Introduction

In this Lab, I'll be demonstrating how to set up and deploy active directory services with Microsoft Windows Server 2019. The setup will involve domain active directory domain services deployment, remote access and network address translation deployment, DHCP and router services deployment. We will also register the server as a domain controller. Prior to the following instructions, one virtual machine was created running Microsoft Windows Sever 2019 Standard (GUI) with two virtual NICs, one for internal communication with domain clients, and one for NAT connection to our home router which clients can use to connect to the internet through. The server was renamed to Domain controller, the ethernet connections were renamed in network settings as it applies, the internal NIC was configured with the below network details. To test our deployment, a Windows 10 Pro virtual machine will act as a client with one internal connection to the server NIC. Below is a visual representation of the overview of the project and the setup *Figure 1*.

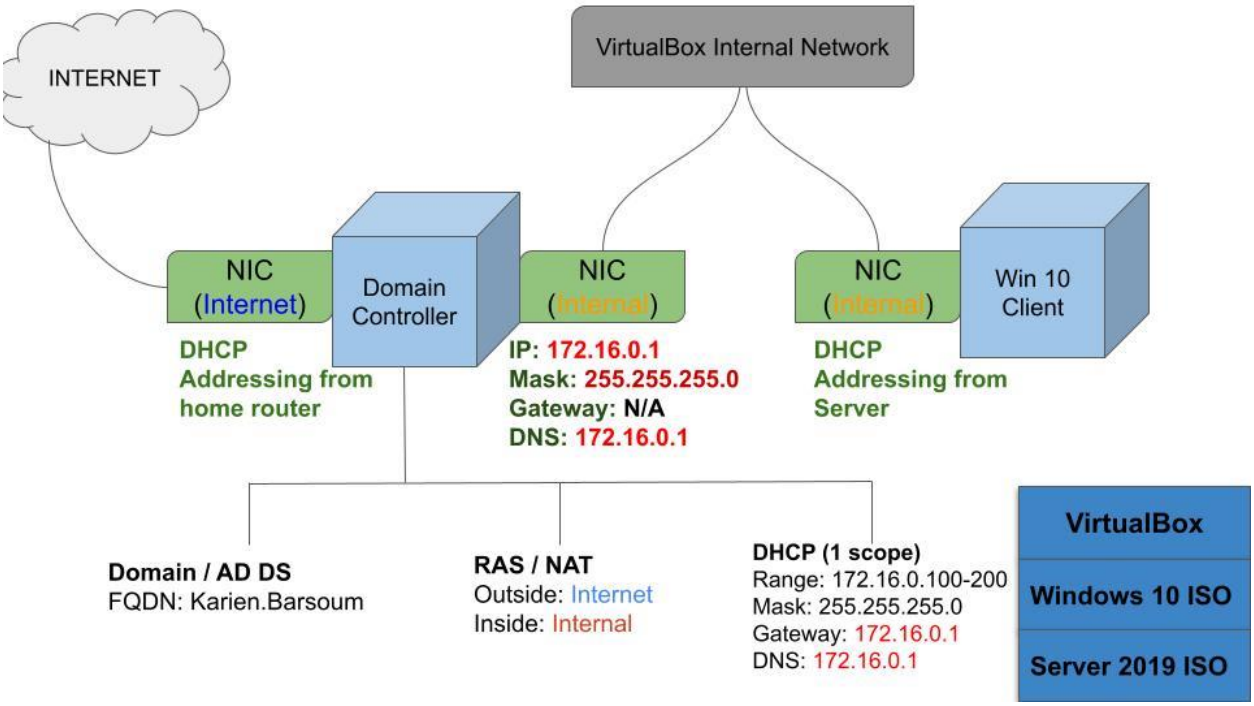


Figure 1

Installing Active Directory Domain Services

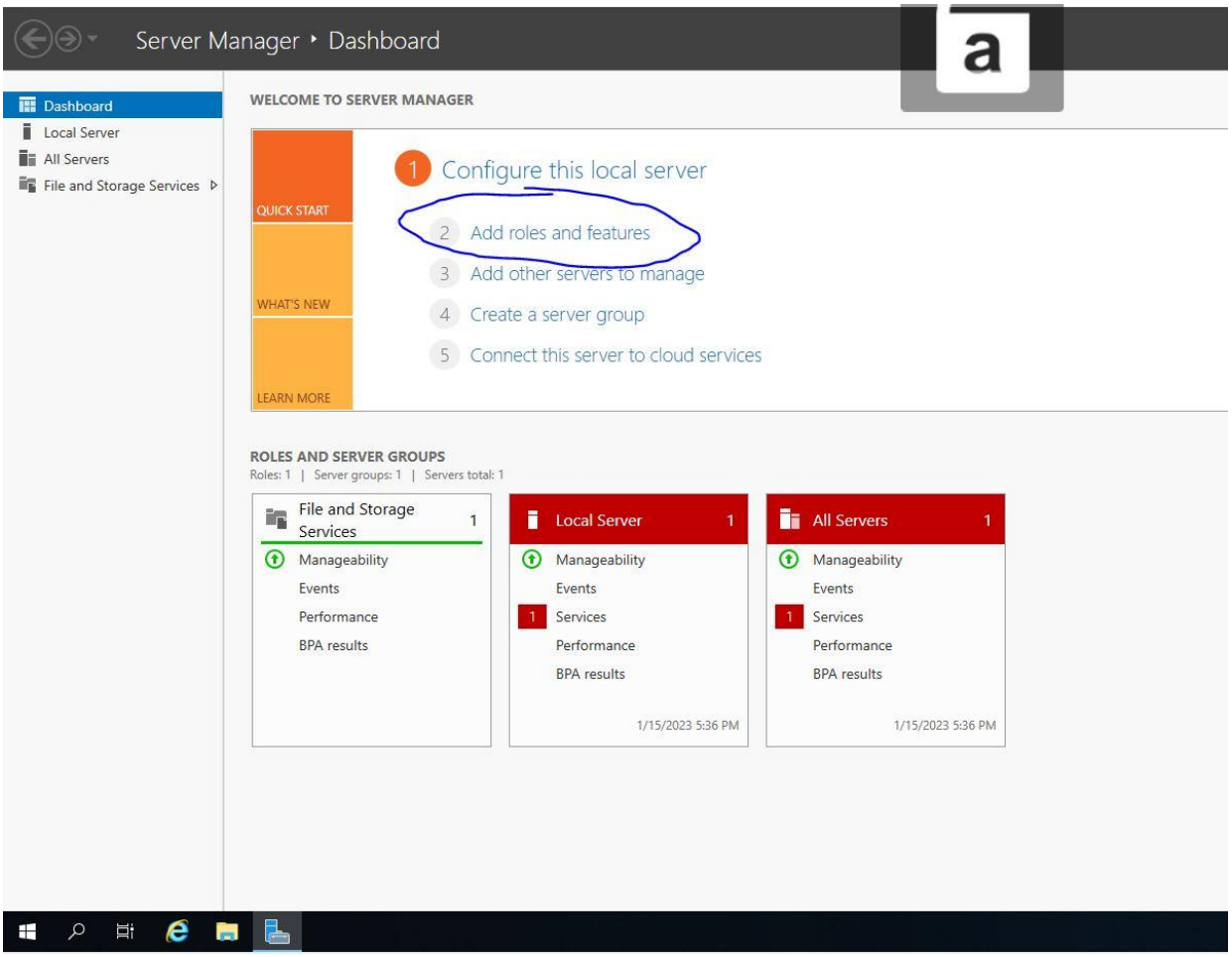


Figure 2

With Server Manager open, click on add roles and features *Figure 2*. Click next on “Before You Begin” and “Installation Type”. On the “Server Selection” page, you will see that the only server available to install AD DS is the one we created, and it’s selected by default. Now click next. On the “Server Roles” page, choose Active Directory Domain Services and confirm Add Features. Click Next on “Features”, “AS DS”, and click Install *Figure 3*. This may take a while.

