6.4.1. ABE - 2

Friday, December 12, 2025 20:21

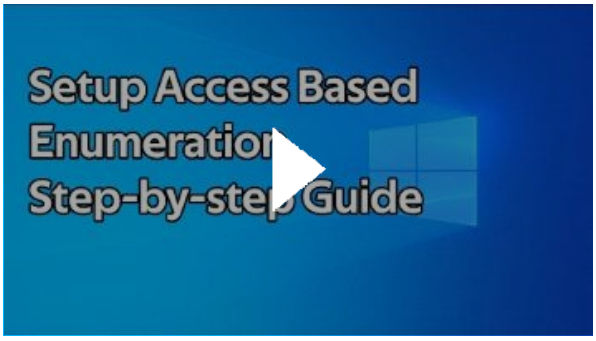
Tämä on harjotus demo, koskien mitä videossa menekään ja harjoitus jatkuu - **Access-Based Enumeration Explained + Hands-On Lab (Windows Server) - Final ton youtube videon playlist listan mukaan.**

Access-based enumeration - ABE

- Windows serverissä oleva joka pilottaa tiedostoa ja kansiota käyttäjältä kenellä EI OLE OIKEUTTA siihen.
- Ainoastaan käyttäjällä on oikeus niihin ja nähdä tiettyjä kansioita, mihin hänellä on oikeus.

Access-Based Enumeration (ABE) on Windows-tiedostopalvelimilla on ominaisuus, joka suodattaa tiedostojen ja kansioiden listauksia niin, että käyttäjät näkevät vain ne kohteet, joihin heillä on käyttöoikeudet (luku- tai listausoikeus), piilottaen muut kohteet automaattisesti, mikä parantaa turvallisuutta ja helpottaa tiedonhallintaa estämällä käyttäjiä näkemästä heille kuulumattomia tiedostoja. ABE ei mu uta varsinaisia käyttöoikeuksia, vaan muuttaa näkyvyyttä ja toimii jaetuissa kansioissa SMB-protokollalla.

Harjoitus demo:
How to enable Access Based Enumeration
Access-Based Enumeration Explained + Hands-On Lab (Windows Server)



OMA DEMO OHJE VIDEON MUKAAN - START HERE;

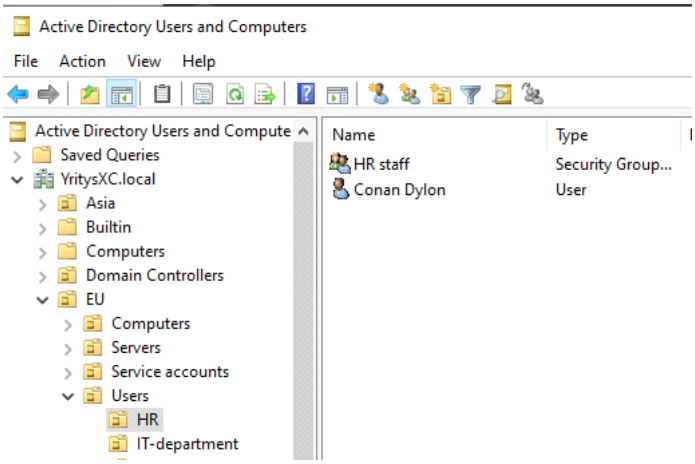
Scenario:

- Luodaan pien simuloiva esim. SHARED (jaettu levy), josta 3 kansiota kuten HR/IT/yhteinen kansio. HR näkee oman HR kansionsa ja IT näkee omansa, että kolmas kansio esim. HR/IT näkee sen *yhteisen kansion*.

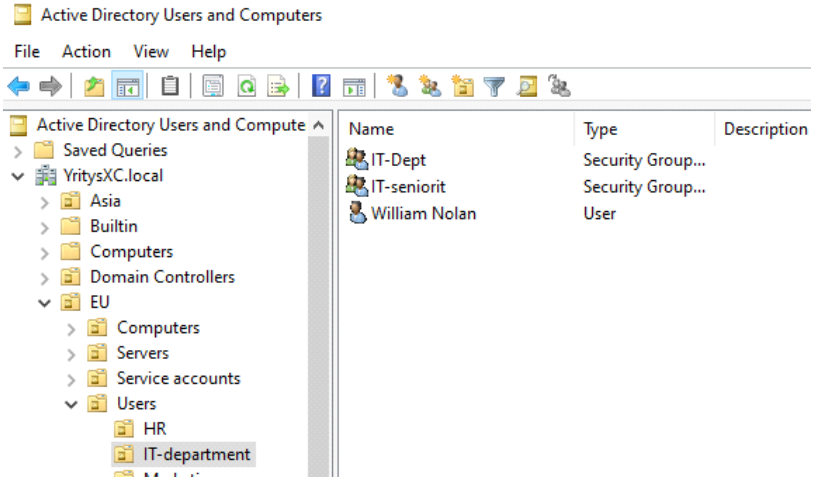
Step 1: SET UP USERS AND GROUPS IN AD (ACTIVE DIRECTORY)

Tässä on esim. Valmis pohja ja nimestä itse saa vapaasti rakentaa ja luo ryhmänsä, että käyttäjä on ryhmän alla.

- Ryhmät pitää olla käyttäen "Group scope (global)" ja "tyyppi" (Security).



Tässä IT yksikköstä käytettään **(IT-Dept)**.



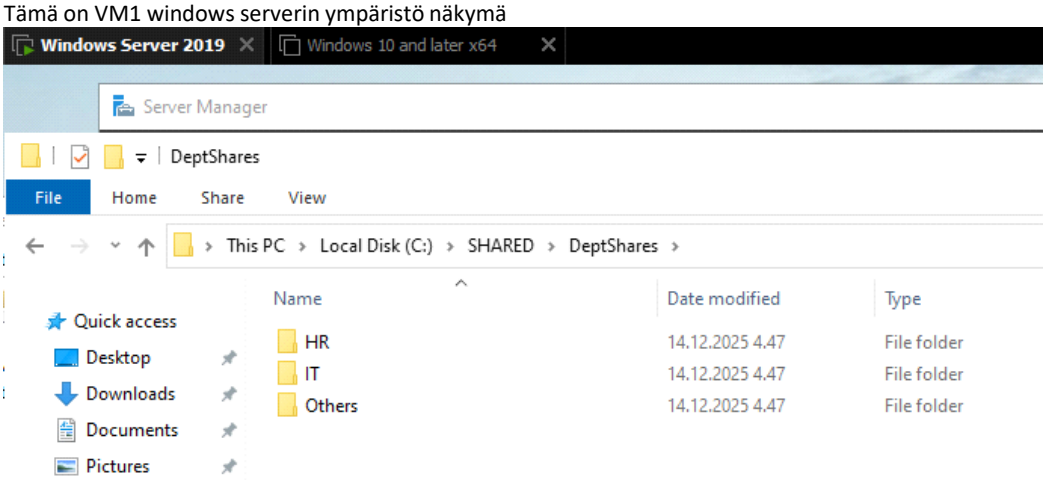
STEP 2: CHREATE SHARED FOLDER WITH SUBFOLDERS

HUOM. Tämä on koskien tuota jaettua kansiota, josta levystä on jaettu yhteinen levy (**SHARED**) tästä on harjoitus (5.2.) ohje ja kertauksena on hiekkalaatikkon/Vmworkstation ympäristö jaettu tiedosto levy.

