

Serveradministration og sikkerhed: Fase 2

Tidsplan:	2
IP Plan:	3
Topology:	3
Bruger Matrix:	4
Fjern server roles fra SkibhusDC (Skibhus.local):	5
Oprettelse WSUS:	9
Cloning af Skibhus VMWare og flytning til Munkebjerg:	11
Oprettelse af brugere:	13
Ændring af IP og PC navne:	15
Mapping af drev og mapper:	17
Krav om password:	20
Skjult Navn på sidste bruger:	21
Baggrundsbillede til hver afdeling:	22
Domain administrator og serveroperator:	24
Superbruger i hver afdeling:	25
Almindelige bruger skal ikke have adgang til CDM eller Powershell:	28
Lås bruger i 25 min ved 5 fejl-login:	29
Security Event logfiler:	30
Active Directory Recycle Bin:	31
Opsætning af WSUS:	33

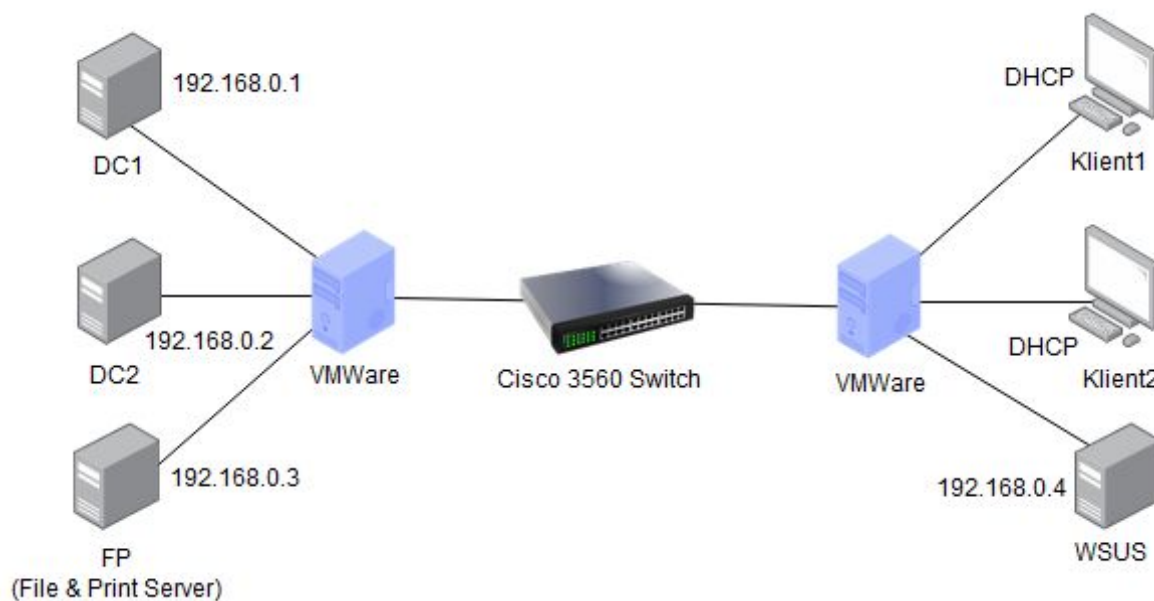
Tidsplan:

Dato	Opgave	Dagbog/fejlløg
Tirsdag 2/6	Udarbejde projektplan. IP-Plan. Bruger Matrix. Clonet og overført VMWare maskinerne.	Går i gang med Fase 2. Nedlægger det gamle domæne. Cloner og flytter den gamle DC og den gamle klient. Oprettet 8 brugere. Retter passwords. Retter IP'er og navne på de to klienter og på den nye DC.
Onsdag 3/6	Opret drev-mapping via GPO på DC1 og oprette drev/mapper på MunkeFP. Påbegynde sikkerhed. Arbejde videre med dokumentation.	Oprettede mapper og drev til alle 8 brugere. Oprettede Rev + Adm mapperne. Mapperne blev oprettet som "drev", så man kan se dem på klienterne så snart man logger ind. GPO voldte "lidt" problemer, men kom i sidste ende til at virke. Lavede topology med draw.io. Har lavet et nyt mere sikkert password for alle brugerne: Munk123456!
Torsdag 4/6	Færdiggøre sikkerhed. Arbejde videre med dokumentation.	9-13) Fuldført 14) Giver lidt problemer, brugeren har stadig adgang til CMD. 14a) Lavede en ny GPO under vores OU i stedet for forest, og nu har brugerene ikke adgang til CMD. Nyt bruger-password når man bliver låst ude af systemet efter 5 forkerte passwords er: Munk1234567
Mandag 8/6	Punkt 15-16	
Tirsdag 9/6	Punkt 18-19	
Onsdag 10/6	Skal være færdig.	
Torsdag 11/6		

IP Plan:

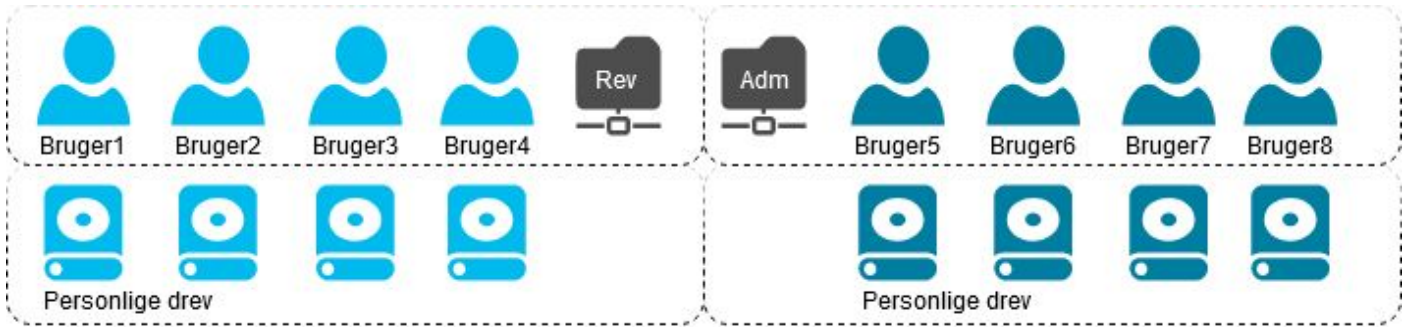
MS Domain name				
Munkebjerg.local				
Navn	IP adresse	Password	DNS	OS
DC1	192.168.10.1	Munk1234	192.168.10.1	Windows Server 2016
DC2	192.168.10.2	Munk1234	192.168.10.1	Windows Server 2016
FP	192.168.10.3	Munk1234	192.168.10.1	Windows Server 2016
WSUS	192.168.10.4	Munk1234	192.168.10.1	Windows Server 2016
Klient1	DHCP	Munk1234	192.168.10.1	Windows 10 Pro
Klient2	DHCP	Munk1234	192.168.10.1	Windows 10 Pro

Topology:



Bruger Matrix:

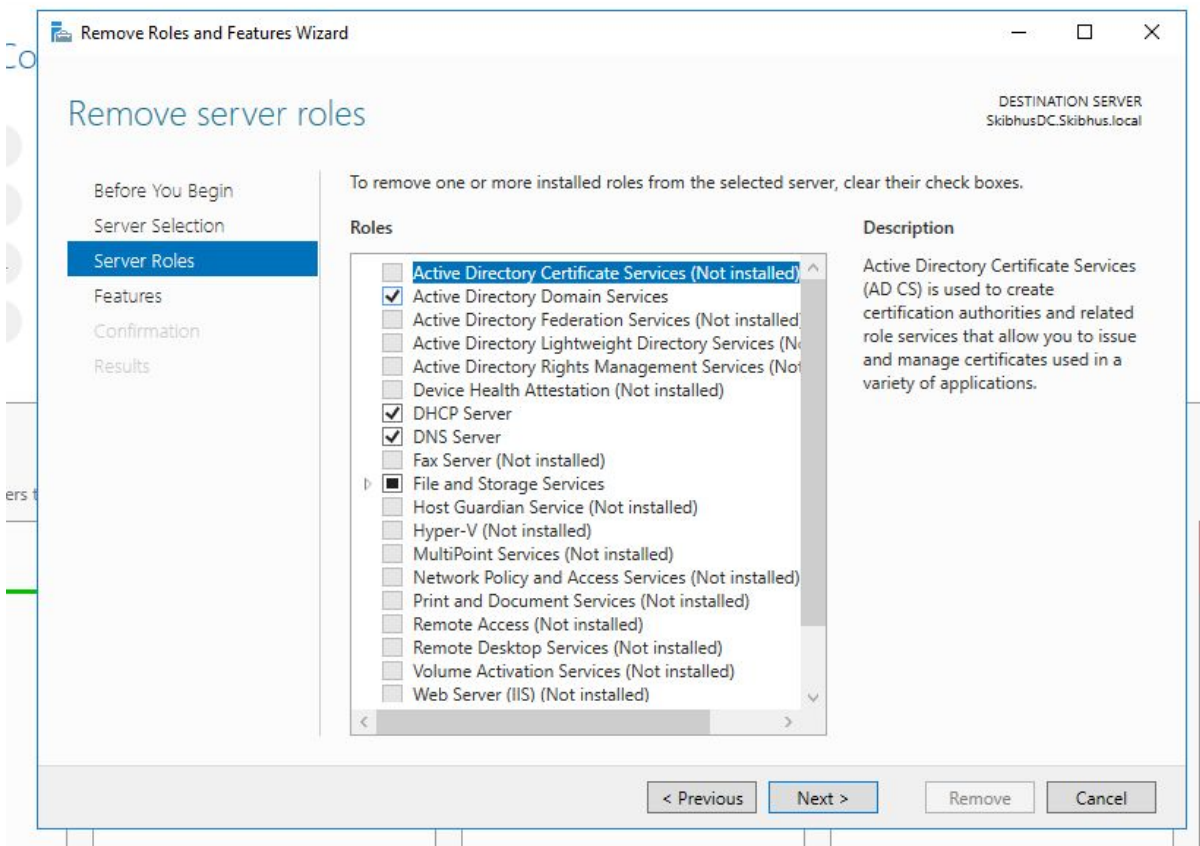
Navn	Organizational Units	Global Security Groups	Domain Local Security Groups	Shared Folder	R	W
Bruger1	Munk_Rev	GS_MunkRev	DLRev	Rev	x	x
Bruger2	Munk_Rev	GS_MunkRev	DLRev	Rev	x	x
Bruger3	Munk_Rev	GS_MunkRev	DLRev	Rev	x	x
Bruger4	Munk_Rev	GS_MunkRev	DLRev	Rev	x	x
Bruger5	Munk_Adm	GS_MunkAdm	DLAdm	Adm	x	x
Bruger6	Munk_Adm	GS_MunkAdm	DLAdm	Adm	x	x
Bruger7	Munk_Adm	GS_MunkAdm	DLAdm	Adm	x	x
Bruger8	Munk_Adm	GS_MunkAdm	DLAdm	Adm	x	x
Note: GS -> DL -> DL rettigheder til mapper						



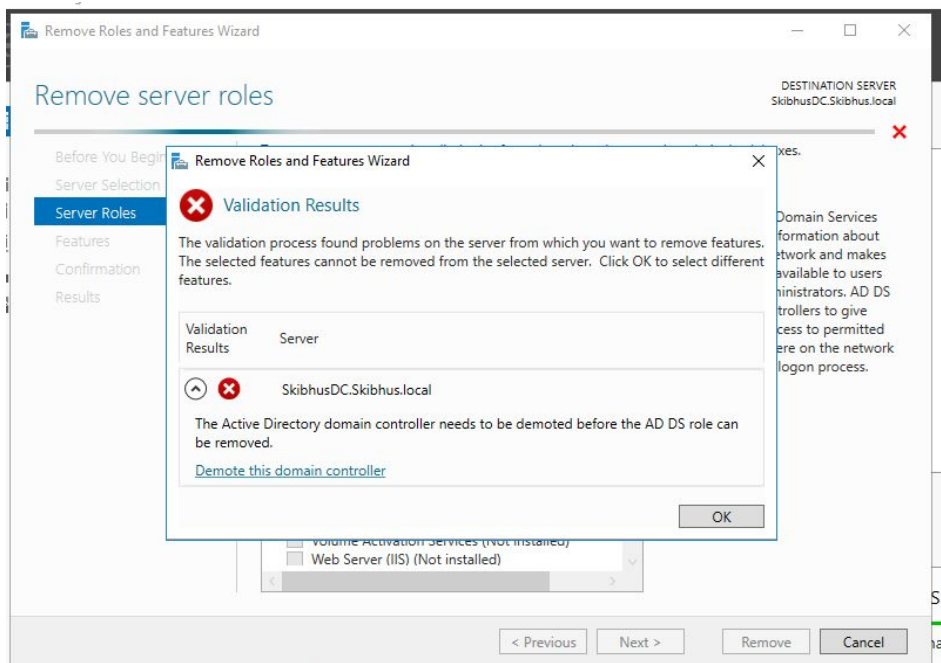
Fjern server roles fra SkibhusDC (Skibhus.local):

Demote og fjern SkibhusDC.Skibhus.local AD DC.

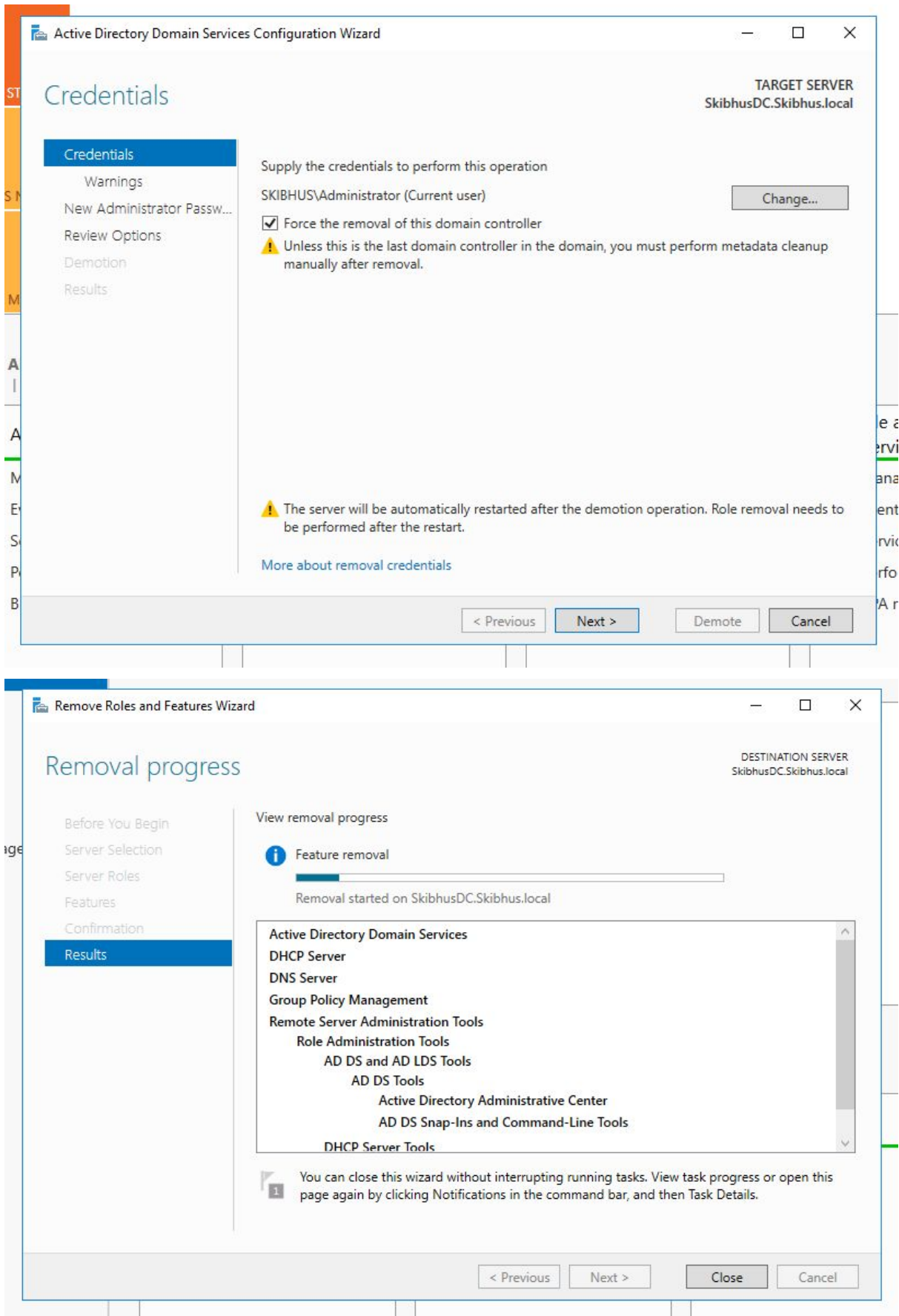
“Manage” -> “Remove Roles and Features” -> Sæt flueben i “Active Directory Domain Service” og “Remove”.

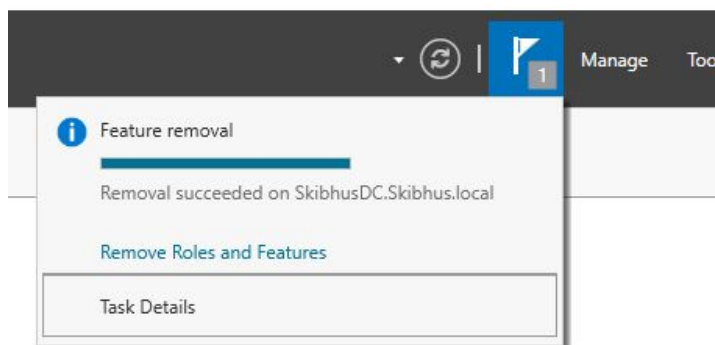


Klik på “Demote this domain controller”.

