How To Configure LDAP Server

Version 1.1
February 2016

QSAN Technology, Inc.

4F., No.103, Ruihu St.,
Neihu Dist., Taipei City 114,
Taiwan (R.O.C.)

Tel: +886-2-7720-2118
Fax: +886-2-7720-0295

Email: sales@qsan.com
Website: www.qsan.com

Introduction

Qsan Unified Storage (TrioNAS and TrioNAS LX series) supports LDAP service, you may use this feature to combine the accounts from your LDAP server, and then you don't have to re-create the accounts one by one on the Unified Storage.

The way to configure the LDAP service on TrioNAS is quite simple. Within a few settings, the accounts on your LDAP server can be loaded into TrioNAS. In this document, we will show you how to create a LDAP server on RHEL 6.1 and use it for authentication on TrioNAS.

Environment

Host OS:	Red Hat Enterprise Linux 6.1
LDAP:	OpenLDAP 2.4.23-15.el6.x86_64 or later
Samba:	Samba 3.5.6-86.el6.x86_64
Storage:	TrioNAS LX Series
Controller firmware:	V1.0.3
QCentral:	V2.1.2 (build 201211131700)
LDAP server IP:	192.168.136.203
TrioNAS IP:	192.168.9.111

Configuration

RPM Pagkages

Before configuring the LDAP server, you have to install the following rpm packages and source files (.tar.gz), so that the LDAP service could run smoothly and without any compatible issues. Here is the order to install the packages we need:

- nscd-2.12-1.25.el6.x86_64.rpm
- db4-devel-4.7.25-16.el6.x86_64.rpm
- db4-4.7.25-16.el6.x86_64.rpm
- db4-utils-4.7.25-16.el6.x86_64.rpm
- openldap-servers-2.4.23-15.el6.x86_64.rpm
- openldap-clients-2.4.23-15.el6.x86_64.rpm
- openldap-2.4.23-15.el6.x86_64.rpm
- openldap-devel-2.4.23-15.el6.x86_64.rpm
- nss_ldap-251.tar.gz or nss_ldap.rpm
- samba-client-3.5.6-86.el6.x86_64.rpm

- samba-winbind-clients-3.5.6-86.el6.x86_64.rpm
- samba-common-3.5.6-86.el6.x86_64.rpm
- samba-3.5.6-86.el6.x86_64.rpm
- perl-Digest-SHA1-2.12-2.el6.x86_64.rpm
- perl-LDAP-0.34-1.el6.rfx.noarch.rpm (perl(Convert::ASN1) is needed)
- XML-SAX.tar.gz
- perl-Crypt-SmbHash.rpm
- IO-Socket-SSL.tar.gz
- XML-NamespaceSupport.tar.gz
- Authen-SASL.tar.gz
- perl-Unicode-Map.rpm
- perl-Unicode-String.rpm
- perl-Unicode-Map8.rpm
- perl-Jcode.rpm
- perl-Unicode-MapUTF8.rpm
- Jcode.tar.gz
- Unicode-String.tar.gz
- Unicode-Map.tar.gz
- Unicode-Map8.tar.gz
- Unicode-MapUTF8.tar.gz
- smbldap-tools-0.9.6-3.el6.noarch.rpm

TIP: If the above RPMs could not be found, or the rpm files could not compatible with the existed RPMs (just like el5 conflicts with el6), you will need to compile it from a source file, such as “Jcode.tar.gz”.

Server Settings

To avoid any connection problems, please check your firewall and selinux settins for making sure the LDAP services could successfully be operated under your environments. If you are not sure how to configure the firewall, please try to close them in your test environment and continue doing the next step.

