Lab 1 – AD on Windows Core

# For this lab

## Discuss:

* What the hardest part of the lab was and why you thought it was hard
* Any problems you had with the lab and what was done to fix the issues (even if the instructor fixed the issue. Pay attention!)
* Improvements you would make to the lab (Two minimum)

## Questions to answer

* What IP did you assign the Active Directory machine?
* What is the FQDN (Fully Qualified Domain Name) of your AD server after you finish installing AD and rebooting?
* Were you successful in recovering a deleted user? What problems were encountered?
* Were you able to get Server Manager working from the Windows 7 computer?

## Figures to include

1. Output of the **ipocnfig/all** command on the AD (core) server
2. Contents of the unattend.txt file (see below. I’m looking for a copy of the text, not actually a screenshot)
3. Commands that add users and make one a Domain Admin
4. The commands that configure and enable remote server management on the Core Domain Controller
5. Message indicating the Windows 7 workstation has been made a member of the domain
6. Active Directory Users and Computers displaying two previously created users
7. The result of the command used to restore a deleted user.

Other things to include

The contents of the unattend.txt file you created in 10-point Currier new font, with paragraph shading of **White, Background 1, Darker 15%** for the contents of the file (See the screenshot for paragraph formatting help and the second paragraph for an example). DO NOT USE A SCREEN SHOT!



**How to shade the contents of the unattend.txt file**

[DCInstall]

ReplicaOrNewDomain=blah

NewDomain=blah.blah

NewDomainDNSName=who.knows

ForestLevel=16

DomainNetbiosName=bob

DomainLevel=4026

SafeModeAdminPassword=lassie

**Example output from unattend.txt file**

**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!**

# Import virtual Machines in VMWARE Lab Manager

log into Virtual lab manager

1. Click on Library
2. Click on the drop-down next to My Library configurations and select **All Library Configurations**
3. Hover over **BTM-618** and select **Clone to Workspace** from the pop-up menu
4. In the clone to Workspace window, under New Configuration, Name, type in **ADonCORE** and click on **OK.**
5. Wait for the machines to finish cloning. (the status indicator will change to – when finished).
6. Click on **Main** on the left menu.
7. Click on the name of the configuration you just created.
8. For each virtual machine, we need to re-create the MAC address. To do this do the following:
	1. Hover over the VM Name and a pop-up menu will display. Select **Properties**.
	2. Scroll down to Network Interfaces. You will see one NIC. Click on the Delete button on the right hand side.



* 1. The NIC will disappear. Click on the **Update** button at the bottom of the screen.
	2. Hover over the VM Name and a pop-up menu will display. Select **Properties**.
	3. Scroll down to Network Interfaces. Click on the **Add Interface** button.
	4. Click on the **Update** button at the bottom of the screen. You now have a different MAC address.
	5. Do this for each virtual machine.
1. Click on **Main** in the left-hand menu bar.
2. Hover over your configuration name and select **Deploy with defaults**.
3. The deployment will take about 5 min.
4. Find your 2008R2Core machine and open the console.

## On the Core machine

Help at: <http://www.windowsnetworking.com/articles_tutorials/Configure-Networking-New-Windows-Core2008-Server-Using-CLI.html>

1. Take a snapshot of the virtual machine. This way you can go back if you mess something up. Think of snapshots like game saves – if you don’t save at important points in the configuration you may have to go way back and do a lot of stuff over again.
2. 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

**netsh firewall set icmpsetting 8**

1. Find the IP address of the local computer

**ipconfig**

1. Set the DNS address to the local IP address, where <IP address> is the IP address of the server you found in the previous step.

