

6.4.2. ABE -3

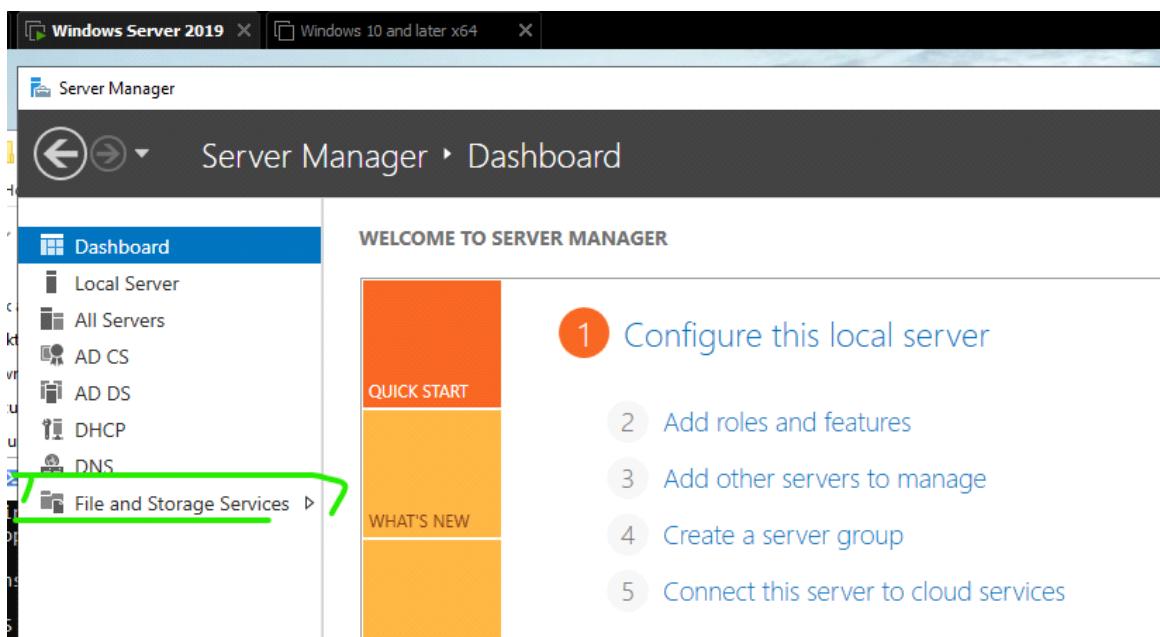
Sunday, December 14, 2025 15:39

Harjoitus steppi jatkuu aikaisemmasta sivusta - 6.4.1. ABE - 2

STEP 5: ENABLE ACCESS-BASED ENUMERATION (ABE)

Viimeinen steppi.

Avataan Windows serverin toi (server manager) näkymänsä ja valitse (File and storage services)

