# AAA ON AN ACCESS SERVER

SONYA LAO
CCNP PER. 1/2

# Purpose

The purpose of this lab is to explore the power of Authentication, Authorization, and Accounting. Our goal was to setup a router connected to a virtual Windows Server running Active Directory so that the router used the server's Active Directory to authenticate and authorize users.

# Background Information

AAA stands for Authentication, Authorization, and Accounting. In this lab, we mainly focused on the authentication portion. Imagine that you have been hired at an exclusive party to serve as the bouncer. Only you and the host have the same key that will unlock the door into the party. Only people that are on a special list can be invited into the party. However, you do not have a copy of the list or their secret passwords. Your job is simply to whisper each person's name and password to the host, who then confirms/denies if the person is on the list. If a person is not on the list and/or does not say their password correctly, they cannot be let in to the party. However, the host is constantly updating her list, so new guests may be added to the list, at the host's discretion.

The router, in connection with a server, operates similarly. The router and the server are connected through Remote Authentication Dial-In User Service (RADIUS), with a shared secret key. Just like with the bouncer and the host, they share a special key that makes the whole authentication process possible. You are like the router. If you get a user that wants to login and access the router's executive mode, the router sends a request packet to the server, who runs the username through its Active Directory database to make sure the user is in the permitted group. If the user is in the group, like the person is on the guest list, then they are allowed into the party/router.

# Lab Summary

There were two main portions to the setup and configuration for this lab. First, I setup the Windows Server through a virtual machine, setting R1 its default gateway. I configured R1 to have an IP address on interface g0/1. Next, I added the roles Active Directory, DNS, and Network Policy Server to the server. Then, I created a domain in DNS, and created a security group in Active Directory. I also added the router as a RADIUS client through Network Policy Server, and noted the shared secret key so that I could configure a matching key on the router. After I finished this setup, I was able to create a network policy that only allowed users to login to the router if they were in my specified security group. Then I created several users and added them to my security group. To test connectivity, I issued several pings from the server to the router.

Once the setup on the Windows Server was complete, I configured the router to recognize the server as its RADIUS server with the same shared secret key, and created an AAA authentication login list to be used by the console. To test my configuration, I attempted to login to the router using a username not in the security group, and ensured that it failed. Then, I added the user into my security group and tried the login again, and checked that login was successful

# Lab Commands

`R1(config)#aaa new-model`
This command enables AAA and immediately applies authentication to all lines and interfaces. Without this command, all other AAA commands are hidden.

`R1(config)#radius-server host [IP address of AAA server]`
To specify an external AAA server, this command is used. It indicates that RADIUS is the preferred security protocol between the router and the server, and details the address of the server.

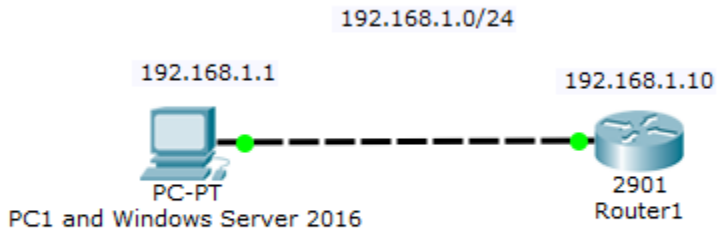
`R1(config)#radius-server key [key]`
This command is to specify the same shared secret key that is on the server. The key is case-sensitive and should match the key configured on the Network Policy Server with this router as a client.

`R1(config)#aaa authentication login [name] group radius`
In order to allow users exec access into the router, the `aaa authentication login` command is used. This command is used to define a list of all available authentication methods. In this version of the command, the `group radius` is the first and only method for authentication, and indicates that RADIUS is to be used for authentication.

```
R1(config)#line con 0
R1(config-line)#login authentication [list name]
```

After the authentication list has been created in global configuration mode, the list can be applied to the console line. The list has to be applied to a line or an interface before it comes into effect.

# Network Diagram




# Configurations

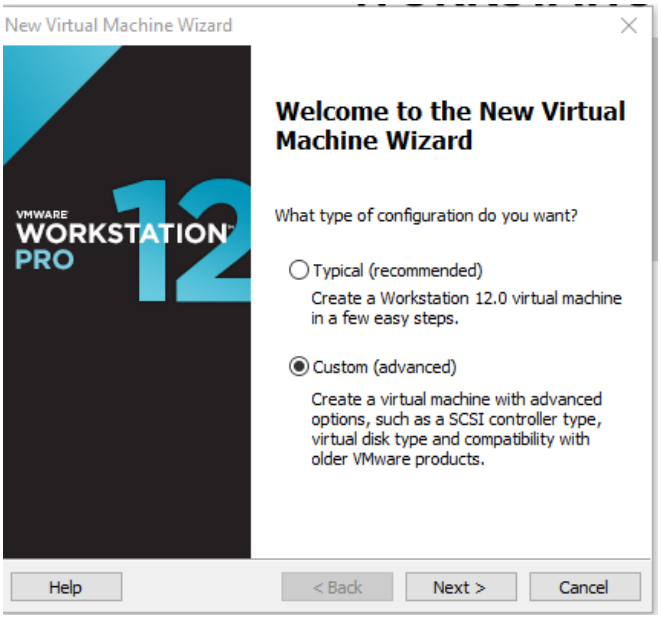
There are two main sections of configuration in this lab, with configuration on the router and setup on the server. Below are the configurations on the router.

