What is UnifiedAUTH?

U400Q Series
U600Q Series

Version 1.0
August 2012

Copyright

Trademarks

Qsan Technology, Inc.

4F., No.103, RuiHu Street,
NeiHu District, Taipei 114
Taiwan, R.O.C.

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

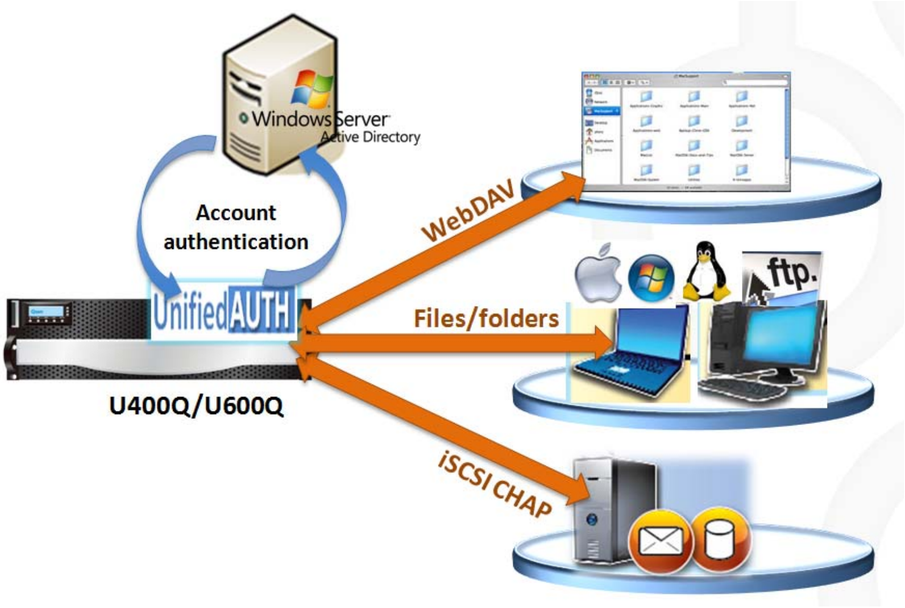
Email: sales@QsanTechnology.com
Website: www.QsanTechnology.com

Introduction

UnifiedAUTH is the abbreviation for unified authentication. In a network environment, data security is critical and essential. The basic approach is to implement access control against those shared folders, which requires the process of authentication and authorization. Authentication requires users to present something they know and can validate themselves. The most common way is by account and password.

In many cases, different file sharing services are hosted at different servers with different sets of account/password. Users need to memorize different sets of account/password for different services such as CIFS, FTP, AFP and iSCSI. Since the goals of Qsan unified storage is to consolidate hardware requirements, reduce management complexity and increase storage efficiency, UnifiedAUTH empowers users with the ability to use the very same set of account/password to access all data services (CIFS, NFS, AFP, FTP, iSCSI, and WebDAV) provided by Qsan unified storage.

It is similar to the idea of single sign on, but not the way it works. You still need to key in your account and password when you establish the data connection for the first time. It's more like the concept of Schengen visa. With a valid Schengen visa, you may travel different countries in Europe.

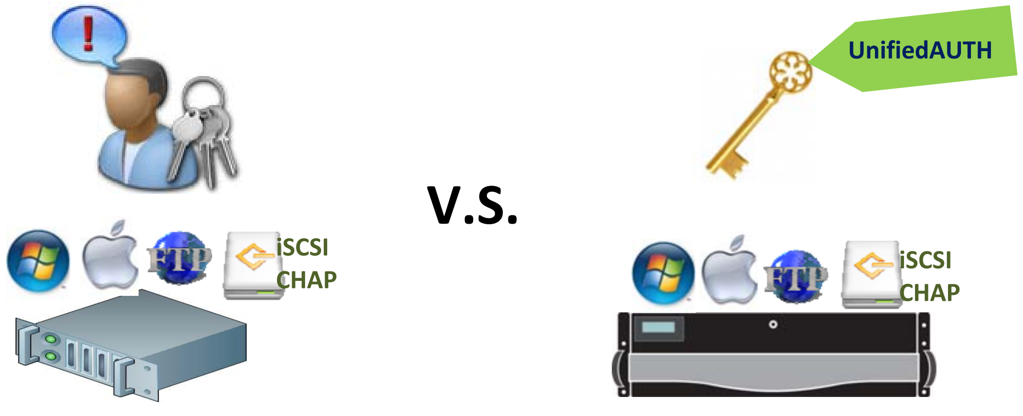


Benefits of UnifiedAUTH

UnifiedAUTH can really come in handy for IT managers. Image that in a medium size company with 200 employees, if the NAS system doesn't support directory services integrated into all data services, a separate FTP account and a separate iSCSI CHAP account along with the directory service account will yield 3 sets of different accounts to manage. It means that IT managers need to maintain 200x3=600 records. It's a nightmare and headache to follow all kinds of requests of account management. For NAS end user, each person needs to memorize 3 different passwords for different data services. If the demands go up, a second or 3rd NAS is added to the environment. More passwords need to be memorized and more account records need to be maintained.

Qsan UnifiedAUTH solves all these problems and gives you a consolidated and proven solution. Benefits are :

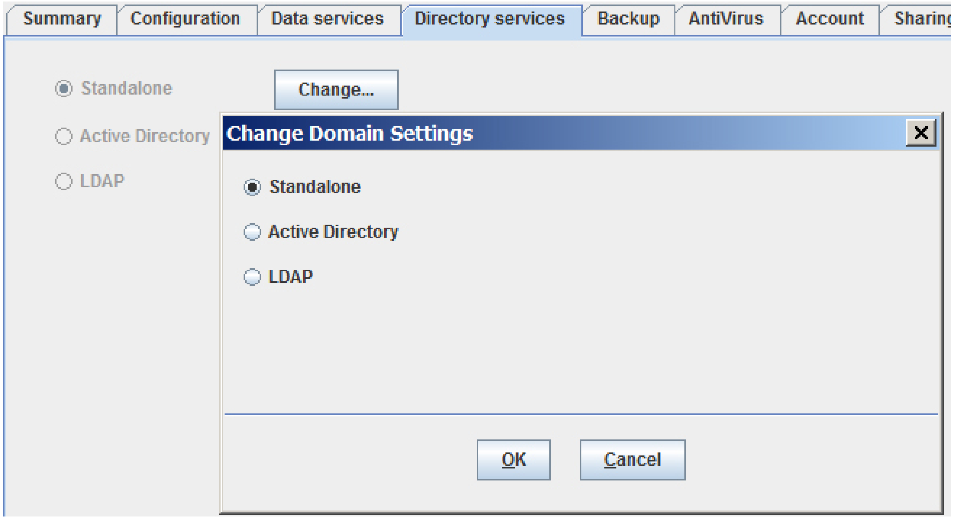
- Easier use of all data services with one set of account and password
- Simplified management



Directory services

A **directory** is a type of database containing descriptive information of entries, that describe people such as name, phone number, email address and of course including account and password. **Directory service** is the function that provides the capability of quickly authenticating user based on their account and password. Please go to the directory service tab in QCentral. Qsan unified storage provides three directory services.

- Standalone (default)
- Microsoft Active Directory
- LDAP



● Standalone
○ Active Directory
○ LDAP

Change Domain Settings

● Standalone
○ Active Directory
○ LDAP

The default service is **Standalone**, which is the local users and groups create in Qsan unified storage. Only one service can be activated at all time. They are mutual exclusive to reduce confusion and increase efficiency. Users will not be able to activate any two services at the same time.

Standalone (default)

When you don't have a directory service in your network environment, you can simply create user account and group account in Qsan unified storage and use them to access all data services provided. Default accounts are **admin** and **user**. Default groups are **administrator_group** and **user_group**.

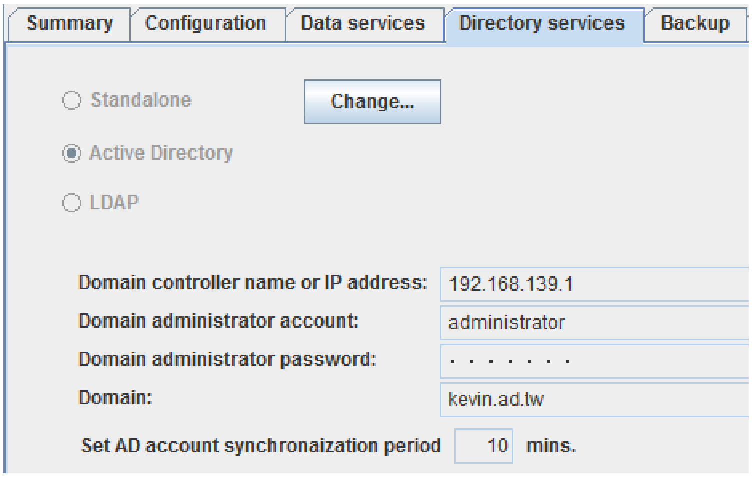
Because UnifiedAUTH integrate with iSCSI CHAP account authentication, the password restriction of at least 12 to 16 characters in length will be enforced in all three directory services.

Before you can create local account, make sure that a storage pool with home directory function enabled is created first. Otherwise, you won't be able to create local account. All functions will be grey out.

Microsoft Active Directory

Qsan unified storage supports Microsoft Active Directory service for both Windows Server 2003 R2 and Server 2008 R2. Both AD account and LDAP account will be considered as **domain** account. You can NOT modify domain account properties. They are for display purpose only. You may modify the domain account on AD server or LDAP server. The maximum number of domain account is 65536.

This is what looks like after joining AD domain (kevin).



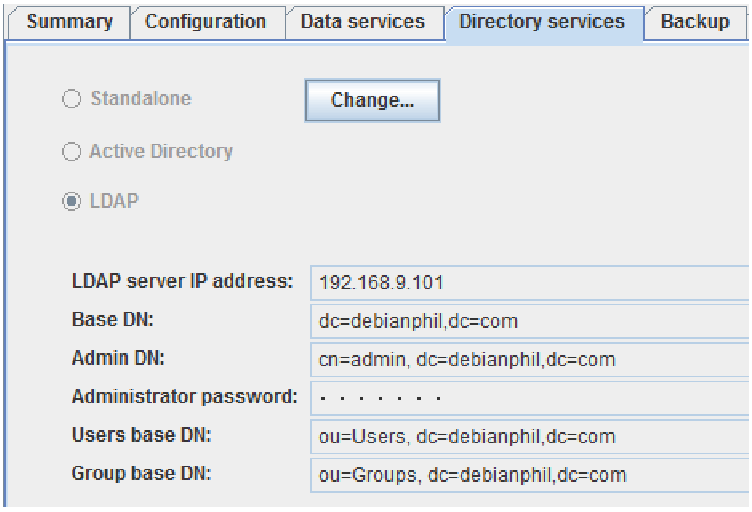
○ Standalone
● Active Directory
○ LDAP

Domain controller name or IP address: 192.168.139.1
Domain administrator account: administrator
Domain administrator password: • • • • • • •
Domain: kevin.ad.tw
Set AD account synchronaization period 10 mins.

LDAP (Lightweight Directory Access Protocol)

Qsan unified storage supports LDAP version 3. LDAP is also a popular directory service in many working environments. LDAP account will be considered as **domain** account. You can NOT modify domain account properties. The maximum number of domain account is 65536.

This is what looks like after logging in LDAP server.



○ Standalone

○ Active Directory

● LDAP

LDAP server IP address: 192.168.9.101

Base DN: dc=debianphil,dc=com

Admin DN: cn=admin, dc=debianphil,dc=com

Administrator password: · · · · · · ·

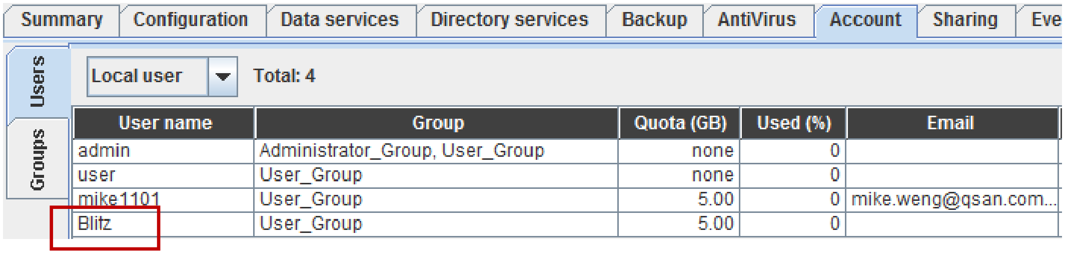
Users base DN: ou=Users, dc=debianphil,dc=com

Group base DN: ou=Groups, dc=debianphil,dc=com

If you don’t know what parameters (base DN) to enter, please consult your IT administrators.