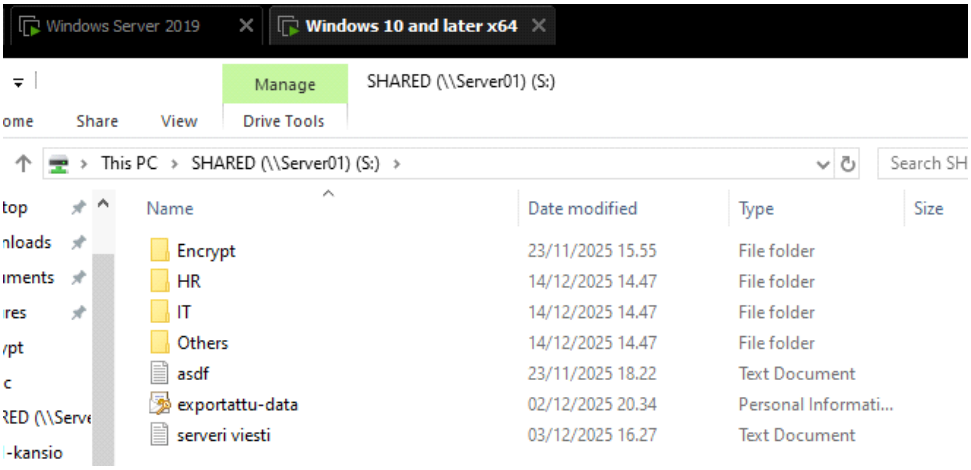
Luodaan esim. Jaettu (SHARED) alle yksi pääkansio joka toimii kuin parent-child kansio, että tässä on **jaettu yhteinen kansio** nimike vaikappa - ja nimeämisellä kannattaa olla tarkanna vaikka onkin harjoitus menetelmä.

- Jos tosi elämässä niin pitää suunnittella/rakentaa/toteuttaa - että henkilökunta/hallinto löytää kyseisen kansion polun.

Tämä on VM1 windows serverin ympäristö näkymä



Tämä on VM2 tavallisen käyttäjän näkymä kansiosta

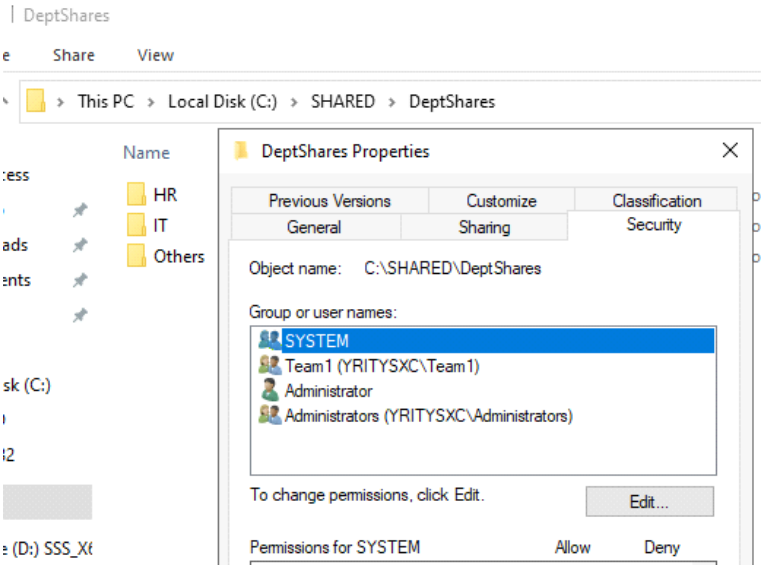


STEP 3: SET NTFS PERMISSIONS

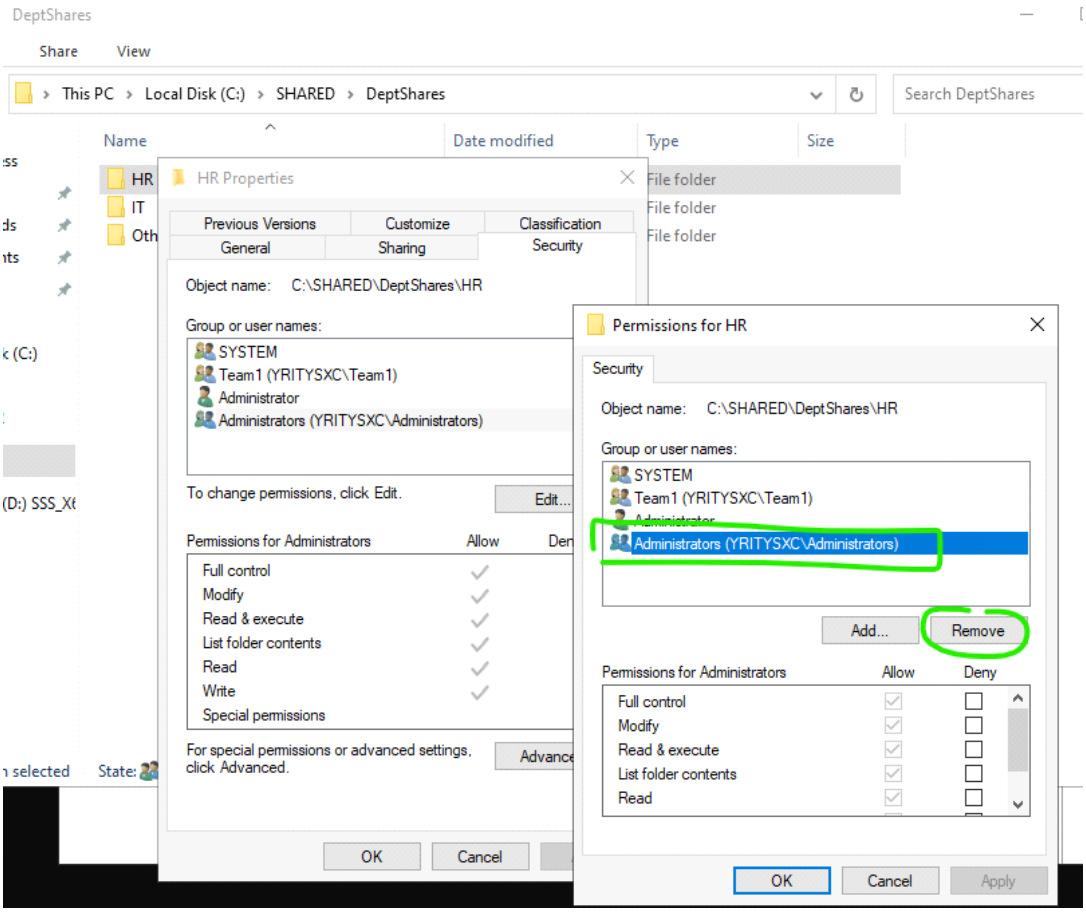
Seuraavaksi asetettaan tämä (SHARED/DeptShares) alikansioon (IT & HR) kansiolle NTFS permission oikeutta.

