ST2612 Tutorial 3 (Week 6)

Recap of Practical 3, Lecture 3 and Lecture 4 (Part 1)

Learning objective of Practical 3:

* Revision on proper preparation for a system to join to a Domain.
  + Key element: proper DNS setting of the client.
* Hands on exercise on security group creation and member assignment.
* Hands on with Security Configuration Wizard with Windows Server 2012R2.
  + This role based configuration wizard will turn off all the non-essential services for the system for you and it may cause you unexpected issue in the subsequent practical sessions.
  + One service, Windows Remote Management, is disable by the SCW and you need to reconfigure it for automatic start up in order for the later part of the practical 3 exercises.
* Hands on with permissions settings and Shared folder creation.
  + Two approach for Shared Folder creation.
    - Use folder properties menu. (Recommended only with client Windows systems. (Win 8.1, win 10).
    - Use New Shares Wizard within Server Manager (Recommended when operating with Windows Servers OS)
      * Explicit option for data encryption.
  + EFS operations and the command line options.
  + Audit log viewing for Logon and folder/file access event.
    - Viewing for Success / Failure logon is straight forward
    - Viewing for Success / Failure folder/file access requires additional setup (Not mentioned in the lab exercises):
      * Need to configure the Audit option at the actual folder / file object level at the advanced security setting menu.
      * Need to ensure the security option "Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings" is set to disabled at the target system.

Ref:

* + - * + [https://www.manageengine.com/products/active-directory-](https://www.manageengine.com/products/active-directory-audit/how-to/audit-failed-access-attempts-to-shared-folder.html#%3A%7E%3Atext%3DNavigate%20to%20Computer%20Configuration%20%2D%3E%20Windows%2Cfor%20both%20success%20and%20failure) [audit/how-to/audit-failed-access-attempts-to-shared-](https://www.manageengine.com/products/active-directory-audit/how-to/audit-failed-access-attempts-to-shared-folder.html#%3A%7E%3Atext%3DNavigate%20to%20Computer%20Configuration%20%2D%3E%20Windows%2Cfor%20both%20success%20and%20failure) [folder.html#:~:text=Navigate%20to%20Computer%20Configura](https://www.manageengine.com/products/active-directory-audit/how-to/audit-failed-access-attempts-to-shared-folder.html#%3A%7E%3Atext%3DNavigate%20to%20Computer%20Configuration%20%2D%3E%20Windows%2Cfor%20both%20success%20and%20failure) [tion%20%2D%3E%20Windows,for%20both%20success%20and](https://www.manageengine.com/products/active-directory-audit/how-to/audit-failed-access-attempts-to-shared-folder.html#%3A%7E%3Atext%3DNavigate%20to%20Computer%20Configuration%20%2D%3E%20Windows%2Cfor%20both%20success%20and%20failure)

[%20failure](https://www.manageengine.com/products/active-directory-audit/how-to/audit-failed-access-attempts-to-shared-folder.html#%3A%7E%3Atext%3DNavigate%20to%20Computer%20Configuration%20%2D%3E%20Windows%2Cfor%20both%20success%20and%20failure).

* + - * + [https://docs.microsoft.com/en-us/windows/security/threat-](https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/audit-force-audit-policy-subcategory-settings-to-override) [protection/security-policy-settings/audit-force-audit-policy-](https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/audit-force-audit-policy-subcategory-settings-to-override) [subcategory-settings-to-override](https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/audit-force-audit-policy-subcategory-settings-to-override)
  + Simple Powershell exercise/experiment.
  + Roaming Profile

Lecture 3 is focus on the following:

* Account and Security Group Management
  + Disable vs Delete Account
  + Security Group Attributes
    - Scope - the domain in which the group exists.
    - Membership capabilities - what type of Active Directory objects can be its member.
    - Permissions - resource permissions that have be granted to the group.
* AGDLP Role based Permission assignment strategy.
* Resource Permission Configuration and File Systems
  + NTFS Folder and File permissions.
    - Explicit permissions vs inherited permissions
    - Positive permissions vs negative permissions (DENY)
    - Cumulative permissions applied for combined NTFS permissions.
  + Configure shared folders and shared folder security
    - Most restricted permissions applied for combined NTFS and Shared Folder permissions.
* Important Features in Windows Server 2016 Active Directory
  + Restart capability
  + Read-Only Domain Controller
  + Cloning domain controllers
  + Fine-grained password policy enhancements
  + Protected users global group
* Introduction to User Profiles Lecture 4 (Beginning Part):
* Install, configure, and troubleshoot DNS
  + How DNS works ?