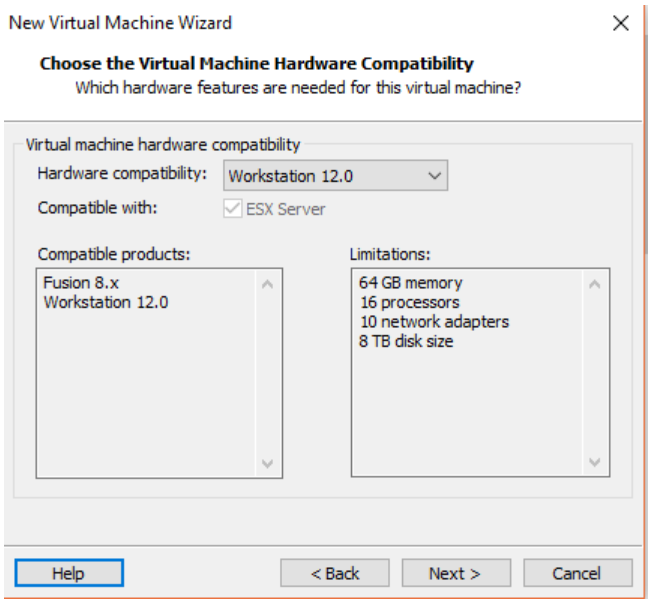
**R1>ping 192.168.1.10**

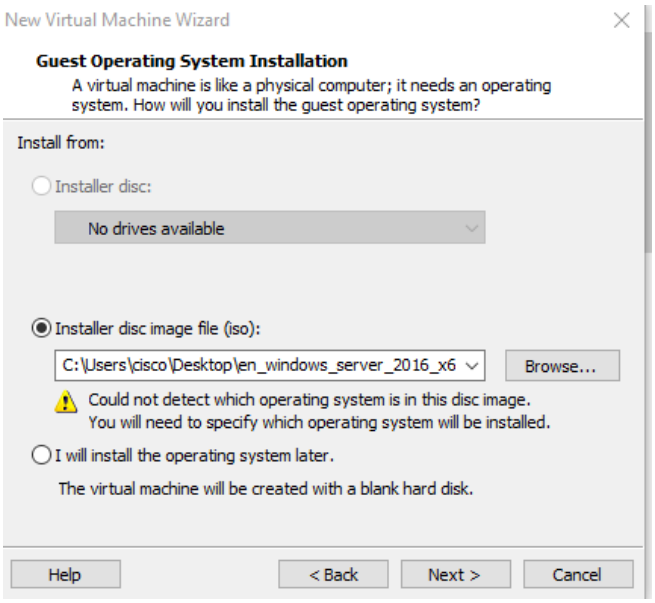
```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

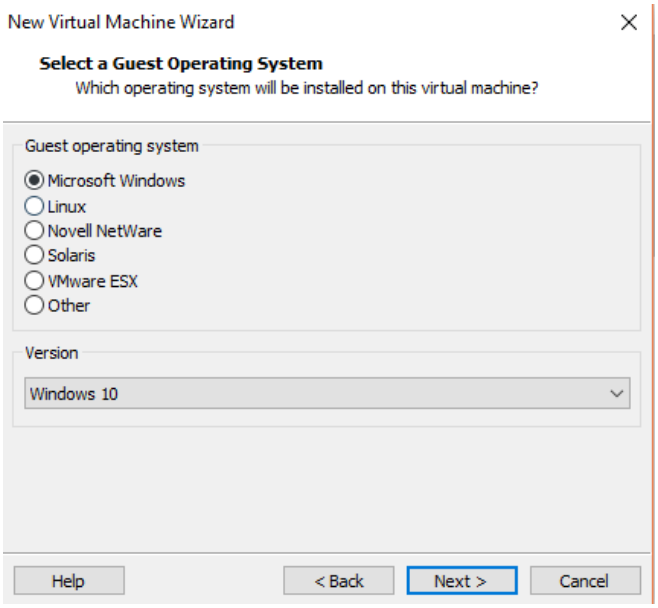
**R1 show run:**