Aloitettaan esim. HR:stä ja oikean hiiren klikkaus (properties) >> security -polkuun.

- Tämä on oletus näkymänsä, mutta tähän (group or user names:) alle nimettään vain HR:llä on oikeus pääsy tähän kansion.
- Administrators (oma yritysverkkoalue\Administrators) - tämä tarkoittaa kaikkilla siis oman yritysverkko alueella on pääsy tähän kansioon.

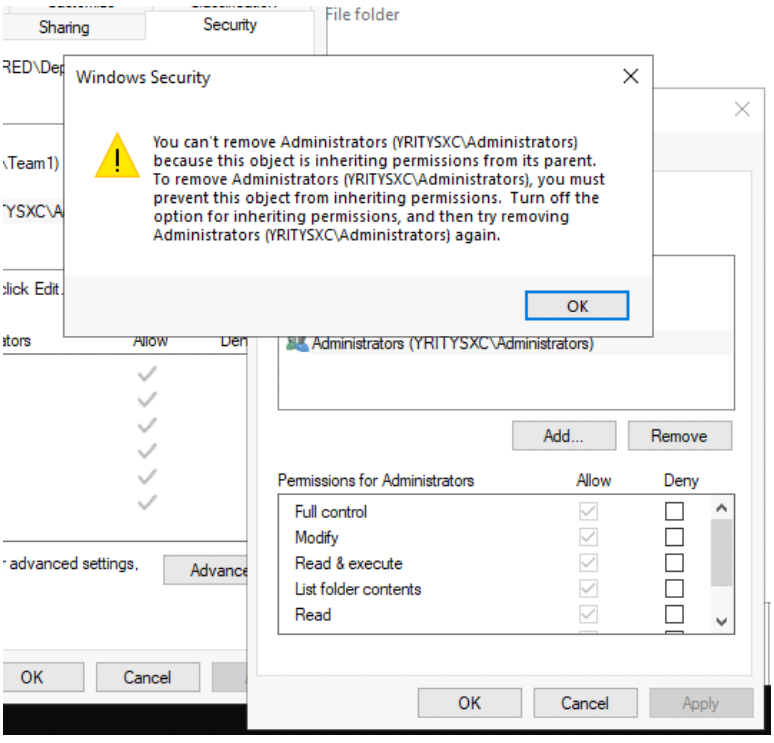


Avataan (edit) - ja poistettaan (Administrators (OMAYRITYSVERKKOALUE\Administrators)