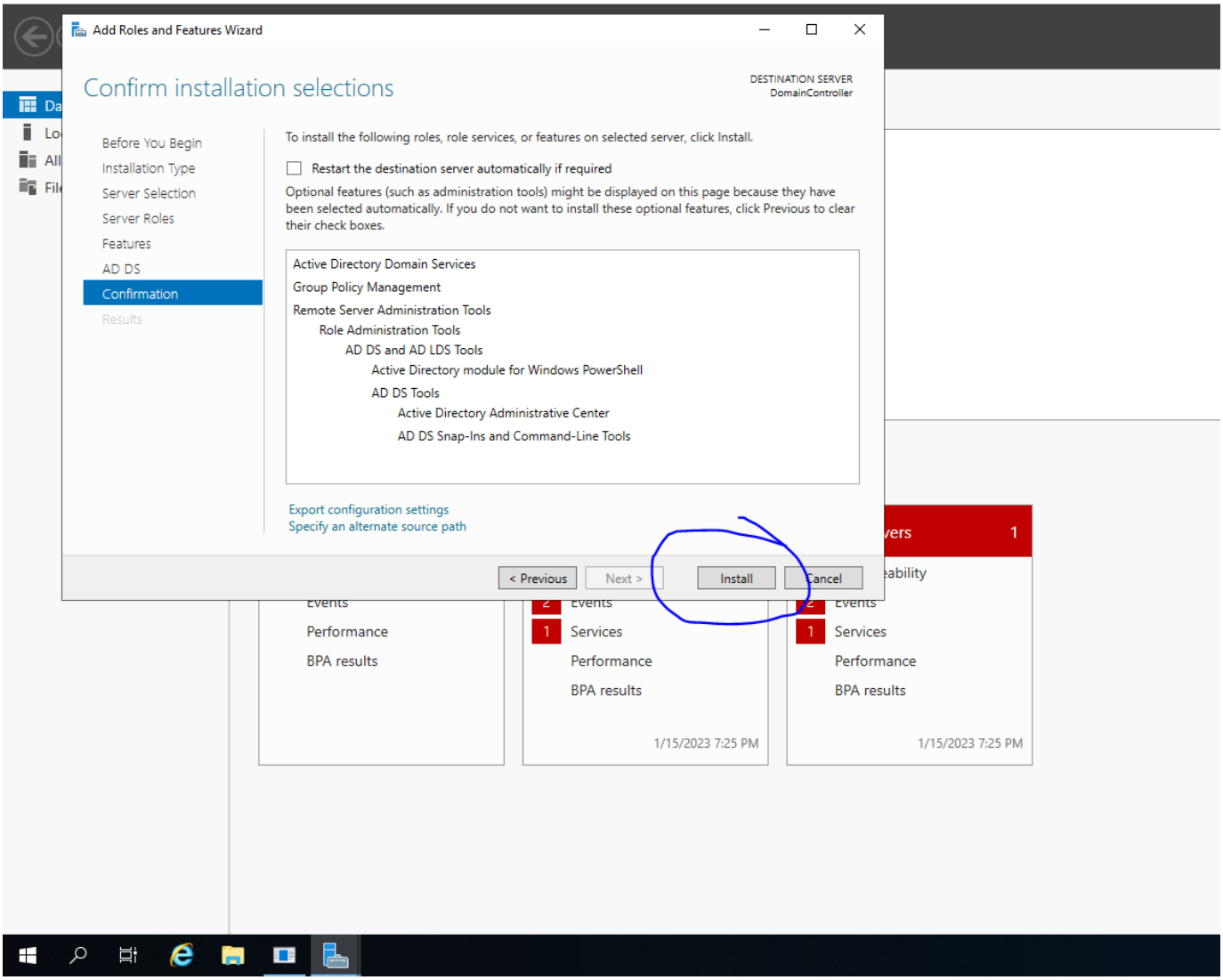

Add Roles and Features Wizard
Confirm installation selections
DESTINATION SERVER
DomainController
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
Confirmation
Results
To install the following roles, role services, or features on selected server, click Install.
Restart 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.
Active Directory Domain Services
Group Policy Management
Remote Server Administration Tools
Role Administration Tools
AD DS and AD LDS Tools
Active Directory module for Windows PowerShell
AD DS Tools
Active Directory Administrative Center
AD DS Snap-Ins and Command-Line Tools
Export configuration settings
Specify an alternate source path
< Previous
Next >
Install
Cancel
Events
Performance
BPA results
Services
Performance
BPA results
1/15/2023 7:25 PM
Services
Performance
BPA results
1/15/2023 7:25 PM

Figure 3

After it is finished installing, you will notice a yellow flag on the top right giving you a notification. Click on it and then choose “Promote this server to a domain controller”. This is how you create the domain. On the “Deployment Configuration” screen, choose add new forest since this domain is brand new and not associated with any prior registered forest. Create your root domain name. I will name mine Karien.Barsoum but you can name it whatever you like (ex. Mynewdomain.com). Click next and add your own DSRM password and confirm it. Click next and next on “Additional Options”, “Paths”, and “Review Options”. Choose Install on “Prerequisites Check” *Figure 4*. You will automatically need to restart your machine. When logging in again, you will notice that your built-in admin account has acquired your domain name.

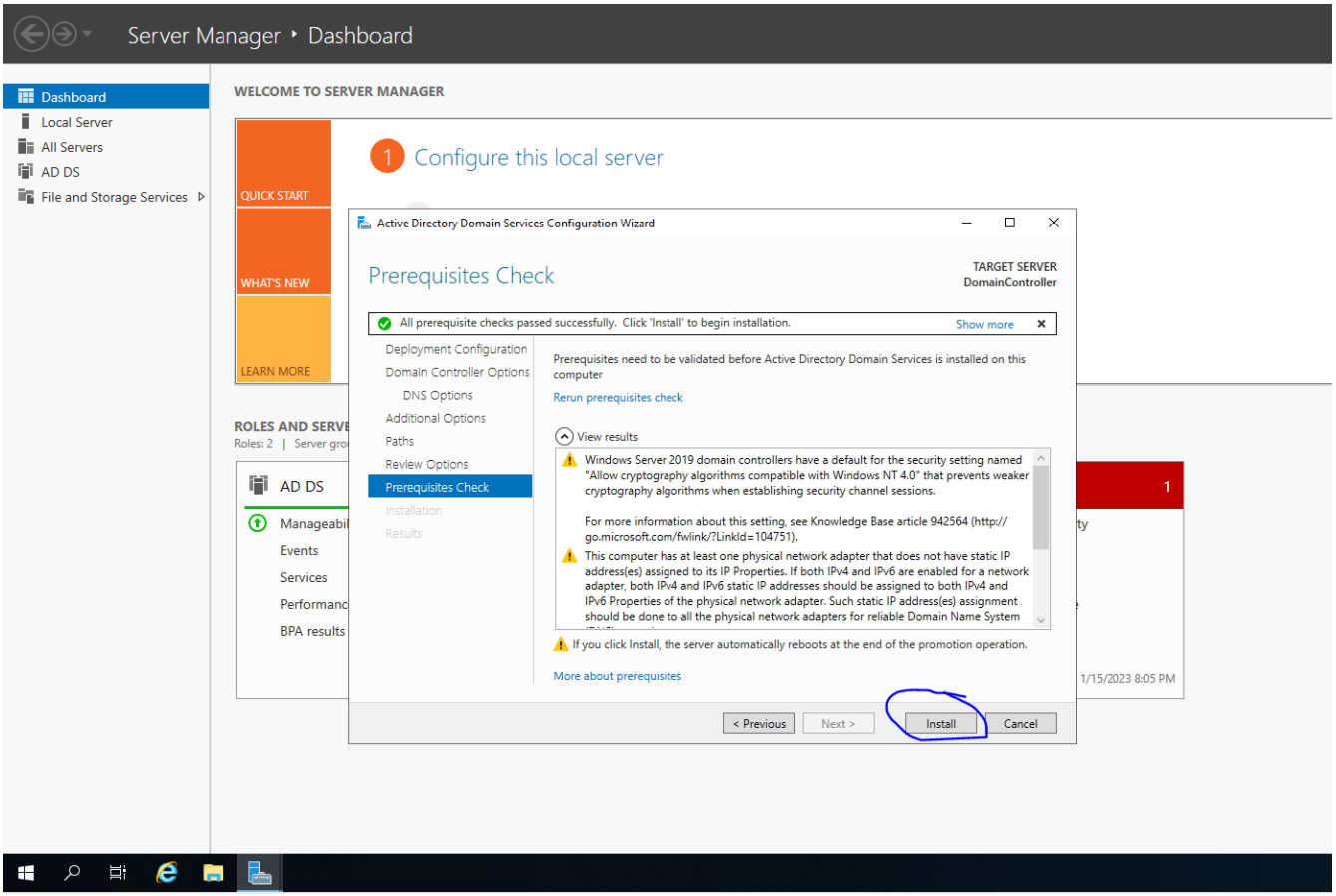


Figure 4

Creating OU, creating user, adding a Domain Admin

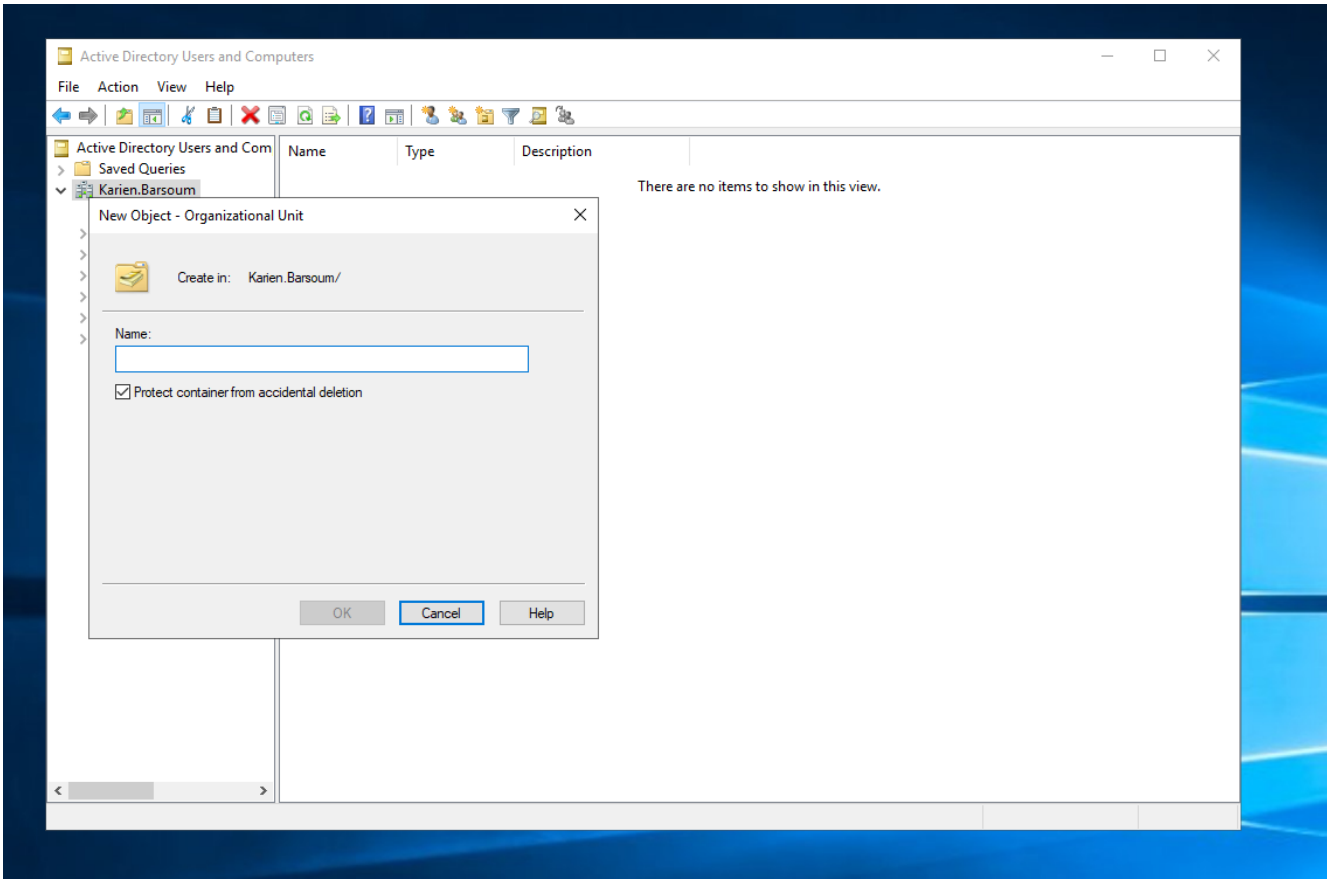


Figure 5

To create a separate admin account from the built-in one, click the start button, expand "Windows Administrative Tools", then choose "Active Directory Users and Computers". You will notice your newly created domain on the right. Right click your domain choose new then Organizational Unit. Name the OU ADMINS for administrator accounts *Figure 5*. Right click the ADMINS OU, choose new, then user. Enter your name in the applicable fields. Most institutions have a naming convention of first initial and lowercase last name. I will choose "a" for admin then "-" and "kbarsoum" to identify me *Figure 6*. Click next, create password, and choose preferred password and account options. In the corporate world, usually the user will create the password on next login, and the password should expire when policy states. I will uncheck user must change password on next login, and check password never expires as this is a lab environment. Click next, and finish. To add this user to domain admins, right click on the created user, properties, then member of, and add. Type in "Domain Admins" in the box, click check names and it should resolve *Figure 7*. Click OK and OK. To use the account, sign out, choose other user, and log in with your domain admin account.

