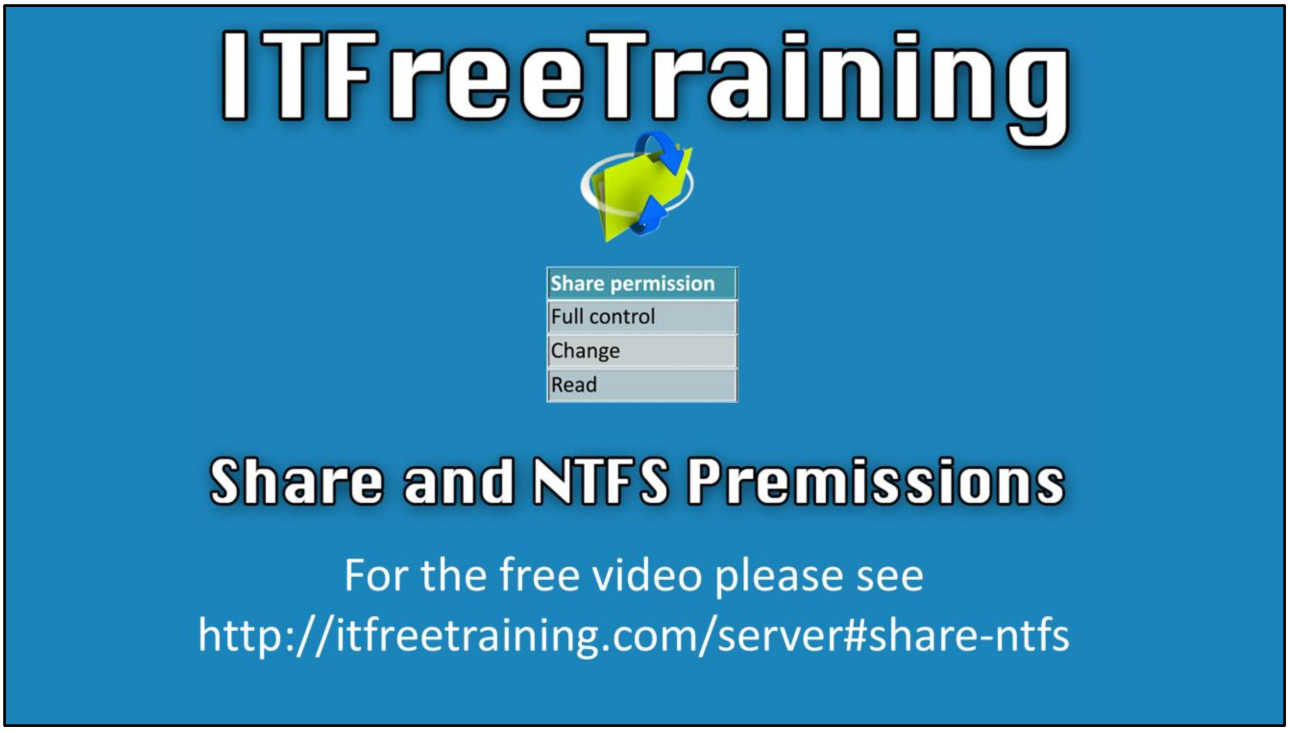


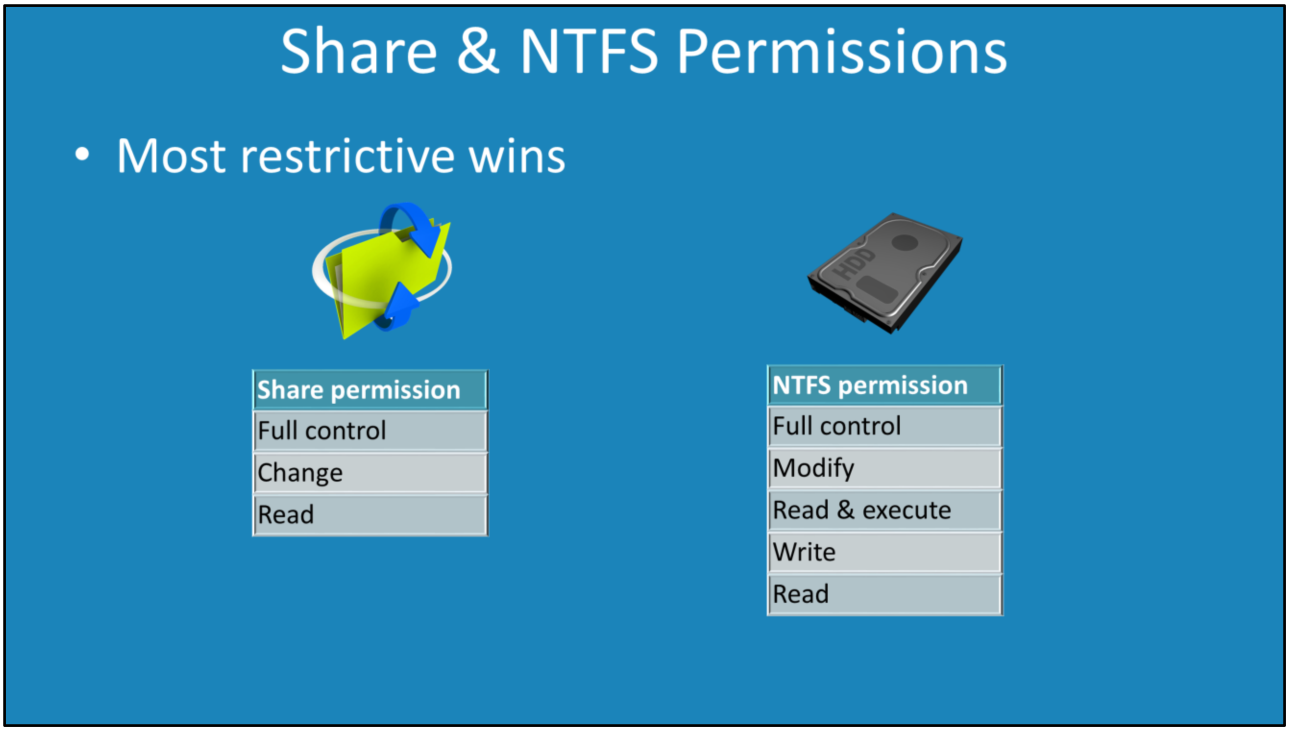
ITFreeTraining

Share permission
Full control
Change
Read

Share and NTFS Premissions

For the free video please see
http://itfreetraining.com/server#share-ntfs

This video will look at what happens to a user access when share and NTFS permissions are used together. Using these effectively together can greatly improve the security of your network while still allowing the user to access what they need to.