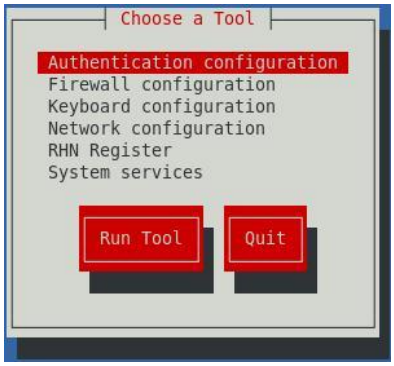
1. Closing the firewall and selinux:

```
[root@qsan ~]# vi /etc/selinux/config >> SELINUX=disable
(Rebooting the system to take affect.)
[root@qsan ~]# iptables -F
```

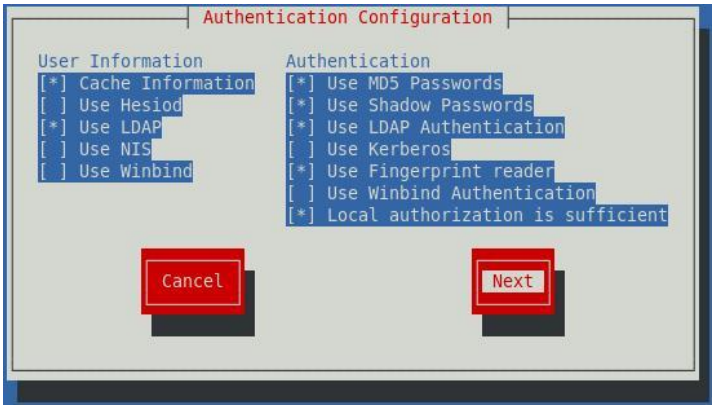
```
[root@qsan ~]# iptables -X
[root@qsan ~]# iptables -Z
[root@qsan ~]# service iptables stop
[root@qsan ~]# service ip6tables stop
```

2. Authentication settings:

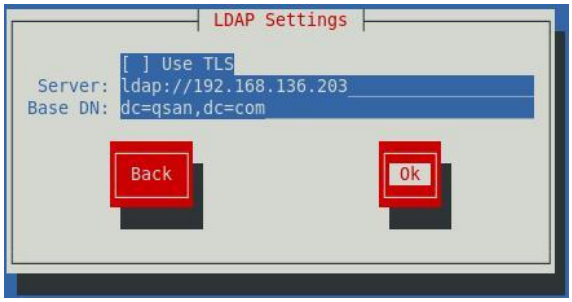
```
[root@qsan ~]# setup
```



3. Choosing the below options:



4. Do not use TLS, and setting the basic LDAP configurations.



Initial Settings of OpenLDAP

5. Copying the files we will need to use later:

```
[root@qsan ~]# cp /usr/share/doc/samba-3.5.6/LDAP/samba.schema /etc/openldap/schema/
[root@qsan ~]# cp /usr/share/openldap-servers/DB_CONFIG.example
/var/lib/ldap/DB_CONFIG
[root@qsan ~]# cp /usr/share/openldap-servers/slapd.conf.obsolete /etc/openldap/slapd.conf
```

6. Setting the password for the LDAP, and configuring the LDAP server:

```
[root@qsan ~]# slappasswd
New password:
Re-enter new password:
{SSHA}M8AfDy1C3j3X+/GlxyeEjVAcToFKD59w
[root@qsan ~]# vi /etc/openldap/slapd.conf
include         /etc/openldap/schema/samba.schema
access to attrs=userPassword,sambaLMPassword,sambaNTPassword
      by self write
      by anonymous auth
      by * none

access to *
      by * read
database        bdb
suffix          "dc=qsan,dc=com"
checkpoint      1024 15
rootdn          "cn=admin,dc=qsan,dc=com"
rootpw          123456
index   objectClass,uidNumber,gidNumber       eq
index   cn,sn,uid,displayName               pres,sub,eq
index   memberUid,mail,givenname            eq,subinitial
index   sambaSID,sambaPrimaryGroupSID,sambaDomainName   eq
#access to *
#       by dn.exact="cn=Manager,dc=my-domain,dc=com" read
#       by * none
```

