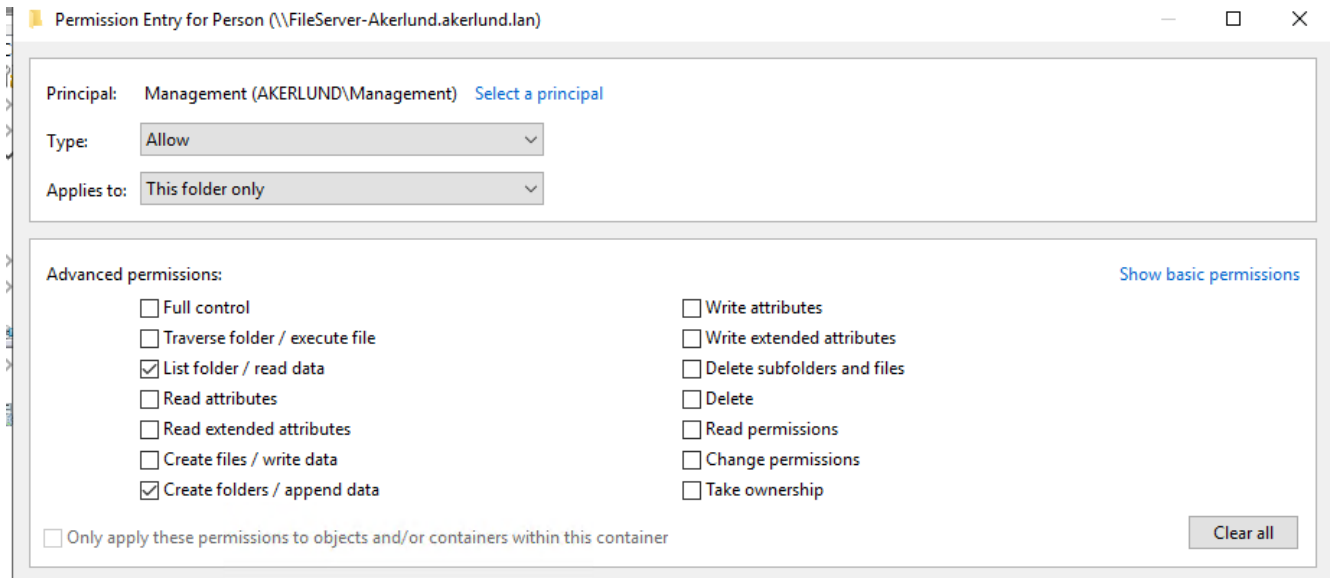
Johdanto

Tämän viikon harjoituksessa on tarkoitus tutustua ryhmäkäytänteihin ja soveltaa niitä omaan toimialueeseen. Viikon tehtävässä luodaan uusia ryhmäkäytänteitä ja linkitetään ne aktiivihakemistossa oleviin organisaatioyksikköihin. Käytännössä määritämme eri käyttäjille ja tietokoneille ”sääntöjä” miten ne toimivat toimialueellani.

Verkkojakojen pääsyoikeudet

Tehtävässä 4 loimme 2 verkkojakoa tiedostopalvelimelle. Tässä tehtävässä määritetään pääsyoikeudet verkkojaoille seuraavasti: Management ja Domain admins ryhmällä on pääsy molempiin verkkojakoihin. Muilla käyttäjillä on vain pääsy toiseen verkkojakoon ”Data”.

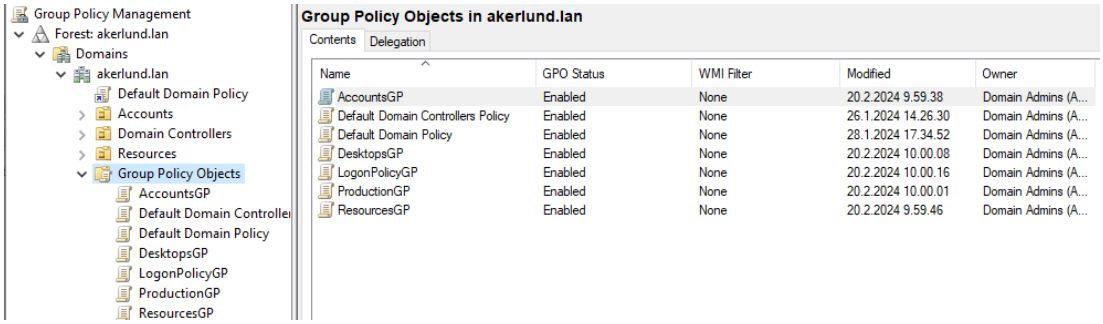
Verkkojaolle ”Person” muutetaan käyttöoikeudet siten että poistetaan periytyvät käyttöoikeudet kansiosta ja lisätään manuaalisesti ”management” ryhmälle oikeudet nähdä kansiot ja luoda uusia kansioita. Tämä tapahtuu Tiedostopalvelimen computer management valikosta. Teen siis muutokset etänä ohjauspalvelimelta.

