

Aia Al-Qasab

Smart Server management (WINDOWS / LINUX)

Server Remote management project plan

Report
Advanced Server development project

2018



South-Eastern Finland
University of Applied Sciences

CONTENTS

1	INTRODUCTION TO SERVER MANAGEMENT	3
2	SMART SERVER MANAGEMENT	5
2.1	Hardware and Software dependencies:.....	6
2.2	Virtual Machine:	6
2.3	Server Configuration.....	7
2.3.1	Windows Server Features	7
2.3.2	Linux Server Features.....	8
3	Servers Configuration (Practical)	9
3.1	Windows Server Configuration.....	9
3.2	Linux Server configuration.....	83
3	CONCLUSION.....	115
	REFERENCES	116

1 INTRODUCTION TO SERVER MANAGEMENT

The cost and complexity of system tuning, and management is leading numerous enterprises to offload their IT demands to hosting/data centers, these hosting centers are making a considerable investment in procuring and operating servers to take on these demanding loads. The growing importance of energy/power consumption of these servers at hosting centers in terms of the electricity cost to keep them powered on, as well as in the design of extensive cooling systems to their operating temperatures within thermal stability limits for server components. Windows Server has powered a generation of organizations, from small business to large enterprises. Customers want to access their applications in a variety of ways and be confident that they can complete their daily tasks in a secure and efficient manner. They simply are not concerned about how IT infrastructures are made up and the challenges that team's supporting these environments experience basis. Windows Server developing the Servers with new features every year, the latest one is Windows Server 2019 that built on the strong foundation of Windows Server 2016 which continues to see great momentum in customer adoption. Windows Server 2016 is the fastest adopted version of Windows Server that required to spend a lot of time with customers to understand the future challenges and where the industry is going. Four themes were consistent: Hybrid, Security, Application platform, and Hyper-converged infrastructure. Hybrid cloud scenarios one that combines on premises and cloud environments working together, that make sense to customers. Extending Active Directory, synchronizing file servers, and backup in the cloud. It also allows for apps running on premises to take advantage of innovation in the cloud such as Artificial Intelligence and IoT. Hybrid cloud enables a future proof, long term approach which plays a central role in cloud strategies for the foreseeable future. Security continues to be a top priority for Windows customers, the number of cyber-security incidents continue to grow and the impact if these incidents is escalating quickly. Application Platform two key aspects to call out for the developer community are improvements to Windows Server containers and Windows Subsystem on Linux (WSL). Tens of millions of container images have been downloaded from the Docker Hub, Windows team had learned from feedback that a smaller container image size will significantly improve experience of develop-

ers and IT pros who are modernizing their existing applications using containers. The goal with Windows Server 2019 to reduce the server core base container image to a third of its current size of 5 GB, this will reduce download time of the image by 72% further optimizing the development time and performance. Hybrid- converged infrastructure (HCI) is one of the latest trends in the server industry today, it market grew 64% in 2016. This trend is primarily because customers understand the value of using x86 servers with high performant local disks to run their compute and storage needs at the same time, also HCI gives the flexibility to easily scale such deployments.

Ubuntu Server 18.04 LTS introduces a new installer, the “live server” installer called Ubiquity for Servers which provides a more user friendly and faster installation experiences, at the time of writing it only supports amd64 processors and does not support LVM or RAID or other more sophisticated storage options, nor does it support reusing existing partitions on the disks of the system that installing. It also requires access to the Ubuntu archive via a proxy. The Server Edition provides a common base for all sorts of server applications, it's a minimalist design providing a platform for a desired services such as file/print services, web hosting, email hosting. There are few differences between the Ubuntu Server Edition and the Ubuntu Desktop Edition, they both use the same apt repositories, making it just as easy to install a server application on the Desktop Edition as it is on the Server Edition. The differences between the two editions are the lack of an X window environment in the Server Edition and the installation process. Ubuntu version 10.10 and prior, had different kernels for the server and desktop editions, Ubuntu no longer has separate server and generic kernel flavors. These have been merged into a single generic kernel flavor to help reduce the maintenance burden over the life of the release.

2 SMART SERVER MANAGEMENT

In this project, it's important to build a virtual machine to manage and configure the server remotely by using features and tools, also provide high security level.

The smart server manager (Standard, Monitor, Automate, Review, Test) is a free server system management solution for IT professionals to monitor and receive proactive email alerts in the event of any system failure (hardware/software). This powerful solution connects seamlessly to server via the on-board BMC (based board management controller).