```
Current configuration: 1679 bytes
Last configuration change at 16:37:46
UTC Thu Jan 5 2017
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R3
aaa new-model
aaa authentication login OKAY group
radius
aaa session-id common
memory-size iomem 10
no ip domain lookup
ip domain name cisco.com
no ipv6 cef
vtp domain cisco
vtp mode transparent
redundancy
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
ip forward-protocol nd
no ip http server
no ip http secure-server
radius-server host 192.168.1.10
radius-server key Ciscoclass
line con 0
 login authentication OKAY
line aux 0
line 2
 no activation-character
 no exec
line vty 0 4
 password admin
 transport input all
scheduler allocate 20000 1000
end
```

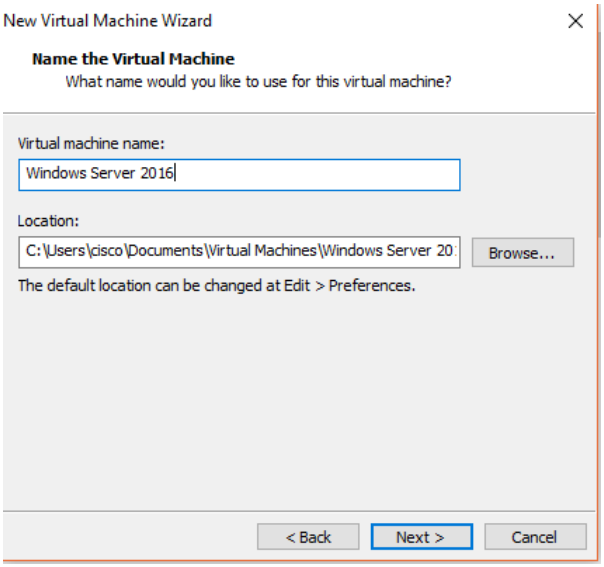


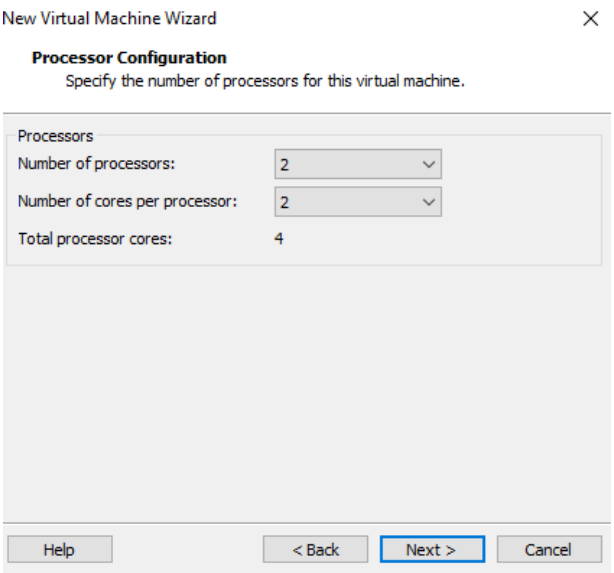



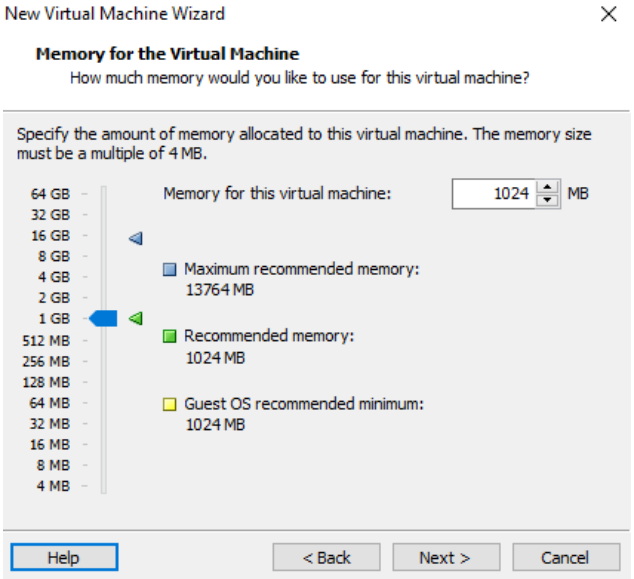



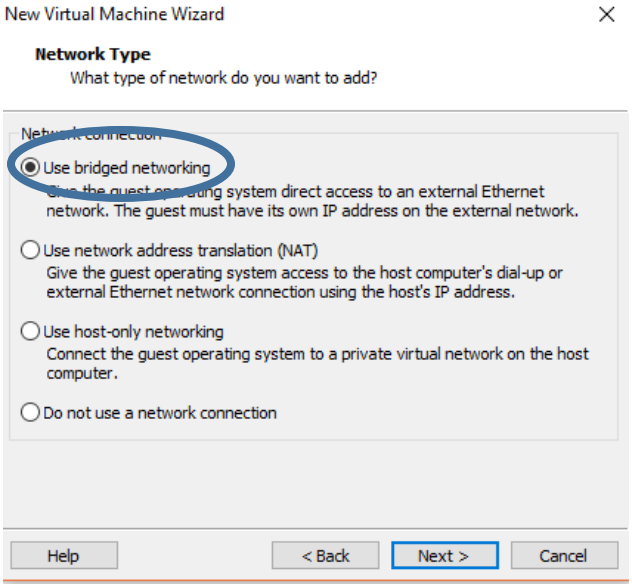



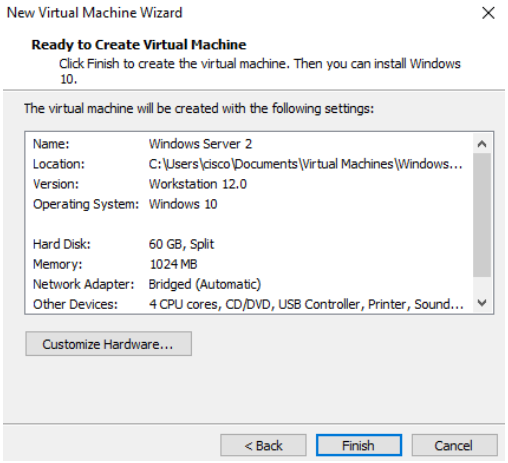

Above is my initial setup on the AAA server. First, I setup the server by creating a new Virtual Machine in VMWare running the Windows Server 2016 operating system. I name the Virtual machine, select the number of processors and memory, and choose to use bridged networking. Then, I booted the virtual machine to set up the Windows Server.

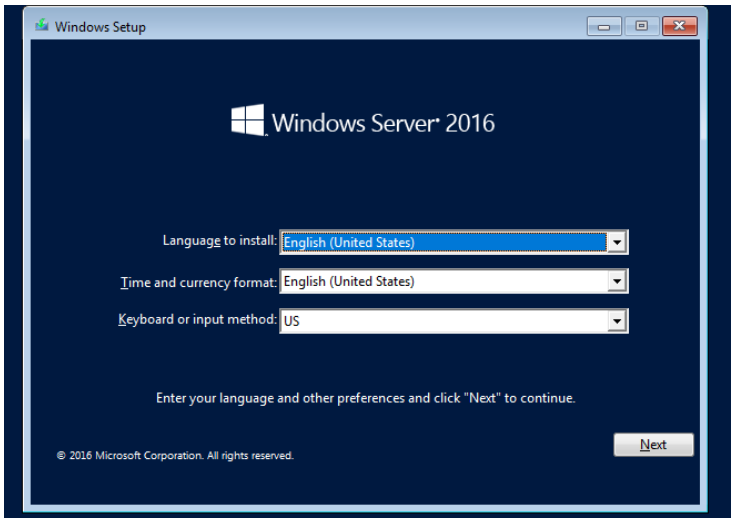

New Virtual Machine Wizard
Name the Virtual Machine
What name would you like to use for this virtual machine?
Virtual machine name:
Windows Server 2016
Location:
C:\Users\cisco\Documents\Virtual Machines\Windows Server 20
Browse...
The default location can be changed at Edit > Preferences.
< Back
Next >
Cancel

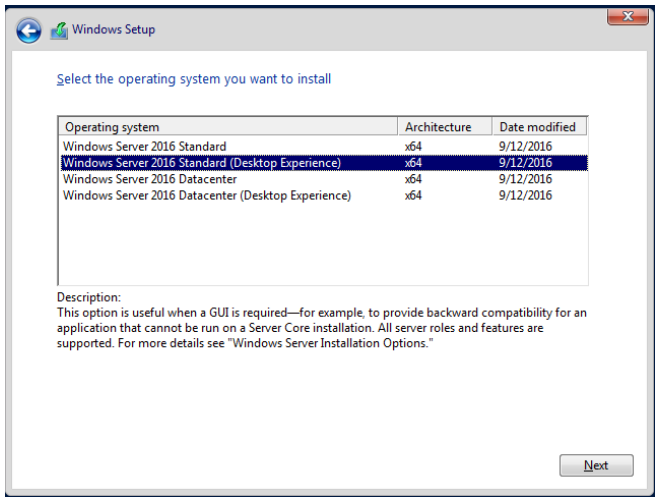

New Virtual Machine Wizard
Processor Configuration
