# Practice M5: Active Directory Activities and Services

For the purpose of this lab and the course, we will consider that we are working in a pure Windows environment either on-premise or in the cloud and using **Hyper-V** as a virtualization solution. All tasks can be achieved under different configuration (another host OS or virtualization solution) with the appropriate adjustments

The expected lab infrastructure (it will evolve throughout the practice) consists of up to three machines – one domain controller (**DC**), and two servers - **SERVER1** and **SERVER2** that will change their roles during the lab. Each machine will have one OS disk and 1 NIC. Windows Server 2019 Standard is enough, Desktop experience or core (managed remotely) – it is up to you

If you are short on resources, you can shrink the infrastructure down to two machines. All tasks should be adjusted accordingly

The overall picture should look like:

A picture containing diagram

Description automatically generated

All machines can have between 1GB and 1,5GB of dynamic RAM or more

Use the provided Lab Setup script to create the lab environment

Create checkpoints of the machines while they are in stopped state. This way, you can reuse them for all parts of this practice

## Part 1: AD Activities & Services 101 (DNS)

### Role installation

Log on to the **SERVER1** with account that has administrative privileges

Start **Server Manager** and navigate to **Manage** and then **Add Roles and Features**

On the first screen click **Next**

Make sure that **Role-based or feature-based installation** is selected and click **Next**

Ensure that **SERVER1** is selected and click **Next**

On the **Select server roles** screen select **DNS Server**

On the dialog screen for the required features click **Add Features**

Then click **Next**

On the **Select features** screen click **Next**

Next, on the role page, click on **Next**

On the confirm installation screen click **Install**

When the installation is complete, click on **Close**

### Standard zones

#### Create a standard forward lookup primary zone

Log on to the **DC** with account that has administrative privileges

Start **Server Manager** and navigate to **Tools** and then click on **DNS** tool

Expand the **DC** server node

Select the **Forward Lookup Zones** node and expand it

Right-click on it and form the context menu choose **New Zone**

On the first screen of the wizard click **Next**

On the **Zone Type** screen, ensure that the **Primary zone** is selected

Deselect the **Store the zone in Active Directory** option and click **Next**

On the **Zone Name** screen, enter **demo.local** in the **Zone name** text box and click **Next**

Make sure that the **Create a new file** option is selected and click **Next**

On the next screen, make sure that the **Do not allow dynamic updates** option is selected and click **Next**

On the summary screen, click **Finish**

#### Create a standard forward lookup secondary zone

Log on to the **SERVER1** with account that has administrative privileges

Start **Server Manager** and navigate to **Tools** and then click on **DNS** tool

Expand the **SERVER1** server node

Select the **Forward Lookup Zones** node and expand it

Right-click on it and form the context menu choose **New Zone**

On the first screen of the wizard click **Next**

Select **Secondary zone** on the zone type screen and click **Next**

Enter **demo.local** in the **Zone name** text field and click **Next**

Enter **192.168.99.2** (the IP of the DC) in the **IP Address** field and click **Next**

On the summary screen, click **Finish**

Now, the new zone must appear under the **Forward Lookup Zones** node. When we click on it, an error is displayed. We will work this out a little bit later

#### Create a standard reverse lookup primary zone

Log on to the **DC** with account that has administrative privileges

Start **Server Manager** and navigate to **Tools** and then click on **DNS** tool

Expand the **DC** server node

Select the **Reverse Lookup Zones**, right-click on it and form the context menu choose **New Zone**

On the first screen of the wizard click **Next**

On the **Zone Type** screen, ensure that the **Primary zone** is selected and click **Next**

On the replication scope screen, click **Next**

Make sure that the **IPv4 Reverse Lookup Zone** is selected on the next screen. Click **Next**

For **Network ID** enter **192.168.99** and click **Next**

On **Dynamic Updates** screen, leave everything as it is and click **Next**

On the summary screen, click **Finish**

### Active Directory integrated zone

Log on to the **DC** with account that has administrative privileges

Start **Server Manager** and navigate to **Tools** and then click on **DNS** tool

Expand the **DC** server node

Right-click on **Forward Lookup Zones** and select **New Zone**

On the first screen of the wizard click **Next**

On the **Zone Type** screen, ensure that the **Primary zone** is selected and **Store the zone in Active Directory** option is selected and click **Next**

On the replication scope screen, click **Next**

On the **Zone Name** screen, enter **company.local** in the **Zone name** text box and click **Next**

On the next screen, make sure that the **Allow only secure dynamic updates** option is selected and click **Next**

On the summary screen, click **Finish**

### Zone delegation

#### Create zone

Log on to **SERVER1** with account that has administrative privileges

Start **Server Manager** and navigate to **Tools** and then click on **DNS** tool

Expand the server node

Expand the **Forward Lookup Zones** node and from the context menu select **New Zone**

