**CSI3670**

**Winter 2019**

**Lab 3: ADDS and PowerShell**

**Synopsis:**

In this lab, you will be installing both Active Directory Domain Services (Windows) and playing around with PowerShell. You’ll also install and remove Hyper-V as shown in class

**Note that Google Cloud will be your playground, and the school VMWare server will be your production environment.**

You will need your Windows password for authentication later, so ensure you have either changed or stored the randomly generated one from Google somewhere!

**Windows – Active Directory Domain Services (AD DS) Installation**

We are going to all become domain administrators. In your Google Cloud Windows VM:

**1) Login to your virtual machine’s Windows partition**

In the Server Manager, click ‘Add Roles and Features.’ Click through, leaving the settings as default (Role-based, your machine out of the server pool, etc.).

Select Active Directory Domain Services out of the list, and click ‘Add Features’ from the popup to install all required features. Click through more until you get to ‘Install’ and let it go.

We will all be domain controllers for the learning experience of it. First, however, you need to set the Administrator password. If you don't do this, the promotion to DC will fail!

Open up Powershell with administrative privileges and type the following:

net user

You should see all the users on the machine. Now type:

net user Administrator \*

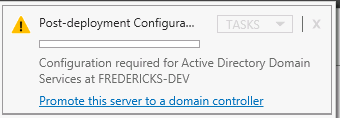
You'll be asked to set a password. For this, use **Temp12345** (obviously you'd use something stronger in a real environment).

If you don't do this, the prerequisites check in the AD DS server promotion will fail, as the Administrator account on a fresh install doesn't have a password.

Time to promote your machine to be a DC. Click this:

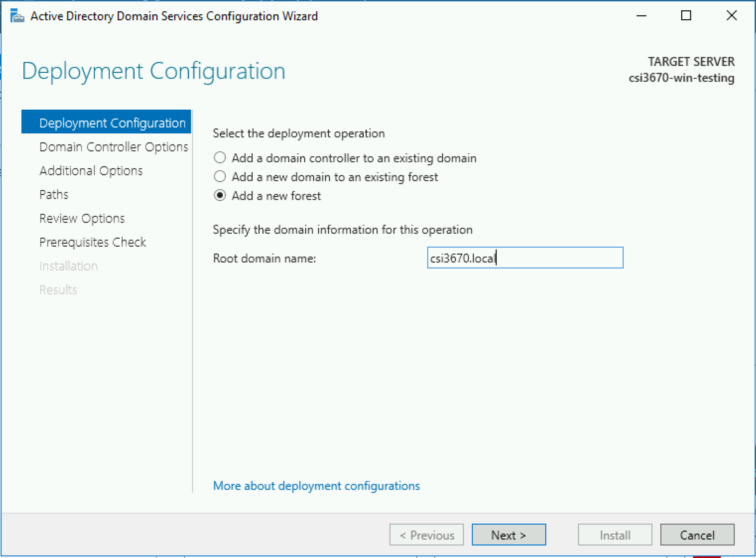
****

And then this:

****

Click Promote this server to a domain controller and let’s continue.

You will now create your own forest. Name it **csi3670.local.**



Moving forward give it a domain services recovery password of **Temp12345**.

Click Next until you get to the NetBIOS domain name. Verify that it seems correct and click next.

Take a screenshot of this step and paste it in Q1.

Hit next until you get to actual installation, then click Install. If your prerequisites check failed, make sure you set the Administrator password.

**2) PowerShell fun with AD!**

Create a file, called Names.txt, on the Desktop

Put in a few names in the following format (we’ll be reading it in as CSV):

UserName, LastName, FirstName

User1, User, 1

User2, User, 2

fredericks, Fredericks, Erik

ma, Ma, Rui

Let’s use PowerShell ISE. Open that up as an Administrator. In the console, move over to the Desktop, as that’s where you stored the file (this bash-like command will auto-expand to Windows-format):

cd ~\Desktop

Create your first script...call it <your-last-name>.lab2.ps1

# Lab 3 – AD PowerShell Basics

# Name: <your name>

# Date: <the date>

# Description: <overview of this script when you’re done>

$users = import-csv Names.txt

write-output $users

You should see a nice list of your text file.

Now, replace write-output with the following code:

foreach ($user in $users)

{

Write-Host -fore yellow $user.FirstName"" $user.LastName" : " $user.UserName

}

Take a screenshot of the output and put it in Q1:

Now, change the above code and Names.txt file to include a Street Address. Add the user’s street address to the Write-Host line of code and take another screenshot, placing it in Q1.

Go back to the Server Manager → Tools → Active Directory Users and Computers (ADUC). Go to View on the menu bar and check ‘Advanced Features.’

Right click on your domain (should be csi3670.local) and click Properties. On the Attribute Editor tab, scroll down to find the distinguishedName field. Take note of what it is. For reference, mine would be *DC=csi3670,DC=local*

Write your distinguished name in Q3.