Specify the number of processors for this virtual machine.
Processors
Number of processors:
2
Number of cores per processor:
2
Total processor cores:
4
Help
< Back
Next >
Cancel

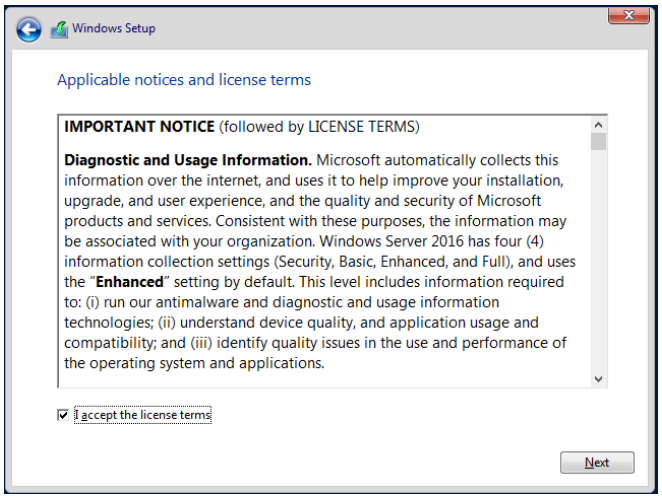

New Virtual Machine Wizard
Memory for the Virtual Machine
How much memory would you like to use for this virtual machine?
Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.
64 GB
32 GB
16 GB
8 GB
4 GB
2 GB
1 GB
512 MB
256 MB
128 MB
64 MB
32 MB
16 MB
8 MB
4 MB
Memory for this virtual machine:
1024
MB
Maximum recommended memory:
13764 MB
Recommended memory:
1024 MB
Guest OS recommended minimum:
1024 MB
Help
< Back
Next >
Cancel

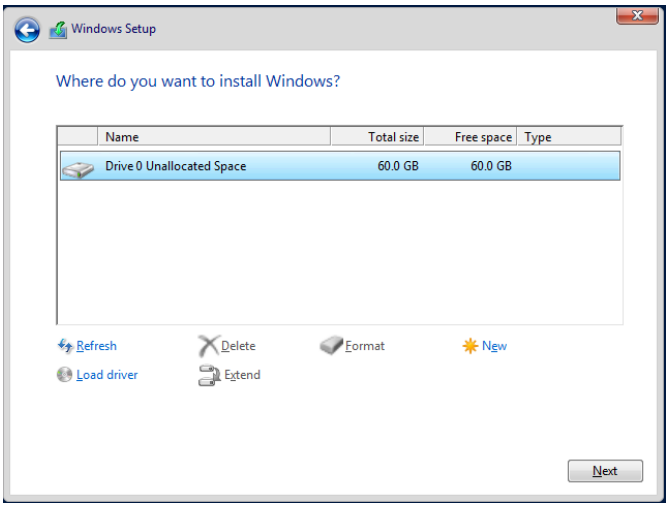

New Virtual Machine Wizard
Network Type
What type of network do you want to add?
Use bridged networking
network. The guest must have its own IP address on the external network.
Use network address translation (NAT)
Give the guest operating system access to the host computer's dial-up or external Ethernet network connection using the host's IP address.
Use host-only networking
Connect the guest operating system to a private virtual network on the host computer.
Do not use a network connection
Help
< Back
Next >
Cancel

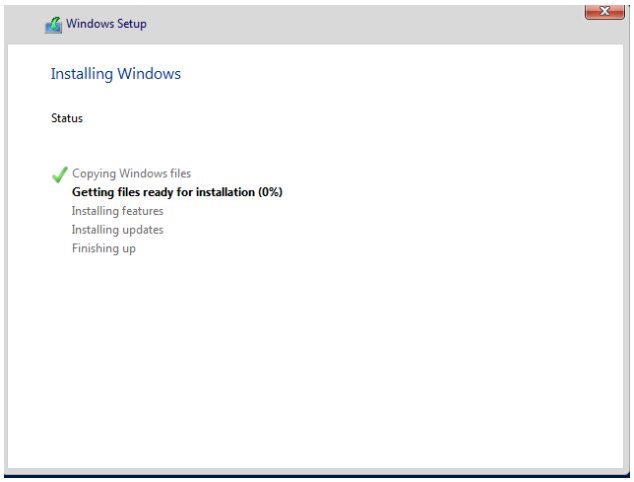

New Virtual Machine Wizard
Ready to Create Virtual Machine
Click Finish to create the virtual machine. Then you can install Windows 10.
The virtual machine will be created with the following settings:
Name: Windows Server 2
Location: C:\Users\cisco\Documents\Virtual Machines\Windows...
Version: Workstation 12.0
Operating System: Windows 10
Hard Disk: 60 GB, Split
Memory: 1024 MB
Network Adapter: Bridged (Automatic)
Other Devices: 4 CPU cores, CD/DVD, USB Controller, Printer, Sound...
Customize Hardware...
