

# TOIMIALUEEN HALLINTA

Noa Julkunen

## Sisällys

Harjoitus 1 .....	2
Virtuaalikoneen asennus .....	2
Virtuaalikoneen verkkoasetukset .....	2
Harjoitus 2 .....	4
Toimialueen luominen .....	4
Harjoitus 3 .....	6
Työaseman asennus .....	6
Harjoitus 4 .....	6
Työaseman liittäminen toimialueeseen .....	6
Harjoitus 5 .....	8
Active Directoryn hallinta .....	8
Hallintatunnuksen luonti Active Directory Users and Computers .....	9
USERS-kansion luonti ja jakaminen .....	10
Käyttäjätilien luonti .....	11
Käyttäjien liittäminen omaan ryhmäänsä .....	11
Käyttäjätilien toiminnan testaus .....	11
Harjoitus 6 .....	11
Kansioden jakaminen ja käyttöoikeuksien määrittäminen .....	11
Kansioden käyttöoikeuksien määrittäminen .....	11
Kansioden käyttöoikeuksien testaus .....	12
Harjoitus 7 .....	15
Ryhmäkäytäntöjen hallinta .....	15
Salasanakäytäntöjen muokkaaminen .....	15
Pasila OU:n ryhmäkäytäntöjen muokkaus .....	17
Verkkolevyn Talous kiinnittäminen T – kirjaimeen .....	19
Kyber OU:n ryhmäkäytäntö .....	21
Pilvi OU:n ryhmäkäytäntö .....	21
Pasila OU:n palomuurisääntö .....	23

## Harjoitus 1

### Virtuaalikoneen asennus

Luodaan Virtualboxiin uusi virtuaalikone alla olevan taulukon tietojen mukaisesti.

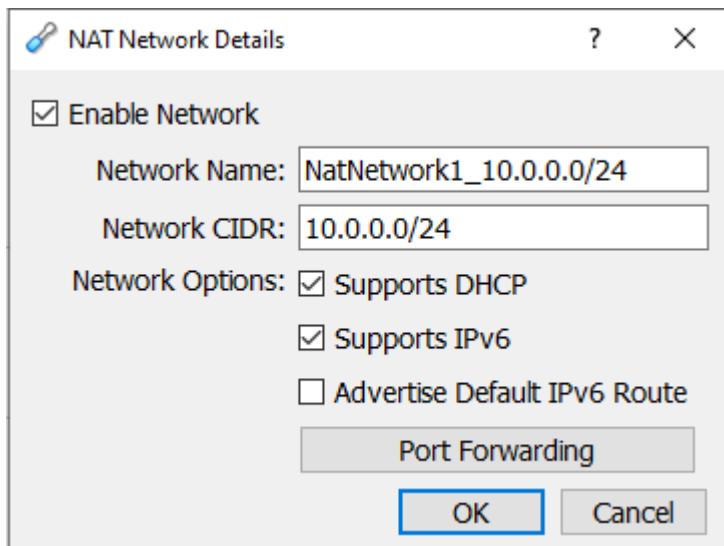
Nimi	Apollo
Käyttöjärjestelmä	Windows 2016 64-bit
Muistin määrä	2048 MB
Kiintolevy	VDI, 40 GB
Näyttömuistin määrä	128 MB
Enable 3D Acceleration	Kyllä
Salasana	Passw0rd\$
Versio	Windows Server 2016 Standard (Desktop Experience)

### Virtuaalikoneen asetukset

Kun uusi virtuaalikone on luotu, määritetään sille Windows Server 2016 .ISO tiedosto käynnistyksen yhteydessä.

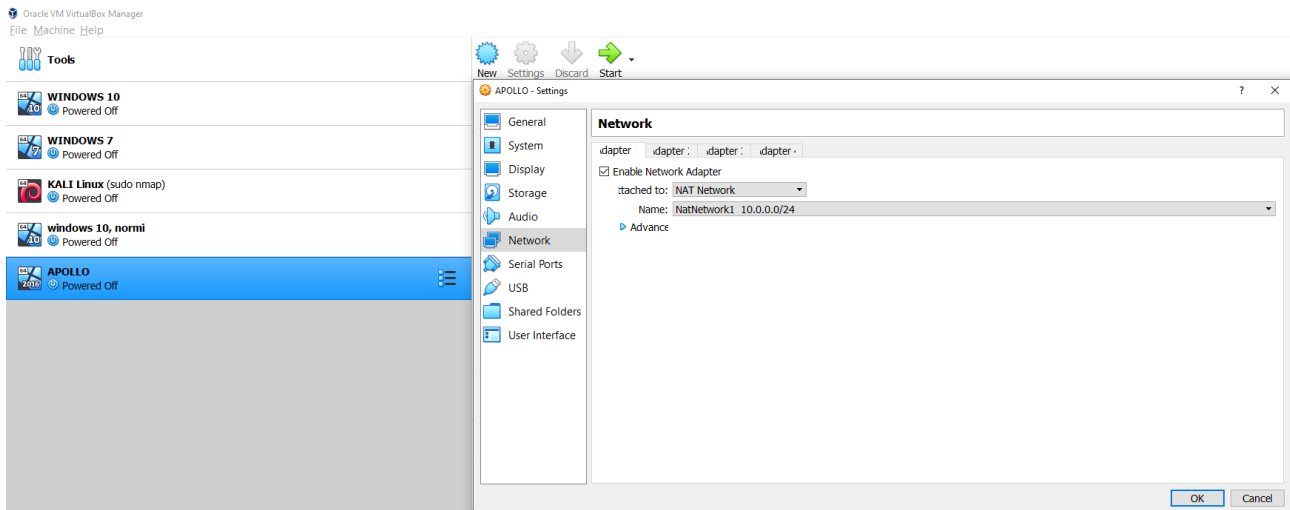
### Virtuaalikoneen verkkoasetukset

Luodaan uusi NAT Network Virtualboxiin (File > Preferences > Network)



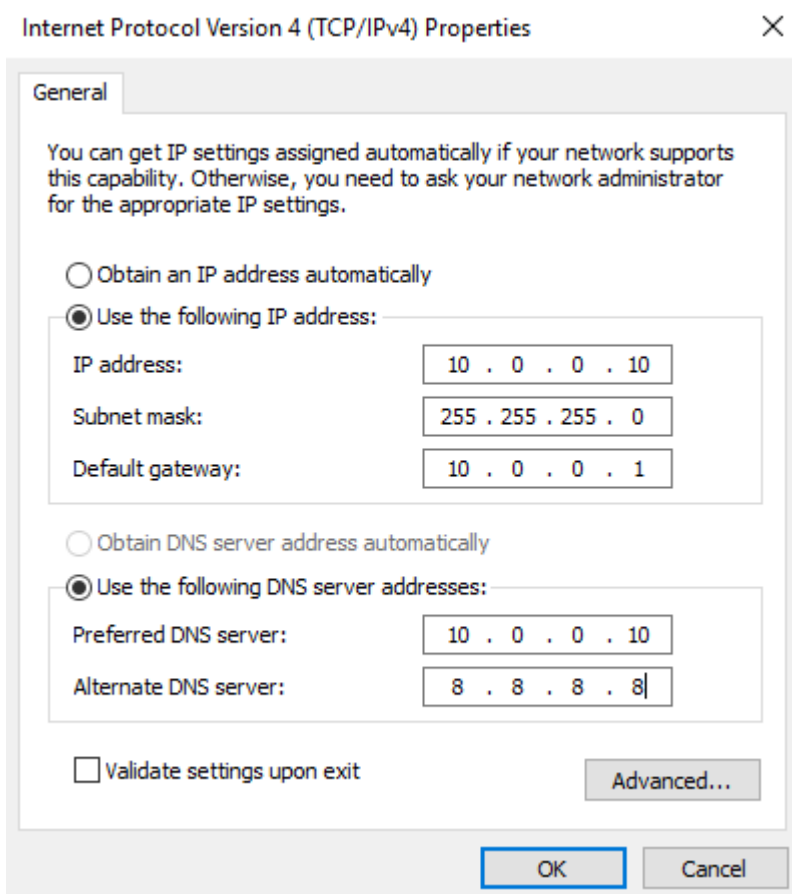
### NAT Networkin asetukset Virtualboxissa

Otetaan luotu NAT Network käyttöön virtuaalikoneelle (Virtuaalikoneen asetukset > Network) ja muutetaan Adapter 1 asetukset vastaamaan alla olevaa kuvaa.



Virtuaalikoneen verkkoasetukset Virtualboxissa

Muokataan virtuaalikoneen verkkoasetuksia vastaamaan alla olevaa kuvaa.



Virtuaalikoneen verkkoasetukset koneella

## Harjoitus 2

### Toimialueen luominen

Luodaan toimialue virtuaalikoneella Server Manager-ohjelmassa. Manage > Add Roles And Features kohta määritetään alla olevan taulukon mukaisesti.

Before You Begin	Next
Installation Type	Role-based or feature-based installation
Server Selection	Varmista että serverin IP-osoite on 10.0.0.10
Server Roles	Active Directory Domain Services
Features	Next
Confirmation	Restart the destination server automatically if required & Install

Add Roles And Features – kohdat

Annetaan toimialueella seuraavaksi nimi (Notifications > Promote this server to a domain controller) ja muuta aukeutuvan ikkunan sisältö vastaamaan alla olevaa kuvaa.

The screenshot shows the 'Active Directory Domain Services Configuration Wizard' window. The title bar reads 'Active Directory Domain Services Configuration Wizard'. The main window has a left-hand navigation pane with the following items: 'Deployment Configuration' (highlighted in blue), 'Domain Controller Options', 'Additional Options', 'Paths', 'Review Options', 'Prerequisites Check', 'Installation', and 'Results'. The main content area is titled 'Deployment Configuration' and shows the 'TARGET SERVER APOLLO'. Under the heading 'Select the deployment operation', there are three radio button options: 'Add a domain controller to an existing domain', 'Add a new domain to an existing forest', and 'Add a new forest' (which is selected). Below this, under the heading 'Specify the domain information for this operation', there is a text box labeled 'Root domain name:' containing the text 'cyberse.local'. At the bottom of the window, there are four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'. A link 'More about deployment configurations' is also visible at the bottom left of the main content area.

Deployment Configuration

Seuraavaksi avautuneen ikkunan sisällön tulisi vastata alla olevaa kuvaa. Salasana toimii Passw0rd\$.

### Domain Controller Options

DNS Options – kohtaan Next ja Additional Options kohdassa varmistetaan että The NetBIOS domain name on CYBERSE.