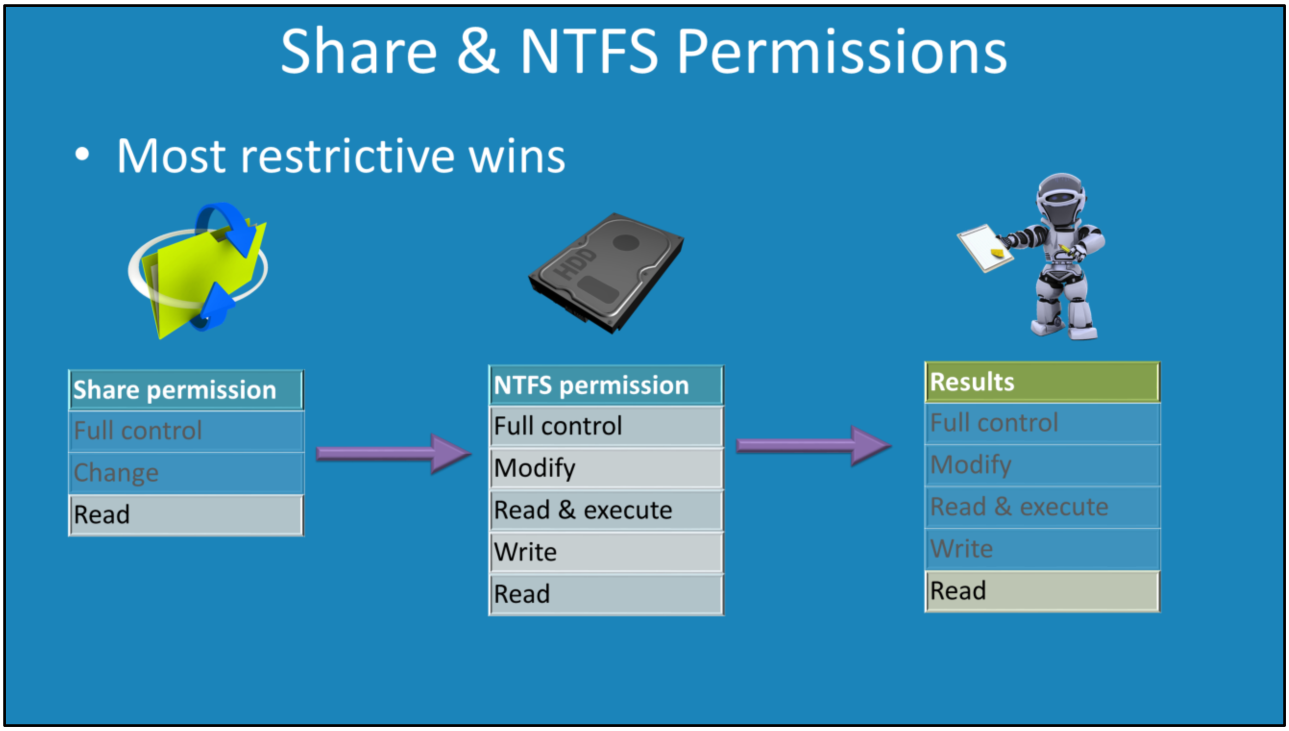
Share & NTFS Permissions

- Most restrictive wins

Share permission
Full control
Change
Read

NTFS permission
Full control
Modify
Read & execute
Write
Read

Share and NTFS Permissions
When you create a file share, you are able to configure 3 basic permissions on the share. Full control gives the user's read/write/delete, the ability to take ownership and change permissions. Change allows the