< Back
Finish
Cancel

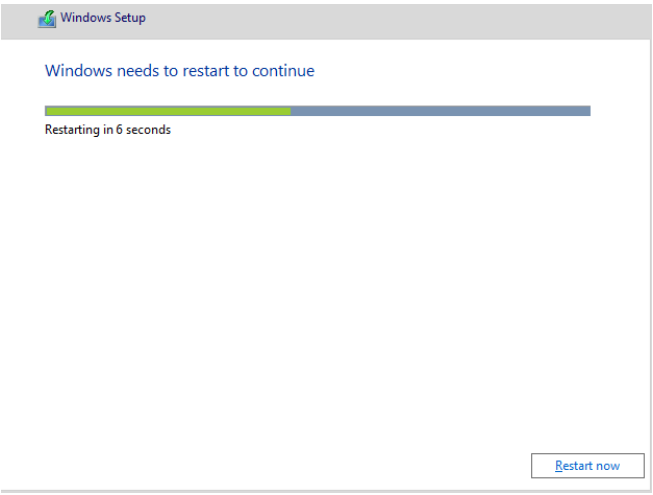

Windows Setup
Windows Server 2016
Language to install: English (United States)
Time and currency format: English (United States)
Keyboard or input method: US
Enter your language and other preferences and click "Next" to continue.
© 2016 Microsoft Corporation. All rights reserved.
Next

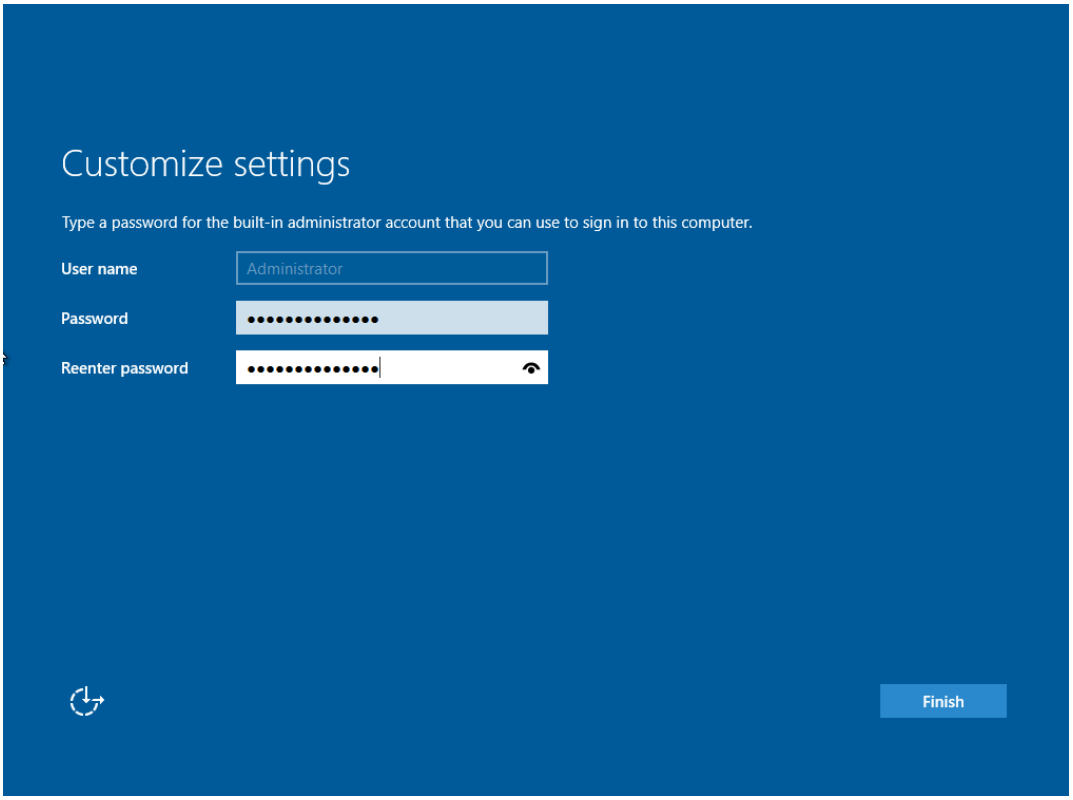

Windows Setup
Select the operating system you want to install
Operating system
Architecture
Date modified
Windows Server 2016 Standard x64 9/12/2016
Windows Server 2016 Standard (Desktop Experience) x64 9/12/2016
Windows Server 2016 Datacenter x64 9/12/2016
Windows Server 2016 Datacenter (Desktop Experience) x64 9/12/2016
Description:
This option is useful when a GUI is required—for example, to provide backward compatibility for an application that cannot be run on a Server Core installation. All server roles and features are supported. For more details see "Windows Server Installation Options."
Next


Windows Setup
Applicable notices and license terms
IMPORTANT NOTICE (followed by LICENSE TERMS)
Diagnostic and Usage Information. Microsoft automatically collects this information over the internet, and uses it to help improve your installation, upgrade, and user experience, and the quality and security of Microsoft products and services. Consistent with these purposes, the information may be associated with your organization. Windows Server 2016 has four (4) information collection settings (Security, Basic, Enhanced, and Full), and uses the "Enhanced" setting by default. This level includes information required to: (i) run our antimalware and diagnostic and usage information technologies; (ii) understand device quality, and application usage and compatibility; and (iii) identify quality issues in the use and performance of the operating system and applications.