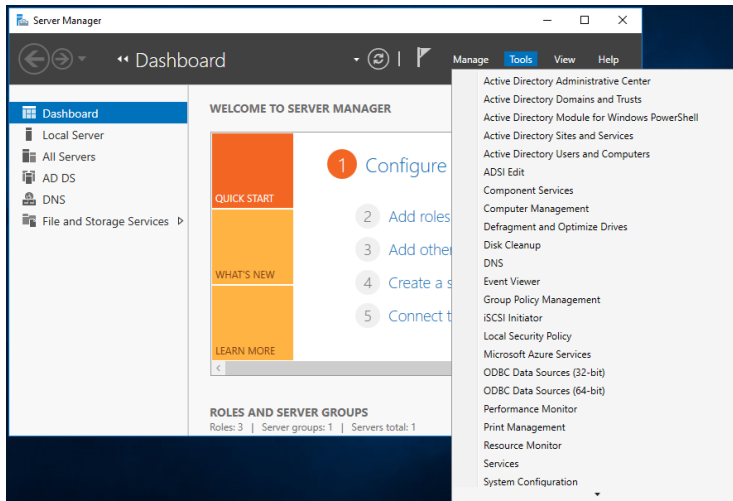
Alla olevassa taulukossa on listattu loput tarvittavat kohdat

DNS Options	Next
Addiotonal Options	The NetBIOS domain name = CYBERSE
Paths	Next
Review Options	Next
Prerequisites Check	Install

Loput kohdat

Virtuaalikone käynnistyy asennuksen aikana uudelleen.

Asennuksen jälkeen Server manager > Tools kohdassa pitäisi näkyä Active Directory- työkalut.



Active Directory – hallintatyökalut asennettuna

## Harjoitus 3

### Työaseman asennus

Luodaan Virtualboxiin toinen uusi virtuaalikone alla olevan taulukon tietojen mukaisesti.

Nimi	Win10
Käyttöjärjestelmä	Windows 10 (64-bit)
Muistin määrä	2048 MB
Kiintolevy	VDI, 40 GB
Näyttömuistin määrä	256 MB
Enable 3D Acceleration	Kyllä
Salasana	Passw0rd\$

Työaseman asetukset

Kun uusi virtuaalikone on luotu, määritetään sille Windows 10 .ISO tiedosto käynnistyksen yhteydessä.

## Harjoitus 4

### Työaseman liittäminen toimialueeseen

Varmistetaan että Työaseman IP-osoite on oikein, katso alla oleva kuva.

Preferred DNS server: Serverin IP-osoite.

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☐ Obtain an IP address automatically

☒ Use the following IP address:

IP address: 10 . 0 . 0 . 9

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 10 . 0 . 0 . 1

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server: 10 . 0 . 0 . 10

Alternative DNS server: . . . .

☐ Validate settings upon exit

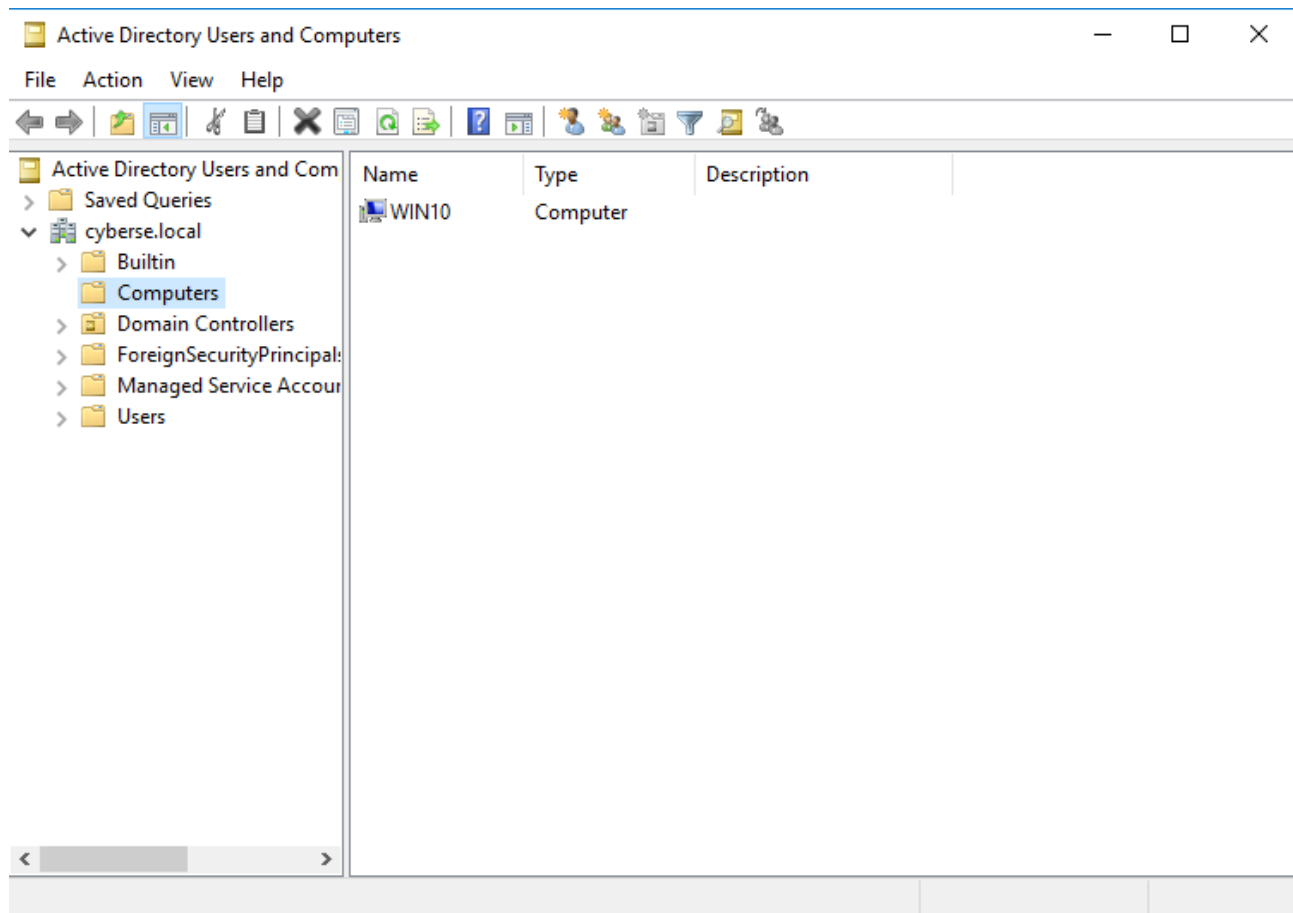
Advanced...

OK Cancel

Työaseman IP-osoite

Avataan Computer Name / Domain Changes (Control Panel > System And Security > System > Change Settings > Change) ja vaihdetaan Member of – kohta domainiksi ja domain on cyberse.local. Avautuvaan ikkunaan annetaan käyttäjänimeksi Administrator ja salasana Passw0rd\$. Työaseman uudelleen käynnistytksen jälkeen WIN10 tietokone näkyy Serverillä Active Directory Users and Computers – kohdassa.





Active Directory Users and Computers - näkymä

## Harjoitus 5

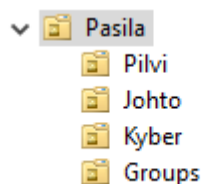
### Active Directoryn hallinta

Luodaan APOLLO-virtuaalikoneelle uusi Hard Disk (Virtualbox APOLLO Settings > Storage > Create New Disk) alla olevan taulukon tietojen mukaisesti.

Hard disk file type	VDI
Storage on physical hard disk	Dynamically allocated
File location and size	Default kansio & 40 GB

Uuden levyn tiedot

Avataan Active Directory Users and Computers (APOLLO-virtuaalikone > Server Manager > Tools Active Directory Users and Computers) ja luodaan uusi Organizational Unit (OU) nimellä Pasila. Seuraavaksi luodaan neljä OU:ta lisää Pasila OU:n sisään, katso alla oleva kuva.



Tarvittavat Organizational Unitit

Seuraavaksi luodaan Groups-kohdan alle seuraavat ryhmät (Group), joiden nimet on taulukossa vasemmalla puolella ja oikealla taulukossa ryhmän näkyvyys.

Palkanlaskenta	Domain local
Budjetin ylläpito	Domain local
Budjetin luku	Domain local
Hallinto	Global
Talous	Global
Palkat	Global
Cloud	Global
Cyber	Global

Tarvittavat ryhmät Groups – kohdassa

Hallintatunnuksen luonti Active Directory Users and Computers

Luodaan hallintatunnus kopioimalla Administrator (cyberse.local > Users) ja täytetään avautuvan ikkunan tiedot.

Copy Object - User

Create in: cyberse.local/Users

First name: Noa Initials: Admin

Last name: Julkunen

Full name: Noa Admin. Julkunen

User logon name: julkunen @cyberse.local

User logon name (pre-Windows 2000): CYBERSE\julkunen

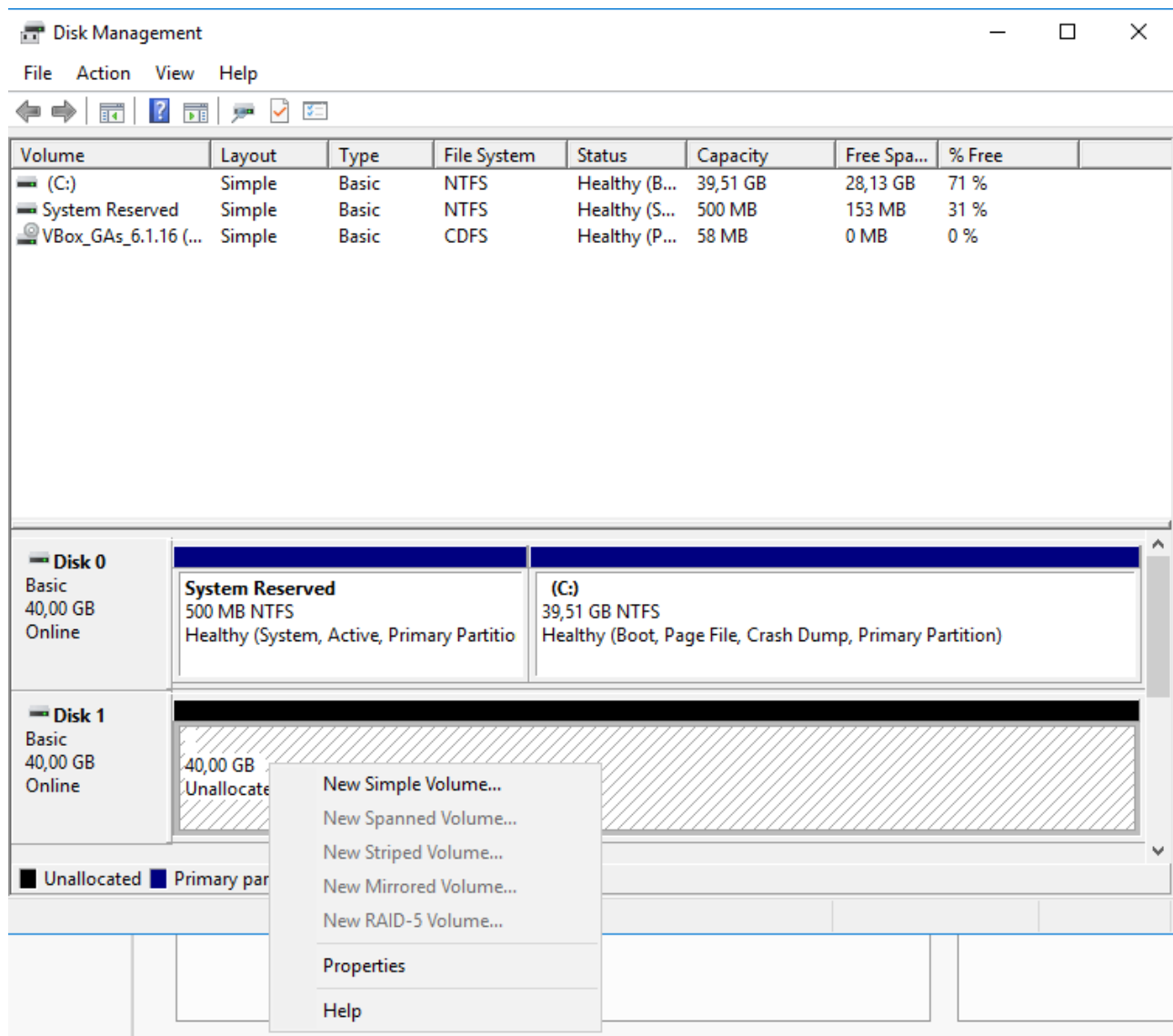
< Back Next > Cancel

Hallintatunnuksen tiedot

Seuraavassa ikkunassa valitse salasana ja varmista, että salasana ei vanhene ikinä. Kun kolmannella ikkunalla painetaan Finish, näkyy luotu tunnus Users-listassa.

