# Solution M5: AD Activities and Services

There are multiple ways to achieve what was requested

As the visual approach is intuitive, the presented solution is implemented with PowerShell

Please note that the solution is far from being optimal. The aim is to illustrate all (or most) individual steps

## Possible Solution Task 1

Check the **M5-Solution-Script-AD-Activities-and-Services.ps1** file

Adjust it to match your situation

Open a **PowerShell** session with **Run as Administrator** on **the Hyper-V** host and execute it

Here, we will explain just the steps related to the actual solution

Once the domain is up and running and all machines are part of it, we can continue

Install DHCP role on **HW5-SRV1** and **HW5-SRV2**

**Invoke-Command -VMName $VM2, $VM3 -Credential $DC -ScriptBlock { Install-WindowsFeature DHCP -IncludeManagementTools }**

Configure DHCP service on both DHCP servers (**HW5-SRV1** and **HW5-SRV2**)

**Invoke-Command -VMName $VM2 -Credential $DC -ScriptBlock { Add-DhcpServerSecurityGroup ; Restart-Service DHCPServer ; Set-ItemProperty -Path registry::HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\ServerManager\Roles\12 -Name ConfigurationState -Value 2 ; Add-DhcpServerInDC -DnsName hw5-srv1.wsaa.lab -IPAddress 192.168.99.10 }**

**Invoke-Command -VMName $VM3 -Credential $DC -ScriptBlock { Restart-Service DHCPServer ; Set-ItemProperty -Path registry::HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\ServerManager\Roles\12 -Name ConfigurationState -Value 2 ; Add-DhcpServerInDC -DnsName hw5-srv2.wsaa.lab -IPAddress 192.168.99.11 }**

Create a DHCP scope (with 2 minutes lease time for demonstration purposes) on SRV1 and set some options

**Invoke-Command -VMName $VM2 -Credential $DC -ScriptBlock { Add-DhcpServerv4Scope -Name "Homework" -StartRange 192.168.99.100 -EndRange 192.168.99.200 -SubnetMask 255.255.255.0 -LeaseDuration 0.0:2:0 }**

**Invoke-Command -VMName $VM2 -Credential $DC -ScriptBlock { Set-DhcpServerv4OptionValue -ScopeId 192.168.99.0 -DnsServer 192.168.99.2 -DnsDomain "wsaa.lab" -Router 192.168.99.1 }**

Create a failover relationship (wait for now)

An active-active relationship could be created with the following command (skip it)

***Invoke-Command -VMName $VM2 -Credential $DC -ScriptBlock { Add-DhcpServerv4Failover -Name "DHCP-FO-AA" -PartnerServer "hw5-srv2.wsaa.lab" -ScopeId 192.168.99.0 -SharedSecret "Secret1" }***

An active-passive relationship could be created with the following command (skip it)

***Invoke-Command -VMName $VM2 -Credential $DC -ScriptBlock { Add-DhcpServerv4Failover -Name "DHCP-FO-AP" -PartnerServer "hw5-srv2.wsaa.lab" -ServerRole Standby -ScopeId 192.168.99.0 }***

An active-active relationship with load balance amount of 50% (use this one)

**Invoke-Command -VMName $VM2 -Credential $DC -ScriptBlock { Add-DhcpServerv4Failover -Name "DHCP-FO-AA-LB" -PartnerServer "hw5-srv2.wsaa.lab" -ScopeId 192.168.99.0 -LoadBalancePercent 50 -MaxClientLeadTime 00:01:00 -AutoStateTransition $False }**

Obtain address on **HW5-SRV3** if it doesn't have one

Use **ipconfig /all** to check from which server it took the address. It should be the **HW5-SRV1** (192.168.99.10)

Either stop the DHCP service on **HW5-SRV1** or change the load balance percentage to 100% for the **HW5-SRV2**

Release and renew the address on **HW5-SRV3**. Check again which DHCP server gave it

## Possible Solution Task 2

Continue with the infrastructure prepared for Task 1

Log on to the **DC** and open a **PowerShell** session with **Run as Administrator**

On **DC** create the Root Key if not created already

**Add-KDSRootKey -EffectiveTime (Get-Date).AddHours(-10)**

Create the service account and associate it with the **HW5-SRV1** machine

**New-ADServiceAccount -Name "HWService" -DNSHostName "HWService.wsaa.lab" -Enabled $True -PrincipalsAllowedToRetrieveManagedPassword HW5-SRV1$**

Log on to **HW5-SRV1** with account that has administrative privileges

Download the service from <https://zahariev.pro/files/wsaa-service.zip>

Extract the service to **C:\WSAA** folder

Register the service with

**New-Service -Name WSAAService -BinaryPathName C:\WSAA\WSAAService.exe**

Make sure that the **C:\Temp** folder is there

Open **Server Manager**, navigate to **Tools** and click on **Services**

Find the **WSAAService** service and double-click on it

Switch to the **Log On** tab

Make sure that the **This account** option is selected and click **Browse**

Click on **Locations** button

Select **Entire Directory** and click **OK**

Enter **HWService**, click **Check Names** and click **OK**

Clear both password related fields and click **OK**

Click **OK** on the dialog showing that **Log On As A Service** right has been granted

Start the service

Check the **C:\Temp** folder for a file **WSAAService.log** and see what is there