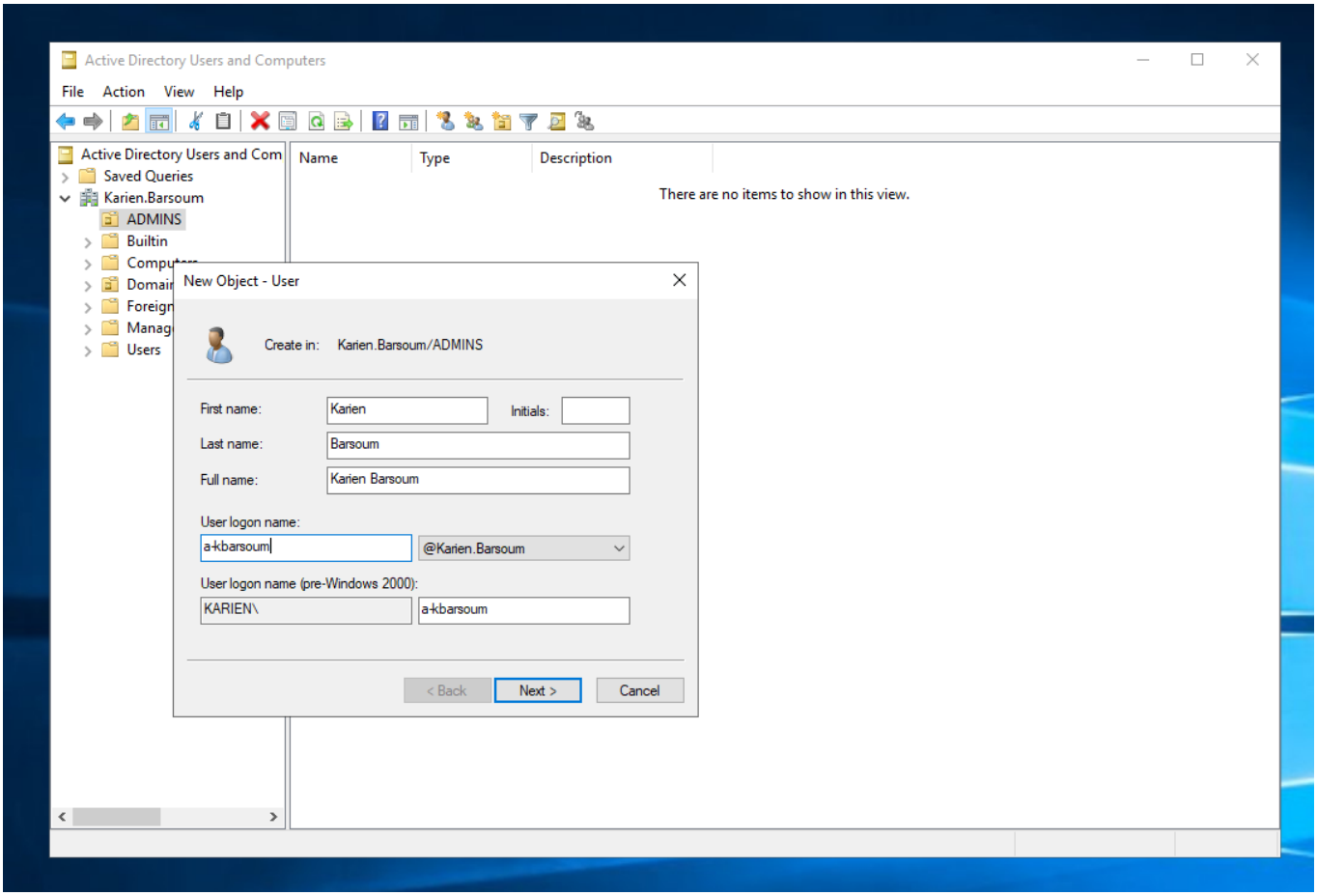

Active Directory Users and Computers
File Action View Help
Active Directory Users and Com
Saved Queries
Karien.Barsoum
ADMINS
Builtin
Users
Name
Type
Description
There are no items to show in this view.
New Object - User
Create in: Karien.Barsoum/ADMINS
First name:
Karien
Initials:
Last name:
Barsoum
Full name:
Karien Barsoum
User logon name:
a-kbarsoum
@Karien.Barsoum
User logon name (pre-Windows 2000):
KARIEN\
a-kbarsoum
< Back
Next >
Cancel

Figure 6

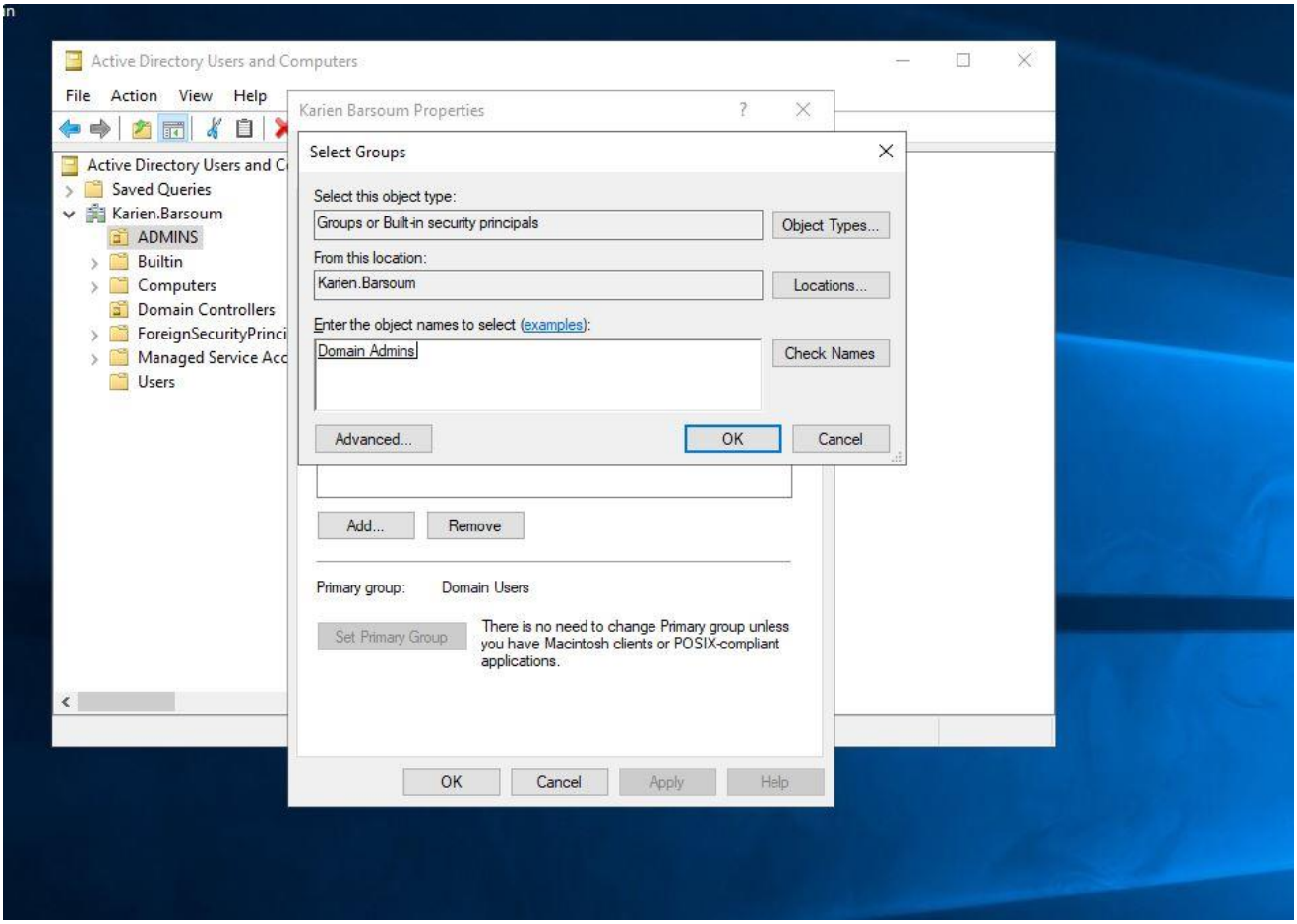

Active Directory Users and Computers
File Action View Help
Active Directory Users and C
Saved Queries
Karien.Barsoum
ADMINS
Builtin
Computers
Domain Controllers
ForeignSecurityPrinci
Managed Service Acc
Users
Karien Barsoum Properties
Select Groups
Select this object type:
Groups or Built-in security principals
Object Types...
From this location:
Karien.Barsoum
Locations...
Enter the object names to select (examples):
Domain Admins
Check Names
Advanced...
OK
Cancel
Add...
Remove
Primary group: Domain Users
Set Primary Group
There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.
OK
Cancel
Apply
Help