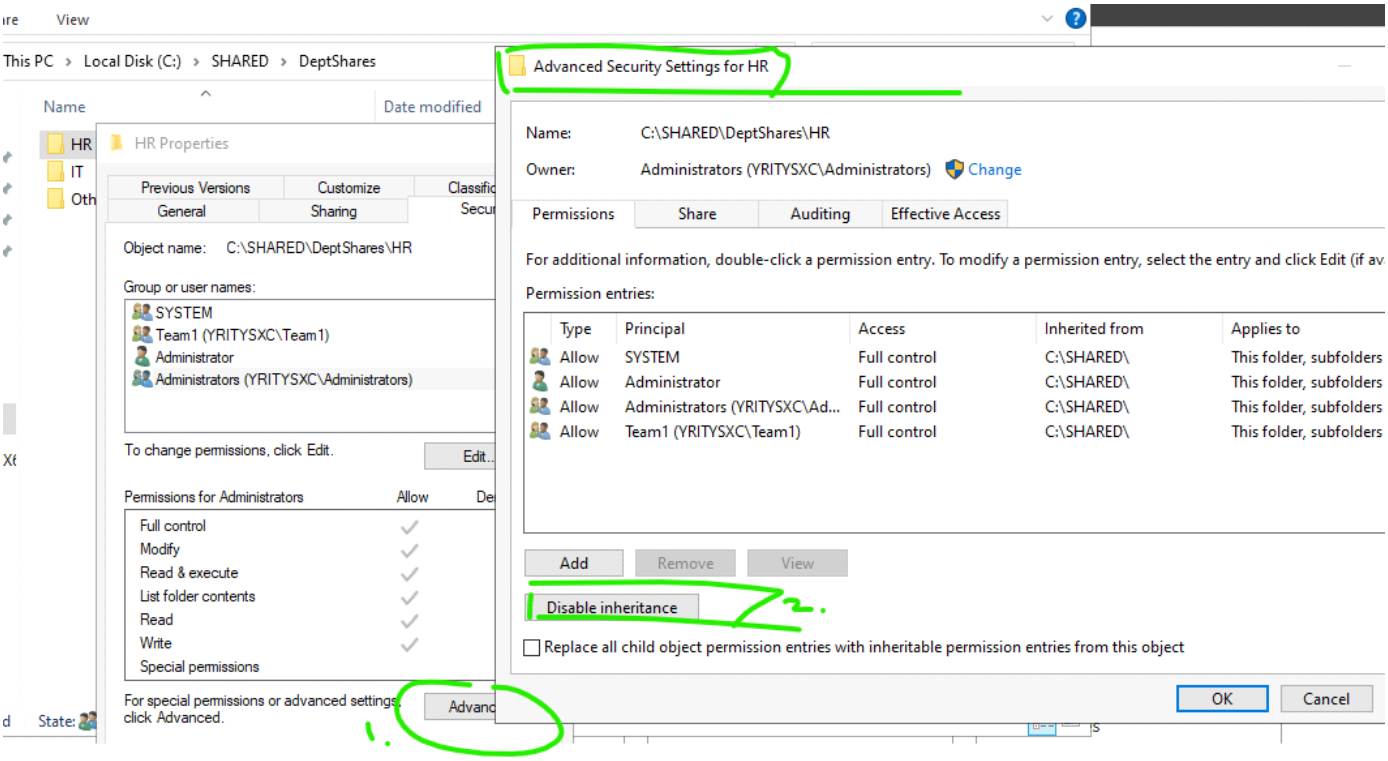


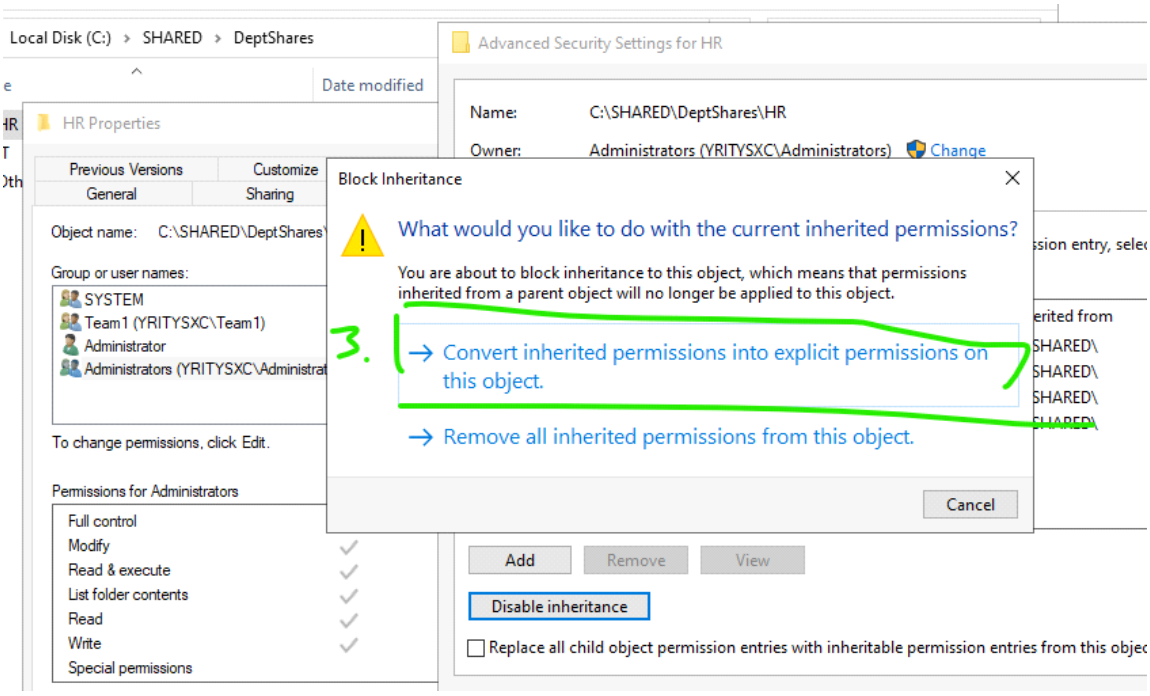
Siitä sen jälkeen tulee ponnahtaa pieni ilmoitus

- Se antaa vain varoituksen ettei tätä pysty poistaa koska perimisen oikeudesta koska sen kansio parent:istä.
- Joten joudutaan poistaa tästä "administrator" tästä kansion asetuksesta kikka kolmosella.
- Avataan "advanced" asetuksesta



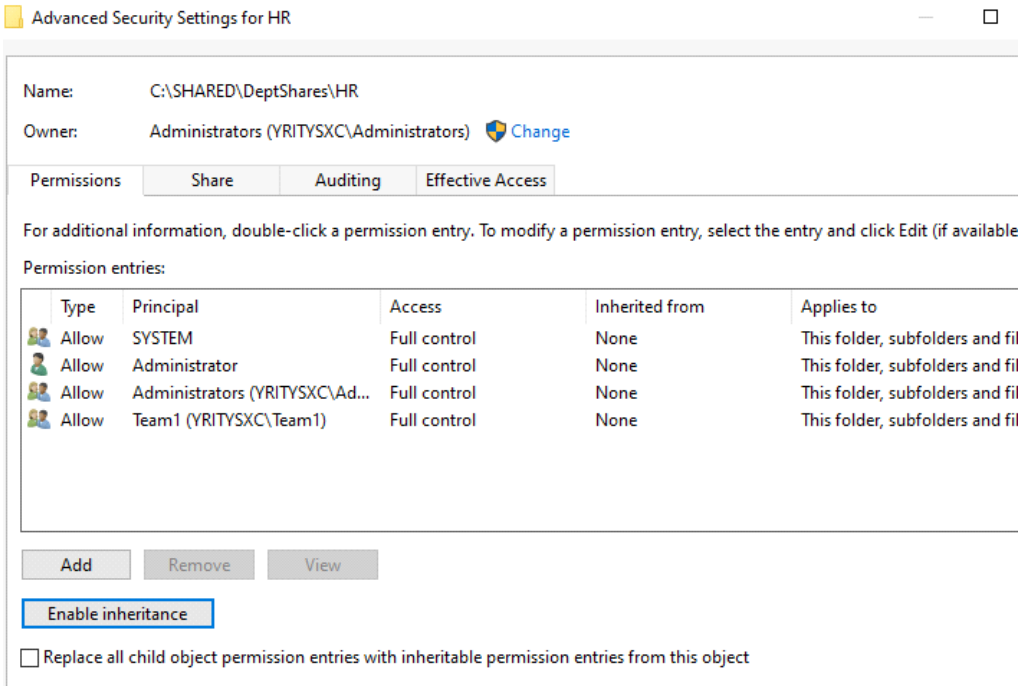
Tästä valittaan "disable inheritance" asetus ja siitä ensimmäinen vaihtoehto.



