**CSI3670**

**Winter 2021**

**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.

**Note that Google Cloud will be your playground, and the school VMWare server will be your production environment. Do everything on your Google Cloud instance for this lab!**

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 – Setup**

Open up Windows Server. Open the Server Manager if it’s not already open. Click the “Add roles and features” link. If the “Before you Begin” page pops up, click “Next.” Under Installation Type, choose “role-based for feature-based installation” and click “Next.” Under “Server Selection, choose “Select a server from the server pool” and choose your windows VM. Click “Next.” Under “Server Roles,” click the checkbox next to “Web Server (IIS).” The “Include management tools (if applicable)” box should be checked. Click “Add Features” and then “Next.” Click “Next” three more times, then click “Install.”

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

We are going to all become domain administrators. Once again, 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. Set it to be something you'll remember, as I won't have access to fix it for you if you forget.

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

Time to promote your machine to be a DC. In the Server Manager Dashboard, click this:

****

And then this:

Graphical user interface, text, application

Description automatically generated

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

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

Graphical user interface, text, application

Description automatically generated

On the next page, leave everything as default and give it a domain services recovery password, again something you'll remember.

Click Next until you get to the NetBIOS domain name. Verify that it seems correct (for mine, CSI3670).

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 text file in Notepad, called Names, 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

bowers,Bowers,Kate

kakarala,Kakarala,Navya

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 in Notepad...call it <your-last-name>.lab3.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 of the output, 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, copy and paste the following into your script file:

Import-Module ActiveDirectory

$users = import-csv Names.txt

foreach ($user in $users)

{

$ou = "CN=Users,DC=csi3670,DC=local"

$pw = "Ch@ng3M31mm3d1@t3ly"

$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, click Properties, 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 kbowers -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. In the ADUC window, 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). Click Okay, then Apply, and Okay again. Do the same for your TA’s account (nkakarala).

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.

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 your Server Manager Dashboard that shows that Hyper-V is installed and paste into Q1.

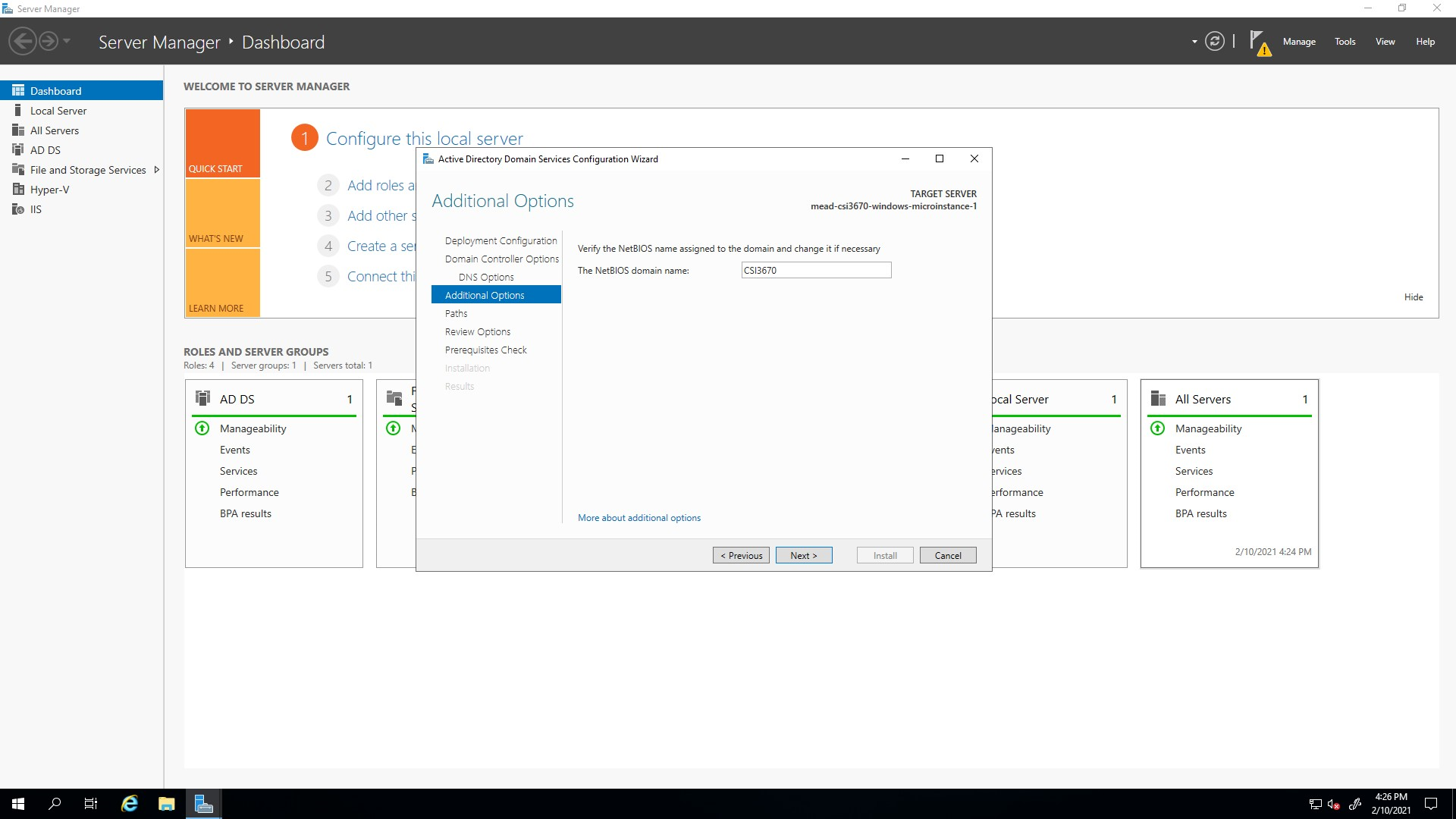
Go into the Hyper-V management tools (hint, check under the Tools menu...as with...all other things we’ve done here). Add a new virtual machine, leaving the default options (but limit the hard drive size to 10GB). Take a screenshot of it in the Hyper-V Manager after it has been created and paste into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