(Disabling the above settings by adding "#" at the beginning.)

```
[root@qsan ~]# vi /etc/openldap/ldap.conf
URI ldap://192.168.136.203
BASE dc=qsan,dc=com
#TLS_CACERTDIR /etc/openldap/cacerts

[root@qsan ~]# vi /etc/ldap.conf
host 192.168.136.203
base dc=qsan,dc=com
binddn cn=admin,dc=qsan,dc=com
bindpw 123456
rootbinddn cn=admin,dc=qsan,dc=com

[root@qsan ~]# echo 123456 > /etc/ldap.secret
[root@qsan ~]# chmod 600 /etc/ldap.secret
```

7. Creating a root and turning on the LDAP service:

```
[root@qsan ~]# mkdir /etc/openldap/data
[root@qsan ~]# cd /etc/openldap/data
[root@qsan data]# vi root.ldif
#root
dn: dc=qsan,dc=com
dc: qsan
objectClass: dcObject
objectClass: organizationalUnit
ou: qsan.com

[root@qsan data]# rm -rf /etc/openldap/slapd.d/*
[root@qsan data]# slapadd -v -l ./root.ldif
[root@qsan data]# mkdir /atemp
(Deleting the old settings, importing the root.ldif and creating a temp directory for storing some scripts.)

[root@qsan data]# vi /atemp/lrestart.sh
(Making a script for restarting the LDAP service.)
slaptest -f /etc/openldap/slapd.conf -F /etc/openldap/slapd.d
sync
```

```
chown -R ldap:ldap /var/lib/ldap
chown -R ldap:ldap /etc/openldap/slapd.d
[root@qsan data]# sh /atemp/lrestart.sh
(There will be a slapd.conf file created under the /etc/openldap/. If there are any modifications in slapd.conf in the future, please executing the below commands for taking affects:
service slapd stop
rm -rf /etc/openldap/slapd.d/*
sh /atemp/lrestart.sh
service slapd start)
[root@qsan data]# service slapd start
[root@qsan data]# ldapsearch -x
(Checking if the root.ldif has successfully imported or not.)
# extended LDIF
#
# LDAPv3
# base <dc=qsan,dc=com> (default) with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# qsan.com
dn: dc=qsan,dc=com
dc: qsan
objectClass: dcObject
objectClass: organizationalUnit
ou: qsan.com

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

Samba

8. Samba's configuration file:

```
[root@qsan data]# vi /etc/samba/smb.conf
[global]
workgroup = WORKGROUP
(This workgroup must be corresponding to the workgroup on the LDAP service on the TrioNAS, the default is WORKGROUP.)
server string = qsan samba
netbios name = qsan
domain master = yes
local master = yes
domain logons = yes
client lanman auth = yes
client ntlmv2 auth = yes
lanman auth = yes
ntlm auth = yes
security = user
os level = 40
ldap ssl = off
ldap passwd sync = yes
passdb backend = ldapsam:ldap://192.168.136.203
ldap admin dn = cn=admin,dc=qsan,dc=com
ldap suffix = dc=qsan,dc=com
ldap group suffix = ou=Groups
ldap user suffix = ou=Users
ldap machine suffix = ou=Machines
add user script = /usr/sbin/smbldap-useradd -m "%u"
ldap delete dn = yes
idmap backend = ldap:ldap:/192.168.136.203
idmap uid = 1000000-5000000
idmap gid = 1000000-5000000
delete user script = /usr/sbin/smbldap-userdel "%u"
add machine script = /usr/sbin/smbldap-useradd -w "%u"
add group script = /usr/sbin/smbldap-groupadd -p "%g"
#delete group script = /usr/sbin/smbldap-groupdel "%g"
add user to group script = /usr/sbin/smbldap-groupmod -m "%u" "%g"
delete user from group script = /usr/sbin/smbldap-groupmod -x "%u" "%g"
set primary group script = /usr/sbin/smbldap-usermod -g "%g" "%u"
```

