

Install and configure ADDS on Windows Server 2022 Core in Azure (Part 1)

markswinkels.nl/install-and-configure-adds-on-windows-server-2022-core-in-azure-part-1

Mark

December 27, 2021

Today, I'm going to show you how to install and configure Active Directory Domain Services on Windows Server 2022 Core edition on Azure.

I've used some ARM templates to deploy my two domain controllers in Azure, based on Windows Server 2022 Core edition. These servers are in a separate subnet within my Azure environment. In this example, I've two domain controllers, mss-dc-core001 and mss-dc-core002.

The first step is to configure the following things:

- Machine name
- Static IP from the Azure Portal (NOT within the VM)
- Static DNS from the Azure Portal (NOT within the VM)
- Date and Time
- Install all the latest updates

Showing 1 to 3 of 3 records.

Name	Resource group	Location	Status	Operating system	Private IP address	Public IP address	Size	Disks
mss-dc-core001	Az... V MSS-RG-DC-CORE	West Europe	Running	Windows	192.168.1.110	-	Standard_D2as_v5	2
mss-dc-core002	Az... V MSS-RG-DC-CORE	West Europe	Running	Windows	192.168.1.111	-	Standard_D2as_v5	2

IP forwarding settings

IP forwarding Disabled Enabled

Virtual network mss-vn-prod

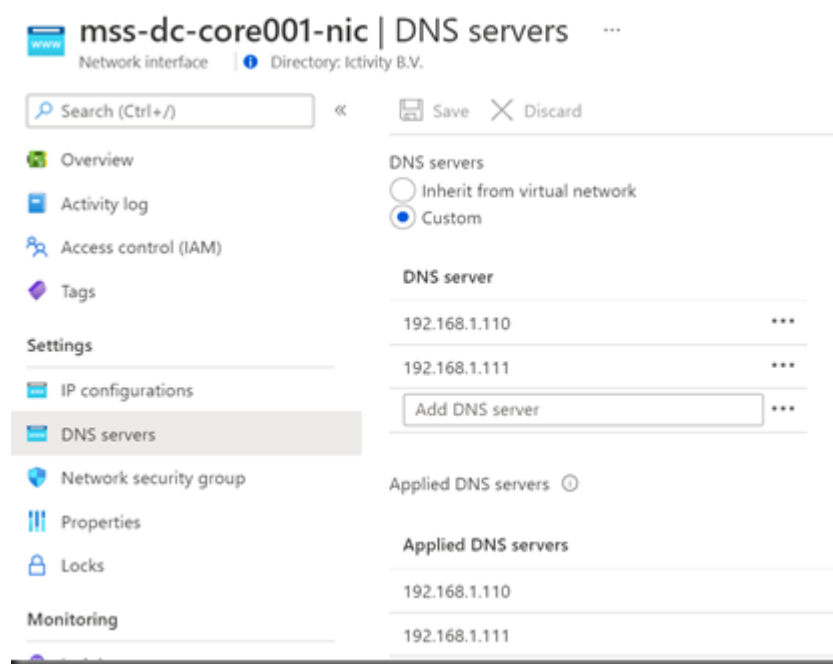
Gateway Load balancer None

IP configurations

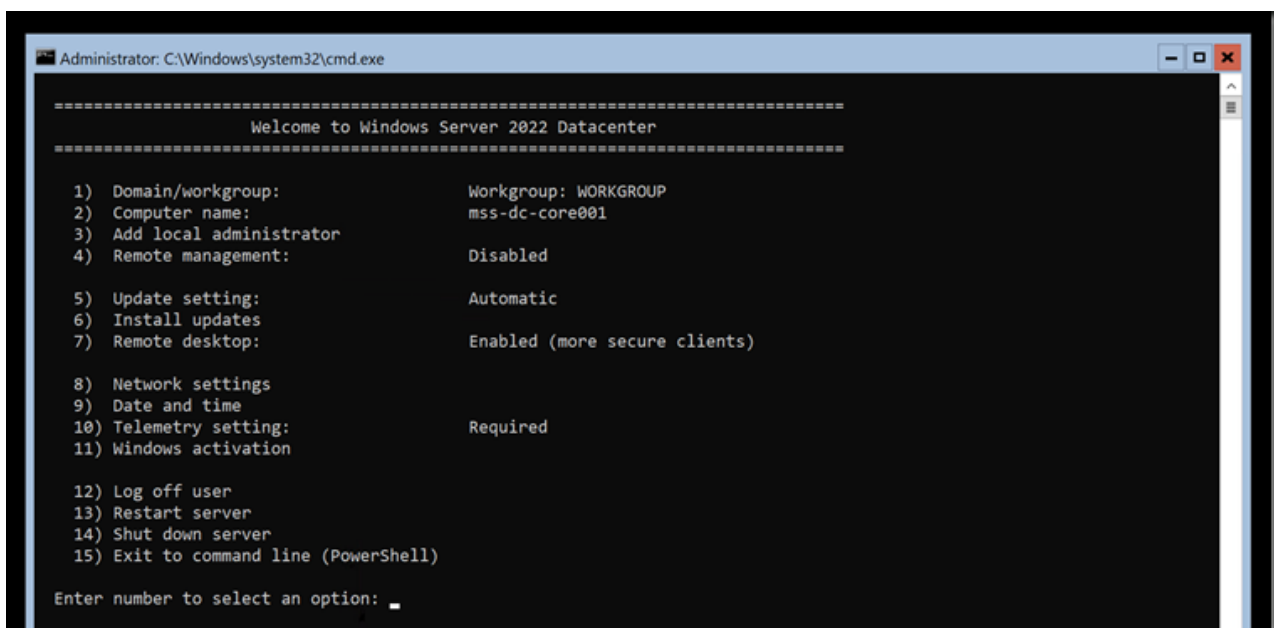
Subnet mss-sn-prod-dc (192.168.1.0/24)

Search IP configurations

Name	IP Version	Type	Private IP address	Public IP address
ipconfig1	IPv4	Primary	192.168.1.110 (Static)	-



After logging in to the first domain controllers, there's just one big black screen with 'SCONFIG' open, that's all!



The next step is to prepare the data partition on our second disk to place the ADDS database, NETLOGON and SYSVOL directories. For this configuration, we are using DISKPART. We have created a new volume on the second disk It's drive D: with 16 GiB storage and disk caching is disabled.

