Storageflex
NETWORK DATA STORAGE SOLUTIONS

Importing data from Linux LDAP server to HA3969U

Application Notes

Abstract:
This document describes how to import data and records from Linux LDAP servers to Storageflex HA3969U systems, and by doing so leverage existing directory service information for storage system authentication and access privilege settings.

Copyright © 2015 Storageflex Inc. All rights reserved. Storageflex is registered trademarks of Storageflex Inc. All other marks and names mentioned herein may be trademarks of their respective owners. The information contained herein is subject to change without notice. Content provided as is, without express or implied warranties of any kind

AN_EN_201408_GL_1.0

Table of Contents

Copyright © 2015 Storageflex Inc. All rights reserved.

Products covered in this document

These application notes apply to the following models:

HA3969U 12 Bay
HA3969U 16 Bay

Copyright © 2015 Storageflex Inc. All rights reserved.

Preface

LDAP server integration aims to alleviate many of the difficulties encountered by IT management and administration when handling a large number of user accounts across multiple network platforms and hardware units. After integrating LDAP server, all associated networking equipment can import and share user information from a single source, greatly reducing management complexity.

About LDAP

LDAP stands for Lightweight Directory Access Protocol, and offers an application protocol for the access and maintenance of information distributed across directory services via an internet protocol network, or IP. LDAP was designed to provide easier record set organization, typically using hierarchical structures. It is especially useful in enterprises and corporations, for example in company-wide email directory management. The initial concepts behind LDAP were developed with experience gathered from the management of telephone line subscriber directories, which include information such as name, address, and phone number per user.

OpenLDAP in Linux

OpenLDAP is an open source software implementation of the Lightweight Directory Access Protocol. Customers can use open source code to build LDAP server in Unix-based systems. Currently, numerous OpenLDAP software RPM packages are available online to choose from. You can read more about the OpenLDAP project here: http://www.openldap.org/

Purpose of this document

Offer guidance for importing user information from an existing LDAP server and introduce the types of entries in LDAP servers that can be successfully imported, and then demonstrate a typical entry as an example.

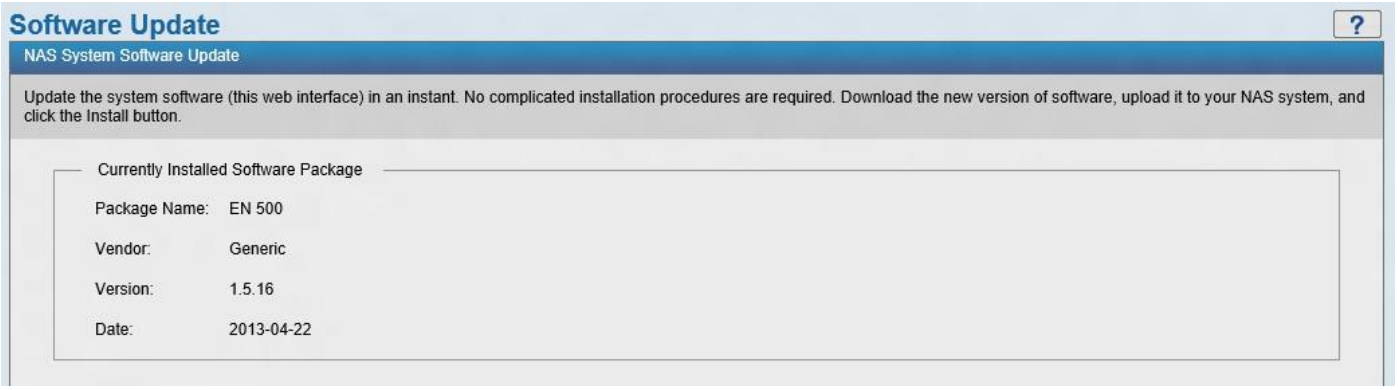
Copyright © 2015 Storageflex Inc. All rights reserved.

Environment preparation

Storage preparation

Check firmware version

Make sure the firmware package is the latest version.