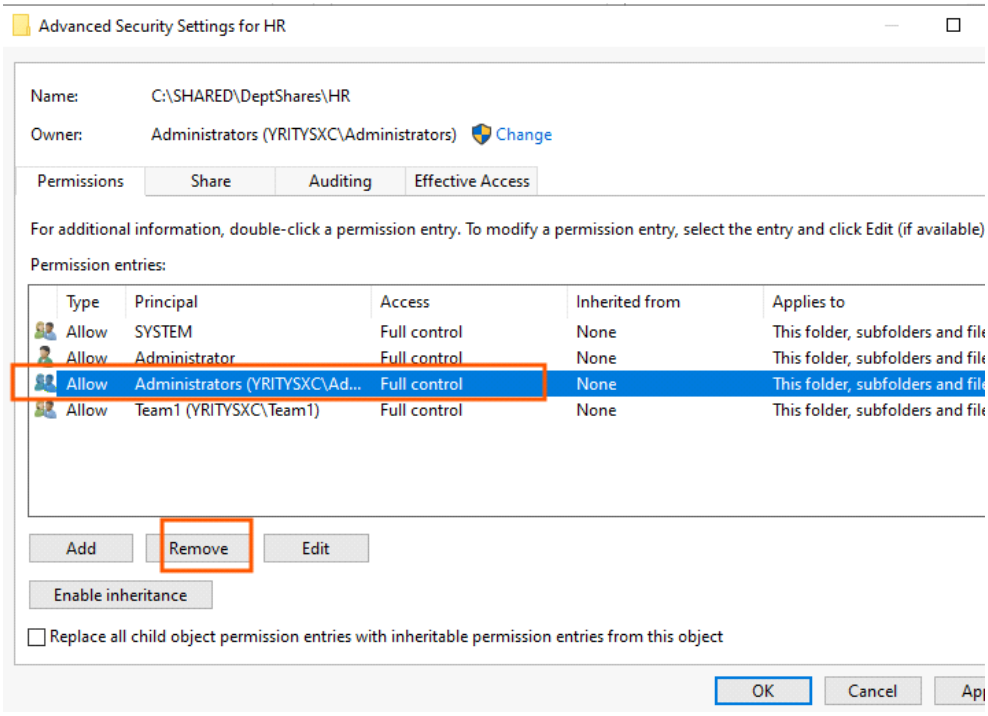


Tästä huomataan muutoksensa

- Poistettaan "yritysverkkoalueen\administrator"

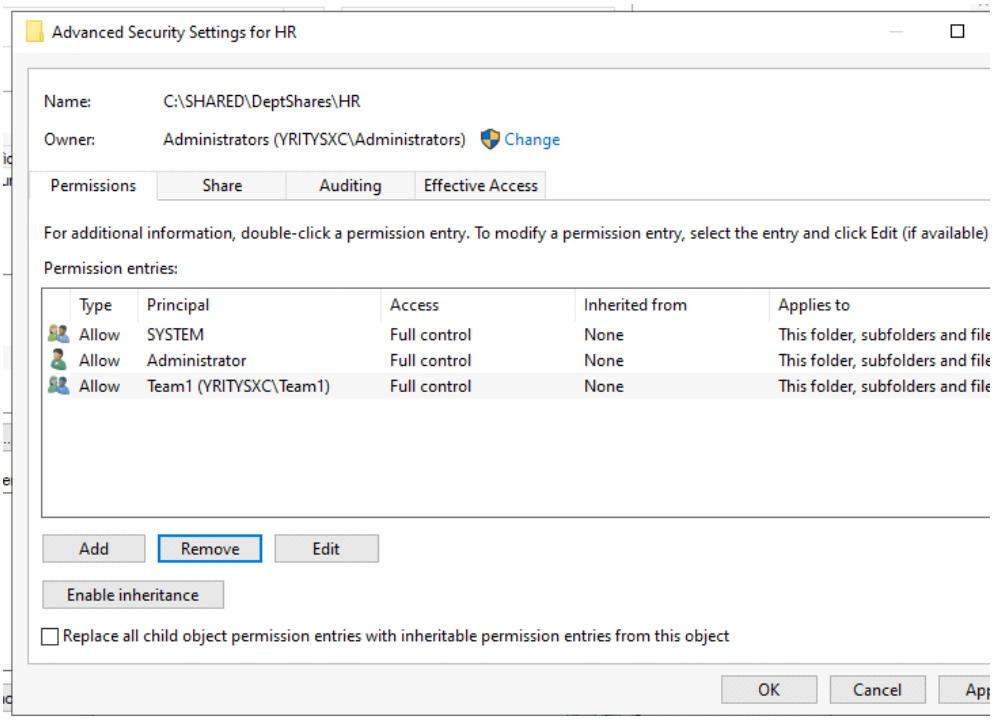


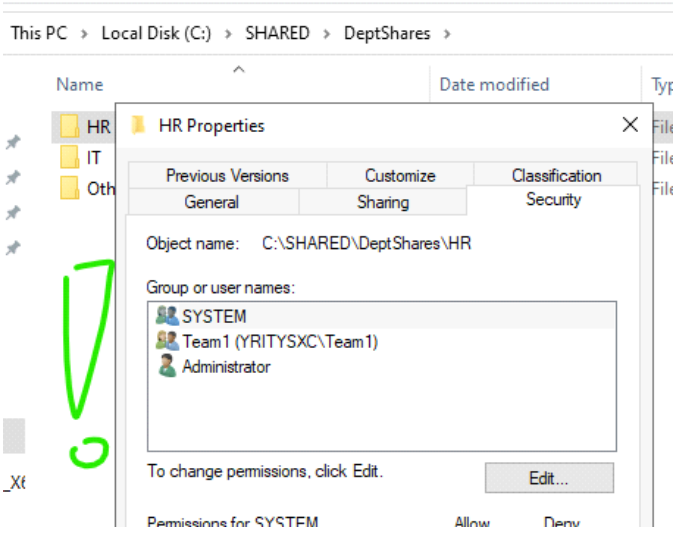
BEFORE:



AFTER:

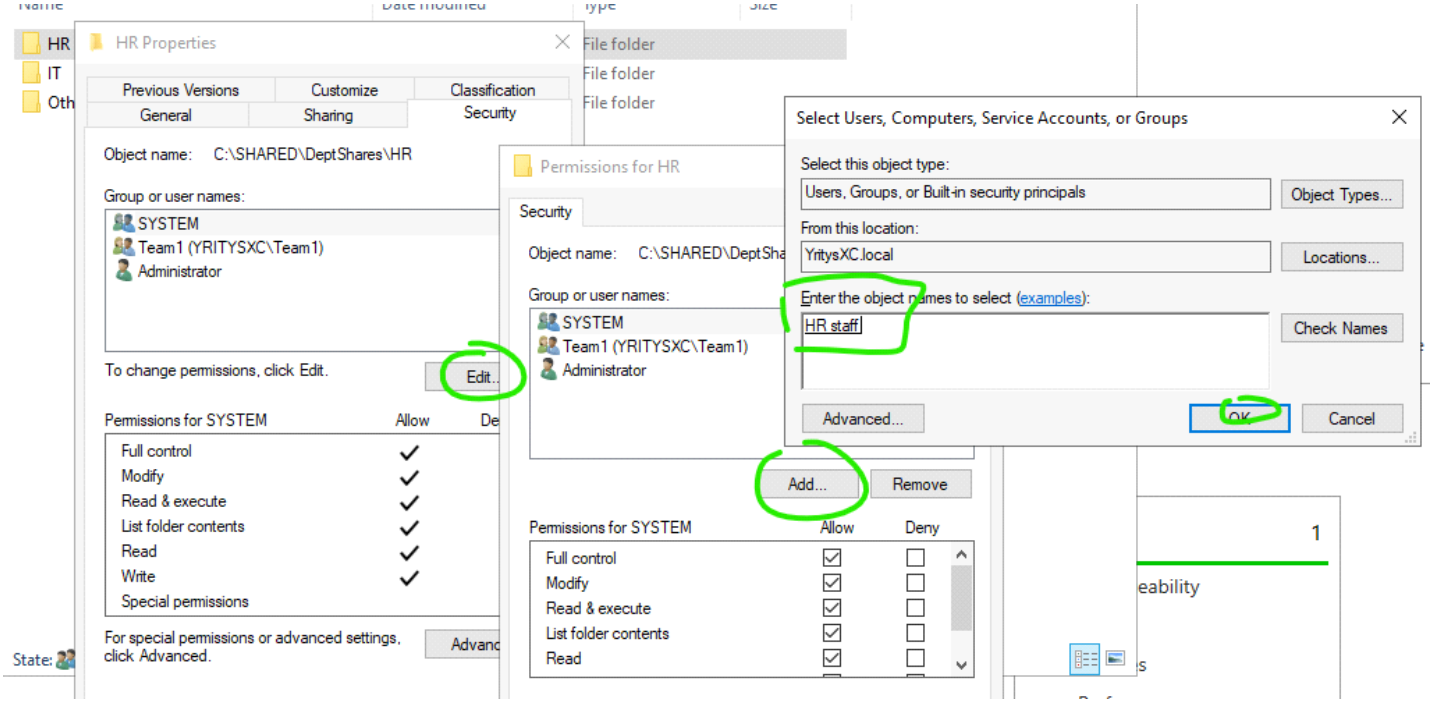
- Apply ja OK

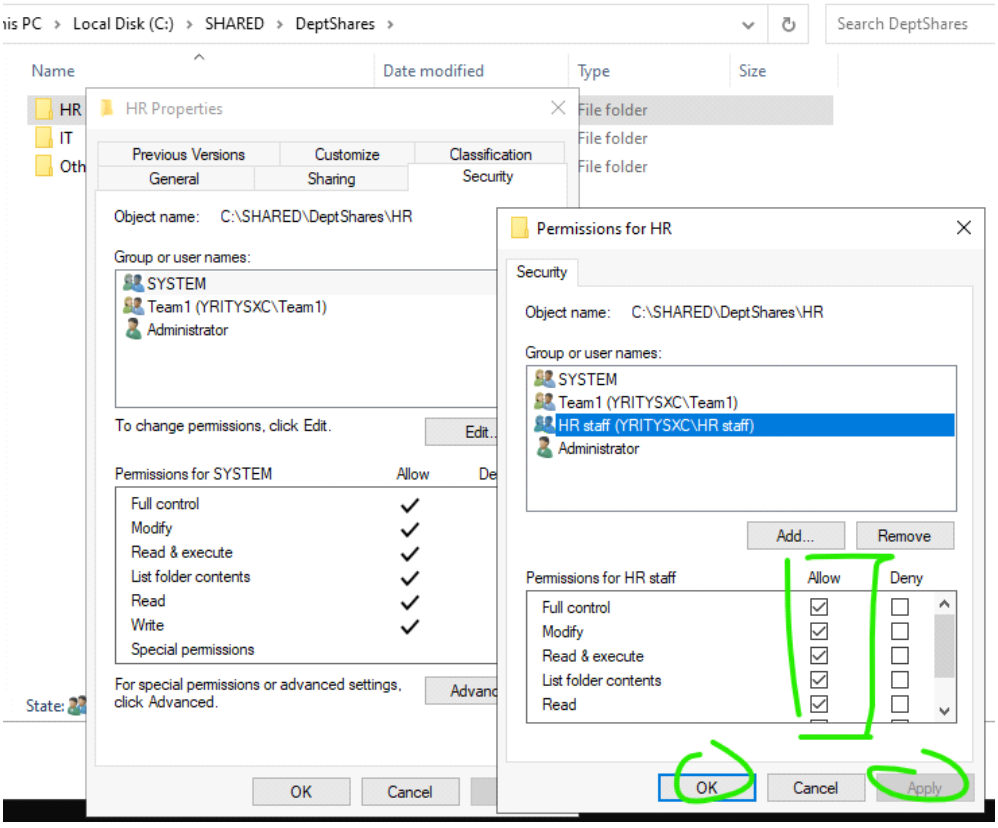


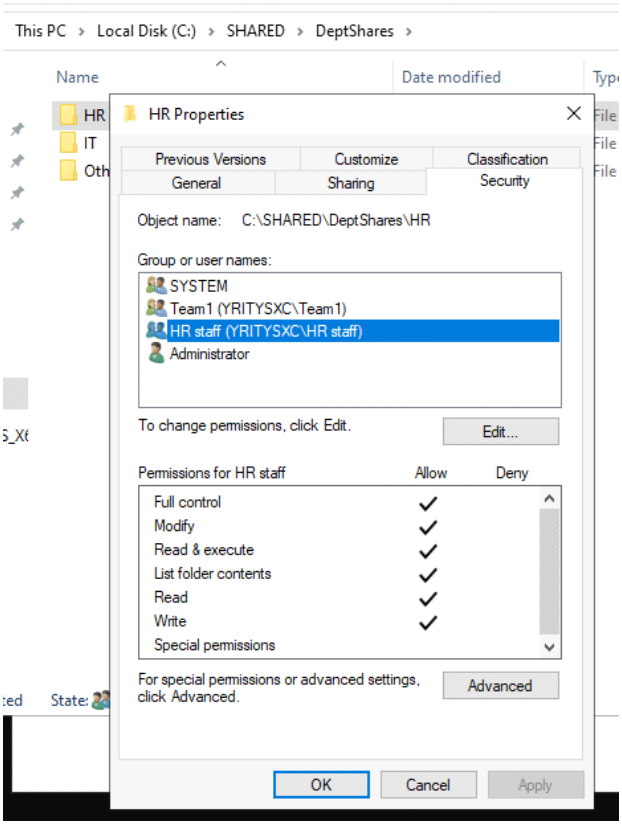


Nyt lisätään se HR tähän ryhmityksen alle. Eli nyt (ylemmän kuvan mukaan) "edit"

