Windows Servers TTTS0500

Lab 4 – Groups and File Services

Task 1 – Creating groups

1. Using Active Directory Users and Computers MMC, create the following Domain Local security groups:

   a. Marketing-rwx

   b. Marketing-r

   c. HR-rwx

   d. HR-r

2. Using dsadd command line tool, create the following Domain Local security groups:

   a. Management-rwx

   ```
   C:\Users\Administrator.DC1.000>dsadd group "CN=Management-rwx, dc=M3227, dc=local" -secgrp yes -scope L
   dsadd succeeded:CN=Management-rwx,dc=M3227,dc=local
   ```

   b. Public-rwx

3. Using PowerShell, create the following Global security groups:

   a. Marketing

   b. Management

   c. HR

   d. ICT

   e. Sales

   ```
   PS C:\Users\Administrator.DC1.000> New-ADGroup -name "Marketing" -groupscope Global
   PS C:\Users\Administrator.DC1.000> New-ADGroup -name "Management" -groupscope Global
   PS C:\Users\Administrator.DC1.000> New-ADGroup -name "HR" -groupscope Global
   PS C:\Users\Administrator.DC1.000> New-ADGroup -name "ICT" -groupscope Global
   PS C:\Users\Administrator.DC1.000> New-ADGroup -name "Sales" -groupscope Global
   ```

4. Using Active Directory Administrative Center, create the following Global security group:

   a. Public

b. Expand PowerShell history in ADAC

    i. Copy the commands used in creating the group from ADAC PowerShell history and paste in your lab document

```
☐ Get-ADObject
        -LDAPFilter:"(objectClass=organizationalPerson)"
        -Properties:lastKnownParent,sAMAccountType,systemFlags,userAccountControl,displayName,description,whenChanged,location,m...
        -ResultPageSize:"100"                                                                          12.3.2019 10.19.51
        -ResultSetSize:"20201"
        -SearchBase:"CN=Users,DC=m3227,DC=local"
        -SearchScope:"OneLevel"
        -Server:"dc1.m3227.local"
☐ Get-ADObject
        -LDAPFilter:"(!objectClass=organizationalPerson)"
        -Properties:isDeleted,whenChanged,allowedChildClassesEffective,allowedChildClasses,lastKnownParent,sAMAccountType,systemFla...
        -ResultPageSize:"100"                                                                          12.3.2019 10.19.51
        -ResultSetSize:"20195"
        -SearchBase:"CN=Users,DC=m3227,DC=local"
        -SearchScope:"OneLevel"
        -Server:"dc1.m3227.local"
```

Task 2 – Group nesting

1. Add the following Global security groups as members to the following Domain Local groups:

Global group	Domain Local Group
Marketing	Marketing-rwx
HR	Marketing-r
Management	Management-rwx
HR	HR-rwx
Marketing	HR-r
All Global groups	Public-rwx

Task 3 – Add users to Global groups

1. Add the users in your OUs as members to the corresponding Global groups

Organizational Unit (OU) users	Global group
Marketing OU users	Marketing
Managemet OU users	Management
HR OU users	HR
ICT OU users	ICT
Sales OU users	Sales

Task 4 – Configuring File Services on fs1

1. Check the settings for correct internal network on fs1

2. Launch fs1 VM

    a. Check hostname

    b. Check IP Addressing

    c. Join fs1 to domain

3. Install File S erver role

    a. Do not forget Resource Manager

Task 5 - Granting access

1. Create the following network shares and add required sharing permissions:

    a. Marketing

      b. Management

      c. HR

      d. Public

2. Add the following NTFS permissions to the shares

      a. Marketing-share:

            i. Marketing-rwx: Full Control
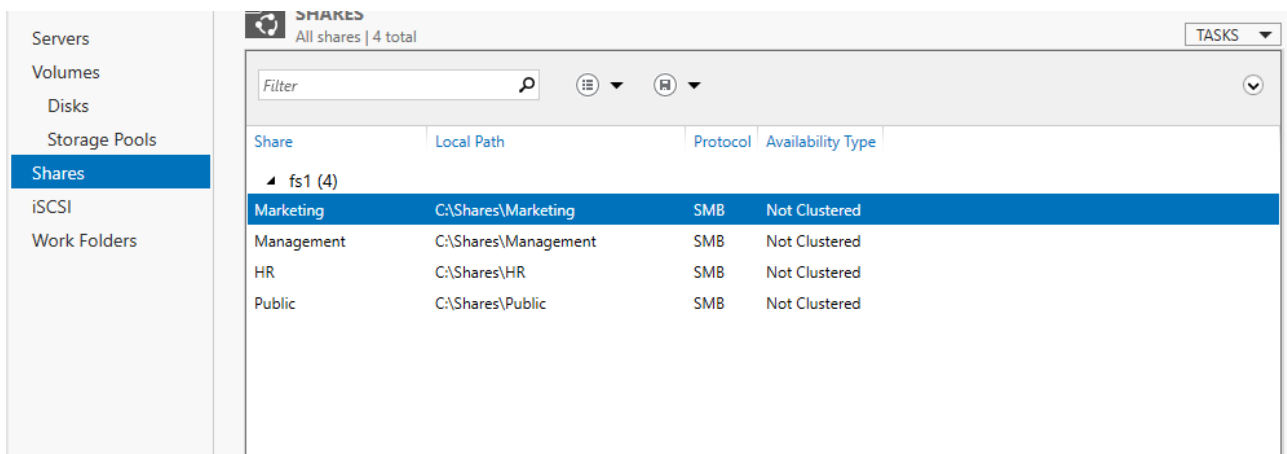
            ii. Marketing-r: Read ja List Folder Content

      b. Management-share:

            i. Management-rwx: Full Control

      c. HR-share

            i. HR-rwx: Full Control

            ii. HR-r: Read ja List Folder Content

Servers	SHARES				TASKS ▼

All shares | 4 total

Servers
Volumes
  Disks
  Storage Pools
Shares
iSCSI
Work Folders

Share	Local Path	Protocol	Availability Type
▲ fs1 (4)			
Marketing	C:\Shares\Marketing	SMB	Not Clustered
Management	C:\Shares\Management	SMB	Not Clustered
HR	C:\Shares\HR	SMB	Not Clustered
Public	C:\Shares\Public	SMB	Not Clustered

3. Install NTFSSecurity PowerShell module and add the following permissions via PowerShell

      a. Install-Module -Name NTFSSecurity or https://github.com/raandree/NTFSSecurity

      b. Public-share

            i. Public-rwx: Full Control

```
PS C:\Users\Administrator> Add-NTFSAccess -Path 'C:\Shares\Public' -Account 'Public-rwx' -AccessRights Fullcontrol
PS C:\Users\Administrator> Get-NTFSAccess -Path 'C:\Shares\Public'


   Path: C:\Shares\Public (Inheritance enabled)


Account                          Access Rights   Applies to                Type    IsInherited   InheritedFrom
-------                          -------------   ----------                ----    -----------   -------------
M3227\Public-rwx                 FullControl     ThisFolderSubfoldersAn... Allow   False
NT AUTHORITY\SYSTEM              FullControl     ThisFolderSubfoldersAn... Allow   True          C:
BUILTIN\Administrators           FullControl     ThisFolderSubfoldersAn... Allow   True          C:
BUILTIN\Users                    ReadAndExec...  ThisFolderSubfoldersAn... Allow   True          C:
BUILTIN\Users                    CreateDirec...  ThisFolderAndSubfolders   Allow   True          C:
BUILTIN\Users                    CreateFiles     ThisFolderAndSubfolders   Allow   True          C:
CREATOR OWNER                    GenericAll      SubfoldersAndFilesOnly    Allow   True          C:
```

Verify assigned permissions (screen captures)