BMC is a specialized service processor that monitors the physical state of a computer, network server or other hardware device using sensors and communicating with the system administrator through an independent connection. BCM is part of the intelligent platform management interface, usually it's contained in the motherboard or main circuit board of the device to be monitored. The sensors of a BMC measure internal physical variables such as temperature, humidity, power supply voltage, fan, speeds, communications parameters and OS functions. If any of these variables happens to stray outside specified limits, the administrator is notified.

Smart Server Manager can also be set to send email alerts to IT administrators in the event any of these monitored components experience a technical issue. It includes operating system monitoring for Windows/Linux platforms, and virtual machine performance monitoring, within OS monitoring users can view the status and remotely trouble running processes and applications, as well as view the system resource status of the hardware being used by the given OS.

Smart Server Manager monitors Virtual Machines VMs via its VM management function and supports VMs from both VMware and Microsoft Hyper-V, the management tool allows for the performance of the VM hosts and guest OS to be monitored to the component is becoming a bottle neck, thereby allowing IT administrators to determine whether to allocate more hardware resources to the VM.

SSM is 100% agentless, meaning that it only needs to be installed once on a core system, and then all other servers on the network can be monitored and no additional installation required. The system can support up to 250 devices including physical hardware, OS and VMs.

2.1 Hardware and Software dependencies:

Minimum hardware requirements for SSM installation:

- System processor 2 GHz
- System memory 2 GB RAM
- Free disk space 4 GB (more disks space need depending in the nodes management and the amount of history information needed)
- BMC chip for remote manageability.

Minimum Software requirements for SSM installation:

- Windows Server last version 2019
- Linux Server 18.04.1 LTS

Smart Server Manager should be run across a gigabit Ethernet network dedicated to system management and the first Ethernet port used by the operating systems deployed. It's recommended to route the OS connection from NIC 1 along the BMC port to ensure maximum bandwidth and functionality.

2.2 Virtual Machine:

VMware Server is a free virtualization product for Microsoft Windows and Linux servers. It enables users to quickly provision new server capacity by partitioning a physical server into multiple virtual machines, it's used to provision a wide variety of plug and play virtual applications for commonly used infrastructure.

Features of VMware Server:

- Support for 32-bit and 64-bit Guest Operating system.
- Two-Way virtual SMP (Symmetric Multiprocessing) experimental support.
- Connect to VMware GSX virtual Machines and Hosts.
- Upgrade and use GSX Virtual Machines.
- More existing virtual machines.
- Compatible with VMware workstation virtual machines.
- Configure virtual hardware devices to be automatically detected.
- Take and revert to snapshots in the background.
- Support for VMware virtual machine importer.
- Support for VirtualCenter.

2.3 Server Configuration

2.3.1 Windows Server Features

Windows Server has over 300 new features and connectivity with the cloud. Explaining those features will take much time, but in this project it will include the most important features that needs to be installed. Cloud Technology was intended with Windows Server, it's the practice of using a network of remote servers to store, manage and process data rather than local server. Windows Server extends these technologies to corporations to be used in the same way for their employees. All corporate data using either virtual machines or individual workstations can be backed up directly to the cloud either on or off site, Cloud technologies are the driving force for the way the world conducts business today and in the future.

Windows configuration's part will include:

- Active Directory, DNS and Name Resolution in Windows Server.
- Smart Card Certificate
- Dynamic access control: File shares, Reimagined.
- Web Server Management with IIS.
- VPNs.
- Server Virtualization with Hyper- V
- Patch management.
- Web Server Management with IIS.

Active Directory is in many ways the keystone piece of Windows networking, the central database of user and machine authentication data. ADs include several useful new capabilities for Active Directory Certificate Services, Active Directory Rights management services and Active Directory domain services. The feature focus on deployment and manageability, it's making fast and easy to deploy AD services and to have more flexibility accessing files with better security.

Also by configuring Virtualization, it allows to put multiple computer operating systems in one physical machine. Breaking one physical server up into a bunch of virtual machines is one of the most significant changes in server management in the past. By installing Hyper –V features, client hyper –v gives

desktop Windows Hyper –v technology without the need for installing a server OS, also Hyper –V module for Windows PowerShell provides more than 160 cmdlets to manage Hyper –V.

Servers are not good without the ability to talk to one another but being able to communicate with other systems means that infected systems and can be unsecure. IP address management framework is a set of technologies for managing, monitoring and auditing IP address space. By monitoring DHCP and DNS, IPAM can locate IP address servers within a network and allows user to manage from a single central UI.

Remote Server management is one of the challenges to access and control servers between sites, it require more security features and policies to configure, VPN feature used to provide access to a private network over a public network. It's a private connection that is created over a public network such as the Internet, Windows Server Remote Access role enables the traditional Routing and Remote Access Service features, but it get a massive upgrade with the enhanced Direct Access functionality that also comes bundled with this role.