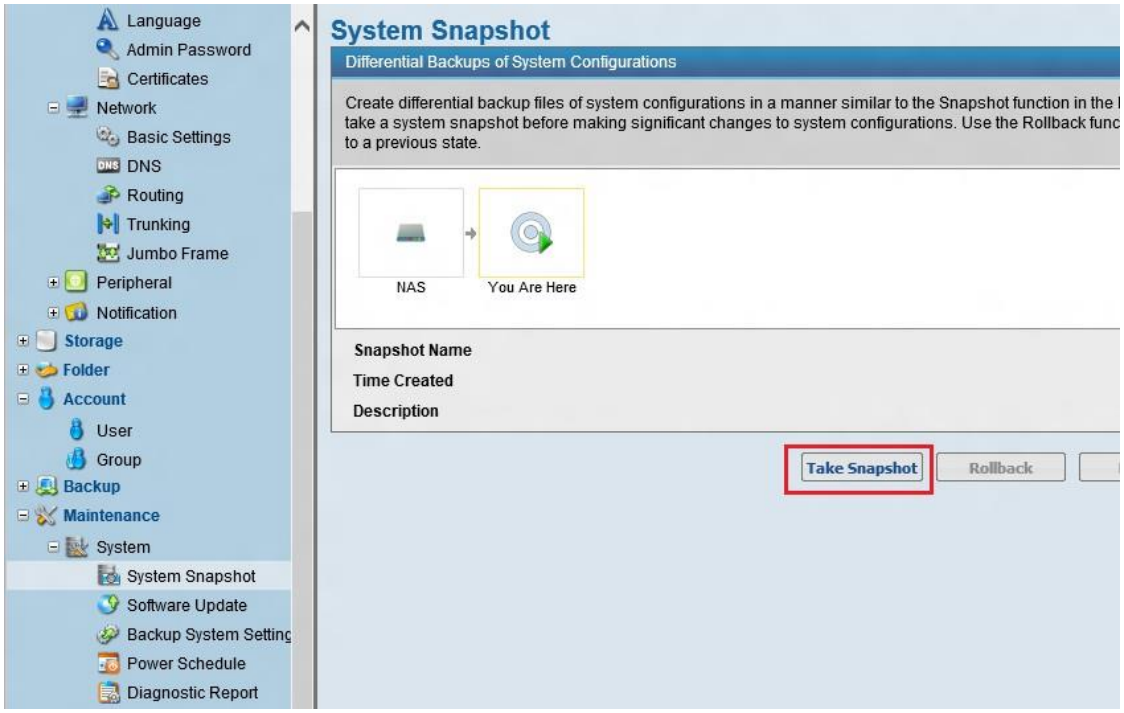


Copyright © 2015 Storageflex Inc. All rights reserved.

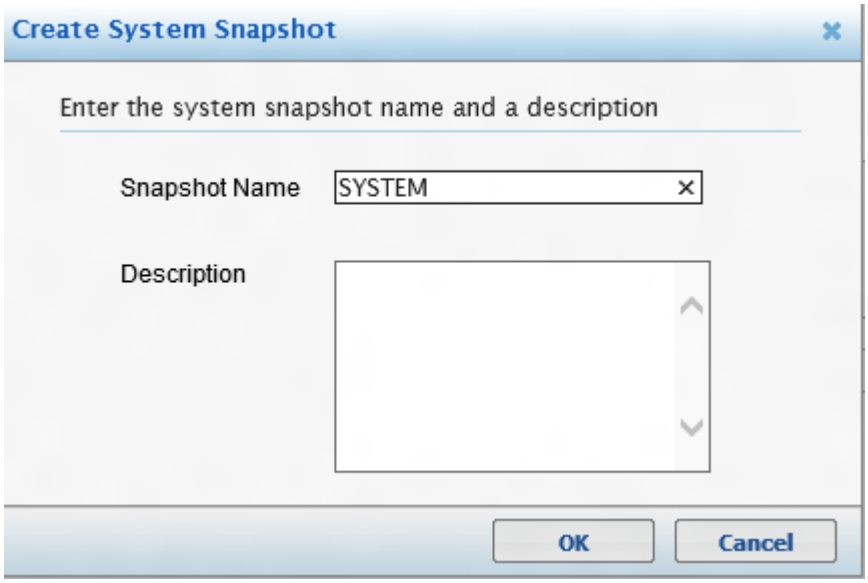
System backup via snapshot

Take a snapshot before proceeding with making changes to file settings to guard against errors that may occur during the importation process of LDAP user accounts.