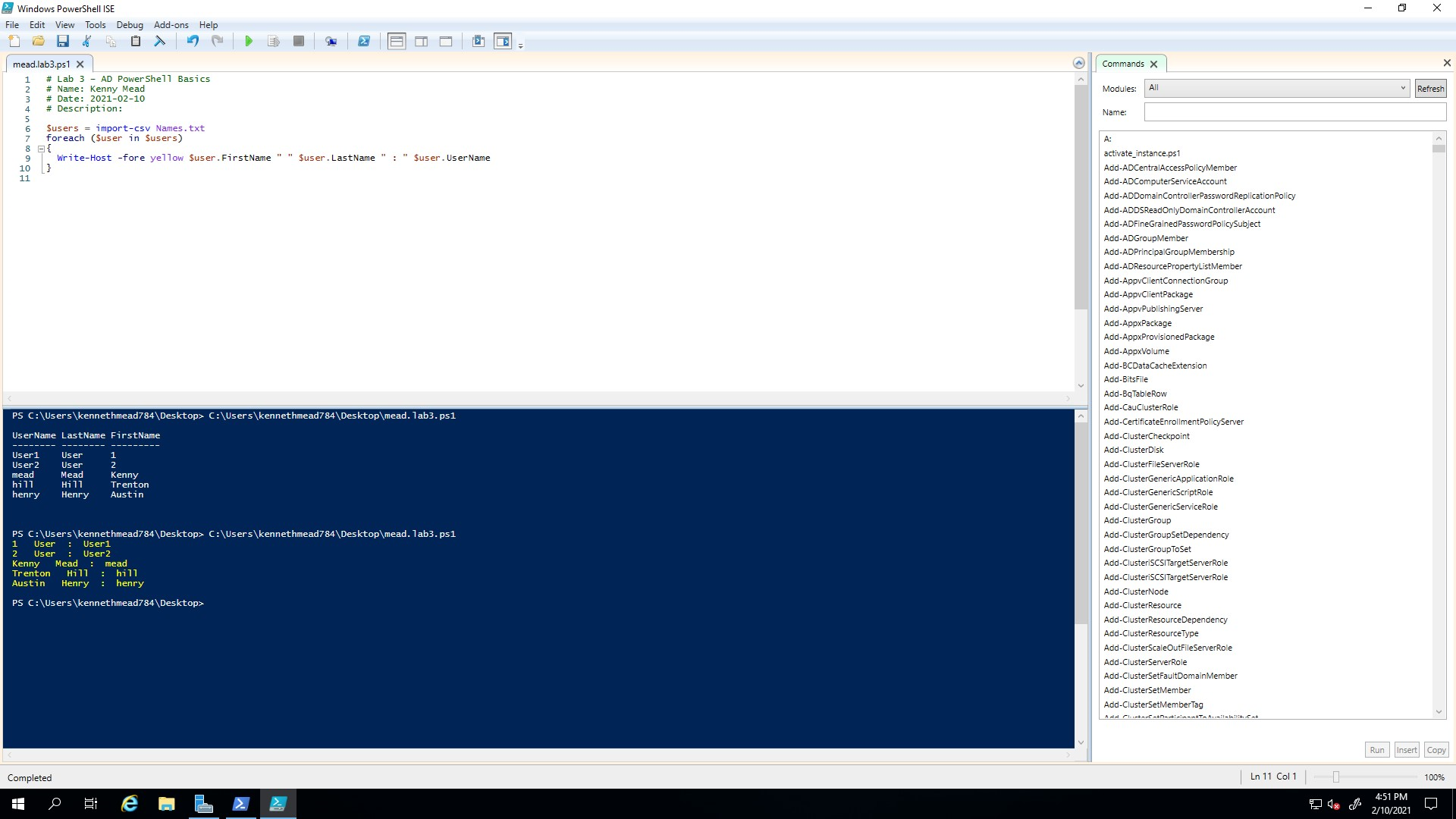
Delete the VM. Take a screenshot of the Hyper-V Manager after it has been deleted.