user to read/write/delete, and read allows the user to read. NTFS has five basic permissions. Full control has the same effect as share full control and read has the same effect and the read share permission. The modify permission in NTFS is the same and the change permission in share permission.



Share & NTFS Permissions

- Most restrictive wins

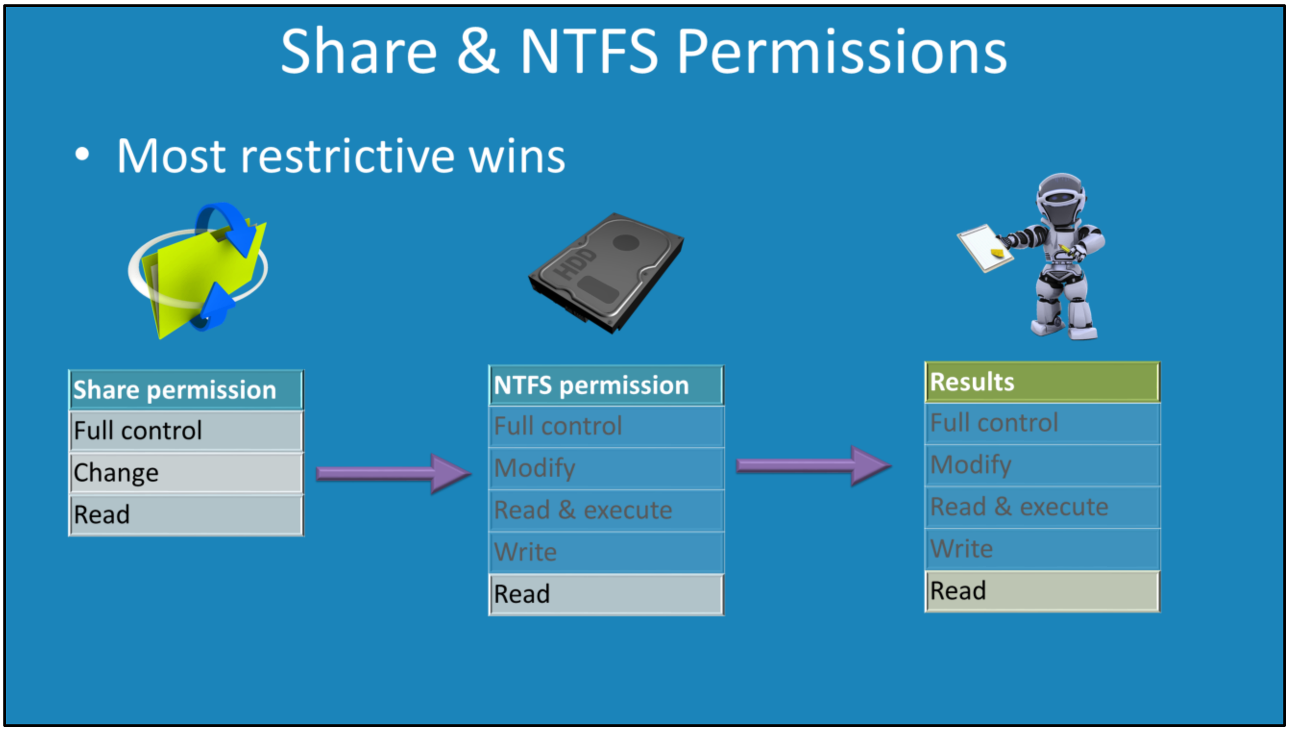
Share permission
Full control
Change
Read