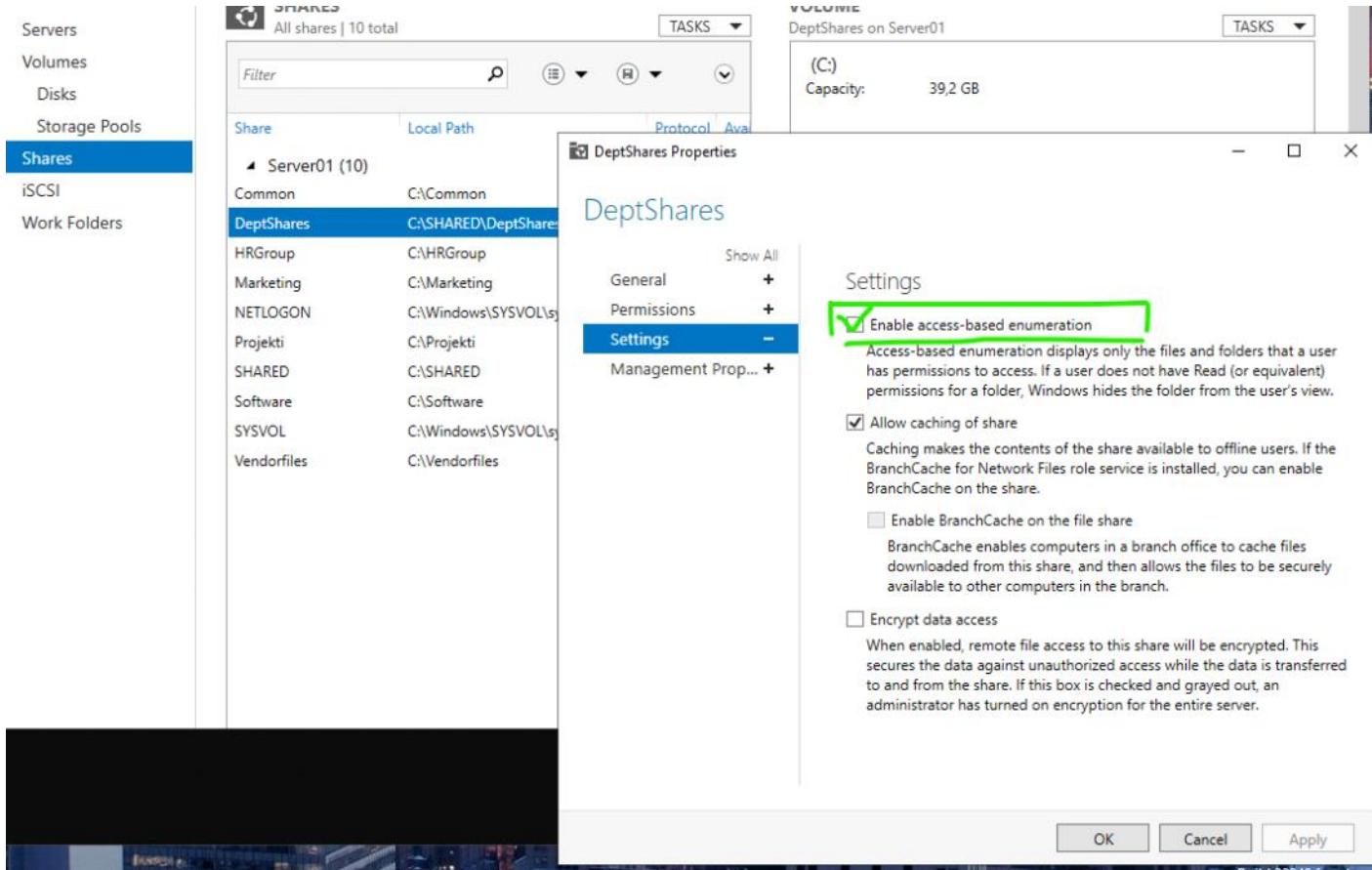


Polku (Shares) ja tästä nähdään näitä kansioita mitä on jaettuja pääkansioita esim. Omaan yritysverkkoalueelle / kuin haluttaan jakaa omaan organisaatioon.

- Valitaan toi "DeptShares" ja kaksois klikkaus (properties)

Tässä on se (ABE) enable access-based enumartion - tämä on se josta halutaan asettaa se **näkyvyyden vastuu oikeudesta** ja mihin ollaan asetettu ne kansion tyypit/ryhmät.

- Asettaaan se päälle ja sen pitäisi asettaa kaikkiin erilaisiin tiedostoihin ja kansioihin tämä toiminta.



FINAL STEP - TEST

Viimeisenä testaan että toimiiko ja avataan VM2 - ja kirjauduttaan noi aikaisemman luoneen käyttäjät eli:

- IT Dept - William Nola (Salasana123)
- HR staff - Conan Dylon (Salasana123)
- Molemmilla on sitten ensimmäisen kirjautumisen jälkeen luoda uusi salasana.

Voishan sitä kokeilla jos esim. Pääseekö esim. Ja jos on luonut <\\SERVER01> kansion niin sillä kautta päästään serveriin yhteyttä. Muistutuksena oman VM1 (windows server) pitää olla niin pääsee tuohon jaettuun kansion alle, että ei pääse ilman yhteyttä ja jos ei ole päällä.

Kirjauduttaan vaikappa HR tunnarilla sisään ja muistutus asetettiin admin käyttäjä , että käyttäjä ensimmäisen kirjautumisen jälkeen tulee asettaa uusi salasana.