```
logon path = \\%L\profiles\%U
logon drive = P:
logon home = \\%L\%U
socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
case sensitive = No
default case = lower
preserve case = yes
short preserve case = Yes
#character set = iso8859-1
#domain admin group = @admin
dns proxy = No
wins support = Yes
winbind use default domain = Yes
nt acl support = Yes
msdfs root = Yes
hide files = /desktop.ini/ntuser.ini/NTUSER.*/
unix charset = iso-8859-15
display charset = iso-8859-15
dos charset = 850
[netlogon]
path = /home/netlogon
writable = No
browseable = No
write list = Administrator
[profiles]
path = /home/profiles
browseable = No
writeable = Yes
profile acls = yes
create mask = 0700
directory mask = 0700
[homes]
comment = Personal
browseable = No
writeable = Yes
```

(The above settings are based on our environments, please modifying them per your own LDAP server environment.)

9. Turning on the Samba service:

```
[root@qsan data]# vi /atemp/srestart.sh
service smb restart && service nmb restart
[root@qsan data]# smbpasswd -w 123456
Setting stored password for "cn=admin,dc=qsan,dc=com" in secrets.tdb
[root@qsan data]# sh /atemp/srestart.sh
[root@qsan data]# mkdir /home/netlogon
[root@qsan data]# mkdir /home/profiles
[root@qsan data]# chmod 777 /home/profiles/
```

Samba-tools

10. Configuring:

```
[root@qsan data]# perl /usr/share/doc/smbldap-tools-0.9.6/configure.pl
-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
 smbldap-tools script configuration
 -=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
Before starting, check
 . if your samba controller is up and running.
 . if the domain SID is defined (you can get it with the 'net getlocalsid')

 . you can leave the configuration using the Ctrl-c key combination
 . empty value can be set with the "." character
-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
Looking for configuration files...

Samba Configuration File Path [/etc/samba/smb.conf] > Enter
The default directory in which the smbldap configuration files are stored is shown.
If you need to change this, enter the full directory path, then press enter to continue.
Smbldap-tools Configuration Directory Path [/etc/smbldap-tools] > Enter
-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
Let's start configuring the smbldap-tools scripts ...

. workgroup name: name of the domain Samba acts as a PDC for
  workgroup name [WORKGROUP] > Enter
```

```
. netbios name: netbios name of the samba controller
  netbios name [qsan] > Enter
. logon drive: local path to which the home directory will be connected (for NT Workstations).
Ex: 'H:'
  logon drive [P:] > Enter
. logon home: home directory location (for Win95/98 or NT Workstation).
  (use %U as username) Ex:'\\qsan\%U'
  logon home (press the "." character if you don't want homeDirectory) [\\%L\%U] > Enter
. logon path: directory where roaming profiles are stored. Ex:'\\qsan\profiles\%U'
  logon path (press the "." character if you don't want roaming profiles) [\\%L\profiles\%U] > .
(Entering a “.” for this option)
. home directory prefix (use %U as username) [/home/%U] > Enter
. default users' homeDirectory mode [700] > Enter
. default user netlogon script (use %U as username) [] > Enter
  default password validation time (time in days) [45] > Enter
. ldap suffix [dc=qsan,dc=com] > Enter
. ldap group suffix [ou=Groups] > Enter
. ldap user suffix [ou=Users] > Enter
. ldap machine suffix [ou=Machines] > Enter
. Idmap suffix [ou=Idmap] > Enter
. sambaUnixIdPooldn: object where you want to store the next uidNumber
  and gidNumber available for new users and groups
  sambaUnixIdPooldn object (relative to ${suffix}) [sambaDomainName=WORKGROUP] > Enter
. ldap master server: IP address or DNS name of the master (writable) ldap server
  ldap master server [192.168.136.203] > Enter
. ldap master port [389] > Enter
. ldap master bind dn [cn=admin,dc=qsan,dc=com] > Enter
. ldap master bind password [] > 123456
. ldap slave server: IP address or DNS name of the slave ldap server: can also be the master one
  ldap slave server [192.168.136.203] > Enter
. ldap slave port [389] > Enter
. ldap slave bind dn [cn=admin,dc=qsan,dc=com] > Enter
. ldap slave bind password [] > 123456
. ldap tls support (1/0) [0] > Enter
. SID for domain WORKGROUP: SID of the domain (can be obtained with 'net getlocalsid qsan')
  SID for domain WORKGROUP [S-1-5-21-1181471589-3805607923-3098382096] > Enter
(If the SID number is empty or wrong, please enter the SID number manually)
```

