JetStor SAS 716U / 724U Windows ACL Configurations

Feature Introduction

Nowadays on almost every single NAS unit available on the market, share permission control (ACL) is one of the basic elements for providing data services to user clients. However for scenarios where a more complicated ACL is required, usually Windows based environment, Linux based NAS appliance units often fail to satisfy the crowd with native Linux ACL function.

In cases like this, leveraging Windows ACL is no doubt an enhancement solution to replace the original Linux ACL function provided on the NAS unit.

What is Windows ACL?

The Windows ACL is used for determining which users can access server resources at specific levels. The security token created from Windows Server 2008’ s security sub system, upon login authentication, contains the user’ s security identifier (SID) which represents the Active Directory groups the user belongs to.

Why do you need ACL?

The purpose of ACL is to control Group/User access for Windows Server 2008 folder resources. When a user attempts to access an NTFS Folder/File the SID token is compared to the Access Control List (ACL) to determine if the user has access to the Folder/File resource based on the user’ s group member status.

Environment Requirements

Prior to configuring the Windows ACL, a few elements are required:

1. Microsoft Windows AD environment

For JetStor NAS units, only when a Windows AD is present and both the samba client (Windows AD clients) and the samba server (JetStor NAS) are joined to the AD can the user credential used to access the data share be synchronized between them.

2. JetStor NAS unit with Windows ACL support

The Windows ACL feature is only supported after firmware version 1.3.0 and is NOT available on U110/U120 firmware. Please make sure you have the right firmware version that supports Windows ACL. Please also make sure the JetStor NAS unit is joined to the AD. *(Refer to the next chapter for instructions of how to join a JetStor NAS to an AD environment)*.

3. A client with dedicated Windows OS for configuring Windows ACL

Up to now we have identified the following OS types to be compatible with Windows ACL: Windows Server 2008, Windows 7 Pro, Windows 8/8.1 Pro, and Windows Server 2012.

Windows ACL relative settings on JetStor NAS

For using Windows ACL, firstly the JetStor NAS unit has to be joined to the Windows AD environment with the following settings:

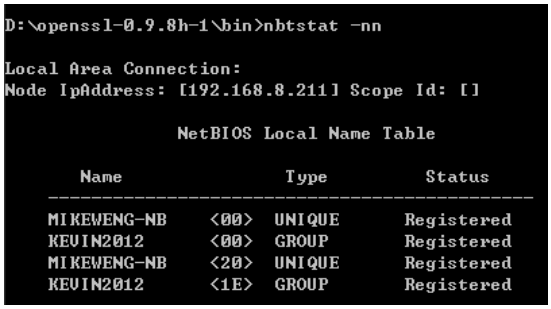
1. DNS settings:

In the JetStor NAS Web UI, browse to Network configuration-> DNS settings, and enter the IP address of the DNS server, as well as the DNS search path. (If your domain is ad.JetStor.com, enter it in the DNS search path without hostname). Make sure the DNS server belongs to the AD and is able to resolve the domain controllers' host names.

2. Directory Service settings:

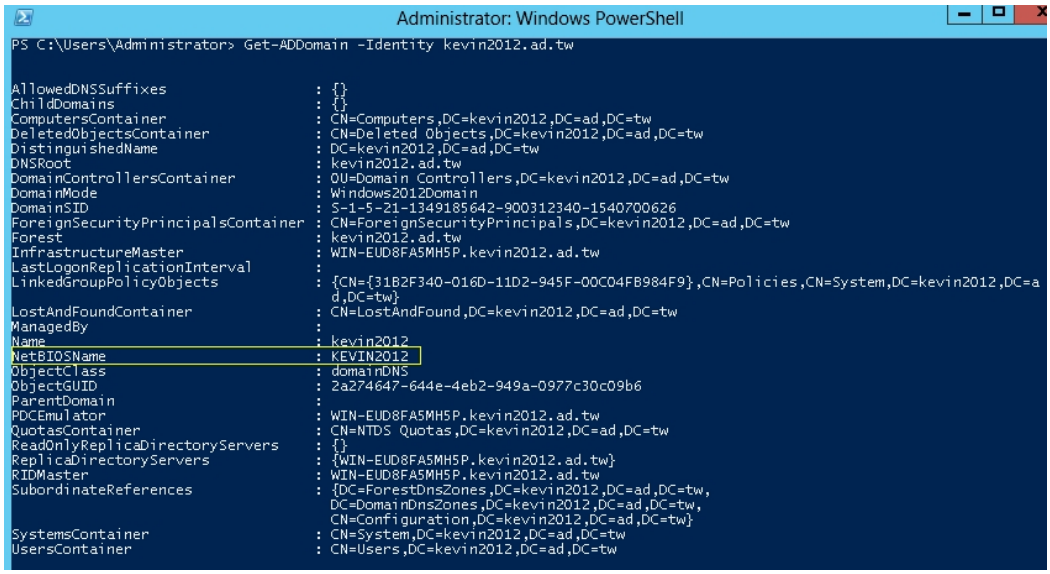
The next step is to browse to Application configuration -> directory services page and there are several settings to be configured:

a. Domain controller name or IP address: Specify the target DC, IP address preferred.
b. Domain administrator account: Enter a domain admin account name
c. Domain administrator password: Enter the domain admin account password
d. Fully qualified domain name (FQDN): Enter the full domain name, please notice this is just the domain name, do not include the host name (correct example: ad.JetStor.com, wrong example: ~~dc01~~.ad.JetStor.com)
e. NetBIOS domain name: The NetBIOS domain name usually refers to the first section of the domain' s FQDN. For example for ad.JetStor.com the NetBIOS domain name is usually ad, unless specifically modified in the AD environment configurations)
   On a windows AD client this can be verified by entering the following command:

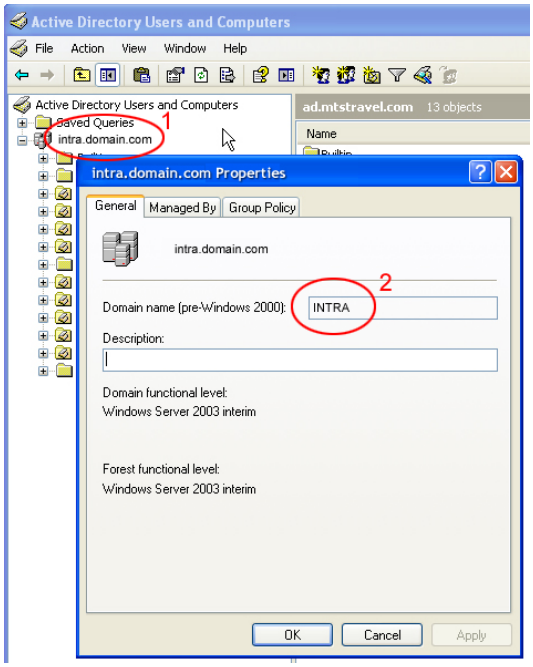


   Once the client computer is joined to AD, the 00 Group entity output from this command usually indicates the NetBIOS name of the domain.

Or on a Windows 2008/2012 DC, this can also be checked from:



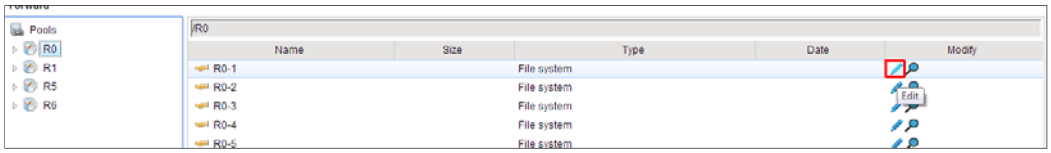
Or on a Windows 2003 DC, check this in AD Users and Computers management console:



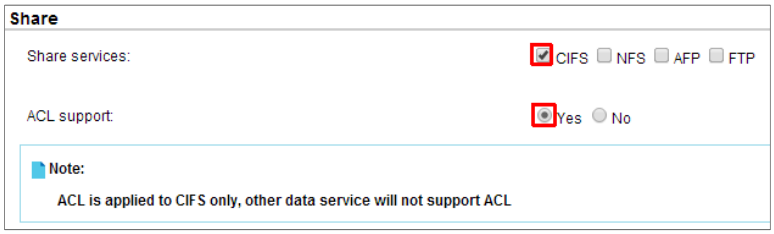
f. Set AD account sync period: This option specifies how frequently the JetStor NAS unit obtains an update of user/group account list from the DC. Ideally it can be set to 10~15 minutes.

3. Share settings:

Check to the **Storage configuration-> Share page**, and browse to the folder that contains the target share folder you wish to configure, and click on **Edit** icon of the target folder:



And then enable the Windows ACL support for the share:



Make sure the CIFS share option is enabled, and the ACL support is also checked for the share in this page.