Standalone with different data services

Let’s create a local user called Blitz and use the home directory for testing. We will demonstrate with CIFS, FTP and iSCSI services.



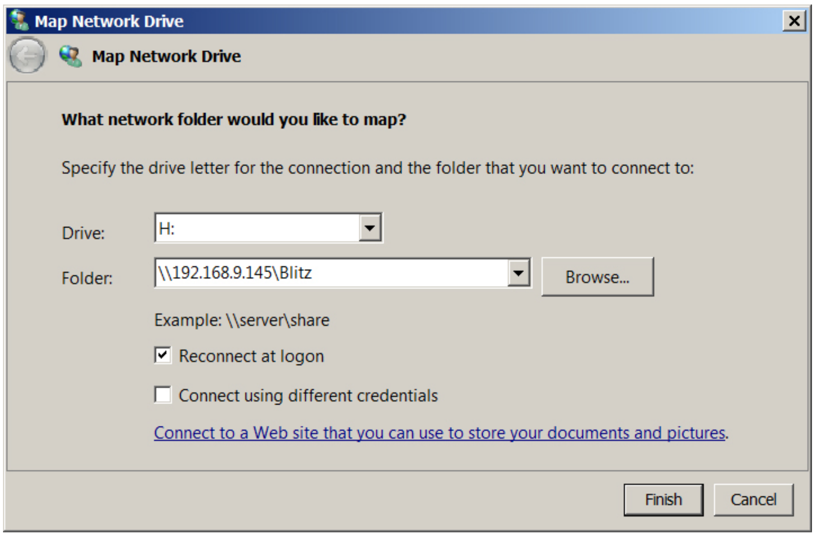
Total: 4

User name	Group	Quota (GB)	Used (%)	Email
admin	Administrator_Group, User_Group	none	0	
user	User_Group	none	0	
mike1101	User_Group	5.00	0	mike.weng@qsan.com...
Blitz	User_Group	5.00	0	

Suppose the network port IP is 192.168.9.145

Standalone with CIFS/Samba

In Win7, let’s try to set up a network drive with letter – H.



Map Network Drive

Map Network Drive

What network folder would you like to map?

Specify the drive letter for the connection and the folder that you want to connect to:

Drive: H:

Folder: \\192.168.9.145\Blitz Browse...

Example: \\server\share

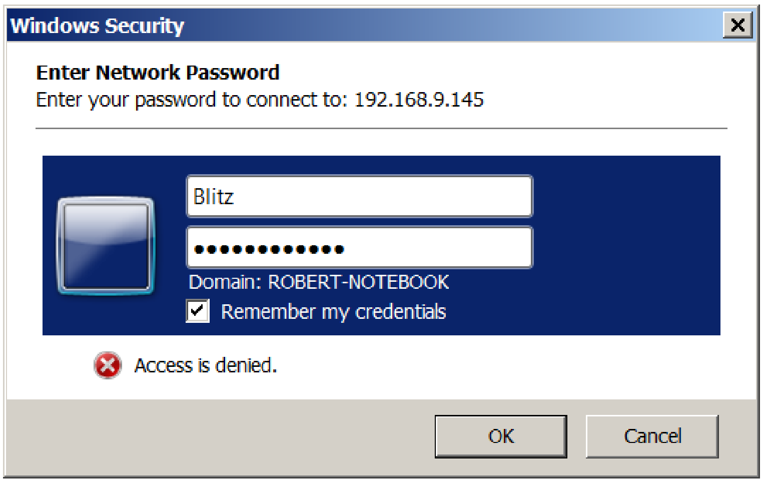
☑ Reconnect at logon

□ Connect using different credentials

Connect to a Web site that you can use to store your documents and pictures.

Finish Cancel

A dialog box will pop up for account and password. Put in Blitz and its password.



Windows Security

Enter Network Password

Enter your password to connect to: 192.168.9.145

Blitz

●●●●●●●●●●●●

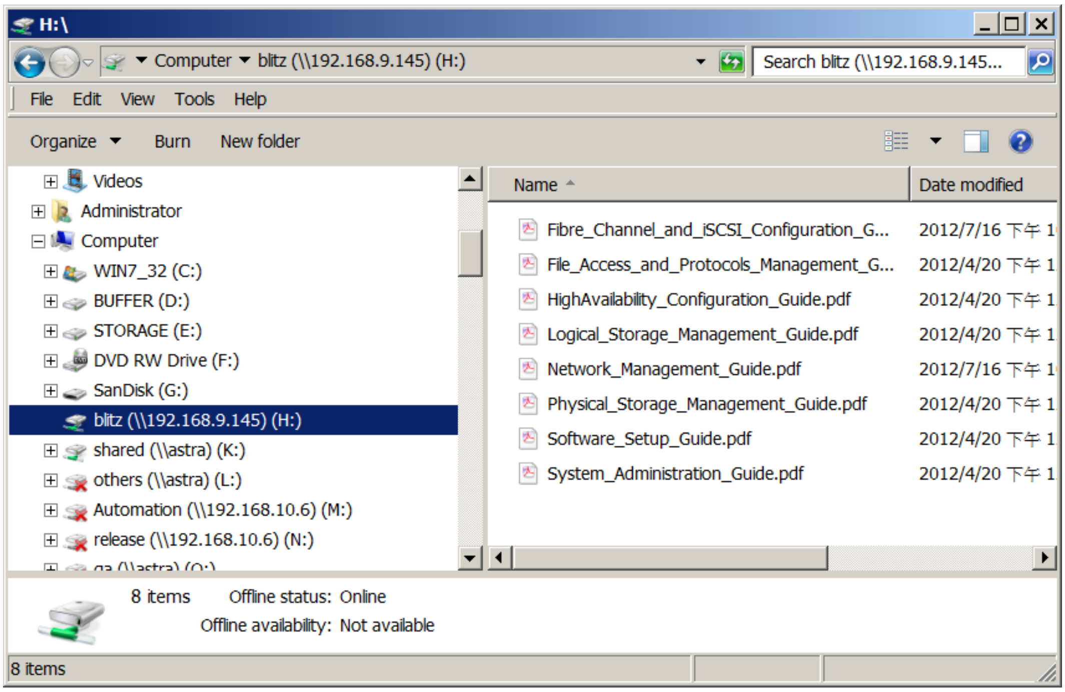
Domain: ROBERT-NOTEBOOK

☑ Remember my credentials

Access is denied.

OK Cancel

Now you may access Blitz home directory as drive H. Let's put some files inside.



H:\

Computer ▸ blitz (\\192.168.9.145) (H:)

Search blitz (\\192.168.9.145...

- Videos
- Administrator
- Computer
  - WIN7_32 (C:)
  - BUFFER (D:)
  - STORAGE (E:)
  - DVD RW Drive (F:)
  - SanDisk (G:)
  - blitz (\\192.168.9.145) (H:)
  - shared (\\astra) (K:)
  - others (\\astra) (L:)
  - Automation (\\192.168.10.6) (M:)
  - release (\\192.168.10.6) (N:)
  - qa (\\astra) (O:)

Name	Date modified
Fibre_Channel_and_iSCSI_Configuration_G...	2012/7/16 下午 1
File_Access_and_Protocols_Management_G...	2012/4/20 下午 1
HighAvailability_Configuration_Guide.pdf	2012/4/20 下午 1
Logical_Storage_Management_Guide.pdf	2012/4/20 下午 1
Network_Management_Guide.pdf	2012/7/16 下午 1
Physical_Storage_Management_Guide.pdf	2012/4/20 下午 1
Software_Setup_Guide.pdf	2012/4/20 下午 1
System_Administration_Guide.pdf	2012/4/20 下午 1

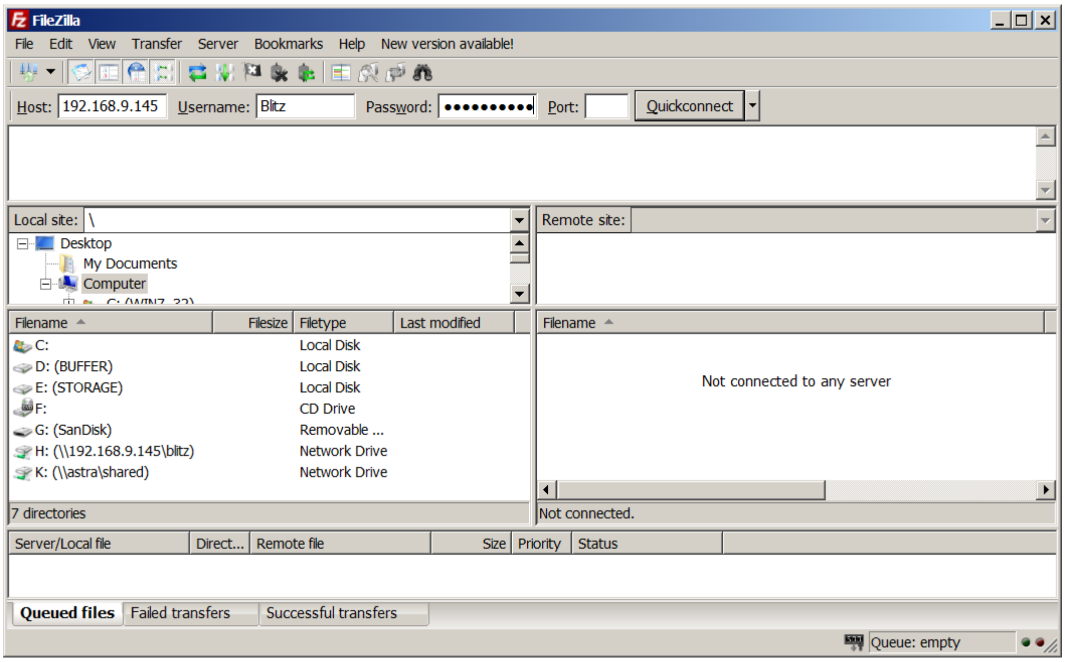
8 items Offline status: Online

Offline availability: Not available

8 items

Standalone with FTP

In win7, use FileZilla to connect to Blitz home directory. Use the same Blitz account and password for access.



Host: 192.168.9.145 Username: Blitz Password: •••••••••• Port:

Local site: \

Desktop
My Documents
Computer

Remote site:

Filename	Filesize	Filetype	Last modified
C:		Local Disk	
D: (BUFFER)		Local Disk	
E: (STORAGE)		Local Disk	
F:		CD Drive	
G: (SanDisk)		Removable ...	
H: (\\192.168.9.145\blitz)		Network Drive	
K: (\\astra\shared)		Network Drive	

Not connected to any server

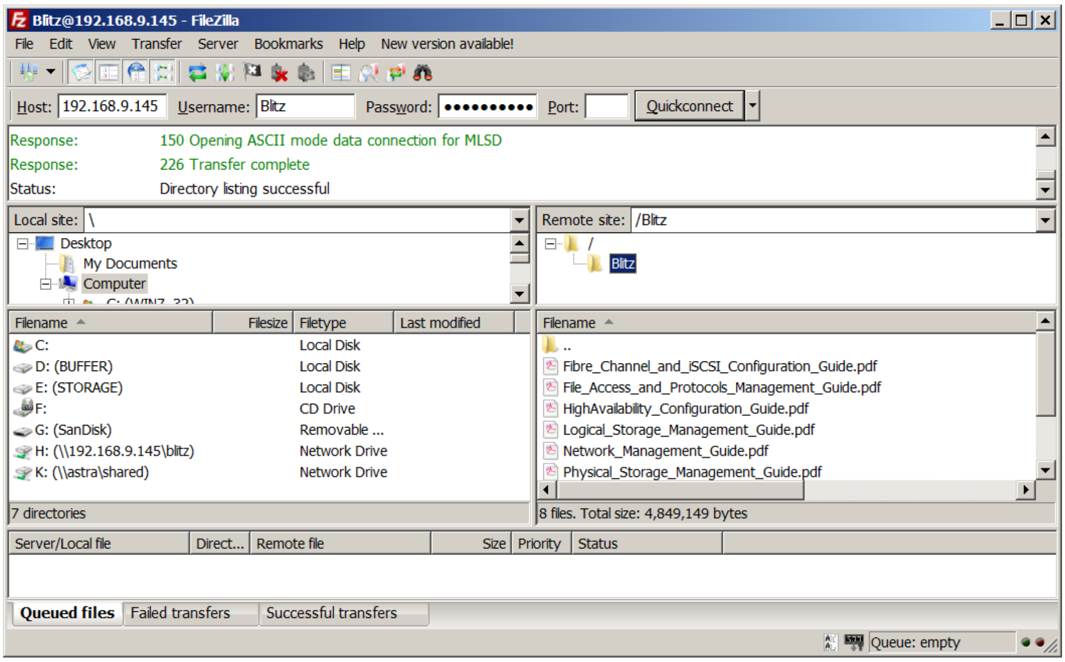
7 directories

Not connected.