Click **Next** on the first screen

Make sure the **Primary zone** is selected and click **Next**

Enter **marketing.company.local** for **Zone name** and click **Next**

Accept **Zone File** settings and click **Next**

Click **Next** on the dynamic updates screen

On the summary screen, click **Finish**

#### Delegate zone

Log on to the **DC** with account that has administrative privileges

Start **Server Manager** and navigate to **Tools** and then click on **DNS** tool

Expand the **DC** server node

Expand the **Forward Lookup Zones** node and select the **company.local** node

Invoke its context menu and select **New Delegation**

Click **Next** on the first screen

Enter **marketing** in the **Delegated domain** text box and click **Next**

On name servers screen click **Add**

Enter **SERVER1** in the **Server fully qualified domain name** and click **Resolve**

Click **OK** to close the **New name server** dialog window

Click **Next**

On the summary screen, click **Finish**

### Stub zones

#### Create zone

Log on to **SERVER1** with account that has administrative privileges

Start **Server Manager** and navigate to **Tools** and then click on **DNS** tool

Expand the server node

Expand the **Forward Lookup Zones** node and from the context menu select **New Zone**

Click **Next** on the first screen

Make sure the **Primary zone** is selected and click **Next**

Enter **company.pri** for **Zone name** and click **Next**

Accept **Zone File** settings and click **Next**

Click **Next** on the dynamic updates screen

On the summary screen, click **Finish**

#### Stub zone

Log on to the **DC** with account that has administrative privileges

Start **Server Manager** and navigate to **Tools** and then click on **DNS** tool

Expand the **DC** server node

Expand the **Forward Lookup Zones** node, invoke its context menu and select **New Zone**

Click **Next** on the first screen

Select **Stub Zone** and click **Next**

Accept the proposed replication settings and click **Next**

Enter **company.pri** as **Zone name** and click **Next**

Enter **192.168.99.11** as **IP Address** and press **Enter**. Click **Next**

Click **Finish** on the summary screen

The zone will appear but initially will show an error. After a while, refresh the information, you will see that the error is gone

### Forwarding

#### Forwarders

Log on to the **SERVER1** with account that has administrative privileges

Start **Server Manager** and navigate to **Tools** and then click on **DNS** tool

Select the server node and choose **Properties** from its context menu

Switch to the **Forwarders** tab and click the **Edit** button

Enter **192.168.99.2** and press **Enter**. Then click **OK**

Click **OK** to close the properties window

#### Conditional forwarders

While still on **SERVER1**, create a new primary forward lookup zone **home.lab**

When done, log on to the **DC** with account that has administrative privileges

Start **Server Manager** and navigate to **Tools** and then click on **DNS** tool

Expand the server node and select the **Conditional Forwarders** node

Select **New Conditional Forwarder** from the context menu

Enter **home.lab** in the **DNS Domain** text field

Enter **192.168.99.11** in the **IP Address** field, press **Enter** and click **OK**

Open command line session and execute **nslookup -type=soa home.lab**

Then, execute **nslookup -type=ns home.lab**

Both commands should return information for the zone provided by **SERVER1**

### Zone transferring

Log on to the **DC** with account that has administrative privileges

Start **Server Manager** and navigate to **Tools** and then click on **DNS** tool

Expand the server node and the **Forward Lookup Zones** node

Select **demo.local** zone, invoke its context menuand click **Properties**

Switch to **Zone Transfers** tab

Change the selection to **Only to the following servers** and click **Edit**

Enter **192.168.99.11** as **IP Address** and press **Enter**. Then click **OK**

Click **OK** to close the zone properties window

Log on to the **SERVER1** with account that has administrative privileges

Start **Server Manager** and navigate to **Tools** and then click on **DNS** tool

Expand the server node and then the **Forward Lookup Zones** node

Select **demo.local** zone and press **F5** key to refresh

Now, the error must disappear, and we should see information about the zone

### Resource records

Log on to the **DC** with account that has administrative privileges

Start **Server Manager** and navigate to **Tools** and then click on **DNS** tool

Select the **WSAA.LAB** zone and from its context menu select **Properties**

Examine both tabs **Start of Authority** and **Name Servers**. Close the dialog window

Select again the **WSAA.LAB** zone and from its context menu this time select **New Host (A or AAAA)**

Type **VM1** in the **Name** text field

Enter **192.168.99.231** in the **IP address** field and click **Add Host** button and then **OK** on the message box

While still on the same scree, type **VM2** in the **Name** text field

Enter **192.168.99.232** in the **IP address** field and select **Create associated pointer (PTR) record** option

Click **Add Host** button and then **OK** on the message box

Click **Done** to close the window

Expand the **Reverse Lookup Zones** node and navigate to **99.168.192.in-addr.arpa**

Here, we can see the record for **192.168.99.232** but not the one for **192.168.99.231**. Let’s add one

Right-click the reverse zone and select **New Pointer (PTR)**

Change the **Host IP Address** to **192.168.99.231** and enter **VM1** in the **Host name** field. Click **OK**

Okay, now we have both records, but they are different. The last one we added is without a domain part