A. Click "Take Snapshot"

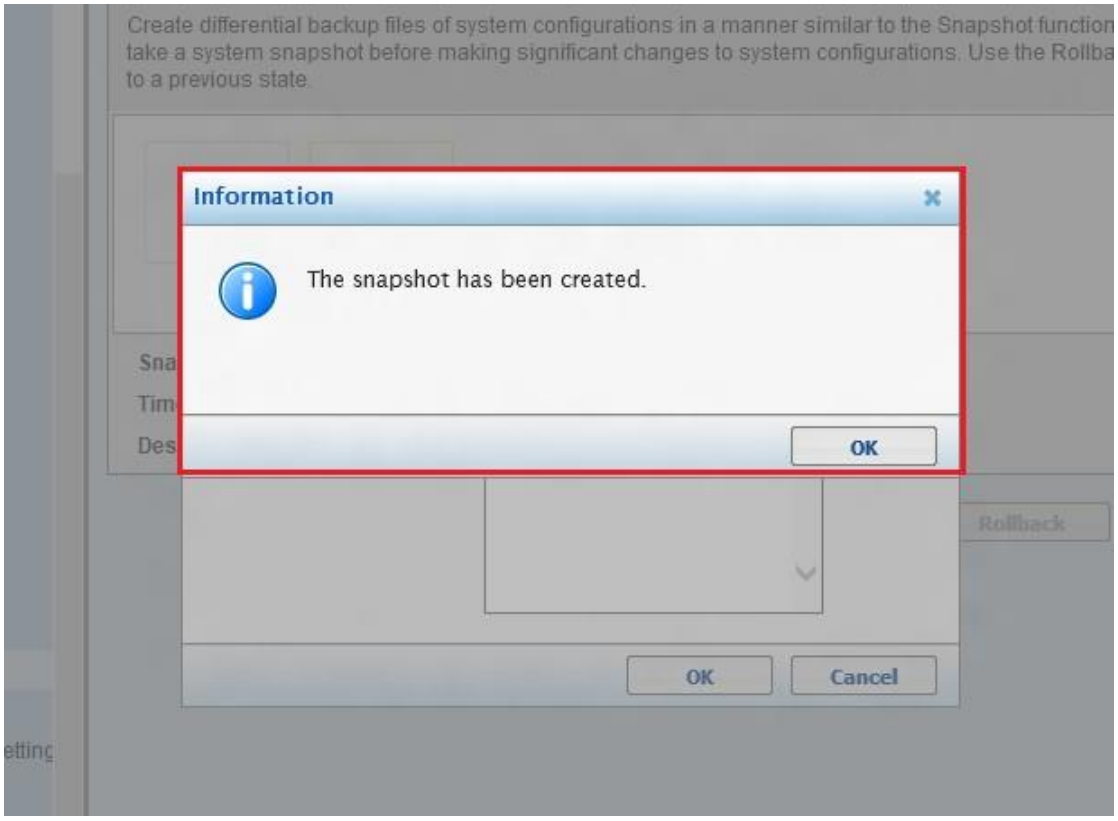


B. Set snapshot image name

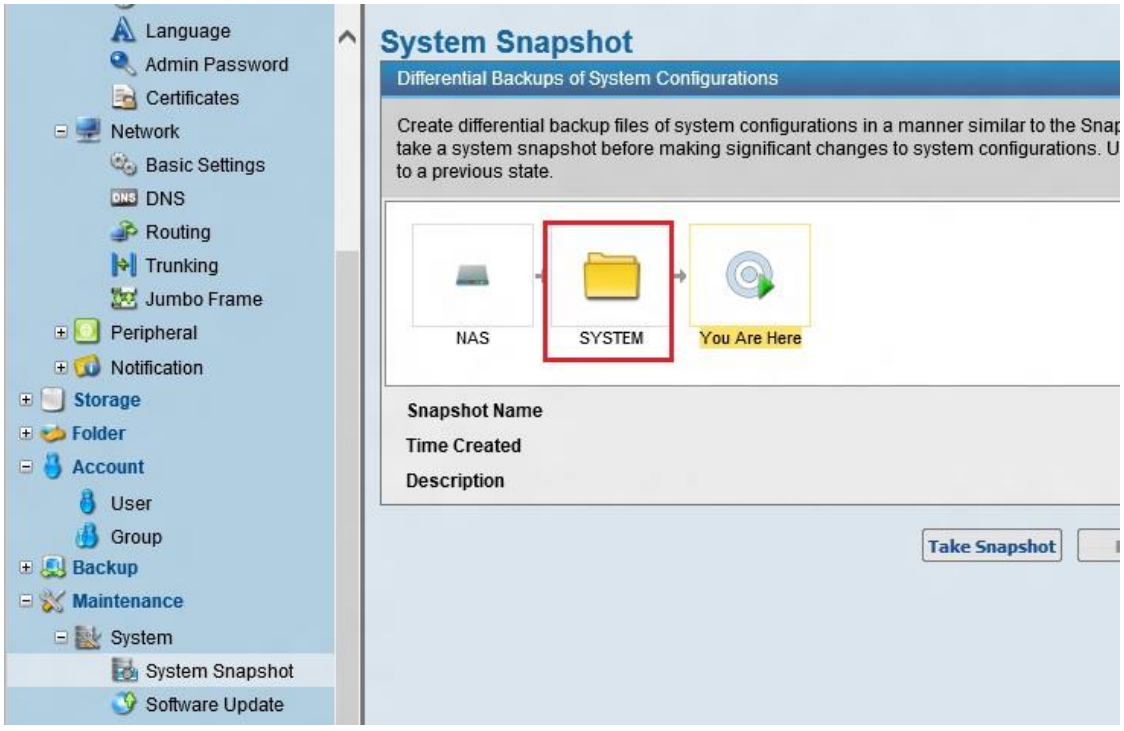


C. Check information shown

Copyright © 2015 Storageflex Inc. All rights reserved.



D. Ensure snapshot image is created



Downtime preparation for system reboot

A. Arrange downtime for HA3969U reboot procedure
B. Downtime in this case means only the time required to reboot

Copyright © 2015 Storageflex Inc. All rights reserved.

LDAP server check

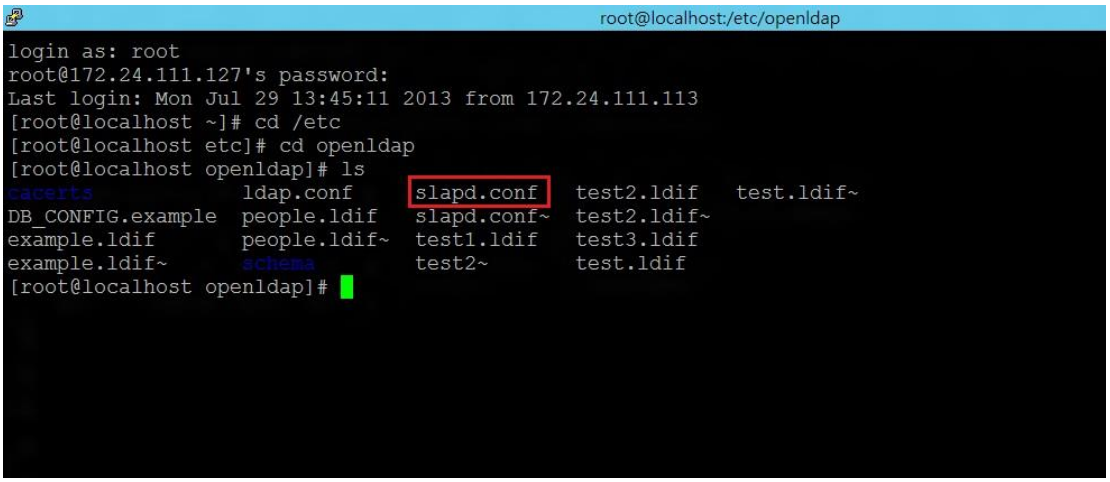
Existing LDAP server with accounts