Seuraavaksi luodaan levyhallinnassa (Windows Startmenu > Disk Management) uusi Data - niminen NTFS osio, jonka koko on 10 GT.

Disk Management – ikkunassa valitaan alhaalla Disk 1 ja painetaan oikeaa hiiren painiketta jonka jälkeen valitaan New Simple Volume.



Uuden osion luonti

Tämän jälkeen aukeaa New Simple Volume Wizard johon syötetään oikeat tiedot (Nimi = Data, Koko = 10 GT, File System = NTFS).

#### USERS-kansion luonti ja jakaminen

Luodaan Resurssienhallinnassa Data – levyllä "USERS" kansio. Seuraavaksi se jaetaan Authenticated Users – ryhmälle.

Kansion Properties > Sharing > Advanced Sharing> Share this folder > Permissions > Add > Object Types > Built-in security principals > OK > Locations > Users> Enter the object names to select = Authenticated Users> OK > Everyone > Remove > Authenticated Users > Full Control = Allow > OK > OK> Security > Advanced > Disable Inheritance > Convert inherited permissions into explicit permissions on this object > OK > Edit > CREATOR OWNER > Remove > Users > Remove > OK > Close.

## Käyttäjätilien luonti

Luodaan Active Directory Users and Computers – ikkunassa alla olevan taulukon mukaiset käyttäjätilit. Jokaisen käyttäjän kotihakemisto on Connect: (K:) To: <\\\\Apollo\\users\\%username%>.

OU	Nimi	Kirjautumisnimi	Ryhmä	Salasana
<b>Johto</b>	Jaana Jokisalo	jaana.jokisalo	Palkat	PasswOrd\$
	Jaska Jokunen	jaska.jokunen	Hallinto	PasswOrd\$
	Juha Jokela	juha.jokela	Talous	PasswOrd\$
<b>Pilvi</b>	Pasi Paasi	pasi.paasi	Cloud	PasswOrd\$
	Pirjo Pakkarinen	pirjo.pakkarinen	Cloud	PasswOrd\$
<b>Kyber</b>	Kalle Kaarna	kalle.kaarna	Kyber	PasswOrd\$
	Kaisa Kangas	kaisa.kangas	Kyber	PasswOrd\$
	Noa Julkunen	noa.julkunen		PasswOrd\$

## Käyttäjätilit

Kun käyttäjät on luotu, määritetään niille kotihakemisto valitsemalla kaikki käyttäjät Users – välilehdellä > Properties > Profile > Home folder – ruutuun raksi > Connect > K: > <\\\\Apollo\\users\\%username%> > Apply > OK.

## Käyttäjien liittäminen omaan ryhmäänsä

Valitaan haluttu ryhmä, jonne halutaan liittää käyttäjä. Oikean ryhmän Properties – valikossa Members – kohdassa valitaan "Add" ja kenttään kirjoitetaan lisättävän henkilön nimi > Check Names > OK > Apply > OK.

Kun yllä olevan taulukon käyttäjätilit on oikeassa käyttäjätili-ryhmässä, liitetään ryhmä haluttuun ryhmään.

Haluttu henkilö-ryhmä > Properties > Member of > Haluttu määränpää ryhmä > Check names > Apply > OK.

## Käyttäjätilien toiminnan testaus

Kirjaudutaan Windows-10 työasemalla "Other user" kohdassa halutun käyttäjän kirjautusnimellä ja salasanalla. Ensimmäisen kirjautumisen yhdessä Ei tarvitse vaihtaa salasanaa koska jokaisen käyttäjän kohdalle on laitettu "Password never expires" käyttäjätilien asetuksissa. Resurssienhallinnassa näkyy nyt polussa C:\\Users käyttäjän nimeä vastaava kansio – johon on täydet käyttöoikeudet.

## Harjoitus 6

### Kansioden jakaminen ja käyttöoikeuksien määrittäminen

Luodaan Data-levylle uusi kansio nimeltä Palkat. Jaetaan kansio toimialueen kesken siten, että Palkanlaskenta ryhmällä on kansioon muokkausoikeudet, Administrators- ja System- ryhmillä oletus oikeudet ja muilla käyttäjillä ei ole mitään oikeuksia kansioon. Luo olla olevan taulukon mukaiset kansiot Data-levylle.

Kansion nimi	Kaikki oikeudet	Lukuoikeudet	Ei oikeuksia
Palkat	Administrators	Palkanlaskenta	Loput ryhmät
TALOUS	Administrators, Budjetin ylläpito	Budjetin luku	Loput ryhmät
Adminjako	Administrator	Loput käyttäjät	--

## Kansioden käyttöoikeudet

### Kansioden käyttöoikeuksien määrittäminen

Kohdekansion properties > Sharing > Advanced Sharing > Permissions > Add / Remove halutut ryhmät (tai käyttäjät) ja määritä oikeudet. > OK > OK > Security > Edit > Muokkaa ryhmien (tai käyttäjien) oikeuksia. > OK.

### Kansioiden käyttöoikeuksien testaus


Kirjaudutaan Windows 10-työasemalle käyttäjätunnuksella, jolla on käyttöoikeudet kansioon Palkat.

Käyttäjätunnus	Salasana	Palkat - käyttöoikeus
jaana.jokisalo	Password\$	Kyllä
kalle.kaarna	Passw0rd\$	Ei

Testattavien käyttäjien tiedot

Avataan Map Network Drive (Resurssienhallinta > Network päällä hiiren oikea painike > Map network drive...) ja muokataan aukeava ikkuna vastaamaan alla olevaa kuvaa.

✕

 Map Network Drive

### What network folder would you like to map?

Specify the drive letter for the connection and the folder that you want to connect to:

Drive:  ▼

Folder:  ▼

Example: \\server\share

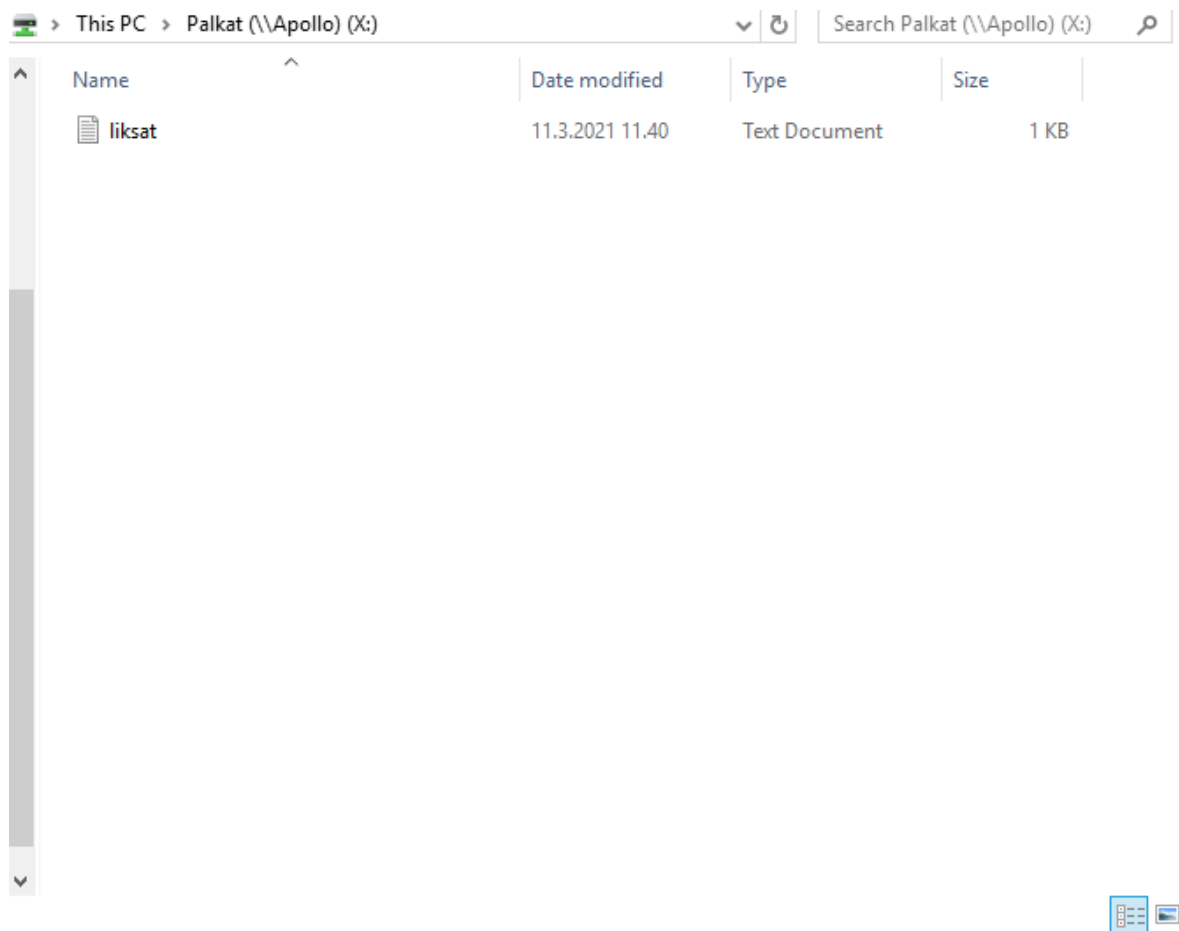
☒ Reconnect at sign-in

☒ Connect using different credentials

[Connect to a website that you can use to store your documents and pictures.](#)

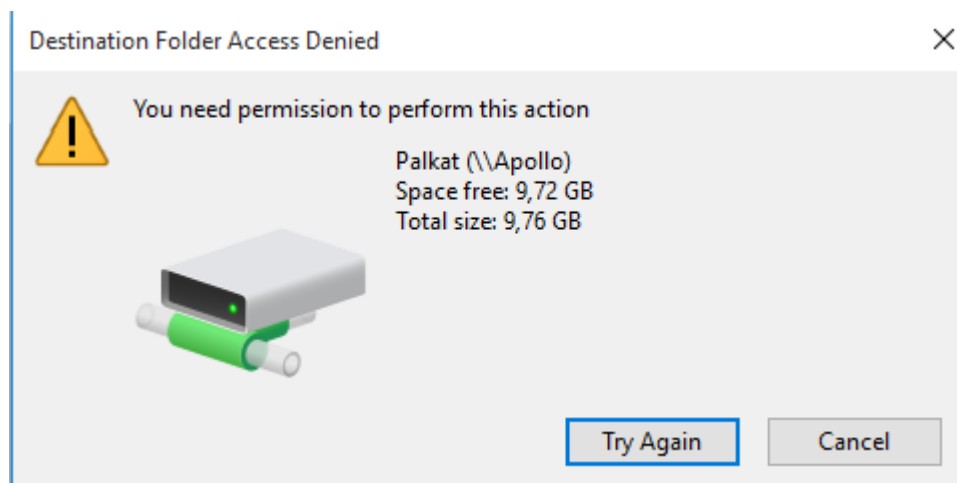
Map Network Drive – ikkuna

Avautuvaan Windows Security – ikkunaan kirjoitetaan käyttäjätunnus ja salasana, joilla kirjaututtiin työasemalle. Jos käyttäjällä on käyttöoikeudet kansioon, voi Palkat – kansion sisältöä katsoa This PC > Network locations – kohdan alta.