Double click on the **192.168.99.231** record to open its properties

Change the **Host name** to **VM1.wsaa.lab.** (including the trailing dot symbol) and click **OK**

Switch to the **Forward Lookup Zones / WSAA.LAB**

Let’s add one more **A** record. Right-click the **WSAA.LAB** and from its context menu this time select **New Host (A or AAAA)**

Type **VM3** in the **Name** text field

Enter **192.168.99.233** in the **IP address** field and select **Create associated pointer (PTR) record** option

Click **Add Host** button and then **OK** on the message box

Click **Done** to close the window

Now, let’s add a different type of record. Right-click the **WSAA.LAB** and from its context menu this time select **New Alias (CNAME)**

Type **WEB** in the **Alias name** text field

Enter **VM3.wsaa.lab** in the **Fully qualified domain name** field and click **OK** button

Open **Command Prompt** and type **nslookup vm3.wsaa.lab**

Now type **nslookup 192.168.99.233**

And now, type **nslookup web.wsaa.lab**

Let’s create a different type of record – a mail exchanger one. Return to the **DNS Manager** tool

Right-click the **WSAA.LAB** and from its context menu this time select **New Mail Exchanger (MX)**

Leave the **Host or child domain** text field empty

Enter **VM1.wsaa.lab** in the **Fully qualified domain name** field and click **OK** button

Right-click the **WSAA.LAB** and from its context menu this time select **New Mail Exchanger (MX)**

Leave the **Host or child domain** text field empty

Enter **VM2.wsaa.lab** in the **Fully qualified domain name** field, set the **Mail server priority** to **20** and click **OK** button

Double-click on one of all record types created so far (**Host (A)**, **Alias (CNAME)** and **Mail Exchanger (MX)**) to see their properties and then close the property windows

Switch to advanced view by clicking on **View > Advanced** and go to the properties of the same records. There should be a different set of options now. Close the properties windows

### Round robin

Create three **Host (A)** records for **www.wsaa.lab** and for every record use different IP address. For example, **192.168.99.241, 192.168.99.242** and **192.168.99.243**

Open **Command Prompt** and type **nslookup www.wsaa.lab**

Now type **nslookup www.wsaa.lab**

Execute the command again. The order must be different

Now, execute **ping www.wsaa.lab**

Again, re-execute the command a few more times. At some point the address will change

### Scavenging

Log on to the **DC** with account that has administrative privileges

Start **Server Manager** and navigate to **Tools** and then click on **DNS** tool

Select the server node and invoke its context menu. Click on **Set Aging/Scavenging for All Zones**

Turn on the **Scavenge stale resource records** option

Click **OK** to close the properties window

When asked if we want to apply changes to Active Directory-integrated zones, select the **Apply these settings** option and click **OK**

Now, let’s adjust scavenging setting on zone level. Select the **WSAA.LAB** zone and click **Properties** in its context menu

Click the **Aging** button

Turn on the **Scavenge stale resource records** option

Click **OK** to close the properties window and then again **OK**

### Troubleshooting

Let’s execute a few commands in an interactive fashion

Log on to the **DC** with account that has administrative privileges

Open **Command Prompt** and type **nslookup**

Type **set type=soa** and press **Enter**

Now type **wsaa.lab** and press **Enter**

This will return information about the zone

Now, let’s see what information will be returned for the MX record

Type **set type=mx** and press **Enter**

Now type **wsaa.lab** and press **Enter**

Close the command prompt and return to the **DNS Manager** tool

Select the server, invoke the context menu and select **Properties**

Switch to **Monitoring** tab

Turn on both **Select a test type** options and click **Test Now**

Both tests should pass. If the recursive one fails, go to the **Forwarders** tab and remove the entries

Close the properties window with the **OK** button

We can use also the **Event Viewer > Application and Services Logs > DNS Server** for capturing information about the DNS service

### Logging

Navigate to **DNS Manager** tool on the **DC** machine

Select the server, invoke the context menu, and select **Properties**

Switch to **Debug Logging** tab

Enable the **Log packets for debugging**

You can adjust what packets to be captured. Let’s leave everything as it is

Enter **C:\DNS.log** in the **File path and name** text box in the **Log file** section and click **OK**

Open **Command Prompt** and type **nslookup vm3.wsaa.lab**

Now, navigate to the logging file and explore its contents

### Clean up

Stop all the machines and restore their state to the checkpoint taken before this part of the practice

## Part 2: AD Activities & Services 102 (DHCP)

### Role installation

Log on to the **DC** with account that has administrative privileges

Start **Server Manager** and navigate to **Manage** and then **Add Roles and Features**

On the first screen click **Next**

Make sure that **Role-based or feature-based installation** is selected and click **Next**