A. We suggest customers prepare one LDAP server for examination and evaluation
B. This test LDAP server should include all user accounts
C. The test LDAP server will be the target server for HA3969U

Acquire base DN for LDAP server

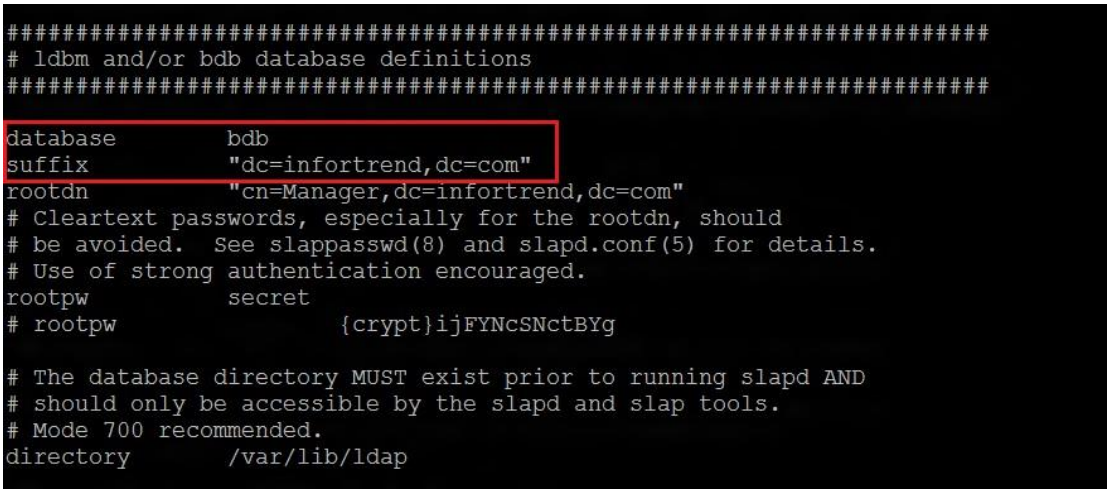
Before starting LDAP configuration from HA3969U, check the LDAP server using the following steps. In this section, several ways to find LDAP server base DN will be introduced. Users may choose a suitable method for detecting LDAP server base DN as applies to each situation.