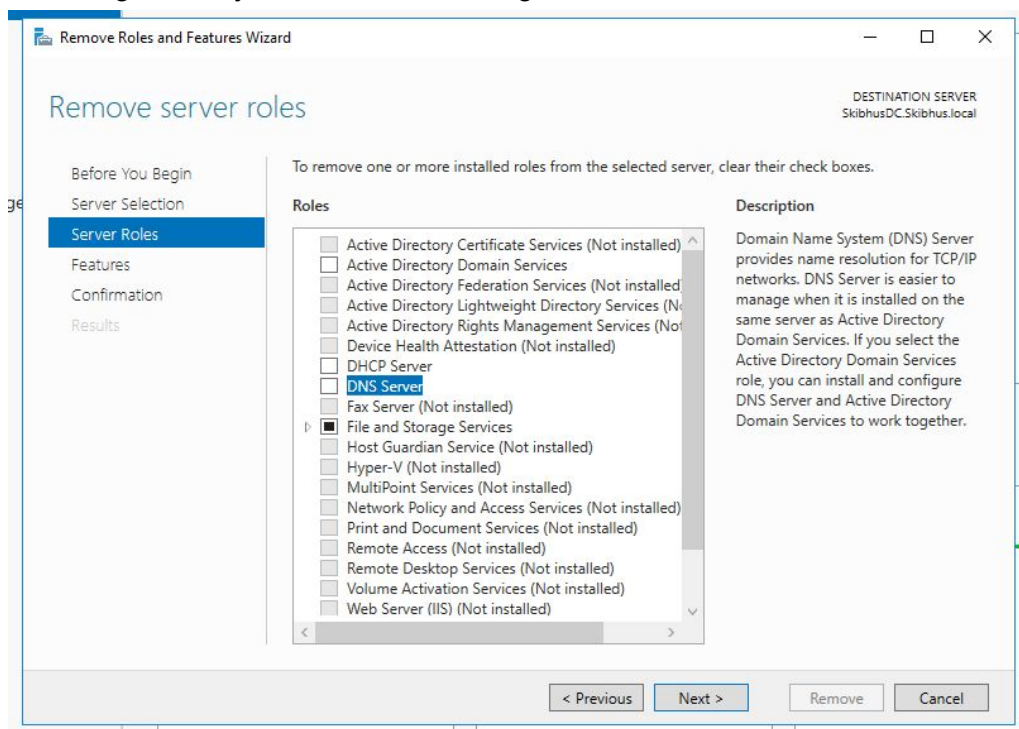


Vælg "Force the removal of this domain controller".

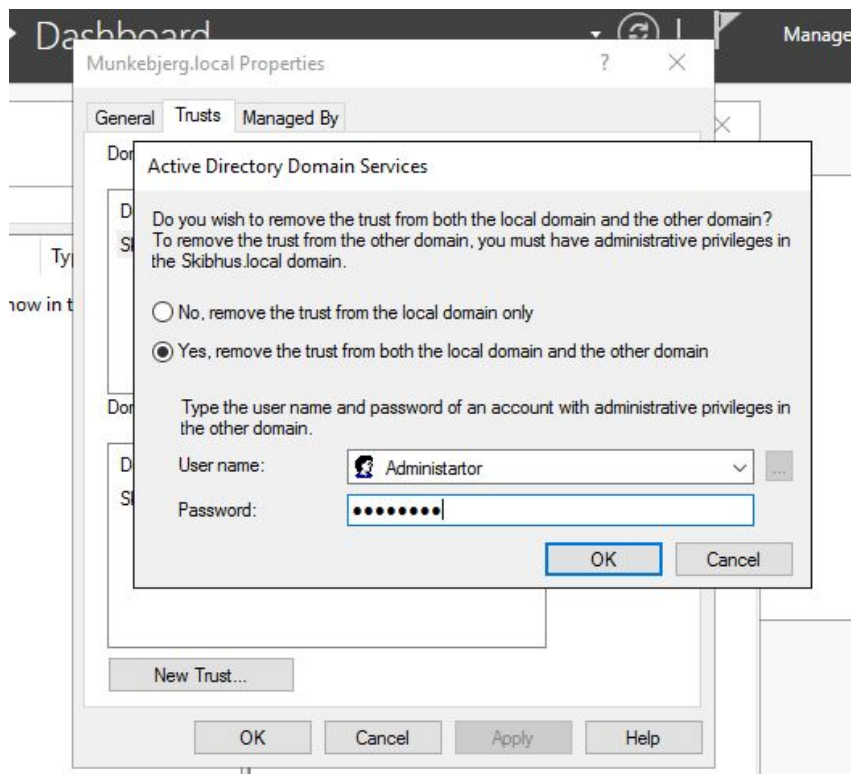
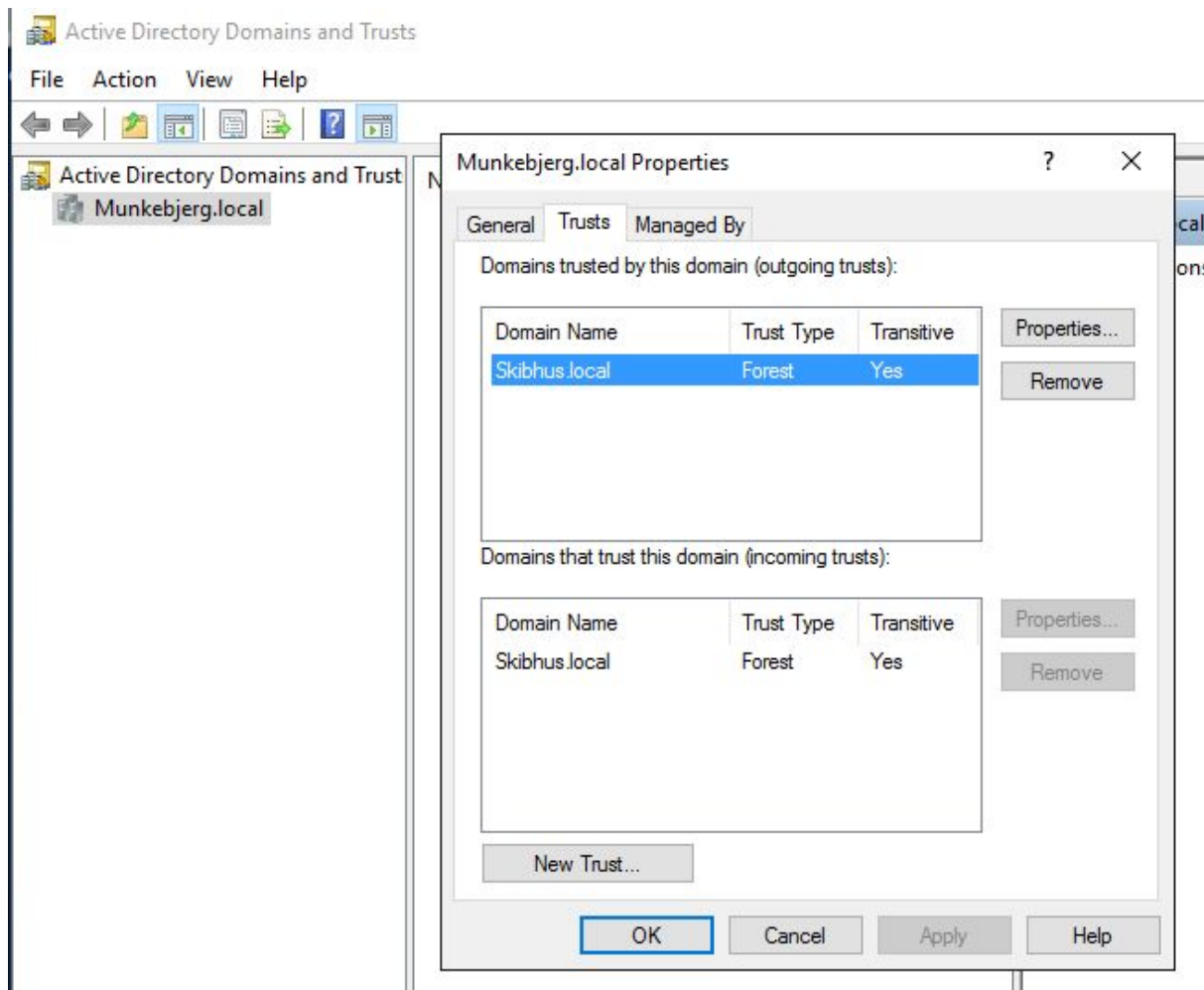




Efter en genstart fjernes AD DS, DNS og DHCP fra skibhus serveren.

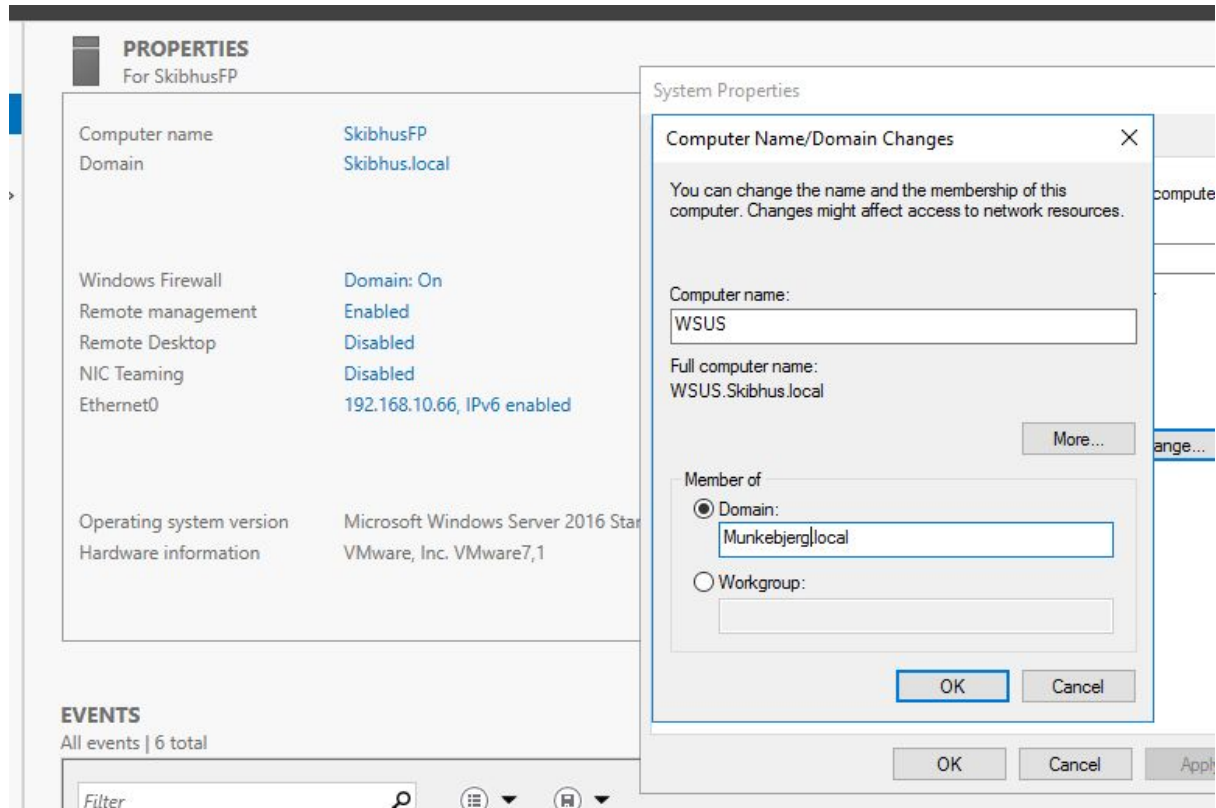


Fjerner trust fra begge DC maskiner.

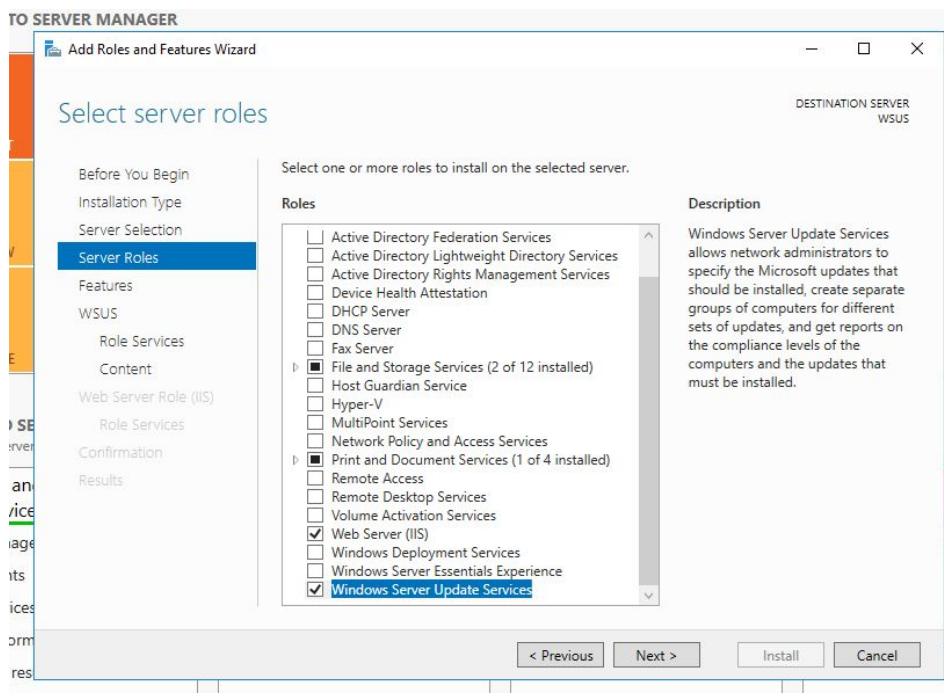


Oprettelse WSUS:

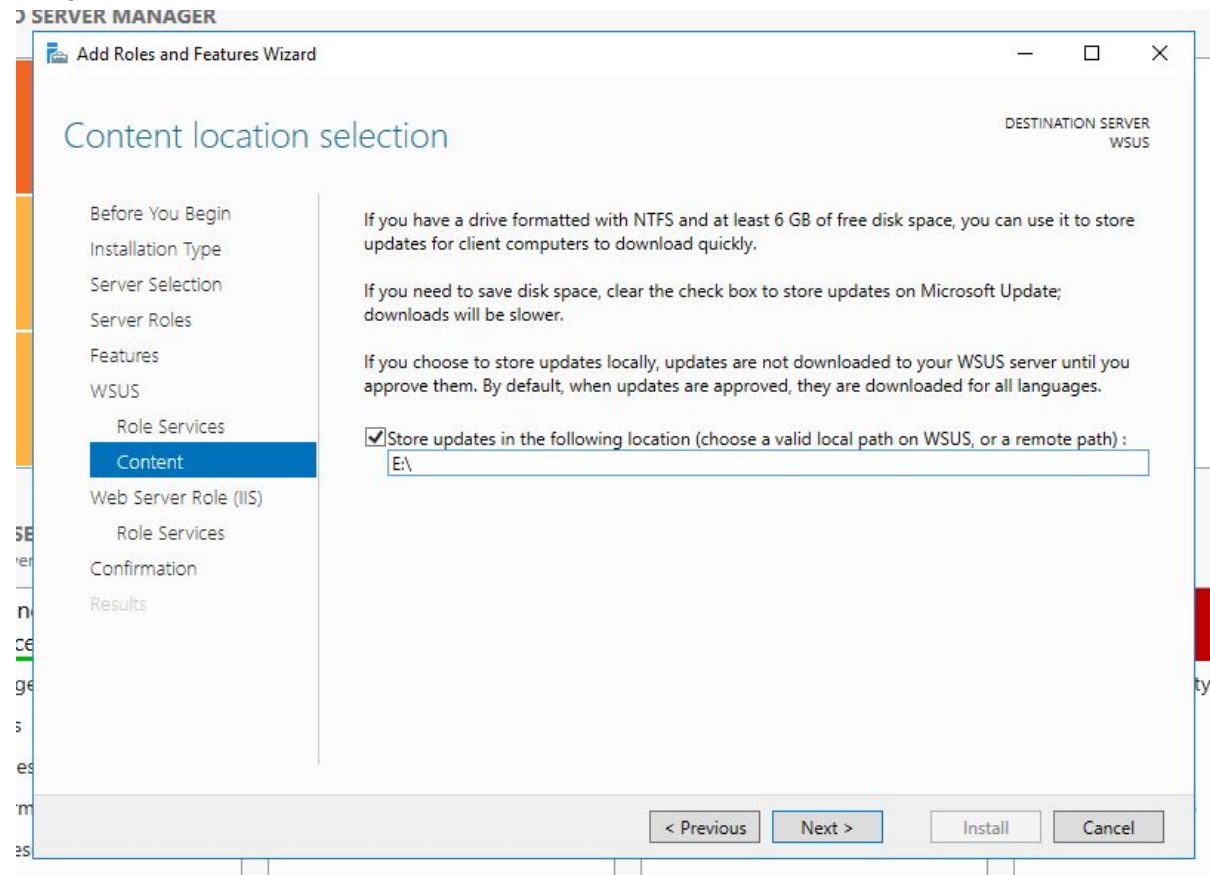
Ændrer navn og domain på den gamle fil og print server (SkibhusFP).