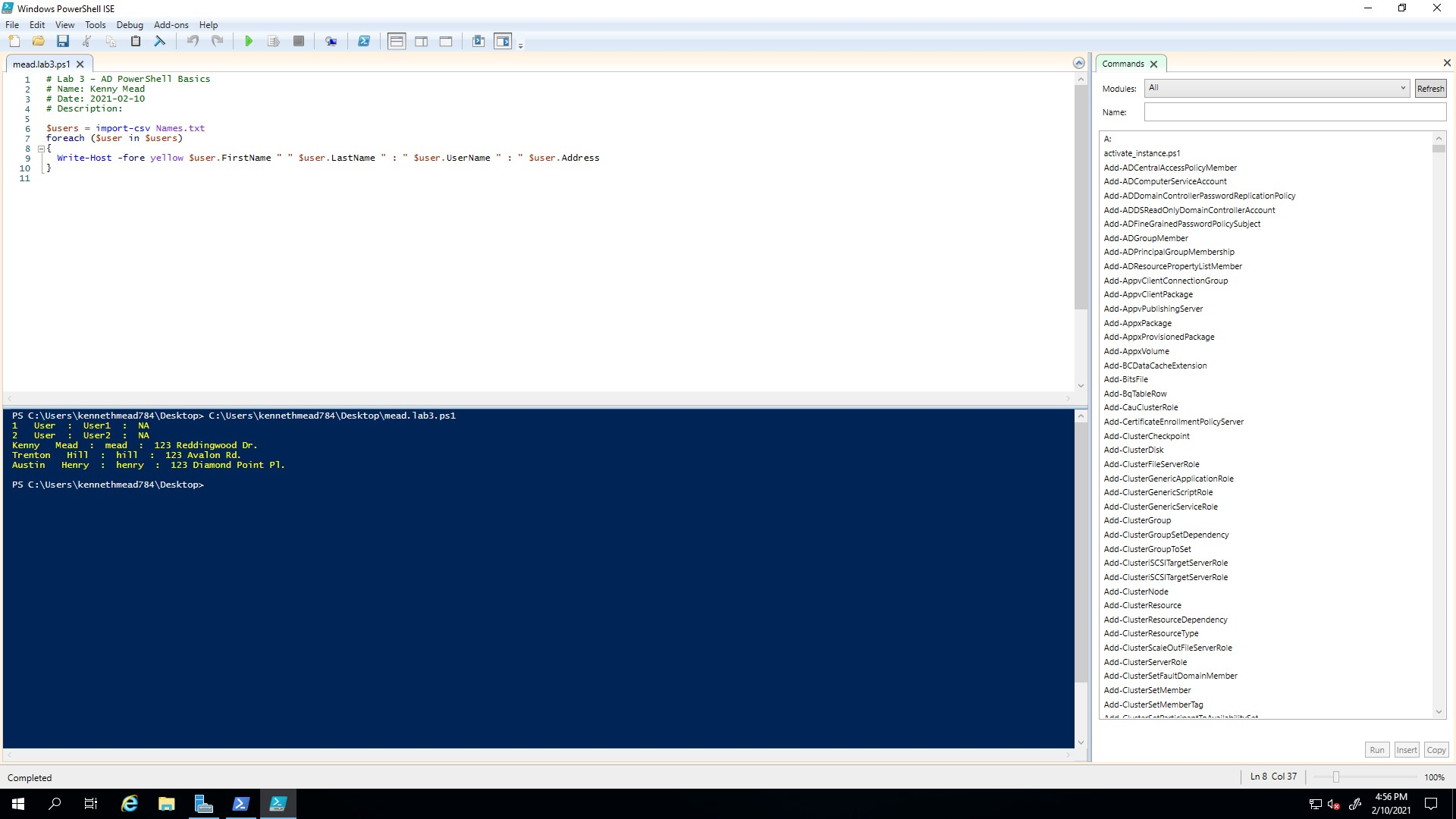
Now, follow the steps to remove Hyper-V as it is effectively useless to us. See the slides from the Hyper-V / ESX lecture. Take a screenshot of the Server Manager without Hyper-V available and paste into Q1.