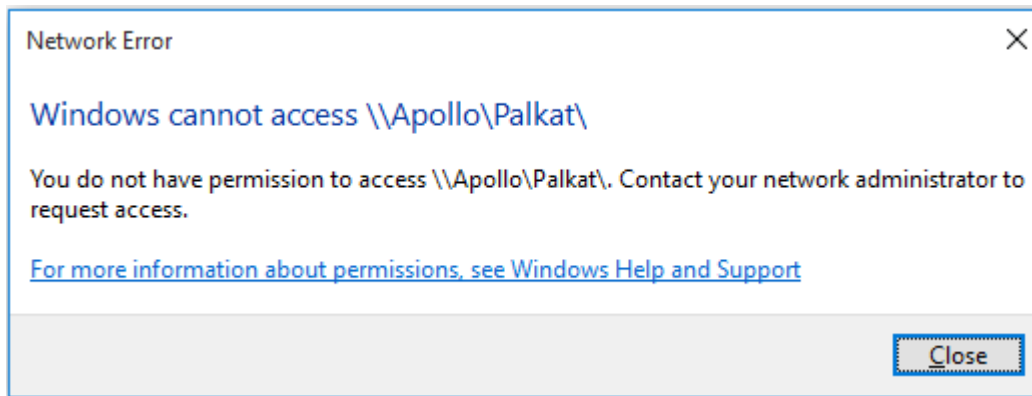
Palkat – kansion sisältö työasemalla

Jos samalla käyttäjällä (jaana.jokisalo) yrittää lisätä / muokata tiedostoa, aukeaa alla olevan kuvan virheilmoitus. Virheilmoitus tulee, koska Palkanlaskenta – ryhmällä on ainoastaan lukuoikeudet.



Virheilmoitus, kun lukuoikeudet ei riitä

Jos käyttäjällä ei ole käyttöoikeuksia kansioon, aukeaa olla olevan kuvan virheilmoitus.



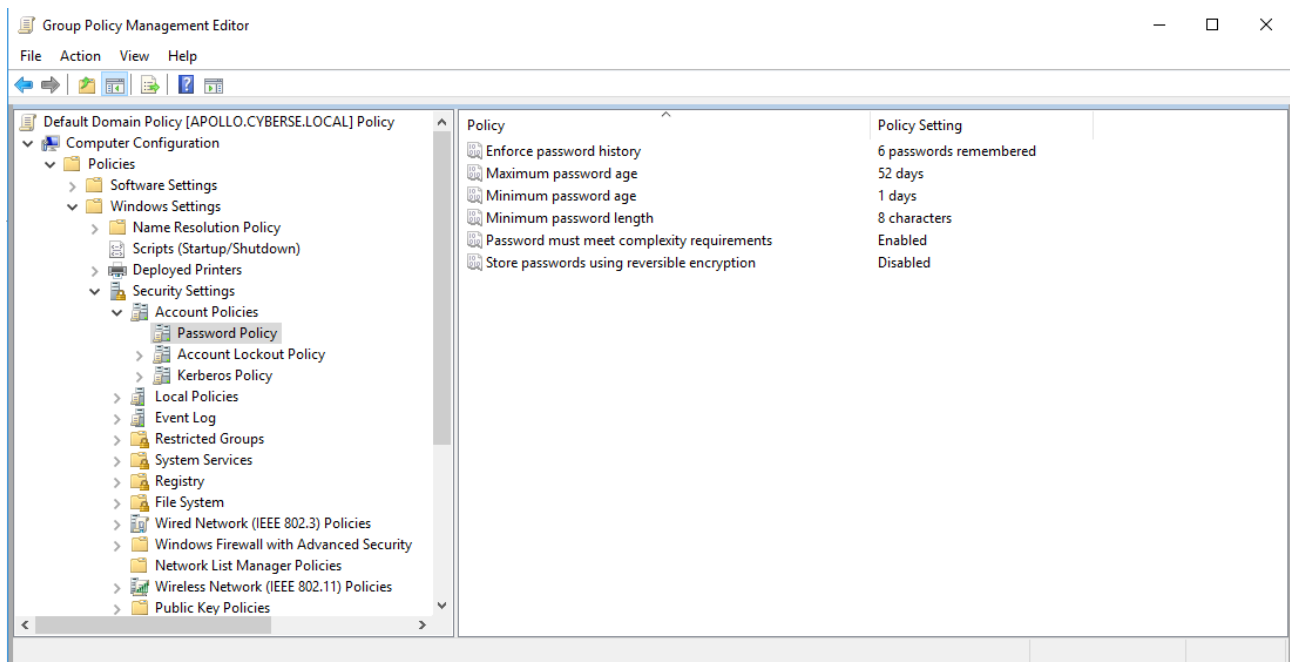
Virheilmoitus, kun käyttöoikeuksia ei ole

## Harjoitus 7

### Ryhmäkäytäntöjen hallinta

#### Salasanakäytäntöjen muokkaaminen

Avataan Group Policy Management (Server Manager Tools > Group Policy Management) josta etsitään kohta Default Domain Policy (Forest: cyberse.local > Domains > cyberse.local > Default Domain policy). Avataan seuraavaksi Group Policy Management Editor hiiren oikealla näppäimellä Default Domain Policyn päällä ja valitaan avautuvasta valikosta **Edit**. Seuraavaksi muokataan Password Policyjä. Alla olevassa kuvassa vasemmalla puolella näkyy muokattavan kohteen sijainti ja oikealla tilanne muokkauksen jälkeen.



#### Salasanakäytäntöjen muokkaus

Policy	Selitys
Enforce password history	Jotta vanhaa salasanaa voi käyttää, täytyy välissä olla 6 eri salasanaa.
Maximum password age	Salasanoja ei voi käyttää pidempään kuin 52 päivää
Minimum password age	Salasanoja ei voi vaihtaa montaa kertaa päivässä, vain 1 päivän välein.
Minimum password length	Salasanan täytyy olla vähintään 8 merkkiä pitkä
Password must meet complexity requirements	Salasanan täytyy pitää sisällään erilaisia merkkejä
Store passwords using reversible encryption	Salasanoja ei tallenneta merkkijonoina.

#### Salasanakäytäntöjen selitteet

##### Account Lockout Policy

Samassa sijainnissa (Account Policies) valitaan Account Lockout Policy. Muutetaan Account lockout threshold arvoksi 3 ja muut kohdat suositelluiksi arvoiksi.

Policy	Asetus	Selite
Account lockout duration	30 minutes	Aika, jonka käyttäjä on lukittu jos salasana annetaan tarpeeksi monta kertaa väärin.



Account lockout threshold	3 invalid logon attempts	3 kertaa voi antaa väärän salasanan, ennen kuin käyttäjä lukitaan
Reset account lockout counter after	30 minutes	Aika, jolloin kirjautumista voi yrittää uudelleen annettuaan väärän salasanan tarpeeksi monta kertaa

### Account Lockout Policyt

**Default Domain Policy**
Scope Details Settings Delegation

**Default Domain Policy**  
 Data collected on: 12.3.2021 9.05.55

**Computer Configuration (Enabled)**

**Policies**

**Windows Settings**

**Security Settings**

**Account Policies/Password Policy**

Policy	Setting
Enforce password history	6 passwords remembered
Maximum password age	52 days
Minimum password age	1 days
Minimum password length	8 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

**Account Policies/Account Lockout Policy**

Policy	Setting
Account lockout duration	30 minutes
Account lockout threshold	3 invalid logon attempts
Reset account lockout counter after	30 minutes

**Account Policies/Kerberos Policy**

Policy	Setting
Enforce user logon restrictions	Enabled
Maximum lifetime for service ticket	600 minutes
Maximum lifetime for user ticket	10 hours
Maximum lifetime for user ticket renewal	7 days
Maximum tolerance for computer clock synchronization	5 minutes

**Local Policies/Security Options**

**Network Access**

Policy	Setting
Network access: Allow anonymous SID/Name translation	Disabled

**Network Security**

Policy	Setting
Network security: Do not store LAN Manager hash value on next password change	Enabled
Network security: Force logoff when logon hours expire	Disabled

**Public Key Policies/Encrypting File System**

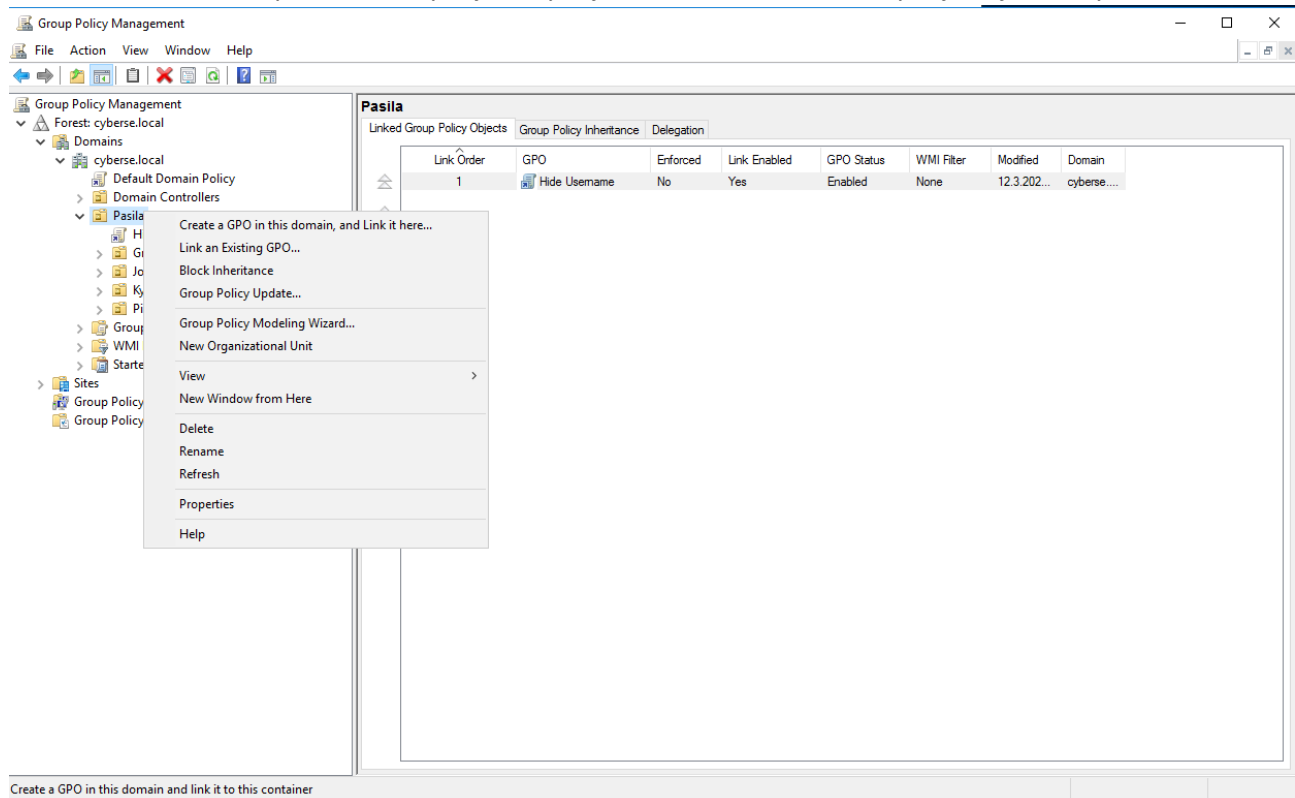
**Certificates**

### Default Domain Policy

Yllä olevasta kuvasta näkee aikaisemmat muutokset koottuna yhdelle sivulle (Group Policy Management > Forest: cyberse.local > Domains > cyberse.local > Default Domain Policy > Settings – välilehti).