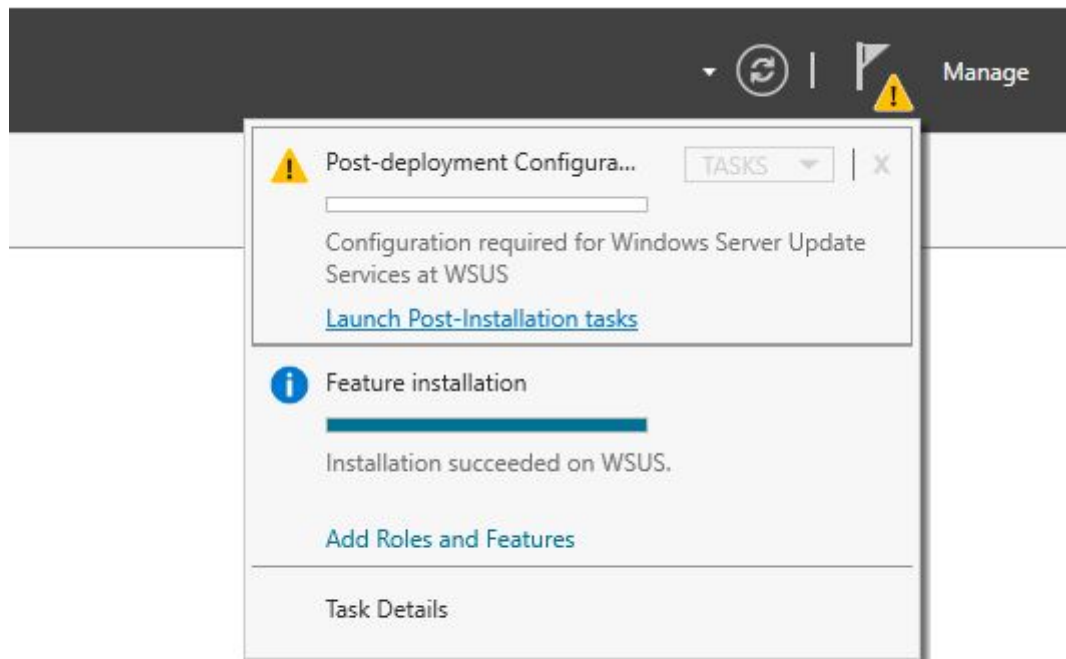
Installer WSUS via “Add Roles and Features Wizard”.



Vælg drev/mappe lokation. E:\

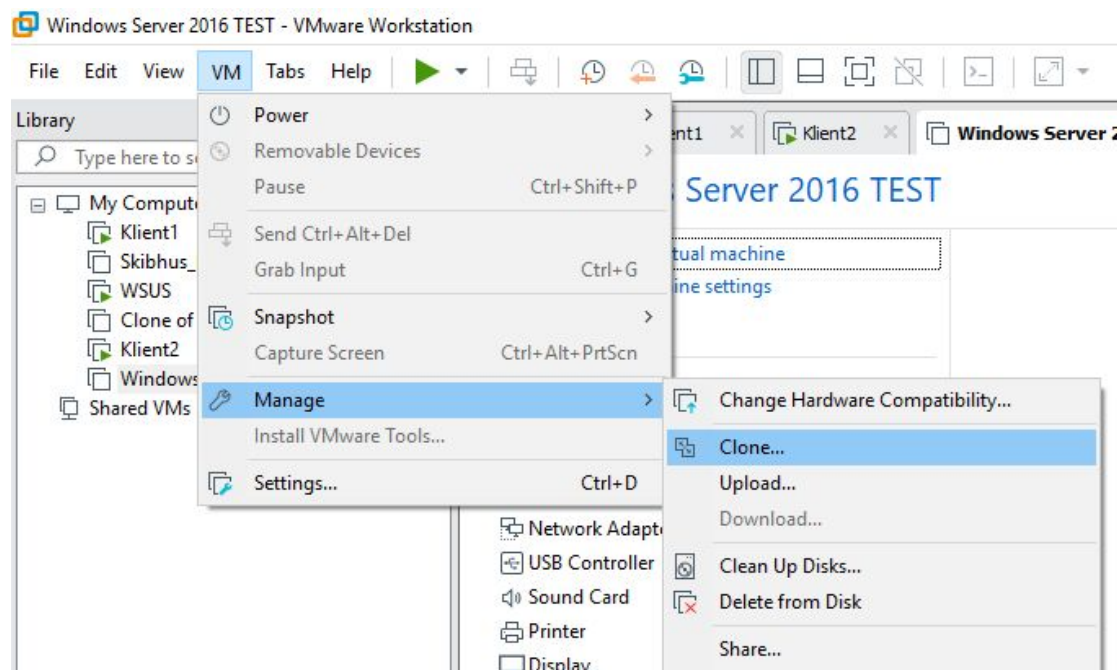


Klik på "Launch Post-Installation tasks".

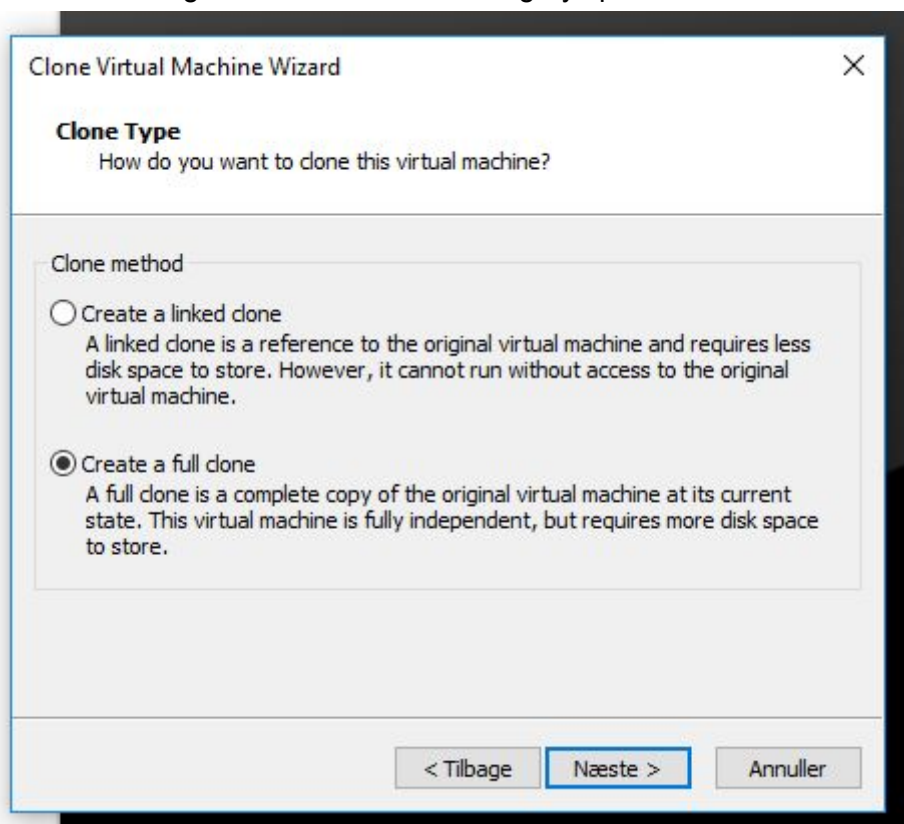


Cloning af Skibhus VMWare og flytning til Munkebjerg:

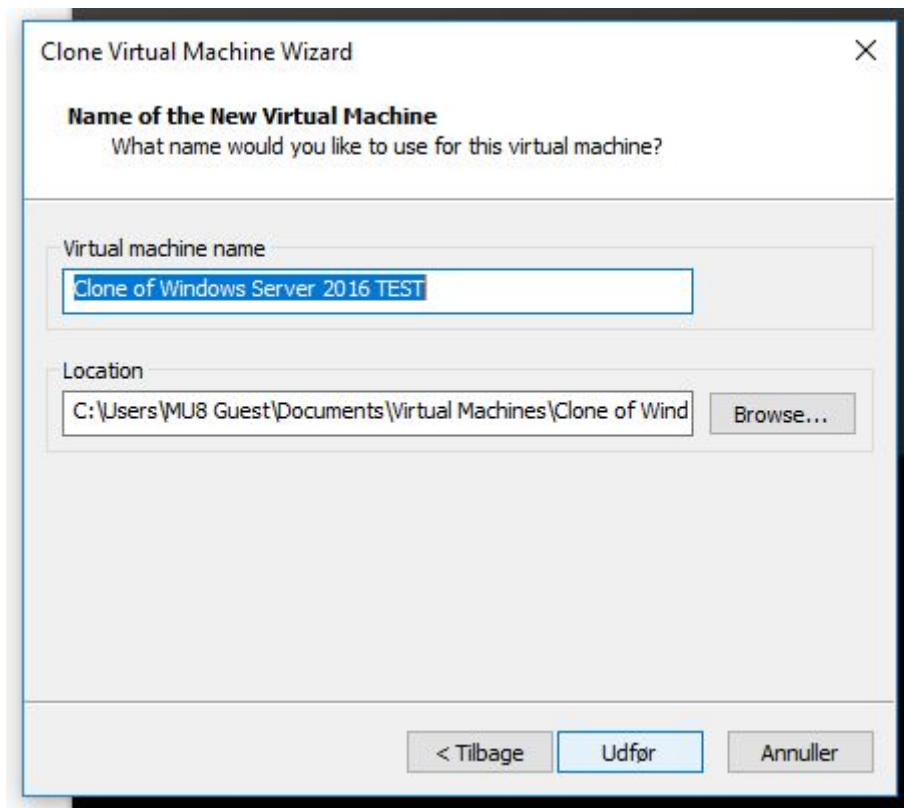
Vi kloner og flytter Skibhus DC til Munkebjerg i VMWare.



Her skal der vælges "Create a full clone" og tryk på "Næste".

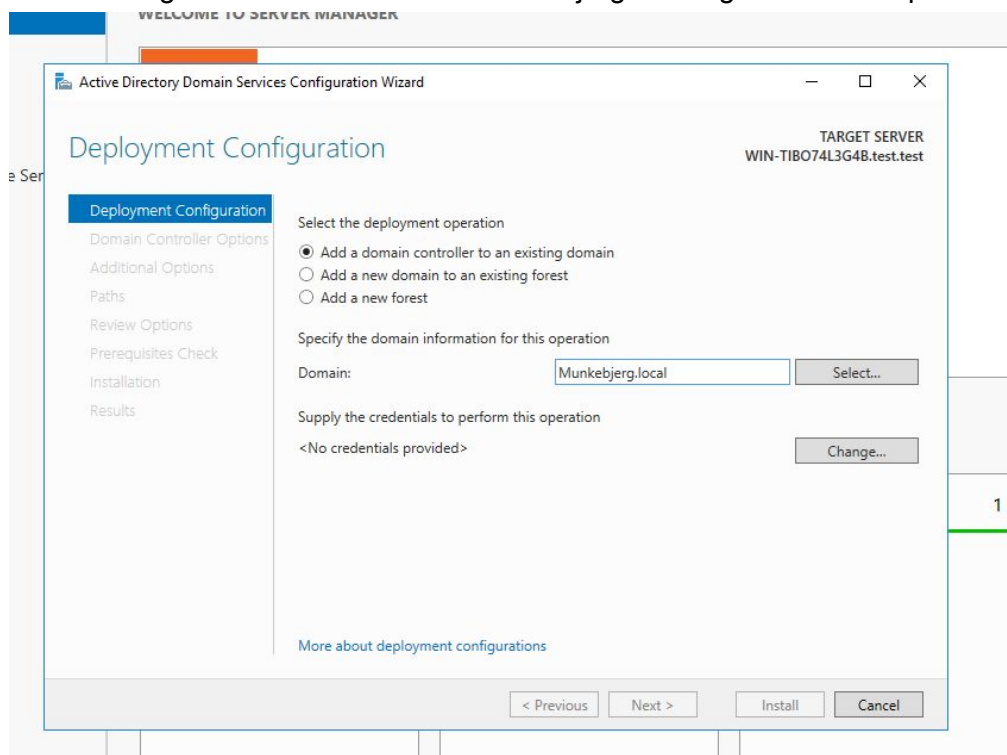


Navngiv din VM-clone.



The image shows a 'Clone Virtual Machine Wizard' dialog box. The title bar says 'Clone Virtual Machine Wizard' with a close button. The main heading is 'Name of the New Virtual Machine' with the question 'What name would you like to use for this virtual machine?'. Below this, there is a text box labeled 'Virtual machine name' containing the text 'Clone of Windows Server 2016 TEST'. Below that is a text box labeled 'Location' containing the path 'C:\Users\MU8 Guest\Documents\Virtual Machines\Clone of Wind'. To the right of the 'Location' text box is a 'Browse...' button. At the bottom of the dialog are three buttons: '< Tilbage', 'Udfør', and 'Annuller'.

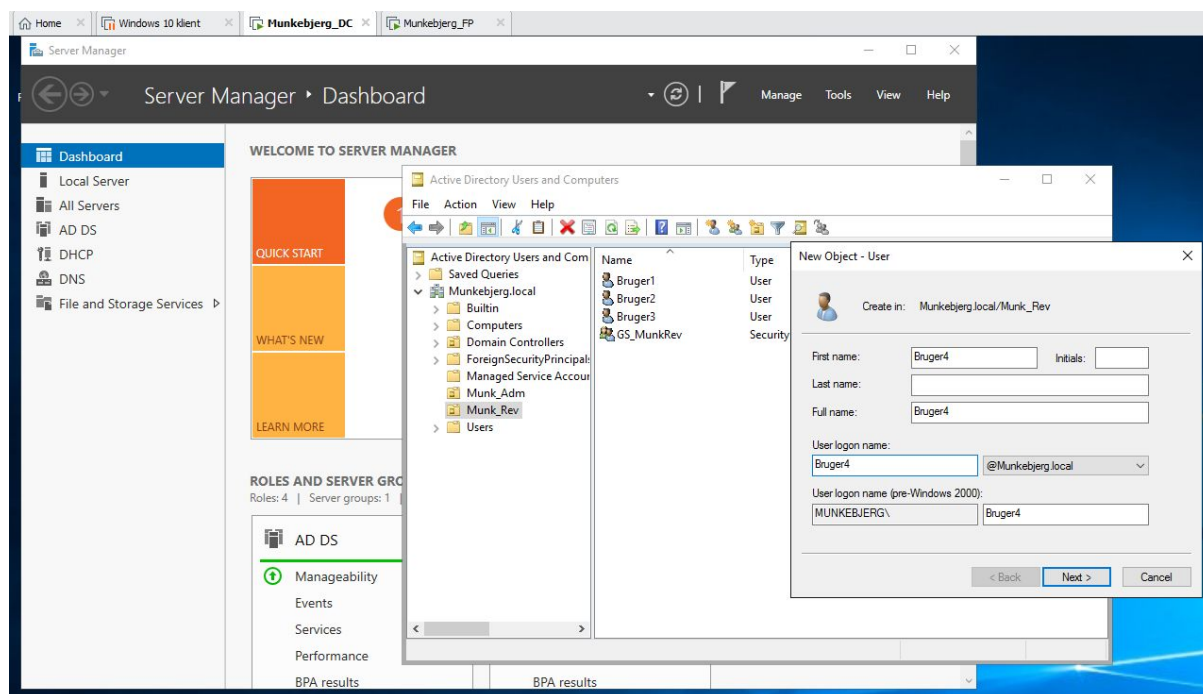
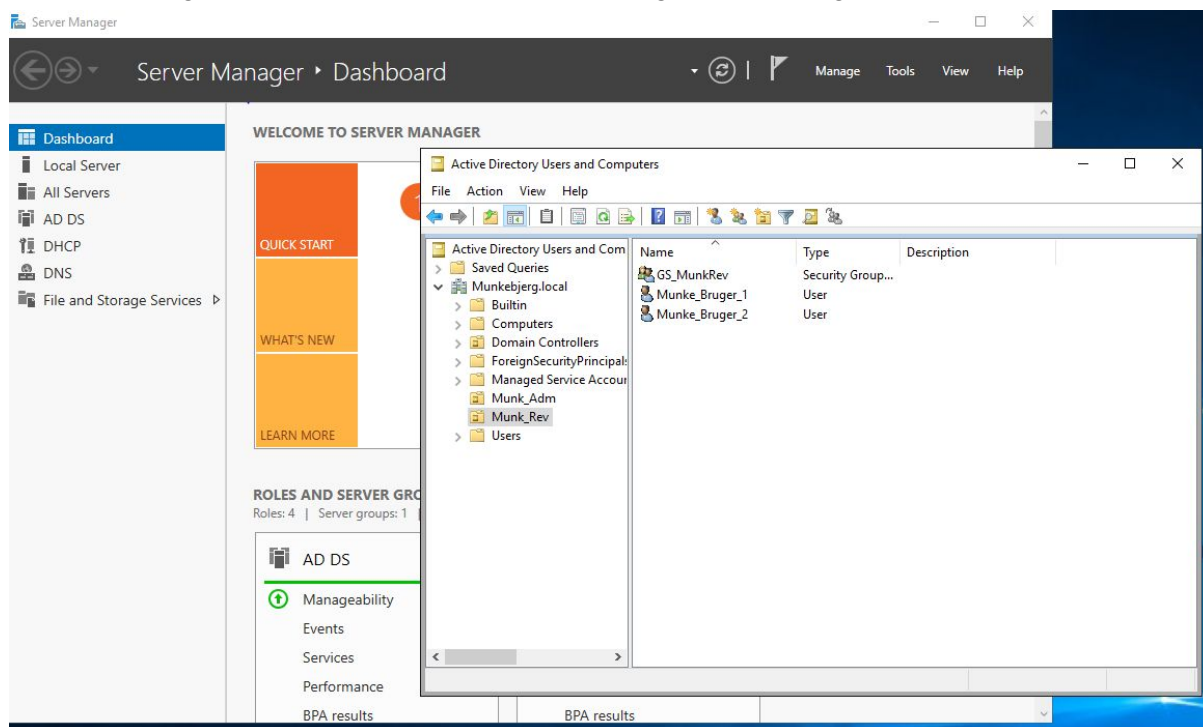
Melder den gamle Skibhus DC ind i Munkebjerg.local og sætter den op som Munkebjerg DC2.