Figure 7

Installing RAS / NAT

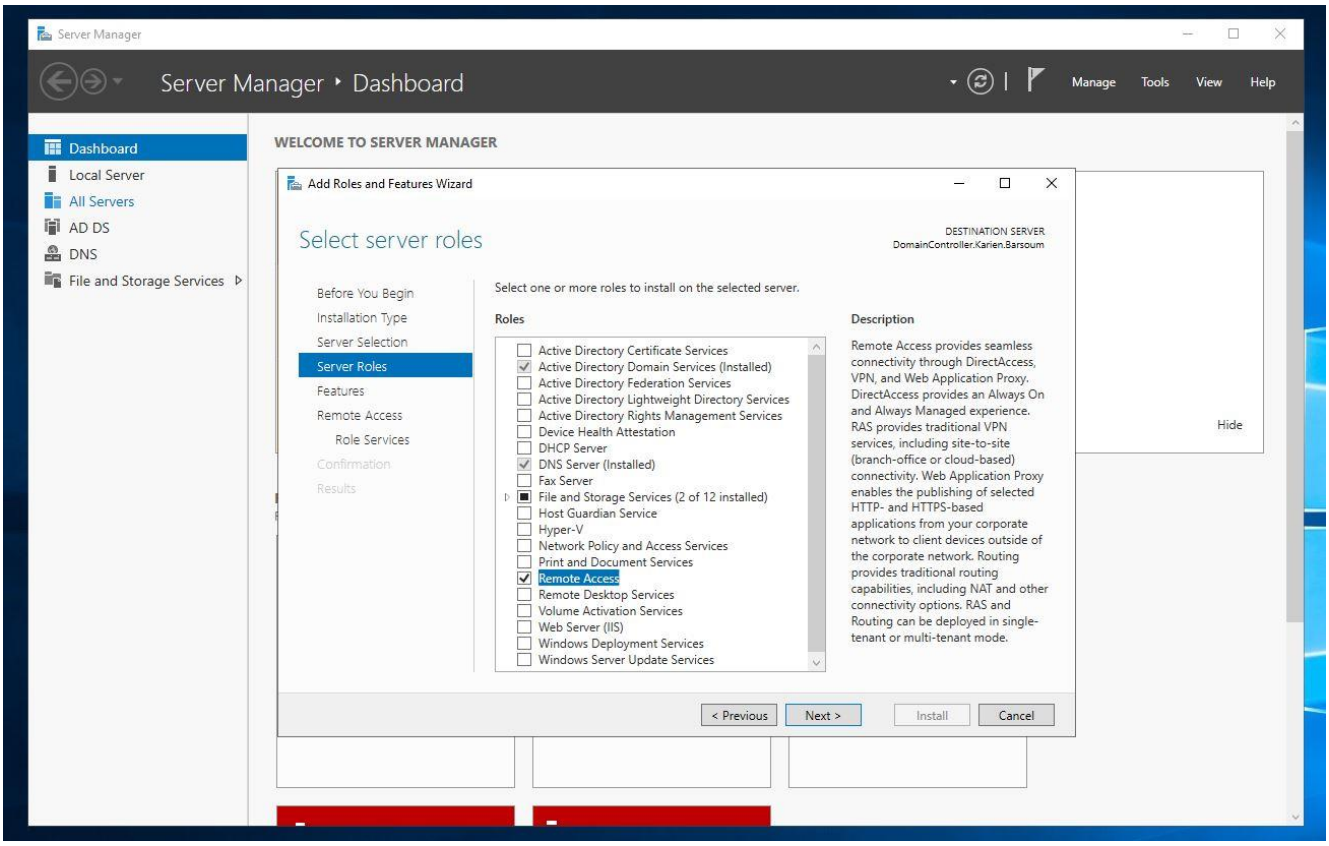


Figure 8

After signing back in, repeat previous steps to add roles, then check “Remote Access” at the “Server Roles” screen *Figure 8*. Click next, check “Routing” on the “Add features” screen (it will automatically select DirectAccess) *Figure 9*, click next, then next, next, and install.

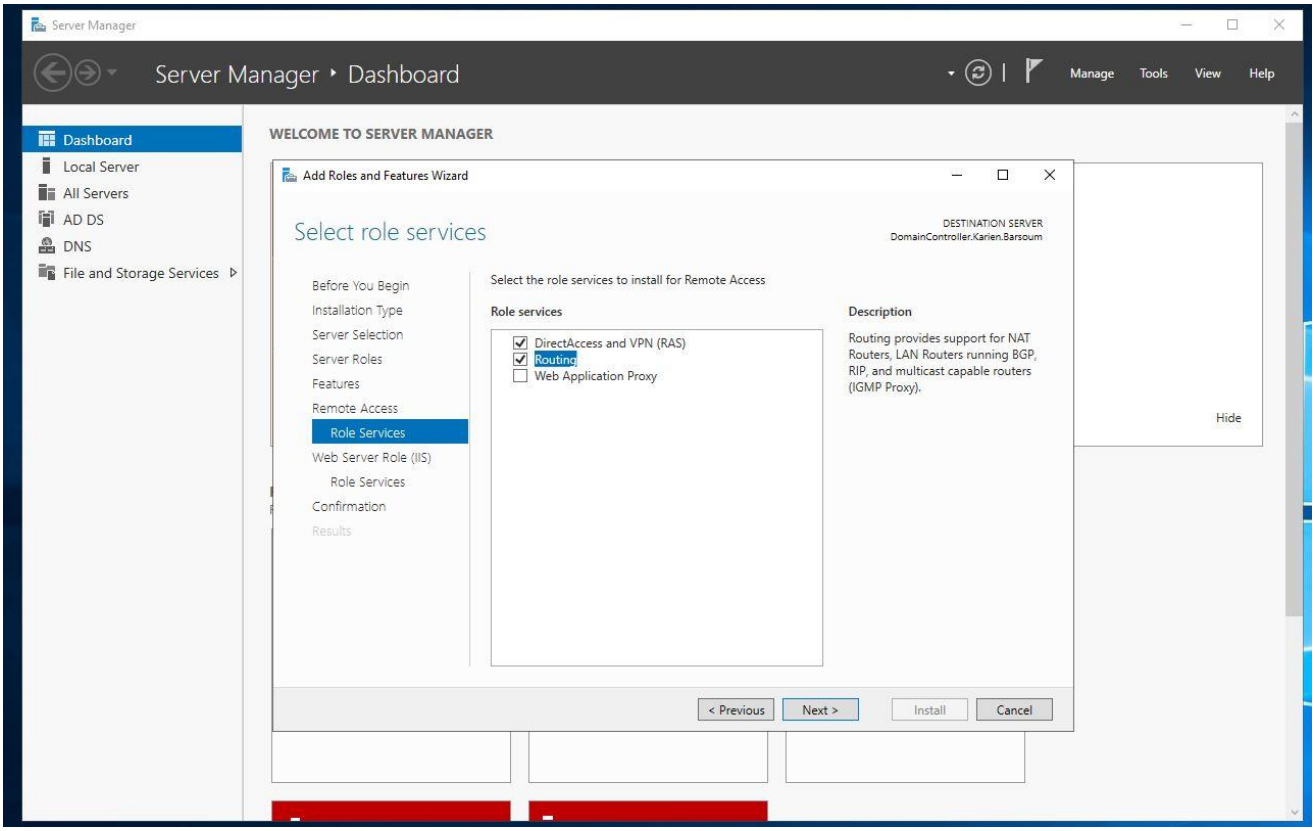


Figure 9

After installing Remote Access, you will need to go to tools, Routing and Remote Access, right click your domain controller, then “Configure and Enable Routing and Remote Access”. You will be met with the setup wizard. Check “NAT”, click next. You should be able to see both interfaces. If not, you will need to close out of the wizard and Routing and Remote access window, then proceed to the setup wizard again. You should be able to see the two interfaces now. Check “Use public interface to connect to the internet”, then highlight the internet interface *Figure 10*. Click next, then finish.

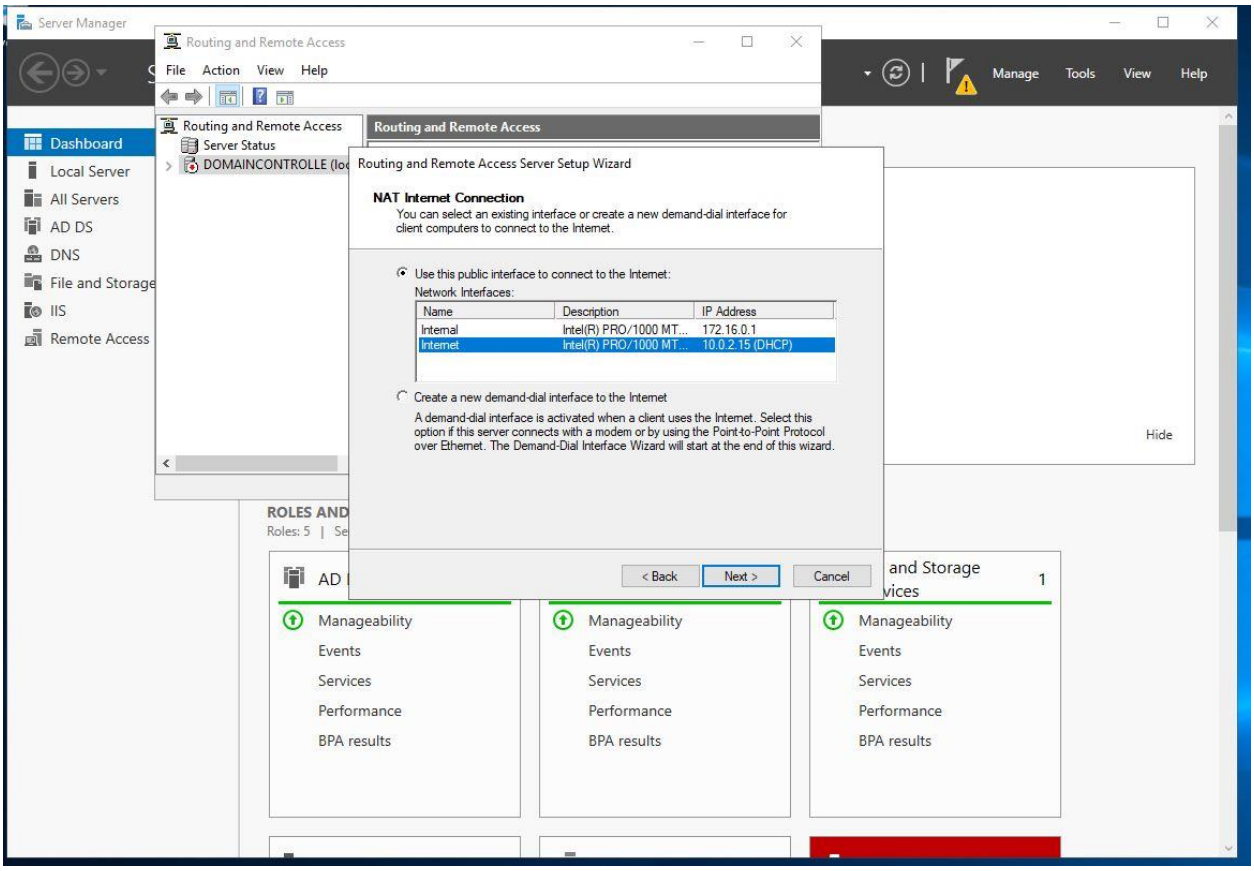


Figure 10

DHCP setup and deployment

With RAS / NAT set up, the next thing to do is setup DHCP services so that clients that connect to the server will be able to have their IP addresses dynamically addresses to them with no work to be done from us. Repeat steps from previous installations by adding rolls and features within the Server Manager. This time select DHCP services *Figure 11*. Click add features on the pop up, then next until you can install DHCP. After DHCP is done installing, close the window.

Navigate to tools, then DHCP. You will be met with the control panel on *Figure 12*.