Ensure that **DC** is selected and click **Next**

On the **Select server roles** screen select **DHCP Server**

On the dialog screen for the required features click **Add Features**

Then click **Next**

On the **Select features** screen click **Next**

Next, on the role page, click on **Next**

On the confirm installation screen click **Install**

When the installation is complete, click on **Close**

### Post-installation configuration

Click on the yellow sign near the flag in **Server Manager**

On the first screen click **Next**

Make sure that **WSAA\Administrator** credentials are going to be used (or the current user with administrative privileges) and click **Commit**

Finally, click **Close**

### Simple scope

Log on to **DC** machine with account that has administrative privileges

Open **Server Manager** and select **DHCP** from **Tools** menu

Select the **IPv4** node, invoke the context menu, and select **New Scope**

On the first screen click **Next**

In the **Name** field enter **Simple Scope** and click **Next**

Enter **192.168.99.100** and **192.168.99.200** for scope start and end address and click **Next**

On the next screen click **Next**

On the screen for lease duration click **Next**

On the screen for DHCP options click **Next**

Enter **192.168.99.1** on the screen for default gateway and click **Add** and then **Next**

On the next screen click **Next**

On the screen for WINS servers click **Next**

Make sure that **Yes, I want to activate the scope now** is selected and click **Next**

Close the wizard by clicking on **Finish**

Now, we can add an additional machine in the same network and test if it will receive an IP address and if it could be joined to the domain

### Vendor class

Log on to **DC** machine with account that has administrative privileges

Open **Server Manager** and select **DHCP** from **Tools** menu

Expand tree nodes, right-click on **IPv4** and select **Define Vendor Classes**

Click the **Add** button to add a new one

Enter **Cisco Phones** both in the **Display name** and **Description** text boxes

Click under the **ASCII** column and type **Cisco UX-430**

Click **OK** to create the new class

Again, click on **Add** to create a class for printers

Enter **Lexmark Printers** in the **Display name** field

Enter **Lexmark Network Laser Printers** in the **Description** field

Click under the **ASCII** column and type **Lexmark LX-CX320dn**

Click **OK** to confirm the creation of the new class

Click **Close** to exit the vendor classes window

### DHCP policy

Log on to **DC** machine with account that has administrative privileges

Open **Server Manager** and select **DHCP** from **Tools** menu

Expand tree nodes, right-click on **IPv4** and select **New Scope**

Click **Next**

Enter **Printer Scope** in the **Name** field and click **Next**

Enter **192.168.70.50** for **Start IP address** and **192.168.70.90** for **End IP address**

Accept the proposed **Length** and **Subnet mask** and click **Next**

On the exclusions screen click **Next**

Accept the proposed **Lease duration** and click **Next**

Click **Next** on the options screen

Enter **192.168.70.254** in the **IP address** field, click **Add** and then click **Next**

Accept values on the next screen and click **Next**

Do not enter anything on the WINS servers screen and click **Next**

Make sure that **Yes, I want to activate this scope now** option is selected and click **Next**

Finally, click **Finish**

Now, expand the newly created scope node

Select the **Policies** node and from the context menu select **New Policy**

Type **Lexmark** in the **Policy Name** field and click **Next**

Click **Add** to include some decision rules

Make sure that the **Vendor Class** is selected in the **Criteria** drop-downand **Operator** is set to **Equals**

Then select **Lexmark Printers** from the **Value** drop-down list and click **Add** and then **OK**

We can construct rules that are a bit more complex. Let’s stick to this simple one and click **Next**

We can configure address range for this particular policy. We will give the whole range to those printers

Select **No** and click **Next**

We can set specific options that must be applied to those devices, or use the ones already configured. Click **Next**

On the summary screen click **Finish**

Now, that we have our policy created, we can use its context menu if we want to adjust some properties

### DHCP superscope

Being on **DC**, open the **DHCP** console if not already open

Choose **New Scope** from the context menu of the **IPv4** node

Click **Next**

Enter **Scope 1** in the **Name** field and click **Next**

Enter **192.168.80.20** for **Start IP address** and **192.168.80.240** for **End IP address**

Accept the proposed **Length** and **Subnet mask** and click **Next**

On the exclusions screen click **Next**

Accept the proposed **Lease duration** and click **Next**

Click **Next** on the options screen

Enter **192.168.80.254** in the **IP address** field, click **Add** and then click **Next**

Accept values on the next screen and click **Next**

Do not enter anything on the WINS servers screen and click **Next**

Make sure that **Yes, I want to activate this scope now** option is selected and click **Next**

Finally, click **Finish**

Again, choose **New Scope** from the context menu of the **IPv4** node

Click **Next**

Enter **Scope 2** in the **Name** field and click **Next**

Enter **192.168.81.20** for **Start IP address** and **192.168.81.240** for **End IP address**

Accept the proposed **Length** and **Subnet mask** and click **Next**

On the exclusions screen click **Next**

Accept the proposed **Lease duration** and click **Next**

Click **Next** on the options screen

Enter **192.168.81.254** in the **IP address** field, click **Add** and then click **Next**

Accept values on the next screen and click **Next**

Do not enter anything on the WINS servers screen and click **Next**

Make sure that **Yes, I want to activate this scope now** option is selected and click **Next**