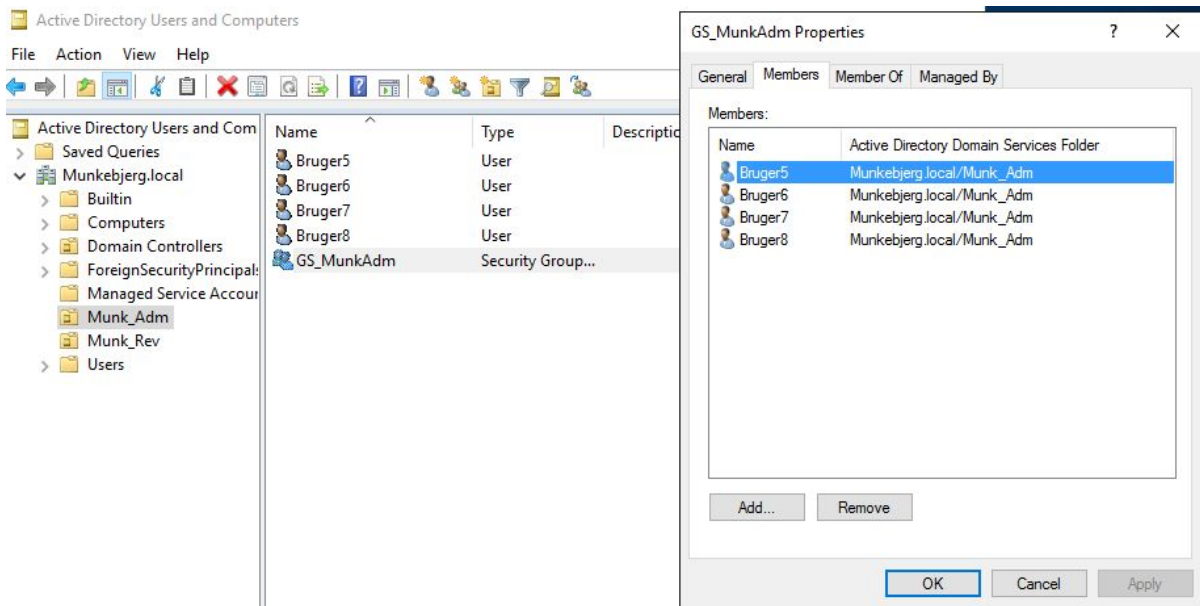
The image shows the 'Active Directory Domain Services Configuration Wizard' window, specifically the 'Deployment Configuration' step. The title bar says 'Active Directory Domain Services Configuration Wizard'. The main heading is 'Deployment Configuration'. On the right, it says 'TARGET SERVER WIN-TIB074L3G4B.test.test'. On the left, there is a navigation pane with the following items: 'Deployment Configuration' (selected), 'Domain Controller Options', 'Additional Options', 'Paths', 'Review Options', 'Prerequisites Check', 'Installation', and 'Results'. The main area contains the following options: 'Select the deployment operation' with three radio buttons: 'Add a domain controller to an existing domain' (selected), 'Add a new domain to an existing forest', and 'Add a new forest'. Below this is 'Specify the domain information for this operation' with a 'Domain:' label and a text box containing 'Munkebjerg.local', and a 'Select...' button. Below that is 'Supply the credentials to perform this operation' with the text '<No credentials provided>' and a 'Change...' button. At the bottom, there is a link 'More about deployment configurations'. At the very bottom are four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'. On the right side of the window, there is a small green bar with the number '1'.

Oprettelse af brugere:

Her bliver brugernes navn ændret fra "Munke_Bruger_1" til "Bruger1" osv.

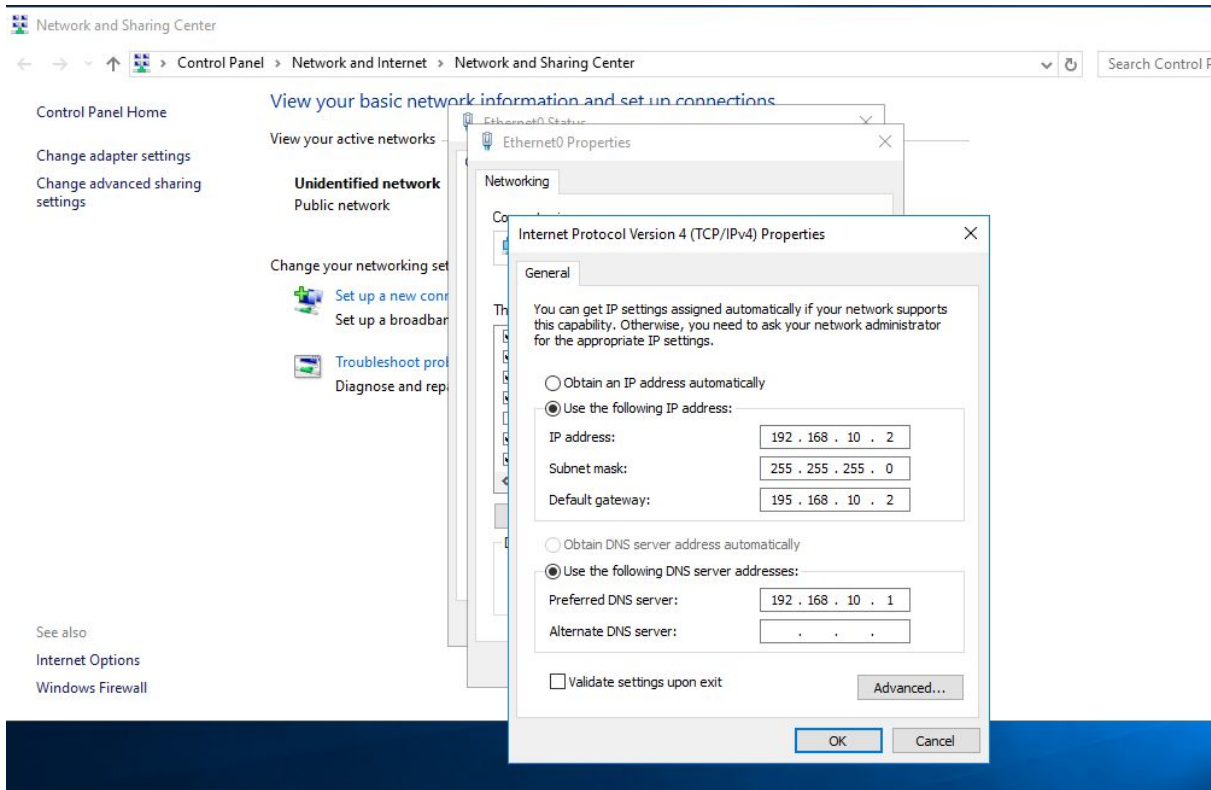
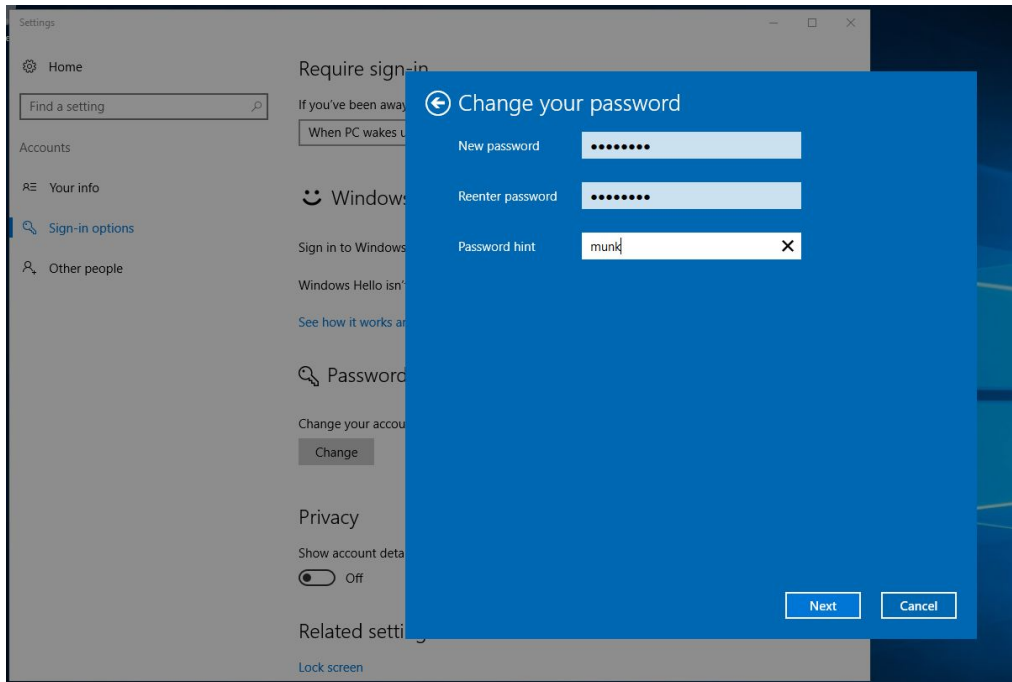


Vi melder de nye bruger ind i GS og GS ind i DL.



Ændring af IP og PC navne:

Der bliver skiftet navn og password på pc'erne, ændret Ip'er , og installeret AD og DNS på den nye GC. Forest bliver sat op til eksisterende Munkebjerg.local




Home

DC1

DC2

Munkebjerg_FP


Recycle Bin

Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
DC2.Munkebjerg.local

Before You Begin

Installation Type

Server Selection

Server Roles

Features

AD DS

DNS Server

DHCP Server

Confirmation

Results

Select one or more roles to install on the selected server.

Roles

☐ Active Directory Certificate Services

☒ Active Directory Domain Services

☐ Active Directory Federation Services

☐ Active Directory Lightweight Directory Services

☐ Active Directory Rights Management Services

☐ Device Health Attestation

☒ DHCP Server

☒ DNS Server

☐ Fax Server

☒ File and Storage Services (2 of 12 installed)

☐ Host Guardian Service

☐ Hyper-V

☐ MultiPoint Services

☐ Network Policy and Access Services

☐ Print and Document Services

☐ Remote Access

☐ Remote Desktop Services

☐ Volume Activation Services

☐ Web Server (IIS)

☐ Windows Deployment Services

Description

Dynamic Host Configuration Protocol (DHCP) Server enables you to centrally configure, manage, and provide temporary IP addresses and related information for client computers.

< Previous

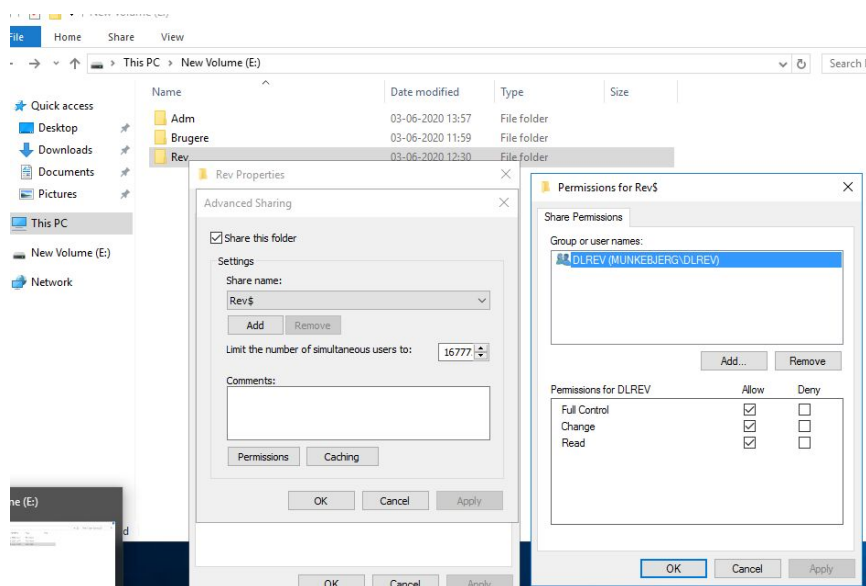
Next >

Install

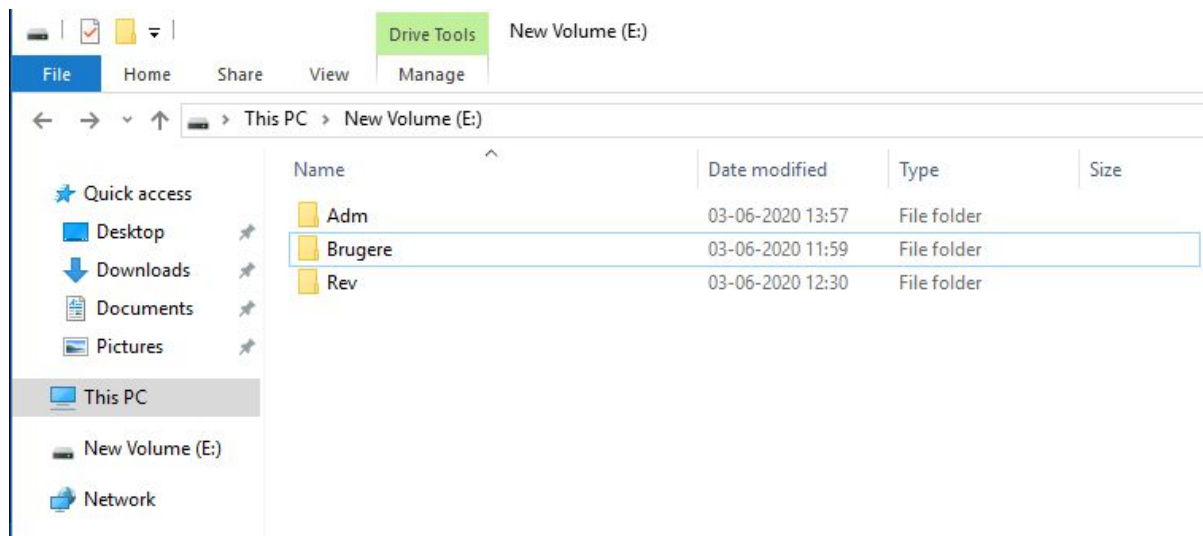
Cancel

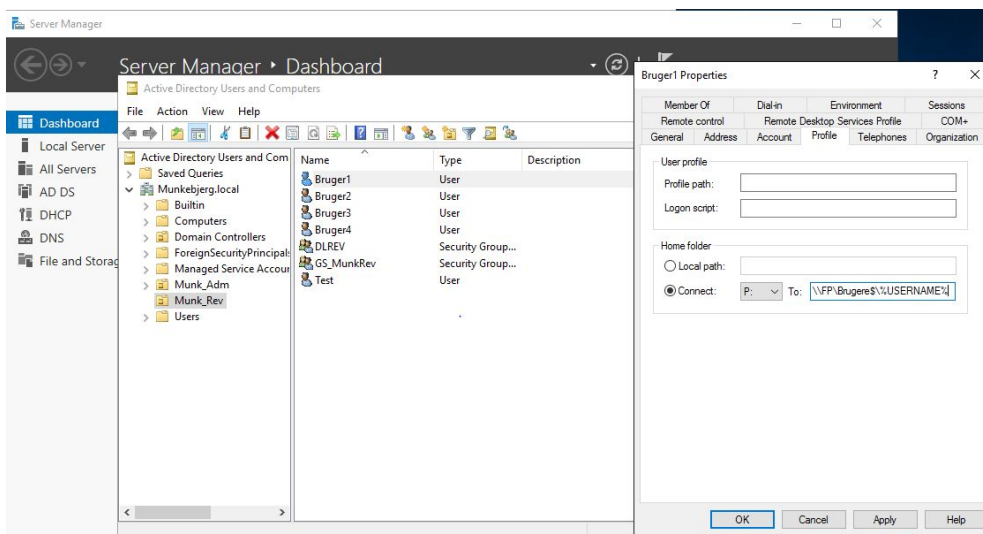
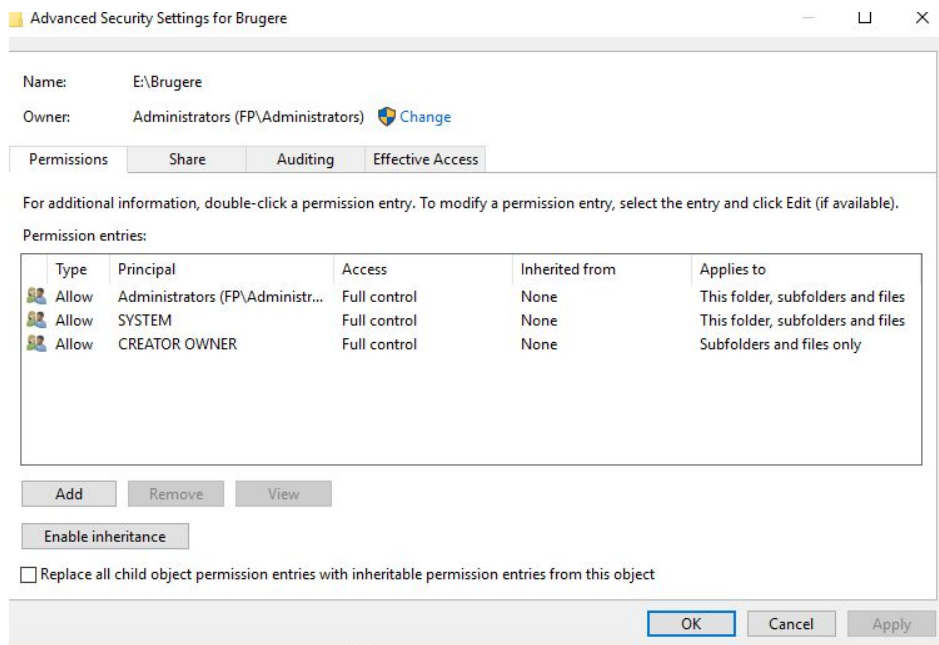
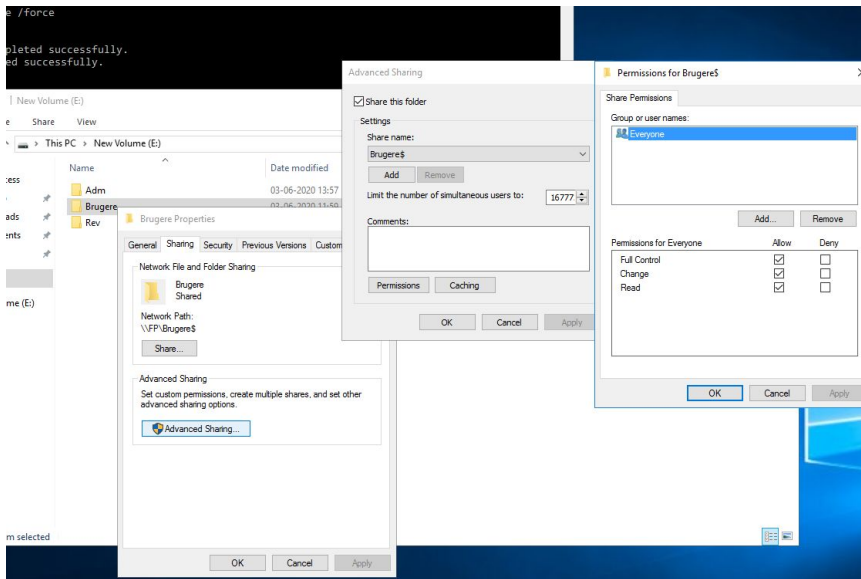
Mapping af drev og mapper:

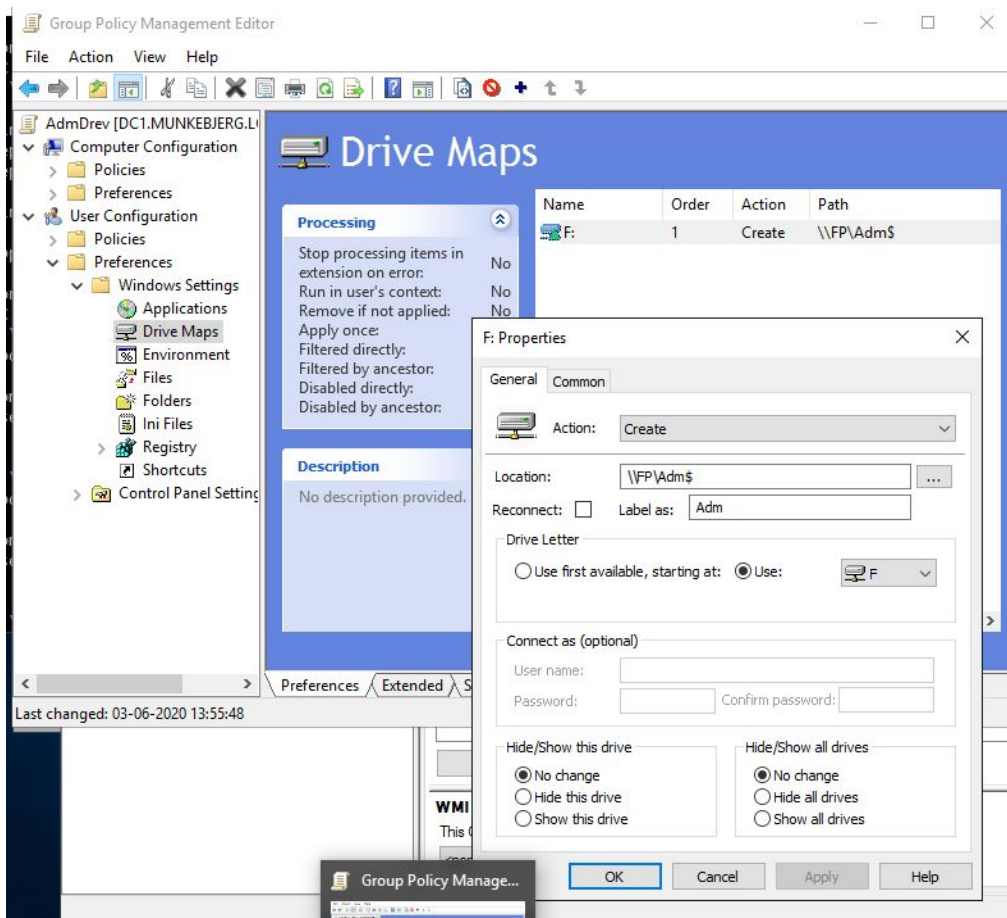
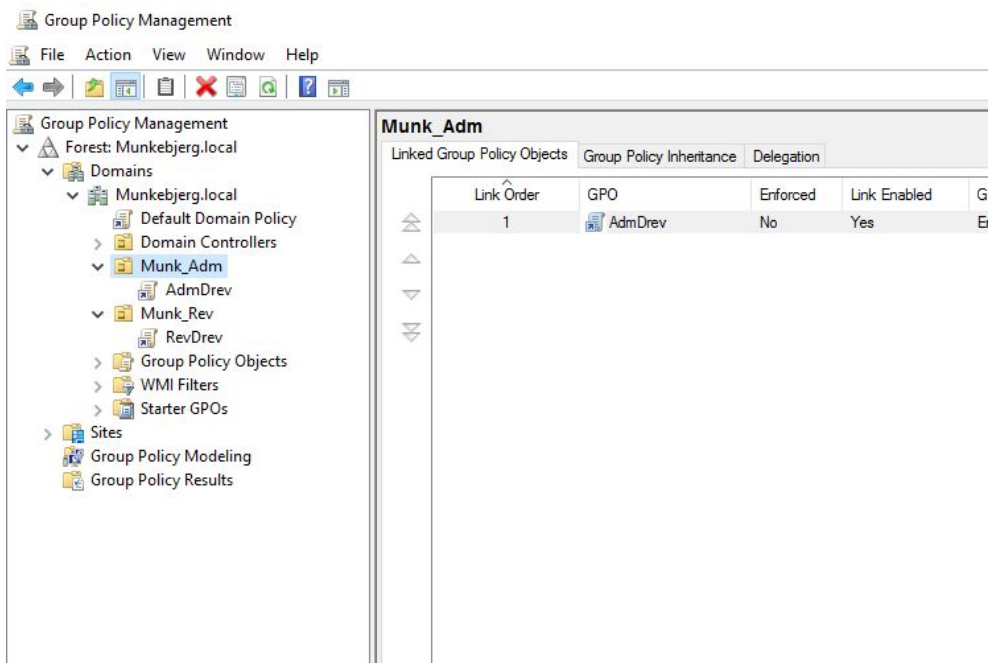
Oprettet mapper på vores fil og printer server. Her bliver de mappet til pågældende OU som skal have adgang til dem. Der bliver lavet en mappe til Rev, Adm og en personlig til brugerne.



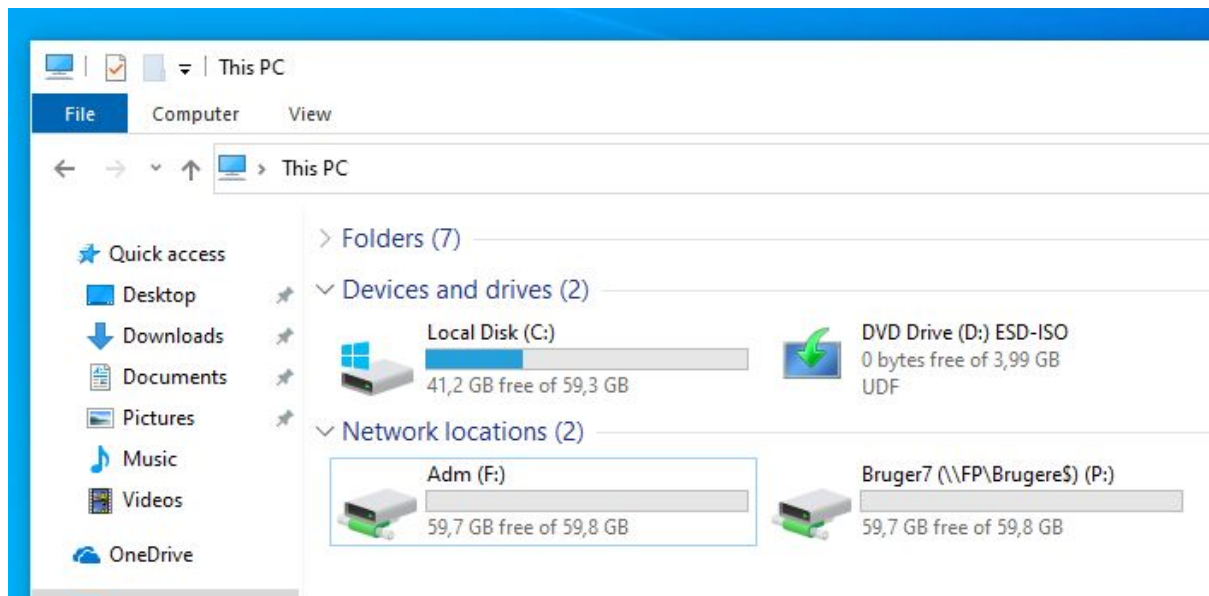
Til den personlige mappe har vi brugt %USERNAME% så den selv opretter en mappe til den bruger. Hvorimod Rev og Adm bliver lavet some GPO'er og igennem DL grupper. Vi har brugt "\$" for at skjule mapperne (drev) for andre som ikke skal kunne se dem.





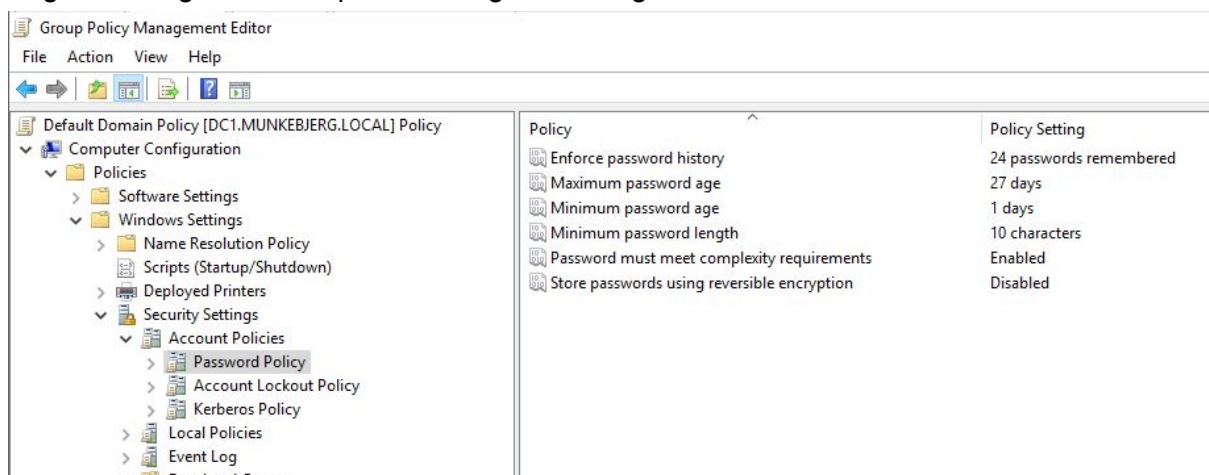


Her viser vi at "Bruger5" har adgang til Adm drevet og hans egen personlige drev:



Krav om password:

Vi har under GPO>Default Domain Policy>Windows Settings>Password Policy, sat password minimum length til 10 og maximum password age til 27 dage.



Vi har under GPO>Default Domain Policy>Windows settings>Local policy>Security Options, ændret følgende, "Do not display last Username". Hvilket gør at man på en klient ikke kan se hvem der sidst har logget ind.



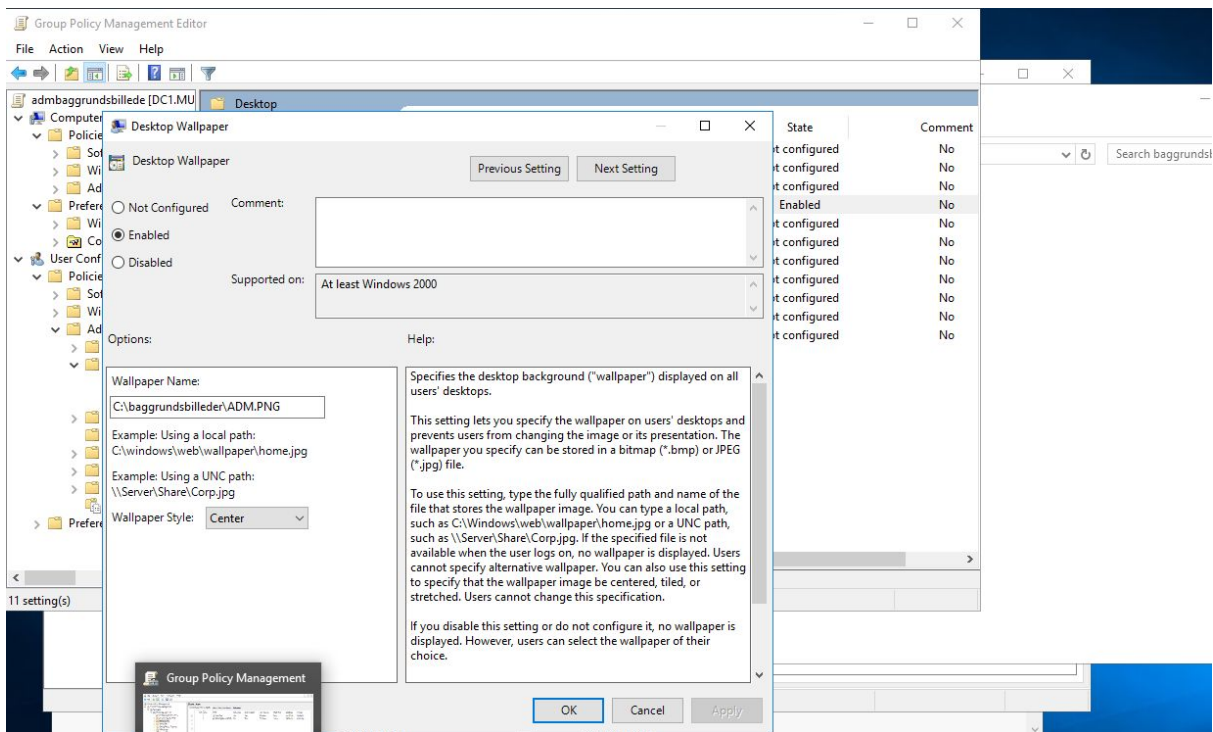
Baggrundsbillede til hver afdeling:

Under henholdsvis Adm og Rev, har vi lavet en ny GPO til at give hver afdeling deres eget baggrundsbillede.

The screenshot shows the Group Policy Management Editor interface. At the top, there are tabs for 'Linked Group Policy Objects', 'Group Policy Inheritance', and 'Delegation'. Below these is a table listing GPOs:

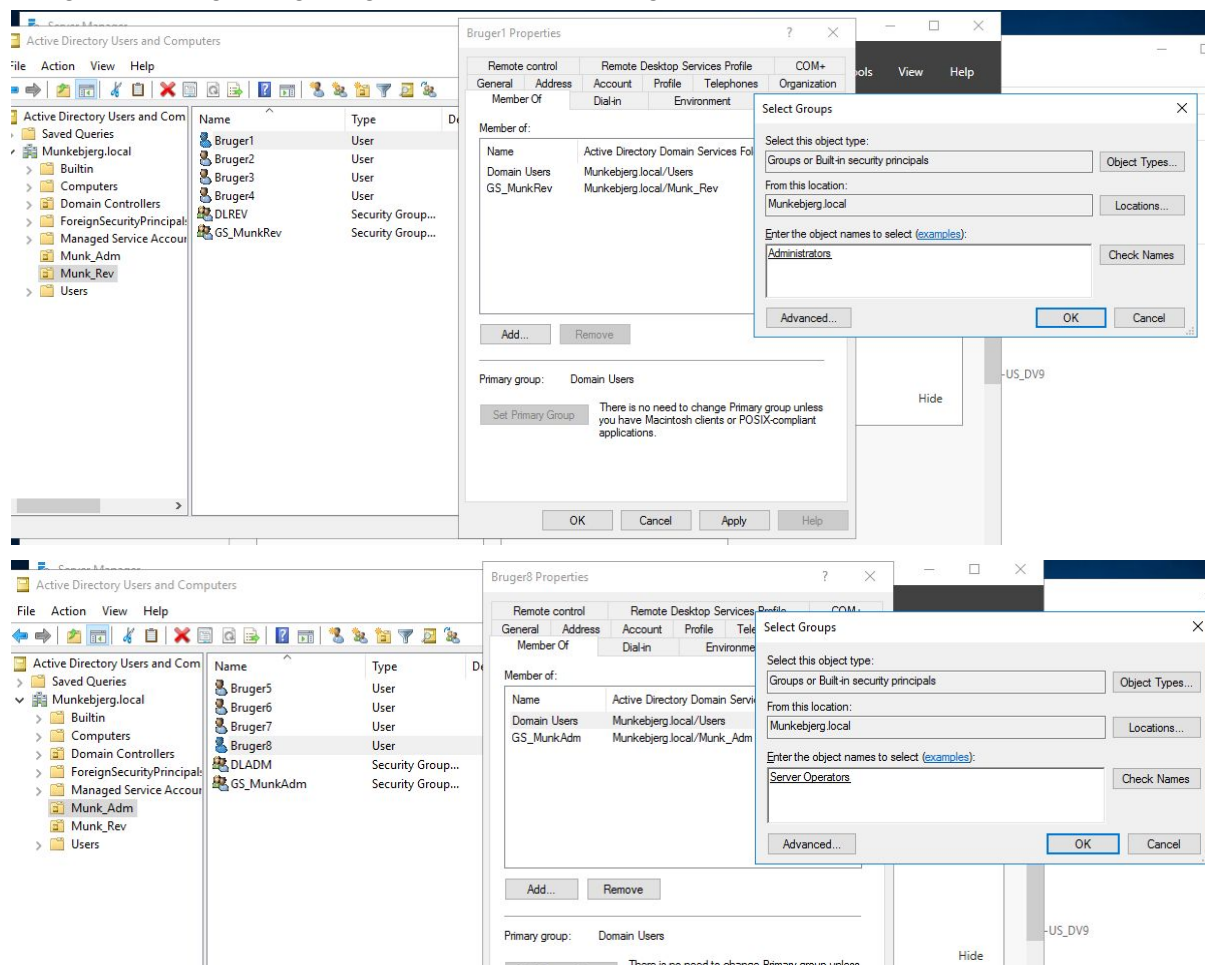
Link Order	GPO	Enforced	Link Enabled	GPO Status	WMI Filter	Modified	Domain
1	AdmDrev	No	Yes	Enabled	None	03-06-20...	Munkebj...
2	admbaggrundsbillede	No	Yes	Enabled	None	04-06-20...	Munkebj...