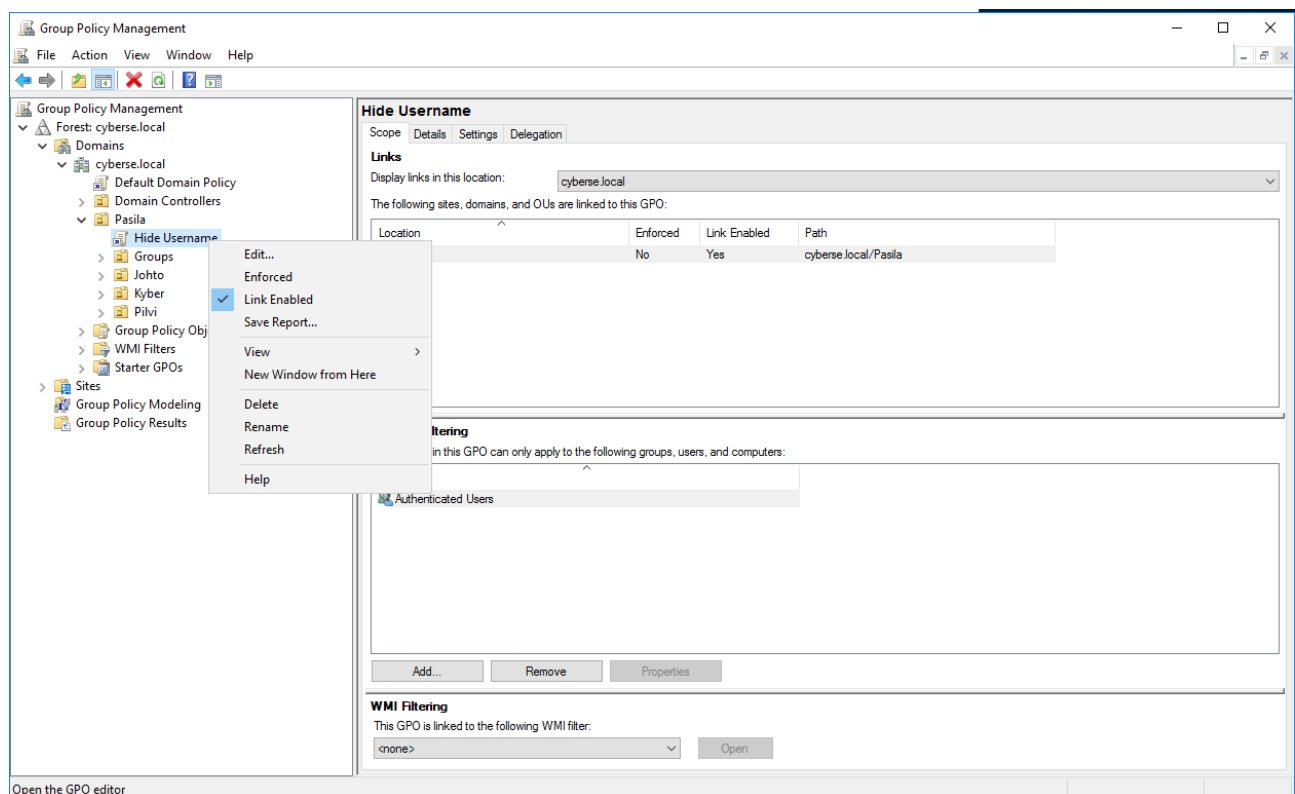
## Pasila OU:n ryhmäkäytäntöjen muokkaus

Piilotetaan aiemman työaseman käyttäjän käyttäjätunnus kun seuraava käyttäjä kirjautuu työasemalle.



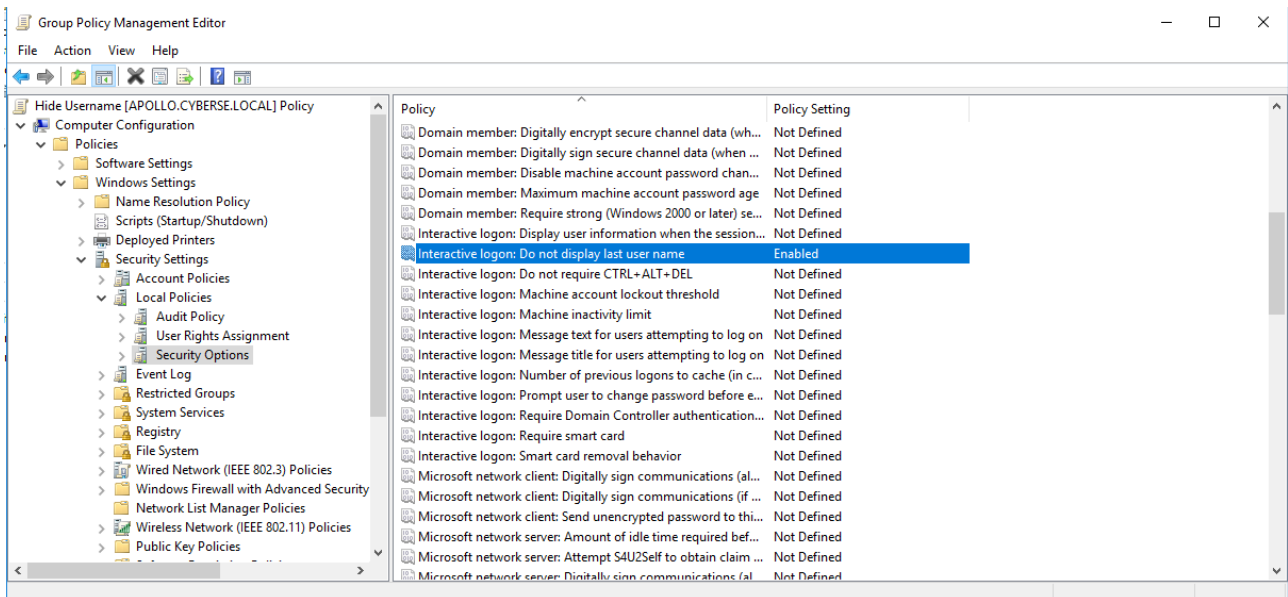
## GPO:n luominen

Navigoidaan kuvan osoittamaan sijaintiin ja valitaan **Create a GPO in this domain, and link it here...** - kohta ja annetaan nimeksi "Hide Username"



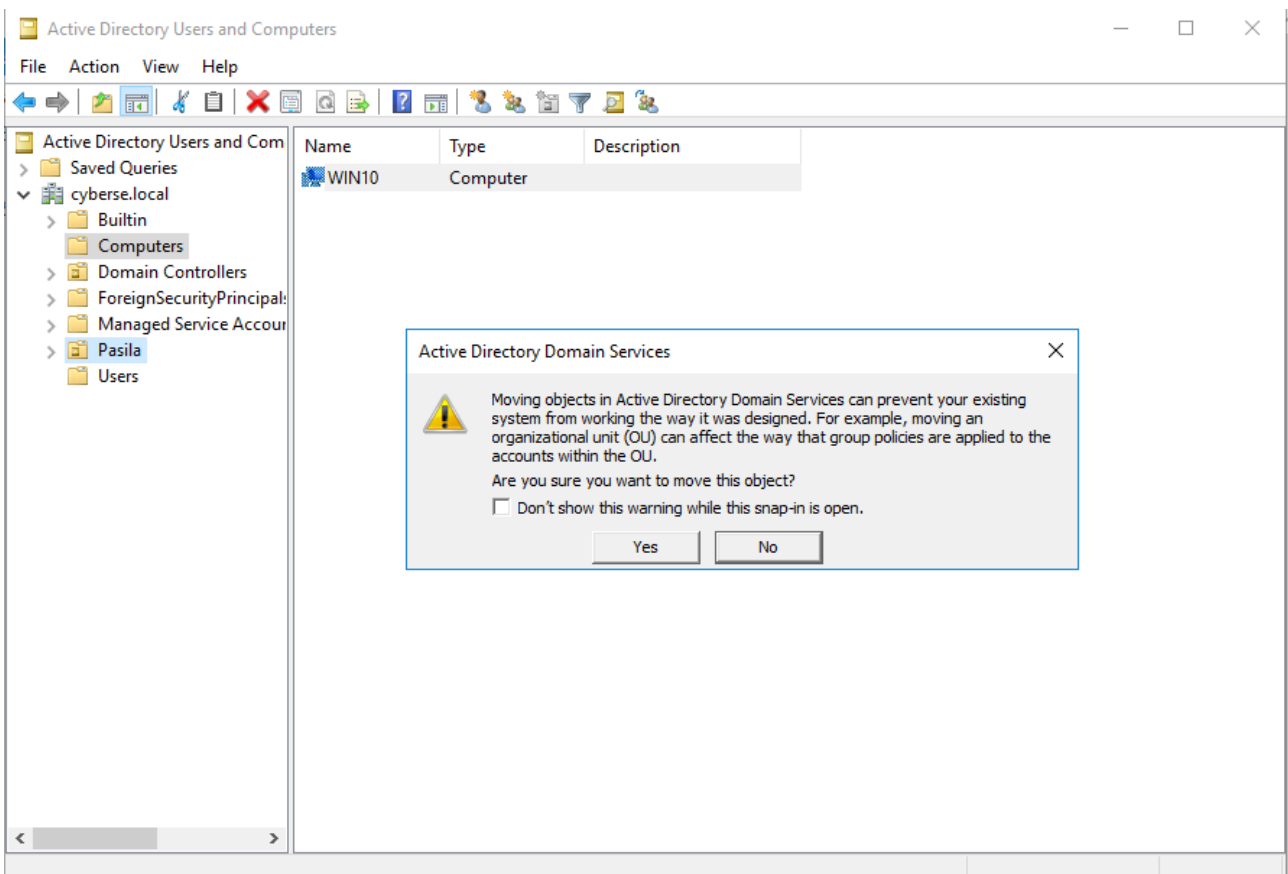
## Käyttäjätunnuksen piilottaminen muilta kirjautujilta

Valitaan **Edit** – kohta listasta.



