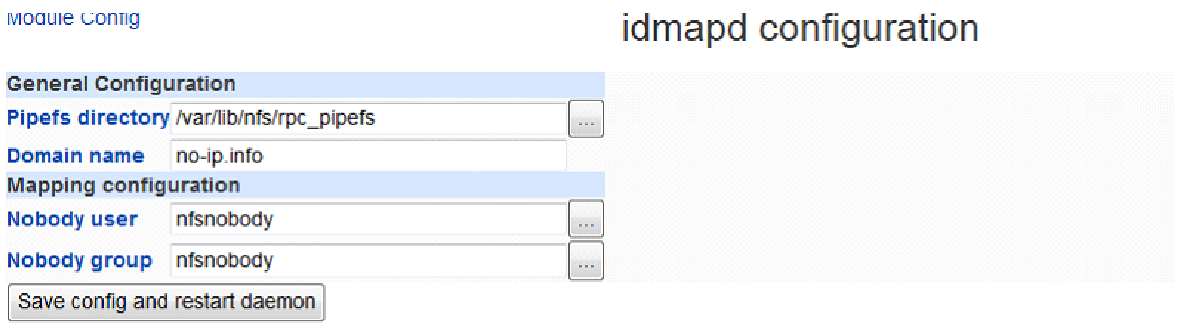
Select all. | Invert selection. | Add a new export.
Delete Selected Exports
Disable Selected
Enable Selected
Apply Changes

Click this button to apply the current file exports configuration. This will make all the directories listed above available with the options specified.

Modify /etc/idmapd.conf

Change the domain listed to the current domain.

Update the user mapping for **nobody**.



General Configuration

Pipefs directory	/var/lib/nfs/rpc_pipefs
Domain name	no-ip.info

Mapping configuration

Nobody user	nfsnobody
Nobody group	nfsnobody

Modify /etc/sysconfig/nfs

Enable Secure NFS

Add the following line to `/etc/sysconfig/nfs:`

```
SECURE_NFS=yes
```

If the network includes **NFSv3** and a **firewall**, add the following definitions as well. Choose ports that are appropriate to the environment, although the values listed below have been successful in our environments.

```
STATD_PORT=4000
LOCKD_TCPPORT=4001
LOCKD_UDPPORT=4001
MOUNTD_PORT=4002
RQUOTAD_PORT=4003
```