# Overview

To achieve greater reliability in DNS, you will need to configure secondary DNS zones. These zones contain copies of the primary zone. In this guided practice, you will enable zone transfers and create secondary zones. In addition, you will configure conditional forwarders to forwarder queries to other servers for specific zones.

# Objectives

* + Configure DNS on Windows server.
  + Plan a name resolution strategy.

## Skills Reviewed

* Installing DNS server role.
* Adding resource records to a DNS zone.
* DNS client configuration.

## New Skills

* Configuring DNS zone transfers.
* Creating DNS secondary lookup zones.
* Creating DNS conditional forwarders.

## References

# Initial conditions

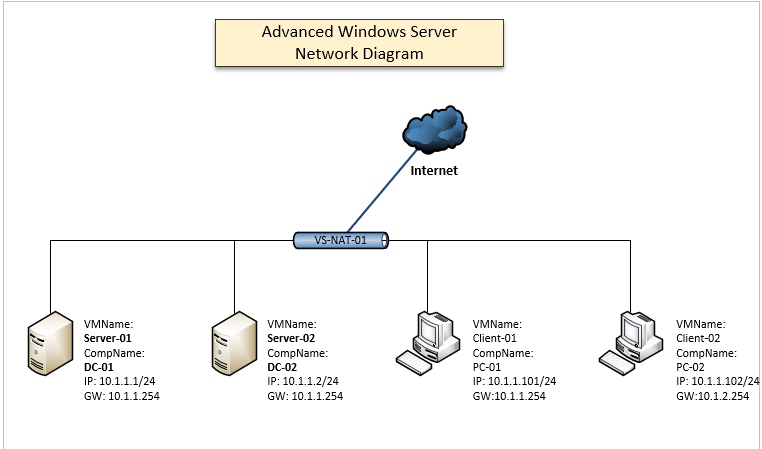
* Guided Practice – **Creating DNS Resource Records in Windows** is complete

# Final Conditions

* A secondary lookup zone for the **kmw.net** and **kmw.org** DNS zones on **Server-02.**
* All servers configured to use the DNS server on **Server-01**.

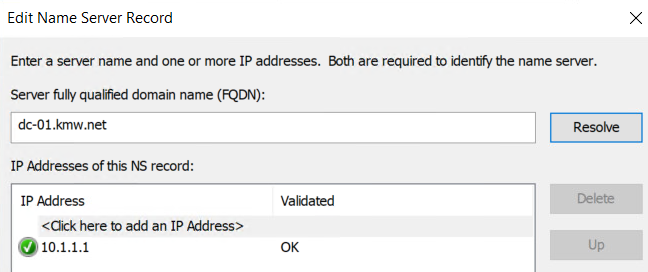
# Instructions

## Setup



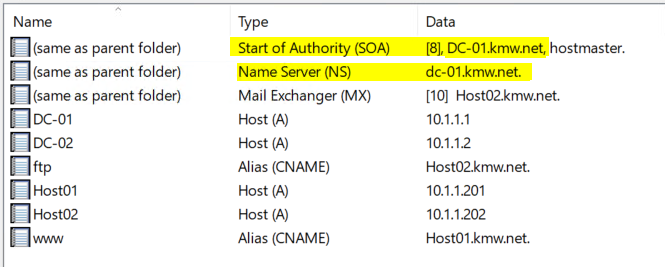
In the previous Guided Practice exercise, you practiced adding resources records for hosts that were not on your network. The diagram above is the topology for your network. Add the resource records for these servers.

1. On the **Server-01** virtual machine, add an **Address** **record** for the **DC-01** virtual machine in the **kmw.net** and **kmw.org** zones.
2. Adda **PTR** record for the **DC-01** computer.
3. On the **Server-01** virtual machine, add an **Address** **record** for the **DC-02** virtual machine in the **kmw.net** and **kmw.org** zones.
4. Adda **PTR** record for the **DC-02** computer.
5. Configure the **NS** record in **kmw.net** to point to **DC-01** host record.
   1. In the **kmw.net** zone, right click the **Name Server (NS)** record and select **Properties**. **Kmw.net** **Properties** opens to the **Name Servers** tab.
   2. Select **dc-01** name server and click the **Edit…** button.
   3. On the **Edit Name Server Record** page, in the **Server fully qualified domain name (FQDN):** box enter the **DC-01.kmw.net**. and then click **Resolve**. The name should resolve to the IP address of **DC-01**.



* 1. Click OK two times.

1. Configure the **NS** record in **kmw.org** to point to **DC-01** host record.
2. Configure the **Primary server:** in the **SOA** record in the **kmw.net** domain as **DC-01.kmw.net**. Date for the SOA and NS records should show **DC-01.kmw.net** and shown in the figure below.