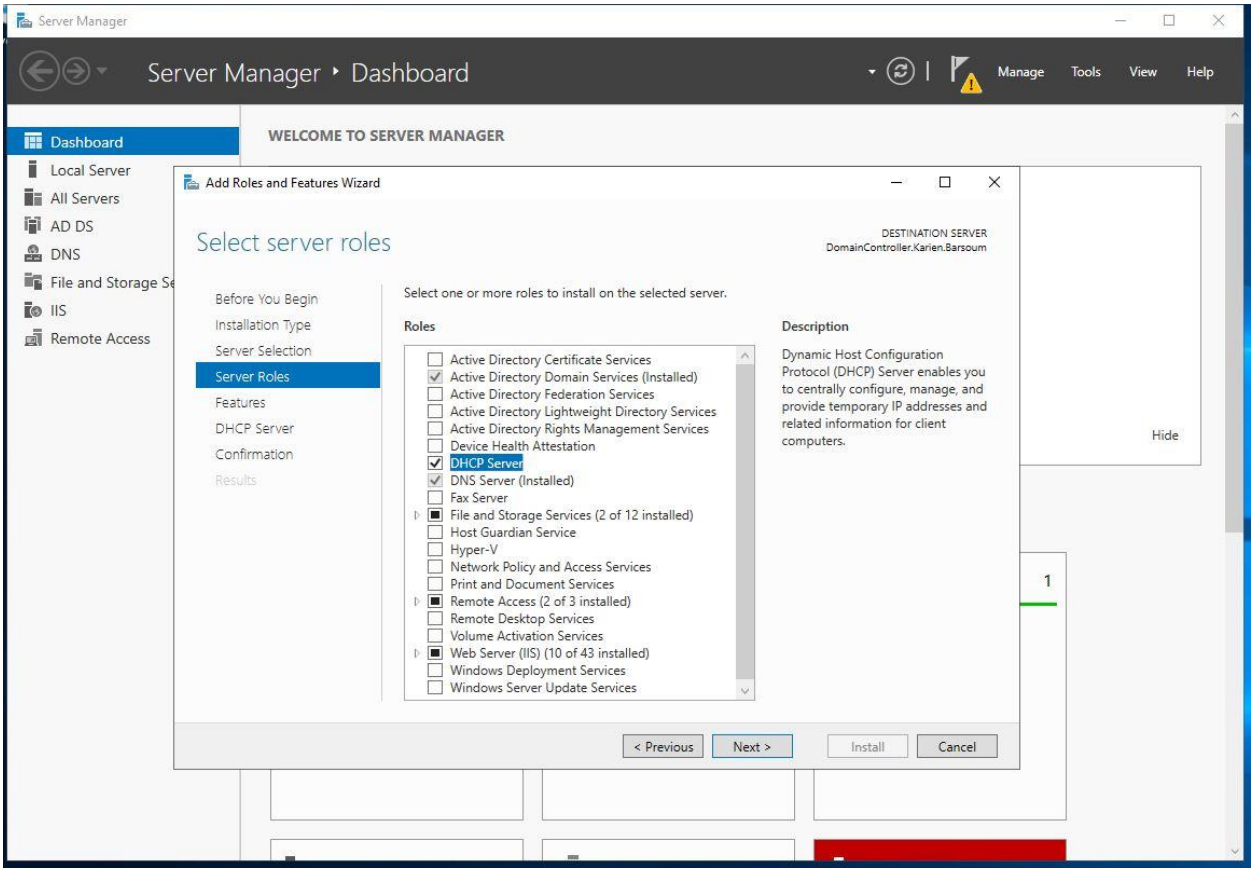


Figure 11

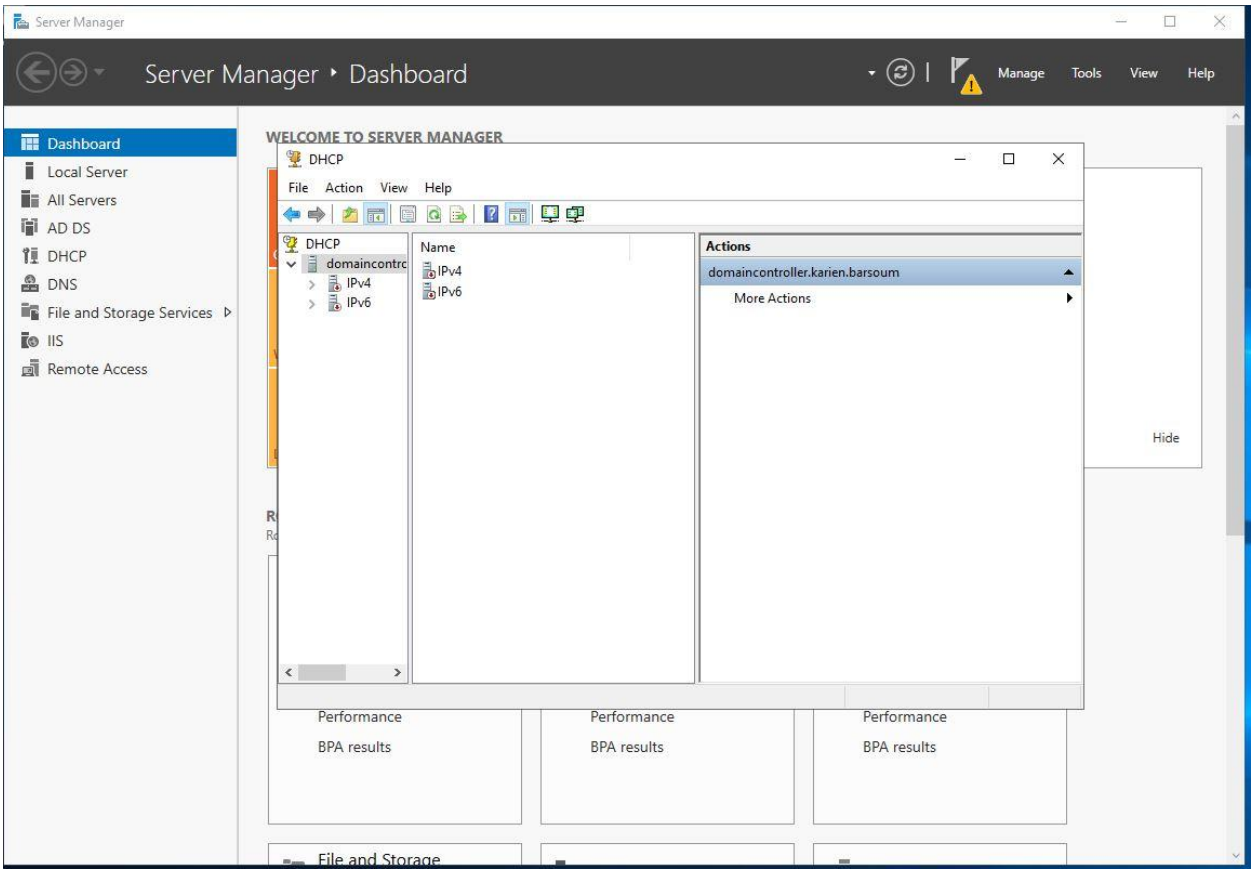


Figure 12

At this stage, we'll need to create the pool of addresses that the DHCP server will dynamically choose from as clients connect to it. We will use a pool/range of 172.16.0.100 –200/24 for clients to have. Expand the domain, then right click on IPv4, choose new scope, click next. I recommend adding the name of the new scope as the address range, click next, enter the start and end IP address with the length of 24/subnet mask of 255.255.255.0 where it applies *Figure 13*. Then, click next, click next again on exclusions, then choose the lease duration of 8 days. The lease duration is how long a client can keep an IP address before it expires. In places life cafes, or public offices that customers visit, the lease duration should be shorter. A shorter lease duration is also good for security reasons. Click next, and on the "Router (Default Gateway)" page enter the Domain Controllers internal NIC as the default gateway for the clients. That would be 172.16.0.1. Make sure to click add, then click next. On the Domain Name and DNS Servers, the DNS server is provided by the domain controller with active directory so do not change it. Click next and next on WINS server, make sure to activate the scope now then click next and finish. Once done close the wizard, then right click on your DHCP server, choose authorize to authorize the server, then right click and refresh the server to make sure the

changes take effect.