1. Leverage information from configuration files used by the LDAP server's database:
   A. Open the configuration file used by the LDAP server's database. By default, this file should be slapd.conf. (note: LDAP server administrators may use other files as the database configuration file, please verify the location of this file before continuing)



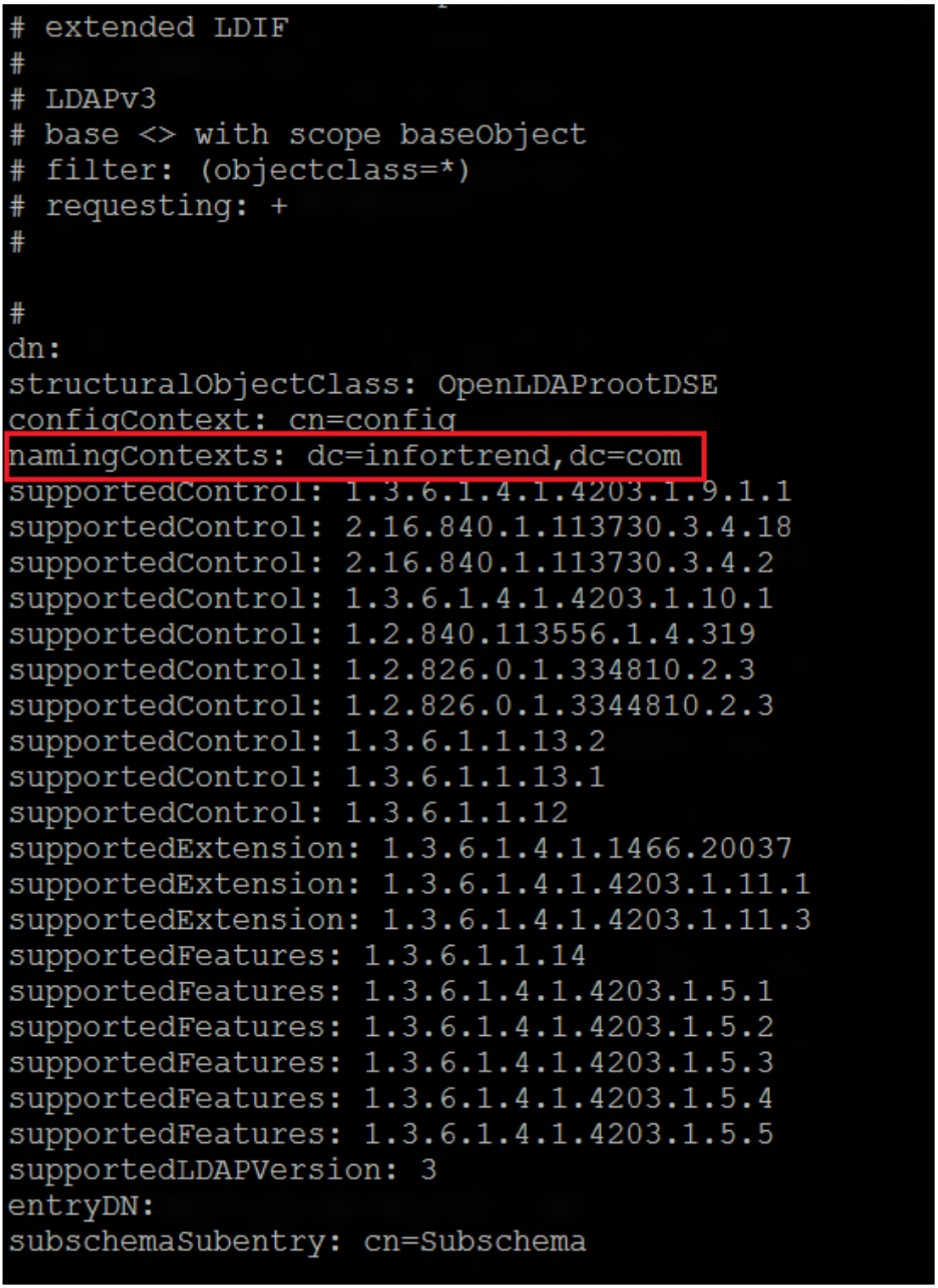
   B. Open the configuration file. The string following "suffix" is the LDAP server's base DN: "dc=Storageflex,dc=com"

Copyright © 2015 Storageflex Inc. All rights reserved.