Forward lookup zone (Local DNS holds record)

First, local DNS checks caches

**Root name server approach below**

Resolving name server, Root name server, Top level domain (TLD) name servers, authoritative name servers

Forwarder

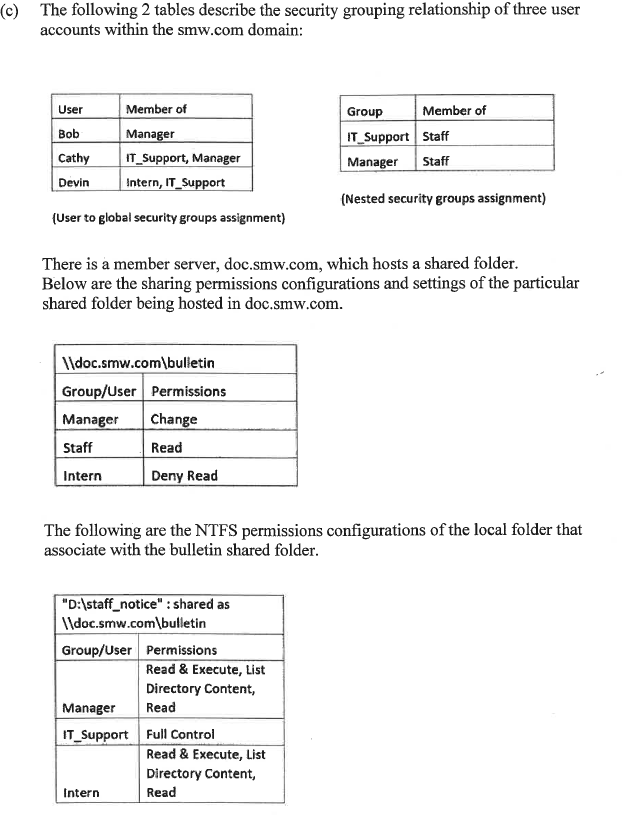
* + Root Hints vs Forwarders vs Stub Zones.
  + Forward lookup vs Reverse Lookup
  + Common DNS attacks and Customized in-house Forwarder/
* Using Microsoft Baseline Security Analyzer
  + MBSA has been replaced by Microsoft Security Compliance Toolkit 1.0 (SCT)
* Using Microsoft ‘Security Compliance Manager’
  + Serve as a repository of baseline configurations for the Enterprise.
* Security Enhancement of Server 2016 Self-evaluation Check list
* A user account, Mary, belongs to two global security groups: G1 and G2. The permission settings given to G1 only allows it to have read only access to a file X. The permission settings of G2 allows it to have read and change access to the file X.

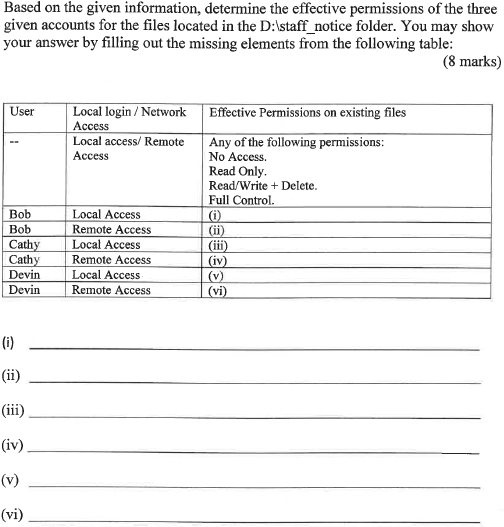
What will be the effective access right of Mary having for the file

Continue on the previous question. If the file X is under the folder d:\data and this folder has been shared as \\memsrv1\netShare. The shared folder permission settings only allow security group, G3, to have read only access to it. Mary is also a member of G3.

What will be the effective access right of Mary having for the file X, when she is access it via the network?

* + The following is a question of ST2612 MST in AY2019/2020 S2. Try to answer it.





1. Read Only.  
   (ii) Read Only.  
   (iii) Full Control.  
   (iv) Read/Write + Delete  
   (v) Full Control.  
   (vi) No Access.
2. read
3. read
4. Full control

(iv) change

1. Full control
2. Deny read

* What is DNS reverse lookup?
* By default, not all the hosts are having their reverse lookup (PTR) entries set up at the DNS Zone. Name a reason of why we may want to setup the PTR entries for some the hosts.
* Please compare the iterative lookup and the recursive lookup in terms of efficiency, and the possible security implications.
* List three best practices to tighten the security of a DNS service in an Active Directory network.
* List two functions of SCM.
* The following is a question of ST2612 MST in AY2019/2020 S2. Try to answer it.

Briefly describe three possible ways for a Windows Server 2016 DNS to resolve the name address queries for its clients. (9 marks)

Nano Test Questions (Will be given by your tutor).

Q1.

Q2.

Q3.

Submit your answers to the Nano Test Journal before the end of the class.

~ That's All ~