NTFS permission
Full control
Modify
Read & execute
Write
Read

Results
Full control
Modify
Read & execute
Write
Read

If you have configured different shares and NTFS permissions, the important point to remember is that that most restrictive permission will always win. Consider some examples.

1) If the share permission was set to read, and the NTFS set to full control, the user, when accessing the share, would get the permission read.



Share & NTFS Permissions

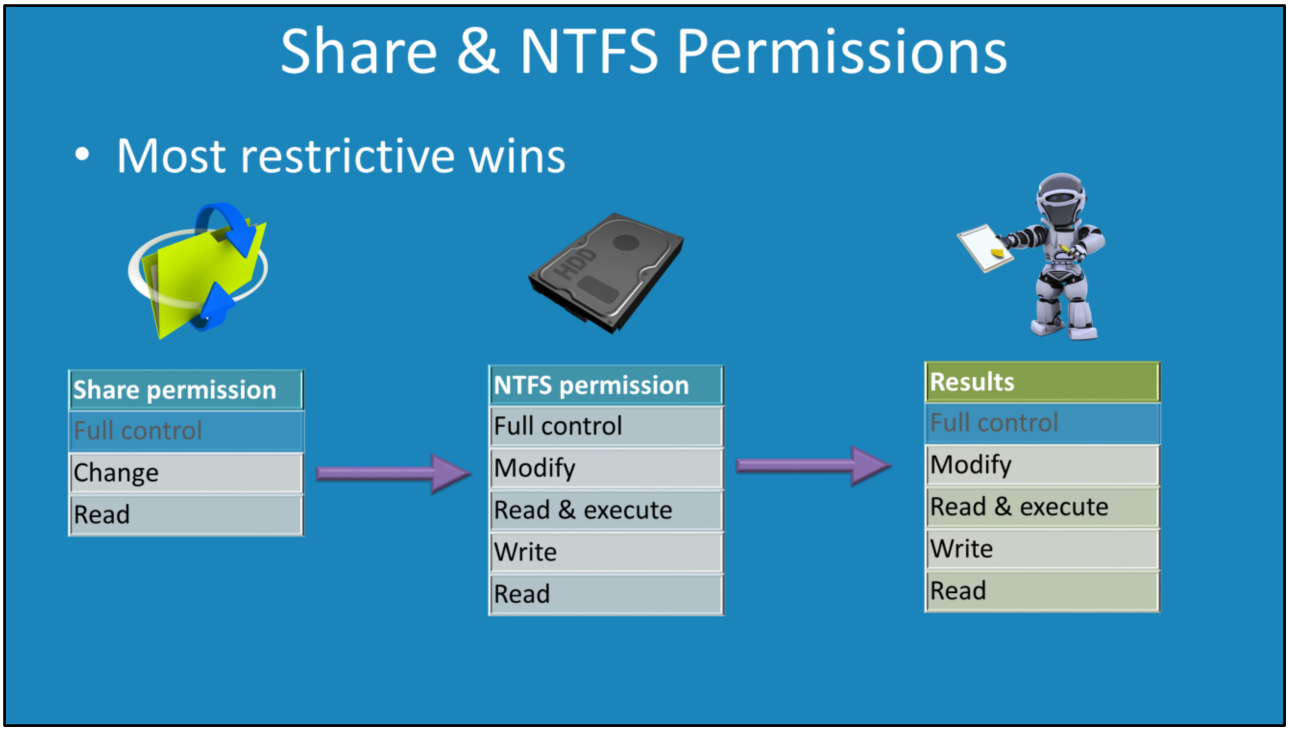
- Most restrictive wins

Share permission
Full control
Change
Read

NTFS permission
Full control
Modify
Read & execute
Write
Read

Results
Full control
Modify
Read & execute
Write
Read