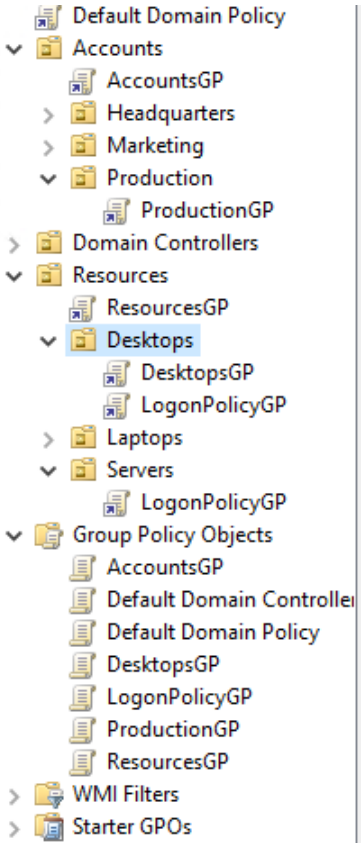


Viimeistelynä lisään ryhmän ”management” jakoluetteloon että oikeudet tulevat verkon yli käyttäjille.

Ryhmäkäytäntöjen lisäys

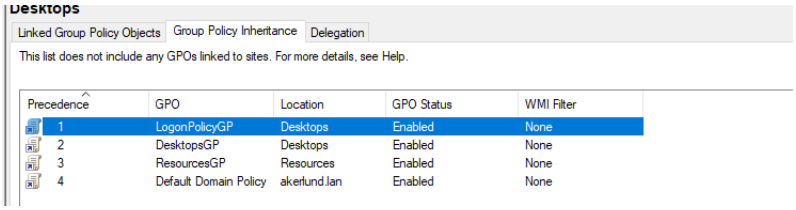
Aloitan luomaan ryhmäkäytänteitä eri ryhmille. Tämä tapahtuu ohjauspalvelimelta ”Group Policy Management” valikosta. Luon 5 uutta ryhmäkäytännettä: AccountsGP, ResourcersGP, ProductionGP, DesktopsGP ja LogonPolicyGP. Luon ne kansioon Group Policy Objects.





Juuri luomani ryhmäkäytänteet eivät ole vielä missään käytössä. Seuraavaksi linkitän käytänteet oikeisiin ryhmiin. Vieressä kuvankaappaus toteutuksesta.

Resources ryhmän sisällä on useita ryhmäkäytänteitä. Tarkastan että oikeudet periytyvät oikein ja että prioriteettijärjestys on oikein. Voin tehdä tämän tarkastamalla ”Group Policy Inheritance” valikon:



Tämä varmistaa sen, että jos ryhmäkäytänteissä on päällekkäisiä määrityksiä ryhmä priorisoi käytänteet oikein.

Ryhmäkäytäntöjen sisältö

Aloitamme muokkaamalla Default Domain Policy käytännettä. Muokkauksia tehdään Group Policy editorilla ja etsimme valikoista oikeat vaihtoehdot. Default Domain Policy muokataan siten että otetaan pois internet Explorer varoitukset. Tämä tapahtuu ottamalla Internet asetuksista pois vaihtoehdon Protected Mode. Lisäksi otetaan käyttöön salasanavaatimuksen kirjautumiseen, otetaan interaktiivinen kirjautuminen käyttöön (Ei vaadita Ctrl+Alt+Del kirjautumisen yhteydessä) ja sallitaan skriptien ajaminen etänä tai paikallisesti.