2.3.2 Linux Server Features.

The secure Shell tools are a set of client and server applications that all the administrator to do basic communication between client computers and Linux Server, the tools includes ssh, scp, sftp, and many others. Because communication is encrypted between the server and the clients, these tools are more secure than similar, older tools.

With Secure Shell tools, both the authentication process and all communications that follow are encrypted. Communications from telnet commands expose passwords and all data to someone sniffing the network. Telnet is only used for testing access to remote ports or doing other tasks that don't expose the private data.

In this part of the project, Linux will be configured with more advanced security features, because many Windows server programs are designed around

proprietary or semi proprietary Microsoft protocols, or provide extended features that can be accessed from Microsoft clients. Linux servers must necessarily either play catch up or use alternative protocols.

And because Linux doesn't run the popular Windows programs except under emulators, file format compatibility may be an issue.

Linux configuration's part will include:

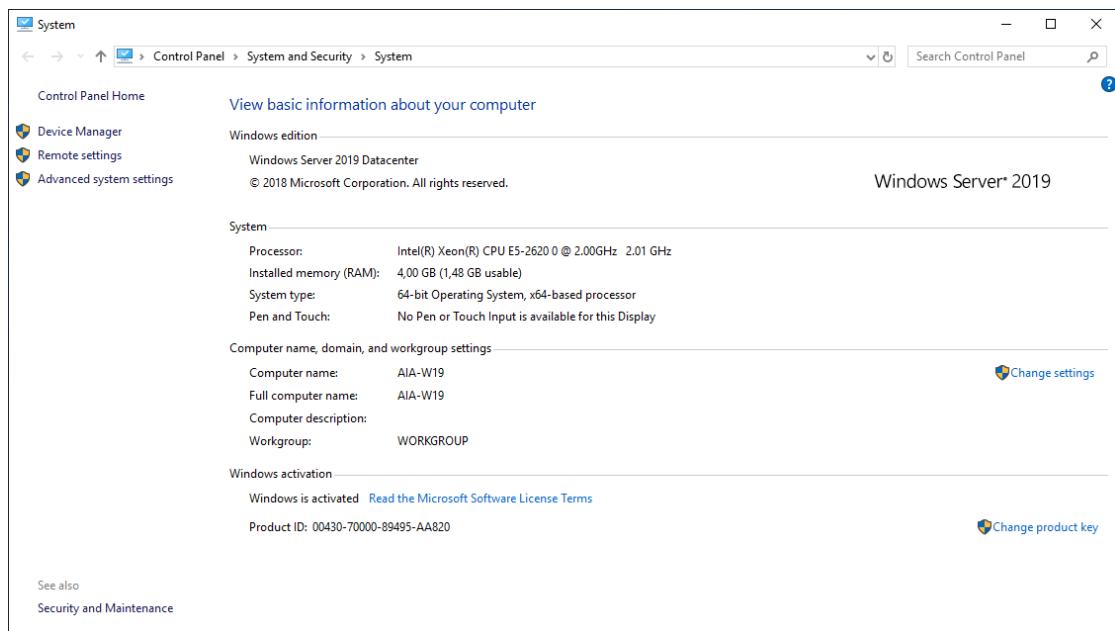
- Configuring System logging.
- Administering Networking.
- Starting and Stopping Services.
- Configuring a Web Server.
- Configuration an FTP Server.
- Advanced Linux Security.
- Enhancing Linux Security with SELinux.

