Lab 4 preparation

By the end of this lab you should have:

1 Domain Controller running Windows 2008r2 Enterprise server CORE

1 Windows 2008 r2 Enterprise server (full install) member server.

1 Windows 7 client computer

1 Windows 2008r2 Enterprise server CORE file server

**NOTE: the commands in this lab can be easily miss-typed. Pay careful attention to the commands and make sure they are successful *before* continuing!**

## 0: Clone Machines

* First, clone one set of servers (all three) from the library to your workspace naming it the collection NAP-1. Remember to delete and re-add network adapters before deploying.
* Next, clone another server (only one this time – the server ‘DC’) to your workspace naming it NAP-2. Remember to delete and re-add the network adapter before deploying. Also, if you can; rename this server from DC to SERVER. This machine will be in a different group, but it will still be able to interact with your other virtual lab machines.
* When finished you should have one set of three virtual computers and one set of one virtual computer.

## 1: Domain Controller

1. Set the administrator password

**net user administrator \***

1. Disable IPv6. The following Disables IPv6 for Vista/Windows 7/2008/2008r2 (REF: <http://support.microsoft.com/kb/929852>)
   1. From the command prompt, type in **regedit**
   2. If prompted for User Account Control, click Continue.
   3. Expand HKEY\_LOCAL\_MACHINE 🡪SYSTEM 🡪CurrentControlSet 🡪Services 🡪TCPIP6 🡪Parameters
   4. From the menu Select Edit 🡪 New 🡪 Key 🡪DWORD (32-bit) Value
   5. Name the key **DisabledComponents**
   6. Double click on the new key to edit the value.
   7. In the **Value data:** field, enter **ff**[[1]](#footnote-1).
   8. Click on **OK**
   9. Close the Registry Editor
2. Enable ICMP PING in the Firewall

**netsh advfirewall firewall add rule name=”ICMP Allow incoming V4 echo request” protocol=icmpv4:8,any dir=in action=allow**

1. Set the time zone to **(GMT -5:00) Eastern Time (US & Canada)**

**control timedate.cpl**

1. Set the DNS address to the local IP address, where <IP address> is the IP address of the server.

**netsh int ip set dns "Local Area Connection" static <IP address>**

1. Change the computer name to DC-lastname (where lastname is your last name)

**wmic computersystem where name=”%COMPUTERNAME%” call rename name=”DC-Lastname”**

1. Restart

**shutdown /r /t 0**

1. Run unattended AD setup using unattended answer file.
   1. Run **notepad.exe** from the command prompt.
   2. Put all necessary information to make the virtual machine a domain controller.
   3. Make sure to set the forest and domain functional level to 2008 (Level 4).
   4. Your domain name should be lastname.local (for example, barker.local)
   5. Also install DNS.
   6. Save the file name as C:\unattend.txt
   7. Include a copy of the text from the unattend.txt file in your report

Example file (yours won’t look exactly like this):

**[DCInstall]**

**InstallDNS=yes**

**ReplicaOrNewDomain=Domain**

**NewDomain=Forest**

**NewDomainDNSName=texas.local**

**SafeModeAdminPassword=Password1**

**DomainLevel=4**

**ForestLevel=4**

The command to set up a domain controller using an unattended install file:

**dcpromo /unattend:C:\unattend.txt**

1. Restart if the computer didn’t restart as part of the AD install (you can force a reboot in the unattend.txt file, but it is not included above. The line would be RebootOnCompletion=yes)
2. Once the server restarts, log in and create two user accounts for yourself.
   1. From the CMD prompt, type in:

**net user FiresName.LastName yourpassword /add** (ex: net user Cary.Barker Password1 /add)

* 1. Create an administrative account: From the CMD prompt, type in:

**net user FirstNameØLastName yourpassword /add** (where Ø is a zero).

* 1. Add your new account to the “Domain Admins” group for administration:

**net group “Domain Admins” FirstNameØLastName /add**

1. Enable Terminal services

**cd /windows/system32**

**cscript scregedit.wsf /ar 0**

1. Enable remote management: (REF: <http://technet.microsoft.com/en-us/library/dd759202.aspx>)
   1. Install the following features by typing in the below command(s): NetFx2-ServerCore, MicrosoftWindowsPowerShell, ServerManager-PSH-Cmdlets, BestPractices-PSH-Cmdlets
      * You can either enable these features through entering one long command or four separate commands:

This is one long command:

**Dism.exe /Online /Enable-Feature /FeatureName:NetFx2-ServerCore /FeatureName:MicrosoftWindowsPowerShell /FeatureName:ServerManager-PSH-Cmdlets /FeatureName:BestPractices-PSH-Cmdlets**

Or use four separate commands:

**Dism.exe /Online /Enable-Feature /FeatureName:NetFx2-ServerCore**

**Dism.exe /Online /Enable-Feature /FeatureName:MicrosoftWindowsPowerShell**

**Dism.exe /Online /Enable-Feature /FeatureName:ServerManager-PSH-Cmdlets**

**Dism.exe /Online /Enable-Feature /FeatureName:BestPractices-PSH-Cmdlets**

* 1. Reboot the computer: **shutdown /r /t 0**
  2. Log back in as administrator
  3. At the command open up a powershell prompt: type in **powershell** and hit <Enter>.
  4. Run the following commands and save a screenshot for your report. The screenshot should be labeled figure 4:
     + Enter the following commands (this also enables WinRM for accepting WinRS commands):
     + **Set-ExecutionPolicy -ExecutionPolicy RemoteSigned**
     + **Configure-SMRemoting.ps1 -force -enable**
  5. You have finished configuring the Windows 2008core Domain Controller.

