



NAStorage
Administrator Guide
Security Policy for SMB/CIFS environment

Version 1.00
10/01/2002

Prepared by:

Eric Chen
TS Engineer
Ingrasys Technology Inc.
E-mail: support@ingrasys.com

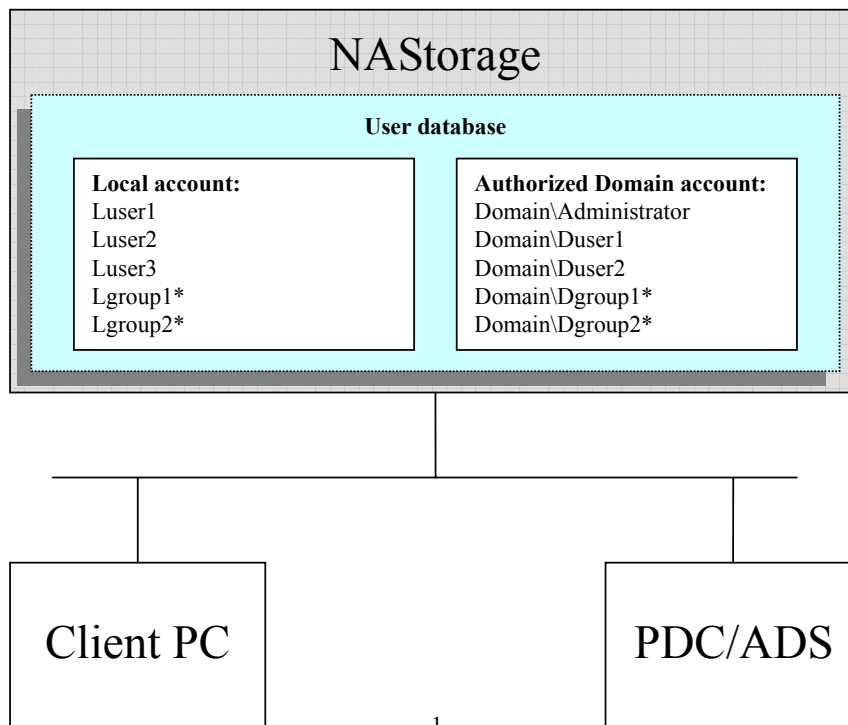
Security Policy for SMB/CIFS environment

In SMB/CIFS network environment, NAStorage allows two kinds of user account for security control purpose. A brief description will be given in the following paragraph.

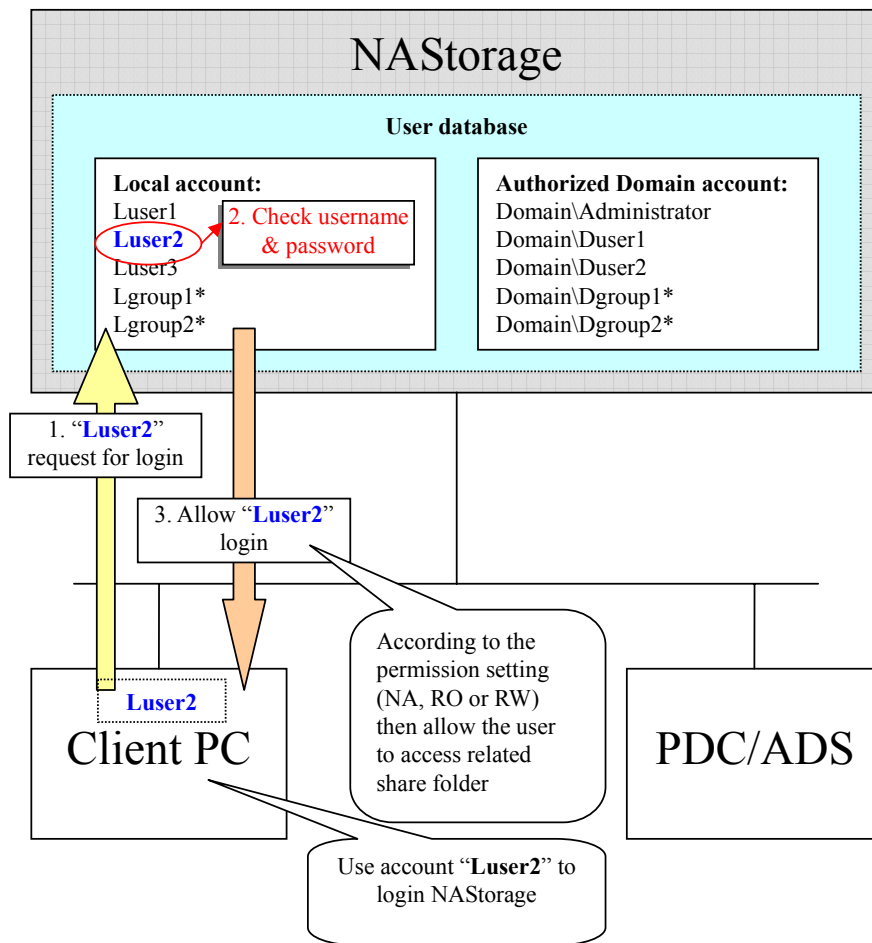
- ※ **Local Account:** It means the administrator can add user account manually when there isn't any PDC/ADS exist in the network. The local account will be stored in NAStorage.
- ※ **Domain Account:** It means we can integrate security policy between NAStorage and existing PDC/ADS; we can use Admin Home Page of NAStorage to get account list from existing PDC/ADS then add some authorized user or group account to user database of NAStorage.

What is user database?