- Ja täys oikeudet (Full control) HR henkilökunnille.
- Apply ja OK


HR Properties
Previous Versions
Customize
Classification
General
Sharing
Security
Object name: C:\SHARED\DeptShares\HR
Group or user names:
SYSTEM
Team1 (YRITYSXC\Team1)
Administrator
To change permissions, click Edit.
Edit...
Permissions for SYSTEM
Allow
Full control
Modify
Read & execute
List folder contents
Read
Write
Special permissions
For special permissions or advanced settings, click Advanced.
Permissions for HR
Security
Object name: C:\SHARED\DeptSha
Group or user names:
SYSTEM
Team1 (YRITYSXC\Team1)
Administrator
Add...
Remove
Permissions for SYSTEM
Allow
Deny
Full control
Modify
Read & execute
List folder contents
Read
Select Users, Computers, Service Accounts, or Groups
Select this object type:
Users, Groups, or Built-in security principals
Object Types...
From this location:
YritysXC.local
Locations...
Enter the object names to select (examples):
HR staff
Check Names
Advanced...
OK
Cancel

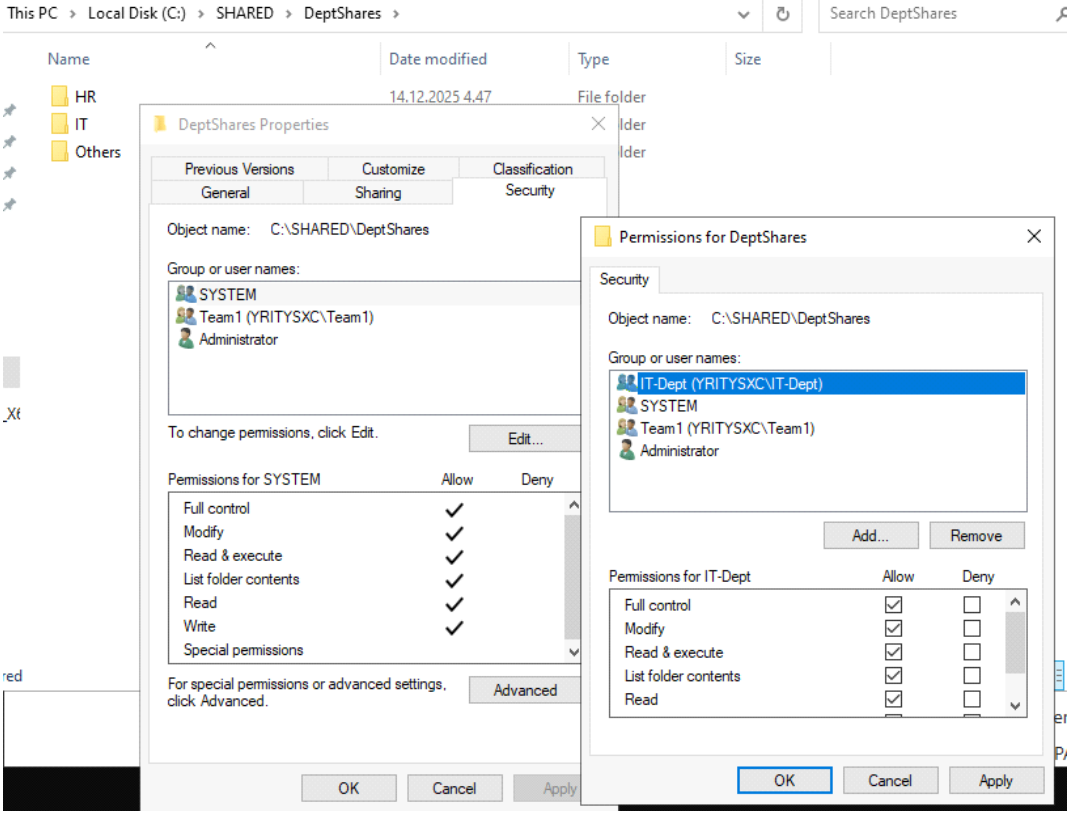

Search DeptShares
Name
Date modified
Type
Size
HR Properties
File folder
Previous Versions
Customize
Classification
General
Sharing
Security
Object name: C:\SHARED\DeptShares\HR
Group or user names:
SYSTEM
Team1 (YRITYSXC\Team1)
Administrator
To change permissions, click Edit.
Edit...
Permissions for SYSTEM
Allow
Full control
Modify
Read & execute
List folder contents
Read
Write
Special permissions
For special permissions or advanced settings, click Advanced.
OK
Cancel
Permissions for HR
Security
Object name: C:\SHARED\DeptShares\HR
Group or user names:
SYSTEM
Team1 (YRITYSXC\Team1)
HR staff (YRITYSXC\HR staff)
Administrator
Add...
Remove
Permissions for HR staff
Allow
Deny
Full control
Modify
Read & execute
List folder contents
Read
OK
Cancel
Apply



Ja tehdään tästä sama idea kuin (IT) kansiolle.
(välivaiheet skipattua) ei turhia toistoja ja kuin HR kansio asetuksien konfigurointi/määritys.