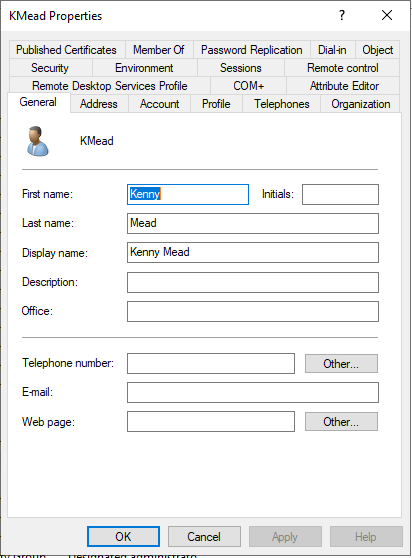
**Homework**

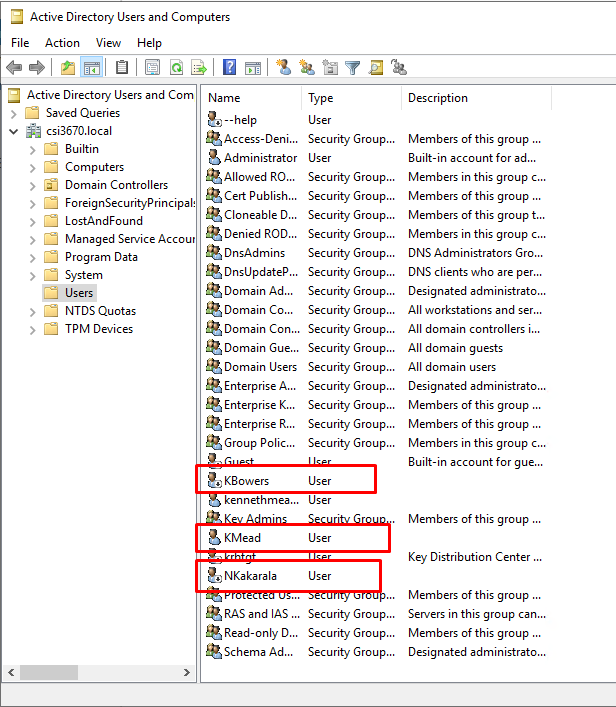
1) Ensure you’ve taken all required screenshots and put them where requested throughout the lab manual.