Finally, click **Finish**

Now, let’s combine **Scope 1** and **Scope 2** into a **Superscope**

Select **IPv4** and from the context menu choose **New Superscope**

Click **Next** on the welcome screen

Then, enter **Superscope** in the **Name** field and click **Next**

Select both **Scope 1** and **Scope 2** using the **Ctrl** key and click **Next**

On the summary screen click **Finish** to create the superscope

### Multicast scope

Being on **DC**, open the **DHCP** console if not already open

Choose **New Multicast Scope** from the context menu of the **IPv4** node

Click **Next** on the welcome screen

Enter **Multicast Scope** in the **Name** field and click **Next**

Following the hint, enter **224.0.0.0** for **Start IP address** and **224.255.255.255** for **End IP address** and click **Next**

On the exclusions screen click **Next**

On the lease duration screen click **Next**

On the activation screen, make sure that **Yes** is selected and click **Next**

Click **Finish** to complete the process

### IPv6 scope

IPv6 scope creation is simpler compared to IPv4

Being on **DC**, open the **DHCP** console if not already open

Choose **New Scope** from the context menu of the **IPv6** node

Click **Next** on the welcome screen

Enter **Scope V6** in the **Name** text box and click **Next**

Enter **2001:db8::** in the **Prefix** field and click **Next**

On the exclusion screen click **Next**

Leave the **preferred** and **valid life time** values as proposed and click **Next**

Click **Finish** to initiate the process

### Name protection

Enabling DHCP name protection is matter of just one click

Being on the **DC** machine, open **DHCP** console if not already open

Select the **IPv4** node, invoke the context menu and select **Properties**

Switch to **DNS** tab and click **Configure** button

Turn on the **Enable Name Protection** option and click **OK**

Click **OK** to close the **IPv4 Properties** window

### Exclusion Lists

Go to the DHCP client machine

Check what is its MAC address and write it down

Return on the DC machine and open **DHCP** console if not already open

Select the **IPv4** node, invoke the context menu and select **Properties**

Switch to the **Filters** tab

Select the **Enable Deny List** option

Confirm with the **OK** button

Now, open the **Filters** node under **IPv4** and select the **Deny** node

Invoke the context menu and select **New Filter**

Enter the copied MAC address and click the **Add** button

Click the **Close** button to close the dialog box

Select again the **Deny** node and invoke the context menu

Select the **Enable** option

Now, return to the DHCP client machine

Open a terminal session

Execute the following command to release the current address

**ipconfig /release**

Then, ask for a new one with

**ipconfig /renew**

After a while the prompt will return and if we check, we will see that there is an APIPA address set up

Return to the DC machine and disable the deny filter

### Reservations

Being on the **DC** machine, open **DHCP** console if not already open

Select the **IPv4** node and open the **Simple Scope** node

Select the **Reservations** node

Invoke the context menu and select **New Reservation**

Enter a name

For the **IP address**, use 192.168.99.199

Enter the MAC address copied earlier

Click the **Add** button to add the record

Click the **Close** button to close the dialog box

Return to the DHCP client machine

Open a terminal session

Execute the following command to ask for a new address

**ipconfig /renew**

After a while the prompt will return indicating that the desired address was set up

### Clean up

Stop all the machines and restore their state to the checkpoint taken in the beginning of the practice

## Part 3: AD Activities & Services 103 (AD Activities)

### Service account

Log on to **DC** with account that has administrative privileges

Open **Server Manager**, navigate to **Tools** and click on **Active Directory Users and Computers**

Expand the **WSAA.LAB** node

Right-click and select **New > Organizational Unit**

Enter **Service Accounts** and click **OK**

Right-click the OU just created and select **New > User**

Enter **App1** in the **First name** field

Enter **Service** in the **Last name** field

Enter **App1Service** in the **User logon name** field

Click **Next**

Enter **Password1** in both **Password** and **Confirm** fields

De-select **User must change password at next logon**

Select **Password never expires**

Click **Next**

Click **Finish**

### Managed service account

Log on to **DC** with account that has administrative privileges

Open **Server Manager**, navigate to **Tools** and click on **Active Directory Users and Computers**

Expand the **WSAA.LAB** node

Right-click **Computers** node and select **New > Group**

Enter **ServerGroup** and click **OK**

Right-click the group just created and select **Properties**

Switch to **Members** tab

Click **Add**

Click on **Object Types**, select **Computers** and click **OK**

Enter **SERVER1**, click **Check Names** and click **OK**

Click **OK**

Open a **PowerShell** session and execute

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

While in **PowerShell**, execute the following command to create a service account

**New-ADServiceAccount -Name App2Service -DNSHostName App2Service.wsaa.lab -PrincipalsAllowedToRetrieveManagedPassword ServerGroup**

Continue on the terminal. Let’s associate the account to a computer account. Execute