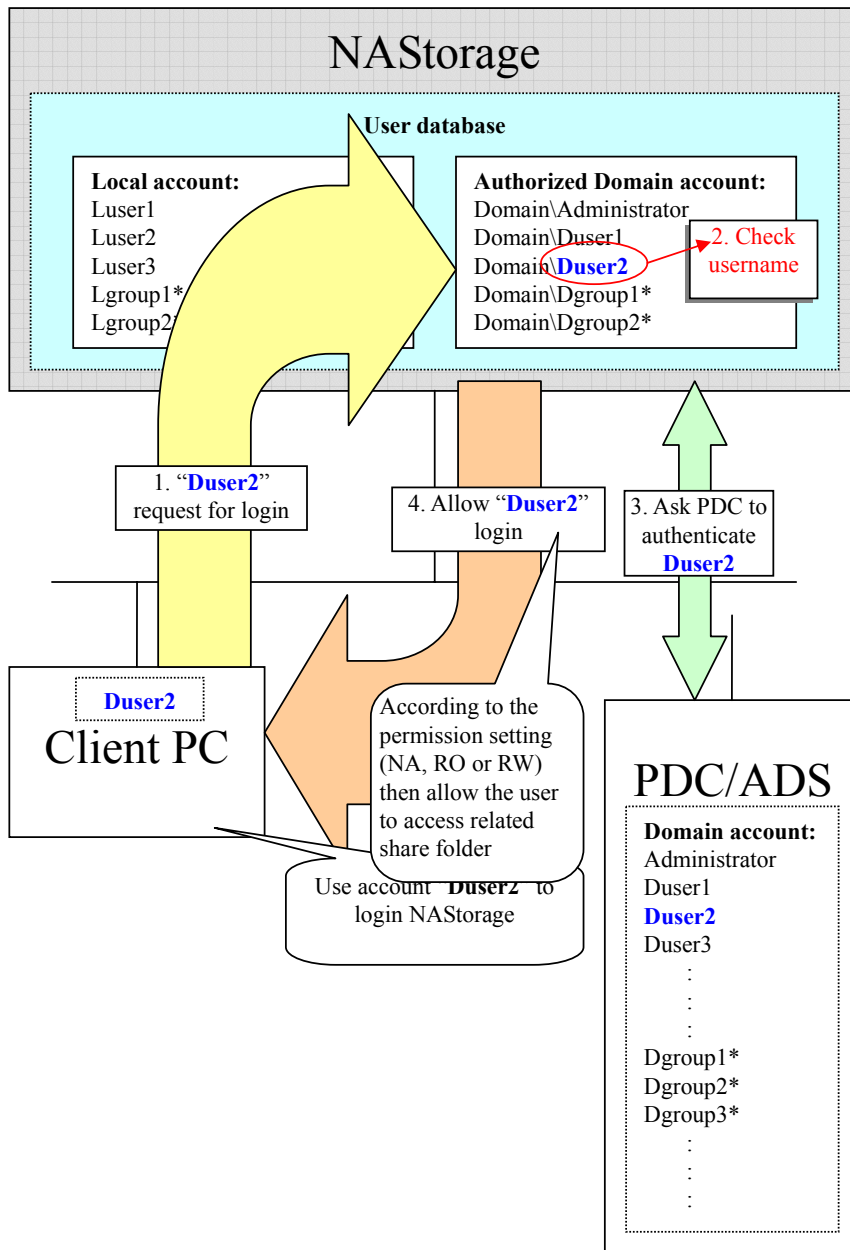
NAStorage save accounts to its **user database** for easily manage all of accounts and backup account purpose, it will include created local accounts and authorized domain accounts. Accounts inside user database can be set permission to Share or ACL node of NAStorage.



Below is the authentication process flow of client that uses **Local account** to login NASTorage:

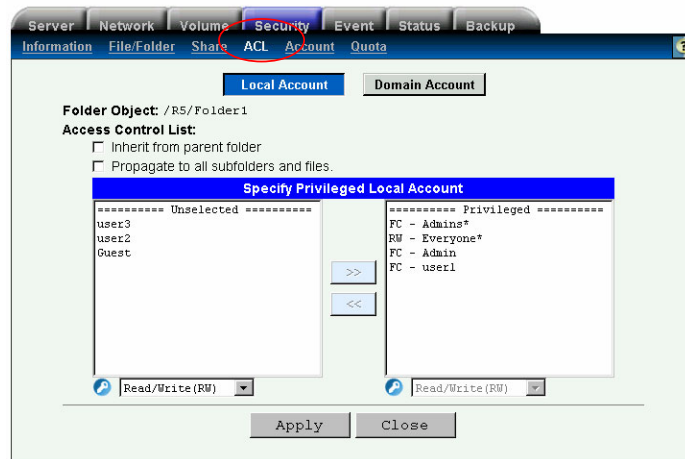


Below is the authentication process flow of client that uses **Domain account** to login NAStorage:



How about ACL inside NAStorage

NAStorage can set ACL (*Access Control List*) nodes for **file level** security control. ACL is a list associated with file/folder that contains information about which users or groups have permission to access or modify the file/folder. Each user or group can be set to a specific ACL node, such as a directory (Folder) or file. Each node has a unique security attribute that identifies which users have access to it.