2. Use ldapsearch to find the LDAP server's base DN
   Log in from any server which supports ldapsearch. Then, enter "ldapsearch -h LDAP_server_IP -x -s base -b "" "(objectclass=*)" + ". The string following "namingContexts" is the base DN

Copyright © 2015 Storageflex Inc. All rights reserved.



Acquire DN for superuser

1. Find the superuser's DN in the configuration file
   Open the configuration file used by the LDAP server, and then find the string following "rootdn".
   In this example, the rootdn is " cn=Manager, dc=Storageflex, dc=com"

Copyright © 2015 Storageflex Inc. All rights reserved.

```
#######################################################################
# ldbm and/or bdb database definitions
#######################################################################

database        bdb
suffix          "dc=infortrend,dc=com"
rootdn          "cn=Manager,dc=infortrend,dc=com"
# Cleartext passwords, especially for the rootdn, should
# be avoided.  See slappasswd(8) and slapd.conf(5) for details.
# Use of strong authentication encouraged.
rootpw          secret
# rootpw                {crypt}ijFYNcSNctBYg

# 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/lib/ldap

# Indices to maintain for this database
index objectClass                       eq,pres
index ou,cn,mail,surname,givenname      eq,pres,sub
index uidNumber,gidNumber,loginShell    eq,pres
index uid,memberUid                     eq,pres,sub
index nisMapName,nisMapEntry            eq,pres,sub

# Replicas of this database
#replogfile /var/lib/ldap/openldap-master-replog
#replica host=ldap-1.example.com:389 starttls=critical
#     bindmethod=sasl saslmech=GSSAPI
#     authcId=host/ldap-master.example.com@EXAMPLE.COM
```

2. Find superuser DN using ldapsearch
   If you know the superuser's RDN, you can try to obtain their DN with the ldapsearch command. In the command line, enter "ldapsearch -x -h LDAP_server_IP -b "base DN" "(RDN)" ". In this example, the RDN is "cn=Manager". Note: you can also use this method to look up other DNs with superuser authority. Also, if the superuser entry is not built into the directory, use the configuration file to obtain superuser status

```
[root@localhost openldap]# vi slapd.conf
[root@localhost openldap]# ldapsearch  -h 172.24.111.127 -x  -b "dc=infortrend,dc=com" "(cn=manager)"
# extended LDIF
#
# LDAPv3
# base <dc=infortrend,dc=com> with scope subtree
# filter: (cn=manager)
# requesting: ALL
#

# Manager, infortrend.com
dn: cn=Manager,dc=infortrend,dc=com
cn: Manager
objectClass: organizationalRole
```

Check the format of account entry

LDAP user accounts need to meet the following criteria to let HA3969U successfully import from them:

1. The entry must be defined using nis.shema. The example is a typical entry using nis.shema:

Copyright © 2015 Storageflex Inc. All rights reserved.

```
# mike.chen, user, login, infortrend.com
dn: cn=mike.chen,ou=user,ou=login,dc=infortrend,dc=com
cn: mike.chen
objectClass: account
objectClass: posixAccount
objectClass: shadowAccount
userPassword:: c3IxMjM0NTY=
shadowLastChange: 11108
shadowMax: 99999
shadowWarning: 7
shadowFlag: 0
loginShell: /bin/bash
uidNumber: 600
gidNumber: 510
homeDirectory: /home/mike.chen
gecos: Nicole Coon
uid: sr123456
```