**Add-ADComputerServiceAccount -Identity SERVER1 -ServiceAccount App2Service**

Log on to **SERVER1** with account that has administrative privileges

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

Find the **SNMP Trap** 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 **App2Service**, 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

*You can check the result of the above by starting the* ***Local Security Policy*** *tool ad going to* ***Local Policies > User Rights Assignment > Log on as a service***

*You may need to restart the machine(SERVER1) before you can use the managed service account*

### Virtual accounts

Log on to **SERVER1** with account that has administrative privileges

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

Find the **SNMP Trap** service and double-click on it

Switch to the **Log On** tab

If the settings here are disabled, then you must open a CMD shell with run as administrator and execute:

**sc managedaccount SNMPTrap false**

Then close the shell and return to the properties window of the service

Make sure that the **This account** option is selected

Enter **NT Service\SNMPTrap**

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

### Kerberos delegation

Log on to **DC** with account that has administrative privileges

Open **Server Manager**, navigate to **Tools** and click on **ADSI Edit**

Right-click the **ADSI Edit** node and select **Connect to**

Confirm with **OK**

Expand **Default naming context [DC.WSAA.LAB]** node

Expand the **DC=WSAA,DC=LAB** node

Select **OU=Service Accounts**

Select the **CN=App1Service** item in the middle section

Right-click and select **Properties**

Find the **servicePrincipalName** attribute and click **Edit**

Enter **http/portal.wsaa.lab:443** in the **Value to add** field and click **Add**

Click **OK**

Click **OK**

Switch to **Server Manager**, navigate to **Tools** and click on **Active Directory Users and Computers**

Navigate to the **Service Accounts** OU

Right-click the **App1Service** and select **Properties**

Switch to the **Delegation** tab

Select **Trust this user for delegation to any service (Kerberos only)**

Click **OK**

Open a CMD shell and type:

**setspn -l app1service**

You should see the SPN added earlier

We can add another one here by executing for example this:

**setspn -a web/portal.wsaa.lab:80 app1service**

Now, if we execute the previous command, we will see both SPNs

Return to the ADSI Edit tool to see how those two SPNs appear there

### Kerberos policy settings

Log on to **DC** with account that has administrative privileges

Open **Server Manager**, navigate to **Tools** and click on **Group Policy Management**

Navigate to the **Default Domain Policy** node

Open the policy for editing

Expand **Policies** node under **Computer Configuration**

Expand **Windows Settings**

Expand **Security Settings**

Expand **Account Policies**

Select **Kerberos Policy**

Explore available settings

Close **Group Policy Management Editor** and **Group Policy Management**

### Backing up system state \*

#### Installation

Log on to **DC** with account that has administrative privileges

Open **Server Manager**, navigate to **Manage** and click on **Add Roles and Features**

On the first page of the **Add Roles and Features** wizard click **Next**

Confirm that you are going to do a **Role-baser or feature-based installation** and click **Next**

On next screen, ensure that **DC** is selected and click **Next**

On the **Server Roles** screen click **Next**

On the **Features** page select **Windows Server Backup** and click **Next**

Click **Install** on confirmation page to start the installation process

Once the process is complete click **Close**

#### Shared folder

Log on to **SERVER1** with account that has administrative privileges

Create a folder **C:\BAK** and share it with **Full Control** for **Everyone**

#### Backup

Return to **DC**

Open **Server Manager**, navigate to **Tools** and click on **Windows Server Backup**

Select **Local Backup** in the left pane

Click **Backup Once** under **Actions**

Make sure that **Different options** option is selected and click **Next**

Select **Custom** and click **Next**

Click **Add Items**

Select **System state** and click **OK**

Click **Next**

Select **Remote shared folder** and click **Next**

Enter [\\SERVER1\BAK](file:///\\SERVER1\BAK) in the **Location** field and click **Next**

Click **Backup**

Once the process is complete, click **Close**

### Restoring system state \*

Log on to **DC** with account that has administrative privileges

Open **Server Manager**, navigate to **Tools** and click on **Active Directory Users and Computers**

Delete the **App1 Service** account

Close the **Active Directory Users and Computers**

Open a **Command Prompt** with **Run as administrator**

Type **msconfig.exe** and press **Enter**

Switch to **Boot** tab

Select **Safe boot** and **Active Directory repair**

Click **OK**

Click **Restart**

Login as local administrator

Navigate to **Tools** and click on **Windows Server Backup**

Select **Local Backup**

Click **Recover** under **Actions** pane

Select **A backup stored on another location** and click **Next**

Select **Remote shared folder** and click **Next**

Enter [**\\SERVER1\BAK**](file:///\\SERVER1\BAK)in the text field and click **Next**

Select the correct backup date and click **Next**

Select **System state** and click **Next**

Make sure that only the **Original location** option is selected and click **Next**

Click **OK** on the warning message box

Click **OK** to confirm that you want to continue

Select the **Automatically reboot the server to complete the recovery process** option and click **Recover**