Server/Local file	Direct...	Remote file	Size	Priority	Status

Queue: empty

Click Quickconnect button. And you may access the files through FTP using the same account and password.


Blitz@192.168.9.145 - FileZilla
File Edit View Transfer Server Bookmarks Help New version available!
Quickconnect
Queued files
Failed transfers
Successful transfers

Host: 192.168.9.145 Username: Blitz Password: •••••••••• Port:

```
Response:     150 Opening ASCII mode data connection for MLSD
Response:     226 Transfer complete
Status:       Directory listing successful
```

Local site: \

Desktop
My Documents
Computer

Remote site: /Blitz

/
Blitz

Filename	Filesize	Filetype	Last modified
C:		Local Disk	
D: (BUFFER)		Local Disk	
E: (STORAGE)		Local Disk	
F:		CD Drive	
G: (SanDisk)		Removable ...	
H: (\\192.168.9.145\blitz)		Network Drive	
K: (\\astra\shared)		Network Drive	

Filename
..
Fibre_Channel_and_iSCSI_Configuration_Guide.pdf
File_Access_and_Protocols_Management_Guide.pdf
HighAvailability_Configuration_Guide.pdf
Logical_Storage_Management_Guide.pdf
Network_Management_Guide.pdf
Physical_Storage_Management_Guide.pdf

7 directories

8 files. Total size: 4,849,149 bytes

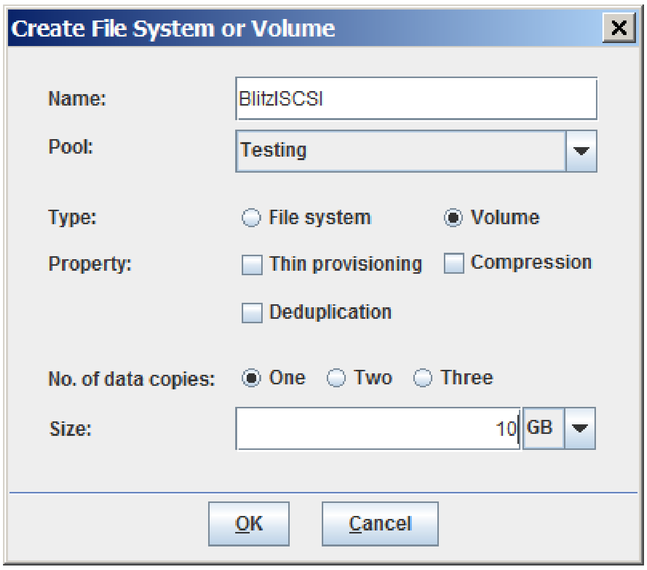
Server/Local file	Direct...	Remote file	Size	Priority	Status

Queue: empty

Standalone with iSCSI CHAP authentication

Let’s create an iSCSI volume and set up the CHAP account using Blitz.

1. First, create a 10GB volume.



Create File System or Volume

Name: BlitzISCSI

Pool: Testing

Type: ○ File system ● Volume

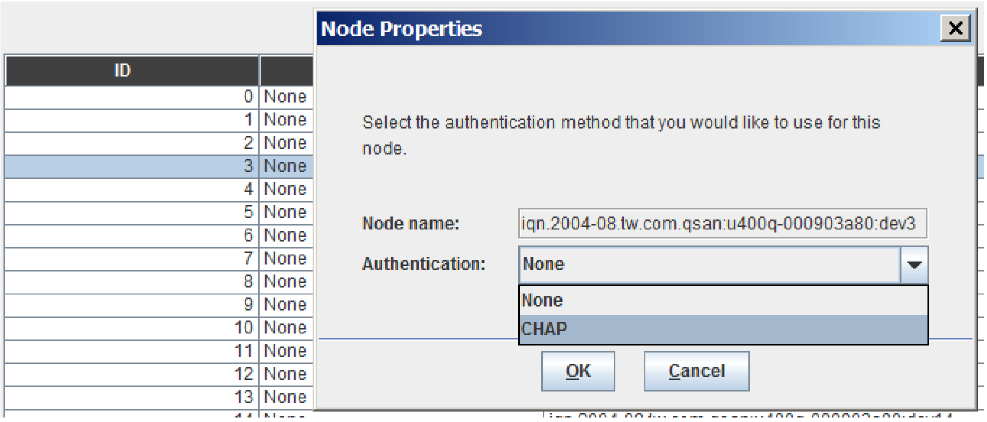
Property: □ Thin provisioning □ Compression

□ Deduplication

No. of data copies: ● One ○ Two ○ Three

Size: 10 GB

2. Go to **Data services** -> **iSCSI** tab. Pick up a node ID (Let's use 3) and right click to select **Properties**. Select **CHAP** to enable CHAP account function.



ID	
0	None
1	None
2	None
3	None
4	None
5	None
6	None
7	None
8	None
9	None
10	None
11	None
12	None
13	None

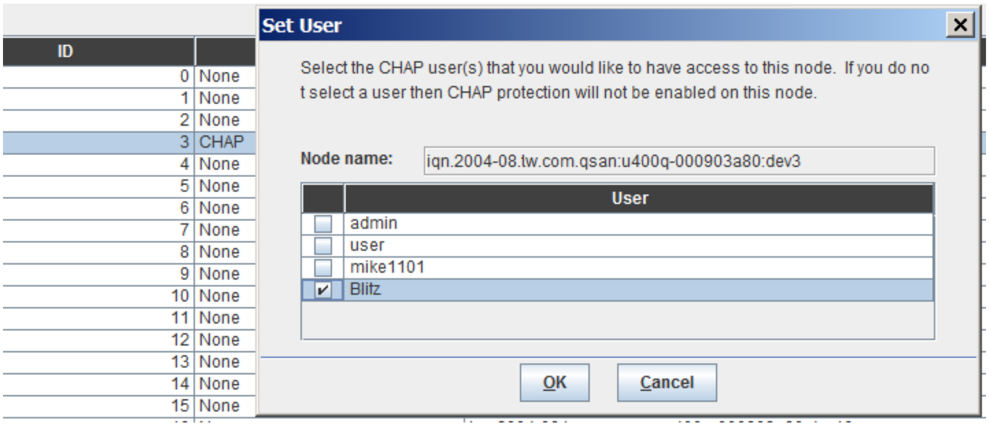
Node Properties

Select the authentication method that you would like to use for this node.

Node name: iqn.2004-08.tw.com.qsan:u400q-000903a80:dev3

Authentication: None

3. Right click and select **Set user**. Select Blitz.



ID	
0	None
1	None
2	None
3	CHAP
4	None
5	None
6	None
7	None
8	None
9	None
10	None
11	None
12	None
13	None
14	None
15	None

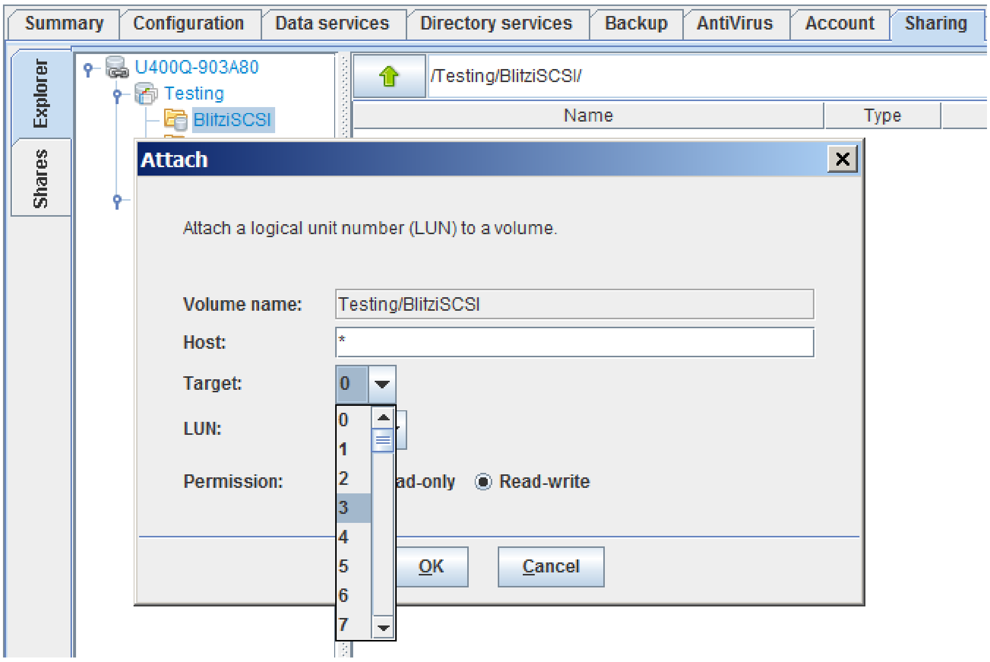
Set User

Select the CHAP user(s) that you would like to have access to this node. If you do no t select a user then CHAP protection will not be enabled on this node.

Node name: iqn.2004-08.tw.com.qsan:u400q-000903a80:dev3

	User
□	admin
□	user
□	mike1101
☑	Blitz

4. Go to **Sharing** tab. Right click on the BlitzISCSI volume we just created in step 1. And select the target node as 3 and attach LUN.



Attach

Attach a logical unit number (LUN) to a volume.

Volume name: Testing/BlitziSCSI

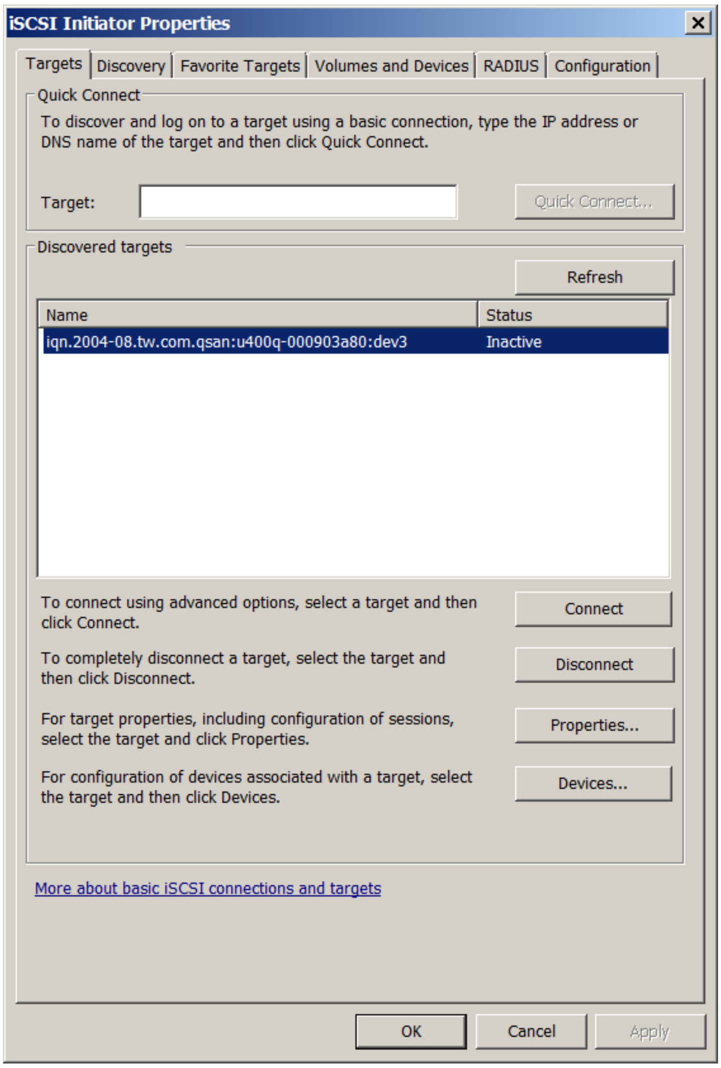
Host: *

Target: 0

LUN:

Permission: ○ Read-only ● Read-write

5. Let’s try to use iSCSI initiator to attach Blitz volume. In Win7, launch iSCSI initiator and put in the network IP to discover our portal.



iSCSI Initiator Properties

Quick Connect

To discover and log on to a target using a basic connection, type the IP address or DNS name of the target and then click Quick Connect.