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

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

**control timedate.cpl**

1. Enable Terminal services

**cd /windows/system32**

**cscript scregedit.wsf /ar 0**

**cscript scregedit.wsf /cs 0 🡨 enables lower security (optional)**

1. Change the computer name to AIT-Lastname

There are several ways to do this. Here are two:

* **netdom renamecomputer %computername% /NewName:AIT-barker**
* **wmic computersystem where name=”%COMPUTERNAME%” call rename name=”AIT-barker”**
1. Restart

**shutdown /r /t 0**

1. Log back in again
2. Take note of the current networking status for your report:
	1. Run the following command and save a screenshot for your report. The screenshot should be labeled figure 1:

**ipconfig /all**

1. Open notepad.exe and create an unattended setup text file with instructions for setting up a domain. Example file is below.
	1. Your file will differ slightly from this file.
	2. Do NOT use the same NewDomainDNSName as the one listed below.
		* Your NewDomainDNSName should be Lastname.local – for example, cbarker.local).
	3. Make sure to set the forest and domain functional level to 2008r2 (Level 4).
	4. Make sure to also install DNS.
	5. Save the file as C:\unattend.txt. Include the text from this file in your lab report as figure 2:

**[DCInstall]**

**InstallDNS=yes**

**ReplicaOrNewDomain=Domain**

**NewDomain=Forest**

**NewDomainDNSName=XXXXXXX.XXX**

**RebootOnCompletion=yes**

**SafeModeAdminPassword=Password1**

**DomainLevel=4**

**ForestLevel=4**

1. Run unattended AD setup using the unattended answer file. The following command is used to set up the domain using the file you created:

**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, as included above)
2. Once the server restarts, log in and create two user accounts for yourself.
	1. Run the following commands and save a screenshot for your report. The screenshot should be labeled figure 3:
	2. From the CMD prompt, type in:
		* **net user FiresName.LastName yourpassword /add** (ex: net user Cary.Barker Password1 /add)
	3. Create an administrative account: From the CMD prompt, type in:
		* **net user FirstNameØLastName yourpassword /add** (where Ø is a zero).
	4. Add your new account to the “Domain Admins” group for administration:
		* **net group “Domain Admins” FirstNameØLastName /add**
3. 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.

## On the Windows 7 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. Ping IP address of AD server to test connectivity.
4. 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**.
	8. Click on **OK**
	9. Close the Registry Editor
5. Change DNS server to the IP address of the AD server you created in the first part of this lab.
6. Change computer name and join the domain you created.
	1. To change the computer name:
		1. Click on Start, right-click 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 ”Computer name:” enter **Firstname1**. (where Firstname is your first name)
		5. Click on **OK**.
		6. Click on **OK** in the Computer Name /Domain Changes window.
		7. Click on **Close**
		8. Click on **Restart Now**.
		9. Let the computer reboot.
	2. To join the domain
		1. Click on Start, 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: ait618.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”. Take a screenshot of this message and label it figure 5 in your lab report.
		9. Click on **OK**
	3. Restart the computer as directed.
7. Once the computer is back up, hit <Ctrl> + <Alt> + <Ins> (or whatever simulates Ctrl Alt Delete) to get to the password prompt. Click on the **Switch Use**r button.
8. Click on the **Other User** entry on the right.
9. Log in with your domain admin account (the '0' account you created earlier).
10. Install Remote Server Administration Tools on the Windows7 machine.
	1. Log in with the administrative user account you created earlier (FirstName0LastName)
	2. Install the Remote Server Administration tools for Windows 7 x64. The file name to download will be amd64fre\_GRMSATX\_MSU.msu. (http://go.microsoft.com/fwlink/?LinkID=137379) <http://www.microsoft.com/downloads/details.aspx?FamilyID=7d2f6ad7-656b-4313-a005-4e344e43997d&displaylang=en>).
	3. Install the program and follow the prompts. Next, the components must be enabled.
	4. Go into Control Panel.
	5. Click on the “Programs”
	6. Click on “turn windows features on or off” under “Programs and Features” (you’ll need admin rights for this too)
	7. Wait
	8. Find and expand **Remote Server Administration Tools**.
		1. Expand **Feature Administration Tools**. Put a check next to **Group Policy Management Tools** and **Windows System Resource Manager Tools**.
		2. Expand Role Administration Tools 🡪 Active Directory Certificate Services Tools
			1. Put a check next to **Certification Authority Tools**
		3. Expand Role Administration Tools 🡪AD DS and AD LDS Tools
			1. Put a check next to **Active Directory Module for Windows PowerShell**
		4. Expand Role Administration Tools 🡪AD DS and AD LDS Tools 🡪 AD DS Tools
			1. Put a check next to **Active Directory Administrative Center** and **AD DS Snap-ins and Command-line Tools**
		5. Expand Role Administration Tools
			1. Put a check next to **DHCP Server Tools**, **DNS Server Tools** and **Remote Desktop Services Tools**.
		6. Expand File Services Tools
			1. Put a check next to **Distributed File System Tools**, **File server Resource Manager Tools** and **Share and Storage Management Tools**.
		7. Put a check next to **Server Manager.**