I accept the license terms
Next

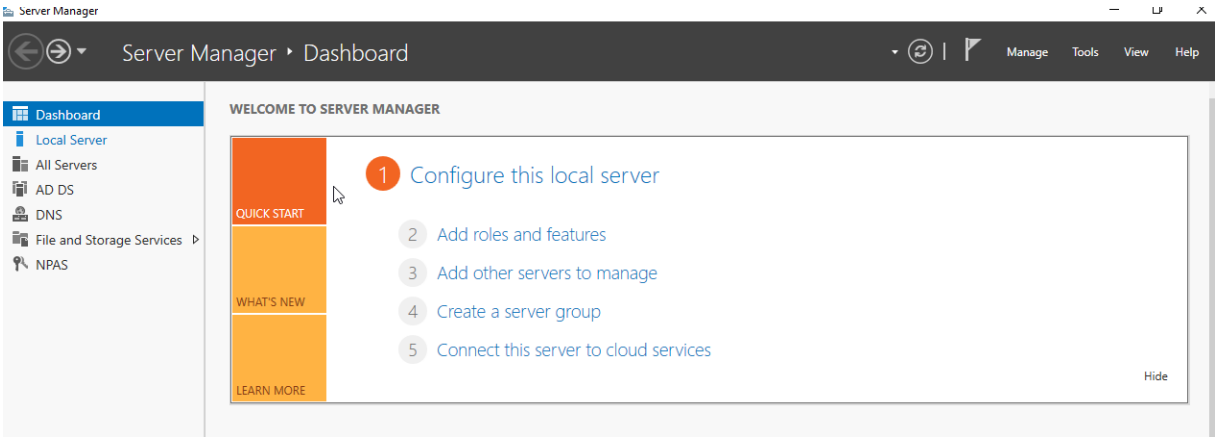

Windows Setup
Where do you want to install Windows?
Name
Total size
Free space
Type
Drive 0 Unallocated Space 60.0 GB 60.0 GB
Refresh
Delete
Format
New
Load driver
Extend
Next


Windows Setup
Installing Windows
Status
Copying Windows files
Getting files ready for installation (0%)
Installing features
Installing updates
Finishing up

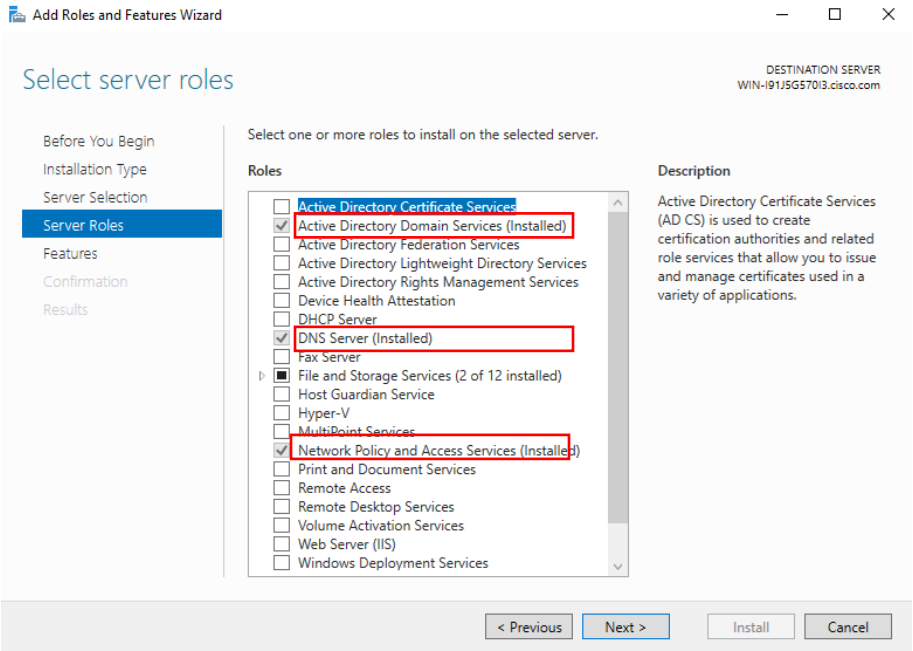

Windows Setup
Windows needs to restart to continue
Restarting in 6 seconds
Restart now


Customize settings
Type a password for the built-in administrator account that you can use to sign in to this computer.
User name
Administrator
Password
Reenter password
Finish

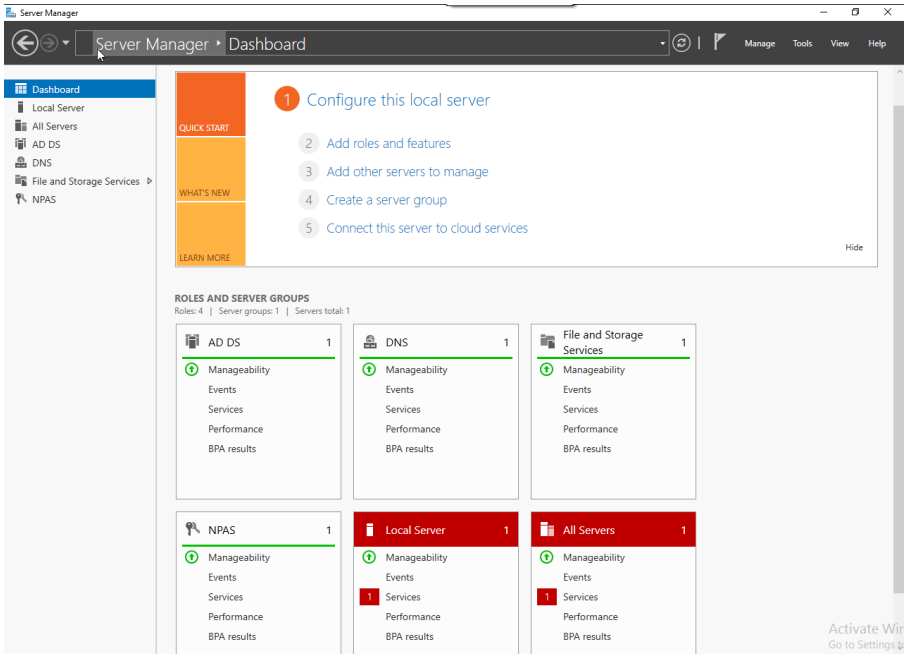

Press Ctrl+Alt+Delete to unlock.
9:06
Tuesday, January 31



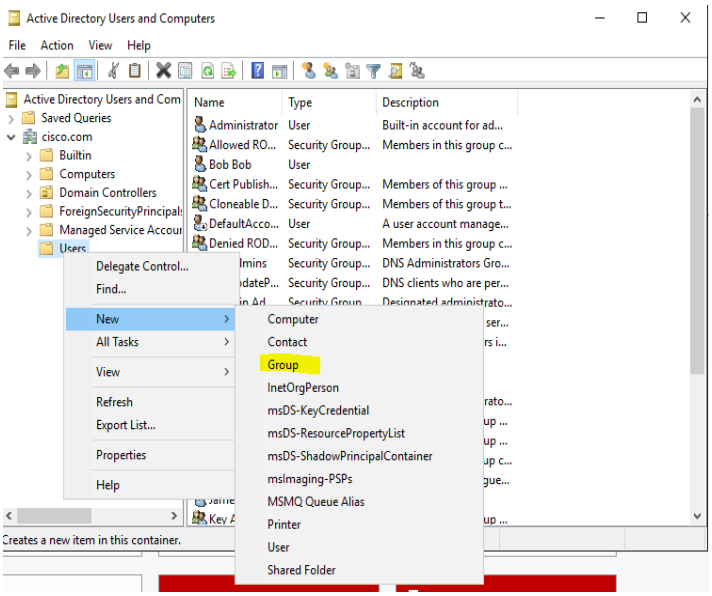

Once the initial Windows Server was setup, then I added the functionalities Active Directory, DNS Server, and Network Policy and Access Services to the server.

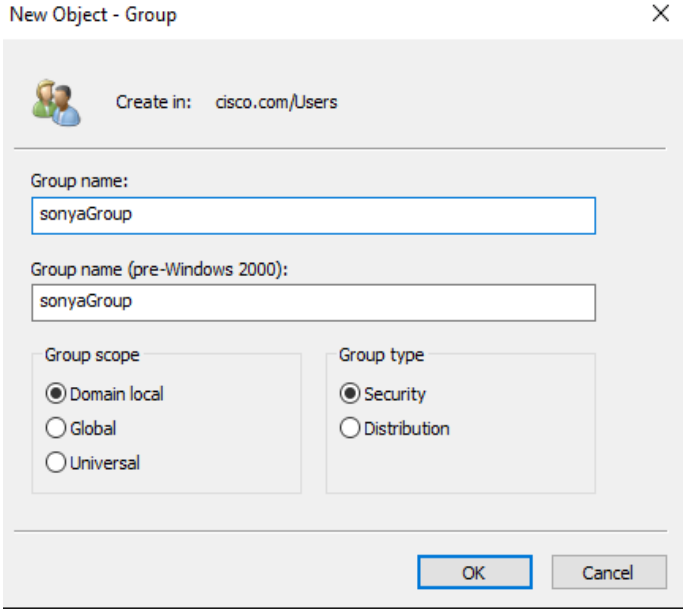


Once those functionalities were added to the server, they each became a different role of the server, as seen in the photo below. First, I entered the DNS properties page and created a domain, “cisco.com” (not pictured)

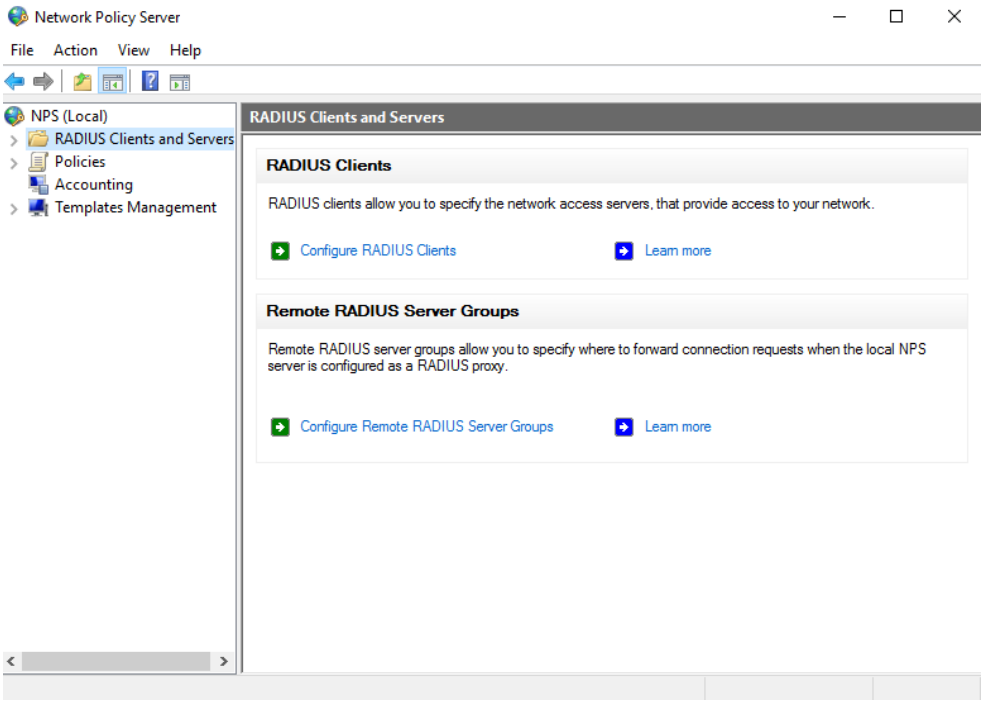


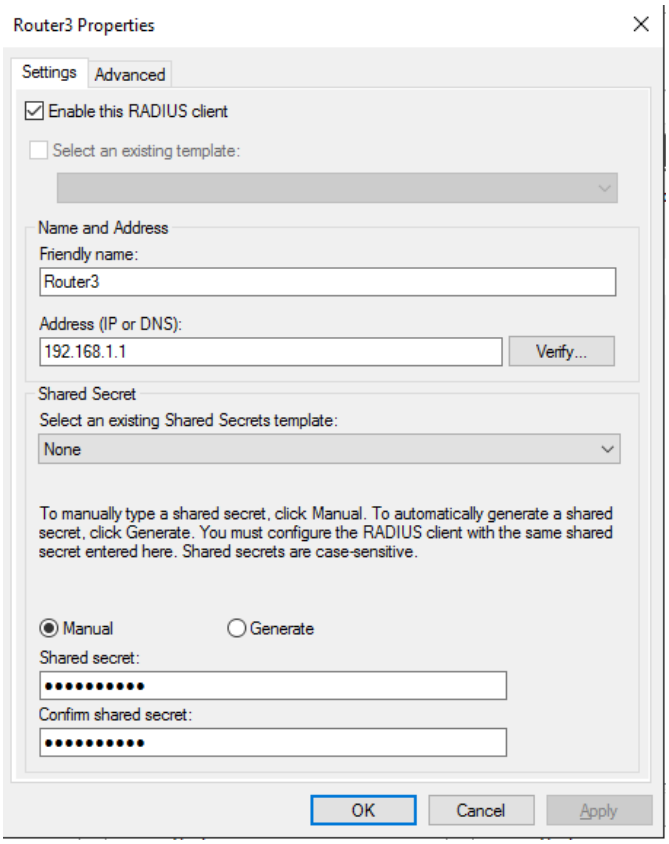

Next, I opened the Active Directory Users and Computers window to create a new security group. Once I have this group created in my domain, I can create a Network Policy that is applicable to this group.

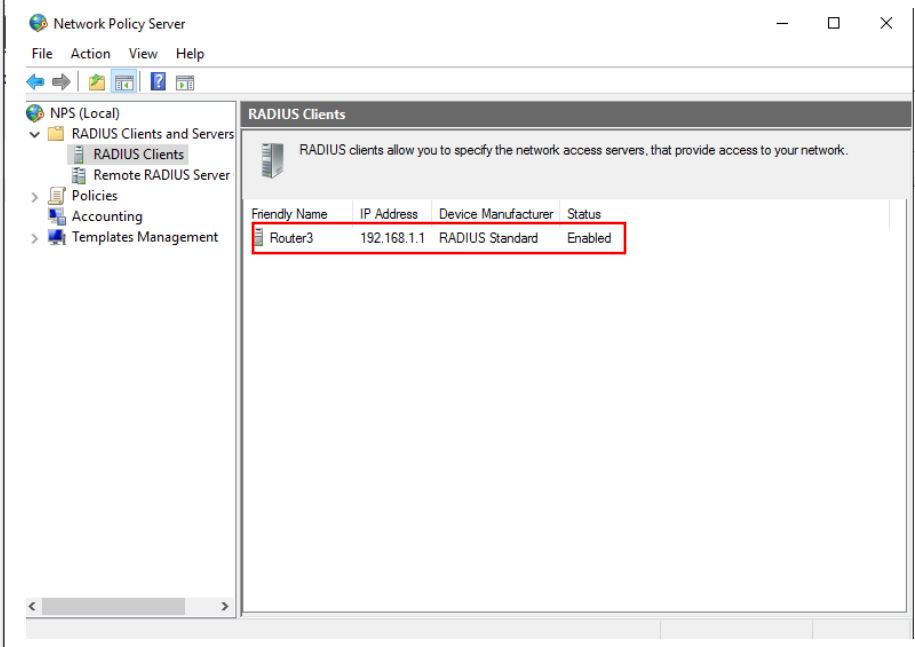