Target:

Discovered targets

Name	Status
iqn.2004-08.tw.com.qsan:u400q-000903a80:dev3	Inactive

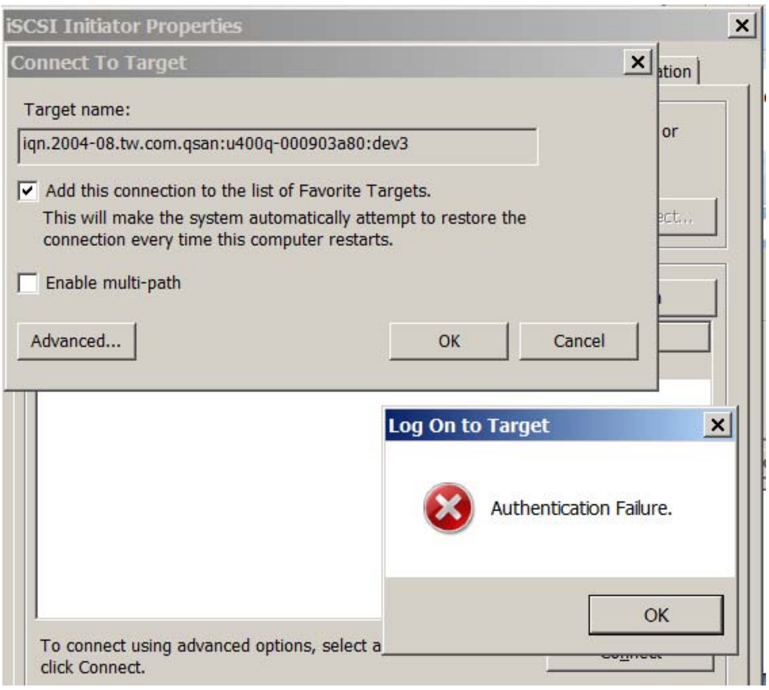
To connect using advanced options, select a target and then click Connect.

To completely disconnect a target, select the target and then click Disconnect.

For target properties, including configuration of sessions, select the target and click Properties.

For configuration of devices associated with a target, select the target and then click Devices.

6. If you click Connect without setting up the CHAP account, you will get authentication failure.



iSCSI Initiator Properties

Connect To Target

Target name:

iqn.2004-08.tw.com.qsan:u400q-000903a80:dev3

☑ Add this connection to the list of Favorite Targets.
This will make the system automatically attempt to restore the connection every time this computer restarts.

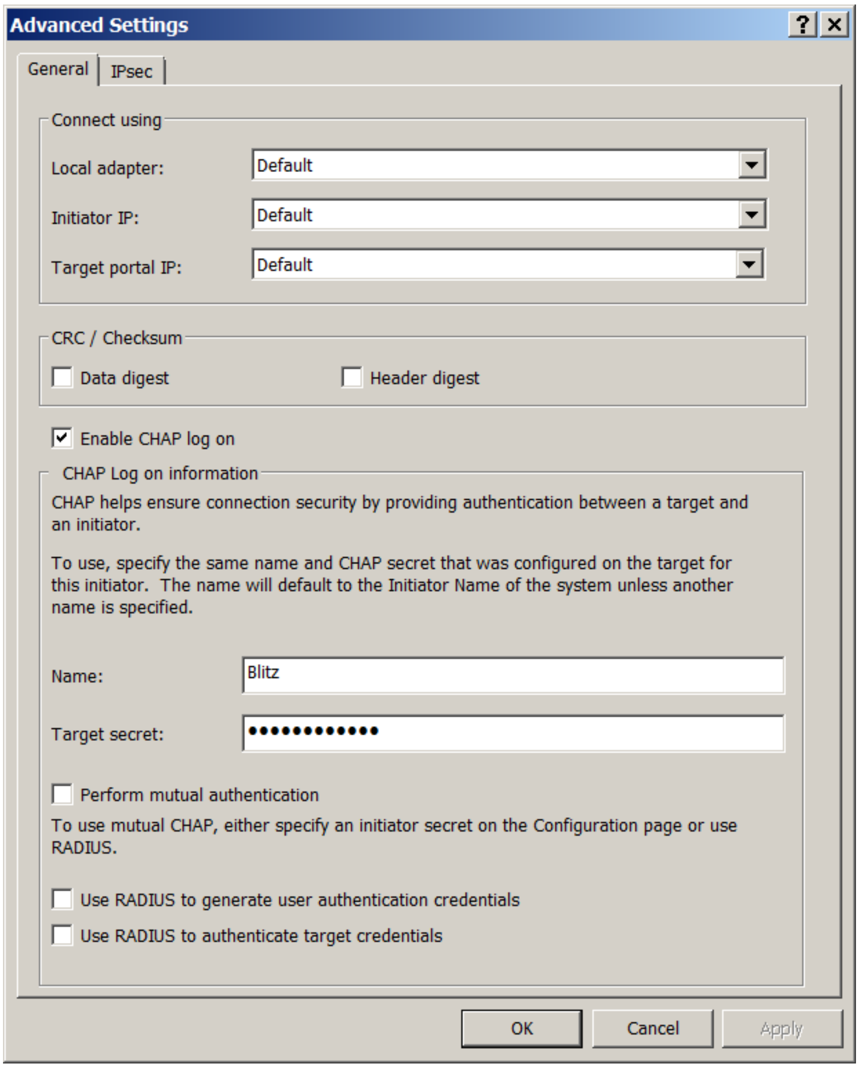
☐ Enable multi-path

Log On to Target

Authentication Failure.

To connect using advanced options, select a
click Connect.

7. Click **Advanced** button and set up CHAP account using Blitz account and password. Click **Ok**



Advanced Settings

Connect using

Local adapter: Default

Initiator IP: Default

Target portal IP: Default

CRC / Checksum

☐ Data digest ☐ Header digest

☑ Enable CHAP log on

CHAP Log on information

CHAP helps ensure connection security by providing authentication between a target and an initiator.

To use, specify the same name and CHAP secret that was configured on the target for this initiator. The name will default to the Initiator Name of the system unless another name is specified.

Name: Blitz

Target secret: ••••••••••••

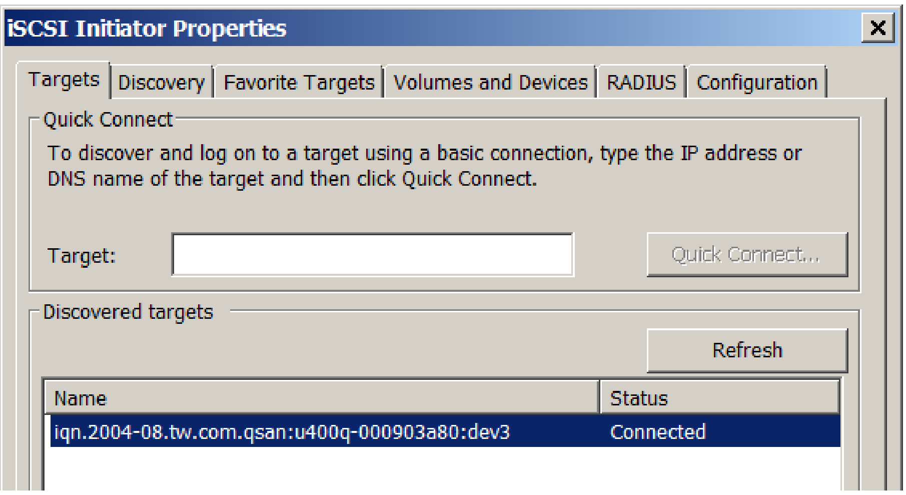
☐ Perform mutual authentication

To use mutual CHAP, either specify an initiator secret on the Configuration page or use RADIUS.

☐ Use RADIUS to generate user authentication credentials

☐ Use RADIUS to authenticate target credentials

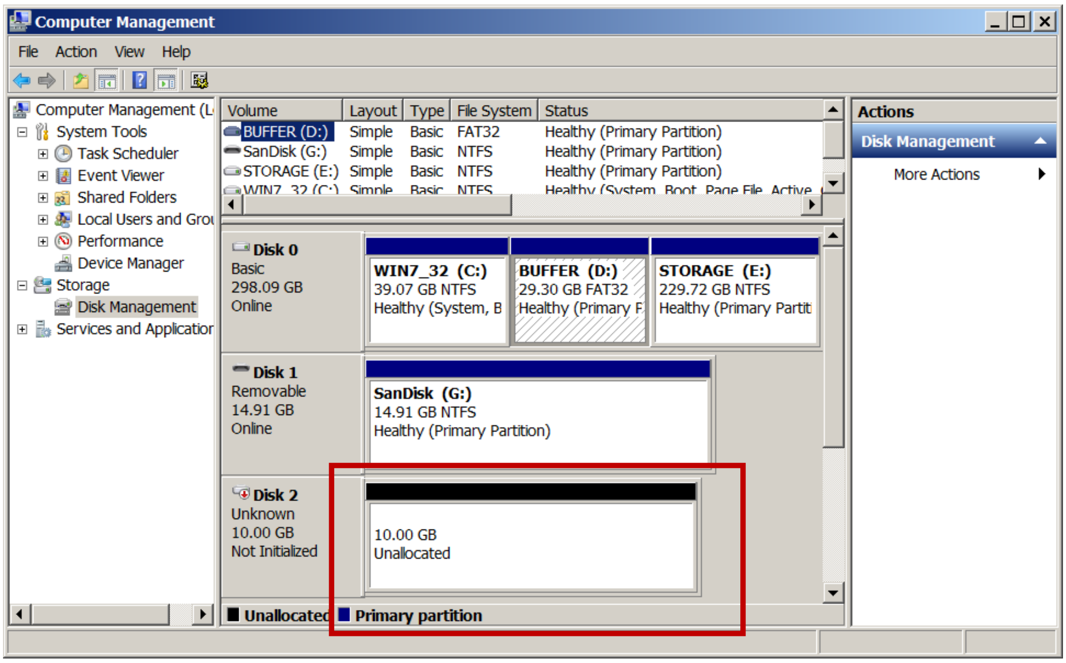
8. You will see the iSCSI connection is set up and a new drive with size 10GB is available.



To discover and log on to a target using a basic connection, type the IP address or DNS name of the target and then click Quick Connect.

Target:

Name	Status
iqn.2004-08.tw.com.qsan:u400q-000903a80:dev3	Connected



Volume	Layout	Type	File System	Status
BUFFER (D:)	Simple	Basic	FAT32	Healthy (Primary Partition)
SanDisk (G:)	Simple	Basic	NTFS	Healthy (Primary Partition)
STORAGE (E:)	Simple	Basic	NTFS	Healthy (Primary Partition)
WIN7_32 (C:)	Simple	Basic	NTFS	Healthy (System, Boot, Page File, Active,

Disk 0
Basic
298.09 GB
Online

WIN7_32 (C:)
39.07 GB NTFS
Healthy (System, B

BUFFER (D:)
29.30 GB FAT32
Healthy (Primary F

STORAGE (E:)
229.72 GB NTFS
Healthy (Primary Partit

Disk 1
Removable
14.91 GB
Online

SanDisk (G:)
14.91 GB NTFS
Healthy (Primary Partition)

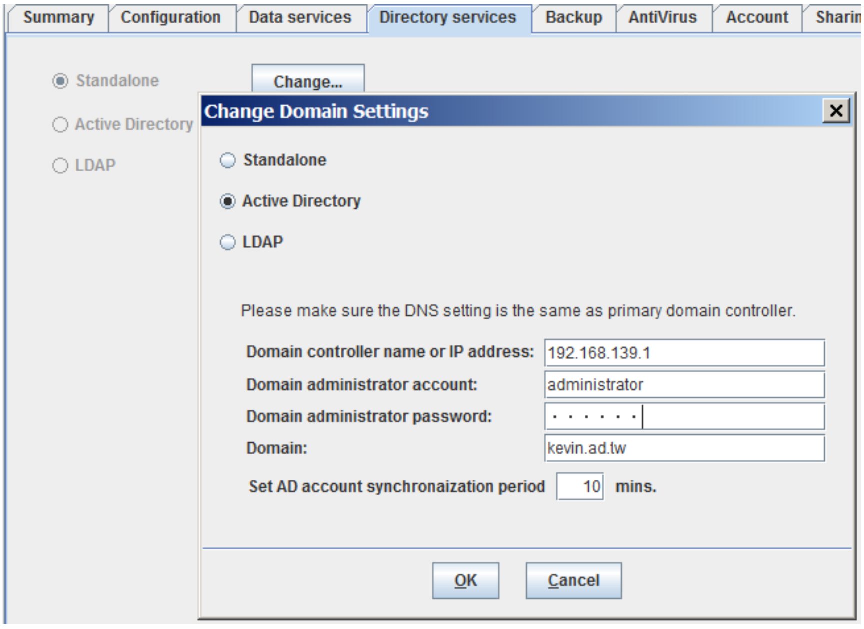
Disk 2
Unknown
10.00 GB
Not Initialized

10.00 GB
Unallocated

■ Unallocated ■ Primary partition

MS Active Directory with different data services

Let’s select MS AD as directory service and join AD domain with the following information.