Below the table, the 'Group Policy Management Editor' window is open, showing the configuration for the 'admbaggrundsbillede [DC1.MUNKE]' GPO. The left pane shows the tree structure: 'Computer Configuration' > 'User Configuration' > 'Policies' > 'Administrative Templates' > 'Desktop'. The right pane shows the 'Desktop Wallpaper' policy, which is currently set to 'Not Configured'. The 'Setting' list on the right includes: 'Enable Active Desktop', 'Disable Active Desktop', 'Prohibit changes', 'Desktop Wallpaper' (selected), 'Prohibit adding items', 'Prohibit closing items', 'Prohibit deleting items', 'Prohibit editing items', 'Disable all items', 'Add/Delete items', and 'Allow only bitmapped wallpaper'.



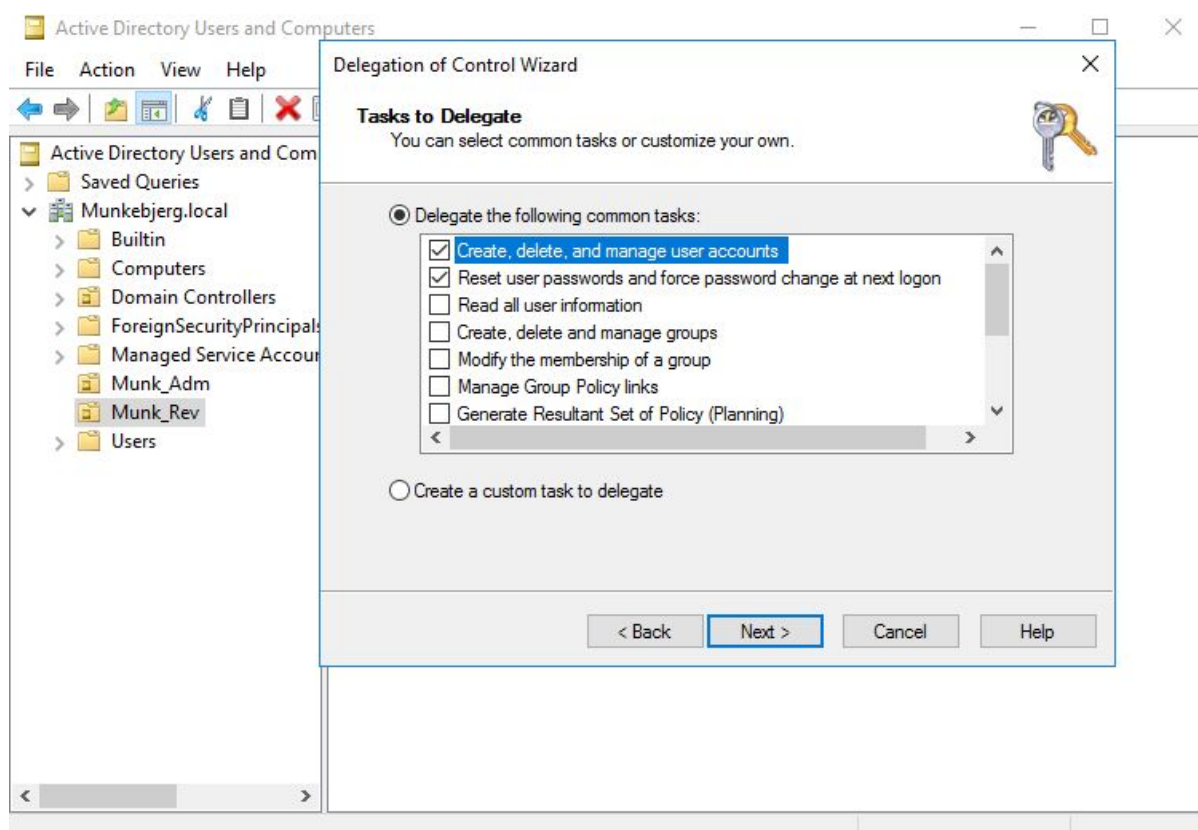
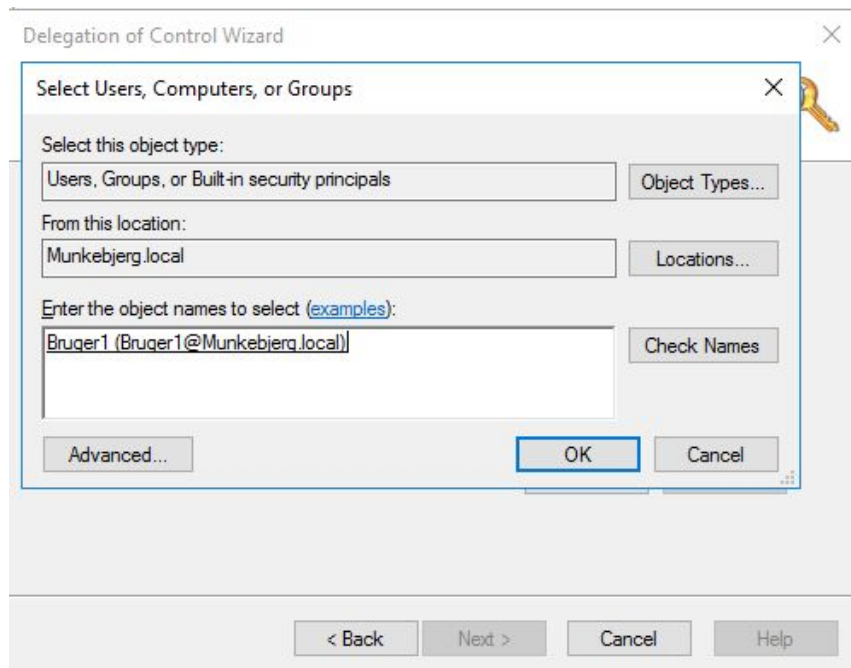
Domain administrator og serveroperator:

Her giver vi Bruger1 og Bruger8 Domain Admin og Serveroperator.

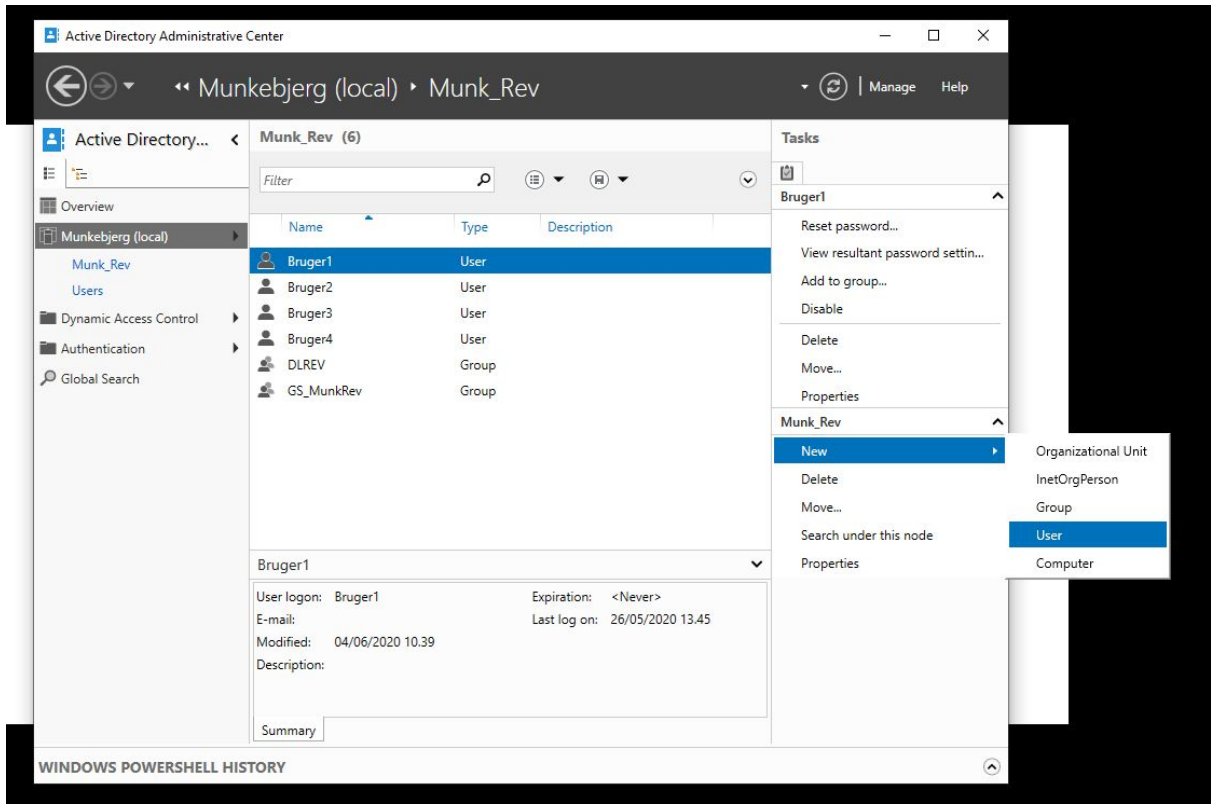
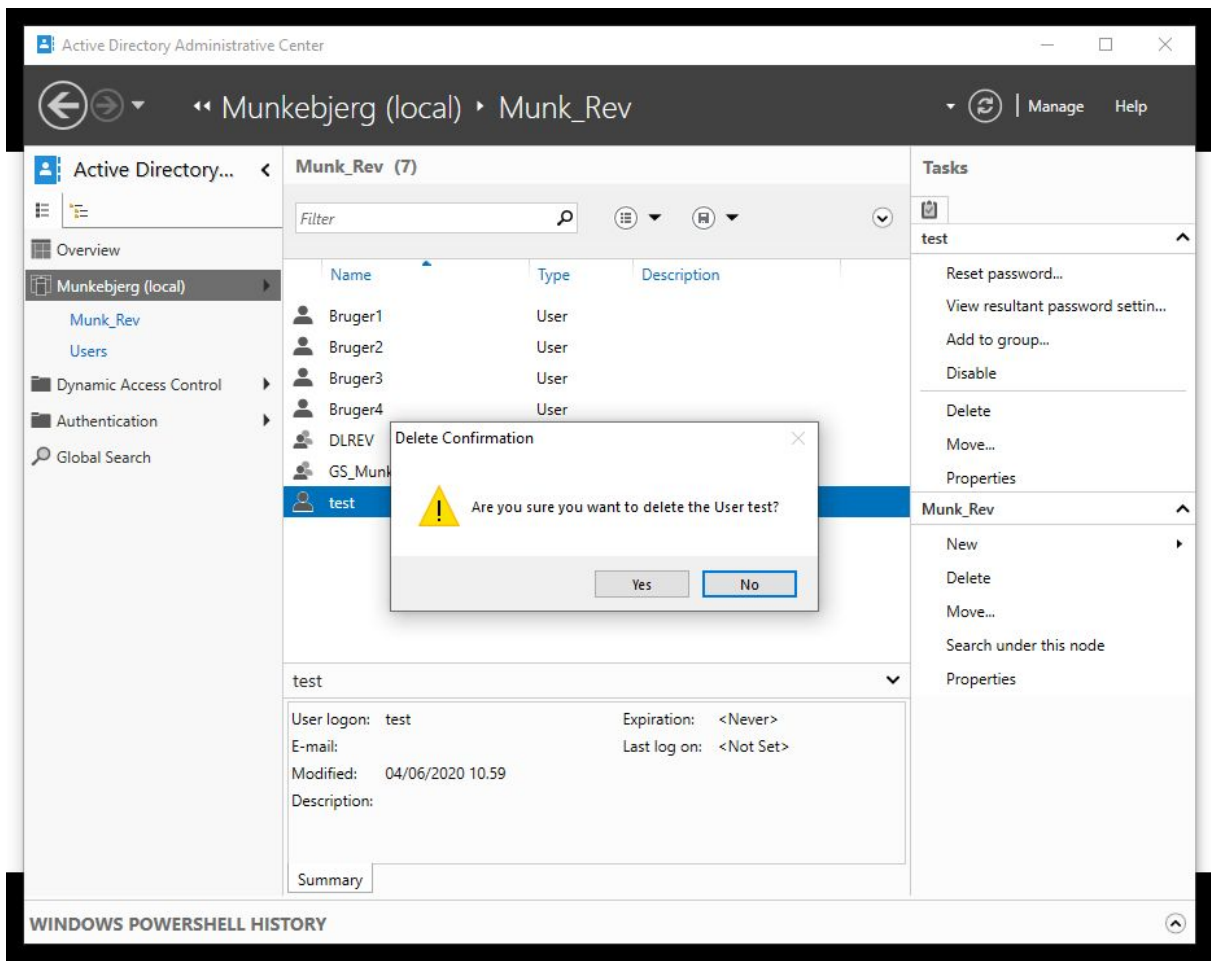


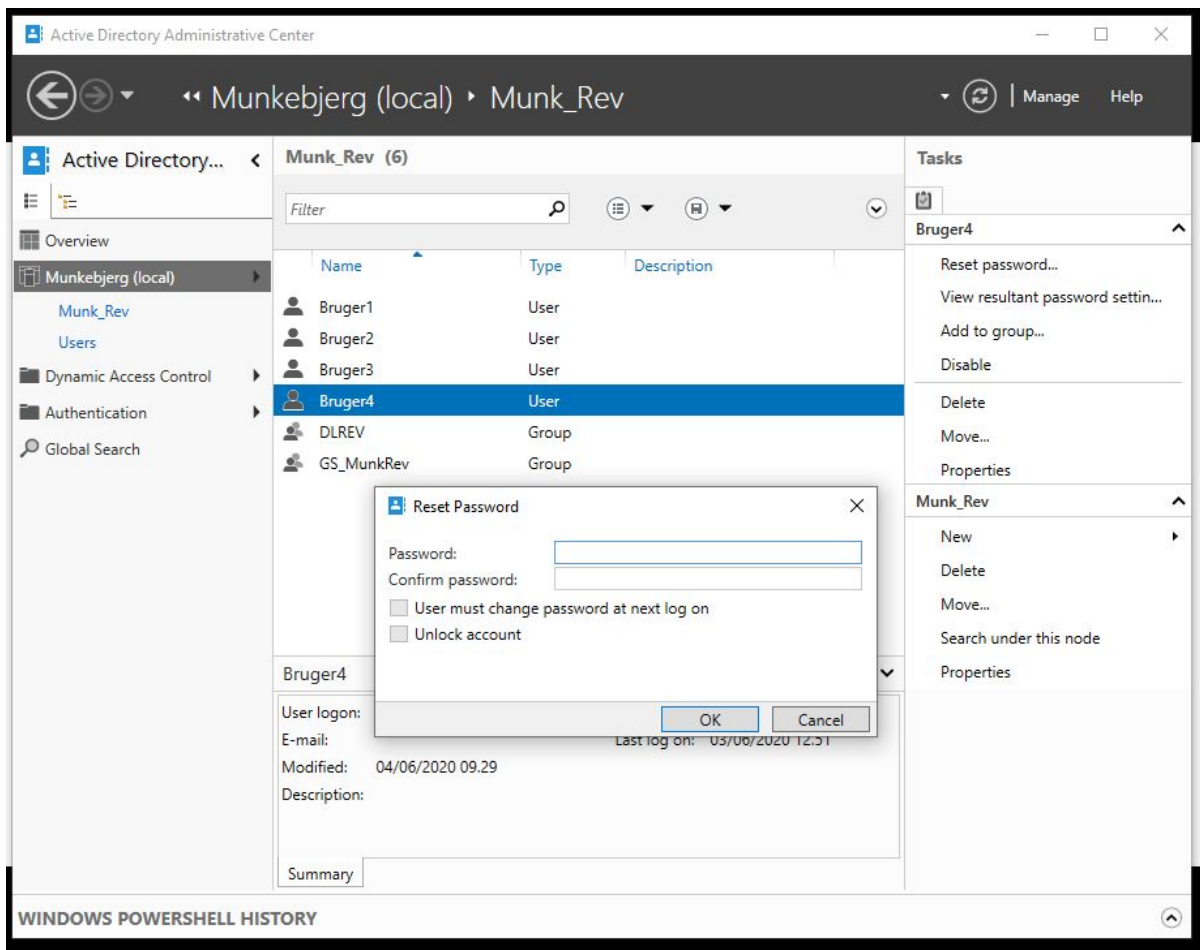
Superbruger i hver afdeling:

Vi har lavet Bruger1 og Bruger8 til superbruger med rettigheder til at lave og slette brugere og ændre og nulstille deres passwords. Efter her har vi installeret RSAT som man bruger på klienten sammen med superbruger til at ændre de her passwords og brugerindstillinger:



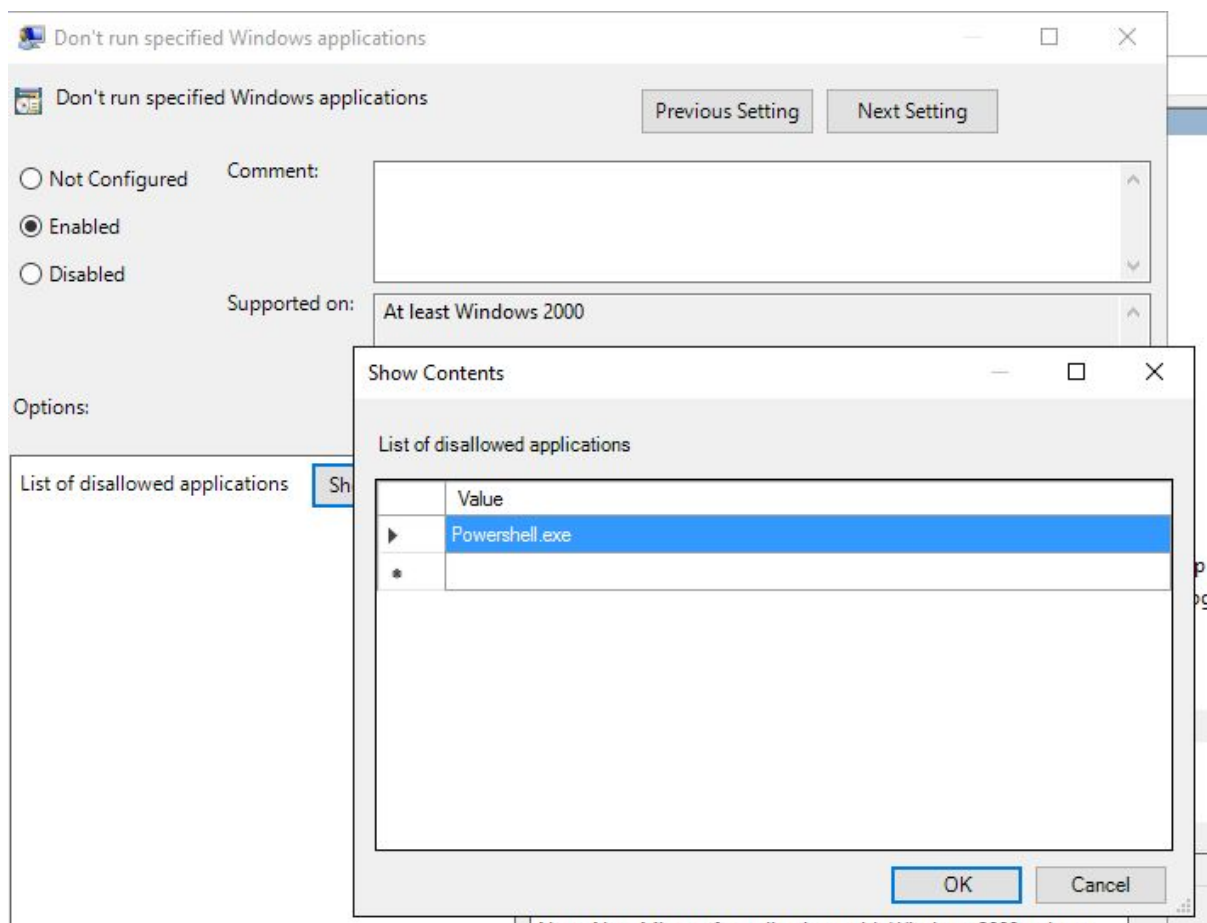
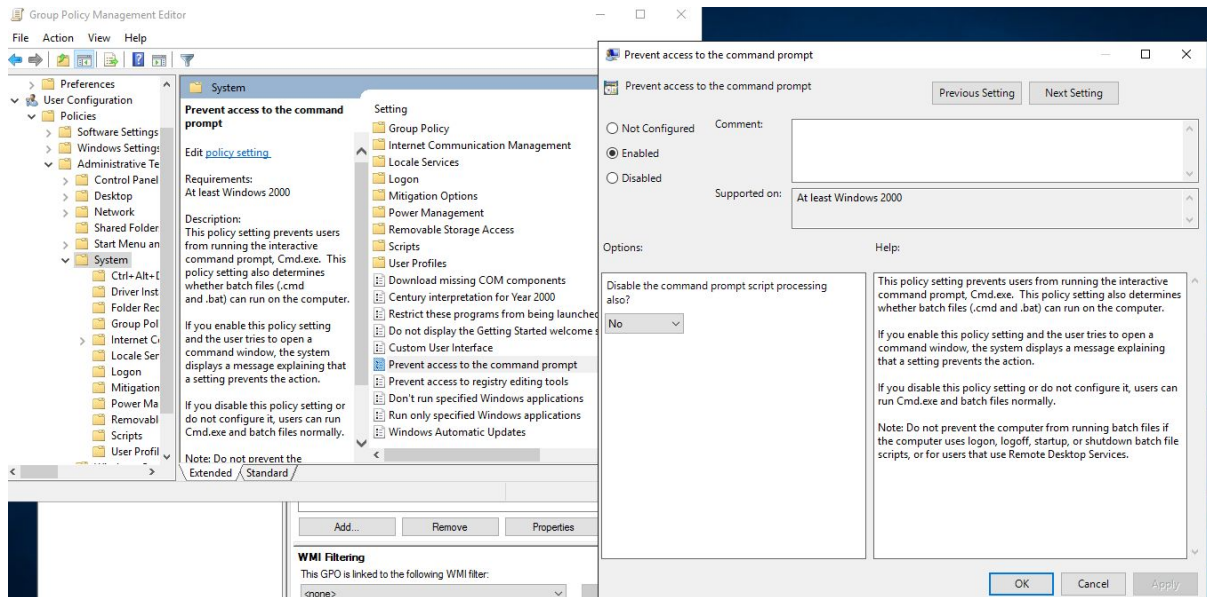
Her viser vi brugen af Server admin toolkit:





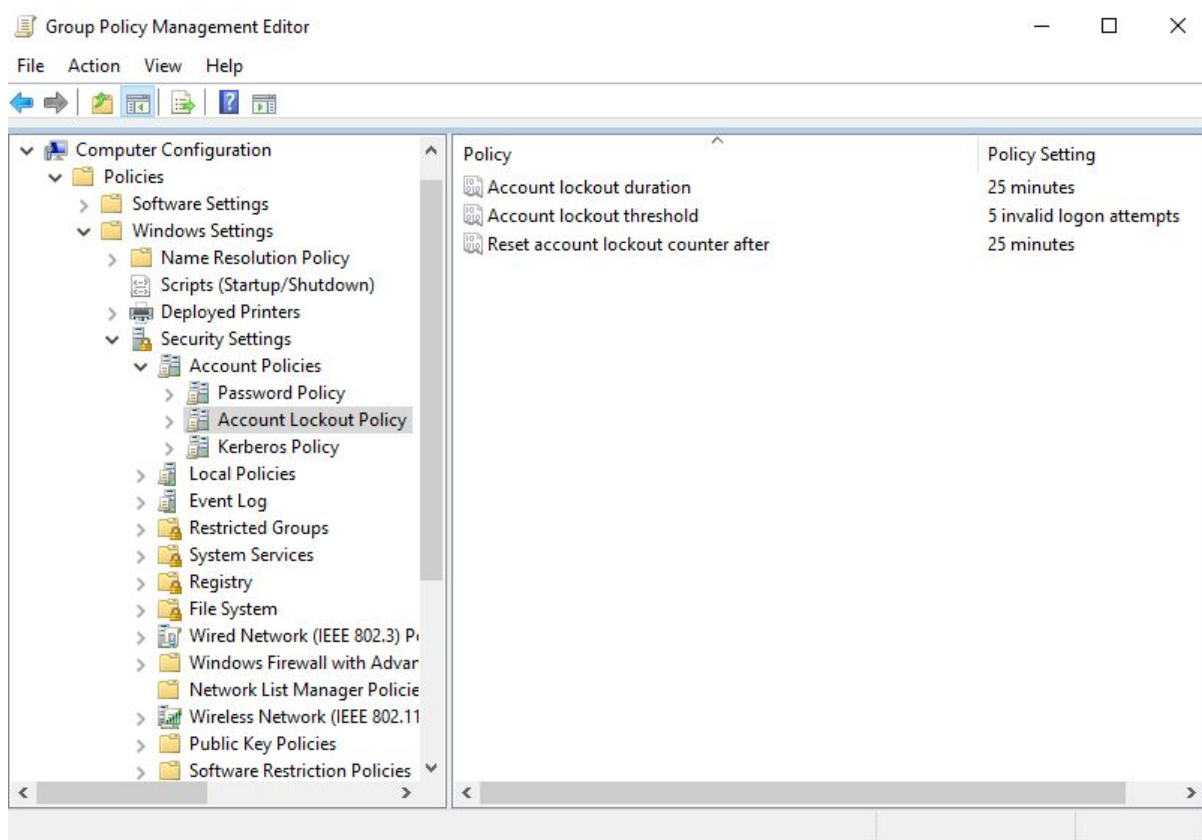
Almindelige bruger skal ikke have adgang til CDM eller Powershell:

Vi har lavet en ny GPO og under security filtering sat både vore rev og adm ind. Der næst har vi enabled policy: prevent access to the command prompt og, don't run specific windows applications, hvor vi har skrevet Powershell.exe.

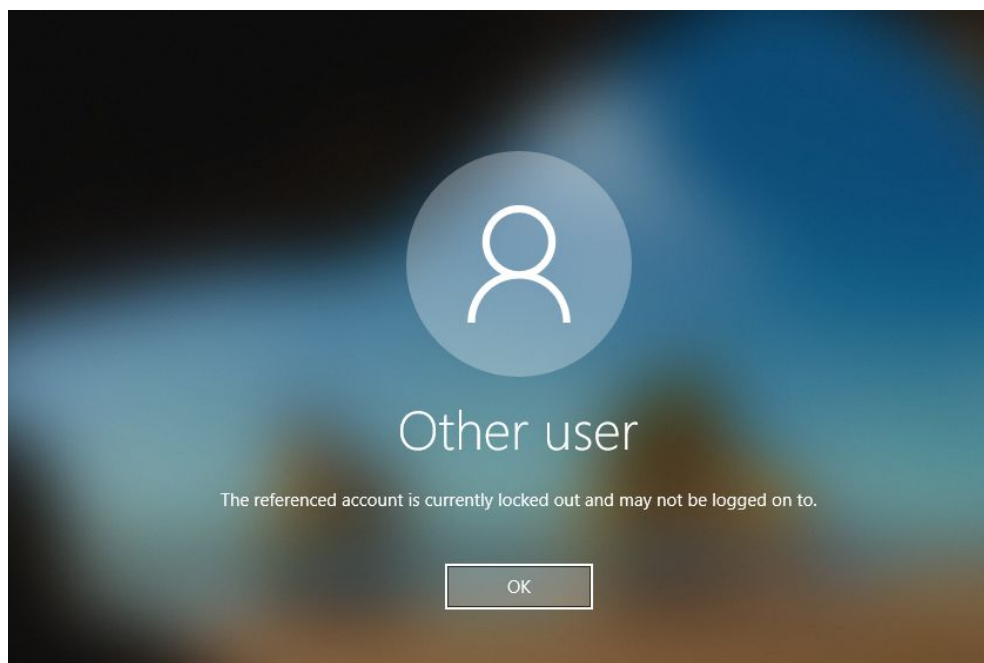


Lås bruger i 25 min ved 5 fejl-login:

I denne policy ændre vi account lockout threshold til 5 og lockout duration til 25 min:

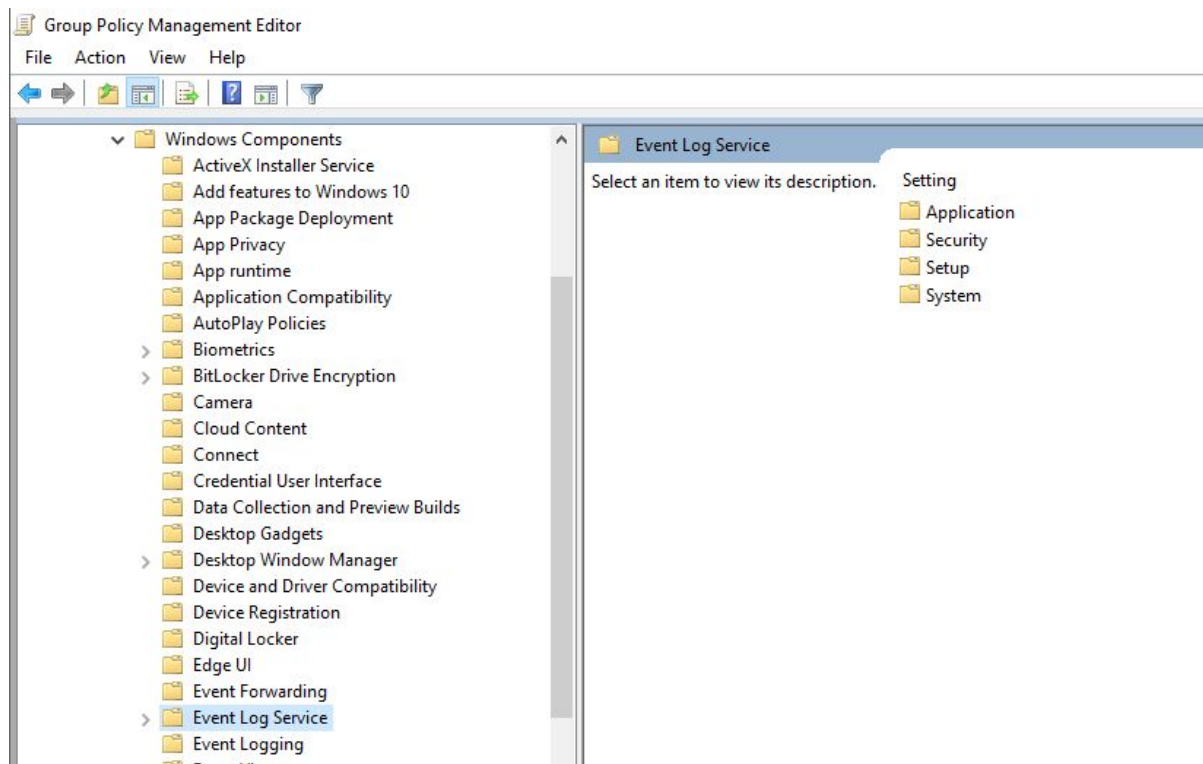


Her er resultatet:

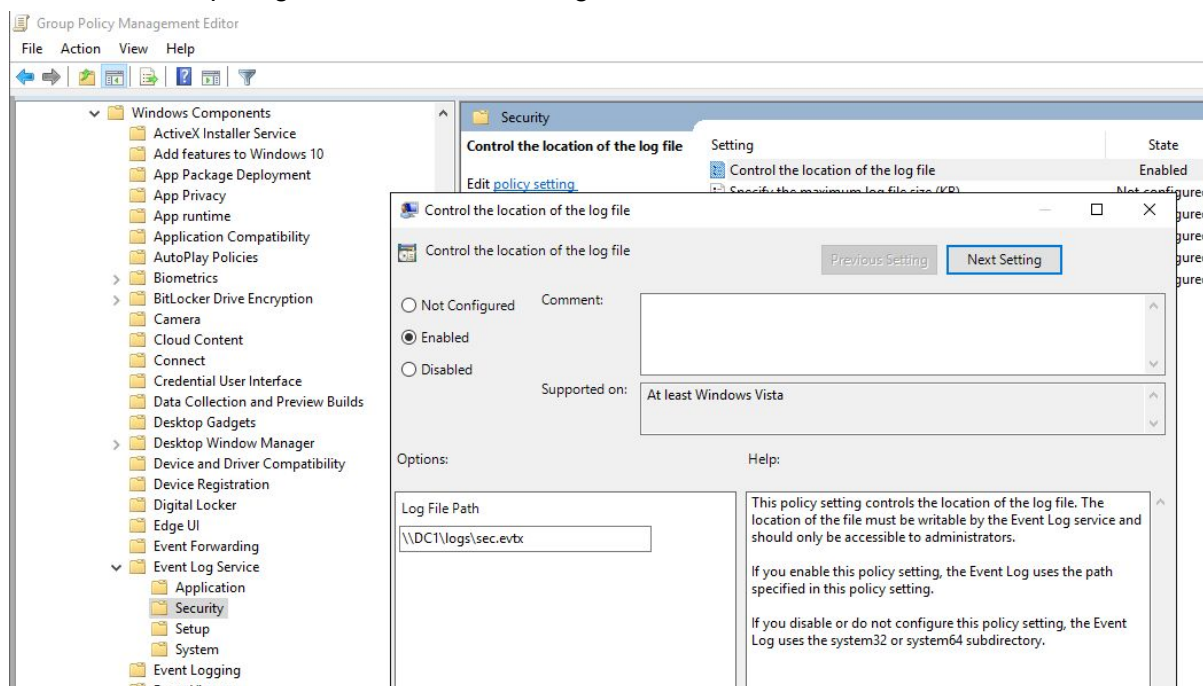


Security Event logfiler:

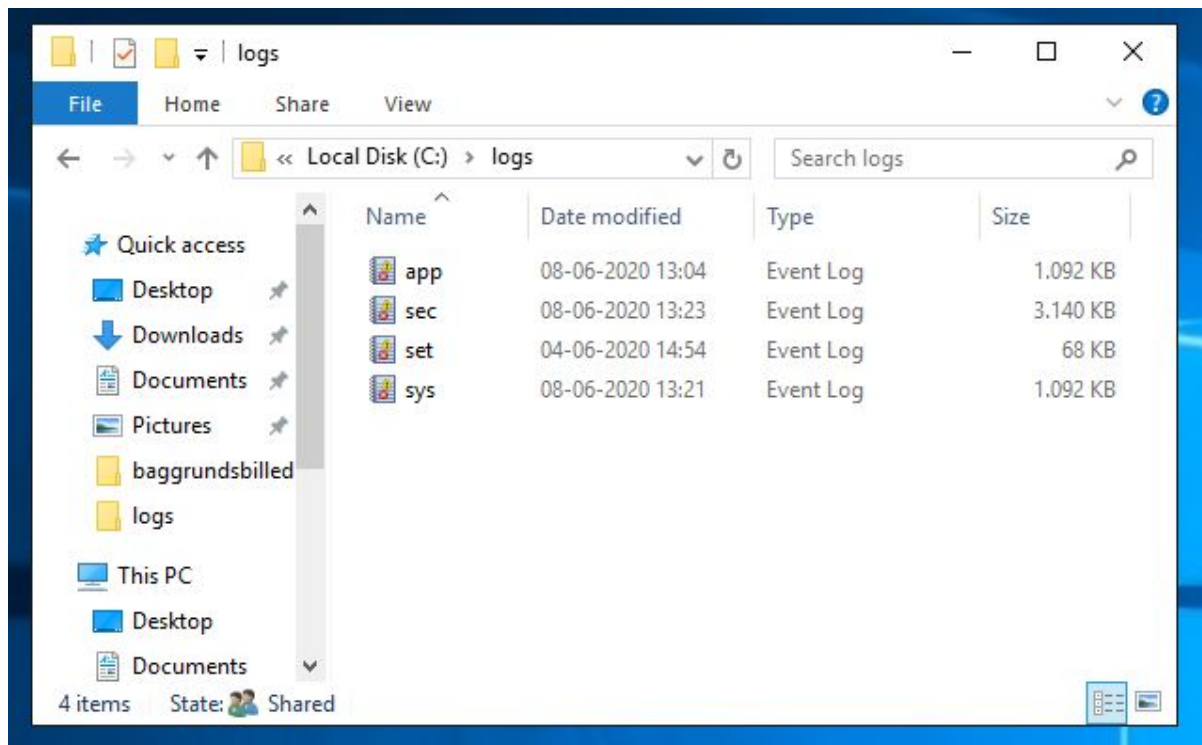
Naviger til "GPO", "Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Security" og sæt en location hvor filerne skal gemmes.