1. When you are sure everything is working correctly, take note of the IP address; you will need it in the next section

2: Nap server - Windows 2008r2 Enterprise full install

1. Enable ICMP PING in the Firewall

**netsh advfirewall firewall add rule name=”ICMP Allow incoming V4 echo request” protocol=icmpv4:8,any dir=in action=allow**

1. Set the time zone to **(GMT -5:00) Eastern Time (US & Canada)**

**control timedate.cpl**

1. Change the computer name to NAP-lastname

**wmic computersystem where name=”%COMPUTERNAME%” call rename name=”NAP-lastname”**

1. Restart

**shutdown /r /t 0**

1. Enable remote management:
   1. Open an administrative powershell command prompt: Click on **Start 🡪 All Programs 🡪 Accessories 🡪 Windows PowerShell**. Right-click on **Windows PowerShell** and select **Run as administrator**.
   2. Enter the following commands (this also enables WinRM for accepting WinRS commands):

**Set-ExecutionPolicy -ExecutionPolicy RemoteSigned**

Hit Y <enter> when prompted.

**Configure-SMRemoting.ps1 -force -enable**

1. Enable RDP through the firewall.

**Netsh advfirewall firewall set rule group=”Remote Desktop” new enable=yes**

1. Disable IPv6. The following Disables IPv6 for Vista/Windows 7/2008/2008r2 (REF: <http://support.microsoft.com/kb/929852>)
   1. From the command prompt, type in **regedit**
   2. If prompted for User Account Control, click Continue.
   3. Expand HKEY\_LOCAL\_MACHINE 🡪SYSTEM 🡪CurrentControlSet 🡪Services 🡪TCPIP6 🡪Parameters
   4. From the menu Select Edit 🡪 New 🡪 Key 🡪DWORD (32-bit) Value
   5. Name the key **DisabledComponents**
   6. Double click on the new key to edit the value.
   7. In the **Value data:** field, enter **ff**[[2]](#footnote-2).
   8. Click on **OK**
   9. Close the Registry Editor

#### Add the server to the domain

1. Make sure the domain controller you created is turned on.
2. Ping IP address of Domain Controller.
3. Change DNS server to the IP address of the AD server you created.
   1. Run ncpa.cpl to open the network control panel.
   2. Right-click **Local Area Connection** and choose **properties**.
   3. Click on **Internet Protocol Version 4 (TCP/IPv4)** and click on the **Properties** button.
   4. Click on the radio button next to Use the following DNS server address:
   5. Next to **Preferred DNS server:** type in the IP address of your Domain Controller.
   6. Click on OK then Close.
4. Change the computer name to NAP-lastname

**wmic computersystem where name=”%COMPUTERNAME%” call rename name=”NAP-lastname”**

1. Restart

**shutdown /r /t 0**

1. Join the domain you created.
   1. Right-click the computer and select properties.
   2. Under “Computer name, domain, and workgroup settings” click on “Change settings”
   3. In the “System Properties” window, click “change”
   4. Under “Member of” click on the radio button next to “Domain:”
   5. Type in your domain name (for example: 2008core.local).
   6. Enter your administrative user name and password.
   7. Wait
   8. You should be presented with a box saying “Welcome to the xxxx domain”.
   9. Click on “OK”
   10. Restart the computer as directed.

# 3: Windows 7 Client computer

## On the Windows 7 virtual Workstation

1. Make sure networking location is set to “Work”. (If you missed this, look in Network and Sharing Center” in “Network and Internet”, click on the “Customize” link and set to Private. Most importantly, “Network discovery” needs to be enabled.)
2. Strip down GUI for better performance:
   1. Under “Get started with Windows”, click on “View computer details”
   2. At the bottom left, Click “Performance”
   3. In “Performance Information and Tools” Click on “Adjust visual effects” on the menu on the left.
   4. Click on the radio button for “Adjust for best performance”. And click on “Apply”.
   5. Be amazed at how much faster things are now.
3. Make sure the domain controller you created is turned on
4. Ping IP address of AD server
5. Change DNS server to the IP address of the AD server you created.
6. Change the computer name to CLIENT-lastname

**wmic computersystem where name=”%COMPUTERNAME%” call rename name=”CLIENT-lastname”**

1. Restart

**shutdown /r /t 0**

1. Join the domain you created.
   1. Right-click the computer and select properties.
   2. Under “Computer name, domain, and workgroup settings” click on “Change settings”
   3. In the “System Properties” window, click “change”
   4. Under “Member of” click on the radio button next to “Domain:”
   5. Type in your domain name (for example: 2008core.local).
   6. Enter your administrative user name and password.
   7. Wait
   8. You should be presented with a box saying “Welcome to the xxxx domain”.
   9. Click on “OK”
   10. Restart the computer as directed.
2. Logon using your domain admin account.