```
Administrator: C:\Windows\system32\cmd.exe
WARNING: To launch Server Configuration tool again, run "SConfig"
PS C:\> diskpart

Microsoft DiskPart version 10.0.20348.1

Copyright (C) Microsoft Corporation.
On computer: mss-dc-core001

DISKPART> list disk

Disk ###  Status       Size      Free      Dyn  Gpt
-----  -
Disk 0    Online       127 GB    1024 KB
Disk 1    Online       16 GB      0 B

DISKPART> select disk 1

Disk 1 is now the selected disk.

DISKPART> list volume

Volume ###  Ltr  Label        Fs      Type          Size      Status       Info
-----  -
Volume 0    Ltr  System Rese  NTFS     Partition     500 MB    Healthy      System
Volume 1    C    Windows      NTFS     Partition     126 GB    Healthy      Boot
Volume 2    D

DISKPART> _
```

After the first configuration of the servers, we are ready to start the installation of the necessary services and features. Press '15' to enter Powershell.

Install-windowsfeature -name AD-Domain-Services -IncludeManagementTools

```
Administrator: C:\Windows\system32\cmd.exe
PS C:\> Install-windowsfeature -name AD-Domain-Services -IncludeManagementTools

Start Installation...
20%
[ooooooooooooooooooooo ]
```

Install-ADDSForest -DomainName "network.lab" -DomainMode 7 -ForestMode 7 - DatabasePath "D:\NTDS" -SYSVOLPath "D:\SYSVOL" -LogPath "D:\Logs"

```
Administrator: C:\Windows\system32\cmd.exe
PS C:\> Install-ADDSForest -DomainName "network.lab" -DomainMode 7 -ForestMode 7 -DatabasePath "D:\NTDS" -SYSVOLPath "D:\SYSVOL" -LogPath "D:\Logs"

Install-ADDSForest

Validating environment and user input
Verifying prerequisites for domain controller operation...
[

algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security
channel sessions.

For more information about this setting, see Knowledge Base article 942564
(http://go.microsoft.com/fwlink/?LinkId=104751).