Sætter location på log filerne. Eks.: \\DC1\logs\sec.evtx



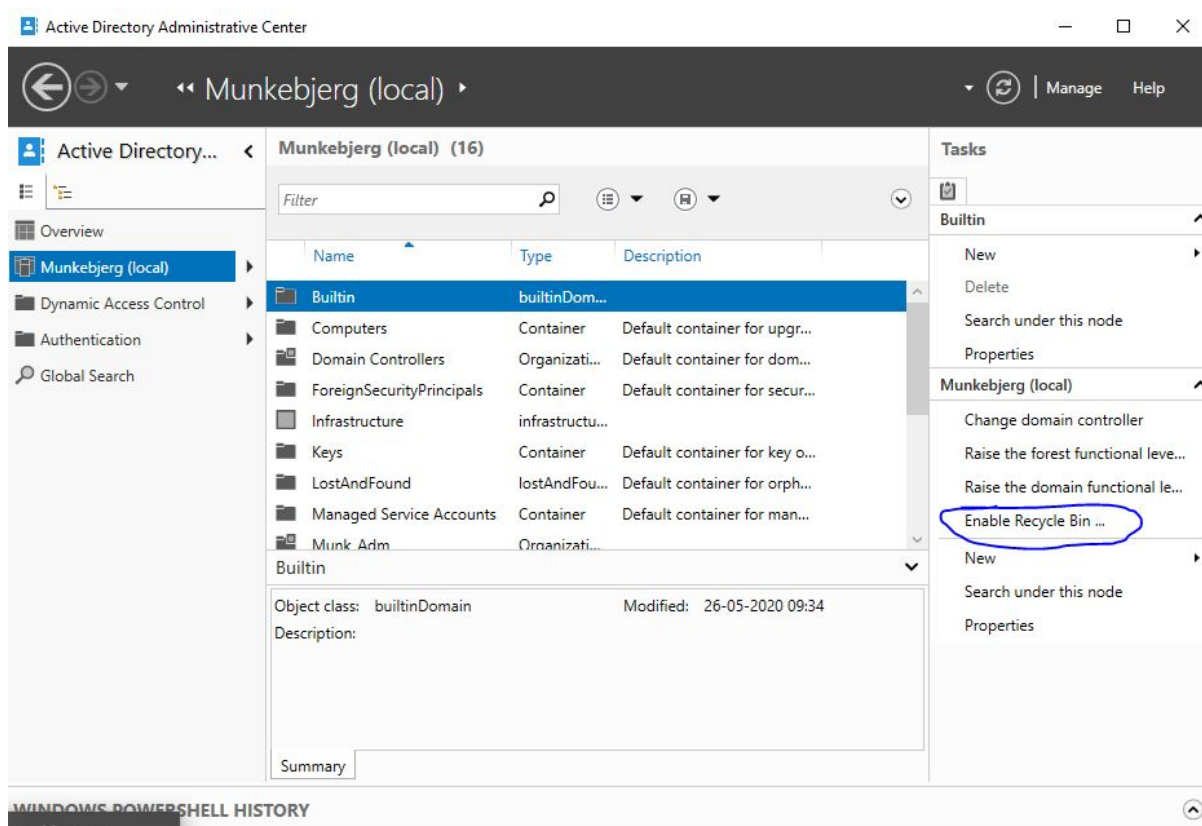
Herunder kan du se selve log-filerne. C:/logs



For at læse filen er det nødvendigt at kopiere filen til f.eks skrivebordet, da man ikke kan læse log-filen uden at lave en kopi, da man ellers vil få en fejlmeddelelse der siger filen er i brug.

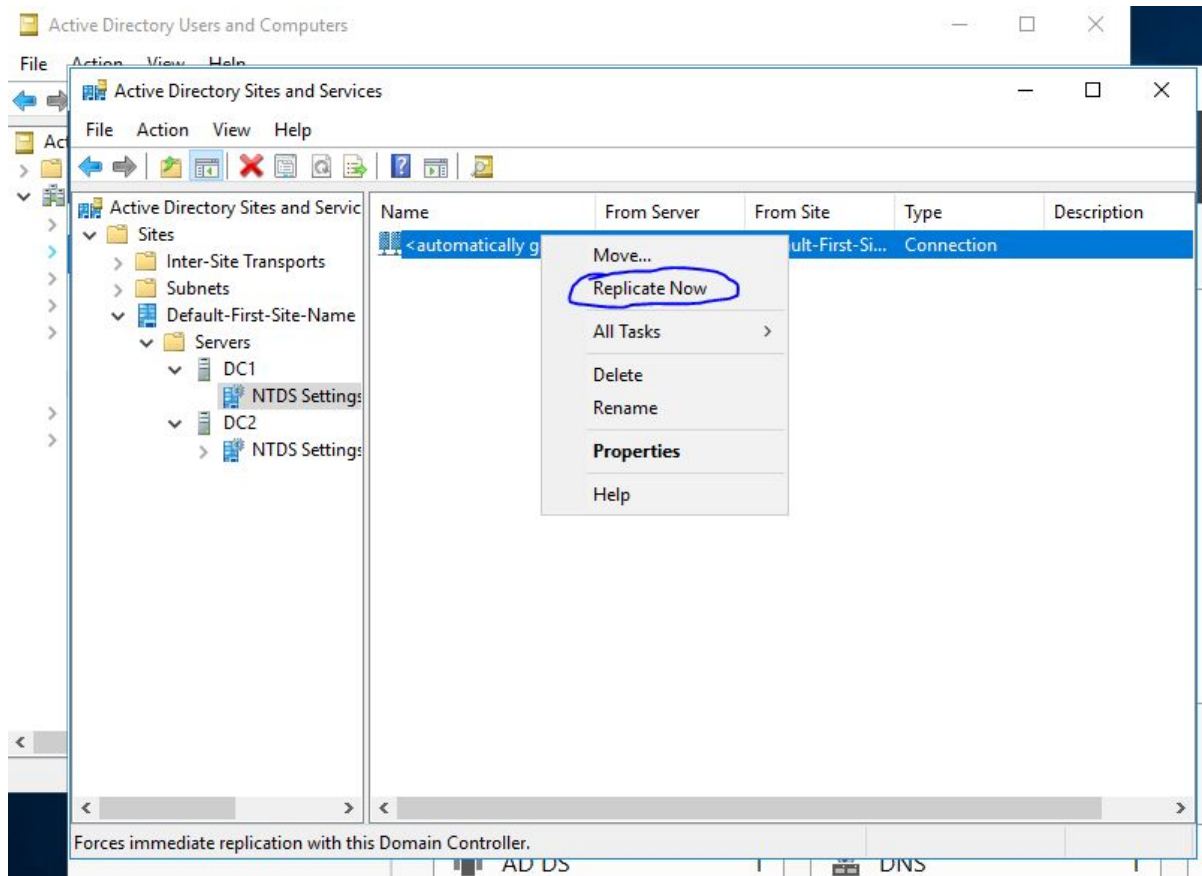
Active Directory Recycle Bin:

Gå til "Tools" og "Active Directory Administrative Center". Vælg domæne (Munkebjerg.local) og tryk derefter på "Enable Recycle Bin .."

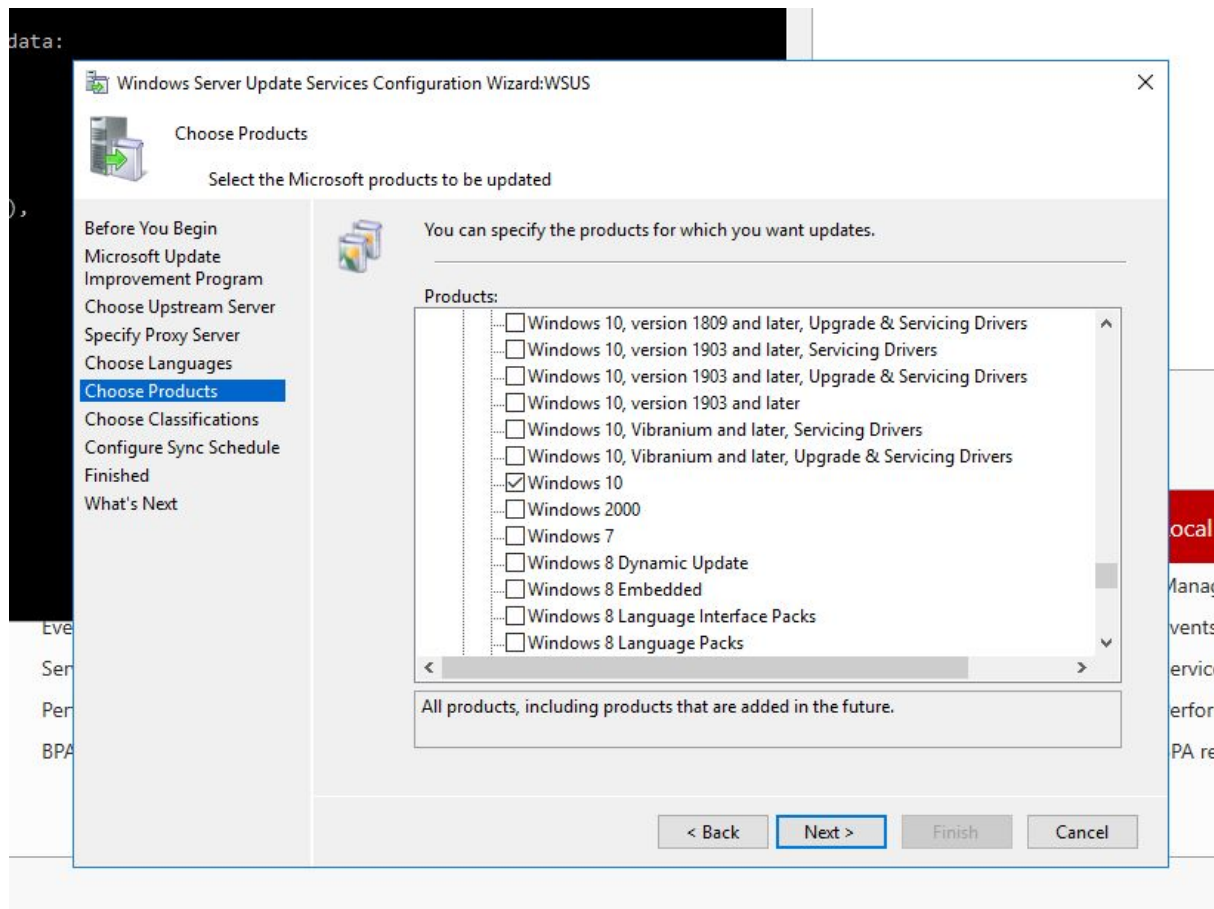


Efter du har slettet en bruger eller lignende kan de findes under "Deleted Objects".

For at gennemføre "Enable Recycle Bin" kan det være nødvendigt at gøre følgende:



Opsætning af WSUS:



Windows Server Update Services Configuration Wizard:WSUS

Choose Classifications

Select the update classifications you want to download

Before You Begin
Microsoft Update Improvement Program
Choose Upstream Server
Specify Proxy Server
Choose Languages
Choose Products
Choose Classifications
Configure Sync Schedule
Finished
What's Next

You can specify what classification of updates you want to synchronize.

Classifications:

- ☐ All Classifications
- ☒ Critical Updates
- ☒ Definition Updates
- ☐ Driver Sets
- ☐ Drivers
- ☐ Feature Packs
- ☒ Security Updates
- ☐ Service Packs
- ☐ Tools
- ☐ Update Rollups
- ☐ Updates
- ☒ Upgrades

All classifications, including classifications that are added in the future.

< Back Next > Finish Cancel

Windows Server Update Services Configuration Wizard:WSUS

Set Sync Schedule

Configure when this server synchronizes with Microsoft Update

Before You Begin
Microsoft Update Improvement Program
Choose Upstream Server
Specify Proxy Server
Choose Languages
Choose Products
Choose Classifications
Configure Sync Schedule
Finished
What's Next

You can synchronize updates manually or set a schedule for daily automatic synchronization.

☒ Synchronize manually

☐ Synchronize automatically

First synchronization: 18:05:20

Synchronizations per day: 1

Note that when scheduling a daily synchronization from Microsoft Update, the synchronization start time will have a random offset up to 30 minutes after the specified time.

< Back Next > Finish Cancel

Update Services

File Action View Window Help

Update Services

- WSUS
 - Updates
 - All Updates
 - Critical Updates
 - Security Updates
 - WSUS Updates
 - Computers
 - All Computers
 - Unassigned Computers
 - Downstream Servers
 - Synchronizations
 - Reports
 - Options

All Updates (705 updates of 705 shown, 705 total)

Approval: Unapproved Status: Any Refresh

Title	Classification	Installed/Not A...	Approval
Update for Windows 10 for x64-based Systems (KB3141032)	Critical Updates	0%	Not approved
2019-09 Servicing Stack Update for Windows 10 Version 1803 for x64-based Systems (KB4512570)	Security Updates	0%	Install (1/2)
2019-09 Security Update for Adobe Flash Player for Windows 10 Version 1709 for x64-based Systems (KB4516115)	Security Updates	0%	Install (1/2)
2019-09 Security Update for Adobe Flash Player for Windows 10 Version 1709 for x86-based Systems (KB4516115)	Security Updates	0%	Not approved
2019-08 Cumulative Update for Windows 10 Version 1703 for x86-based Systems (KB4511839)	Security Updates	0%	Not approved
2019-08 Cumulative Update for Windows 10 Version 1709 for ARM64-based Systems (KB4511839)	Security Updates	0%	Not approved
2019-09 Cumulative Update for .NET Framework 4.8 for Windows 10 Version 1607 for x64-based Systems (KB4511839)	Security Updates	0%	Not approved
2019-08 Cumulative Update for Windows 10 Version 1809 for ARM64-based Systems (KB4512578)	Security Updates	0%	Not approved
2019-07 Servicing Stack Update for Windows 10 Version 1703 for x64-based Systems (KB4511839)	Security Updates	0%	Not approved
2019-07 Servicing Stack Update for Windows 10 Version 1607 for x86-based Systems (KB4511839)	Security Updates	0%	Not approved
2019-09 Security Update for Adobe Flash Player for Windows 10 Version 1703 for x64-based Systems (KB4516115)	Security Updates	0%	Not approved
2019-09 Security Update for Adobe Flash Player for Windows 10 Version 1803 for x64-based Systems (KB4516115)	Security Updates	0%	Not approved
2019-09 Cumulative Update for Windows 10 Version 1607 for x64-based Systems (KB4516044)	Security Updates	0%	Not approved
2019-09 Security Update for Adobe Flash Player for Windows 10 Version 1803 for ARM64-based Systems (KB4516115)	Security Updates	0%	Not approved
2019-10 Cumulative Update for Windows 10 Version 1709 for x86-based Systems (KB4524150)	Security Updates	0%	Not approved
2019-09 Security Update for Adobe Flash Player for Windows 10 Version 1809 for x86-based Systems (KB4516115)	Security Updates	0%	Not approved
2019-09 Servicing Stack Update for Windows 10 Version 1703 for x86-based Systems (KB4511839)	Security Updates	0%	Not approved
2019-09 Servicing Stack Update for Windows 10 Version 1809 for x64-based Systems (KB4512577)	Security Updates	0%	Not approved
2019-09 Cumulative Update for Windows 10 Version 1809 for ARM64-based Systems (KB4512578)	Security Updates	0%	Not approved
2019-09 Cumulative Update for Windows 10 Version 1803 for ARM64-based Systems (KB4516058)	Security Updates	0%	Not approved
2019-09 Servicing Stack Update for Windows 10 Version 1703 for x86-based Systems (KB4511839)	Security Updates	0%	Not approved

This update is superseded by another update. Before you decline any superseded update, we recommend that you verify it is no longer needed by any computers. To do so, approve the superseding update.

Status:

- Computers with errors: 0
- Computers needing this update: 0
- Computers installed/not applicable: 0
- Computers with no status: 0

MSRC severity: Critical

MSRC number: None

Release date: 10. september 2019

KB article numbers: 4511839

Approve Updates

To approve multiple updates, select the group from this list, click the arrow, and choose the type of approval. If you want a child group to inherit the existing approvals of its parent group, choose Same as Parent. If you want all child groups of a parent to inherit its approvals, click Apply to Children on the parent group.

Computer Group	Approval	Deadline
All Computers	Keep existing approvals	
Unassigned Computers	Install	None

Approved for Install Ctrl+I

Approved for Removal Ctrl+R

Not Approved Ctrl+N

Keep Existing Approvals

Deadline >

Same as Parent Ctrl+P

Apply to Children Ctrl+C

OK Cancel

superseded update, we recommend that you verify it is no longer needed by any computers. To do so, approve the superseding update.

Herunder kan man se de to klient PC'er der er tilknyttet domænet Munkebjerg.local
 For at finde de to klienter var det nødvendigt at skrive følge command i en PowerShell prompt.

```
$updateSession = new-object -com "Microsoft.Update.Session";
$updates=$updateSession.CreateupdateSearcher().Search($criteria).Updates
```

wuaucit /reportnow

Update Services

File Action View Window Help

Update Services

- WSUS
 - Updates
 - Computers
 - All Computers
 - Downstream Servers
 - Synchronizations
 - Reports
 - Options

All Computers (2 computers of 2 shown, 2 total)

Status: Any Refresh

Name	IP Address	Operating System
klient1.munkebjerg.local	192.168.10.72	Windows 10 Pro
klient2.munkebjerg.local	192.168.10.73	Windows 10 Pro