## Asetuksen muokkaaminen

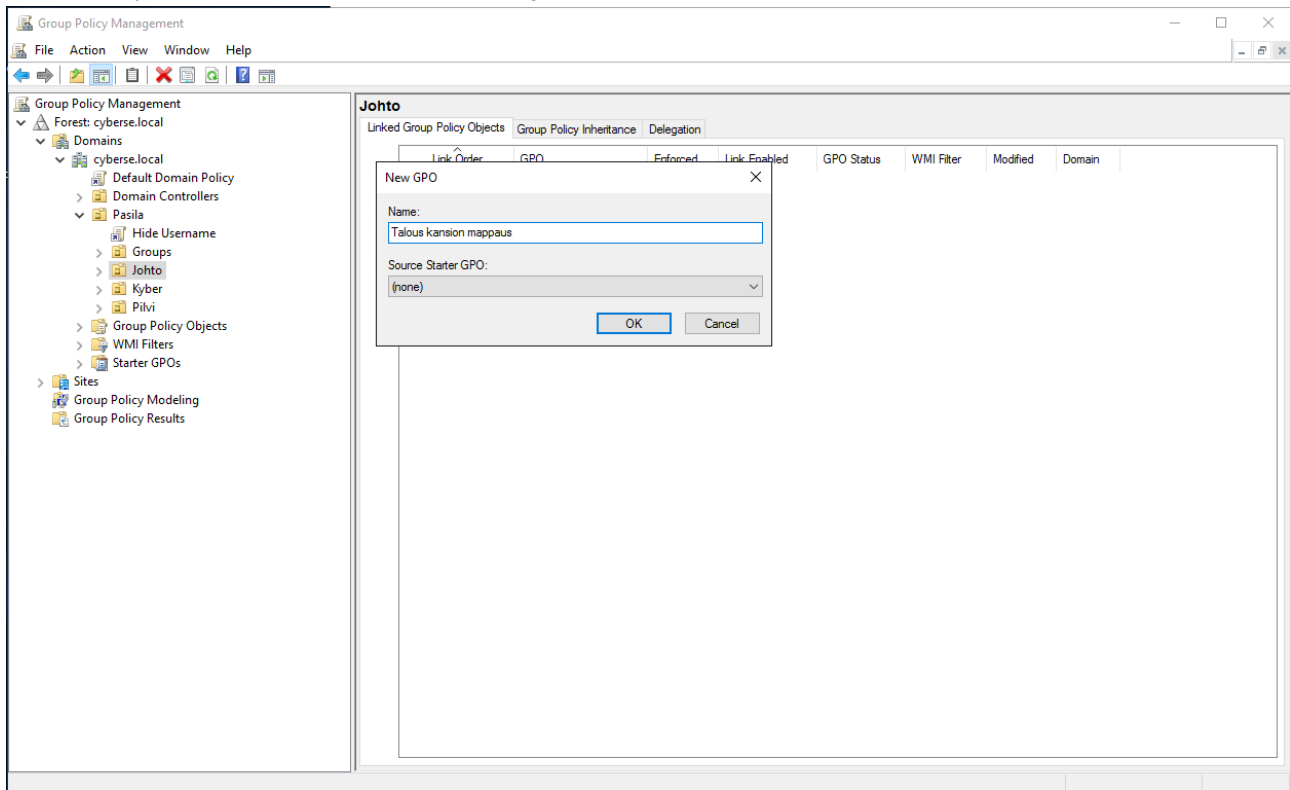
Navigoi kuvan vasemmalla puolella näkyvään sijantiin ja tuplaklikkaa sinisellä merkittyä riviä, jonka jälkeen raksi ruutuun Define this policy setting ja enabled alla olevaan valintaan. Lopuksi OK.



Työaseman siirto Pasila OU:seen

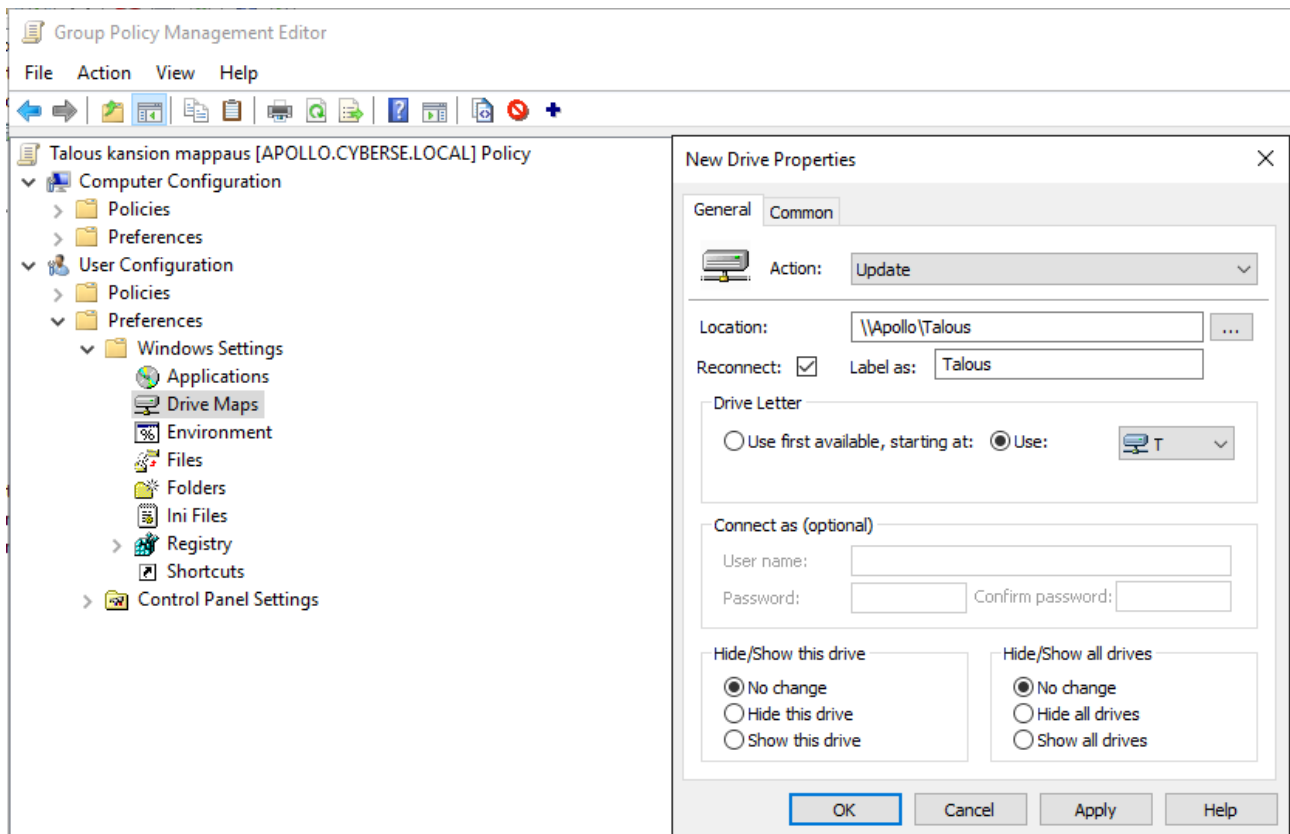
Active Directory Users and Computers kohdassa siirrä **Computers** kohdasta WIN10 työasema **Pasila** kohtaan, aukeavaan varoitukseen yes.

### Verkkolevyn Talous kiinnittäminen T – kirjaimeen



#### GPO:n luonti

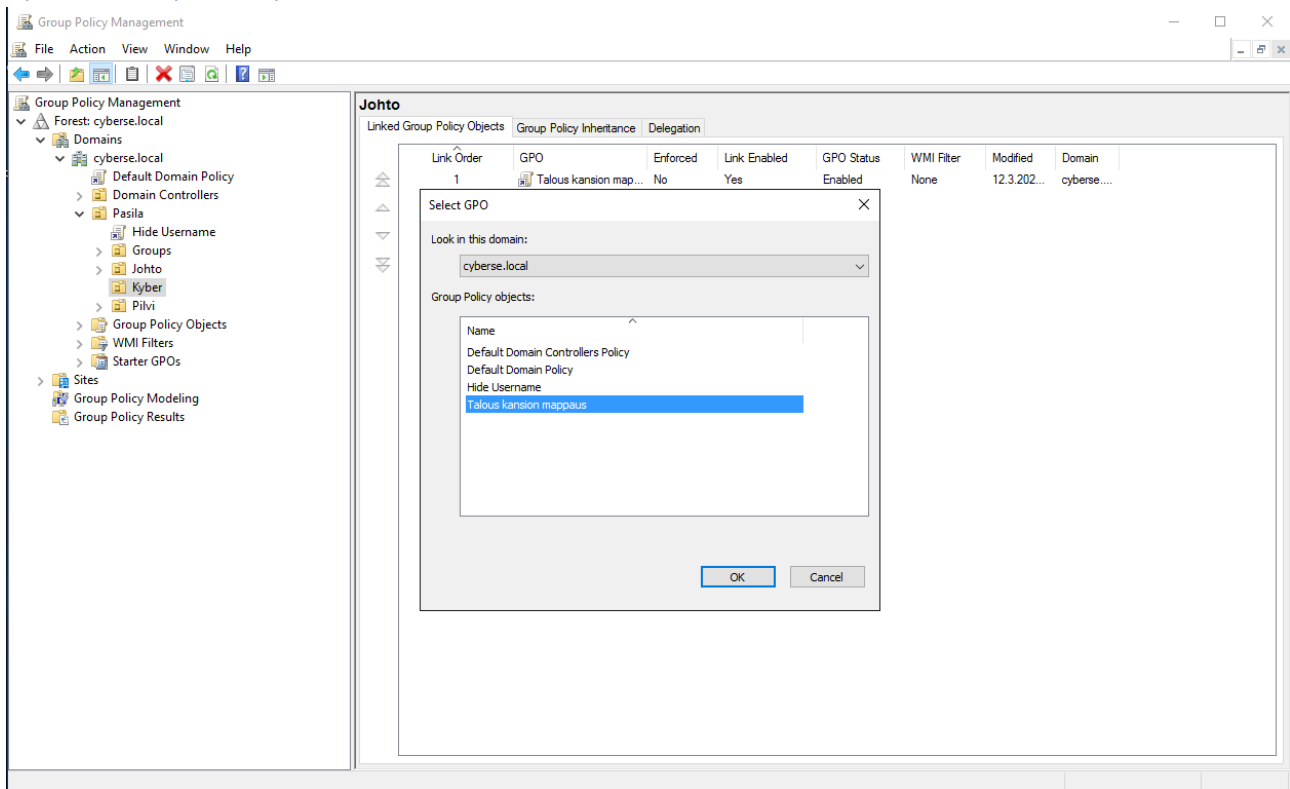
Luo **Talous kansion mappaus** – niminen GPO samalla tavalla kuin aiemmissa kohdissa. GPO:n kohde näkyy vasemmalla laidalla yllä olevassa kuvassa.