-
```

```
Administrator: C:\Windows\system32\cmd.exe
PS C:\> Install-ADDSForest -DomainName "network.lab" -DomainMode 7 -ForestMode 7 -DatabasePath "D:\NTDS" -SYSVOLPath "D:\SYSVOL" -LogPath "D:\Logs"
SafeModeAdministratorPassword: *****
Confirm SafeModeAdministratorPassword: *****

The target server will be configured as a domain controller and restarted when this operation is complete.
Do you want to continue with this operation?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): A
WARNING: Windows Server 2022 domain controllers have a default for the security setting named "Allow cryptography
algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security
channel sessions.

For more information about this setting, see Knowledge Base article 942564
(http://go.microsoft.com/fwlink/?LinkId=104751).

WARNING: This computer has at least one physical network adapter that does not have static IP address(es) assigned to
its IP Properties. If both IPv4 and IPv6 are enabled for a network adapter, both IPv4 and IPv6 static IP addresses
should be assigned to both IPv4 and IPv6 Properties of the physical network adapter. Such static IP address(es)
assignment should be done to all the physical network adapters for reliable Domain Name System (DNS) operation.

WARNING: A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it
does not run Windows DNS server. If you are integrating with an existing DNS infrastructure, you should manually
create a delegation to this DNS server in the parent zone to ensure reliable name resolution from outside the domain
"network.lab". Otherwise, no action is required.

WARNING: Windows Server 2022 domain controllers have a default for the security setting named "Allow cryptography
algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security
channel sessions.

For more information about this setting, see Knowledge Base article 942564
(http://go.microsoft.com/fwlink/?LinkId=104751).

WARNING: This computer has at least one physical network adapter that does not have static IP address(es) assigned to
its IP Properties. If both IPv4 and IPv6 are enabled for a network adapter, both IPv4 and IPv6 static IP addresses
should be assigned to both IPv4 and IPv6 Properties of the physical network adapter. Such static IP address(es)
assignment should be done to all the physical network adapters for reliable Domain Name System (DNS) operation.

WARNING: A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it
does not run Windows DNS server. If you are integrating with an existing DNS infrastructure, you should manually
create a delegation to this DNS server in the parent zone to ensure reliable name resolution from outside the domain
"network.lab". Otherwise, no action is required.

Message Context RebootRequired Status
-----
Operation completed successfully DCPromo.General.3 False Success

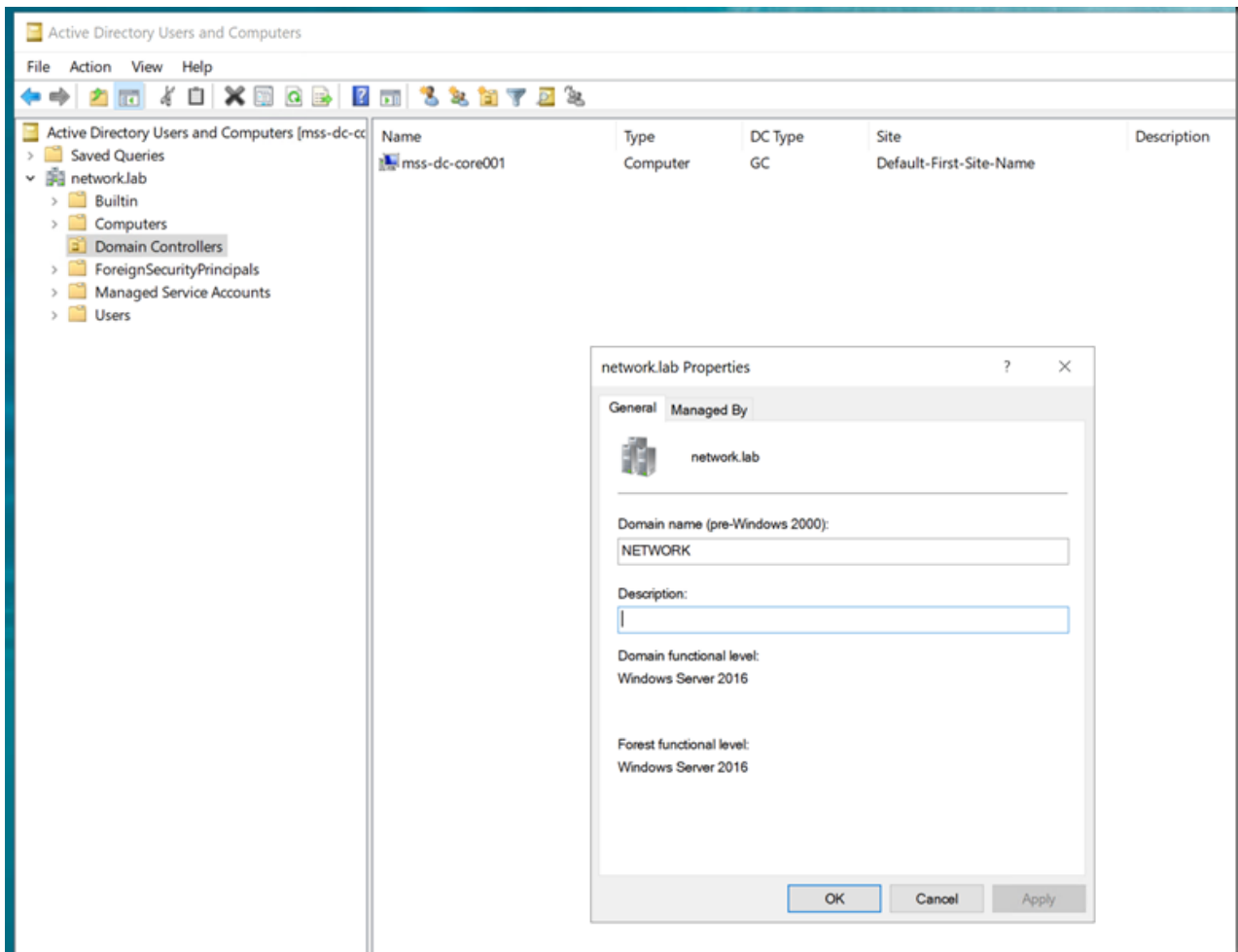
PS C:\>
```