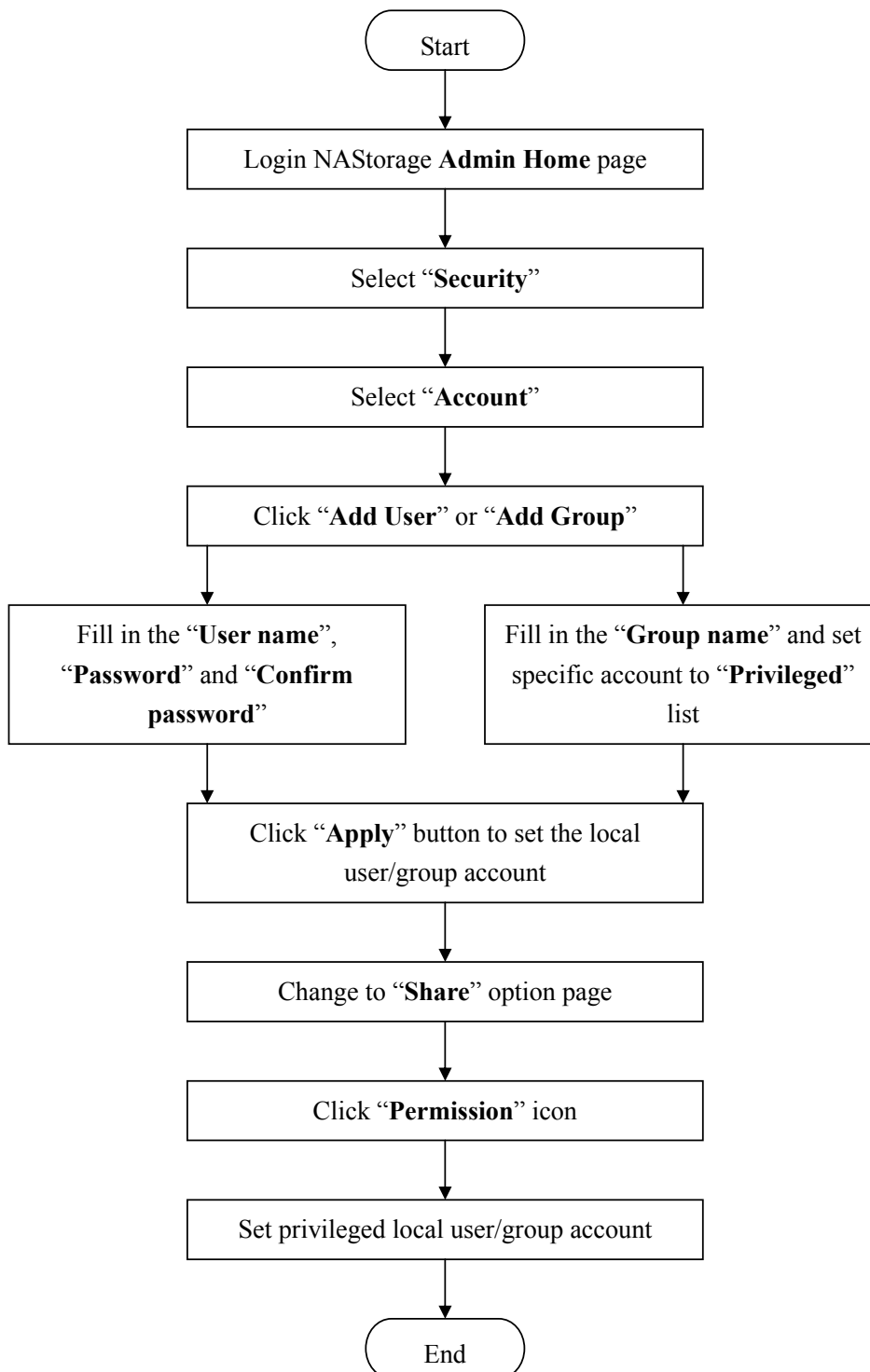
Over all switch for SMB/CIFS Protocol

You should make sure the SMB/CIFS protocol is enabled on your NAStorage; you can find the function in Windows sub menu of Network.



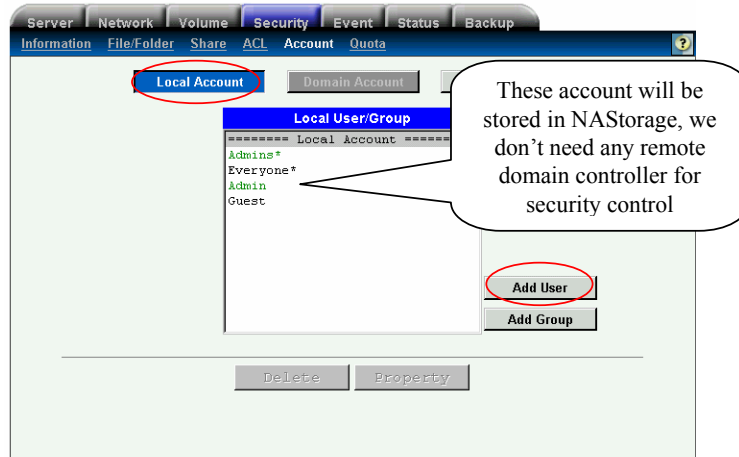
Add Local Account and set permission on

NAStorage:

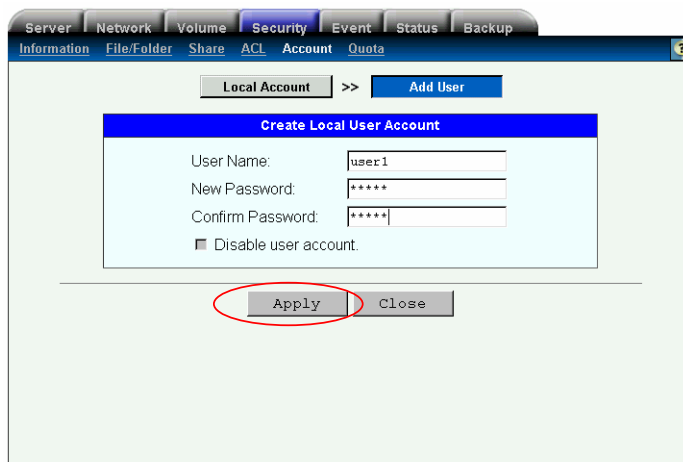


How to create Local User and Group on NASTorage:

1. On **Admin Home** page, select **Security** then select **Account** prepares to add user account manually.
2. Click **Add User** button.

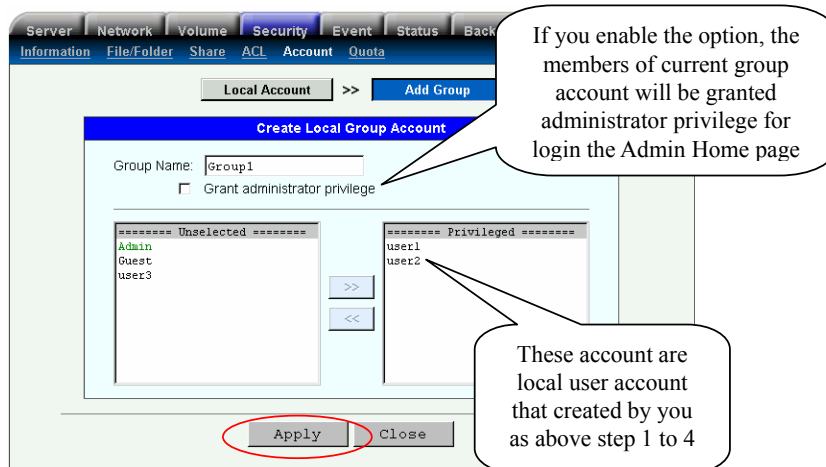


3. Fill in **User Name**, **New Password** and **Confirm Password** as require.
4. Click the **Apply** button to complete creating stage.



5. If you want to add a group of local user, click **Add Group** button, then fill in the group name.

6. Select or multi-select specific users from **Unselected** list to **Privileged** list.
7. Click **Apply** button to complete creating stage.



How to set permission of Local User and Group on NASStorage:

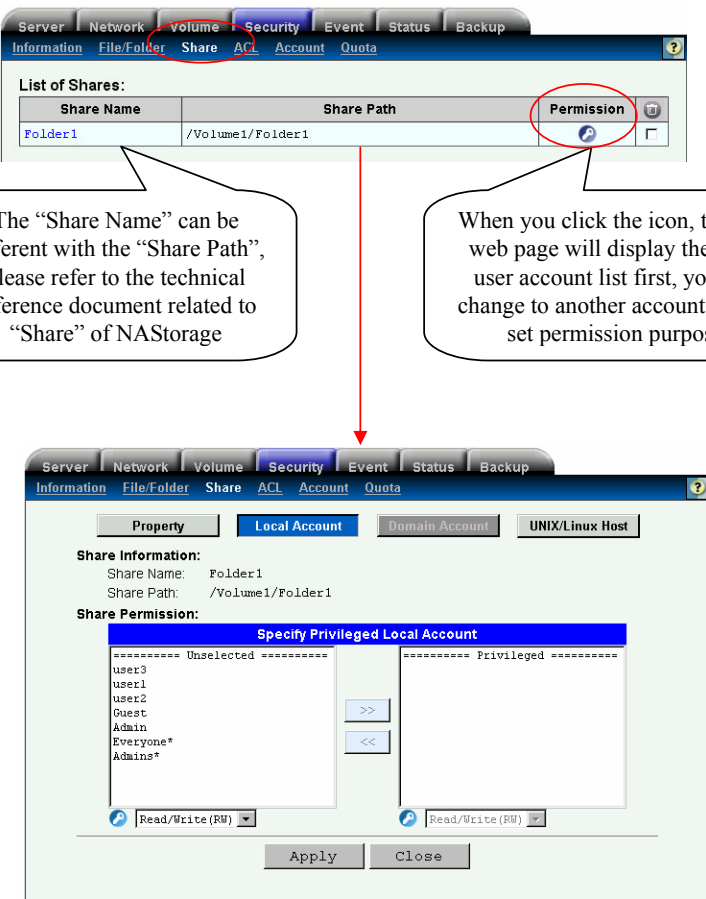
NASStorage provide three kinds of permission to set client's accessible authority:

NA: No Access, login user can't access any shared folders

RO: Read only, login user only can read shared folders

RW: Read/Write, login user can read, modify or save data to shared folders

1. Go to **Share** sub menu of **Security** Page (please make sure you had create shared folders already).
2. Click the **Permission** icon behind the **Share Name** that you want to permit it.