### New Drive Properties

Luodun GPO:n edit kohdassa luo uusi drive (User Configuration > Preferences > Windows Settings > Drive Maps hiiren 2. painike > New > Mapped drive). Oikealla puolella kuvassa näkyy driven sijainti, kirjain ja muut tiedot.

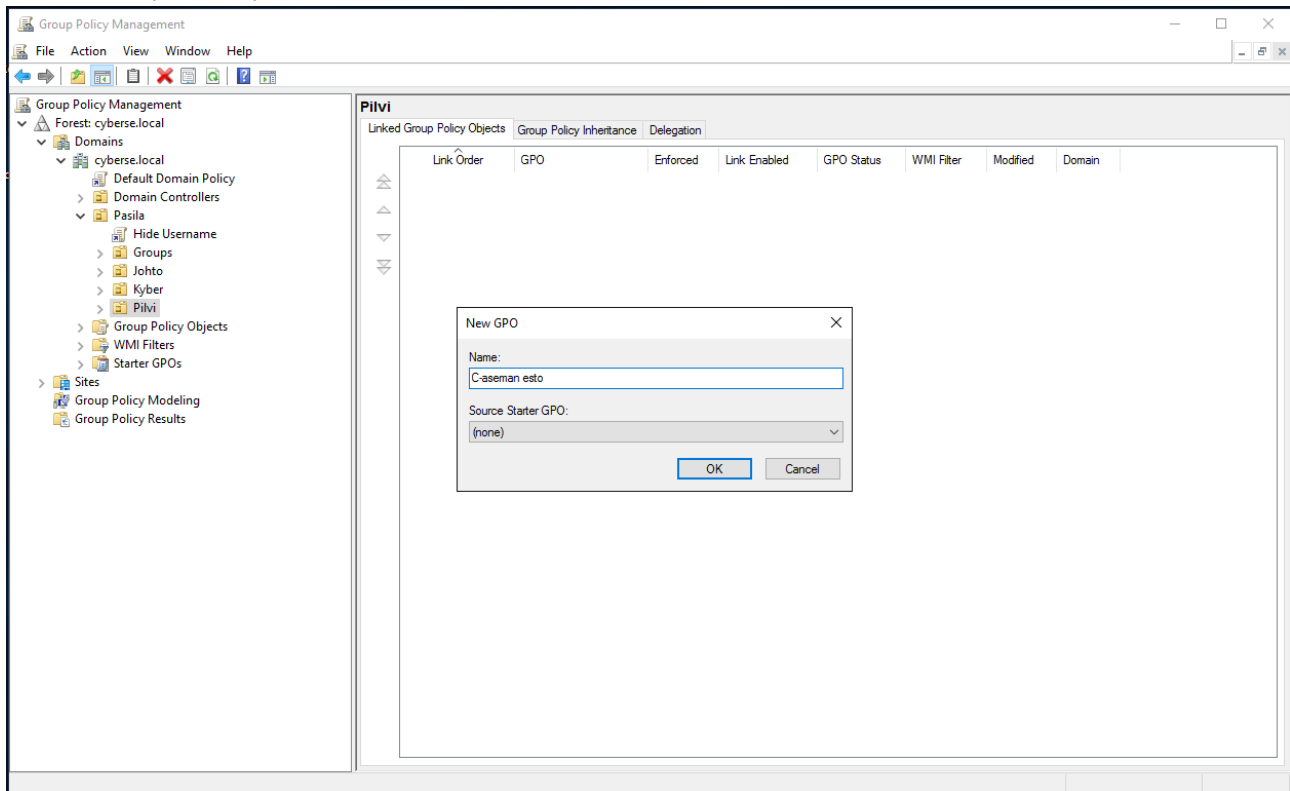
## Kyber OU:n ryhmäkäytäntö



Link an Existing GPO...

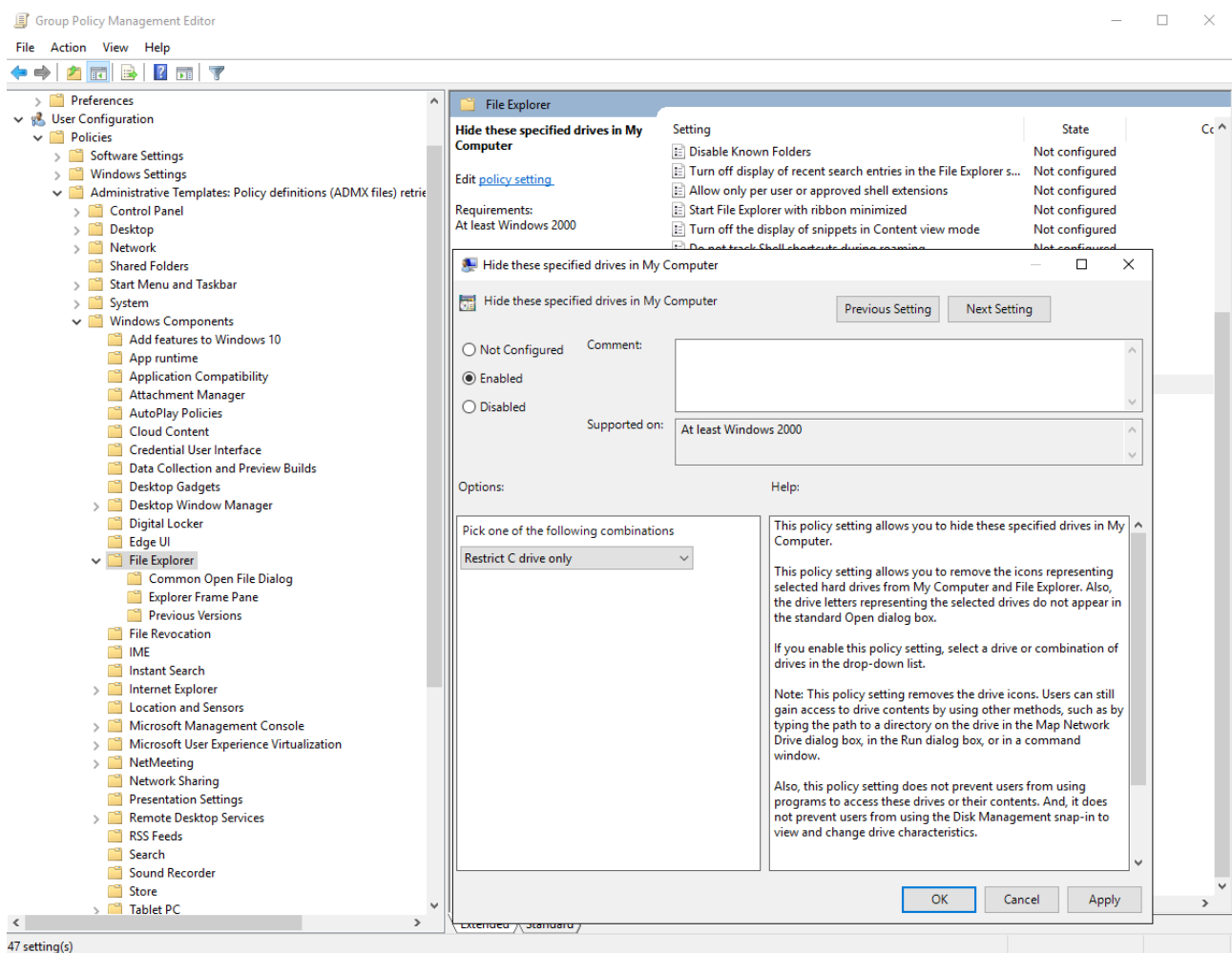
Hiiren 2. painike **Kyber** – kohdan päällä > Link an Existing GPO... > Talous kansion mappaus > OK.

## Pilvi OU:n ryhmäkäytäntö



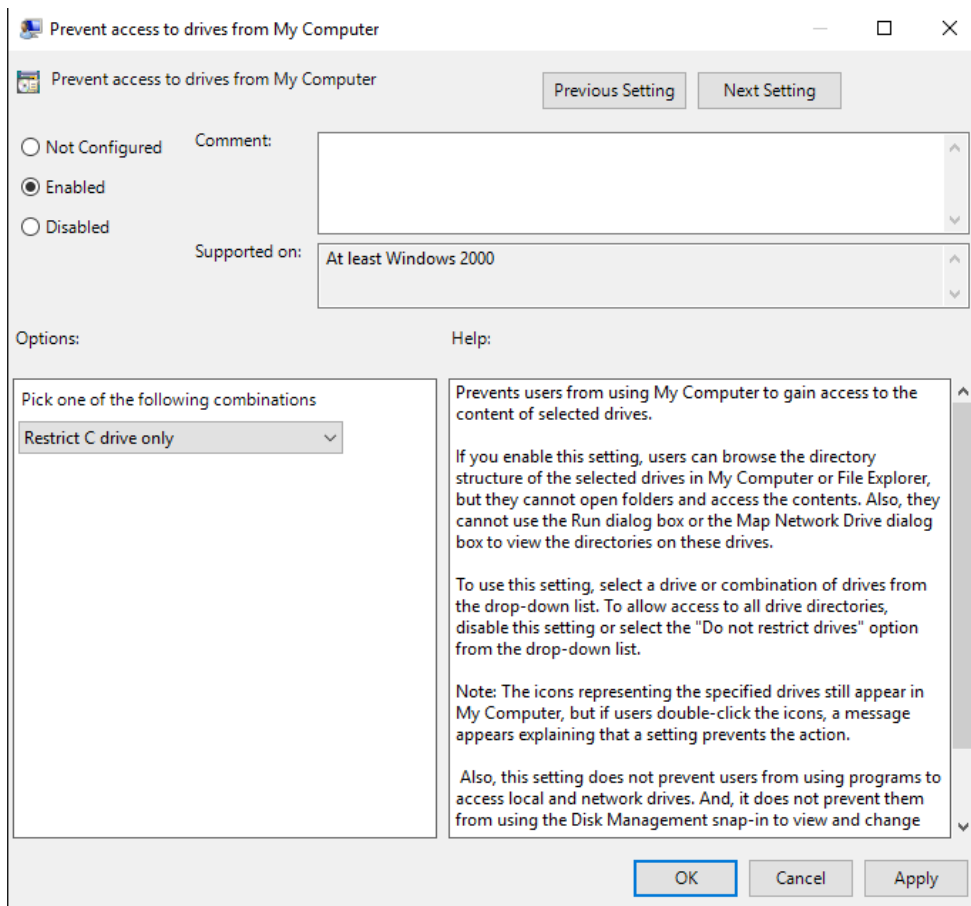
C-aseman esto – GPO

Luo **Pilvi** – kohtaan uusi GPO, jonka nimi on C-aseman esto. Kun GPO on luotu, mennään editoimaan sitä (C-aseman esto > hiiren 2. painike > Edit). Kun Group Policy Management Editor on avaantunut, etsi ”Hide these specified drives in My Computer” – kohta. (Alla oleva kuva.)