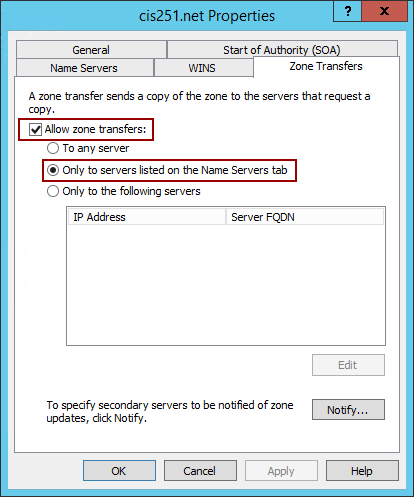
1. Configure the **Primary server:** in the **SOA** record in the **kmw.org** domain as **DC-01.kmw.org** and then verify that **DC-01.kmw.org** is shows in **Data** for **NS** and **SOA** record in the **kmw.org** zone.

## Creating a Secondary Lookup Zone

The **Server-02** virtual machine will be the secondary server for the zones you created in the previous Guided Practice exercise.

Secondary lookup zones are created for redundancy and reliability. These zones contain a copy of the primary zone on another server. There should only be one primary zone and as many secondary zones as you need for redundancy and reliability. To configure a secondary zone, you need the name of the zone and the IP address or name of the server with the primary zone. **Note**: In some documentation these zones are referred to as master (primary) and slave (secondary) zones.

### Configuring a Zone to Allow Zone Transfers

Before you can create a secondary zone, you need to authorize other DNS servers to get a copy of the zone from your server. The most secure way is to add an **NS** record to your domain. The default security will allow zone transfers to any server with a configured **NS** record. The other options are to allow a server with a specific IP address or to allow any server. These can be configured from the **Zone Transfers** tab of the zone properties dialog box shown in the figure.

To add an **NS** Record to the kmw.net zone using the **GUI**, perform the following steps:

1. Logon to the **Server-01** virtual machine as the **administrator** account.
2. Open the **DNS** **Manager** console.
3. Highlight the **kmw.net** folder in the **Forward** **Lookup** **Zones** node in the console tree.
4. Select **Properties** from the **context** **menu** for the **kmw**.**net** node.
5. Select the **Name** **Servers** tab.
6. Click the **Add**… button.
7. Type **DC-02.kmw.net** in the **Server Fully Qualified Domain name**: text box and click the **Resolve** button. This should resolve the IP address but gives a message that this server is not authoritative for this zone. Click **OK**.
8. Click **OK** to exit the properties dialog box.

To add an NS Record to the **kmw.org** zone using the command line, perform the following steps:

1. Logon to the **Server-01** virtual machine as the **administrator** account.
2. Open the **PowerShell** console with administrative rights.
3. Type the following in PowerShell: (Note: in this example “.” refers to the current domain)

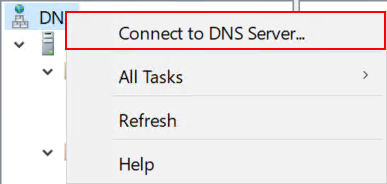
Add-DnsServerResourceRecord -ZoneName kmw.org -NS -Name . -NameServer dc-02.kmw.org

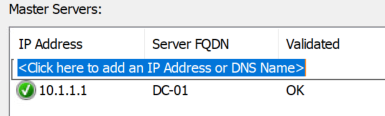
1. Use PowerShell to verify the record was added. You should see output like the figure below.

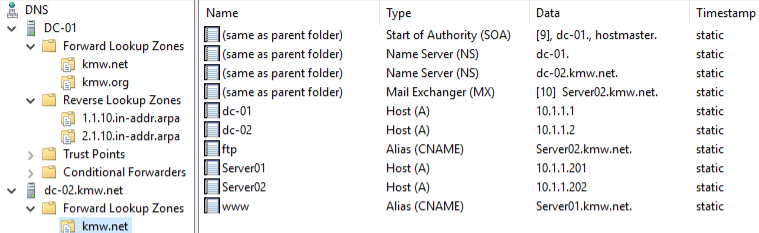


### Creating a Secondary Lookup Zone from the GUI

Perform the following to create a secondary lookup zone from the GUI:

1. Logon to the **Server-01** virtual machine as the **administrator** account
2. Open the **DNS** **Management** console
3. Add the **Server-02** DNS server to the console as follows:
   1. Select the **Connect to DNS Server**… option **from** the **context** **menu** of the DNS node as shown in the figure.
   2. In the **Connect to DNS Server** dialog box **select** the “**The following computer:**” option and type **DC-02.kmw.net.**
   3. Your console should now have a node named **DC-02.kmw.net**. You will work in this node for the remainder of this section.
4. Highlight the **Forward** **Lookup** **Zones** node in the console tree.
5. Select **New Zone**… from the **context** **menu** of the **Forward Lookup Zones** node to launch the **New Zone wizard.**
6. On the **Welcome to the New Zone Wizard** page of the wizard, click **Next**.
7. On the **Zone Type** page of the wizard, select **Secondary** **zone** and then click **Next.**
8. On the **Zone Name** page of the wizard, type **kmw.net** in the **Zone Name**: edit box and click **Nex**t.
9. On the **Master DNS Servers** page of the wizard, type **10.1.1.1** in the **Master Servers**: edit box and click **Next.** The IP address should resolve to **DC-01**.



1. On the **Completing the New Zone Wizard** page of the **New** **Zone** **Wizard**, click **Finish**.
2. Verify the zone was created using one of the methods shown previously. You should see all the records you created in the **KMW.net** zone on the **Server-02** server. **Note**: this may take a little time to happen.

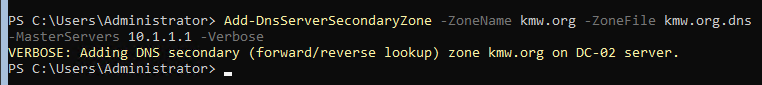
### Creating a Secondary Lookup Zone from the Command Line

Perform the following to create a secondary lookup zone from the GUI:

1. Logon to the **Server-02** virtual machine as the **administrator** account.
2. Open a **PowerShell** console with administrative rights.
3. Type the following in the shell:

Add-DnsServerSecondaryZone -ZoneName kmw.org -ZoneFile kmw.org.dns -MasterServers 10.1.1.1 -Verbose

1. You should see the output shown in the figure below.



1. To enable the zone transfer, login to the **Server-01** virtual machine and type the following command in PowerShell:

Set-DnsServerPrimaryZone -ZoneName kmw.org -Notify NotifyServers -NotifyServers 10.1.1.2 -SecureSecondaries TransferToSecureServers -SecondaryServers 10.1.1.2

1. Return to the **Server-02** virtual machine and type the following in PowerShell to verify the zone transfer:

Get-DnsServerResourceRecord -ZoneName kmw.org

1. Your output should be like that shown below:

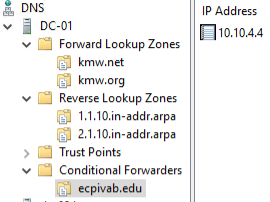
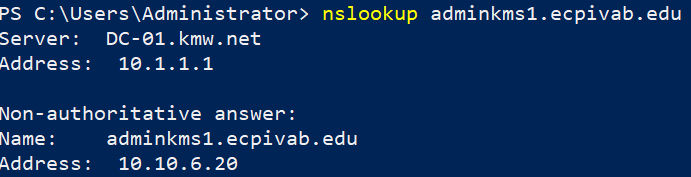
A picture containing table

Description automatically generated

## Configuring Forwarders

A DNS forwarder is used to forward all queries to another DNS server. A conditional forwarder will forward queries for a specific domain to another server. This does not prevent a server from resolving names for zones configured on that server. Your organization would like to do this.

To configure the **Server-01** to forward queries for hosts in the **ecpivab.edu** domain to the DNS Server at **10.10.4.4** using the GUI, perform the following:

1. Logon to the **Server-01** virtual machine as the **administrator** account.
2. Highlight the **Conditional Forwarders** node in the console tree.
3. Select **New Conditional Forwarder…** from the **context** **menu** for the **Conditional Forwarders** node
4. In the **DNS Domain**: edit box of the **New** **Conditional** **Forwarder** dialog box type **ecpivab.edu**
5. In the **IP addresses of the master servers**: edit box of the **New** **Conditional** **Forwarder** dialog box type **10.10.4.4** and click **OK**. When you entered **10.10.4.4**, you received an error. Why was this an expected error?
6. When you are done, your configuration should look like the figure.
7. Use the **nslookup** command to verify that you can resolve names in the **ecpivab.edu** domain.

