Windows Server Configuration

Lab 12

Domain Name System (DNS)

Developed by Florida State College at Jacksonville for iNoVATE-X #1501359 (S-STEM)

This is a temporary template that can be used when developing the labs. Change names and references as needed. This template will still need final approval from the grant coordinator as well as legal.
## Contents

- Introduction .................................................................................................................. 3
- Objectives ....................................................................................................................... 3
- Topology .......................................................................................................................... 4
- Lab Settings ..................................................................................................................... 5
- Additional info ................................................................................................................ 5

### 1 DNS ................................................................................................................................ 6
- 1.1 Installing the DNS Role ............................................................................................. 6
- 1.2 Configuring DNS ......................................................................................................... 18

### 2 DNS Replication and Forwarders .................................................................................. 26
- 2.1 Zone Replication .......................................................................................................... 26
- 2.2 Forwarders and Root Hints .......................................................................................... 31

### 3 DNS Records ................................................................................................................ 35
- 3.1 DNS Cache ................................................................................................................... 35
- 3.2 DNS “A Records” ......................................................................................................... 38
- 3.3 Reverse Lookup Zones and PTR Records ..................................................................... 42

### 4 Research (Optional) ...................................................................................................... 48

## References ....................................................................................................................... 48
Introduction

The purpose of this lab is to introduce the student to concepts related to Domain Name Services (DNS). In this lab the student will install the DNS Role and then configure it. They will also look at DNS Replication and Forwarders. They will also work with DNS records and Reverse Lookup Zones.

Objectives

4.3. Deploy and configure DNS service
4.3.1. Configure Active Directory integration of primary zones,
4.3.2. configure forwarders,
4.3.3. configure Root Hints,
4.3.4. manage DNS cache,
4.3.5. create A and PTR resource records
Topology
Lab Settings

Server: W2K12E-CORE
Username: Administrator
Password: Password1

Server: W2K12R2-ADDC
Username: Administrator
Password: P@ssw0rd1

Additional info
1 DNS

DNS or Domain Name System is used to translate domain names to IP addresses. We as humans have a much easier time remembering words and names rather than a random string of numbers.

1.1 Installing the DNS Role

1. Open the Windows W2K12R2-CORE server by clicking the icon in the topology. Click “PC > Send CTRL+ALT+DEL”.

2. Type **Password1** as the administrator password and hit “Enter”.

3. Type **powershell.exe** and hit “Enter” to start PowerShell.
4. Type `install-windowsfeature server-gui-shell -source wim:d:\sources\install.wim:4` and hit “Enter”.  
   (Note: Installation will take 5-10 minutes.)

```
PS C:\Users\Administrator> install-windowsfeature server-gui-shell -source wim:d:\sources\install.wim:4
```

5. The installation will pause at 68% for a few minutes. Wait for the installation to complete.

```
Start Installation...  
58%                                1
```

```
PS C:\Users\Administrator> set-date -date "7/30/2014 PM"
```

6. Type, `restart-computer` and hit “Enter”.

```
Success Restart Needed Exit Code Feature Result
--------- --------------- --------------------------
True Yes SuccessRestart... (Graphical Management Tools and Infras...
WARNING: You must restart this server to finish the installation process.
WARNING: Windows automatic updating is not enabled. To ensure that your newly-installed role or feature is automatically updated, turn on Windows Update.
```

```
PS C:\Users\Administrator> restart-computer,
```

7. Log in to the upgraded W2K12R2-CORE server by clicking “PC > Send CTRL+ALT+DEL” and entering the password **Password1**.

![Server Manager Dashboard]

9. On the “Server Manager – Dashboard”, select the link next to “Ethernet 3”.

![Server Manager Properties]

10. Right click on “Ethernet 3” and select “Disable”.

![Ethernet 3 Disable]
11. Right click on “Ethernet 4” and select “Disable”.

12. Right click on “Ethernet 2” and select “Properties”.

14. Click the radio button next to “Use the following IP address” and type the following IP address: **192.168.1.125**
   Subnet mask: **255.255.255.0**
   Default gateway: **192.168.1.1**
   Preferred DNS server: **192.168.1.100**
   Click “Ok” twice and close the “Network Connections” window.

15. On the “Server Manager –Dashboard”, left click the start button and begin typing **sysdm.cpl** and select the search results for sysdm.cpl.
16. On the “System Properties” window, click “Change”.

![System Properties window]

Windows uses the following information to identify your computer on the network.

- Computer description: 
  For example: “IIS Production Server” or “Accounting Server”.
- Full computer name: W2K12R2-CORE.mydomain.local
- Domain: mydomain.local

To rename this computer or change its domain or workgroup, click Change.