Hide these specified drives in My Computer

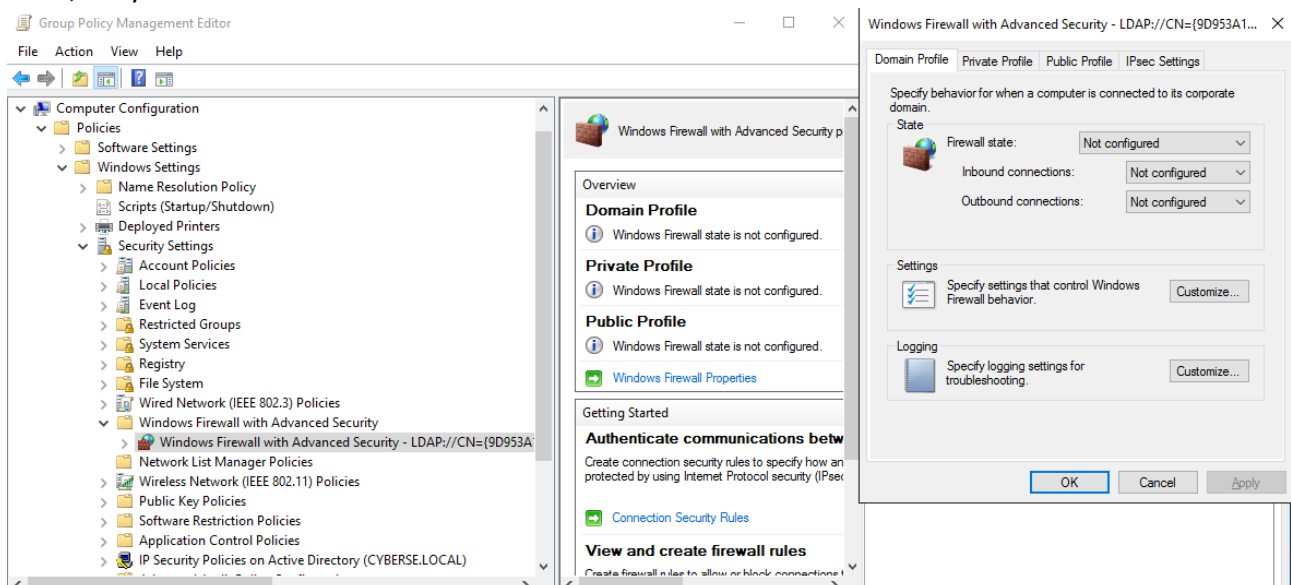
Vasemmalla kuvassa näkyy oikea sijainti, oikealla säännön konfigurointi.



Voimakkaampi esto

Pasila OU:n palomuurisääntö

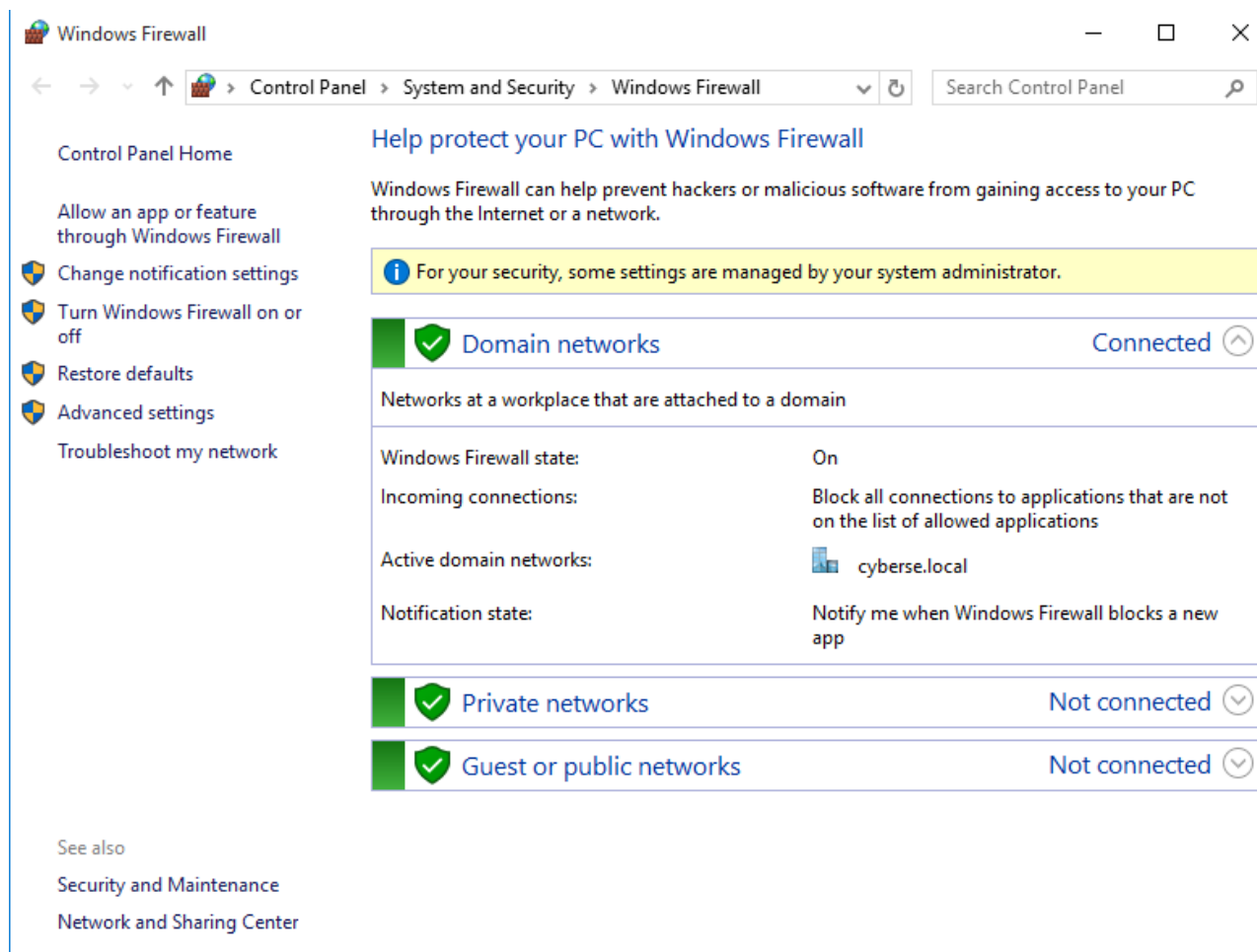
Luodaan uusi GPO nimeltä **Palomuuriasetksia työasemille** kohtaan **Pasila** (Forest: cyberse.local > Domains > cyberse.local > Pasila hiiren 2.painike > Create a GPO in this domain, and Link it here...). Kun GPO on luotu, siirry editoimaan sitä.



Windows Firewall with Advanced Security protection



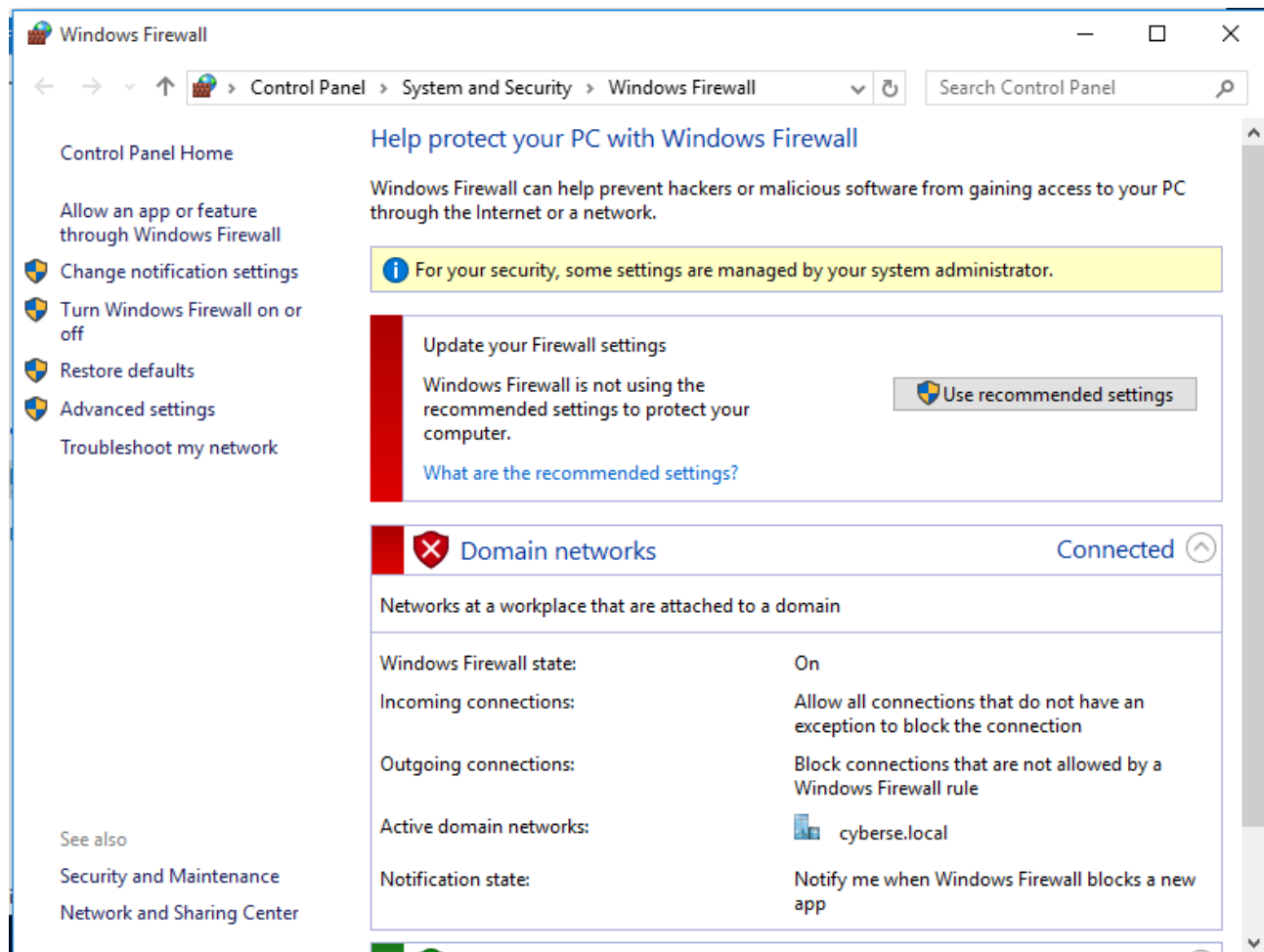
Kuvassa vasemmalla näkyy oikea sijainti, jolloin oikean puoleinen ikkuna aukeaa kun painaa **Windows Firewall Properties** – linkkiä (kuvan keskellä). Oikean puoleisen ikkunan Domain profile, Private Profile ja Public profile – välilehdillä muuta Firewall state = On (recommended).



Palomuri työasemalla

Nyt palomuurissa työasemalla näkyy ilmoitus, että järjestelmänvalvoja hallitsee joitain asetuksia.

**Testataan sallia Domain Profilessa Inbound connections ja Outbound connections = block.**



Firewall työasemalla muutosten jälkeen

Firewall työasemalla näyttää nyt samalta, kun yllä olevan kuvan Firewall.