2) If the share had full control and the NTFS permissions were set to read, the user would once again only have read permission since the most restrictive permission will always win.



Share & NTFS Permissions

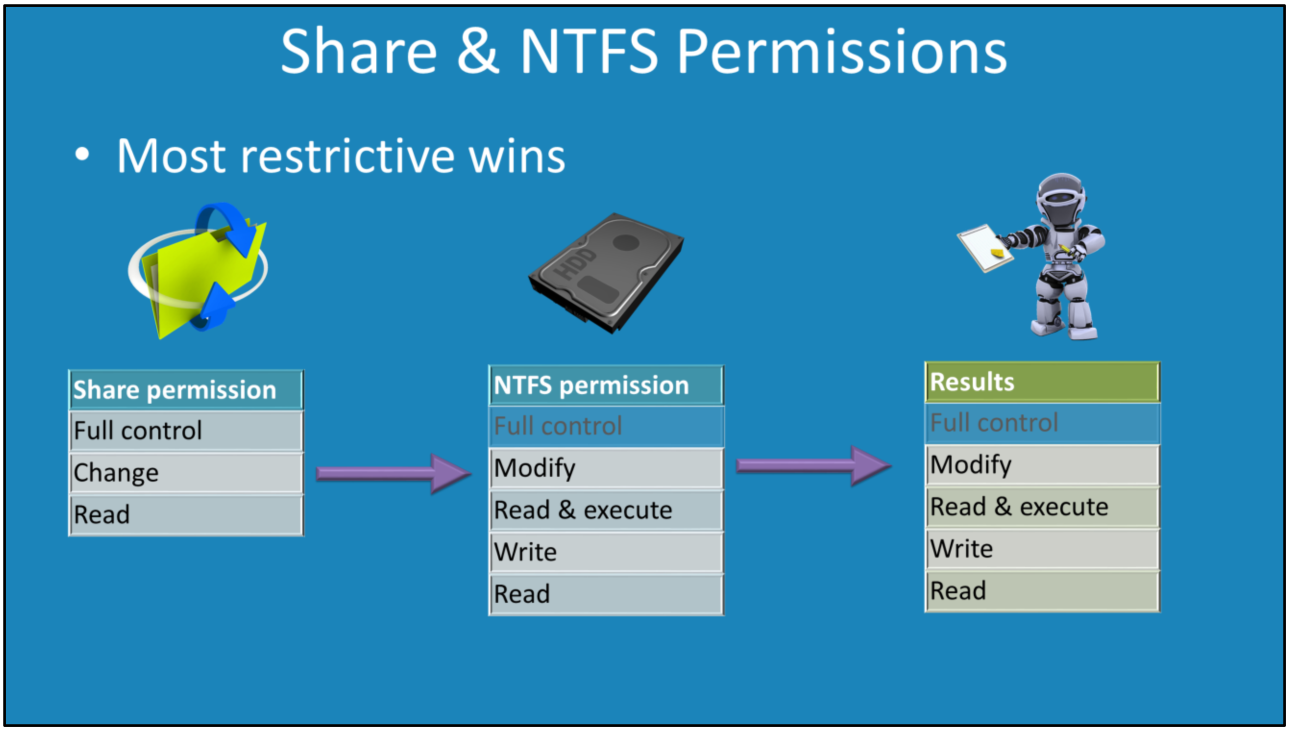
- Most restrictive wins

Share permission
Full control
Change
Read

NTFS permission
Full control
Modify
Read & execute
Write
Read

Results
Full control
Modify
Read & execute
Write
Read

3) If the share permission was set to change and the NTFS permission was set to full control, the user would get modify access. Modify access is essentially the change permission. Since the change permission was the most restrictive permission, the user will have read/write/delete which is change or modify access.