○ Standalone

● Active Directory

○ LDAP

Please make sure the DNS setting is the same as primary domain controller.

Domain controller name or IP address: 192.168.139.1

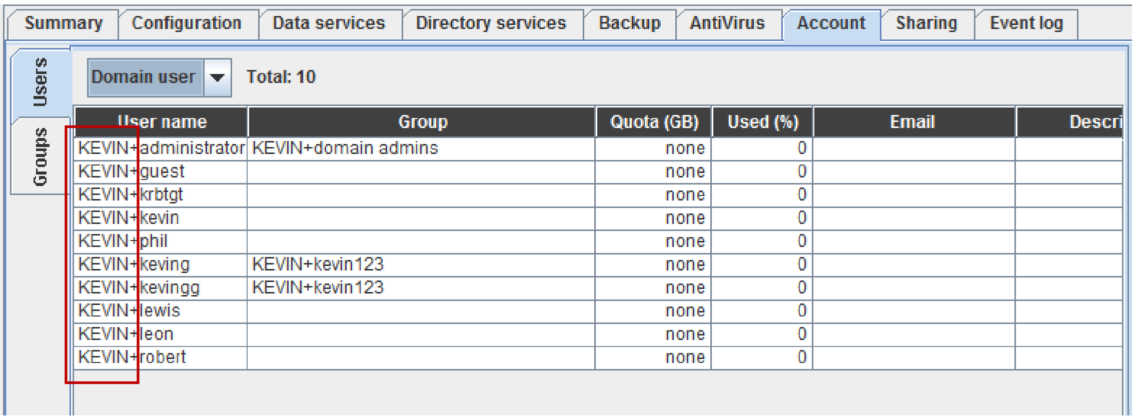
Domain administrator account: administrator

Domain administrator password: · · · · · ·

Domain: kevin.ad.tw

Set AD account synchronaization period 10 mins.

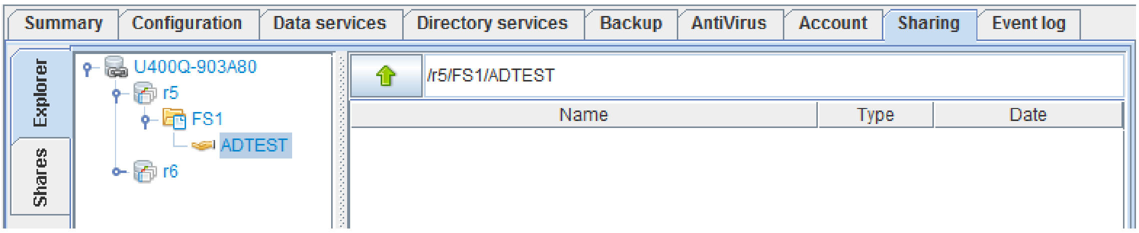
Please make sure the primary DNS setting is the same as the DNS setting on the AD server. After joining AD domain, you will see domain account information as below.

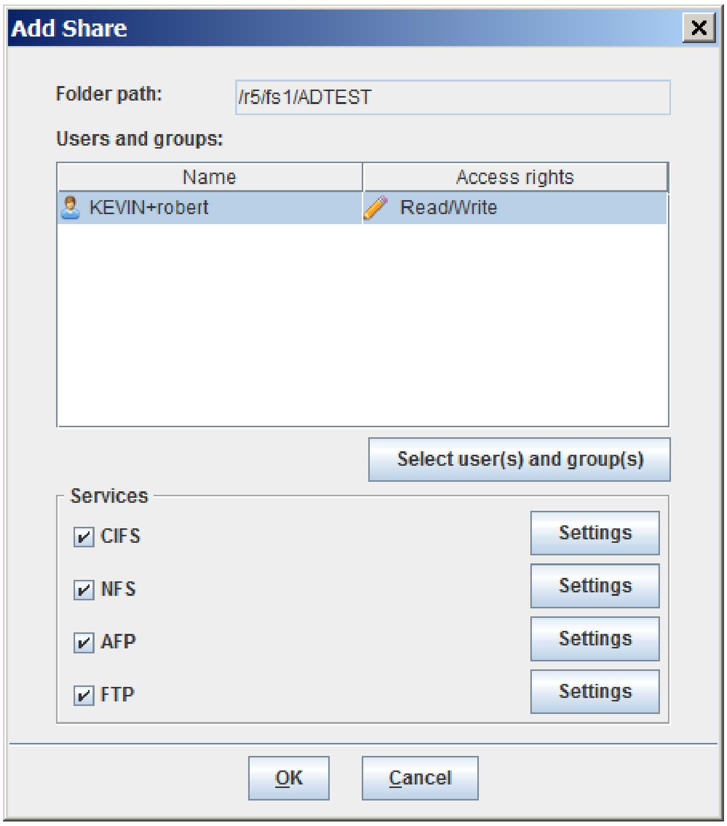


Domain user Total: 10

User name	Group	Quota (GB)	Used (%)	Email	Descri
KEVIN+administrator	KEVIN+domain admins	none	0		
KEVIN+guest		none	0		
KEVIN+krbtgt		none	0		
KEVIN+kevin		none	0		
KEVIN+phil		none	0		
KEVIN+keving	KEVIN+kevin123	none	0		
KEVIN+kevingg	KEVIN+kevin123	none	0		
KEVIN+lewis		none	0		
KEVIN+leon		none	0		
KEVIN+robert		none	0		

We will use domain account “robert" for demonstration in the following sections. A folder named “ADTEST” is created and shared out for all data services as shown below.





Add Share

Folder path: /r5/fs1/ADTEST

Users and groups:

Name	Access rights
KEVIN+robert	Read/Write

Services

☑ CIFS

☑ NFS

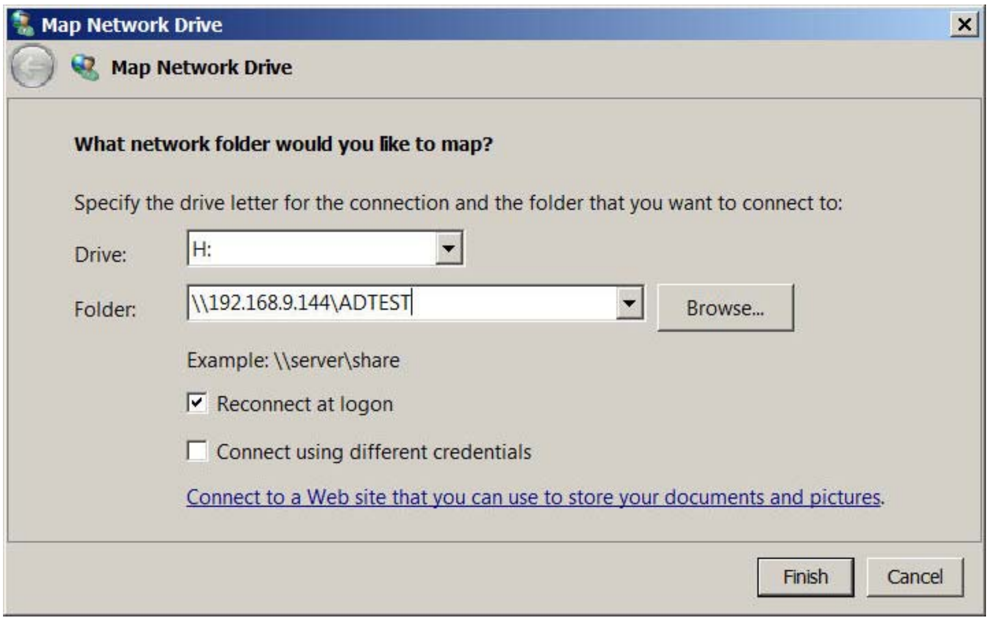
☑ AFP

☑ FTP

Suppose the network port IP is 192.168.9.144. You will see that the same account (kevin\robert) will be used to access all data services (CIFS, FTP, AFP, webDAV, iSCSI). We will introduce CIFS, FTP,and iSCSI for your reference.

Active Directory with CIFS/Samba

In Win7, let's try to set up a network drive with letter – H. In **Explorer**, go to **Tools -> Map network drive**.



Map Network Drive

What network folder would you like to map?

Specify the drive letter for the connection and the folder that you want to connect to:

Drive: H:

Folder: \\192.168.9.144\ADTEST

Example: \\server\share

☑ Reconnect at logon

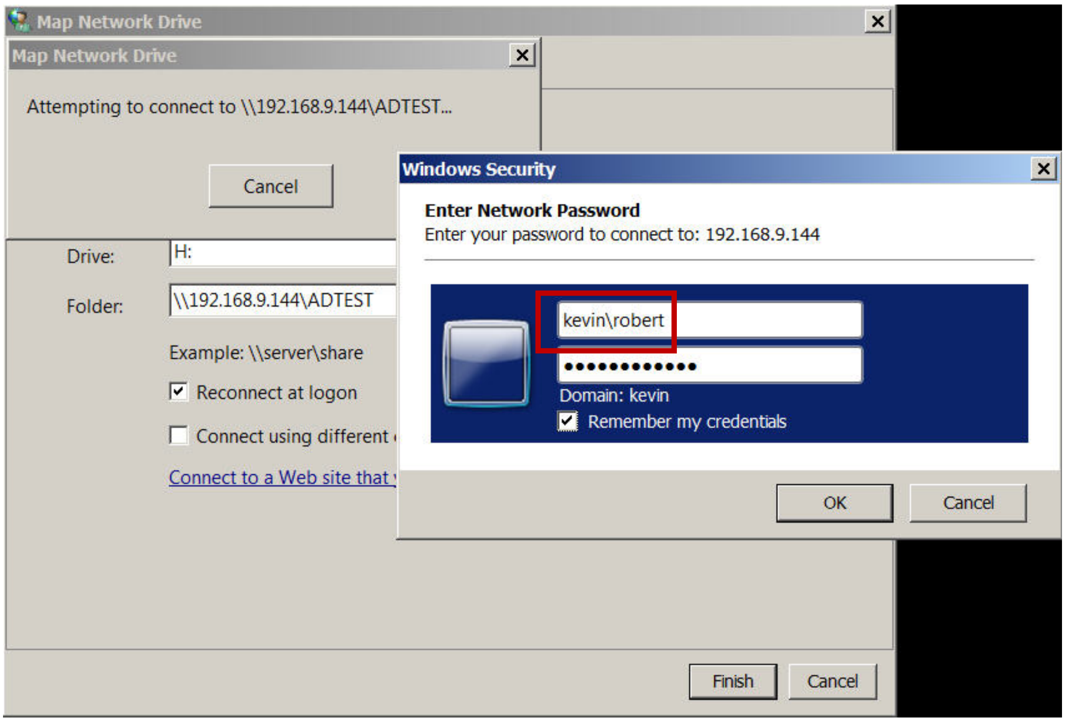
☐ Connect using different credentials

Connect to a Web site that you can use to store your documents and pictures.

Please put in the AD account and password following the Windows domain account syntax.

<domain name>\<account>

http://msdn.microsoft.com/en-us/library/windows/desktop/ms675915(v=vs.85).aspx



Attempting to connect to \\192.168.9.144\ADTEST...