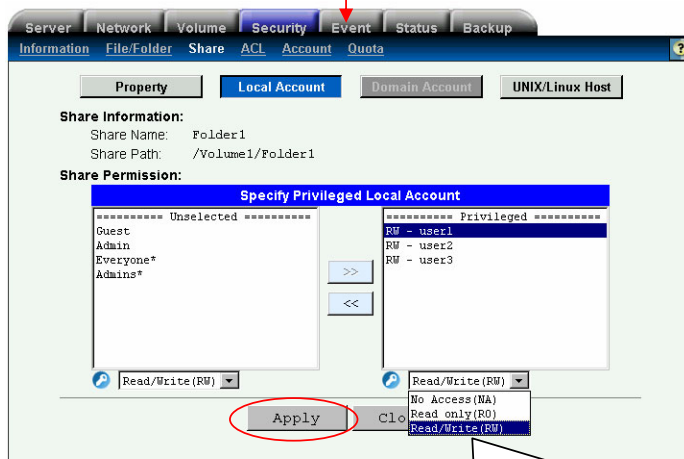
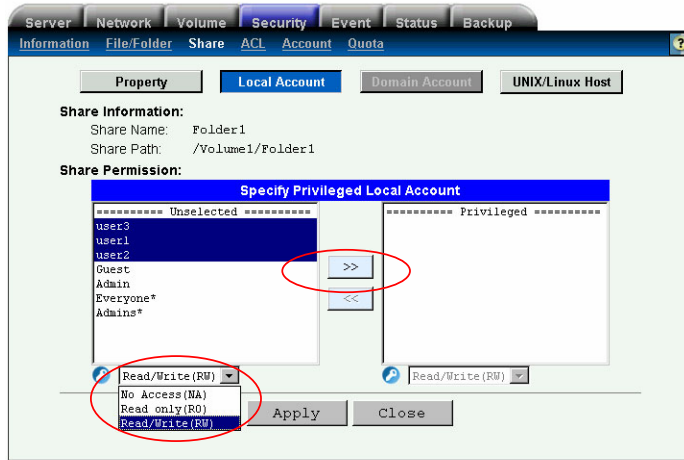


The screenshot shows the 'Security' page with the 'Share' sub-menu selected. A table titled 'List of Shares' contains one entry: 'Folder1' with a share path of '/Volume1/Folder1'. A red circle highlights the 'Permission' icon (a blue padlock) next to the share name. A red arrow points from this icon to a second screenshot of the 'Specify Privileged Local Account' dialog box. This dialog box has tabs for 'Property', 'Local Account', 'Domain Account', and 'UNIX/Linux Host'. The 'Local Account' tab is active, showing 'Share Information' (Name: Folder1, Path: /Volume1/Folder1) and a list of local accounts. The 'Unselected' list includes user3, user1, user2, Guest, Admin, Everyone*, and Admins*. The 'Privileged' list is empty. Below the lists are '>>' and '<<' buttons, and two dropdown menus both set to 'Read/Write (RW)'. 'Apply' and 'Close' buttons are at the bottom.

The "Share Name" can be different with the "Share Path", please refer to the technical reference document related to "Share" of NASStorage

When you click the icon, the first web page will display the local user account list first, you can change to another account list for set permission purpose

3. Select or multi-select specific **Local User/Group** accounts and set relative accessible authority (NA, RO or RW). (The “*” mark means the account is group and “#” mark means the account grant administrator privilege.)
4. Move the specific accounts from **Unselected** list to **Privileged** list
5. Click **Apply** button to complete all procedures.

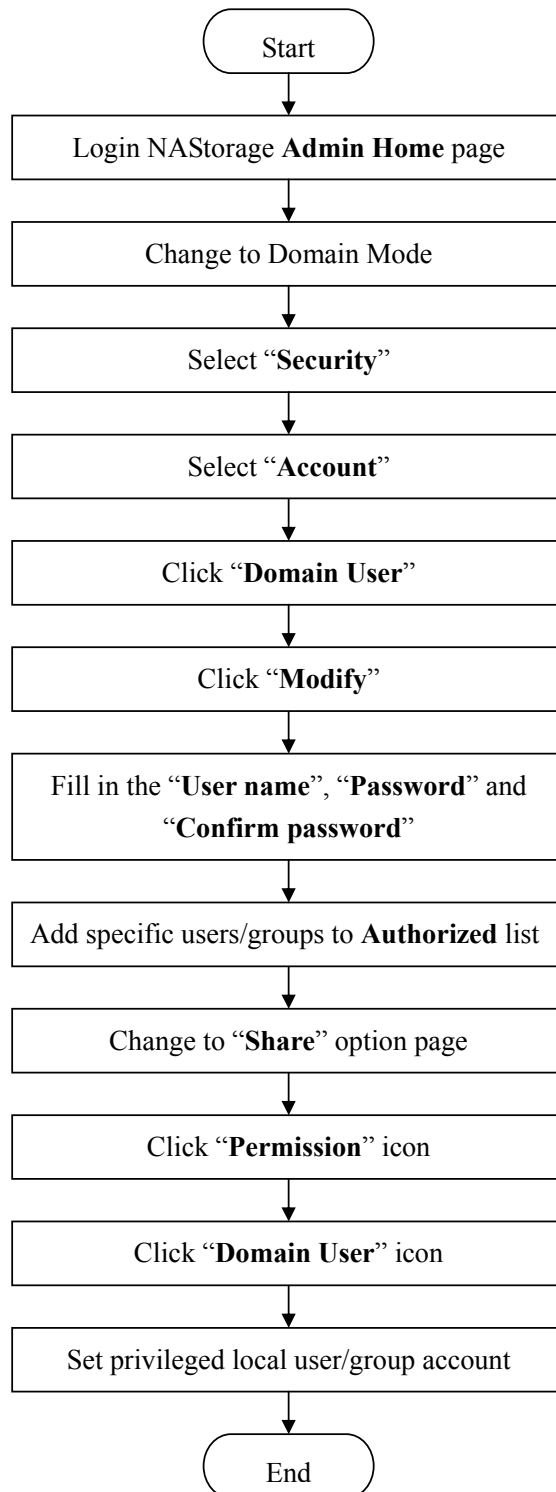


You can change the permission (NA, RO or RW) of privileged account at any time

删除:

Add Domain Account and set permission on

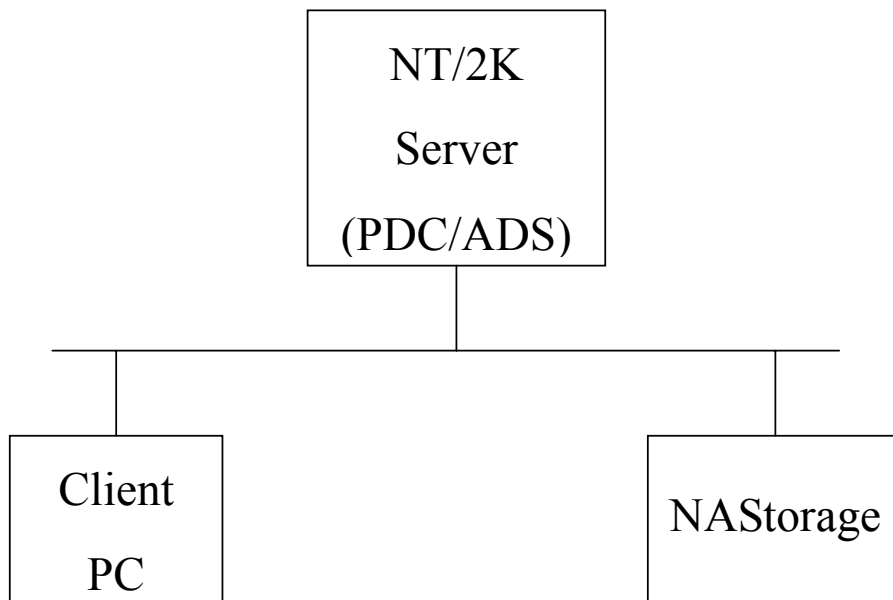
NAStorage:



How to add Domain User and Group on NAStorage:

Note:

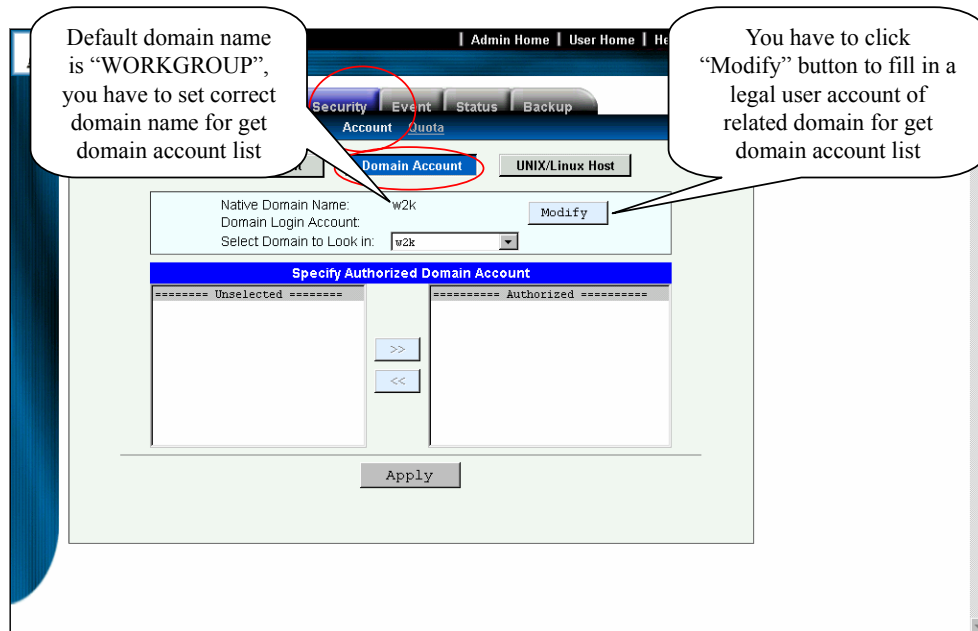
You should have at least one PDC (Primary Domain Controller) or ADS server on your LAN to validate the security control of SMB. PDC/ADS server maintains user security information. NAStorage needs a PDC/ADS server to authenticate the username and password provided by users.



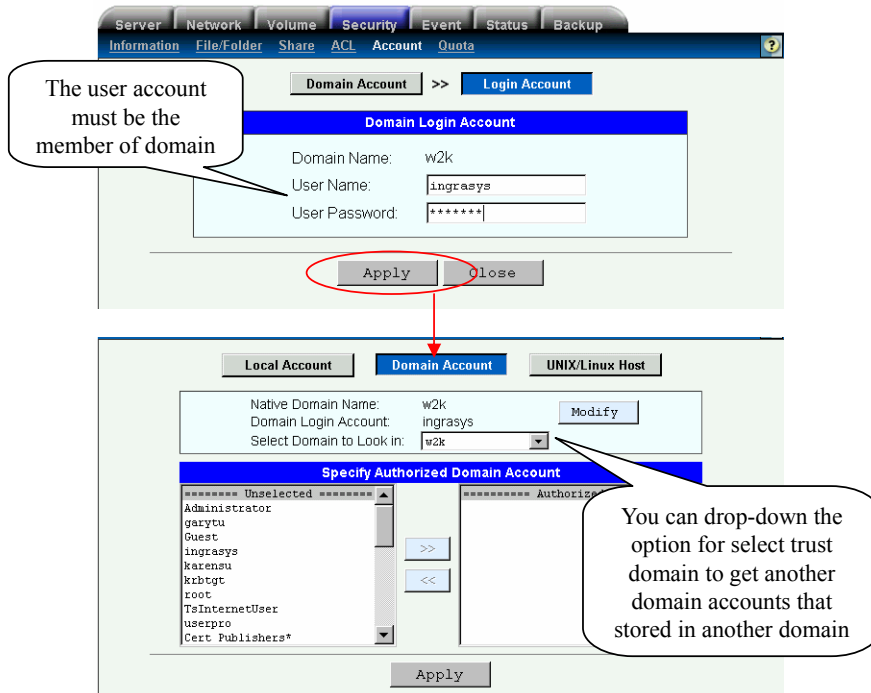
1. On **Admin Home** page, select **Windows** sub menu of **Network** page.
2. Change network mode to **Domain Mode** and fill in the correct domain name. (Assume the current domain is “w2k”)
3. Click **Apply** button and reboot NASTorage.