You're about to be signed out

The computer is being restarted because Active Directory Domain Services was installed or removed.

Close

Because we are using Windows Core edition, we don't have any graphical management tools on the domain controllers. Therefore, we have installed the Remote Server Administration Tools or RSAT on a management server.

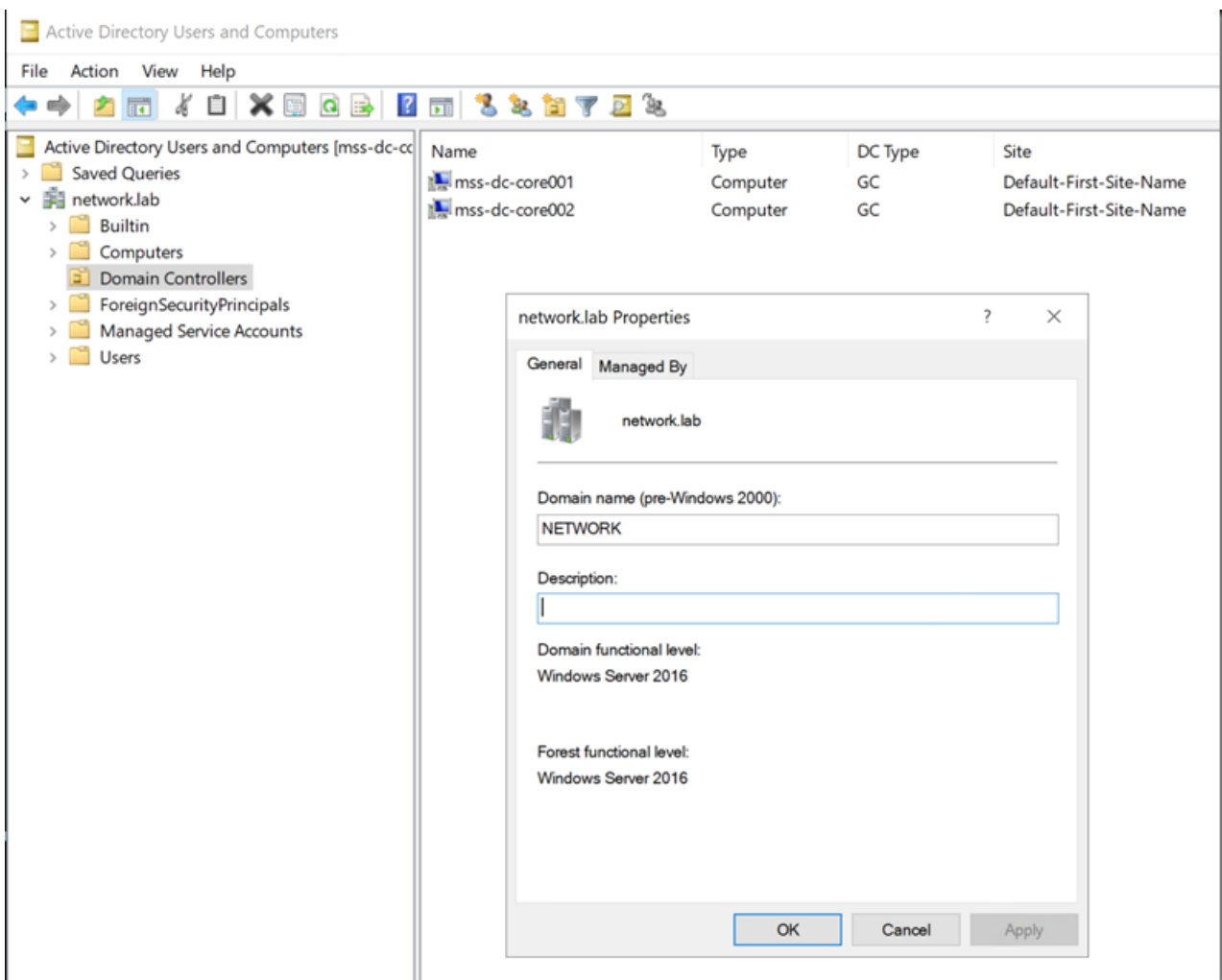
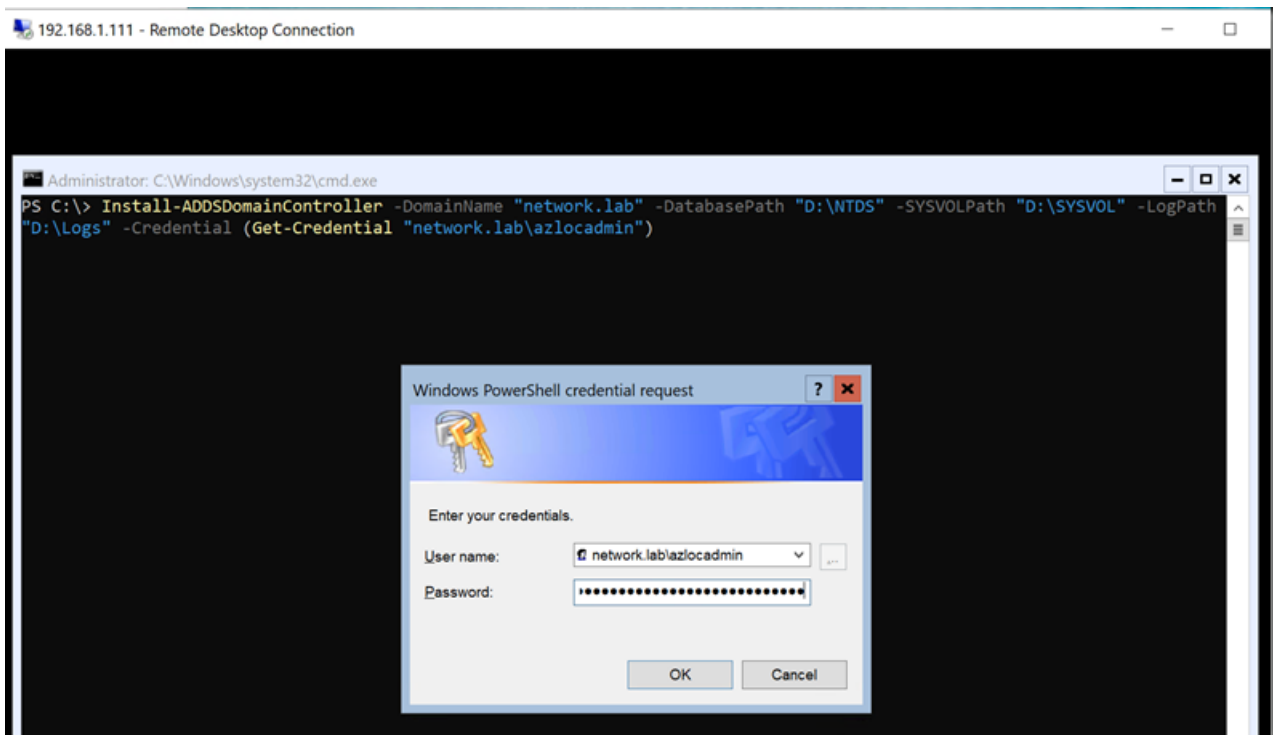