Important: Please notice that the Windows ACL settings can only be adjusted via Windows AD client hosts and there is **NO** options to adjust the Windows ACL attributes for a share in the Web UI.

One extra settings required before an AD user account is allowed to adjust the Windows ACL is to adjust the **share permission** of the account to **Read/Write** in the share ACL list. If the account is not granted read/write permission in the share ACL settings, even if in the Windows ACL it is given read/write permission, the Windows ACL permissions will not take effect.

Configuring Windows ACL on AD clients

Configuration Example

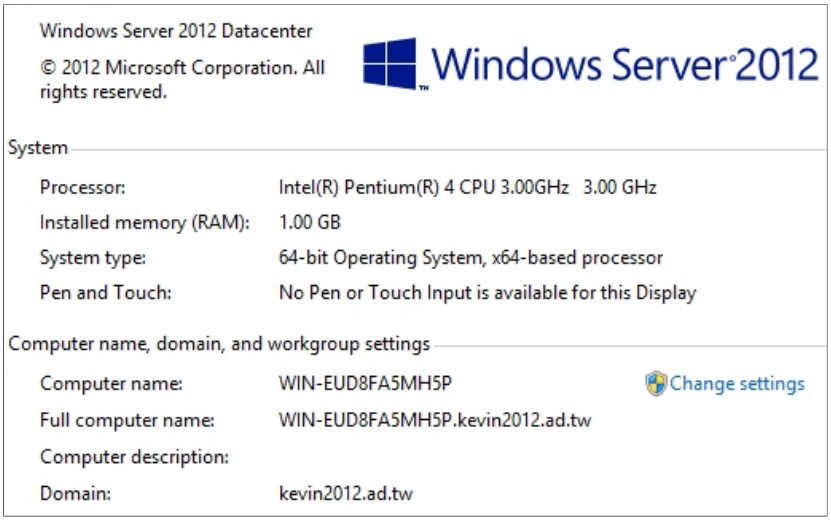
After all the previous mentioned configurations are ready, a Windows AD client is now allowed to further configure Windows ACL attributes for a folder.

In this configuration example we have prepared:

- Windows Server 2012 Active Directory domain controller
- Windows 7 Pro AD client computer
- Firmware version 1.3.0 with ACL support

AD Environment Settings:

- NetBIOS domain name: keivn2012
- Domain FQDN: kevin2012.ad.tw
- DC FQDN: WIN-EUD8FA5MH5P.kevin2012.ad.tw
- DC IP address: 192.168.139.1



With the above environment parameters, the JetStor used in this configuration example can be joined to the domain with the following configurations:

DNS setting

DNS(Domain Name Service) provides a means to translate hostname to IP address. Enter DNS IP addresses below.

- ( ) Obtain DNS server address automatically
- (•) Use the following DNS server address:

Primary DNS:	192.168.139.1
Sceondary DNS:	
DNS search path:	kevin2012.ad.tw

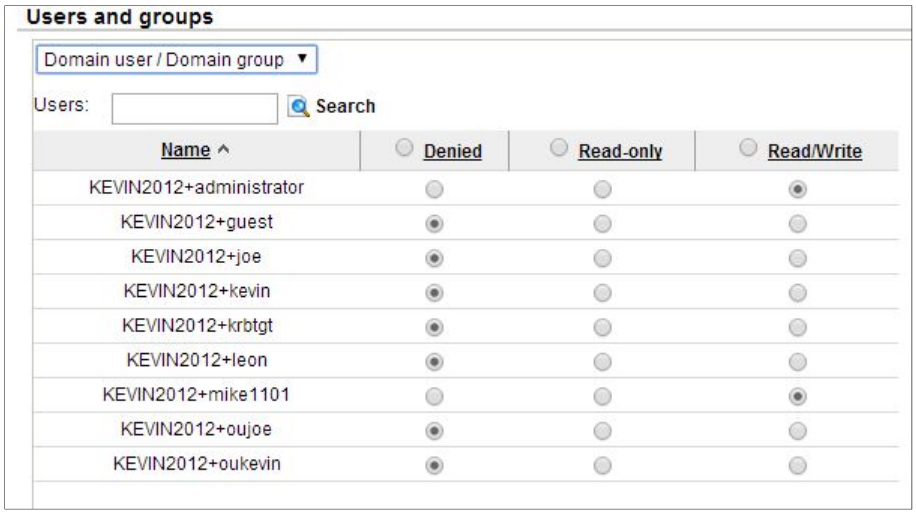
- (•) Active directory

Domain controller name or IP address:	192.168.139.1
Domain administrator account:	Administrator
Domain administrator password:	••••••••
Fully qualified domain name:	kevin2012.ad.tw
NetBIOS domain name:	kevin2012
Set AD account synchronization period:	10 minutes