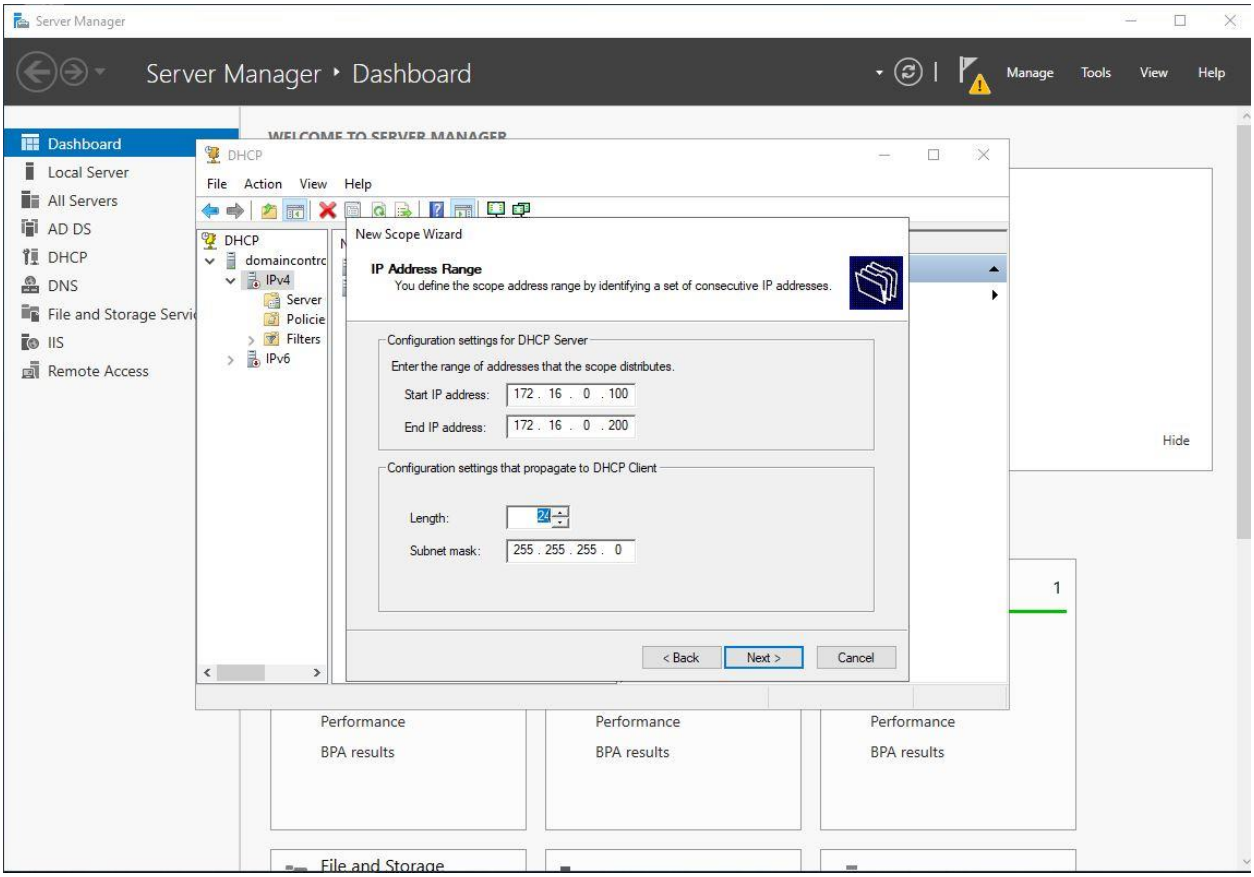


Figure 13

Creating active directory domain accounts with PowerShell automation

Before setting up client machines to connect to the server, they will need to have active directory accounts, that's just how AD DS works. In the typical corporate environment, you might have hundreds of client accounts to set up. This can be a tedious process. To automate the creation of accounts you have access to PowerShell scripting to aid you in the process. Of course, you can create your own PowerShell script to automate this process, but I have went ahead and found a safe script online to use for this. WARNING- You should not be downloading and running random scripts on your machine if you can not analyze the code beforehand and rule out malware. The code I will run is in here https://github.com/joshmadakor1/AD_PS

Properly vet every piece of code you intend to run on your machine.

After downloading the zip file from the link, copy the zip file to your Domain Controller desktop. Extract the folder and open it *Figure 14*. In the folder is a list of 1000 names within a text file (names.txt) to replicate a list of users you might get that you will need to create accounts for. Add your name to the top of the text file and save so that you will also have a user account. Click start, expand Windows PowerShell, and right click Windows PowerShell ISE to run as administrator *Figure 15*. On PowerShell, Go to open, desktop, folder, and open the

_CREATE_USERS file. Before executing the code, we'll need to enable the execution of scripts on the server. Within the terminal, run Set-ExecutionPolicy Unrestricted *Figure 16*. This will bypass the security of the server to allow non-digitally signed code to run. Keep in mind that to maintain security in a corporate setting, this is not to be changed. Respond to the prompt with Yes to all.

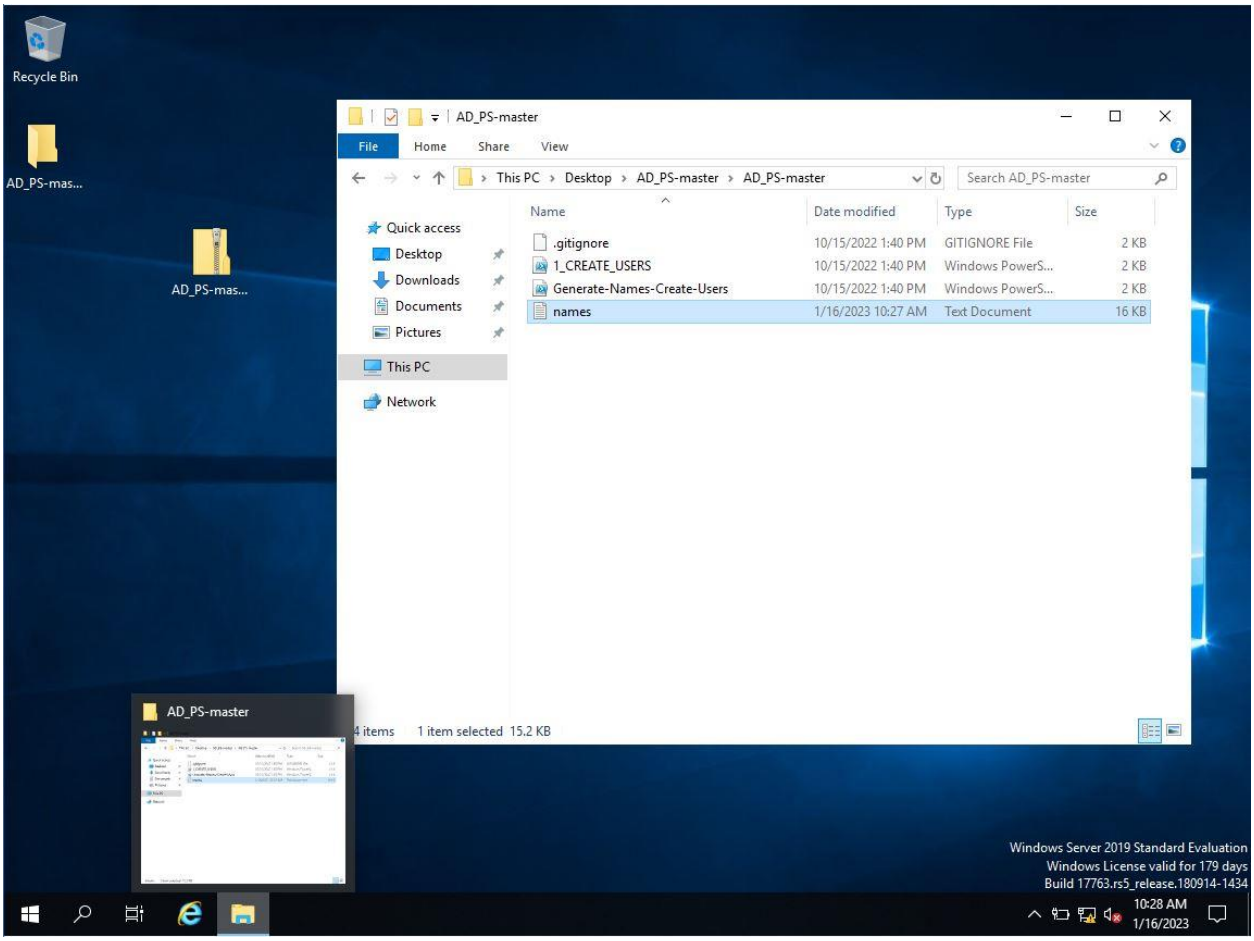


Figure 14

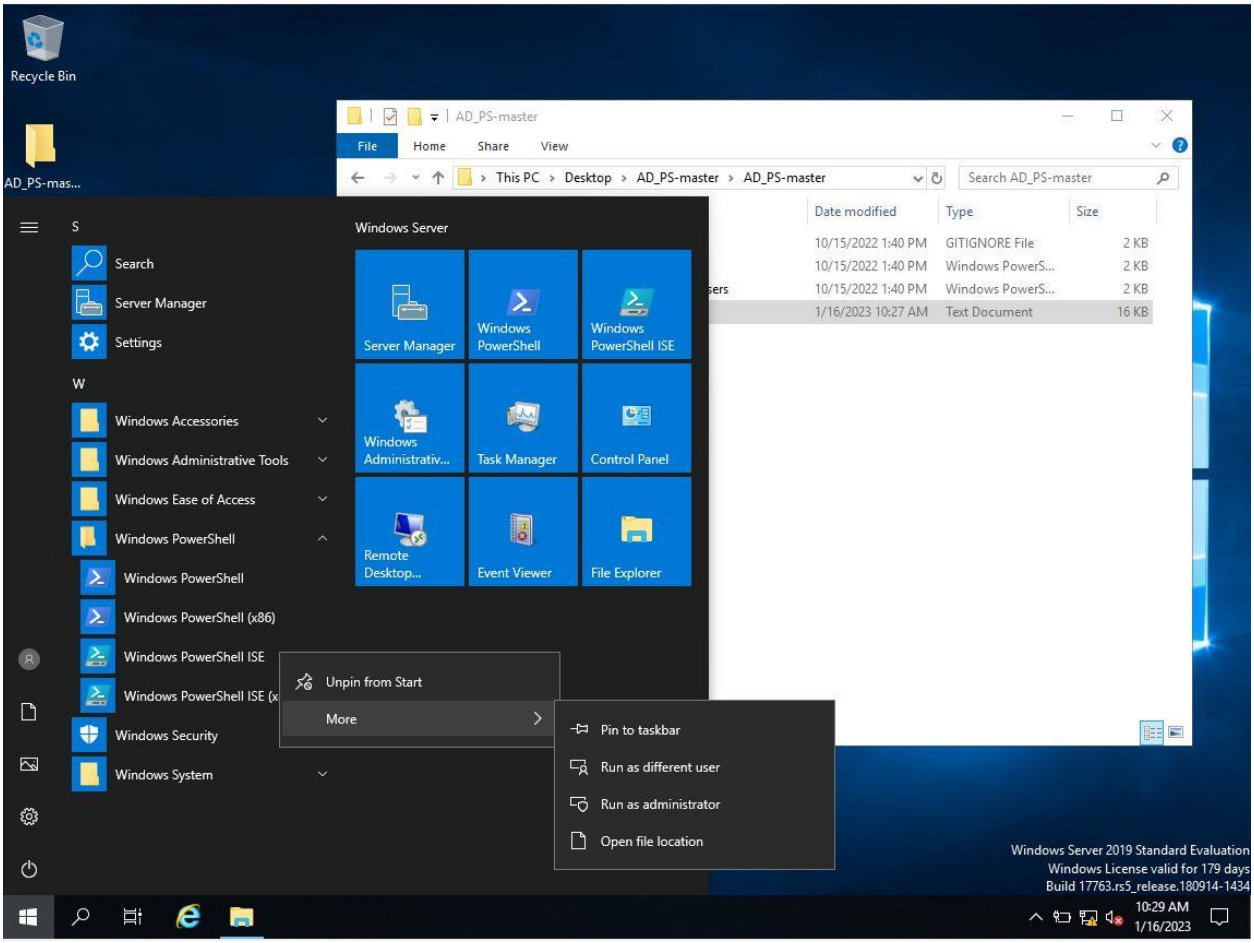

Recycle Bin
AD_PS-mas...
AD_PS-master
File
Home
Share
View
This PC › Desktop › AD_PS-master › AD_PS-master
Search AD_PS-master
Date modified
Type
Size
10/15/2022 1:40 PM
GITIGNORE File
2 KB
10/15/2022 1:40 PM
Windows PowerS...
2 KB
10/15/2022 1:40 PM
Windows PowerS...
2 KB
1/16/2023 10:27 AM
Text Document
16 KB
S
Search
Server Manager
Settings
W
Windows Accessories
Windows Administrative Tools
Windows Ease of Access
Windows PowerShell
Windows PowerShell
Windows PowerShell (x86)
Windows PowerShell ISE
Windows PowerShell ISE (x
Windows Security
Windows System
Windows Server
Server Manager
Windows PowerShell
Windows PowerShell ISE
Windows Administrativ...
Task Manager
Control Panel
Remote Desktop...
Event Viewer
File Explorer
Unpin from Start
More
Pin to taskbar
Run as different user
Run as administrator
Open file location
Windows Server 2019 Standard Evaluation
Windows License valid for 179 days
Build 17763.rs5_release.180914-1434
10:29 AM
1/16/2023