Here we can start 'Active Directory Users & Computers' to take a look into our new created Active Directory environment.

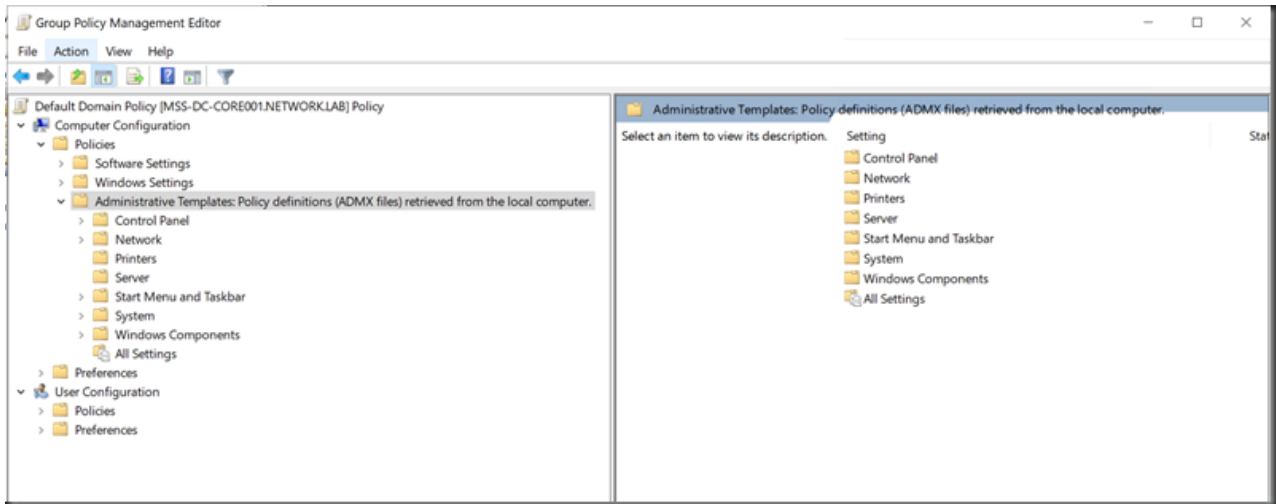
Install-windowsfeature -name AD-Domain-Services, DNS -IncludeManagementTools



Install-ADDSDomainController -DomainName "network.lab" -DatabasePath "D:\NTDS" -SYSVOLPath "D:\SYSVOL" -LogPath "D:\Logs" -Credential (Get-Credential "network.lab\azlocadmin")