- Conan Dylon (yritysxc\conan.dylon) - Salasana123 -- UUS PASS: P@ssw0rd

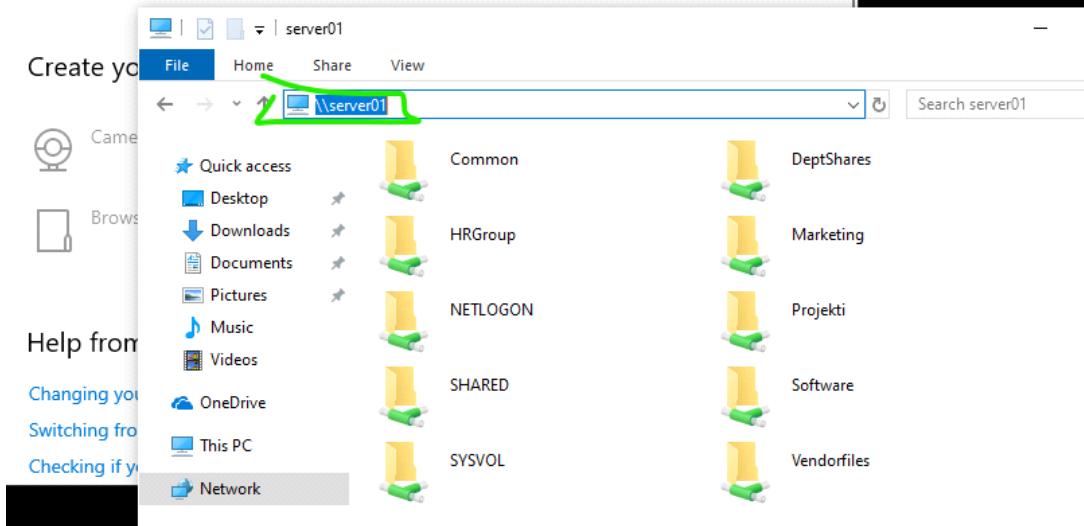
Aava oma "File explorer" (resurssienhallinta) kansio mikälie niin syötä polkuun <\\server01>

Your info



CONAN DYLON

YRITYSX\conan.dylon



Jos ei muista oma serveri nimee niin avaa VM1 windows serveristä

- Tässä on kaksi tapaa tarkistaa oman serverin nimensä, joko powershell tai tuosta "server manager" koneen nimestä.

Server Manager ▶ Local Server

PROPERTIES
For Server01

Computer name
Server01

Domain
YritysXC.local

Administrator: Windows PowerShell

PS C:\Users\Administrator> hostname

Server01

Kansiosta (DeptShares) siihen vaan / toinen metodi on jaettun levyn kautta >> DeptShares

Tämä on HR näkymänsä, ja lisättiin tollainen (pieni muutos) että esim. Eventti kansio perään.

- Pieni muistutus tämä HR (conan) henkilöllä on vain luku oikeus

DeptShares

File Home Share View

Pin to Quick access Copy Paste Cut Copy path Move to... Copy to... Delete Rename New folder New item... New Easy access... Properties