Figure 15

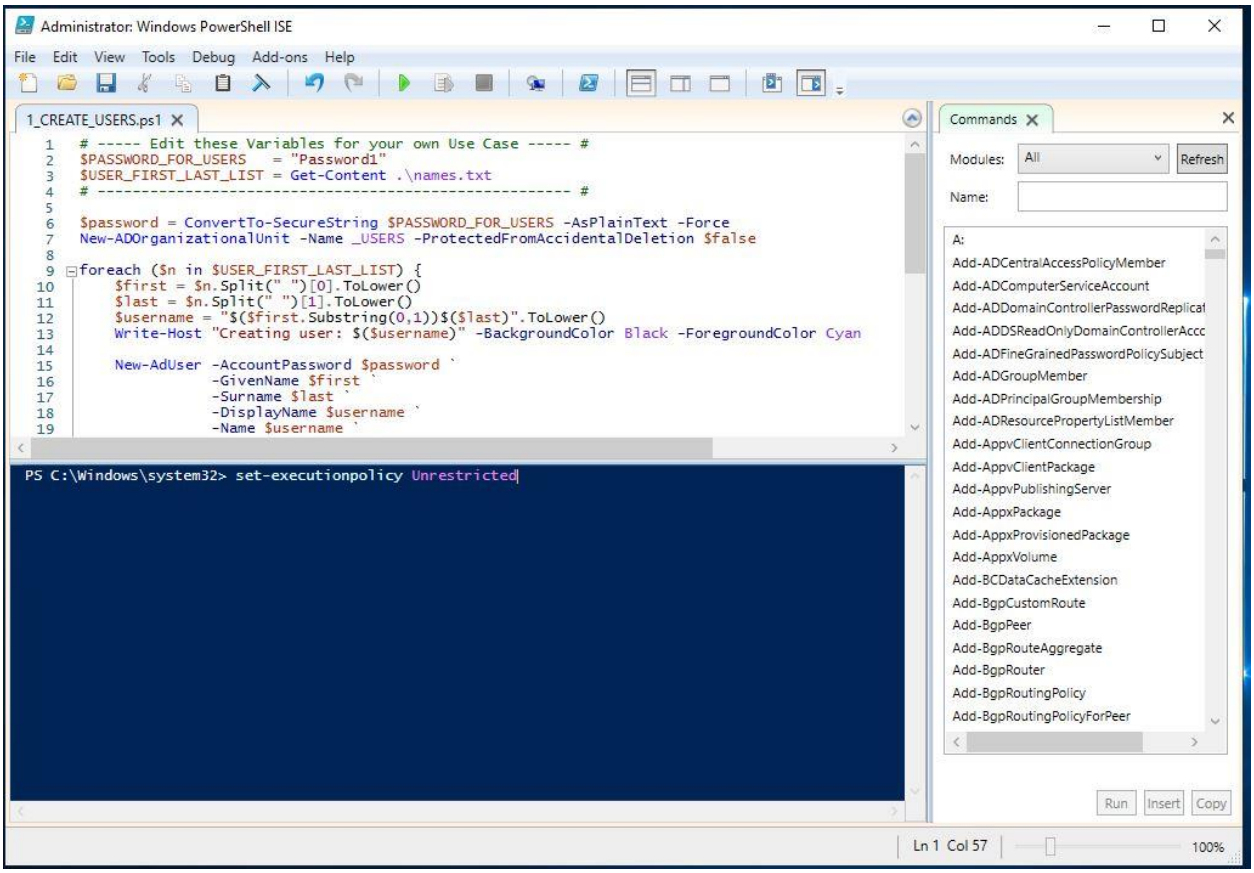
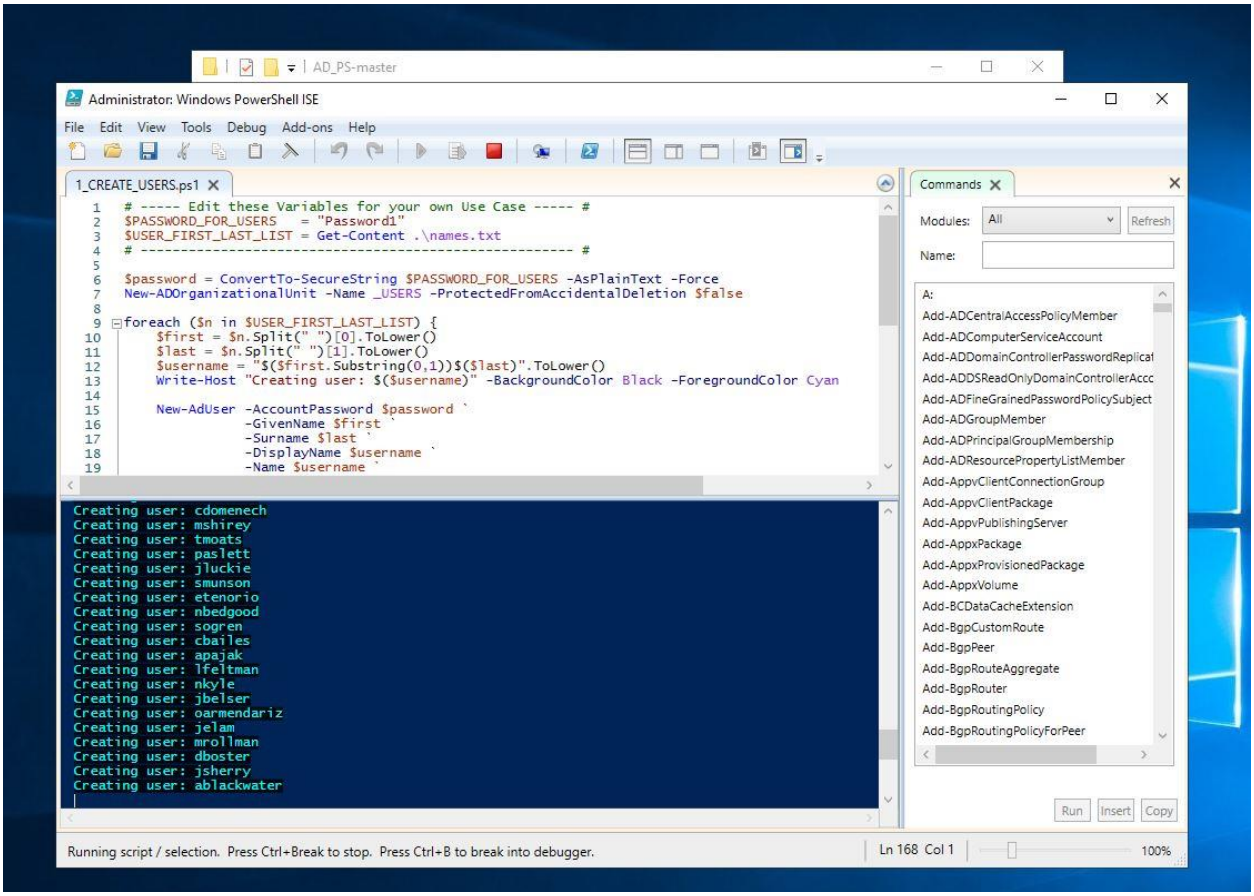


Figure 16

You will need to use the terminal to change directory to the folder where the names.txt file is. Type in cd C:\users\yourusername\desktop\AD_PS-master. You can enter ls and see that the names.txt file is in there. Once you hit the green play button at the top of the screen, respond to the security prompt to run once and the code will run. You will now see the code running *Figure 17.* If you navigate to Active Directory Users and Computers, you will see the accounts created under the _USERS OU which was created by the PowerShell script *Figure 18*.


AD_PS-master
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
1_CREATE_USERS.ps1
----- Edit these Variables for your own Use Case -----
$PASSWORD_FOR_USERS = "Password1"
$USER_FIRST_LAST_LIST = Get-Content .\names.txt

$password = ConvertTo-SecureString $PASSWORD_FOR_USERS -AsPlainText -Force
New-ADOrganizationalUnit -Name _USERS -ProtectedFromAccidentalDeletion $false
foreach ($n in $USER_FIRST_LAST_LIST) {
$first = $n.Split(" ")[0].ToLower()
$last = $n.Split(" ")[1].ToLower()
$username = "$($first.Substring(0,1))$($last)".ToLower()
Write-Host "Creating user: $($username)" -BackgroundColor Black -ForegroundColor Cyan
New-AdUser -AccountPassword $password `
-GivenName $first `
-Surname $last `
-DisplayName $username `
-Name $username `
Creating user: cdomenech
Creating user: mshirey
Creating user: tmoats
Creating user: paslett
Creating user: jluckie
Creating user: smunson
Creating user: etenorio
Creating user: nbedgood
Creating user: sogren
Creating user: cbailes
Creating user: apajak
Creating user: lfeltman
Creating user: nkyle
Creating user: jbelser
Creating user: oarmendariz
Creating user: jelam
Creating user: mrollman
Creating user: dboster
Creating user: jsherry
Creating user: ablackwater
Commands
Modules: All
Refresh
Name:
A:
Add-ADCentralAccessPolicyMember
Add-ADComputerServiceAccount
Add-ADDomainControllerPasswordReplicat
Add-ADDSReadOnlyDomainControllerAccc
Add-ADFineGrainedPasswordPolicySubject
Add-ADGroupMember
Add-ADPrincipalGroupMembership
Add-ADResourcePropertyListMember
Add-AppvClientConnectionGroup
Add-AppvClientPackage
Add-AppvPublishingServer
Add-AppxPackage
Add-AppxProvisionedPackage
Add-AppxVolume
Add-BCDataCacheExtension
Add-BgpCustomRoute
Add-BgpPeer
Add-BgpRouteAggregate
Add-BgpRouter
Add-BgpRoutingPolicy
Add-BgpRoutingPolicyForPeer
Run
Insert
Copy
Running script / selection. Press Ctrl+Break to stop. Press Ctrl+B to break into debugger.
Ln 168 Col 1
100%