```
. unix password encryption: encryption used for unix passwords
  unix password encryption (CRYPT, MD5, SMD5, SSHA, SHA) [SSHA] > Enter
. default user gidNumber [513] > Enter
. default computer gidNumber [515] > Enter
. default login shell [/bin/bash] > Enter
. default skeleton directory [/etc/skel] > Enter
. default domain name to append to mail address [] > qsan.com
-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
backup old configuration files:
  /etc/smbldap-tools/smbldap.conf->/etc/smbldap-tools/smbldap.conf.old
  /etc/smbldap-tools/smbldap_bind.conf->/etc/smbldap-tools/smbldap_bind.conf.old
writing new configuration file:
  /etc/smbldap-tools/smbldap.conf done.
  /etc/smbldap-tools/smbldap_bind.conf done.

[root@qsan data]# smbldap-populate
(Here might be an error message displayed if there were any lacks of .rpm file did not be installed properly, and the population will be stopped.)
Populating LDAP directory for domain WORKGROUP (S-1-5-21-1181471589-3805607923-3098382096)
(using builtin directory structure)

entry dc=qsan,dc=com already exist.
adding new entry: ou=Users,dc=qsan,dc=com
adding new entry: ou=Groups,dc=qsan,dc=com
adding new entry: ou=Machines,dc=qsan,dc=com
adding new entry: ou=Idmap,dc=qsan,dc=com
adding new entry: uid=root,ou=Users,dc=qsan,dc=com
adding new entry: uid=nobody,ou=Users,dc=qsan,dc=com
adding new entry: cn=Domain Admins,ou=Groups,dc=qsan,dc=com
adding new entry: cn=Domain Users,ou=Groups,dc=qsan,dc=com
adding new entry: cn=Domain Guests,ou=Groups,dc=qsan,dc=com
adding new entry: cn=Domain Computers,ou=Groups,dc=qsan,dc=com
adding new entry: cn=Administrators,ou=Groups,dc=qsan,dc=com
adding new entry: cn=Account Operators,ou=Groups,dc=qsan,dc=com
adding new entry: cn=Print Operators,ou=Groups,dc=qsan,dc=com
adding new entry: cn=Backup Operators,ou=Groups,dc=qsan,dc=com
```

```
adding new entry: cn=Replicators,ou=Groups,dc=qsan,dc=com
entry sambaDomainName=WORKGROUP,dc=qsan,dc=com already exist. Updating it...