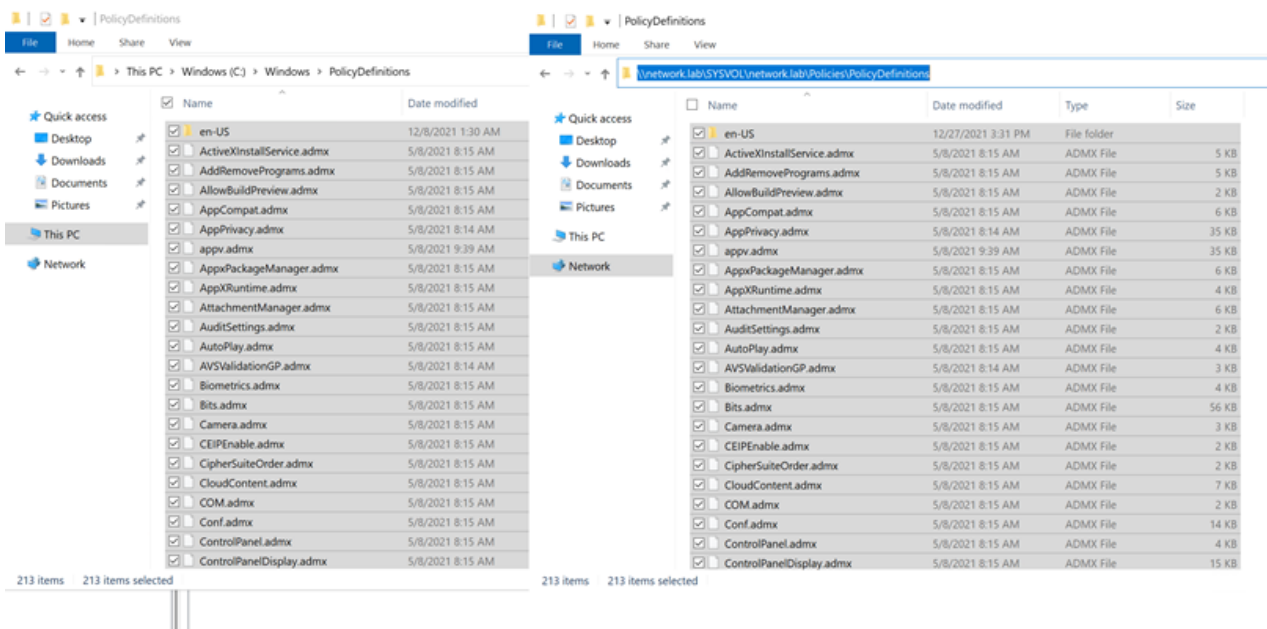
Now we have two active domain controllers in our Active Directory environment, based on Windows Server 2022 Core edition.



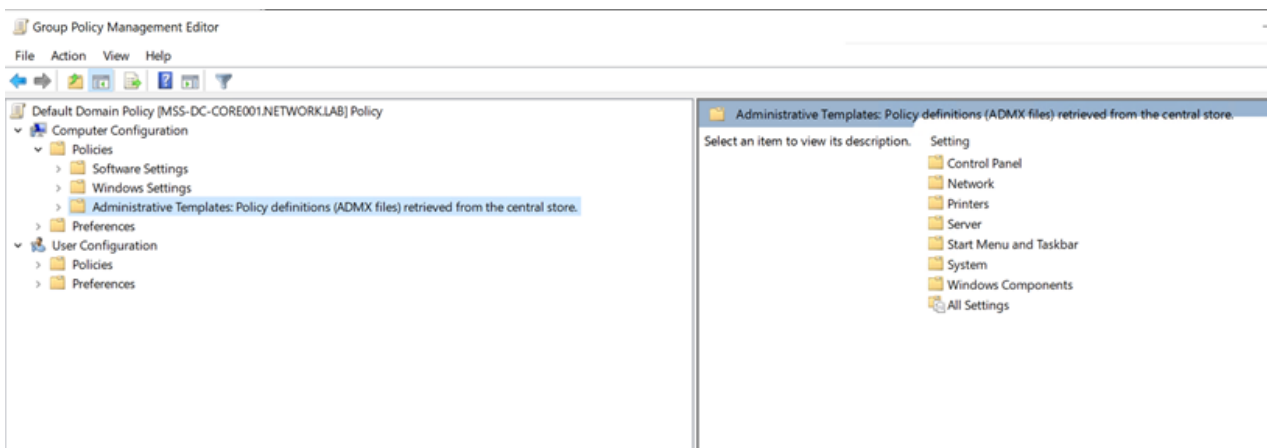
Create a Central Store for your group policy ADMX and ADML files. Copy all the files from:

"C:\Windows\PolicyDefinitions" to

"\\network.lab\SYSVOL\network.lab\Policies\PolicyDefinitions".



Open the Group Policy Editor again and see if the policy definitions are loaded from the Central Store.



Wrap up:

We have created two domain controllers in Azure, based on Windows Server 2022 Core edition (no graphical user interface). We have created a new Active Directory Forest with a single domain 'network.lab'. And last we have created the Central Store for storing the group policy definitions (ADMX and ADML) files.

In the next parts we are going to harden some security settings, configure Log Analytics for monitoring and configure Azure Backup for Back-up and Disaster Recovery.