LogonPolicyGP ryhmäkäytänteelle tehdään seuraavat määritykset: Always wait for the network at computer startup and logon (Enabled),Do not display network selection UI (Enabled)

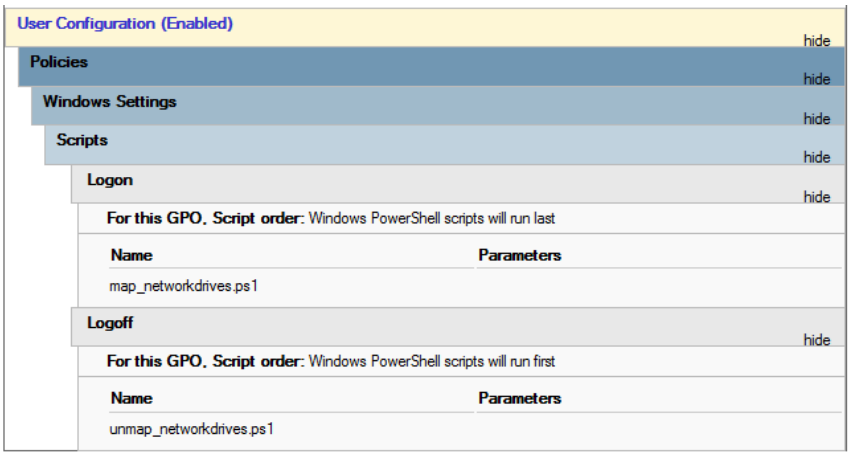
DesktopsGP käytänteellä määritetään seuraava asetus: Interactive logon: Don't display last signed-in (Enabled), Enforce user logon restrictions (Enabled), Maximum lifetime for user ticket renewal (3 days).

DeskTopsGP käytänteelle määritetään verkkojakojen automaattinen mappaus: Turn on Mapper I/O (LTTDIO) driver, Turn on Responder (RSPNDR) driver.

AccountsGP käytänteelle määritämme muutaman Powershell scriptin ajamisen kirjautumisen yhteydessä. Luon powershell scriptin kansioon ” C:\Windows\SYSVOL\domain\Policies\{unique id}\User\Scripts\Logon\”. Scripti sisältää verkkojaon mappauksen. Scripti näyttää seuraavanlaiselta:

```powershell
# MUOKKAA TÄTÄ ARVOA
# EDIT THIS VALUE

$fileServer = "FileServer-Esimerkki.esimerkki.lan"

########################################
# Network share details

$SMBShare = @(
  @{
    LocalDrive = "I:"
    ShareName  = "Data"
    FileServer = $fileServer
    ADGroups   = @()
  },
  @{
    LocalDrive = "J:"
    ShareName  = "Person"
    FileServer = $fileServer
    ADGroups = @("Management", "Domain Admins")
  }

####################################
# Get currently logged-in user information

$user      = [System.Security.Principal.WindowsIdentity]::GetCurrent()
$principal = New-Object System.Security.Principal.WindowsPrincipal($user)

####################################
# Assign network share to a new local
# drive letter on the target client computer

function Set-NetworkShare ($LocalDrive, $FileServer, $ShareName) {
  Invoke-Command -ScriptBlock {
    net use $LocalDrive ("\\" + $FileServer + "\" + $ShareName)
  }
}

###############

for ($i = 0; $i -lt $SMBShare.Length; $i++) {

  if ($SMBShare[$i].ADGroups.Length -eq 0) {
    Set-NetworkShare `
    -LocalDrive $SMBShare[$i].LocalDrive `
    -FileServer $SMBShare[$i].FileServer `
    -ShareName $SMBShare[$i].ShareName

  } else {
    for ($a = 0; $a -lt $SMBShare[$i].ADGroups.Length; $a++) {

      if ($principal.IsInRole($SMBShare[$i].ADGroups[$a])) {

        Set-NetworkShare `
        -LocalDrive $SMBShare[$i].LocalDrive `
        -FileServer $SMBShare[$i].FileServer `
        -ShareName $SMBShare[$i].ShareName
      }
    }
  }
}
```

Scriptistä muutan vielä verkkojakoni nimen. Joka on ”FileServer-Akerlund.Akerlund.lan”. Ryhmäkäytänteenstä otan skriptin ajamisen kirjautumisen yhteydessä. Uloskirjautumisen yhteydessä ”Unmap_networkdrives.ps1” Skripti ajetaan. Tarkastan lopputuloksen group policy editorista.



Tässä vaiheessa huomasin, että määritykset eivät näkynyt asetuksissa heti. Suljin editorin ja käynnistin uudestaan, jolloin määritykset näkyivät.

Yhteenveto

Viikon tehtävässä tehtiin ryhmäkäytänteitä ja määritettiin niille asetuksia. Lisäksi tutustuin powerskriptien liittämiseen ryhmäkäytänteihin. Huomasin tässä vaiheessa, että tämä on huomattavasti tehokkaampi tapa toteuttaa eri toimintoja. Tietenkin tämä on huomattavasti myös haastavampi.