Confirm that you want to continue with **Yes**

After the reboot, log on with local administrator

On the command prompt window press **Enter**

Open a new **Command Prompt** window with **Run as administrator**

Execute **ntdsutil** command

Select **activate instance NTDS** command

Execute the **authoritative restore** command

To mark only the **Service Accounts** OU to be restored with an authoritative restore, execute

**restore subtree "OU=Service Accounts,DC=wsaa,DC=lab"**

On the confirmation dialog click **Yes**

Execute **quit** and then again **quit** once more

Execute **msconfig.exe**

Switch to the **Boot** tab, deselect the **Safe boot** option and click **OK**

When prompted to restart, confirm with **Restart**

Log on normally

Open **Server Manager**, navigate to **Tools** and select **Active Directory Users and Computers**

Check the **Service Accounts** OU if the **App1 Service** account is restored

### Read-only domain controller

Log on to **SERVER2** with account that has administrative privileges

Open **Server Manager**, navigate to **Manage** and click on **Add Roles and Features**

On the first page of the **Add Roles and Features** wizard click **Next**

Confirm that you are going to do a **Role-baser or feature-based installation** and click **Next**

On next screen, ensure that **SERVER2** is selected and click **Next**

On the **Server Roles** screen select **Active Directory Domain Services**

When prompted to install additional features, confirm with **Add Features**

Click **Next**

On the **Features** page click **Next**

On the **AD DS** screen click **Next**

Click **Install** on confirmation page to start the installation process

Once the process is complete click **Close**

Click the yellow triangle next to the flag and select **Promote this server to a domain controller**

Make sure that the **Add a domain controller to an existing domain** option is selected and click **Next**

Select the **Read only domain controller (RODC)**

Type **Password1** in both password-related fields

Click **Next**

Click **Select** to set the **Delegated administrator account**

Enter **App1 Service**, click **Check Names** and then click **OK**

This way **App1 Service** account will be able to do local administrative tasks on the RODC

Click **Next**

On the **Additional Options** screen click **Next**

On the **Paths** screen click **Next**

On the **Review Options** screen click **Next**

On the **Prerequisites Check** click **Install**

When the process is complete, the system will restart automatically

Log on to **DC**

Open **Server Manager**, navigate to **Tools** and select **Active Directory Users and Computers**

Go to **Domain Controllers** OU

Select **SERVER2** and right-click and select **Properties**

Examine **Password Replication Policy** settings

### Child domain \*

#### Unjoin computer

Log on to **SERVER1** with account that has administrative privileges

Open a **PowerShell** session with **Run as administrator** and execute

**Remove-Computer -Restart**

Once the process is complete, computer will reboot

#### Install and configure domain controller

Log on back with the local administrator

Open a **PowerShell** session with **Run as administrator** and execute

**Install-WindowsFeature AD-Domain-Services -IncludeManagementTools**

Return to the **Server Manager** and refresh

Click the yellow triangle next to the flag and select **Promote this server to a domain controller**

Select **Add a new domain to an existing forest**

Enter **WSAA.LAB** in the **Parent domain name** field

Enter **CHILD** in the **New domain name** field

Click the **Change** button

Enter **WSAA\Administrator** and **Password1** and click **OK**

Click **Next**

Enter **Password1** in both recovery password-related fields and click **Next**

On the **DNS** screen click **Next**

On the **Additional Options** screen click **Next**

On the **Paths** screen click **Next**

On the **Review Options** screen click **Next**

On the **Prerequisites Check** screen click **Install**

After the process is complete, the machine will reboot

Log on with the new credentials – **CHILD\Administrator**

### Demote a domain controller \*

While logged on to **SERVER1** start **Server Manager** and execute **Manage > Remove Roles and Features**

Click **Next**

On the **Server destination** screen click **Next**

Deselect **Active Directory Domain Services**

When asked to remove features, confirm with **Remove Features**

Click on the **Demote this domain controller**

Select **Force the removal of this domain controller** option and click **Next**

Select **Proceed with removal** and click **Next**

Enter **Password1** in both password-related fields and click **Next**

Click **Demote**

Once the process is complete, the machine will reboot

### New forest

*NOTE: If you skipped the* ***Child domain*** *and* ***Demote a domain controller*** *exercises then you must unjoin the machine from the domain and then install the AD DS role*

Log on to **SERVER1** as administrator

In **Server Manager** click the yellow triangle next to the flag and select **Promote this server to a domain controller**

Select **Add a new forest**

Enter **DEMO.LAB** in the **Root domain name** field and click **Next**

Enter **Password** in both password-related fields and click **Next**

On the **DNS Options** screen click **Next**

On the **Additional Options** screen click **Next**

On the **Paths** screen click **Next**

On the **Review Options** screen click **Next**

On the **Prerequisites Check** screen click **Install**

Once the process is complete, the machine will reboot

### Multiple UPNs

Log on to **SERVER1** as **DEMO\Administrator**

Open **Server Manager**, navigate to **Tools** and select **Active Directory Domains and Trusts**