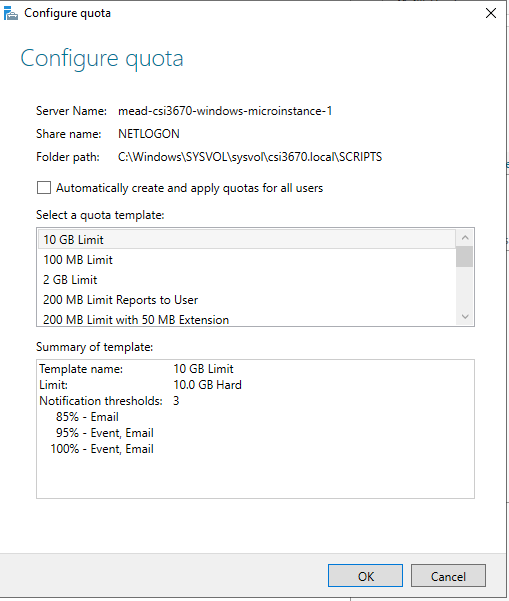


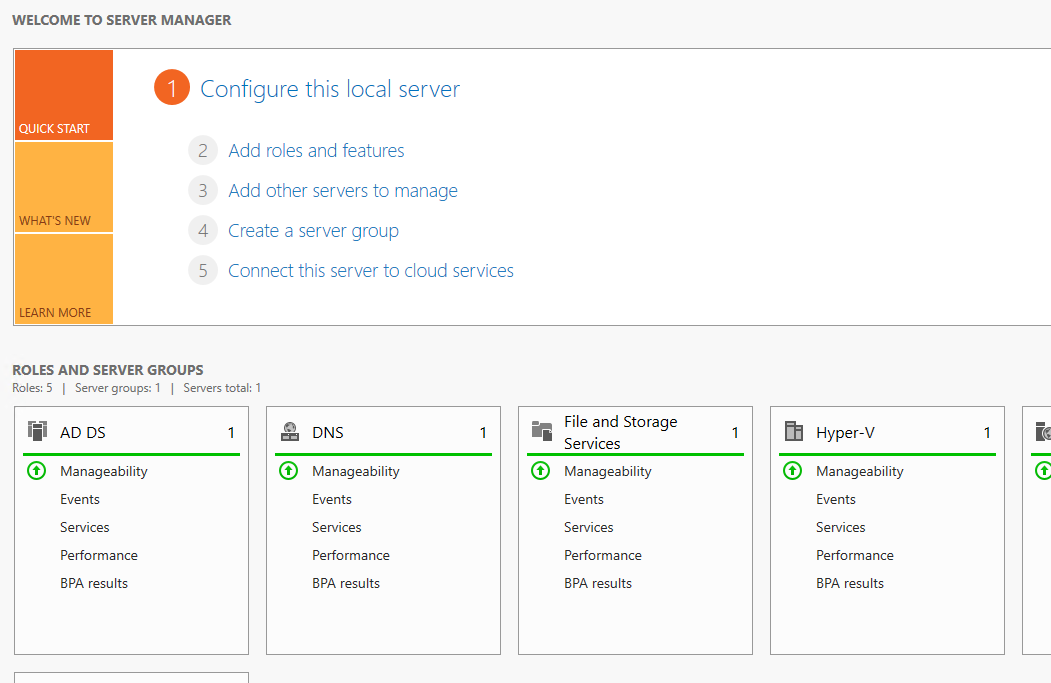


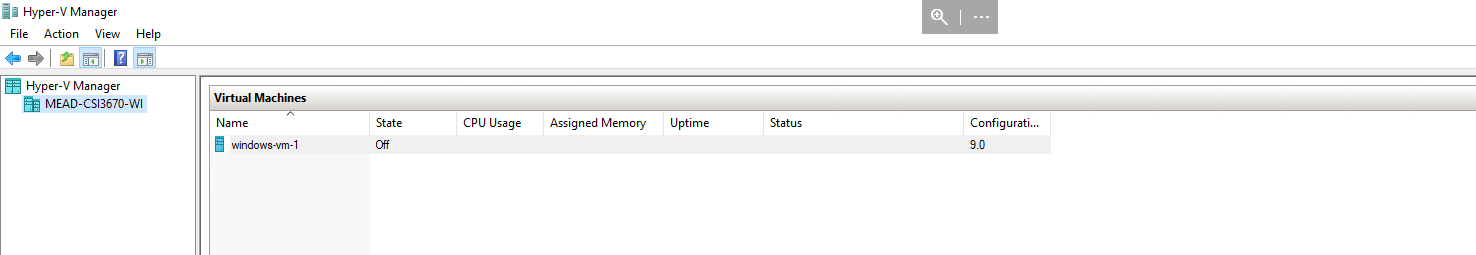


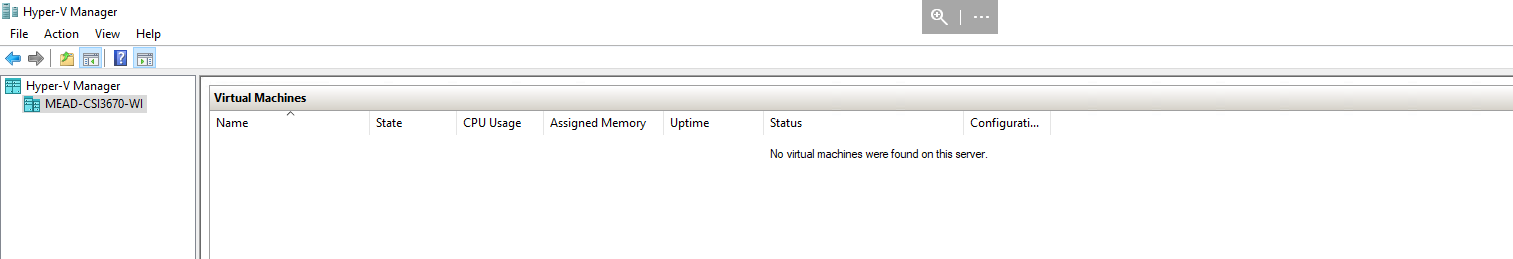


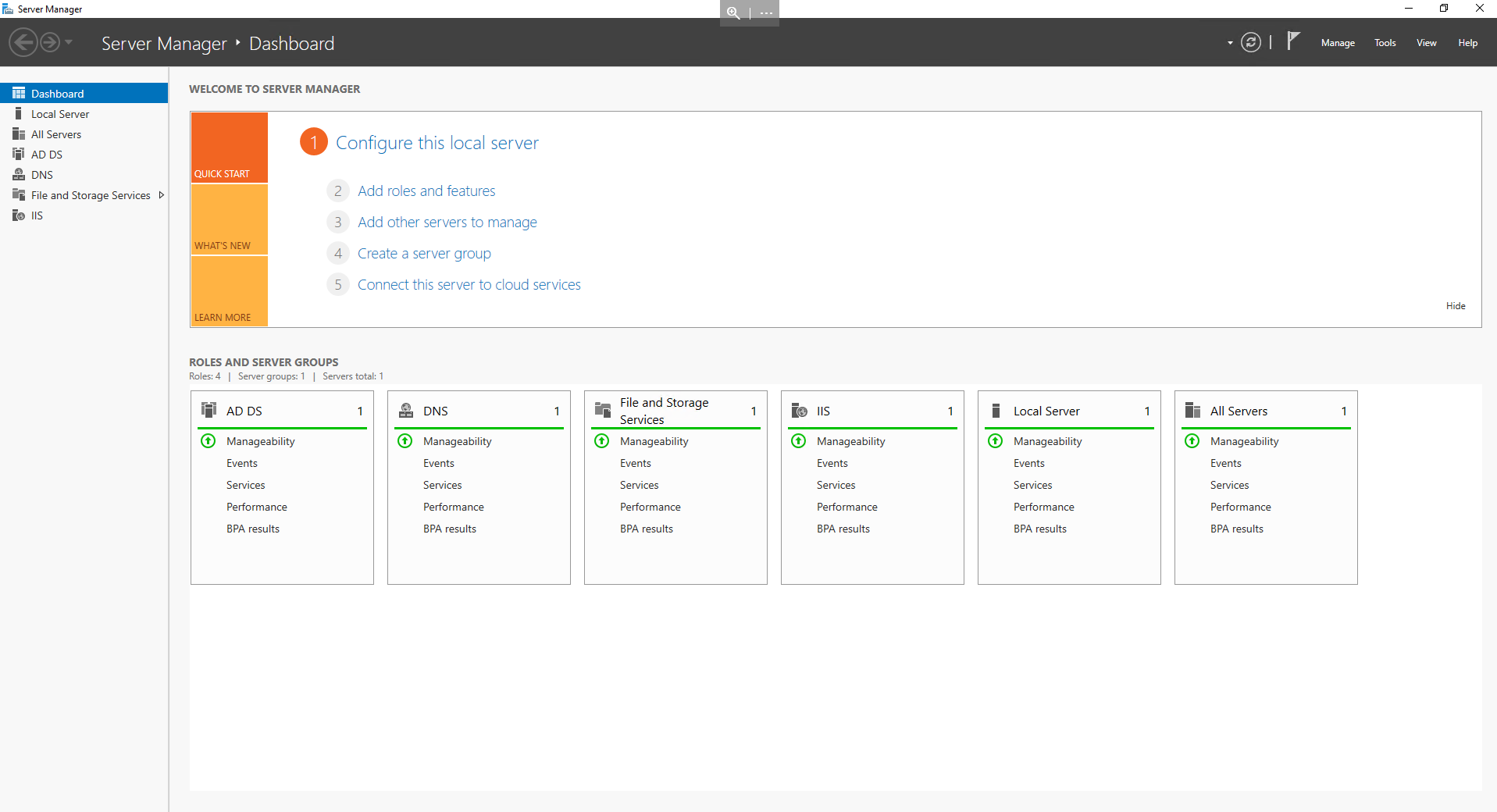












2) What is the purpose of having multiple domain controllers per domain? In more detail, explain what Active Directory does between domain controllers within a domain ?

Having more domain controllers means more potential up-time. Active directory uses domain controllers to authenticate users when they try to access domains.

3) What is your server's distinguished name?



4) Describe your PowerShell script output.

We mimicked what would happen if we added all the users listed in Names.txt to our active directory