Please provide a password for the domain root:
Changing UNIX and samba passwords for root
New password:
Retype new password:
```

Adding Users

11. A few basic commands to add or delete users or groups:

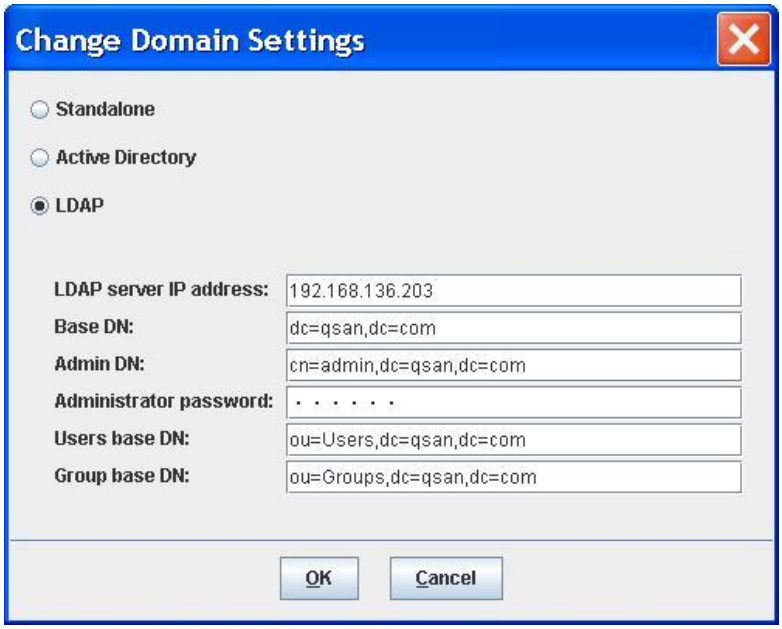
```
# smbldap-useradd -a -m user1          (Adding an user, user1)
# smbldap-groupadd -a -p group1        (Adding a group, group1)
# smbldap-useradd -w winxp$            (Adding a domain computer account, winxp)
# smbldap-groupmod -m user1 group1     (Including user1 into group1)
# smbldap-userdel user1                (Deleting account, user1)
# smbldap-groupdel group1              (Deleting group, group1)
# smbldap-userdel  winxp$              (Deleting domain computer account, winxp)
# smbldap-groupmod -x user1 group1     (Excluding user1 out of group1)
```