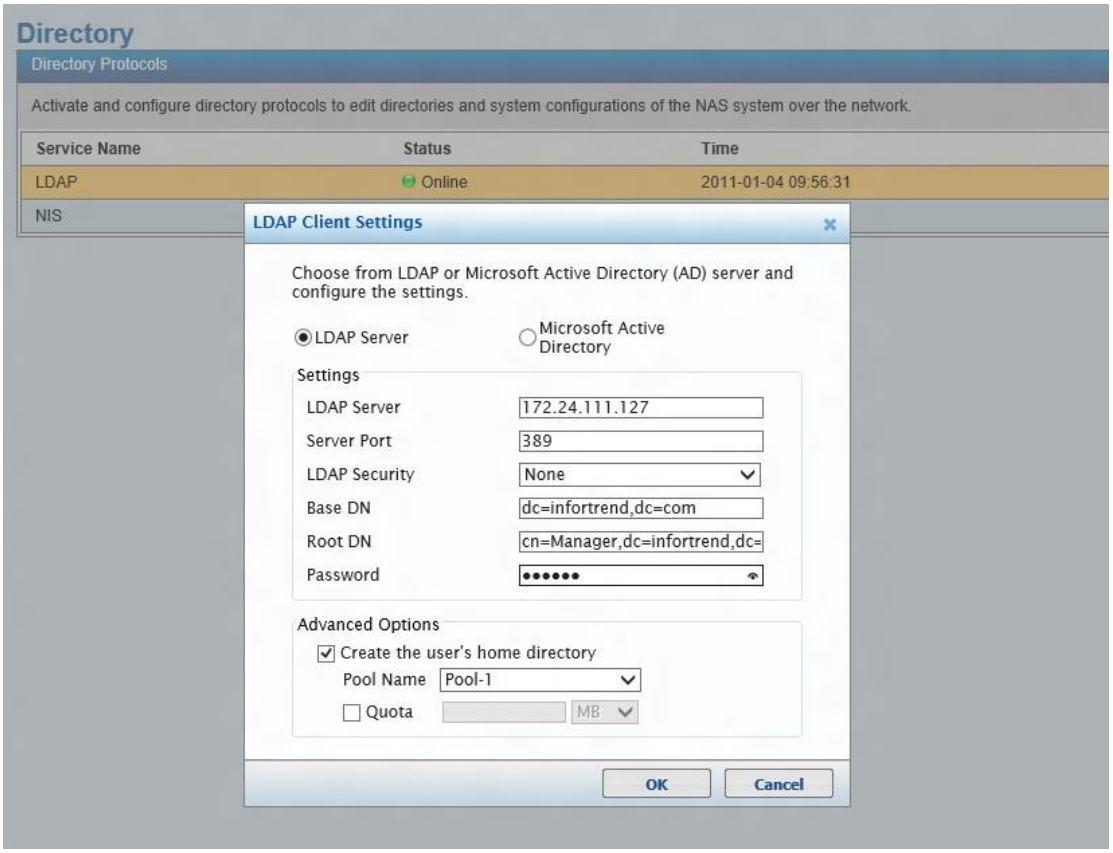
2. The user ID’s first character must be alphabetic. User IDs cannot end with a period

Copyright © 2015 Storageflex Inc. All rights reserved.

Storage configuration

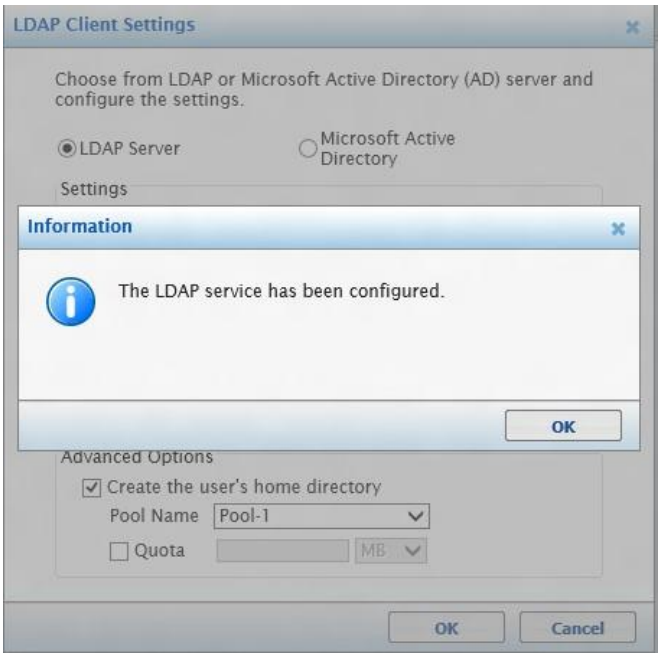
Build a connection with LDAP server

1. Add the following LDAP server information to establish LDAP service:
   A. Enter the LDAP server IP address, base DN, superuser DN (root DN), password for root DN, and server port (LDAP server default is 389)