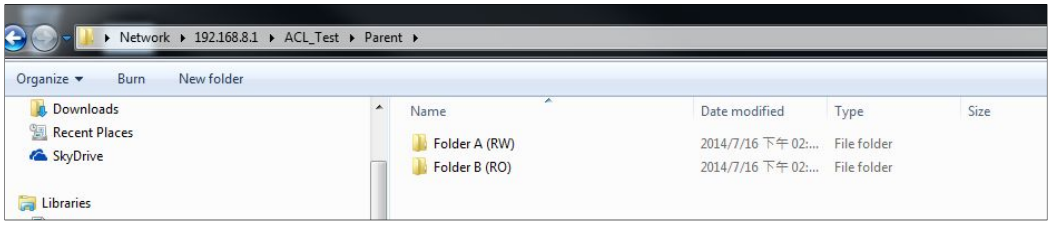
Example Steps for configuring Windows ACL

1. On the U600, create a testing file system (ACL_Test), enable the CIFS share settings and ACL support.

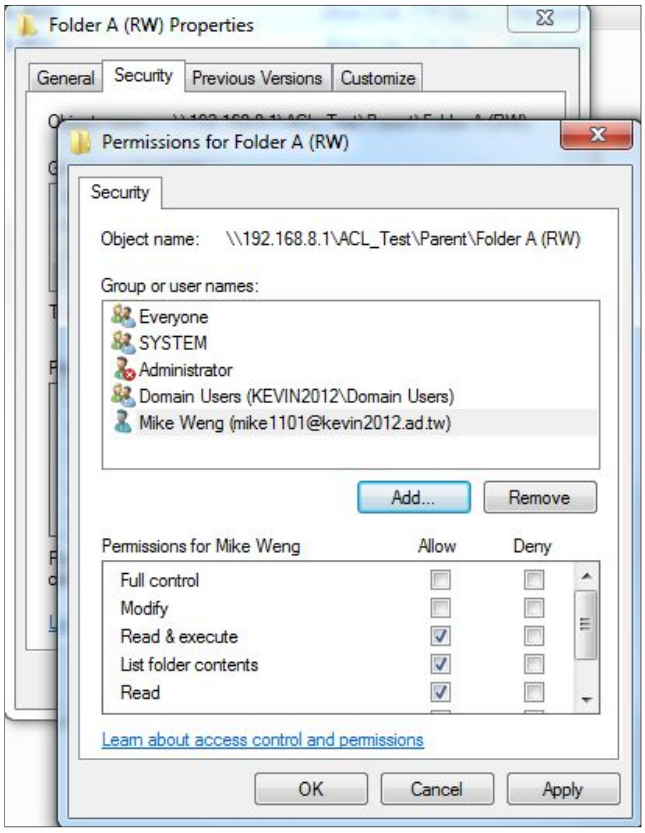
2. Configure share ACL settings, assign R/W permission to a domain admin account (kevin2012\Administrator) and a user account (kevin2012\mike1101) for testing purpose.