Right-click **Active Directory Domains and Trusts** and select **Properties**

Enter **academy.lab** in the **Alternative UPN suffixes** and click **Add**

Enter **demo.wsaa.lab** in the **Alternative UPN suffixes** and click **Add**

Click **OK** to close the properties window

### One-way external trust

#### Conditional forwarder #1

Log on to **DC** with **WSAA\Administrator**

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

Right-click **Conditional Forwarders** and select **New Conditional Forwarder**

Enter **demo.lab** in the **DNS Domain** text field

Enter **192.168.99.10** in the **IP Address** field

Click **OK**

#### Conditional forwarder #2

Log on to **SERVER1** with **DEMO\Administrator**

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

Right-click **Conditional Forwarders** and select **New Conditional Forwarder**

Enter **wsaa.lab** in the **DNS Domain** text field

Enter **192.168.99.2** in the **IP Address** field

Click **OK**

#### Trust

Log on to **DC** with **WSAA\Administrator**

Open **Server Manager**, navigate to **Tools** and click on **Active Directory Domains and Trusts**

Right-click on **WSAA.LAB** and select **Properties**

Switch to **Trusts** tab

You can see that there are both ingoing and outgoing trusts defined for **CHILD.WSAA.LAB**

*NOTE: The above may be not true if you decided to skip the* ***Child domain*** *exercise*

Click on **New Trust** button

Click **Next**

Enter **demo.lab** in the **Name** field and click **Next**

Make sure that the **External trust** option is selected and click **Next**

Select **One-way: outgoing** option and click **Next**

Select **Both this domain and the specified domain** option and click **Next**

If asked for credentials, enter the ones for **DEMO\Administrator** and click **Next**

Select **Domain-wide authentication** option and click **Next**

Click **Next** to create the trust

Click **Next**

Select **Yes, confirm the outgoing trust** and click **Next**

Click **Finish**

If a **SID Filtering** message appears, click **OK**

Now, the new trust must appear in the outgoing list

### Two-way forest trust

#### Remove existing trust

Log on to **DC** with **WSAA\Administrator**

Open **Server Manager**, navigate to **Tools** and click on **Active Directory Domains and Trusts**

Right-click on **WSAA.LAB** and select **Properties**

Switch to **Trusts** tab

Select the **DEMO.LAB** record under **Domains trusted by this domain** and click **Remove**

Select **Yes, remove the trust from both the local domain and the other domain**

Enter credentials for **DEMO\Administrator** and click **OK**

When asked if you are sure, answer **Yes**

If message saying that the trust is not found in the other domain, but will be removed from this, click **OK**

#### New trust

Click **New Trust**

Click **Next**

Enter **demo.lab** in the **Name** field and click **Next**

Make sure that the **Forest trust** option is selected and click **Next**

Select **Two-way** option and click **Next**

Select **Both this domain and the specified domain** option and click **Next**

If asked for credentials, enter the ones for **DEMO\Administrator** and click **Next**

Select **Forest-wide authentication** option and click **Next**

Select **Forest-wide authentication** option and click **Next**

Click **Next** to create the trust

On the **Route Name Suffixes** screen click **Next**

On the **Complete** screen click **Next**

Select **Yes, confirm the outgoing trust** and click **Next**

Select **Yes, confirm the incoming trust** and click **Next**

Click **Finish**

Click **OK** to close **Properties** window

### Test a trust

#### Trust validation

Log on to **DC** with **WSAA\Administrator**

Open **Server Manager**, navigate to **Tools** and click on **Active Directory Domains and Trusts**

Right-click on **WSAA.LAB** and select **Properties**

Switch to **Trusts** tab

Select **demo.lab** under **Domains trusted by this domain (outgoing trusts)** and click **Properties**

Click **Validate**

Select **Yes, validate the incoming trust**

Enter credentials for **DEMO\Administrator** and click **OK**

On the success message window click **OK**

When asked if you want to update name suffix routing, answer with **No**

Click **OK** to close **demo.lab** properties

Click **OK** to close **WSAA.LAB** properties

#### Trust test

Open **File Explorer** on the **DC**

Navigate to **C:\** and create a folder **C:\DATA**

Put a simple **Readme.txt** file there containing for example your name

In order to share the folder, do the following

Right-click and select **Properties**

Switch to **Sharing** taband click on **Advanced Sharing**

Select **Share this folder**

Click **Permissions**

Select **Everyone** and click **Remove**

Click **Add**

Enter **domain users**, click **Check Names** and then **OK**

Select **Allow** for **Full Control**

Click **Add**

Click **Locations**

Select **DEMO.LAB** and click **OK**

Enter **domain users**, click **Check Names** and click **OK**

Select **Allow** for **Full Control**

Click **OK** to close **Permissions for DATA** window

Click **OK** to close **Advanced Sharing** window

Click **Close** to close **DATA Properties**

Log on to **SERVER1** and try to reach **\\DC\DATA**