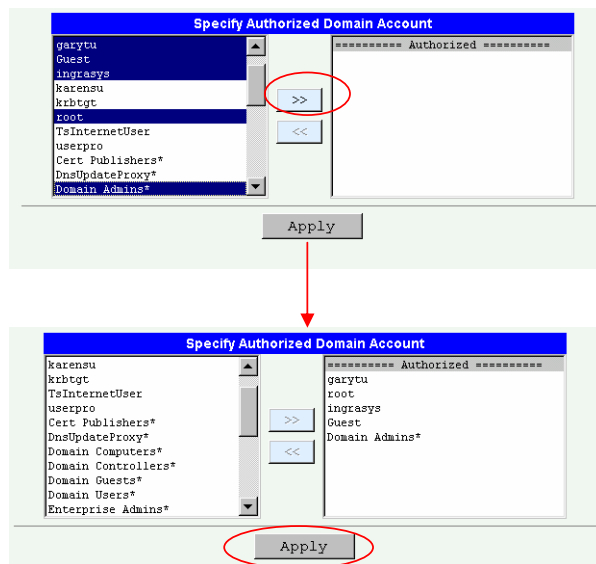
4. On **Admin Home** page, select **Security** then select **Account** prepares to get domain user account.
5. Click **Domain Account** button.



6. Click **Modify** button.
7. Fill in **User Name** and **User Password** as require.
8. Click the **Apply** button to get domain account list.



9. Select or multi-select specific users from **Unselected** list to **Authorized** list. (The "*" mark means the account is group.)
10. Click **Apply** button to complete setting.



✘**Notice:** When you want to set permission of domain user or group, you have to set the **Authorized** domain user or group account in above web page first, these account will stored in local pool (local user database) of NAStorage, once you want to set permission of shared folder in NAStorage, the **Authorized** domain user or group just can be displayed in **Unselected** list for select and you can add those account to **Privileged** list of shared folders to set permission.

How to set permission of Domain user and group on NASStorage:

NASStorage provide three kinds of permission to set client's accessible authority:

NA: No Access, login user can't access any shared folders

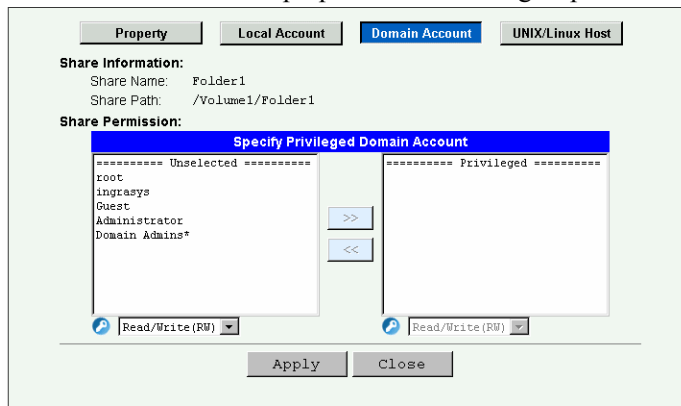
RO: Read only, login user only can read shared folders

RW: Read/Write, login user can read, modify or save data to shared folders

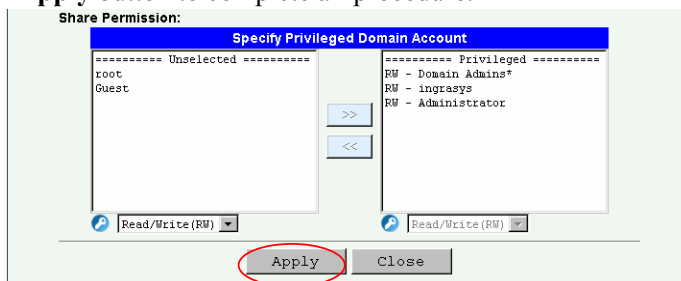
1. Go to **Share** sub menu of **Security** Page.
2. Click the **Permission** icon behind the **Share Name** that you want to permit it.



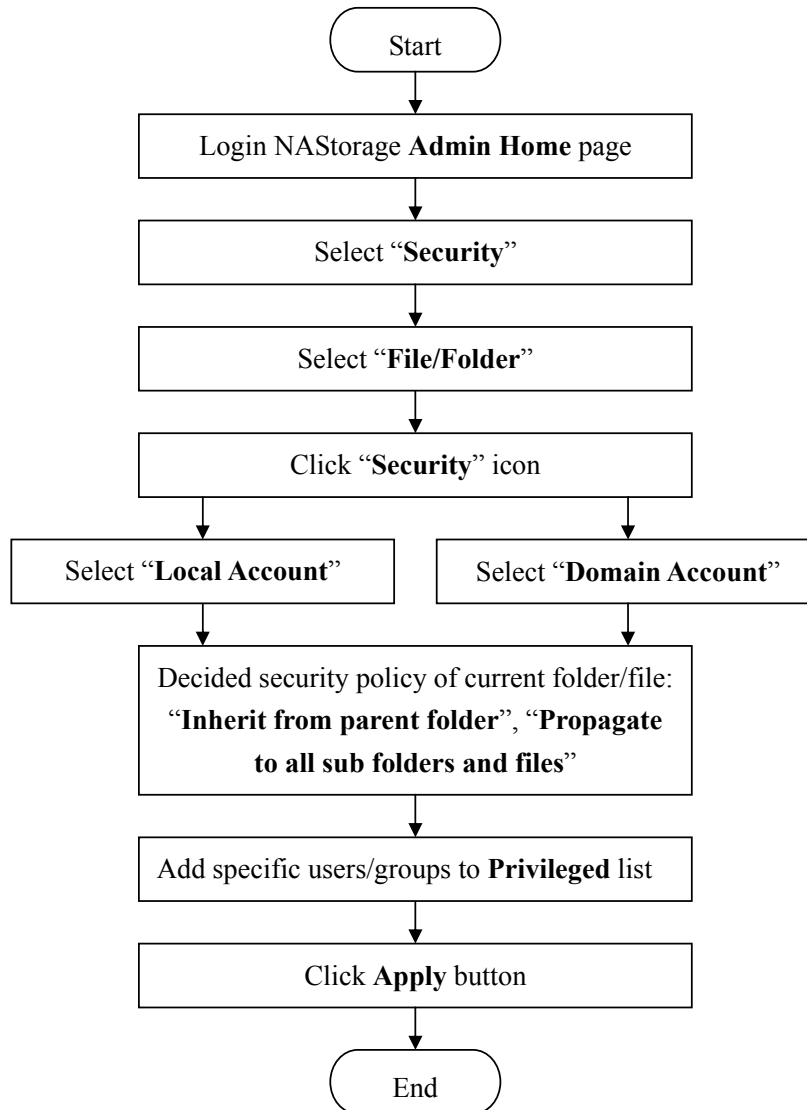
3. Click **Domain Account** button prepares to add user/group accounts.