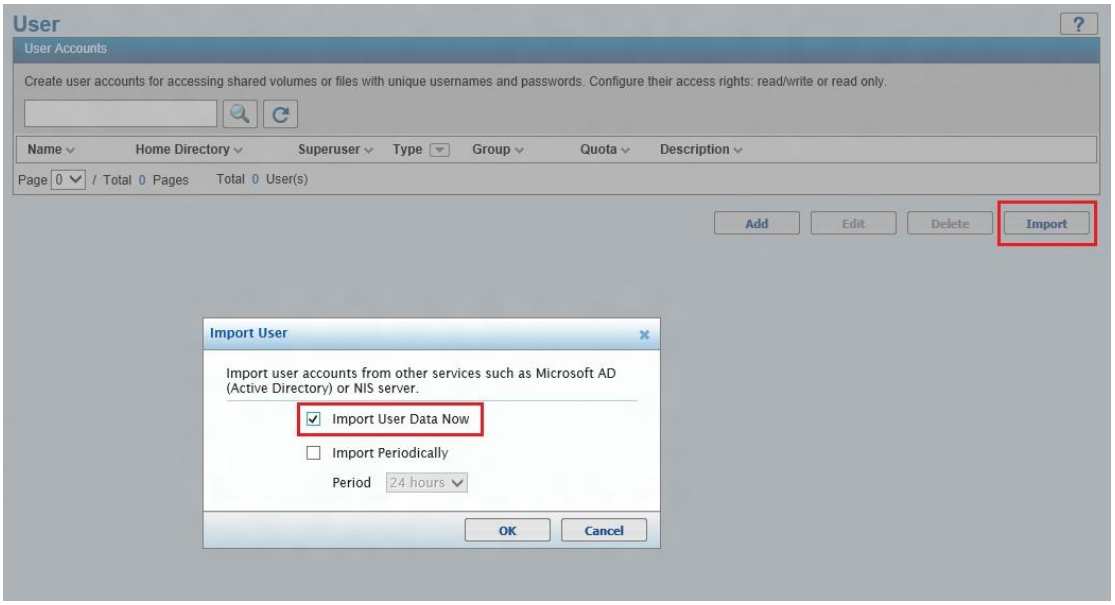
   B. When LDAP configuration is successful, HA3969U has built a connection with LDAP server

Copyright © 2015 Storageflex Inc. All rights reserved.



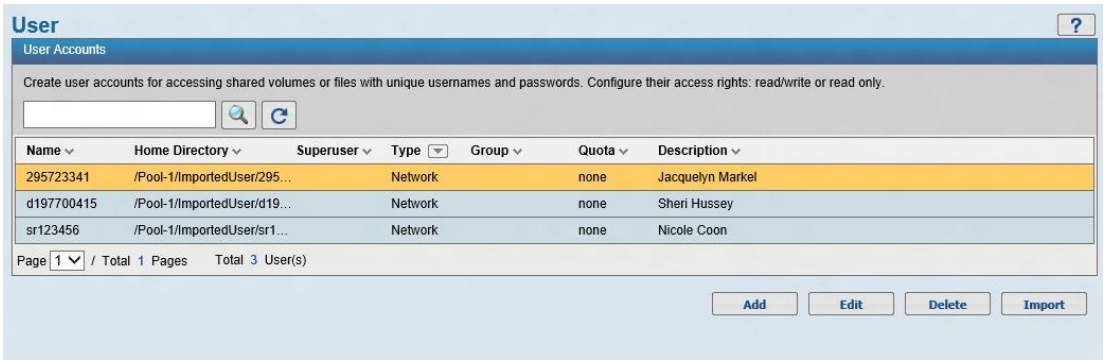
Import user accounts from LDAP server

A. Switch to the "User" tab under "Account", and then run the user account import process



B. Only user accounts defined by nis.schema will be imported (note: if accounts do not meet the criteria in 4.1 and 4.2, they will not work correctly)

Copyright © 2015 Storageflex Inc. All rights reserved.



Copyright © 2015 Storageflex Inc. All rights reserved.

Conclusion

Authorization is an important issue in file sharing, and often results in too many separate instances of user information across different networking platforms and equipment. This complexity, which is quite likely to cause problems, is simplified using LDAP server as a very helpful user information management center. Through integrating with LDAP server, administrators can easily manage even very large user information databases.

Copyright © 2015 Storageflex Inc. All rights reserved.

Appendix

Recovery procedure

If the firmware update fails or user data crashes, simply rollback to the previous snapshot point to recover data.

A. Go to the “Maintenance” tab
B. Click “System”
C. Select the recovery snapshot image
D. Click “Rollback”

Copyright © 2015 Storageflex Inc. All rights reserved.