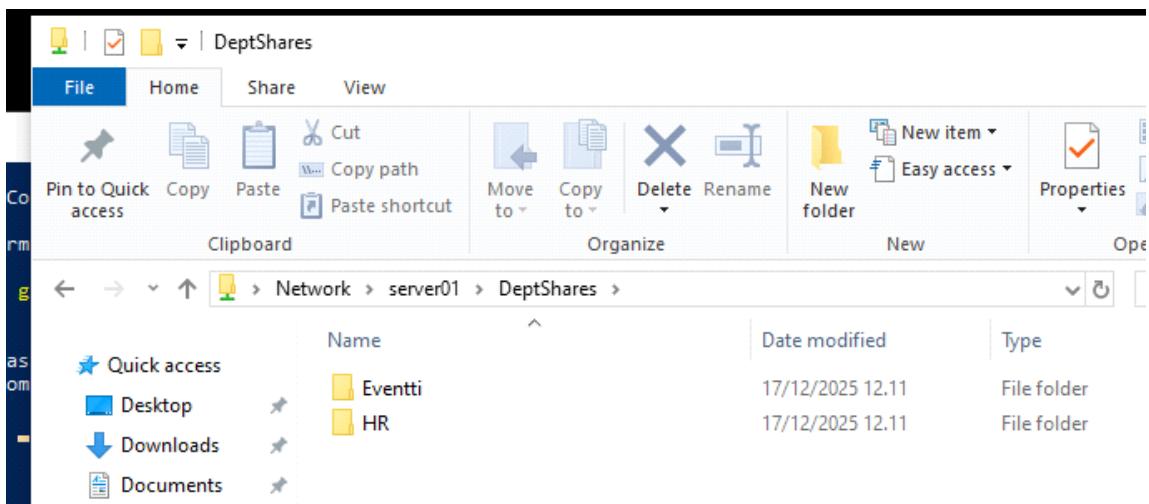
Clipboard

Organize

New

Open

Network > server01 > DeptShares >



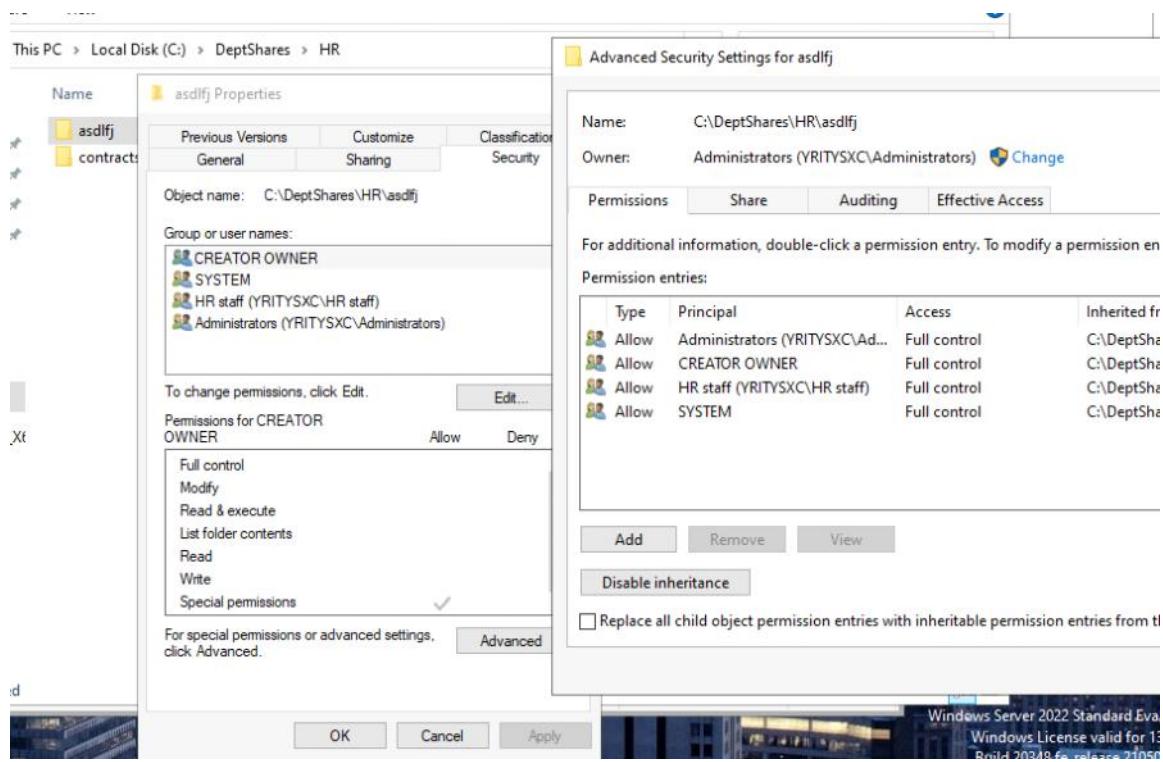
Palataan VM1 windows serveriin ja luo HR kansion alle alikansio (contracts) ja avaa properties

- Tässä nähdään contracts alikansiosista, että HR olla on vain oikeus ja jos IT osasto (IT-dept) ryhmästä ei pääse kuitenkaan HR kansion alle.
- Tämä oikeus antaa jatkuvasti seuraavalle alikansiolle kokoajan kun nyt (HR) kansio toimii kuin pää kansiona.