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

PS C:\Users\kennethmead784\Desktop> Get-ADUser kmead -Properties memberof

DistinguishedName : CN=KMead,CN=Users,DC=csi3670,DC=local

Enabled : True

GivenName : Kenny

MemberOf : {}

Name : KMead

ObjectClass : user

ObjectGUID : c7abbba5-2941-4b7a-b843-0502be1df781

SamAccountName : KMead

SID : S-1-5-21-4255634468-3836234807-1043330837-1106

Surname : Mead

UserPrincipalName : KMead

I am currently not a member of anything

6) Output of the Get-ADUser second run.

PS C:\Users\kennethmead784\Desktop> Get-ADUser kmead -Properties memberof

DistinguishedName : CN=KMead,CN=Users,DC=csi3670,DC=local

Enabled : True

GivenName : Kenny

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

Name : KMead

ObjectClass : user

ObjectGUID : c7abbba5-2941-4b7a-b843-0502be1df781

SamAccountName : KMead

SID : S-1-5-21-4255634468-3836234807-1043330837-1106

Surname : Mead

UserPrincipalName : KMead

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

It is possible to run bare-metals hypervisors inside of a hypervisor, but not possible to run paravirtual hypervisors inside of each other. This is because paravirtual hypervisors look at physical hardware and allow access to its VM’s through an API.

Requires hardware

Requires hardware

Produces

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.

9) 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)