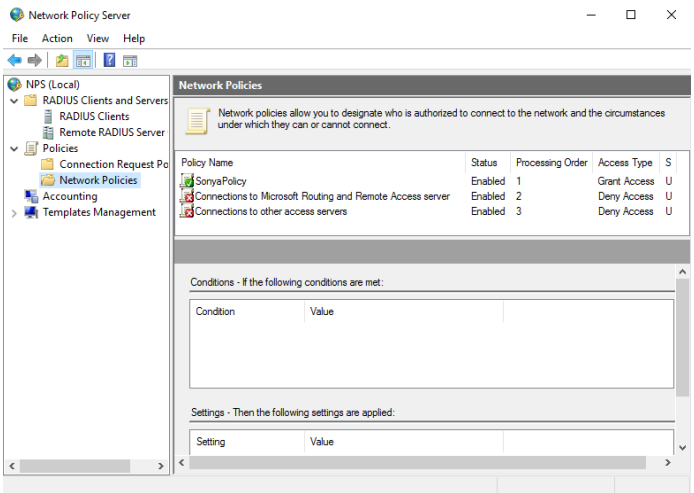



To create a network policy, I opened the Network Policy Server window. First, I added my router, 192.168.1.1 to be a RADIUS client with the shared secret key that I configured on my router. This ensures that the router recognizes this server, and vice versa.



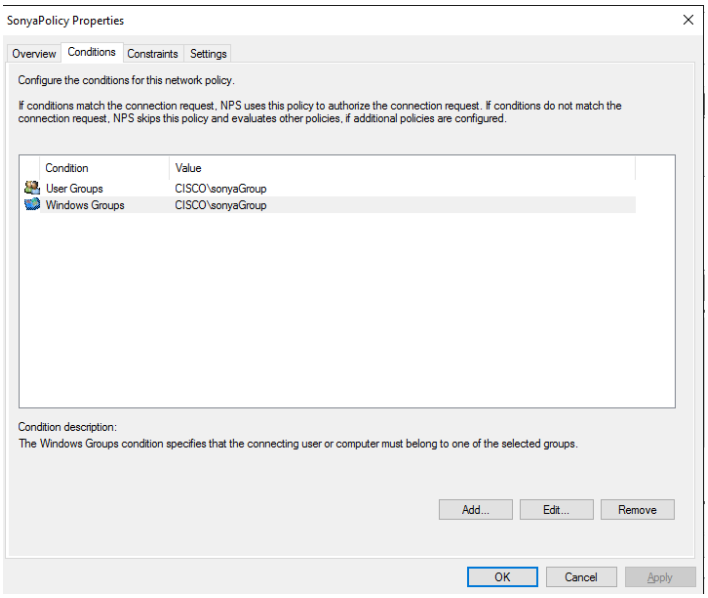



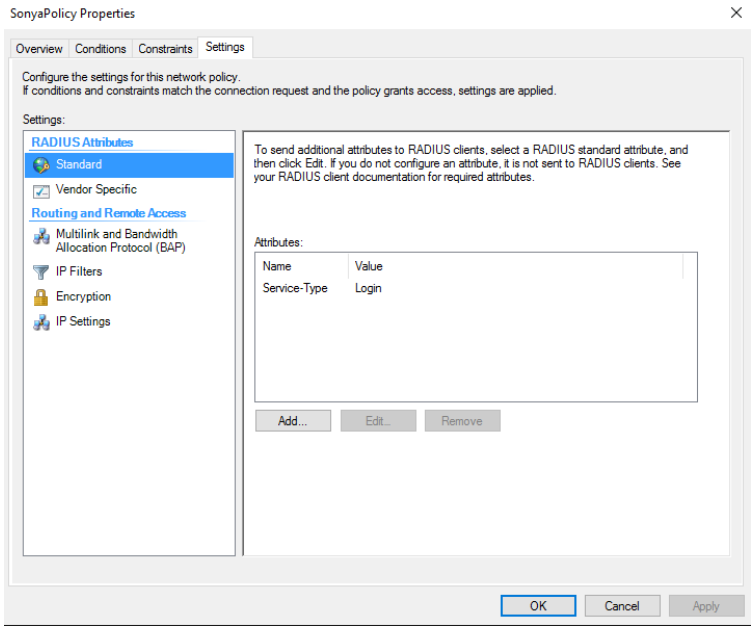






Once the router has been set as a RADIUS client on the server, I can now create a new Network Policy for the server.

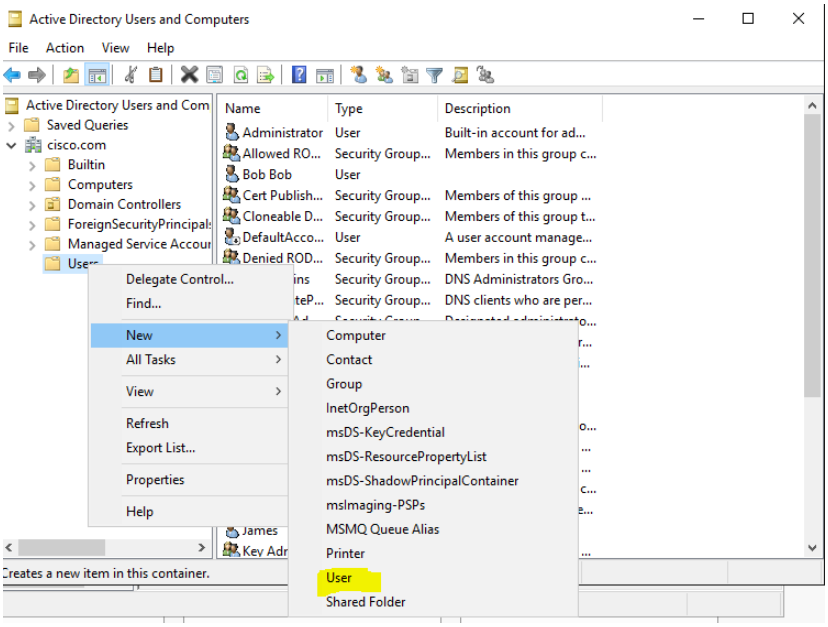
I named my policy “SonyaPolicy”. Under the Conditions tab, I set the settings to only allow users belonging to my newly created group, “sonyaGroup” access.

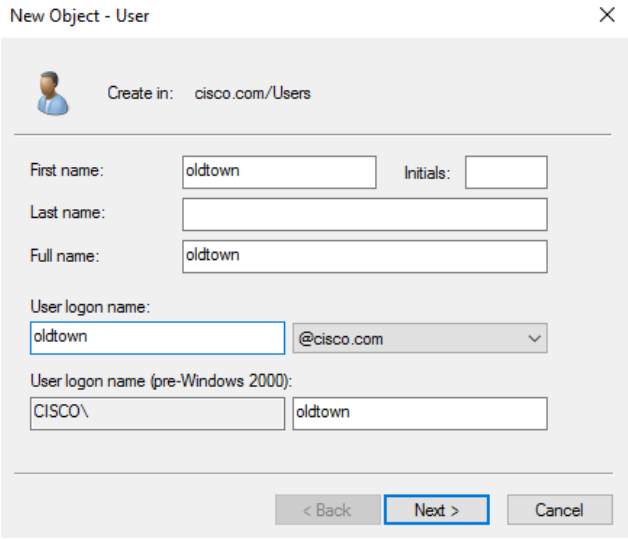



I kept the defaults in the Constraints tab, but in the Settings tab, I added an attribute “Service-Type” with the value of “Login”. This particular setting set the policy to be applicable for login, which is what I wanted.

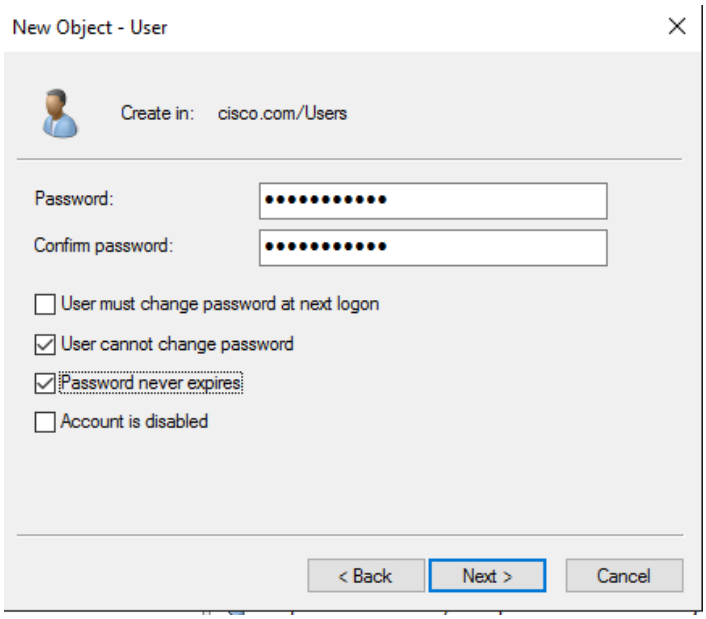
Next, I returned to the Active Directory Users and Computers window to create new users for my group.



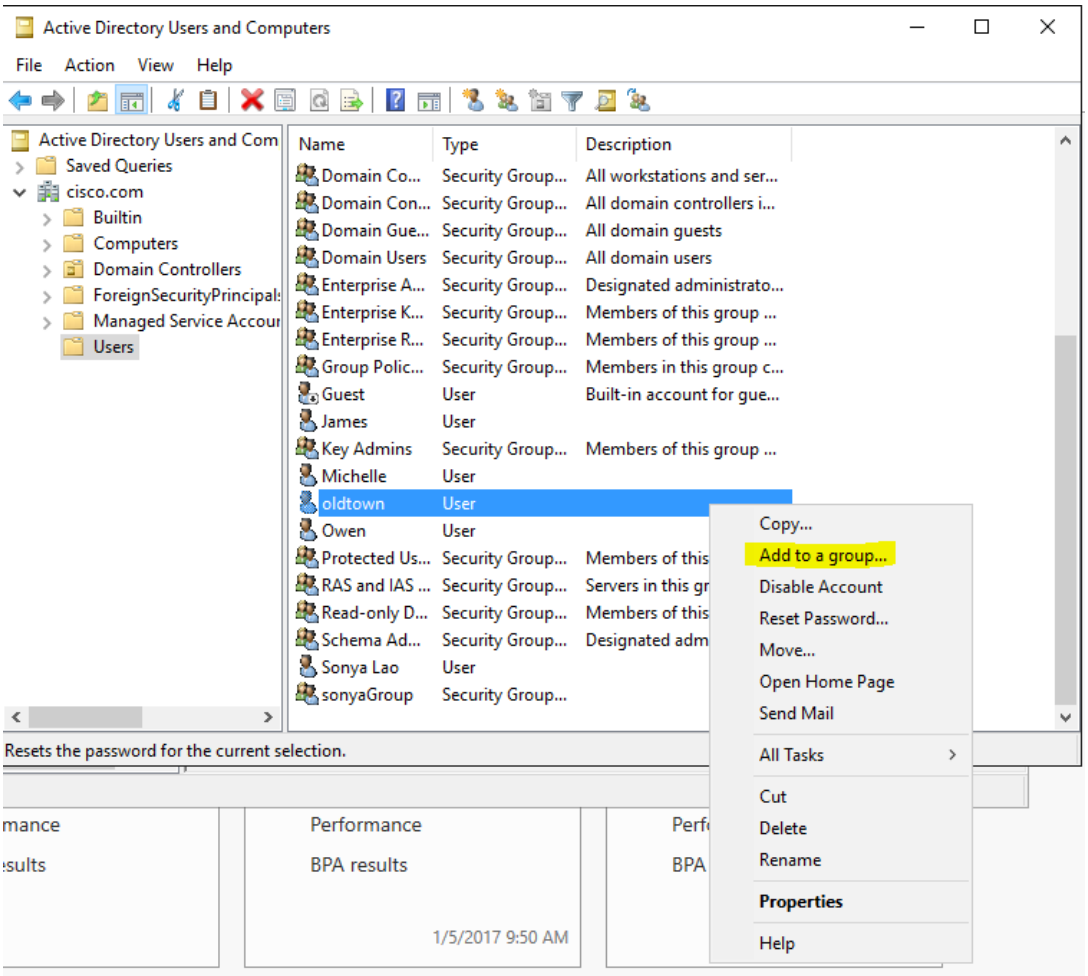



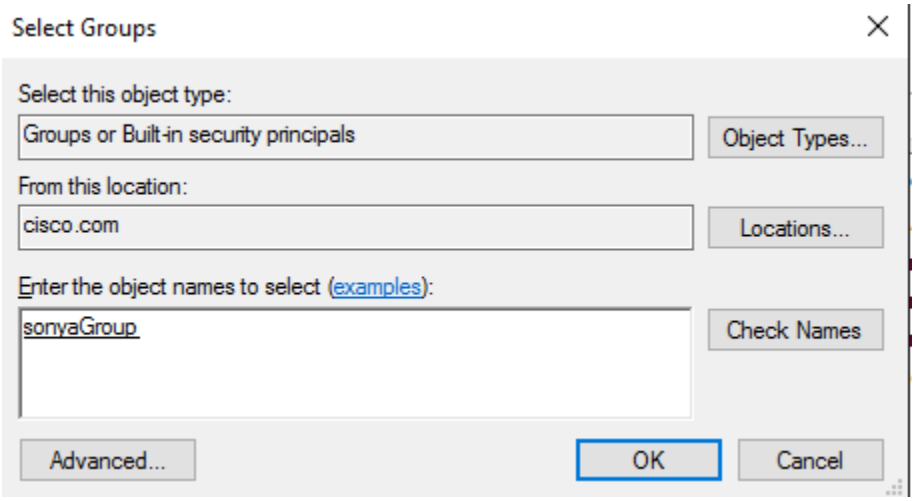

I created this user “oldtown” and checked to make sure it was in the correct domain that I created, “cisco.com”.

Next, I set the password for oldtown and made the password permanent for the user.



Lastly, I added the user “oldtown” to my group, “sonyaGroup”. I repeated this step multiple times, creating several new users, and adding them to my Security group.