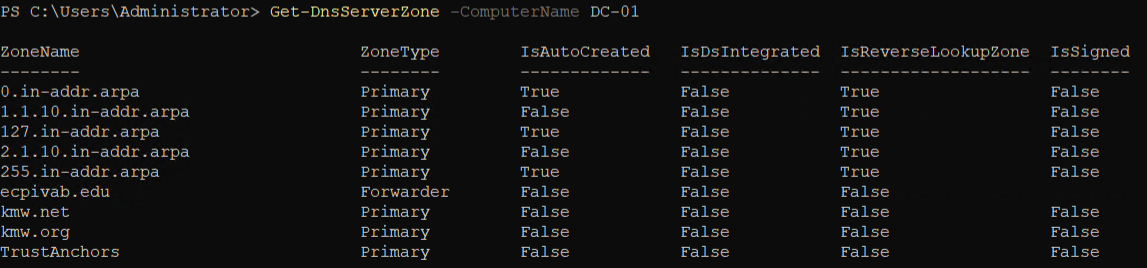
Configure **Server-02** to **forward** **all** **queries** **for** any zone that it is not authoritative for to the DNS Server on **Server-01** using PowerShell, perform the following:

1. Logon to the **Server-02** virtual machine as the **administrator** account.
2. Open the **PowerShell** console with administrative rights.
3. Type the following in PowerShell:

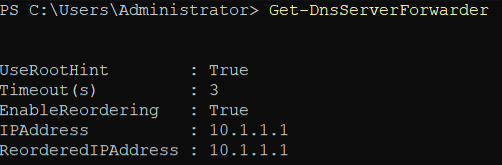
Add-DnsServerForwarder -IPAddress 10.1.1.1

1. Verify the conditional forwarder zone was created with the following command:

Get-DnsServerZone -ComputerName DC-01

1. Your output should look like the figure below.
2. Verify the forwarder was created with the following command:

Get-DnsServerForwarder

1. Your output should look like the figure below.

## Submission Requirements

1. **Download** the **grading** **script** from the assignment page to the **C:\Scripts** folder.
2. Check your lab by running the following command:

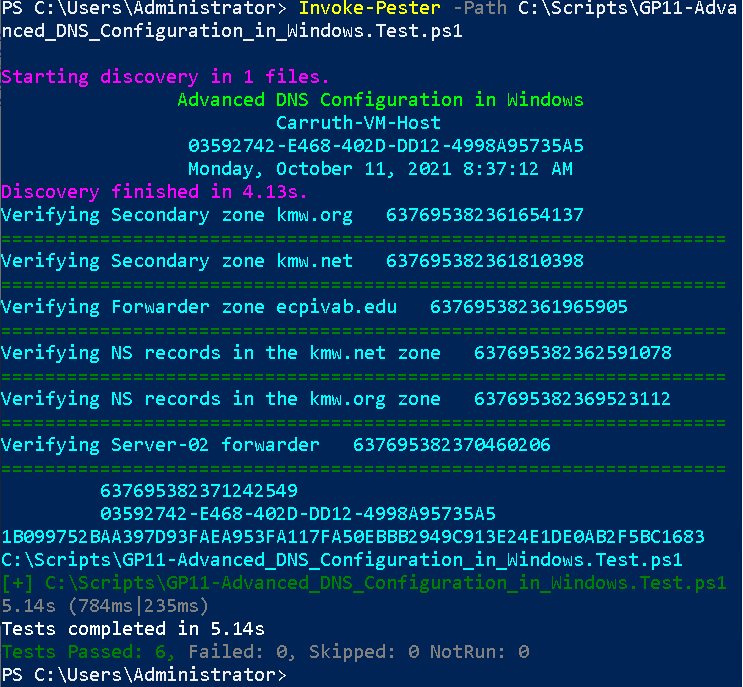
Invoke-Pester -Path C:\Scripts\GP11-Advanced\_DNS\_Configuration\_ in\_Windows.Test.ps1

**Note**: You will see a security warning when running the script. Enter **R** to run the script.

If you want to see more detail, add **-Output Detailed** to the command. This may assist you with troubleshooting

Invoke-Pester -Path C:\Scripts\GP11-Advanced\_DNS\_Configuration\_ in\_Windows.Test.ps1 -Output Detailed

1. You should not see any red in the output. Red in the PowerShell way of telling you that an error condition exists. Most of the time, the output will tell you what is wrong. If it is not obvious, contact your teacher and ask for assistance. You will be learning PowerShell during this term. **Correct** any **errors** you may have and run the script until all the output has no red. You should see the output like the images below.



1. Capture a snippet that shows the PowerShell Command and all its output. If you must use more than one snippet to capture the output, you must have at least **one line of overlap** in the snippets. The text in the snippets **must be legible** when pasted into the Word document. Paste the snippet(s) into a **new** **Word** **document**
2. **Fill** **in** the **information** in the following table. Copy the following table into the **Word** **document** and fill in the information about all the **new** commands used in this lab (the example provided is not a new command and should be deleted):

|  |  |  |
| --- | --- | --- |
| PowerShell Commands | | |
| Command | Example | Description |
| Get-Childitem | Get-Childitem -Path C:\ | Displays the files in the C:\ directory |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

1. **Upload** the **document** in the submission area of the assignment.