12. Creating an user, test1, for testing later:

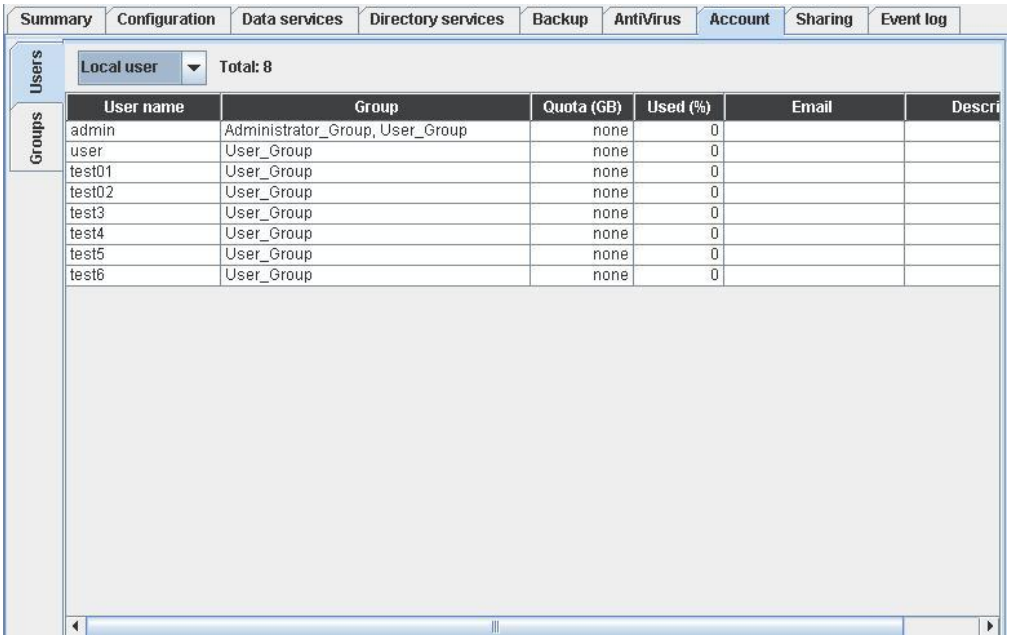
```
[root@qsan data]# smbldap-useradd -a -m test1
[root@qsan data]# smbldap-passwd test1
Changing UNIX and samba passwords for test-antony1
New password:
Retype new password:
```

Checking The Test Account in TrioNAS

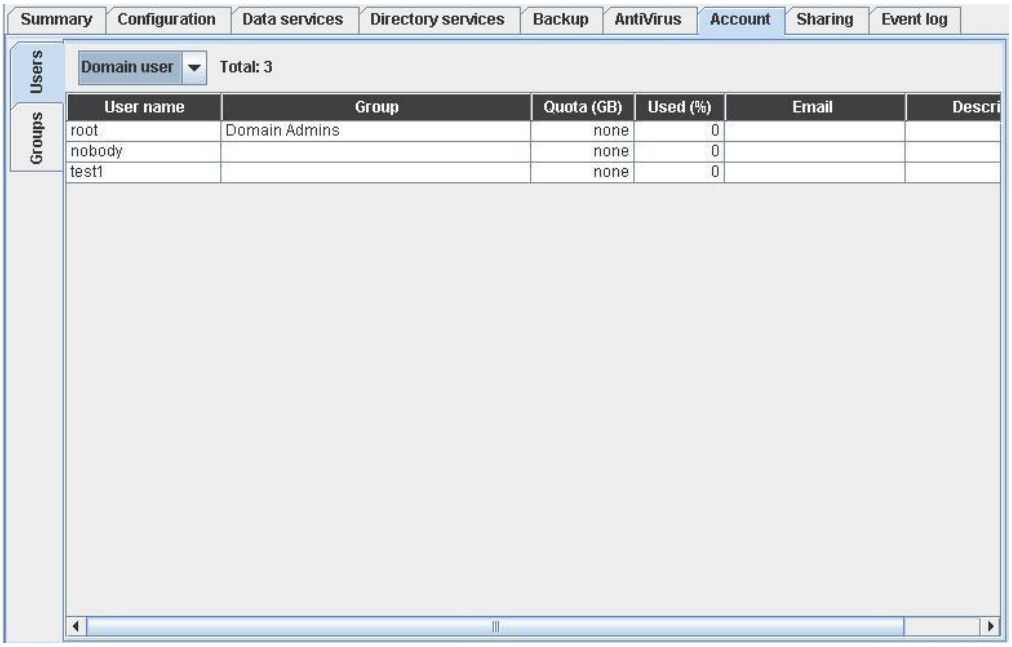
1. Turning on the TrioNAS storage, and then the QCentral for management
2. Logging on the TrioNAS
3. Configuring teh LDAP settings as below graphic:



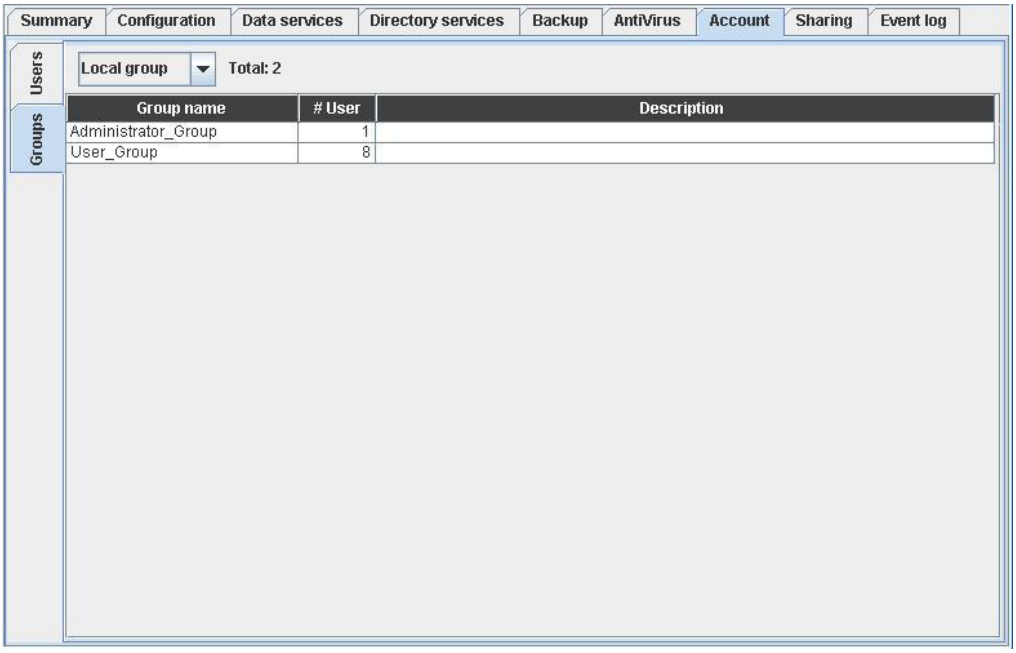
4. Observing if the User and Group could be displayed on both Local and Domain