17. Click the radio button next to “Domain” and type **mydomain.local**. Click “Ok”.

![Computer Name/Domain Changes window]

Computer Name/Domain Changes

You can change the name and the membership of this computer. Changes might affect access to network resources.

- Computer name: W2K12R2-CORE
- Full computer name: W2K12R2-CORE

Member of
- Domain: mydomain.local
- Workgroup: WORKGROUP

[OK] [Cancel]
18. On the “Windows Security” pop-up, type **Administrator** as the user name and **P@ssw0rd1** as the password. Click “Ok”.

![Computer Name/Domain Changes](image)

19. You will be prompted with a “Welcome to the mydomain.local domain” message. Click “Ok”.

![Computer Name/Domain Changes](image)

20. Click “Ok” to restart the computer.
21. Click “Close” on the “System Properties” window.

22. Click “Restart Now”.

23. Log in to the upgraded W2K12R2-CORE server by clicking “PC > Send CTRL+ALT+DEL”.

Press Ctrl+Alt+Delete to sign in.
24. Click the arrow pointing to the left to select a new user.

25. Click on “Other User”. Type `mydomain\administrator` as the user name and `P@ssw0rd1` as the password and hit “Enter”.

26. On the “Server Manager – Dashboard” navigate to “Manage > Add Roles and Features”.
27. On the “Before You Begin” page, click “Next”.

28. On the “Installation Type” page, leave the defaults and click “Next”.
29. On the “Server Selection” page, click “Next”.

![Select destination server](image)

30. On the “Server Roles” page, place a check mark by “DNS Server”. A features window will appear showing dependency features that must be installed. Click “Add Features”.

![Add Roles and Features Wizard](image)
31. On the “Server Roles” page, click “Next”.

32. On the “Features” page, click “Next”.
33. On the “DNS Server” page, read the information on DNS and click “Next”.

Domain Name System (DNS) provides a standard method for associating names with numeric Internet addresses. This makes it possible for users to refer to network computers by using easy-to-remember names instead of a long series of numbers. In addition, DNS provides a hierarchical namespace, ensuring that each host name will be unique across a local or wide-area network. Windows DNS services can be integrated with Dynamic Host Configuration Protocol (DHCP) services on Windows, eliminating the need to add DNS records as computers are added to the network.

Things to note:

- DNS server integration with Active Directory Domain Services automatically replicates DNS data along with other Directory Service data, making it easier to manage DNS.
- Active Directory Domain Services requires a DNS server to be installed on the network. If you are installing a domain controller, you can also install the DNS Server role using Active Directory Domain Services Installation Wizard by selecting the Active Directory Domain Services role.

34. On the “Confirmation” page, click “Install”.

To install the following roles, role services, or features on selected server, click Install.

- Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

- DNS Server
- Remote Server Administration Tools
- Role Administration Tools
- DNS Server Tools
35. On the “Results” page, after the installation completes, click “Close”.

![Installation progress](image)


![Server Manager Dashboard](image)

37. On the “DNS Manager” window, expand W2K12R2-CORE to view the options on the new DNS role.

![DNS Manager](image)

38. In the next steps we will make some changes to the DNS server that has been pre-installed on W2K12R2-ADDC.
1.2 Configuring DNS

1. Open the Windows W2K12R2-ADDC server by clicking the icon in the topology. Click “PC > Send CTRL+ALT+DEL”.

2. Type P@ssw0rd1 as the administrator password and hit “Enter”.


![Image of DNS configuration process]
4. On the “DNS Manager” window, expand “W2K12R2-ADDC”, expand “Forward Lookup Zones” and expand “mydomain.local”. Notice the domain machines that are listed.

5. Right click on “mydomain.local” and select “Delete”.
6. Click “Yes” to delete the zone.

7. Click “Yes” at the warning.

(Note: It is not a good idea to delete Primary DNS zones. We are only deleting the Primary DNS zone so that we can run through configurations.)
8. Right click “Forward Lookup Zones” and select “New Zone”.

9. Click “Next” at the New Zone Wizard.
10. On the “Zone Type” window, leave the default “Primary Zone” selected and notice that we have the option to store the zone in Active Directory. Click “Next”.

![New Zone Wizard](image)

11. Leave the defaults on the Replication Scope window, click “Next”.

![New Zone Wizard](image)
12. For the zone name, type “mydomain.local”, click “Next”.

13. On the “Dynamic Update” window, read the different options, leave the default and click “Next”.

14. On the “Completing the New Zone Wizard” window, click “Finish”.

![New Zone Wizard](image)

15. Expand the new zone “mydomain.local”. You will only see the “W2K12R2-ADDC” host listed.

![DNS Zone Configuration](image)

(Note: Clients present themselves to DNS when added to the domain, otherwise they only update about once every 24 hours. We will expedite that process.)
16. Return to the “W2K12R2-CORE” machine and log in if necessary. Right click the start button and select “Command Prompt”.