## 4: 2008r2 CORE File server

1. Generate a new SID

**cd C:\windows\system32\sysprep**

**sysprep /OOBE /Generalize /shutdown**

1. Set the administrator password

**net user administrator \***

1. Disable IPv6. The following Disables IPv6 for Vista/Windows 7/2008/2008r2 (REF: <http://support.microsoft.com/kb/929852>)
   1. From the command prompt, type in **regedit**
   2. If prompted for User Account Control, click Continue.
   3. Expand HKEY\_LOCAL\_MACHINE 🡪SYSTEM 🡪CurrentControlSet 🡪Services 🡪TCPIP6 🡪Parameters
   4. From the menu Select Edit 🡪 New 🡪 Key 🡪DWORD (32-bit) Value
   5. Name the key **DisabledComponents**
   6. Double click on the new key to edit the value.
   7. In the **Value data:** field, enter **ff**[[3]](#footnote-3).
   8. Click on **OK**
   9. Close the Registry Editor

Try running the command **sconfig**; it may help you with some of the below tasks!

1. Enable ICMP PING in the Firewall

**netsh advfirewall firewall add rule name=”ICMP Allow incoming V4 echo request” protocol=icmpv4:8,any dir=in action=allow**

1. Set the time zone to **(GMT -5:00) Eastern Time (US & Canada)**

**control timedate.cpl**

1. Set the DNS address to the IP address of the Domain Controller, where <IP address> is the IP address of the server.

**netsh int ip set dns "Local Area Connection" static <IP address>**

1. Change the computer name to SERVER-lastname

**netdom renamecomputer %computername% /NewName:SERVER-Lastname**

1. Restart

**shutdown /r /t 0**

1. Enable Terminal services

**cd /windows/system32**

**cscript scregedit.wsf /ar 0**

1. Enable remote management: (REF: <http://technet.microsoft.com/en-us/library/dd759202.aspx>)
   1. Install the following features by typing in the below command(s): NetFx2-ServerCore, MicrosoftWindowsPowerShell, ServerManager-PSH-Cmdlets, BestPractices-PSH-Cmdlets
      * You can either enable these features through entering one long command or four separate commands:

This is one long command:

**Dism.exe /Online /Enable-Feature /FeatureName:NetFx2-ServerCore /FeatureName:MicrosoftWindowsPowerShell /FeatureName:ServerManager-PSH-Cmdlets /FeatureName:BestPractices-PSH-Cmdlets**

Or use four separate commands:

**Dism.exe /Online /Enable-Feature /FeatureName:NetFx2-ServerCore**

**Dism.exe /Online /Enable-Feature /FeatureName:MicrosoftWindowsPowerShell**

**Dism.exe /Online /Enable-Feature /FeatureName:ServerManager-PSH-Cmdlets**

**Dism.exe /Online /Enable-Feature /FeatureName:BestPractices-PSH-Cmdlets**

* 1. Reboot the computer: **shutdown /r /t 0**
  2. Log back in as administrator
  3. At the command open up a powershell prompt: type in **powershell** and hit <Enter>.
  4. Run the following commands and save a screenshot for your report. The screenshot should be labeled figure 4:
     + Enter the following commands (this also enables WinRM for accepting WinRS commands):
     + **Set-ExecutionPolicy -ExecutionPolicy RemoteSigned**
     + **Configure-SMRemoting.ps1 -force -enable**

1. Join the domain (note those extra d’s – they’re not a typo!):

**Netdom join SERVER-Lastname /domain:lastname.local /userd:administrator /password:Password1**

1. Reboot

**Shutdown /r /t 0**

1. Check domain membership:

**Netdom verify SERVER-Lastname /Domain:Lastname.local**

1. While KB article tells you to type in ffffffff, this is unnecessary. ff covers all the flags necessary to disable all IPv6 components except the loopback interface. To re-enable IPv6, change this value to 0 and reboot. [↑](#footnote-ref-1)
2. While KB article tells you to type in ffffffff, this is unnecessary. ff covers all the flags necessary to disable all IPv6 components except the loopback interface. To re-enable IPv6, change this value to 0 and reboot. [↑](#footnote-ref-2)
3. While KB article tells you to type in ffffffff, this is unnecessary. ff covers all the flags necessary to disable all IPv6 components except the loopback interface. To re-enable IPv6, change this value to 0 and reboot. [↑](#footnote-ref-3)