# Problems

After conducting much research online, I found several video tutorials that seemed to suit my needs. I began to follow the tutorials, but soon realized that in each one, there was a special quirk that was not applicable to my lab situation. As a result, I was left halfway through the setup of a new user in the Active Directory User and Services, and had to guess the rest of the steps. Later on, I realized that I never placed the user in a group or under the same domain as the router and had to spend time re-creating a new user and server group.

In addition, once I thought I had everything setup, I tried to ping from my router to the server to no avail, even though everything had been correctly configured. After asking my peers and looking online, I realized that when I first setup the Windows Server virtual machine, I did not choose the setting that allowed for a bridged network. Once I changed the setting for networks to be bridged, then I had connectivity without any problem.

After I believed I had a working setup for AAA, I tried logging in to my own router, to no success. After much trouble shooting, examining my Network Policy and trying to add new users to my server group, I discovered that I had not added a service type in my policy that was specific to login. After that small change was made, I was able to successfully login with any user that was in my security group.

# Conclusion

AAA is a very powerful tool for authentication. It centralizes the user information to be stored on the server and minimizes the chances for an information breach. I could see how this technology could be important for businesses in the real world. I am also grateful for the exposure to Windows Server, as it is a valuable skill to know. I know that in the future, AAA will only become more important, as hackers find new and more advanced ways to breach a network.