17. On the command prompt, type `ipconfig/registerdns` and hit “Enter”.

18. Return to the “W2K12R2-ADDC” machine. On the “DNS Manager”, right click in the open white area and select “Refresh”. If W2K12R2-CORE does not show up, wait a few minutes and refresh again.
2 DNS Replication and Forwarders

For redundancy, there should be at least two DNS servers on a network. Some Zones may require an independent DNS server. Here we can choose which zones to replicate across servers.

2.1 Zone Replication

1. On the “W2K12R2-ADDC” machine, right click on “mydomain.local” and select “Properties”.

![Image of DNS settings with properties selected]
2. Select the “Zone Transfers” tab, place a check mark by “Allow zone transfers” and click “Ok”.


4. On the DNS Manager, expand W2K12-CORE.
5. Left click, then right click “Forward Lookup Zones” and select “New Zone”.

6. On the New Zone window, click “Next”.
7. On the “Zone Type” window, click the radio button next to “Secondary Zone” and click “Next”.

8. On the “Zone Name” window, type `mydomain.local` and click “Next”.

9. On the “Master DNS Servers” window, type **192.168.1.100** and hit “Enter”.

10. Click “Next” then click “Finish”.

![New Zone Wizard](image)

![Completing the New Zone Wizard](image)
11. Expand mydomain.local. You may get an error at first. Wait a couple of minutes and refresh.

12. The DNS entries will appear. You have successfully transferred a Primary Zone to a Secondary Zone.

2.2 Forwarders and Root Hints

1. Click on W2K12R2-CORE, right click on Forwarders and select Properties.
2. On the Properties window, select the Forwarders tab. Read the information regarding forwarders.

3. Click “Edit”, type **8.8.8.8** and click “OK”
4. The address will not resolve because there is no internet connection. The address 8.8.8.8 is the Google public DNS.

![W2K12R2-CORE Properties dialog](image)

5. On the Properties window, select the Root Hints tab.
6. On your **local computer**, open a command prompt and ping one of the root servers.

```
C:\Users\username>ping 192.5.5.241
```

```
Pinging 192.5.5.241 with 32 bytes of data:
Reply from 192.5.5.241: bytes=32 time=31ms TTL=57
Reply from 192.5.5.241: bytes=32 time=31ms TTL=57
Reply from 192.5.5.241: bytes=32 time=31ms TTL=57
Reply from 192.5.5.241: bytes=32 time=33ms TTL=57
```

**Ping statistics for 192.5.5.241:**

- Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
- Approximate round trip times in milliseconds:
  - Minimum = 31ms, Maximum = 33ms, Average = 31ms

7. On your local computer, type **nslookup 192.5.5.241**

```
C:\Users\username>nslookup 192.5.5.241
```

```
Name: f.root-servers.net
Address: 192.5.5.241
```

8. These are the public root DNS servers.

![DNS Server List]

3 DNS Records

Because DNS servers keep a record of addresses that have been resolved, they can sometimes contain incorrect information. DNS can also become poisoned this way by viruses and malware.

3.1 DNS Cache

1. On the W2K12R2-ADDC machine, right click the start button and select “Command Prompt”.

![Command Prompt window]

2. Type `powershell.exe` and hit “Enter” to start PowerShell.

```
C:\Users\Administrator>powershell.exe
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.
PS C:\Users\Administrator>
```

3. Right click the small icon in the upper left corner of the command prompt window and select the Properties option.

![Properties dialog box]
4. Click the “Layout” tab and change the Window Size width to 120. Click “Ok”.

5. On the W2K12R2-ADDC machine, type `Show-DnsServerCache -ComputerName W2K12R2-ADDC` and hit “Enter”. DNS servers will cache resolutions to limit the requests sent to root DNS servers. Close the command prompt window.

![Server Manager - Dashboard](image)

7. On the “DNS Manager” window, expand W2K12R2-ADDC, expand “Forward Lookup Zones” and expand mydomain.local.

![DNS Manager Window](image)

8. Right click on the “Start of Authority” and select Properties.

![Start of Authority Properties](image)
9. DNS cache settings are set by the DNS administrator on this tab, and only available on authoritative DNS servers. Close the properties window.

(Note: Administrators often use the `ipconfig /flushdns` command to clear the DNS cache when troubleshooting DNS errors.)

3.2 DNS “A Records”

10. On the DNS Manager window, notice the timestamp column. Anything with a date is a dynamic update to the DNS record and is subject to change if the addressing changes.
11. Right click the white area and select “New Host (A or AAAA)”.