****

****

****

**The full list of RSAT features to enable**

* 1. Click on **OK**
	2. Wait more. . . in fact, take a break and come back in 5.
	3. Right-click on the **Start** button, select **Properties**.
	4. Click on the **Customize. . .** button.
	5. Scroll down to the bottom, under “System administrative tools”, click the radio button next to **Display on the All Programs menu**.
	6. Click on **OK** twice to exit.
1. Run the RSAT tools
	1. Go to Start 🡪 All Programs 🡪 Administrative Tools; click on **Active Directory Users and Computers**.
	2. Verify you can see the domain and the user accounts created earlier.
	3. Take a screenshot showing the users in AD users and computers and include it in your lab report as figure 6
2. Attempt to RDP to the CORE server.
	1. Click on Start and type in **mstsc**
	2. Type in the name of your domain controller and click on the **Connect** button
	3. Type in the account information for the '0' domain admin account and click on **OK**.
	4. After a short wait, you will see the console come up to the domain controller
	5. type in **hostname** and hit <enter> . You should see the name of your domain controller
	6. type in **logoff** to exit
3. Use Server Manager to administer the 2008core domain controller
	1. Click on the Start button, select All Programs 🡪 Administrative tools 🡪 Server Manager.
	2. Expand Roles 🡪 Active Directory Domain Services 🡪Active Directory Users and Computers 🡪Users. Verify the accounts created earlier can be seen.
	3. Expand Roles 🡪 DNS Server 🡪 DNS 🡪 DomainControllerName 🡪 Forward Lookup Zones 🡪 YourDomainName. Verify you can see the name of the Domain controller and the client computer under the Records pane.

## Active Directory Recycle Bin

The ability to restore deleted Active Directory objects is a very useful feature that is available with Windows 2008R2 domains. However, the Active Directory Recycle Bin is disabled by default. In order to enable it, the forest must be at the Windows 2008r2 Forest functional level. The AD Recycle Bin must be enabled *before* deleting objects if recovery is desired. To be specific: you can't recover objects that were deleted before the AD Recycle Bin was enabled. Also, once the AD Recycle Bin is enabled it cannot be disabled.

1. Add two users and delete one user on the AD server. The first user should not appear when recovering objects since this step is performed before enabling the AD recycle bin.

**net user Deleteme.1 Password1 /add**

**net user Deleteme.2 Password1 /add**

**net user Deleteme.1 /del**

1. Enable Active Directory powershell components (powershell is assumed to already enabled). Type in the following commands:

**dism.exe /Online /Enable-Feature /FeatureName:** **ActiveDirectory-PowerShell**

**powershell**

**Import-Module ActiveDirectory**

1. Enable the AD Recycle bin. Take a screenshot of the following commands and the result. Include the screenshot in your lab report as figure 7. Type in the following command and reply to the prompts:

**Enable-ADOptionalFeature 'Recycle Bin Feature'**

* 1. When asked for scope, type in **ForestOrConfigurationSet**
	2. When asked for target, type in the name of your domain.
	3. On the confirmation dialog box, type in **y**
1. Search for the Deleteme user in both active objects and deleted objects

**Get-ADObject -f 'name -like "Del\*"'** - search 'Del'

**Get-ADObject -f 'name -like "Del\*"' -SearchScope subtree -IncludeDeletedObjects**

1. Go into the Windows 7 management machine and open Active Directory Users and Computers. Select the Users container to verify the one user appears.
2. Delete the other user, either through Active Directory Users and Computers, or from the command line on the AD Core server:

**net user Deleteme.2 /del**

1. Go into the Windows 7 management machine and open Active Directory Users and Computers. Select the Users container to verify the user is gone.
2. On the AD Core server search for the deleted user. Note that the user appears when searching the AD Recycle bin:

**Get-ADObject -f 'name -like "Del\*"'** - search 'Del'

**Get-ADObject -f 'name -like "Del\*"' -SearchScope subtree -IncludeDeletedObjects** - search for deleted 'Del'

1. Restore the user from the AD Recycle Bin
	1. To copy the GUID for the deleted item you want to restore: Right-click in the cmd window and select mark. Use the mouse to click and highlight over the ObjectGUID of the deleted object you want to restore and hit <Enter>.
	2. To paste the GIUD number, type in the command **Restore-ADObject** then right-click in the cmd window and select paste. the format of the command is:

**Restore-ADObject biglongGUIDnumber**

Take a screenshot of the command and the result and include it in your lab report as figure 8

LAB 1 Evaluation Criteria

NAME: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |  |
| --- | --- | --- | --- |
| COMPONENT | POINTS | POINTS EARNED | COMMENTS |
| **Overall look and feel** |
| **Title Page** | 3 |  | Title page neat, clean, includes lab # and lab title, Student’s name, date, e-mail address, class and section number are included. |
| **Table of Contents** | 2 |  |  |
| **Executive Summary** | 5 |  |  |
| **Professional Appearance** | 5 |  | Professional overall look, font etc – readability spelling and grammar |
| **Header** | 2 |  | – Lab Title |
| **Footer**  | 2 |  | – page, course # and student name |
| **Section Headings** | 2 |  |  |
| **Numbered & Labeled Figures** | 2 |  | Tables, Diagrams, Screenshots etc labeled and numbered |
| **Numbered Pages** | 2 |  |  |
| **Content** |
| **Body Content** | 5 |  | Clear and well organized point by point description of the actions takenEach component should have its own section. |
| **Tables/Diagrams** | 5 |  | Any tables and diagrams in 10-point Currier new font, with paragraph shading of White, Background 1, Darker 15% ***. A description must follow each table or diagram, detailing what was going on and why.*** |
| **System Configuration/Reports** |
| **Proper function of** **Windows Vista****Windows 2008** | 10 |  | The following configuration is in place:System is functioning as it should at the end of the lab – Windows 7 can manage the Windows 2008r2 CORE Domain controller (keep in mind that some labs may be designed to break something and/or make it not work like you would expect) |
| **Questions/Discussion addresses issues brought up in the Lab** | 15 |  | Systems are properly configured:* Screenshots included
* AD installed correctly
* Accounts created successfully and configured with proper rights
* IP address set properly
* Computers renamed properly
* AD restore functioning
 |
| **Total:** | 60 |  |  |

# Misc commands (not needed in this lab. They are presented for completeness):

## Updates and activation on Core server

Enable system updates:

cd C:\windows\system32

cscript scregedit.wsf /AU /v

cscript scregedit.wsf /AU 4

Server activation (p335-336 guide)

cscript slmgr.vbs –xpr

cscript slmgr.vbs -ato

Set an IP address

1. Set static IP address

**netsh int ipv4 set addr name="Local Area Connection" static <Assigned IP> <SubnetMask> <DefaultRoute>**

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)