# Practice M3: Active Directory

Note: The lab environment includes up to three machines, but you can do it with just two:

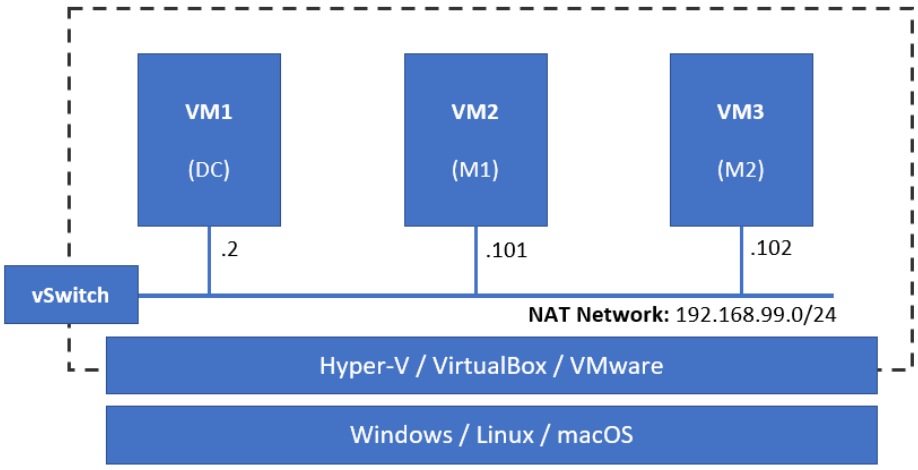
- Machine 1 / DC - Windows Server 2016/2019 Standard (with DE) – one network adapter connected through NAT or Bridge to the host's network
- Machine 2 / SERVER1 - Windows Server 2016/2019 Standard (Core or DE) – one network adapter connected through NAT or Bridge to the host's network
- Machine 3 / SERVER2* - Windows 10 Enterprise - one network adapter connected through NAT or Bridge to the host's network. This one can be skipped or substituted with another Windows Server machine

The following tasks are executed on different machines. It is stated clearly on which machine a task is being executed.

In this document, everything will be implemented with PowerShell only, but of course it could be done graphically or in a mixed way. During the demonstration in class most, or all the steps will be done using the GUI approach

# Part 1: Preparation

Adjust the required connectivity according to the description above. It should look like this:




## Preparation (Machine 1 / DC)

Set an appropriate name

```
PS C:\> Rename-Computer -NewName DC -Restart
```

Get list of network adapters

```
PS C:\> Get-NetAdapter
```

Verify that the names and MAC addresses match the virtual hardware setup.

You may rename the network adapter or leave it with its default name

```
PS C:\> Rename-NetAdapter -Name "Ethernet" -NewName "LAN"
```

Set the IP address of the network adapter if using a NAT network (please adjust the address settings accordingly)

If using a bridged/external network and there is a DHCP server there, skip this command and leave the adapter with the default values

```
PS C:\> New-NetIPAddress -InterfaceAlias "LAN" `
-IPAddress 192.168.99.2 -PrefixLength 24 -DefaultGateway 192.168.99.1
```

## Preparation of the additional machines

On both client machines, we can rename the network adapters with or leave them with their default names:

```
PS C:\> Rename-NetAdapter -Name "Ethernet" -NewName "LAN"
```

And set IP address, for example

```
PS C:\> New-NetIPAddress -InterfaceAlias "LAN" `
-IPAddress 192.168.99.101 -PrefixLength 24 -DefaultGateway 192.168.99.1
```

If you decide to add a third machine, set the IP address to **192.168.99.102**

The DNS server should also be set:

```
PS C:\> Set-DnsClientServerAddress -InterfaceAlias "LAN-Internal" -ServerAddresses ("192.168.99.2")
```

# Part 2: AD Installation and Configuration. Computer Management

## Active Directory Installation (Machine 1)

Install the AD DS server role

```
PS C:\> Install-WindowsFeature AD-Domain-Services -IncludeManagementTools
```

Import the AD DS deployment module

```
PS C:\> Import-Module ADDSDeployment
```

Get list of AD DS deployment commands

```
PS C:\> Get-Command -Module ADDSDeployment
```

Install a new AD forest and domain

```
PS C:\> Install-ADDSForest `
-CreateDnsDelegation:$false `
-DatabasePath "C:\Windows\NTDS" `
-DomainMode "WinThreshold" `
-DomainName "wsa.lab" `
-DomainNetbiosName "WSA" `
-ForestMode "WinThreshold" `
-InstallDns:$true `
-LogPath "C:\Windows\NTDS" `
-NoRebootOnCompletion:$false `
-SysvolPath "C:\Windows\SYSVOL" `
-Force:$true
```

## Create Computer Object in AD (Machine 1 / DC)

Create a new computer object upfront

```
PS C:\> New-ADComputer SERVER1
```

## Prepare and Join Server Core (Machine 2 / SERVER1)

Set an appropriate name

```
PS C:\> Rename-Computer -NewName SERVER1 -Restart
```

Join the machine to the domain

```
PS C:\> Add-Computer -DomainName WSA -DomainCredential Administrator
```

## Prepare and Join Client (Machine 3 / CLIENT1 or SERVER2)

Set an appropriate name

```
PS C:\> Rename-Computer -NewName SERVER2 -Restart
```

Join the machine to the domain

```
PS C:\> Add-Computer -DomainName WSA -DomainCredential Administrator
```

# Part 3: User Management

## Add a Few Organizational Units (Machine 1 / DC)

Create a Parent OU

```
PS C:\> New-ADOrganizationalUnit "Dream Team"
```

Create two additional child OUs

```
PS C:\> New-ADOrganizationalUnit "Sofia" -Path "OU=Dream Team,DC=WSA,DC=LAB"
PS C:\> New-ADOrganizationalUnit "Varna" -Path "OU=Dream Team,DC=WSA,DC=LAB"
```

## Manage Groups and Users (Machine 1 / DC)

Create an AD Group

```
PS C:\> New-ADGroup -Name "Help Desk L3" -SamAccountName HelpDeskL3 `
-GroupCategory Security -GroupScope DomainLocal `
-DisplayName "Help Desk L3 Staff" -Path "CN=Users,DC=WSA,DC=LAB" `
-Description "Members of this group are Help Desk L3 Staff"
```

Create two new AD user objects. One for John Smith:

```
PS C:\> New-ADUser -Name John `
-AccountPassword (ConvertTo-SecureString -AsPlain "Password1" -Force) `
-DisplayName "John Smith" -Enabled $true -GivenName John -Surname Smith `
-UserPrincipalName john.smith@wsa.lab
```

And another one for Jane Hudson:

```
PS C:\> New-ADUser -Name Jane `
-AccountPassword (ConvertTo-SecureString -AsPlain "Password1" -Force) `
-DisplayName "Jane Hudson" -Enabled $true -GivenName Jane -Surname Hudson `
-UserPrincipalName jane.hudson@wsa.lab
```

Add users as group members to the group created earlier

```
PS C:\> Add-ADGroupMember HelpDeskL3 John,Jane
```

Move the users in different OUs. Move John to Varna OU:

```
PS C:\> Get-ADUser John | Move-ADObject -TargetPath 'OU=Varna,OU=Dream Team,DC=WSA,DC=LAB'
```

Then, move Jane to Sofia OU:

```
PS C:\> Get-ADUser Jane | Move-ADObject -TargetPath 'OU=Sofia,OU=Dream Team,DC=WSA,DC=LAB'
```