Share & NTFS Permissions

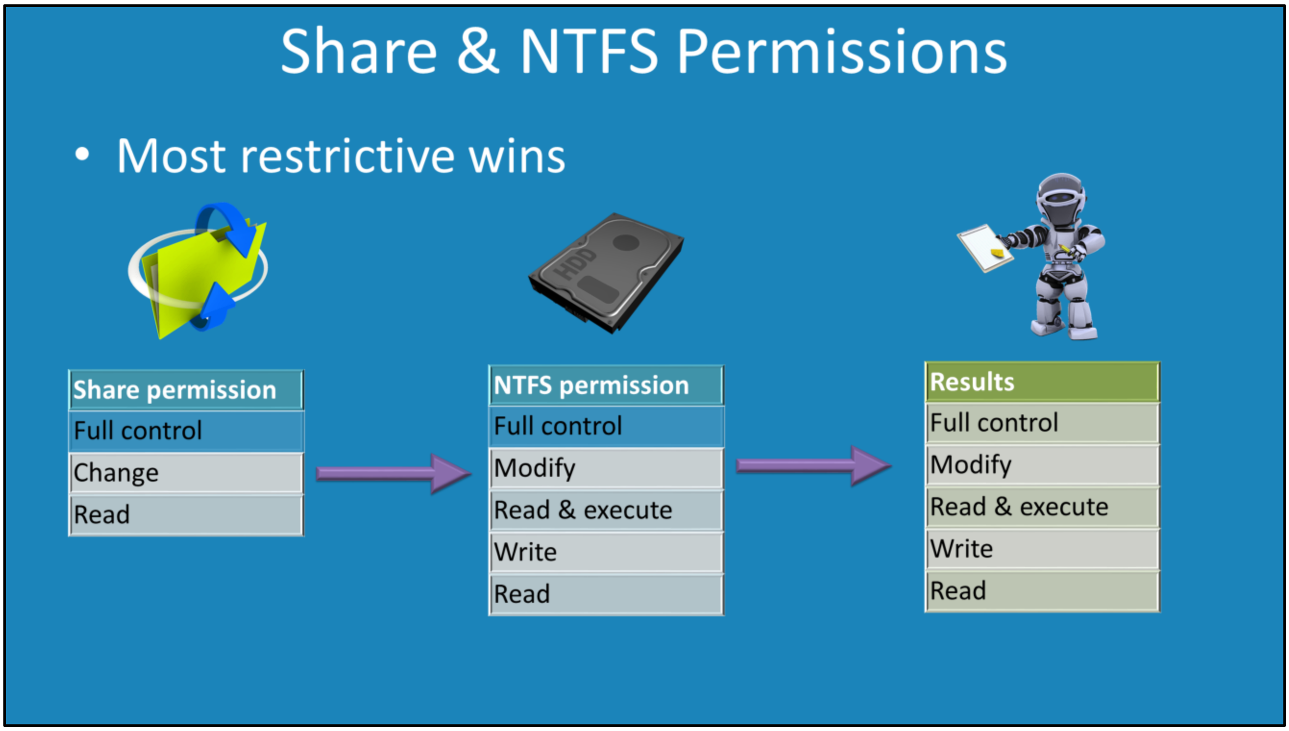
- Most restrictive wins

Share permission
Full control
Change
Read

NTFS permission
Full control
Modify
Read & execute
Write
Read

Results
Full control
Modify
Read & execute
Write
Read

4) If the share permission was set to full control and the NTFS permission was set to modify, the user would get modify access. Modify access is essentially the change permission. Since the change permission was the most restrictive permission, the user will have read/write/delete which is change or modify access.