Drive: H:

Folder: \\192.168.9.144\ADTEST

Example: \\server\share

☑ Reconnect at logon

□ Connect using different

Connect to a Web site that

Enter Network Password

Enter your password to connect to: 192.168.9.144

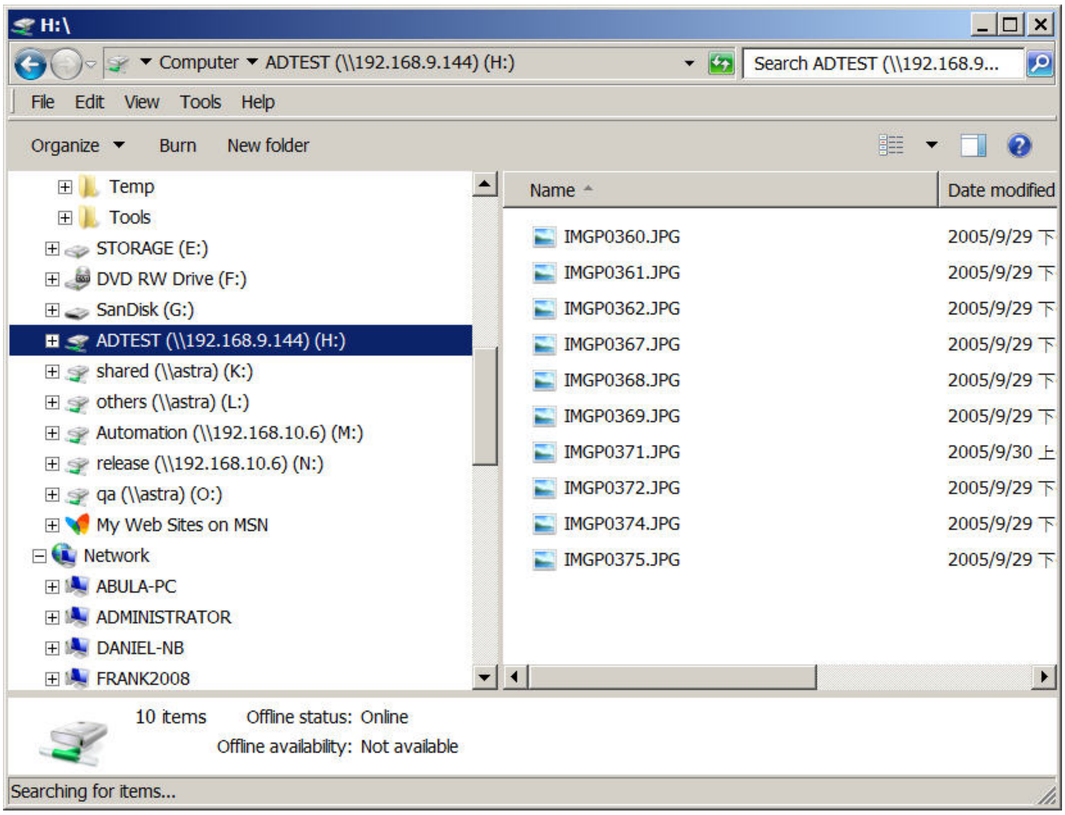
kevin\robert

••••••••••••

Domain: kevin

☑ Remember my credentials

Now you have a network drive –H ready for use. Let’s copy some photo files for identification purpose.



Name	Date modified
IMGP0360.JPG	2005/9/29 下
IMGP0361.JPG	2005/9/29 下
IMGP0362.JPG	2005/9/29 下
IMGP0367.JPG	2005/9/29 下
IMGP0368.JPG	2005/9/29 下
IMGP0369.JPG	2005/9/29 下
IMGP0371.JPG	2005/9/30 上
IMGP0372.JPG	2005/9/29 下
IMGP0374.JPG	2005/9/29 下
IMGP0375.JPG	2005/9/29 下

10 items   Offline status: Online

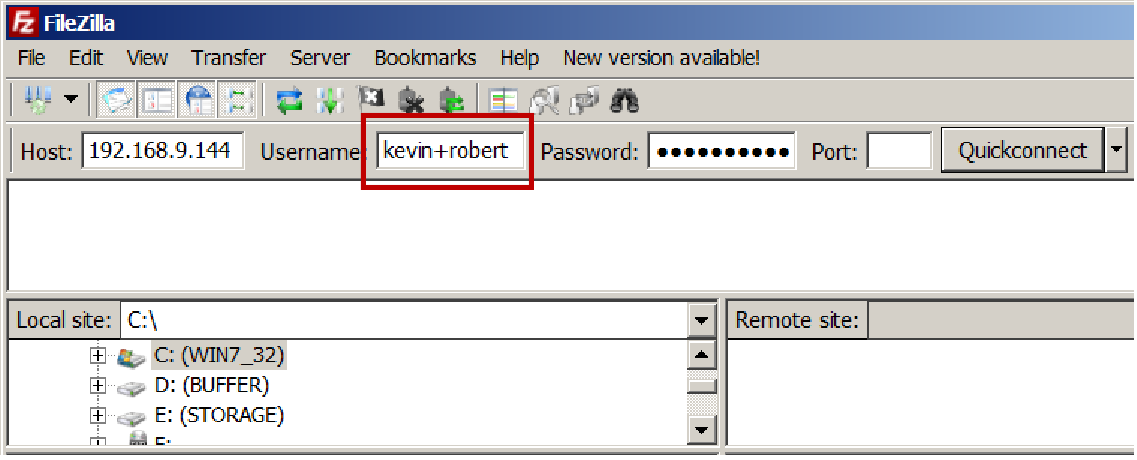
Offline availability: Not available

Searching for items...

Active Directory with FTP

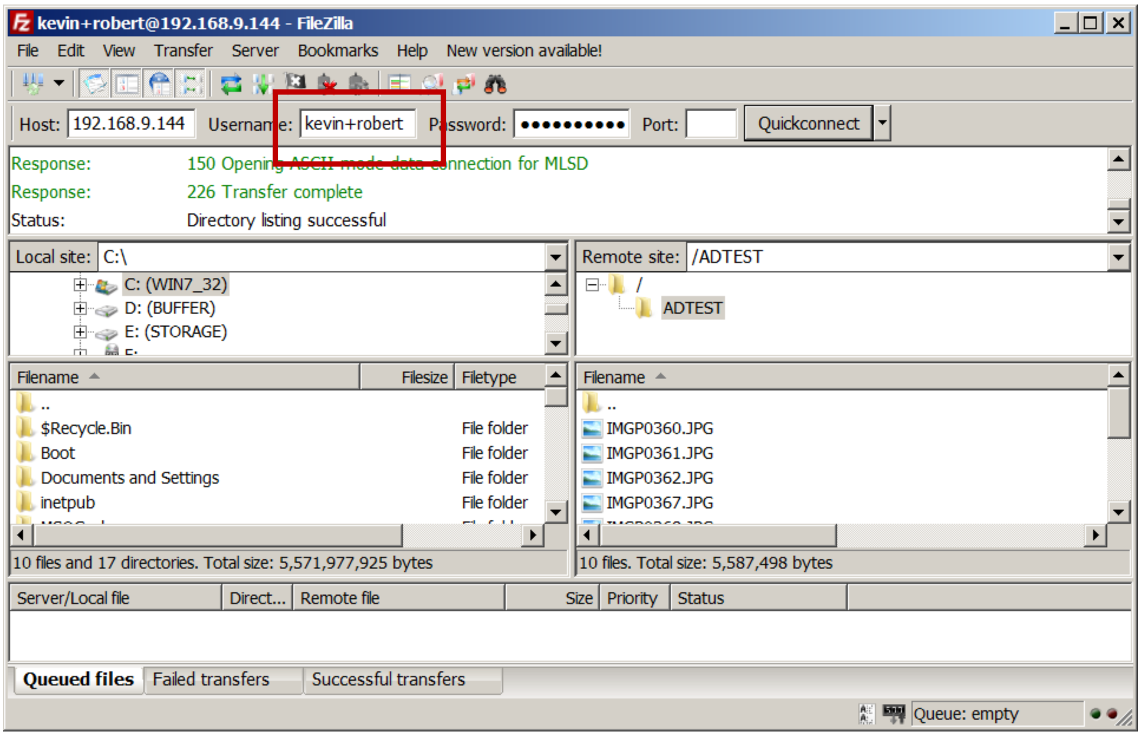
In win7, use FileZilla to connect to the shared folder - ADTEST. Use the same domain account to access data. Please be AWARE that the account syntax is changed to

<domain name>**+**<account>



Host: 192.168.9.144 Username: kevin+robert Password: ●●●●●●●●●● Port:

Click Quickconnect button. And you may access the files through FTP using the same domain account (kevin\robert).



kevin+robert@192.168.9.144 - FileZilla

Host: 192.168.9.144 Username: kevin+robert Password: ●●●●●●●●●● Port:

```
Response:    150 Opening ASCII mode data connection for MLSD
Response:    226 Transfer complete
Status:      Directory listing successful
```

Local site: C:\

Remote site: /ADTEST

Filename	Filesize	Filetype
..		
$Recycle.Bin		File folder
Boot		File folder
Documents and Settings		File folder
inetpub		File folder

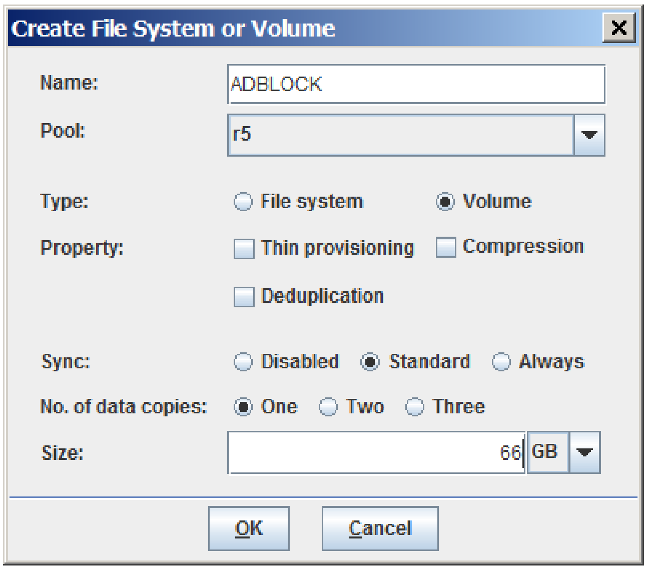
10 files and 17 directories. Total size: 5,571,977,925 bytes

Filename
..
IMGP0360.JPG
IMGP0361.JPG
IMGP0362.JPG
IMGP0367.JPG

10 files. Total size: 5,587,498 bytes

Active Directory with iSCSI CHAP authentication

1. Let’s create an iSCSI volume – ADBLOCK and set up the CHAP authentication using domain account (kevin\robert). First, create a 66GB volume.



Create File System or Volume

Name: ADBLOCK

Pool: r5

Type: ○ File system ● Volume

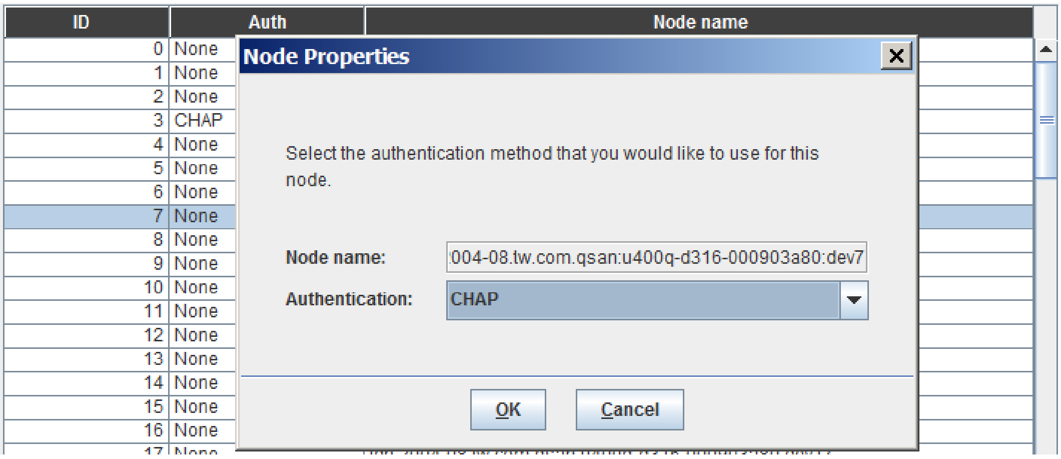
Property: □ Thin provisioning □ Compression □ Deduplication

Sync: ○ Disabled ● Standard ○ Always

No. of data copies: ● One ○ Two ○ Three

Size: 66 GB

2. Go to **Data services** -> **iSCSI** tab. Pick up a node ID (Let’s use 7) and right click to select **Properties**. Select **CHAP** to enable CHAP account function.



ID	Auth	Node name
0	None	
1	None	
2	None	
3	CHAP	
4	None	
5	None	
6	None	
7	None	
8	None	
9	None	
10	None	
11	None	
12	None	
13	None	
14	None	
15	None	
16	None	

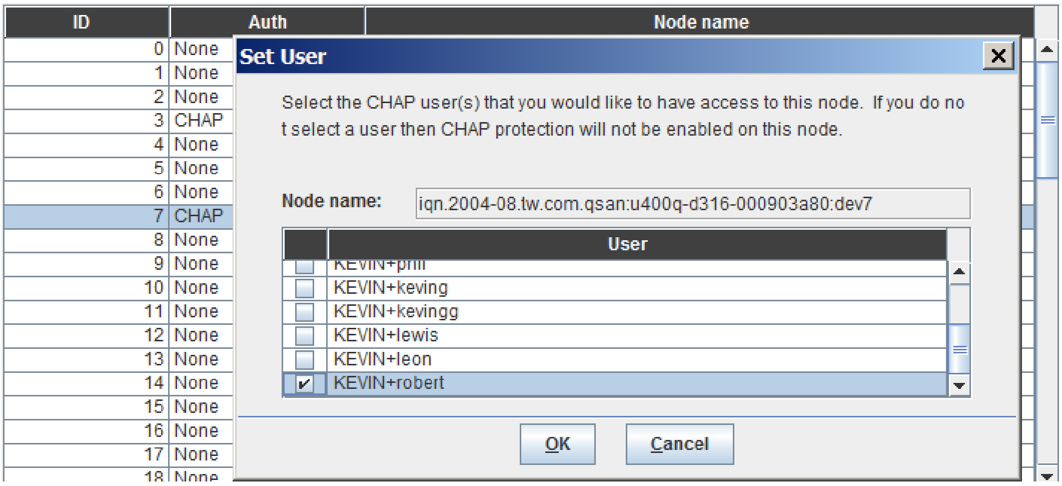
Node Properties

Select the authentication method that you would like to use for this node.