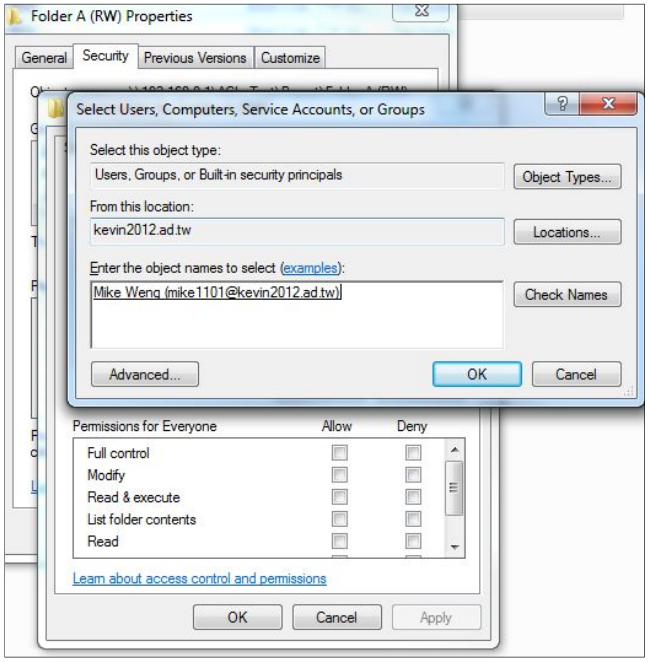


3. Access the share with administrator credential, create a upper layer folder "Parent" and two sub-layer folder "Folder A (RW)" and "Folder B (RO)"

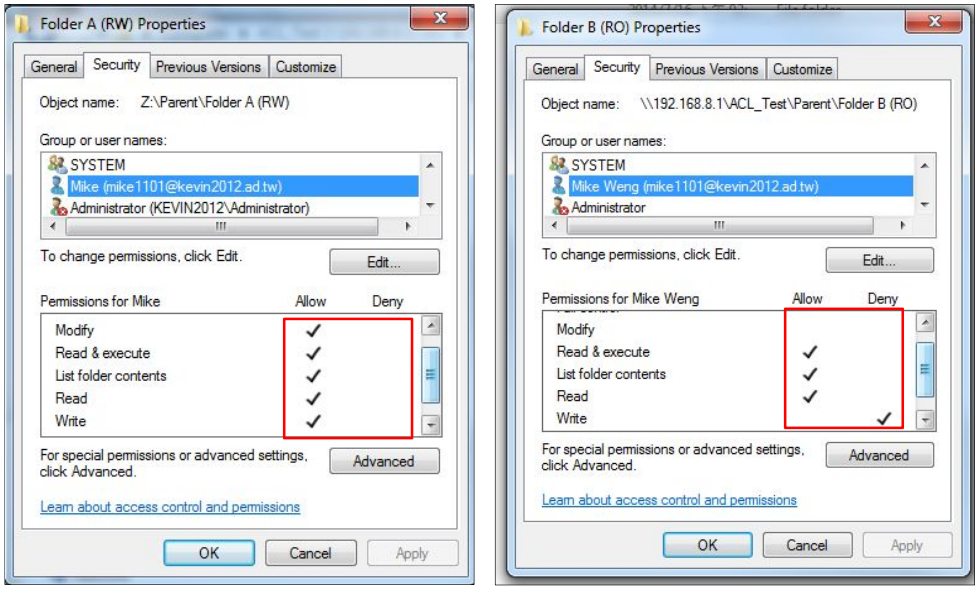


4. Right click on each of the folders, in the security tag, configure the Windows ACL permissions for testing user (kevin2012\mike1101). Click on the Edit button in the security to edit the ACL list and add the testing user account by clicking on the Add button, and search for the user account.

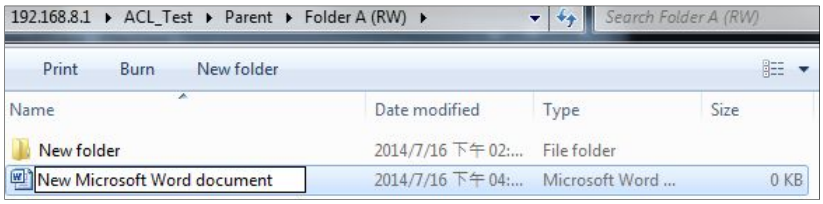




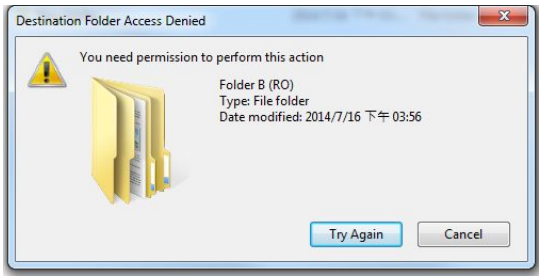
5. Verify the Windows ACL permission settings of these two folders look like this, so that the testing user account has read only permission to the folder A and read/write permission to folder B.



6. On another AD client PC, logon with the testing user (kevin2012\mike1101) credential and access to the share, check if the Windows ACL permission configured is effective
7. The testing user account is able to create/ modify/delete files in the folder A.



8. The testing user account is only able to read files in the folder B, other actions will be denied.



9.