4. Select or multi-select specific **Domain User/Group** accounts and set relative accessible authority (NA, RO or RW). (The "*" mark means the account is group.)
5. Move the specific accounts from **Unselected** list to **Privileged** list
6. Click **Apply** button to complete all procedure.



Set ACL on NASStorage:



How to set ACL on NASStorage

NASStorage provide three kinds of permission to set client's accessible authority:

NA: No Access, login user can't access related shared folders/files

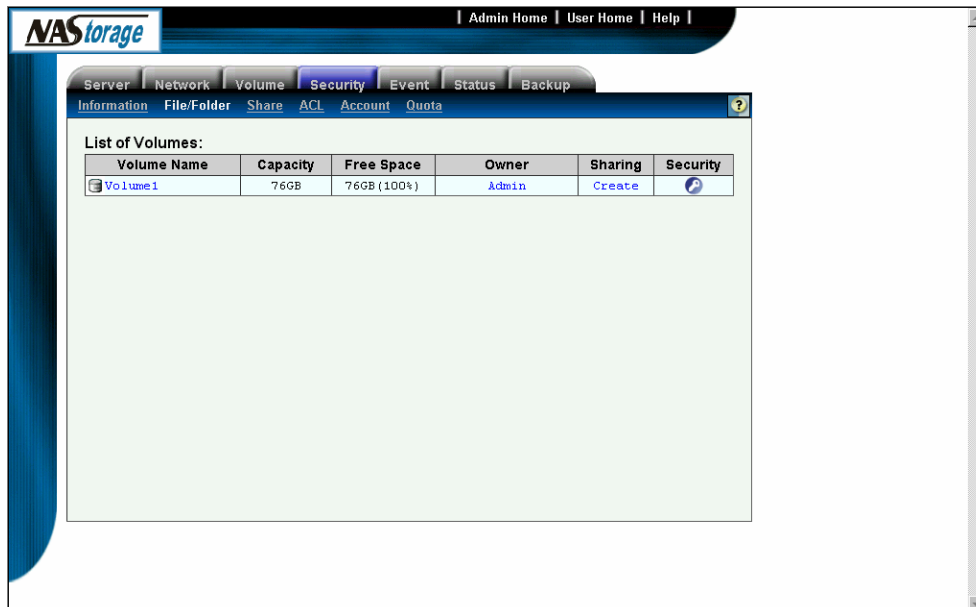
RO: Read only, login user only can read related shared folders/files

WO: Write only, login user only can write data to related shared folders/files

RW: Read/Write, login user can read, modify or save data to shared folders/files

FC: Full Control, login user not only has RW permission, but also can set permission of shared folders/files, you can select a shared folders/files then click right button of mouse to set relative permission

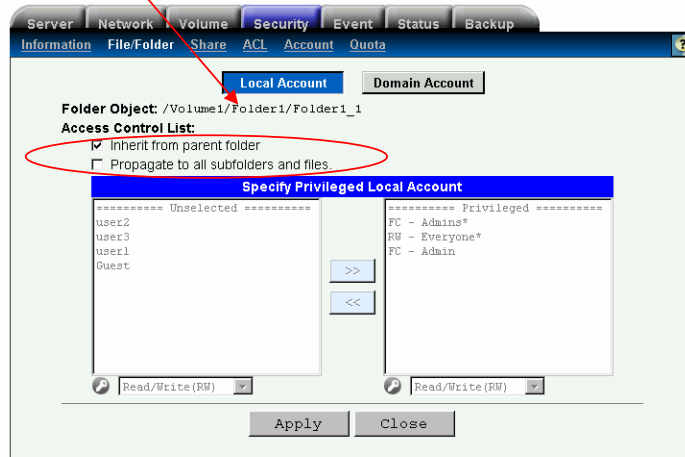
1. Go to **File/Folder** sub menu of **Security** Page.



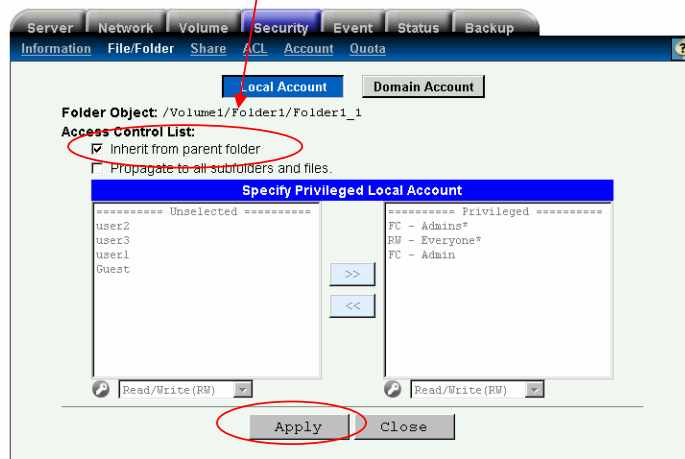
2. Select a folder or file in volume of NASStorage that you want to set ACL node
3. Click the **Security** icon behind the **File/Folder Name** that you want to set it.



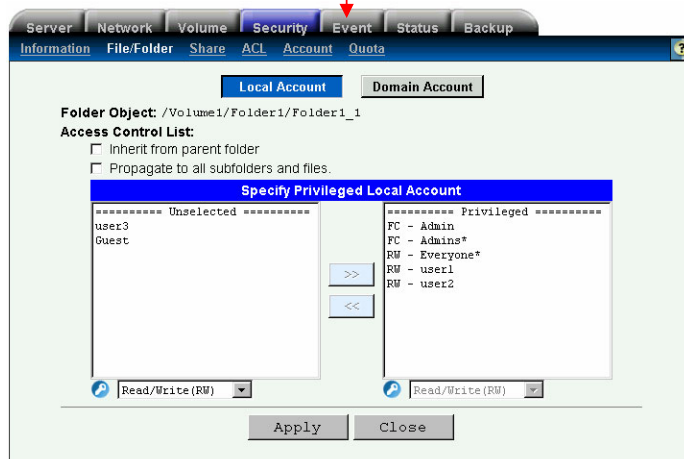
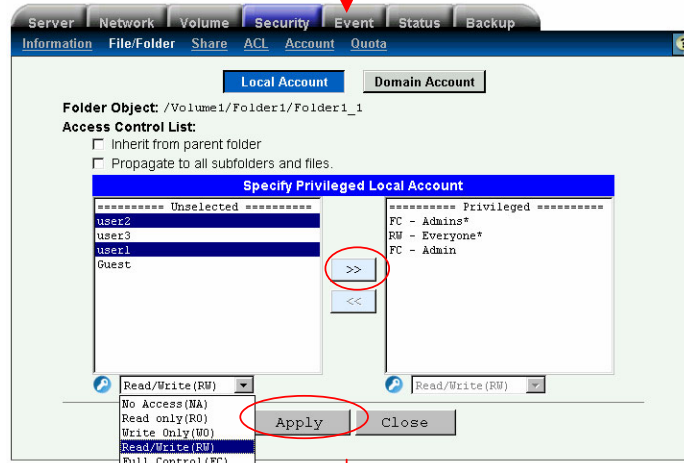
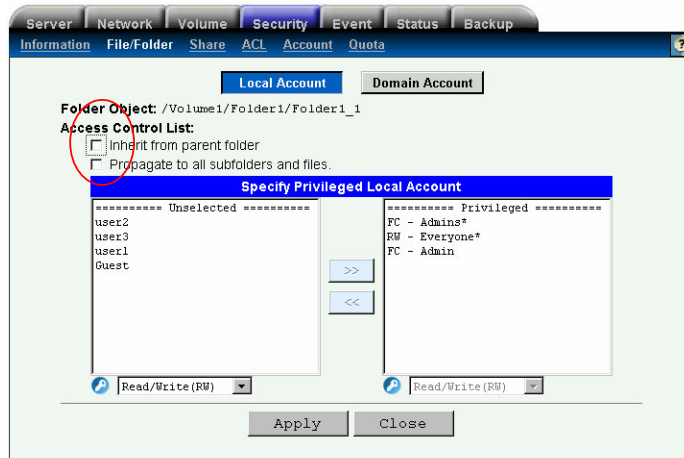
4. If you select **folder**, you can see the page like below
5. Default first page is Local Account page.