Now, add the following code to your script file:

Import-Module ActiveDirectory

foreach ($user in $users)

{

$ou = "CN=Users,DC=cit349,DC=local"

$pw = "Temp12345"

$detailed\_name = $user.FirstName + " " + $user.LastName

$firstletter\_first\_name = $user.FirstName.Substring(0,1)

$SAM = $firstletter\_first\_name + $user.LastName

# This must all be on a single line!

New-AdUser -Name $SAM -SamAccountName $SAM -UserPrincipalName $SAM -DisplayName $detailed\_name -GivenName $user.FirstName -Surname $user.LastName -AccountPassword (ConvertTo-SecureString $pw -AsPlainText -Force) -Enabled $true -Path $ou -WhatIf

}

Describe briefly what happened in Q4.

Now, remove the -WhatIf flag. Run it again. On the ADUC screen, show me that the users were added with a screenshot. You will most likely need to refresh the screen.

Right click on one of the users and take a screenshot of the General tab, pasting it into Q1.

Let’s check the attributes we created for one of the users. In the PowerShell console (not your script file), run:

PS> Get-ADUser efredericks -Properties memberof

Copy and paste the output below into Q5. What does this mean?

Hopefully you noticed I’m not a member of anything other than Domain Users. This needs to be rectified. Right click on my username, properties, Member Of tab, Add, and add Administrators to the ‘Enter the object names to select’ box. Click Check Names when you’ve added it (it should underline). Do the same for your TA’s account (rma).

Run the above command again. It should note I’m an administrator now. Copy and paste that output into Q6.

Lastly, let’s assign some quotas. We don’t want our other users needlessly borking our server.

In the PowerShell prompt:

PS> Install-WindowsFeature -Name FS-Resource-Manager -IncludeManagementTools

Go back into the Server Manager and click on File and Storage Services. Click on Shares. On the bottom right there’s a window that says ‘Quota.’ Click on the ‘To set a quota...’ link. Take a screenshot of the window that appears and paste it into Q1. We’re not going to set a quota right now, but we can in the future as we iterate our AD setup.

**Hyper-V installation**

Open up the slides from the Hyper-V / ESX lecture. Follow through the steps to install Hyper-V. When you’re done, take a screenshot of Hyper-V being installed and paste into Q1.

Go into the Hyper-V management tools (hint, check under the Tools menu...as with...all other things we’ve done here). Add a new virtual machine (but limit the hard drive size to 10GB). Take a screenshot of it after it has been created and paste into Q1.

Now, follow the steps to remove Hyper-V as it is effectively useless to us. Take a screenshot of the Server Manager without Hyper-V available and paste into Q1.

**Homework**

1) Ensure you’ve taken all required screenshots and put them where requested throughout the lab manual.

2) What is the purpose of having multiple domain controllers per domain? In more detail, explain what Active Directory does between domain controllers within a domain ?

3) What is your server's distinguished name?

**DC=csi3670,DC=local**

4) Describe your PowerShell script output.

**The script created new users based on the parameters of the Names.txt file and the variables created and assigned in the script that were passed to the New-AdUser command line. This line was either creating new Admin users or just creating New Users onto the system or domain. The WhatIf flag displayed what the script is currently doing in the New-AdUser command.**

5) What is the purpose of the command run in the lab (Get-ADUser efredericks -Properties memberof)

**PS C:\Users\oulefevref\Desktop> Get-ADUser efredericks -Properties memberof**

**DistinguishedName : CN=EFredericks,CN=Users,DC=csi3670,DC=local**

**Enabled : True**

**GivenName : Erik**

**MemberOf : {}**

**Name : EFredericks**

**ObjectClass : user**

**ObjectGUID : 8ddc5352-b448-4947-900b-ab27c69be490**

**SamAccountName : EFredericks**

**SID : S-1-5-21-1593496284-243477520-438830787-1107**

**Surname : Fredericks**

**UserPrincipalName : EFredericks**

**Display the information and parameters of the User “efredericks”.**

6) Output of the Get-ADUser second run.

**PS C:\Users\oulefevref\Desktop> Get-ADUser efredericks -Properties memberof**

**DistinguishedName : CN=EFredericks,CN=Users,DC=csi3670,DC=local**

**Enabled : True**

**GivenName : Erik**

**MemberOf : {CN=Administrators,CN=Builtin,DC=csi3670,DC=local}**

**Name : EFredericks**

**ObjectClass : user**

**ObjectGUID : 8ddc5352-b448-4947-900b-ab27c69be490**

**SamAccountName : EFredericks**

**SID : S-1-5-21-1593496284-243477520-438830787-1107**

**Surname : Fredericks**

**UserPrincipalName : EFredericks**

7) Why can’t we run a hypervisor within a hypervisor?

8) Assume we’re actually going to create a real environment. Modify the New-ADUser cmdlet from the script above to include a **Street Address, Phone Number, Email Address, Job Title, and membership in the Administrators group**. Note that ‘clicking the GUI’ is not an acceptable answer → it must be a full PowerShell command. To test it, you can either delete the users you've created in ADUC or you can change the usernames to be distinct.

**Extra credit**) With a partner, try to add each other's machines to your Active Directory listing. To do this, you'll need to look into VPC networks, add each other to your GCP projects, etc. Describe the process you took to do it and show me screenshots of your machines in each others' server listing.

Zip up your script and Names.txt file and submit it along with this handout. I’ll be checking your comment block as well, so make sure that you’ve updated it appropriately. Points will be lost if I see any boilerplate text (<your name> for instance)