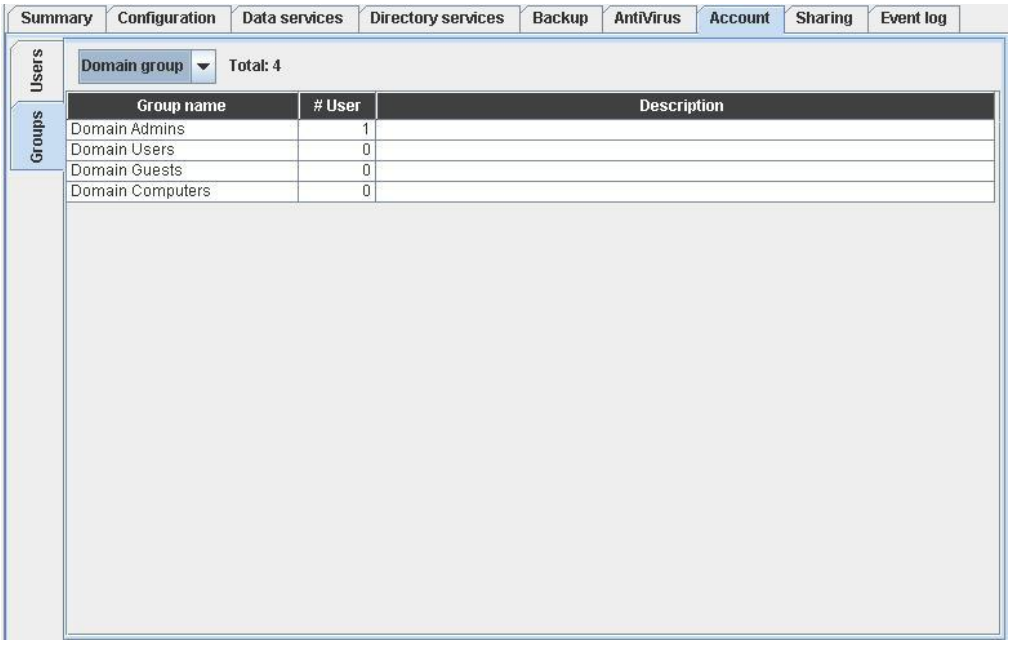
5. Domain users:



6. Local groups:



7. Domain groups:



Summary

We use the RHEL 6.1 for demostration in this document to show how to install and set up the LDAP service. But it is still possible to see different cases of compatibility issue while running the LDAP among different Linux distributions.

Since the LDAP server in this document is created based on the new OpenLDAP version which is quite different comparing the old version, we will suggest to use OpenLDAP with version 2.4.23 or later to prevent any compatibility issue.

Applies To

- TrioNAS (U110 / U210 / U220 / U221)
- TrioNAS LX (U400Q / U600Q)

Reference

- Open LDAP
  http://www.openldap.org/