Node name: 004-08.tw.com.qsan:u400q-d316-000903a80:dev7

Authentication: CHAP

3. Right click and select **Set user**. Select the domain account (kevin\robert).



ID	Auth	Node name
0	None	
1	None	
2	None	
3	CHAP	
4	None	
5	None	
6	None	
7	CHAP	
8	None	
9	None	
10	None	
11	None	
12	None	
13	None	
14	None	
15	None	
16	None	
17	None	
18	None	

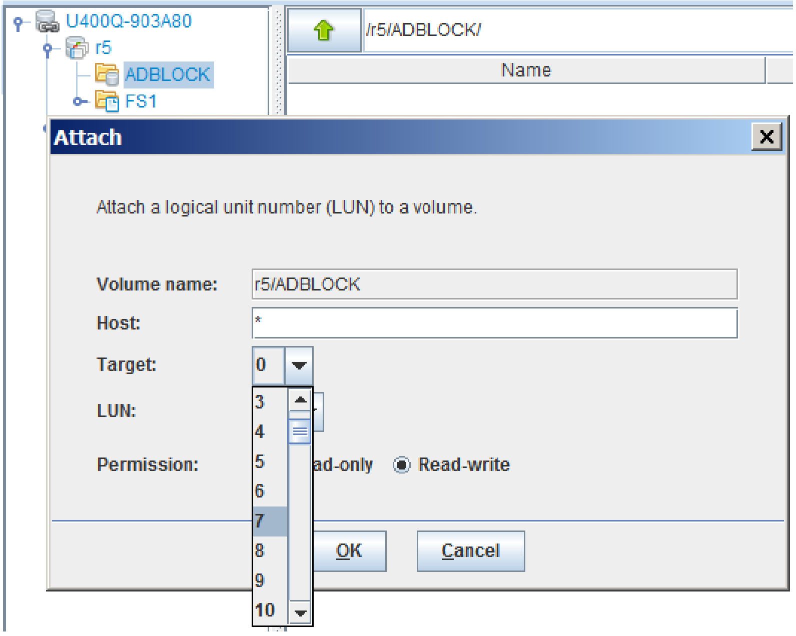
Set User

Select the CHAP user(s) that you would like to have access to this node. If you do no t select a user then CHAP protection will not be enabled on this node.

Node name: iqn.2004-08.tw.com.qsan:u400q-d316-000903a80:dev7

	User
□	KEVIN+phil
□	KEVIN+keving
□	KEVIN+kevingg
□	KEVIN+lewis
□	KEVIN+leon
☑	KEVIN+robert

4. Go to **Sharing** tab. Right click on the ADBLOCK volume we just created in step 1. And select the target node as 7 and attach LUN.



Attach

Attach a logical unit number (LUN) to a volume.

Volume name: r5/ADBLOCK

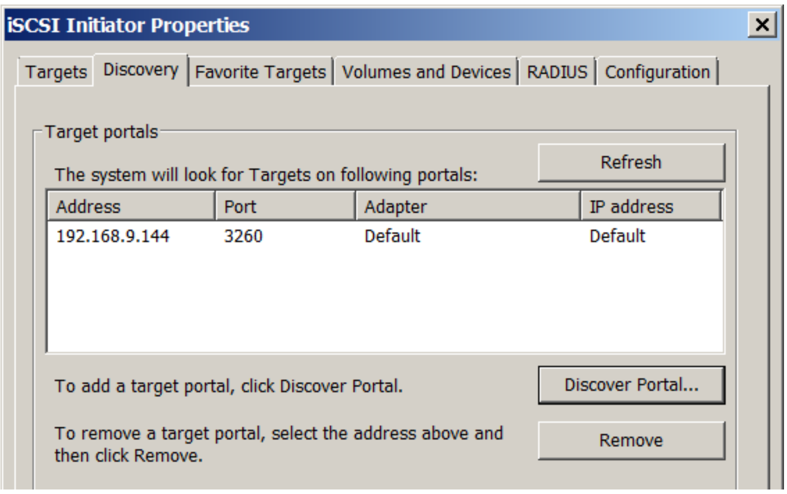
Host: *

Target: 0

LUN:

Permission: ○ ad-only ● Read-write

5. In Win7, launch iSCSI initiator and put in the network IP(192.168.9.144) to discover our portal.



iSCSI Initiator Properties

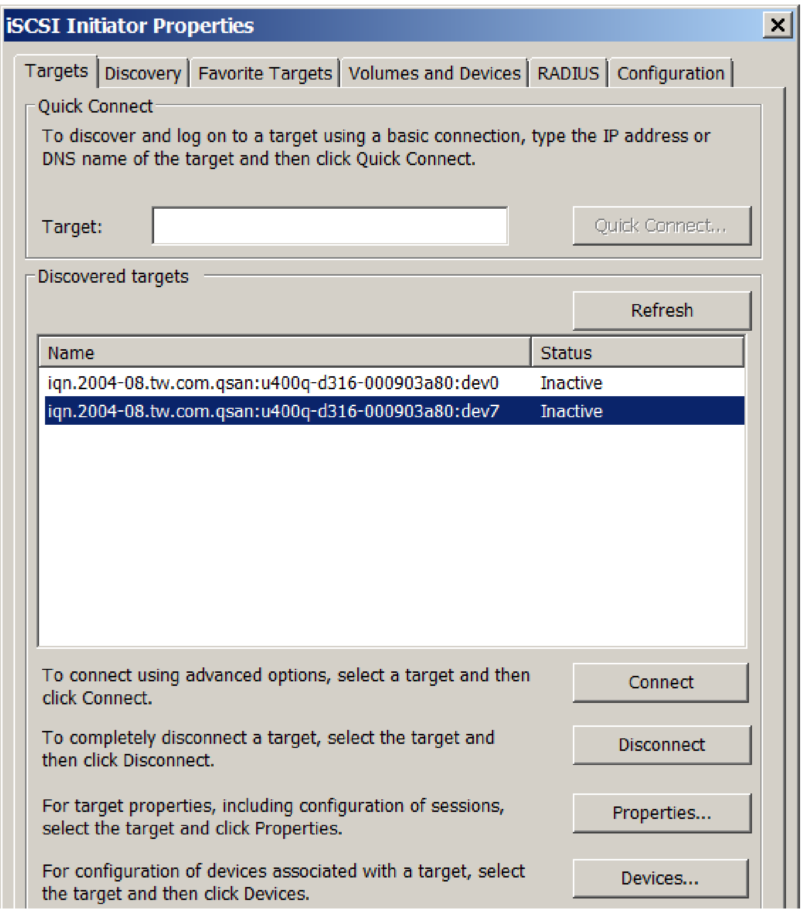
Target portals

The system will look for Targets on following portals:

Address	Port	Adapter	IP address
192.168.9.144	3260	Default	Default

To add a target portal, click Discover Portal.

To remove a target portal, select the address above and then click Remove.



iSCSI Initiator Properties

Targets | Discovery | Favorite Targets | Volumes and Devices | RADIUS | Configuration

Quick Connect

To discover and log on to a target using a basic connection, type the IP address or DNS name of the target and then click Quick Connect.

Target:

Quick Connect...

Discovered targets

Refresh

Name	Status
iqn.2004-08.tw.com.qsan:u400q-d316-000903a80:dev0	Inactive
iqn.2004-08.tw.com.qsan:u400q-d316-000903a80:dev7	Inactive

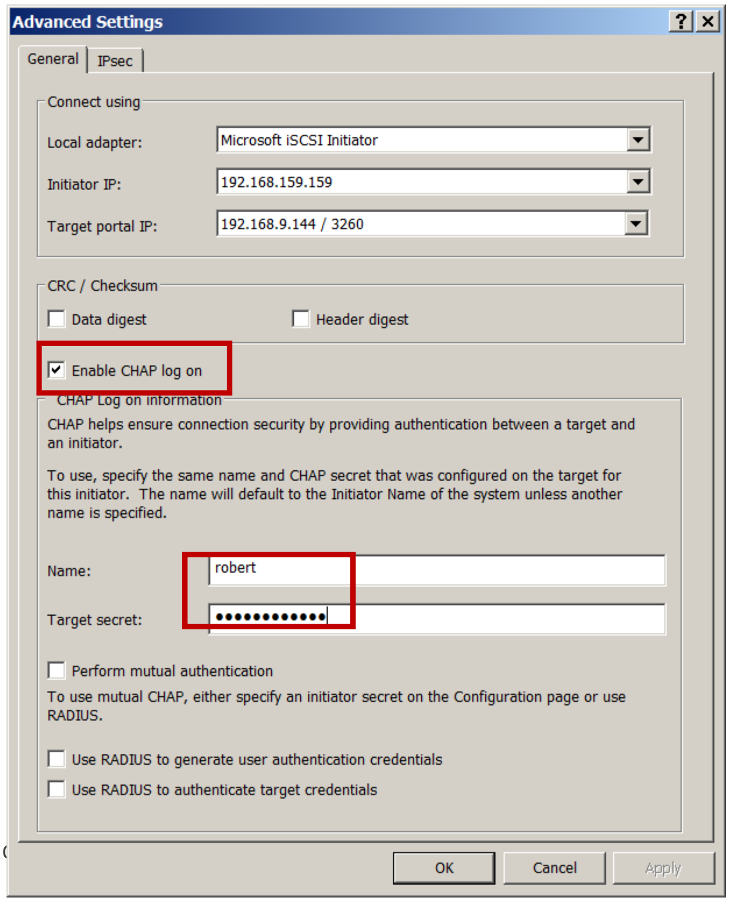
To connect using advanced options, select a target and then click Connect. — Connect

To completely disconnect a target, select the target and then click Disconnect. — Disconnect

For target properties, including configuration of sessions, select the target and click Properties. — Properties...

For configuration of devices associated with a target, select the target and then click Devices. — Devices...

6. Select the proper target (dev7 from step 4) and click **Connect**. And click **Advanced** to set up CHAP account as below.



Advanced Settings

General | IPsec

Connect using

Local adapter: Microsoft iSCSI Initiator

Initiator IP: 192.168.159.159

Target portal IP: 192.168.9.144 / 3260

CRC / Checksum

□ Data digest □ Header digest

☑ Enable CHAP log on

CHAP Log on information

CHAP helps ensure connection security by providing authentication between a target and an initiator.

To use, specify the same name and CHAP secret that was configured on the target for this initiator. The name will default to the Initiator Name of the system unless another name is specified.