Figure 17

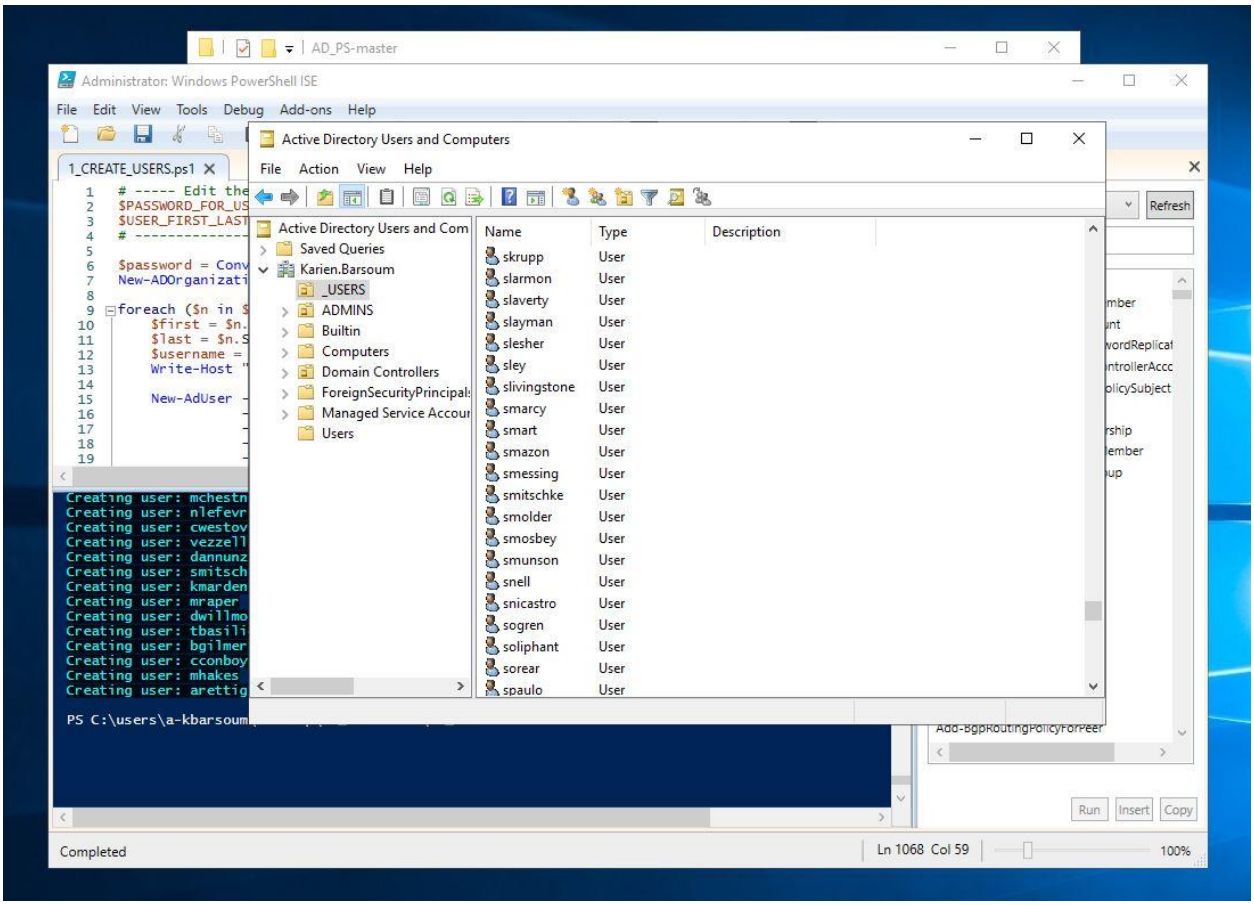


Figure 18

Configuring Windows Client with Active Directory

Turn on your Windows 10 machine. Ping the domain controller to check connectivity. Because the Windows 10 Pro machine is connected to the internal network, connectivity should work fine. You may ping google to check DNS services and check your ipconfig information as well *Figure 19*.

Go to the client machine, right click start, then system. Scroll in the settings to find “Rename this PC (advanced) in blue font and click it. You can join a domain from this. On system properties, click change, then name it “CLIENT1”. Check domain and enter the domain name. After you click OK, you will be prompted to sign in with a domain account. You can sign in with your admin account that was created previously. After signing in, the machine will be registered with the domain controller *Figure 20*.

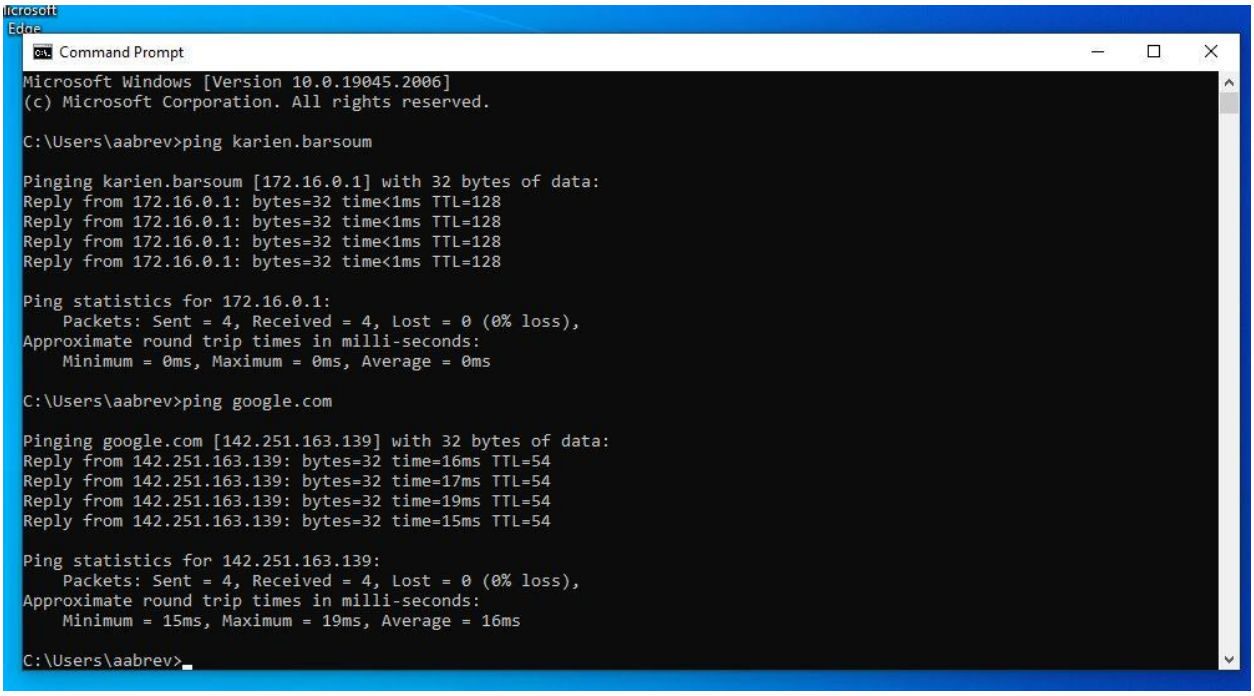


Figure 19

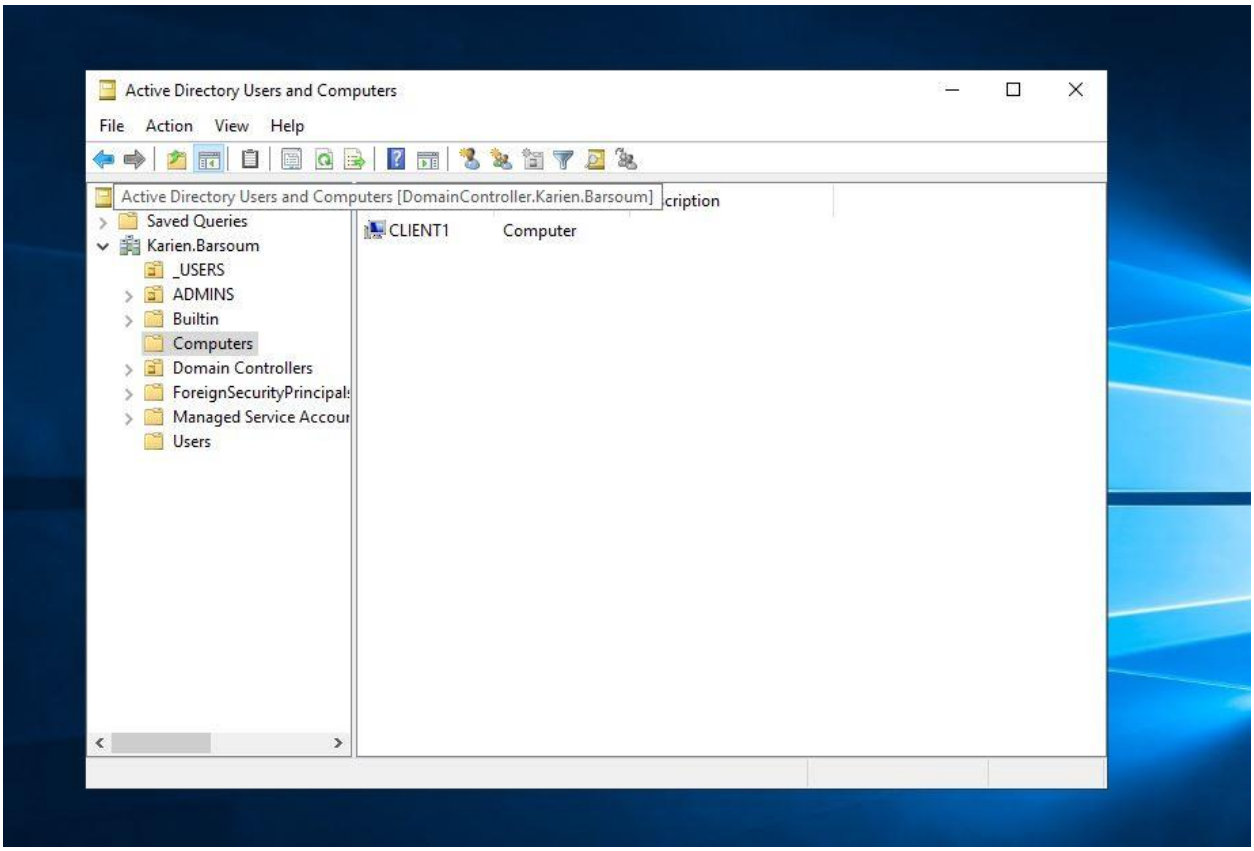


Figure 20