12. On the “New Host” window, type **office** as the name and **192.168.1.20** in the address bar. Click “Add Host”. Click “Done”.

![New Host window](image)
13. Click in the white area and select refresh.

14. The name “office” shows up as a static entry because we manually added the “A Record”.

15. Right click the start button and select command prompt.
16. On the Command Prompt, type **ping office** and hit “Enter”.

```
C:\Users\Administrator>ping office
PING 192.168.1.20 (192.168.1.20) 56(84) bytes of data.
64 bytes from 192.168.1.20: icmp_seq=1 ttl=64 time=1ms
64 bytes from 192.168.1.20: icmp_seq=2 ttl=64 time=1ms
64 bytes from 192.168.1.20: icmp_seq=3 ttl=64 time=1ms
64 bytes from 192.168.1.20: icmp_seq=4 ttl=64 time=1ms
Ping statistics for 192.168.1.20:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss).
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

17. Return to the DNS Manager by clicking the icon in the taskbar.
3.3 Reverse Lookup Zones and PTR Records

18. On the “DNS Manager” window, left click, then right click on “Reverse Lookup Zones” and select “New Zone”.

![Add a New Zone](image)

19. On the “New Zone Wizard” window, click “Next”.

![Welcome to the New Zone Wizard](image)

20. On the “Zone Type” window, leave the default “Primary Zone” and click “Next”.

![Zone Type](image)
21. On the “Active Directory Zone Replication Scope” window, click “Next”.

![Active Directory Zone Replication Scope](image)

22. On the “Reverse Lookup Zone Name” window, click “Next”.

![Reverse Lookup Zone Name](image)
23. On the “Reverse Lookup Zone Name” window, type **192.168.1** for the Network ID and click “Next”.

24. On the “Dynamic Update” window, click “Next”.

---

**Reverse Lookup Zone Name**

A reverse lookup zone translates IP addresses into DNS names.

To identify the reverse lookup zone, type the network ID or the name of the zone.

- **Network ID:**
  
  192.168.1

  The network ID is the portion of the IP addresses that belongs to this zone. Enter the network ID in its normal (not reversed) order.

  If you use a zero in the network ID, it will appear in the zone name. For example, network ID 10 would create zone 10.in-addr.arpa, and network ID 10.0 would create zone 0.10.in-addr.arpa.

- **Reverse lookup zone name:**
  
  1.168.192.in-addr.arpa

---

**Dynamic Update**

You can specify that this DNS zone accepts secure, nonsecure, or no dynamic updates.

Dynamic updates enable DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur.

Select the type of dynamic updates you want to allow:

- **Allow only secure dynamic updates (recommended for Active Directory)**
  
  This option is available only for Active Directory-integrated zones.

- **Allow both nonsecure and secure dynamic updates**
  
  Dynamic updates of resource records are accepted from any client.
  
  **WARNING:** This option is a significant security vulnerability because updates can be accepted from untrusted sources.

- **Do not allow dynamic updates**
  
  Dynamic updates of resource records are not accepted by this zone. You must update these records manually.
25. On the “Completing the New Zone Wizard” window, click “Finish”.

26. Expand Reverse Lookup Zones, left click, then right click on 1.168.192.in.addr.arpa and select “New Pointer (PTR)”.
27. On the “New Resource Record” window, type **192.168.1.20** for the Host IP Address and **office** as the Host name. Click “OK”.

While DNS A Records translate IP addresses from names, Reverse Lookups and PTR records translate names from IP addresses.

28. Right click the start button and select Command Prompt,
29. On the command prompt, type `nslookup 192.168.1.21` and hit “Enter”. The computer will return a response that it cannot find 192.168.1.21 because there is no PTR record.

```
C:\Users\Administrator>nslookup 192.168.1.21
Dns request timed out.
    timeout was 2 seconds.
Server:  Unknown
Address:  ::1
*** Unknown can’t find 192.168.1.21: Non-existent domain
```

30. On the command prompt, type `nslookup 192.168.1.20` and hit “Enter”. The computer will respond that it found the name “office” for the address.

```
C:\Users\Administrator>nslookup 192.168.1.20
Dns request timed out.
    timeout was 2 seconds.
Server:  Unknown
Address:  ::1
Name:  office
Address:  192.168.1.20
```
Take any screenshots and notes required by your instructor and click “I’M DONE” at the top of the topology page. You may complete this lab as many times as you wish by making a new reservation.

4  Research (Optional)

   1. ICAAN
   2. IANA

References

1. Planning DNS Servers

2. Setting up DNS

3. Reverse lookup