IT dept - ryhmille täys oikeudet

- Apply ja ok

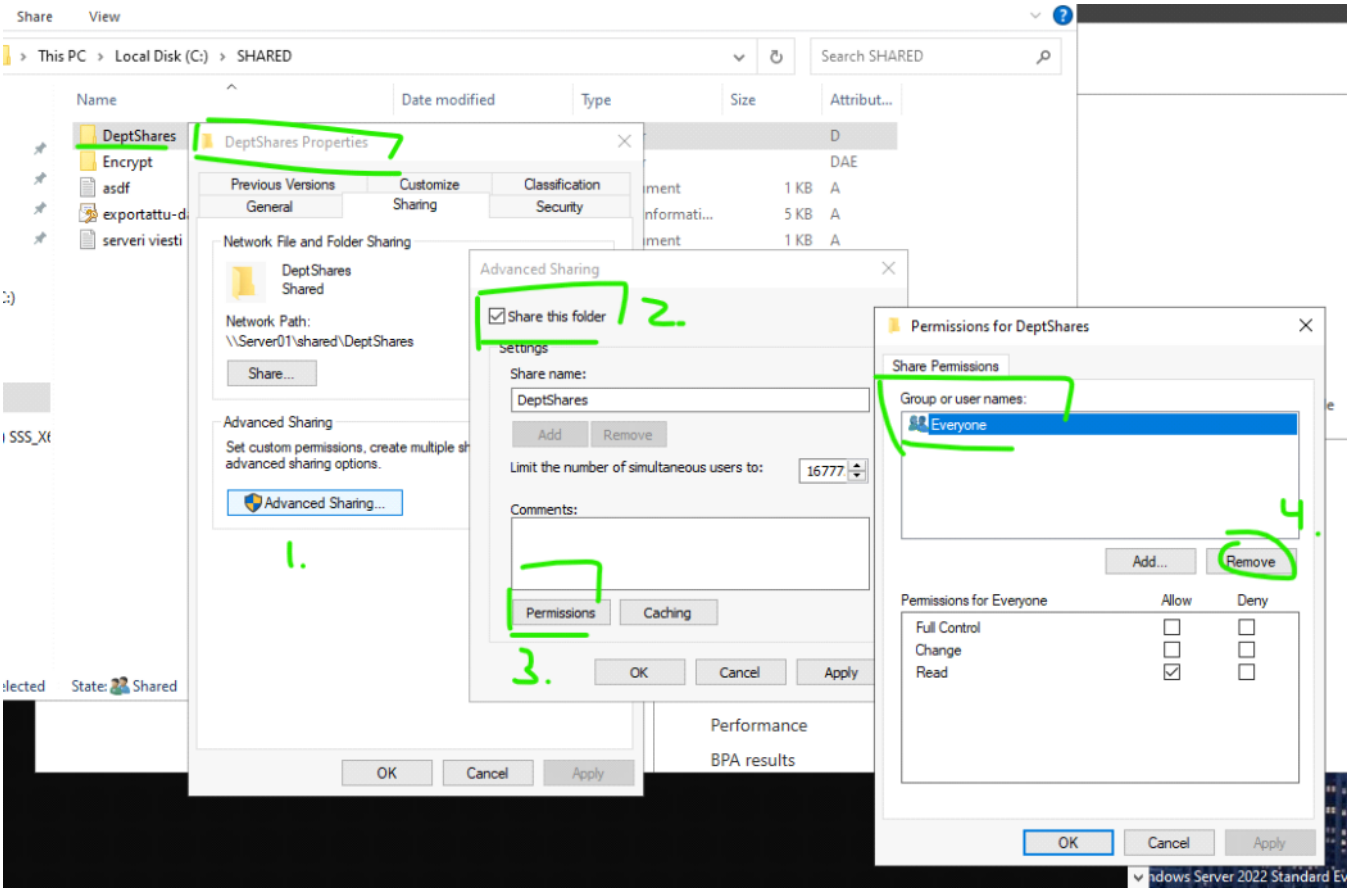


Nyt ollaan asetettu NTFS permission oikeudet näille molemmille kansioille (alikansio)

STEP 4: SHARE THE PARENT FOLDER

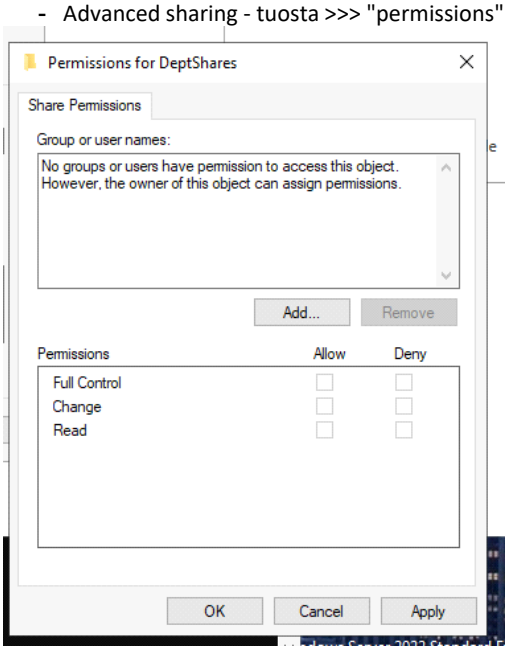
Eli jaettaan näille kahdelle kansioille tolle parenti oikeus eli "**DeptShares**".

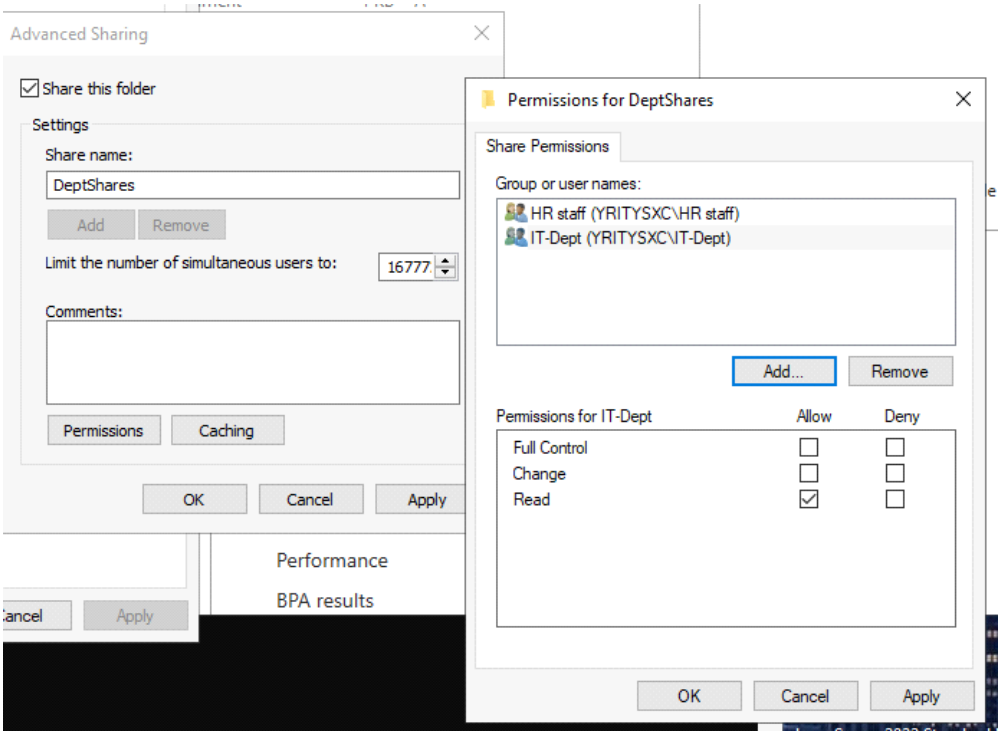
Tästä vaan kuvan mukaan, josta määritettään kansio on jaettava, että samalla poistettaan kuin ryhmitys on kaikkille poistettu



Seuraavaksi, lisätään tähän "DeptShares" kansioon HR ja IT ryhmät.

- Määritä molemmissa ryhmissä on vain "luku" oikeus
- Sitten apply ja OK (2x)
- Advanced sharing - tuosta >>> "permissions" tarkista IT ja HR ryhmät on lisätty alle ja on "read" oikeus.





Nyt kuitenkin HR/IT ryhmillä on oikeus päästäkseen "DeptShares" kansioon, mutta heillä on erikseen pääsy omaan kansioonsa eli pääsy nimettyyn oikeudet.

Viimeinen steppi jatkuu toisessa sivussa :: 6.4.2. ABE -3