Share & NTFS Permissions

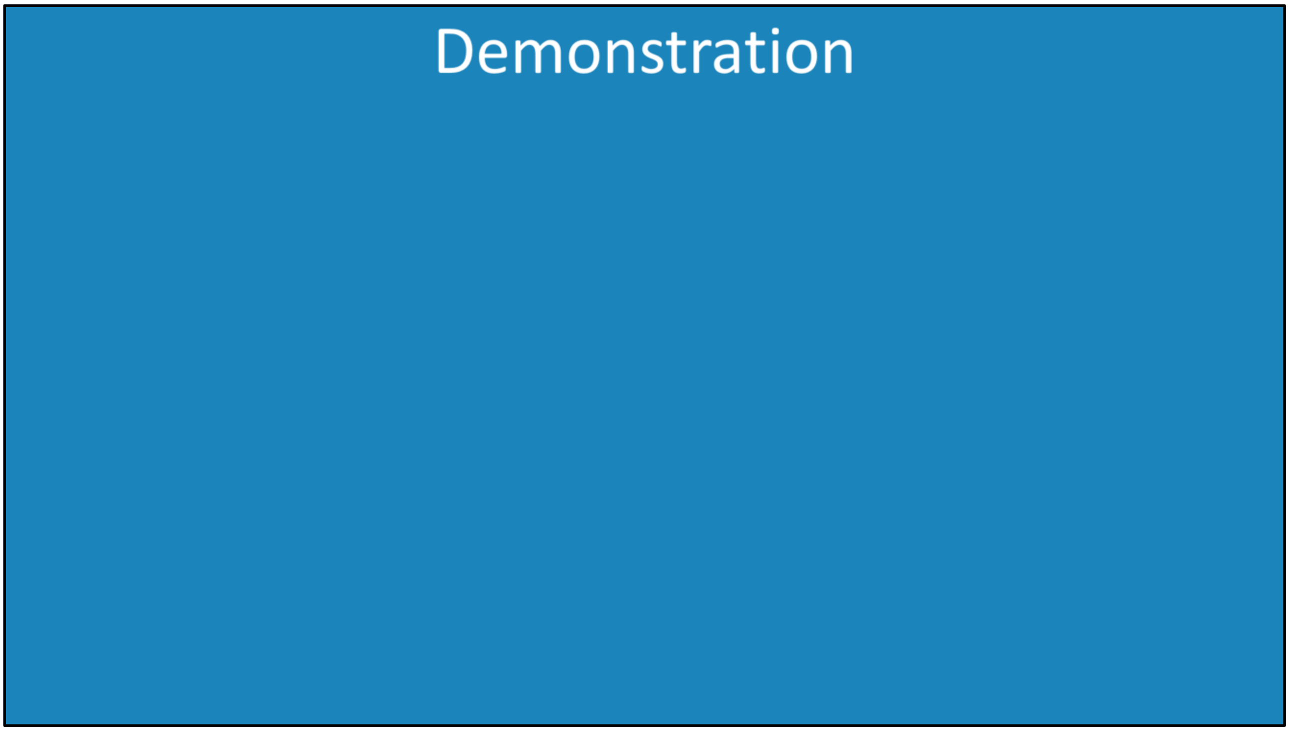
- Most restrictive wins

Share permission
Full control
Change
Read

NTFS permission
Full control
Modify
Read & execute
Write
Read

Results
Full control
Modify
Read & execute
Write
Read

The choice of which permission to use comes down to the choice of the individual administrator. Some administrators configure the share permissions with full control and then subtract permissions using NTFS. Others will configure security at the share level. The important point to remember is that NTFS permission allows granular control while share permissions are a broad stroke approach.