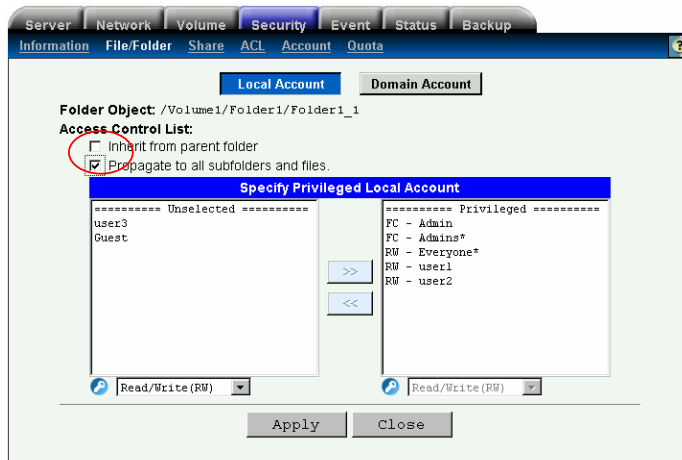
6. Decided security policy of current folder: **“Inherit from parent folder”**, **“Propagate to all sub folders and files”**
 - ※ Inherit from parent folder: This ACL node will inherit the permission of parent folder (up layer folder); it means all of permission will be same as the parent folder.
 - ※ Propagate to all sub folders and files: This ACL node will propagate the permission to all sub folders and files. All of these sub folders and files will inherit this ACL node.
7. You can set four different combinations about the security control like below:
 - a. Just only enable **“Inherit from parent folder”**; you don’t need to set any more, just click Apply button to complete setting. This ACL node will be same as the permission of **Folder1**.



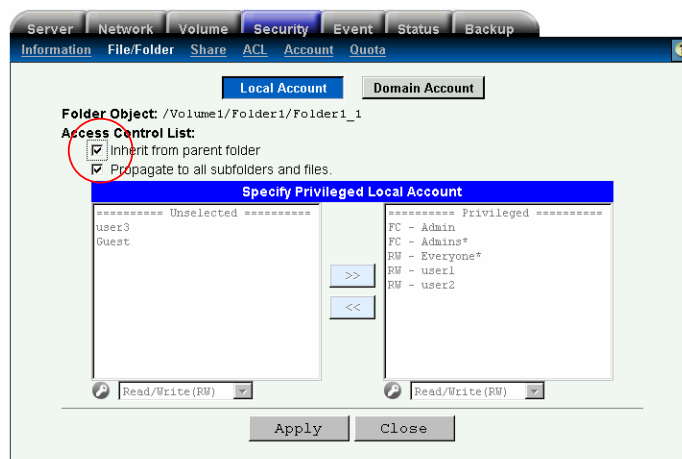
- b. **“Inherit from parent folder”** and **“Propagate to all sub folders and files”** all are disabled, you can multi select some account and add them to privileged list then click **Apply** button to complete setting. The permission will only apply for this folder.



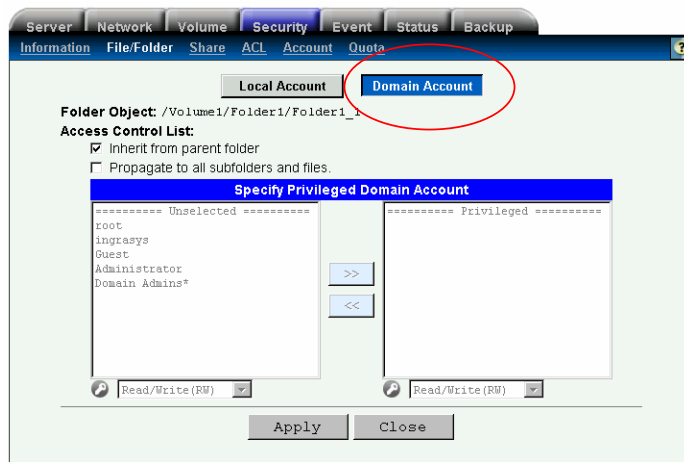
- c. Just only enable “**Propagate to all sub folders and files**”; you can multi select some account and add them to privileged list then click Apply button to complete setting. All sub folders and files will follow the permission of this node.



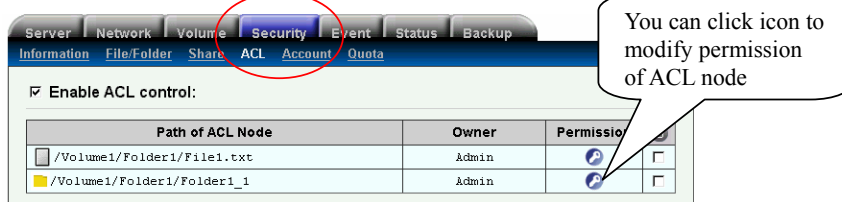
- d. Enable “**Inherit from parent folder**” and “**Propagate to all sub folders and files**” at same time. This ACL node will be same as the permission of Folder1 and its all sub folders and files also are the same.



- Click **Domain Account** button to add privileged domain account list.



- Repeat the step 6 and step 7 as above.
- After add ACL nodes, you can select ACL sub menu of security and check all of ACL nodes that appear in web page like below.



- If you want to modify the permission about ACL node, you can click the permission icon behind the related path of ACL node to do that.