Name: robert

Target secret: ••••••••••••

□ Perform mutual authentication

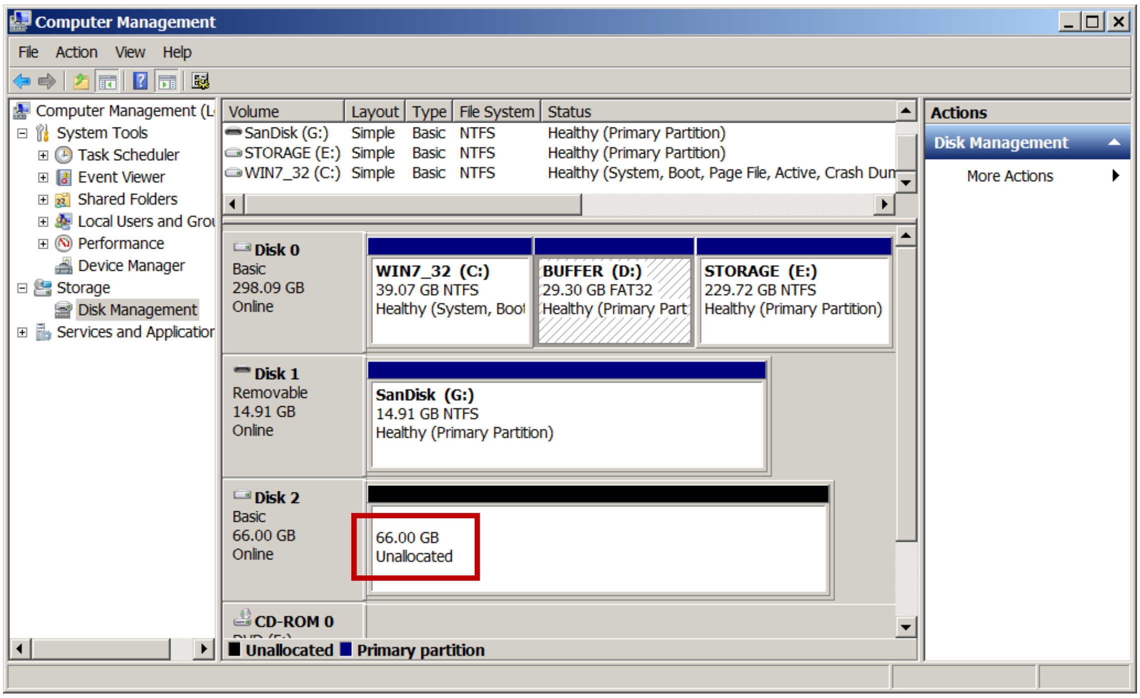
To use mutual CHAP, either specify an initiator secret on the Configuration page or use RADIUS.

□ Use RADIUS to generate user authentication credentials

□ Use RADIUS to authenticate target credentials

OK | Cancel | Apply

7. Click **Ok** to complete the connection. A new drive with size of 66GB is ready for use.



Volume	Layout	Type	File System	Status
SanDisk (G:)	Simple	Basic	NTFS	Healthy (Primary Partition)
STORAGE (E:)	Simple	Basic	NTFS	Healthy (Primary Partition)
WIN7_32 (C:)	Simple	Basic	NTFS	Healthy (System, Boot, Page File, Active, Crash Dum

Disk	Partitions		
Disk 0 Basic 298.09 GB Online	**WIN7_32 (C:)** 39.07 GB NTFS Healthy (System, Boot	**BUFFER (D:)** 29.30 GB FAT32 Healthy (Primary Part	**STORAGE (E:)** 229.72 GB NTFS Healthy (Primary Partition)
Disk 1 Removable 14.91 GB Online	**SanDisk (G:)** 14.91 GB NTFS Healthy (Primary Partition)		
Disk 2 Basic 66.00 GB Online	66.00 GB Unallocated		
CD-ROM 0			

TIP: Please be aware of the following things.

- The client machine running Windows iSCSI initiator doesn't need to join the AD domain. Or the user doesn't have to use domain account to login the client machine. Qsan UnifiedAUTH truly gives users the upmost flexibility.

- In CHAP account input, only account name and password are needed. No special syntax is required.

- CHAP mechanism password is required to be at least 12 to 16 characters. If the domain account password doesn't meet this requirement, you need to change the password on the AD server or LDAP server, which depends on what service you are using.

LDAP with different data services

The process of using LDAP service with different data services is pretty similar to that of Standalone service, which we just introduced in the previous section.

Let's select LDAP service and login LDAP server. We use the following data to login the LDAP server. Please ask your IT managers for the detail information about base DN, admin DN, user base DN, and group base DN.

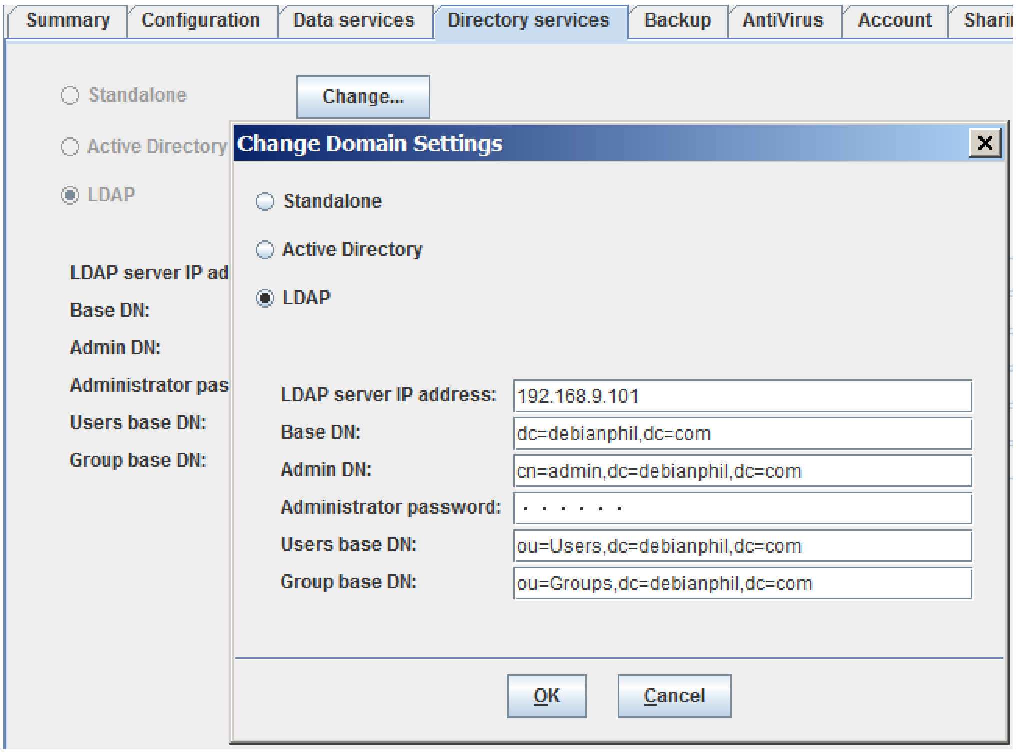
LDAP server IP address : 192.168.9.101

Base DN : dc=debianphil,dc=com

Admin DN : cn=admin, dc=debianphil,dc=com

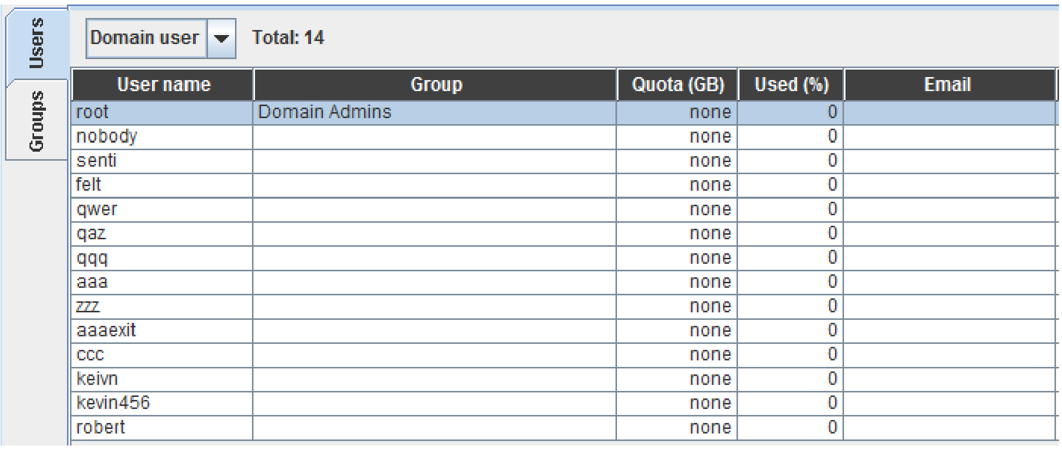
User base DN : ou=Users, dc=debianphil,dc=com

Group base DN : ou=Groups, dc=debianphil,dc=com



LDAP server IP address: 192.168.9.101
Base DN: dc=debianphil,dc=com
Admin DN: cn=admin,dc=debianphil,dc=com
Administrator password: ••••••
Users base DN: ou=Users,dc=debianphil,dc=com
Group base DN: ou=Groups,dc=debianphil,dc=com

In Account tab, domain user and domain group will look like below. You may notice that there is no domain name in here in the fashion of <domain name>+<user name>.

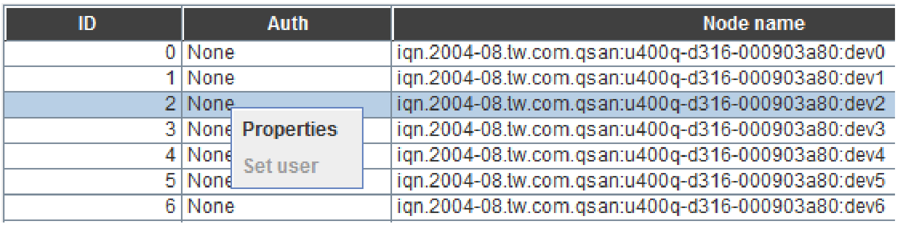


Total: 14

User name	Group	Quota (GB)	Used (%)	Email
root	Domain Admins	none	0	
nobody		none	0	
senti		none	0	
felt		none	0	
qwer		none	0	
qaz		none	0	
qqq		none	0	
aaa		none	0	
zzz		none	0	
aaaexit		none	0	
ccc		none	0	
keivn		none	0	
kevin456		none	0	
robert		none	0	

You can simply use it the same way as you do with Standalone mode.

Please be aware that with LDAP service, it does not support iSCSI CHAP function. After login LDAP server, the CHAP function will be grey out.



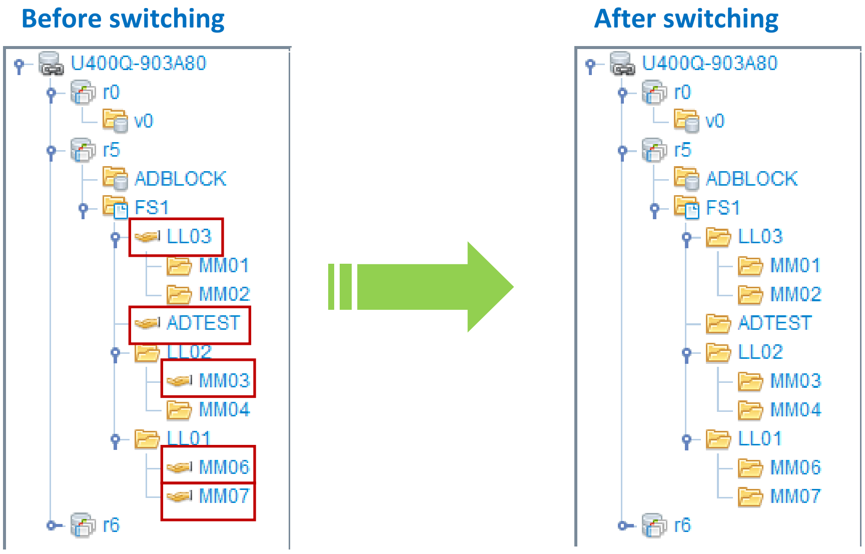
ID	Auth	Node name
0	None	iqn.2004-08.tw.com.qsan:u400q-d316-000903a80:dev0
1	None	iqn.2004-08.tw.com.qsan:u400q-d316-000903a80:dev1
2	None	iqn.2004-08.tw.com.qsan:u400q-d316-000903a80:dev2
3	None	iqn.2004-08.tw.com.qsan:u400q-d316-000903a80:dev3
4	None	iqn.2004-08.tw.com.qsan:u400q-d316-000903a80:dev4
5	None	iqn.2004-08.tw.com.qsan:u400q-d316-000903a80:dev5
6	None	iqn.2004-08.tw.com.qsan:u400q-d316-000903a80:dev6

CAUTION LDAP service doesn’t integrate with iSCSI CHAP authentication. You will not be able to use iSCSI CHAP function after Qsan unified storage logs in LDAP server and uses LDAP service.

Switching to a different directory service

Directory service can be changed for flexibility. If you want to change from one directory service to another, some consequent actions will be taken by the system and please prepare for these.

- If you switch to either MS AD or LDAP, functions (such as **Create**, **Edit**, **Delete**) applied to local users and groups will be disabled.
- If you switch back to Standalone mode, functions (such as **Create**, **Edit**, **Delete**) applied to local users and groups will be enabled again (if home directory is properly configured).
- **Access control settings** for all shares will be deleted. You need to re-create access control from scratch manually.


Before switching
U400Q-903A80
r0
v0
r5
ADBLOCK
FS1
LL03
MM01
MM02
ADTEST
LL02
MM03
MM04
LL01
MM06
MM07
r6
After switching
U400Q-903A80
r0
v0
r5
ADBLOCK
FS1
LL03
MM01
MM02
ADTEST
LL02
MM03
MM04
LL01
MM06
MM07
r6