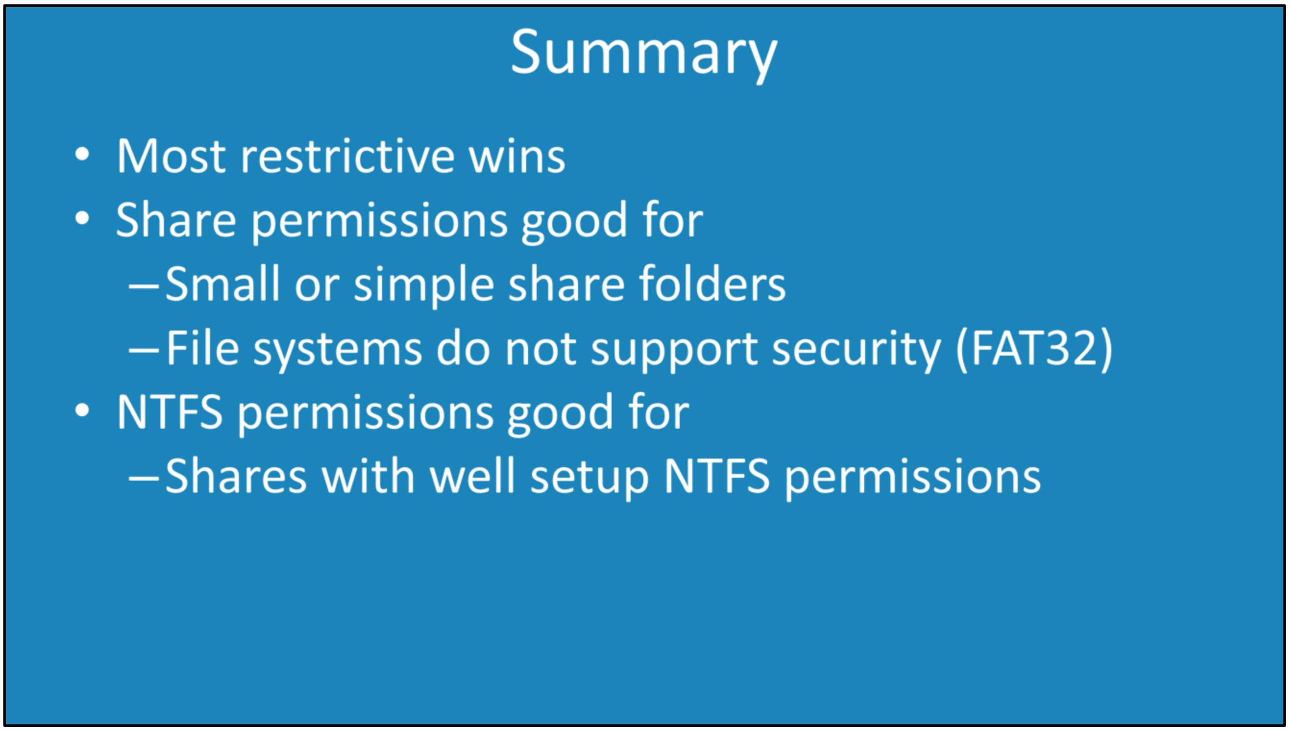


Demonstration

Demonstration

DepData will be configured to allow full control at the share level. Permissions will be subtracted at the folder level using NTFS.
Right click the folder DepData and select properties.
Select the tab sharing and the press the button advanced sharing.
From the advanced sharing dialog press the button at the bottom permissions.
This will show that everyone has full control to the share.
Next select the security tab and notice what permissions have been configured. The users have been configured with modify access. This essentially means that a user accessing the share will lose full control access that was granted at the share level and be left with modify access. However, users like administrators that have been granted full control will be allow to have this access since at the share level it has been configured with full control.

Depdata2 will be configured to share permission for user.
Right click the folder DepData2 and select properties.
Select the tab sharing and then press the button advanced sharing.
From the advanced sharing dialog press the button at the bottom permissions.
In this case, the everyone permission has been added with change access. Also notice the second entry for administrators gives administrators full control. In this example there are only two groups so this is not that difficult for the administrator to configure this. However, if there were more groups, this becomes more work to keep up to date.
Next select the security tab and notice what permissions have been configured. Notice that users and administrators have been configured with full control. However, the user will only get change access because this was what was configured at the folder level. You can see that if an administrator forgot to configure NTFS permissions, the user would not get any additional access as the share permission acts as a safety net to prevent the user getting more permissions then they should have.
Using this method, it is also possible to remove user access. For example, if you want the user to only have read access to a file or folder you would only need to modify the NTFS permission to remove the write access for that user.



Summary

- Most restrictive wins
- Share permissions good for
  - Small or simple share folders
  - File systems do not support security (FAT32)
- NTFS permissions good for
  - Shares with well setup NTFS permissions

Summary

When combining NTFS and share permissions together, remember that the most restrictive permissions win. Share permissions are generally good for small or simple share folders or systems that do not have security like FAT32. If the permissions get more complicated, for example, you have multiple folders that require different permissions for different users, NTFS is a better choice to configure permissions on.

See http://YouTube.com/ITFreeTraining or http://itfreetraining.com for our always free training videos. This is only one video from the many free courses available on YouTube.

References

“Installing and Configuring Windows Server 2012 Exam Ref 70-410” pg 85-86