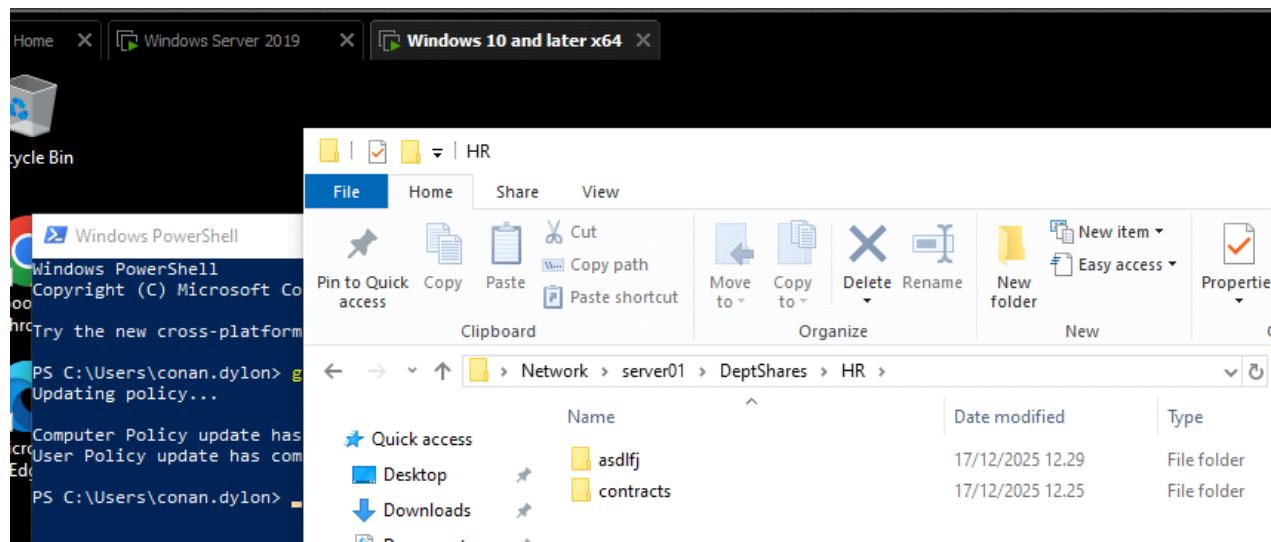
Type	Principal	Access
Allow	Administrators (YRITYSXC\Administrators)	Full control
Allow	CREATOR OWNER	Full control
Allow	HR staff (YRITYSXC\HR staff)	Full control
Allow	SYSTEM	Full control

Sama nytten loin sivuun toisen satunaisen kansion niin sillä tulee olemaan samat oikeudet, koska HR toimii kuin pääkansiona. Pääkansion sisällä alikansioille tulee samat oikeudet ja vain nimettyynä HR staff oikeudella. Tästä on hyvä muokka esim. Tarvittaessa on kirjoitus oikeus että HR jäsenet voivat esim. Muokata/lisätä/poistaa tiedostoja.

- Tämä on sama idea kuin toinen kansio (DeptShares/IT)



Tästäkin pikainen tarkistus huomattaan ja kirjauduttu HR (Conan) käyttäjään niin nähdään se toinen alikansio



PIENI YHTEENVETO JA OMA PIENI POHDINTA - START HERE;

ABE (Access-Based Enumeration) on Windows-ympäristön ominaisuus, joka vaikuttaa siihen, mitä jaettuja kansioita käyttäjä näkee verkkossa. Käytännössä tämä tarkoittaa, että käyttäjä näkee vain ne kansiot, joihin hänenlä on oikeudet – muut kansiot pysyvät piilossa. Tämä voi olla erityisen hyödyllistä organisaatioissa, joissa on paljon jaettuja resursseja eri tiimeille, kuten HR:lle, IT:lle, myynti, laskutus tai jopa muu hallinnon jäsenille.

Esimerkiksi:

- <\\server01\HR> näkyy vain HR-tiimin jäsenille
- <\\server01\IT> näkyy vain IT-tiimille

ABE ei muuta käyttöoikeuksia, vaan vaikuttaa vain **näkyvyteen**. Tämä vähentää virheellisiä klikkauksia ja parantaa käyttäjäkokemusta, etenkin etäyhteyksissä VPN:n kautta tai pilvipalveluissa kuten SharePointissa.

Vertailun kohteena SharePoint ja tällaisia Microsoft pilvipalvelujen kansio ja muu tiedosto kaltaisesta, josta yrityksen oma henkilökunta voi nähdä uutiskirjeitä, yrityksen omia ajankohtaista tietoa, koulutusta, sopimusta ja jne kansioiden alta. Vertailuna tähän Windows ABE menetelmänsä se on täysin erilainen, koska ABE:ssa kaikki materiaalit on serverissa. Jos halutaisiin ottaa kaikki varmuuskopiot niin joudutaisiin jatkuvasti tehdä varmuuskopio jatkuvasti esim. Viikkotain/kuukausittain - jos serveristä tapahtuu muuta kuormitusta. Pilvipalvelujen osalta kaikki on verkostossa, että vain yhteydellä pääsee kiinni ja kirjautumalla omalla tunnuksella.

Oma pieni kommentti: Harjoituksen aikana huomattua, että ABE tekee jaettujen resurssien käytöstä vähä selkeämpää ja turvallisempi. Se auttaa hahmottamaan, mihin se oikeus ja mihin ei, ilman että tarvitsee kokeilla jokaista kansiota erikseen. Käyttäjän osalta osat kansom näkyvyydestä vain nimetyt ovat näkyvillä, ettei muut ovat piilossa. Oikeudesta uskoisin pitää lisätä sinne tiimin alle, jotta käyttäjällä on oikeus nähdä sitä pilottettua kansioita.

Samaan pätee Windows serveristä jos yritys, että yksittäiset yksikköiden/osasto aikovat ottaa tämän ABE näkyvyden toiminnan, niin administrator itsensä pitää dokumentoida järkevään paikkaan ja kaikki administrator kuuluvat henkilöt tietävät tämän prosessin.

⌚ ABE vs. Microsoftin pilvipalvelut (SharePoint & OneDrive)

Ominaisuus / Näkökulma	ABE (Windows Server)	SharePoint / OneDrive (Microsoft 365)
Käyttäjän näkyvyys	Näkee vain kansiot, joihin on käyttöoikeus (ABE pilottaa muut)	Näkee jaetut tiedostot/kansiot, mutta voi nähdä tiedoston nimen, vaikka ei olisi oikeuksia
Käyttöoikeuksien hallinta	Perustuu NTFS-oikeuksiin ja ryhmäjäsenyyksiin	Perustuu SharePointin tai OneDriven jakamisoikeuksiin ja Azure AD -ryhmiin
Tietoturva	Hyvä näkyvyden hallinta, mutta vaatii VPN-yhteyden etäkäytössä	Pilvipohjainen, toimii ilman VPN:ää, mutta jakaminen voi olla riskialttiimpaa, jos ei hallita kunnolla
Varmuuskopiointi	Vaatii erilliset backup-ratkaisut (esim. viikoittain)	Microsoft hoitaa taustalla versionhallinnan ja varmuuskopioinnin pilvessä
Käyttökokemus	Perinteinen, vaatii verkkoasemien käyttöä	Moderna, toimii selaimessa ja mobiilissa, integroitu Teamsiin ja muihin työkaluihin
Skaalautuvuus ja yhteistyö	Rajallinen, vaatii IT-tukea ja manuaalista hallintaa	Erinomainen: reaalialkainen yhteistyö, versiohistoria, kommentointi, jakaminen

Sources:

🔍 Yhteenveto

- **ABE sopii hyvin suljettuihin, roolipohjaisiin ympäristöihin**, joissa halutaan minimoida näkyvyys ja pitää tiedostot tiukasti hallinnassa.
- **SharePoint ja OneDrive taas sopivat paremmin avoimeen yhteistyöhön**, etätyöhön ja skaalautuvaan tiedonhallintaan – mutta vaativat huolellista jakamiskäytäntöjen hallintaa.
- **Varmuuskopioi kaikki jaetut resurssit riippumatta siitä, näkyvätkö ne ABE:n kautta vai eivät.**
- Käytä automaattista varmuuskopointia (esim. viikoittain tai kuukausittain), ja varmista että backup-järjestelmä ei perustu pelkkään käyttäjän näkyvyyteen.
- Dokumentoi, mitkä kansiot ovat pilottettuja ABE:n kautta, jotta ne eivät jää huomaamatta backup-suunnitelmassa.