3. Servers Configuration (Practical)

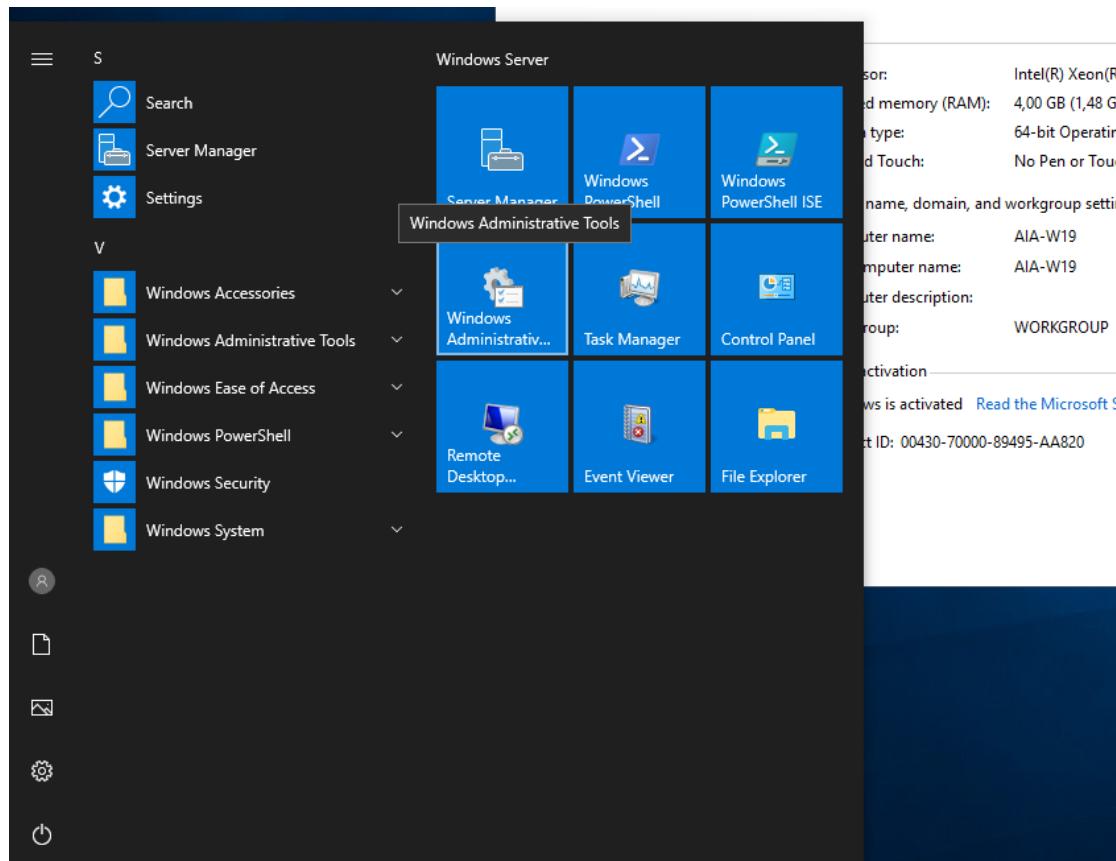
3.1 Windows Server Configuration

➤ Active Directory DNS and Name Resolution in Windows Server:

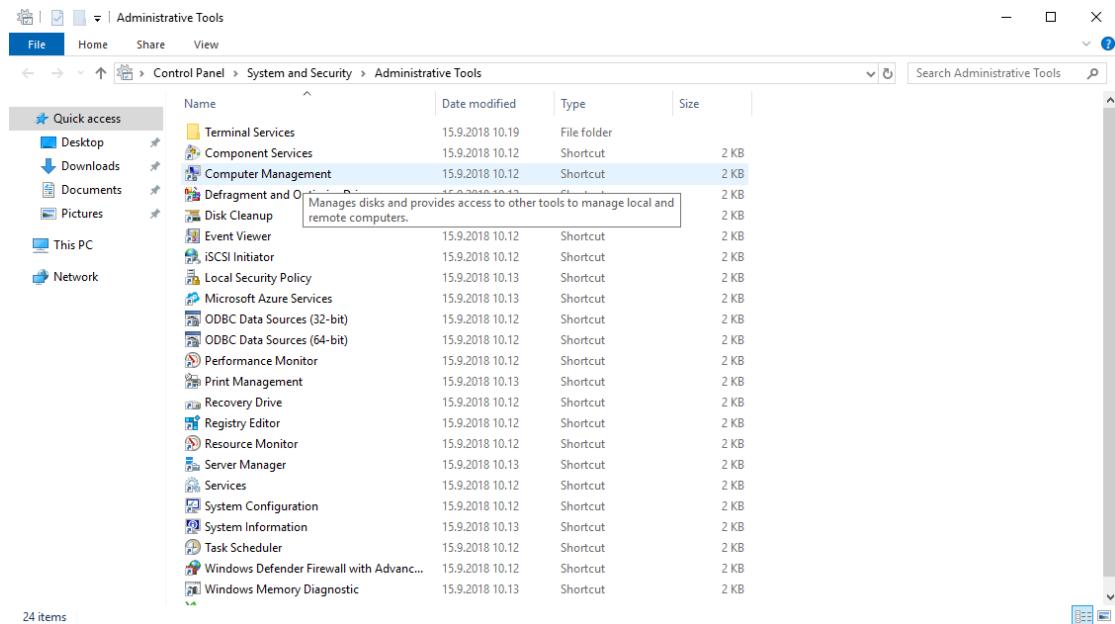
Right-click on **This PC** in your start menu and select **Properties**. If it's activated, you'll find it saying "**Windows is activated**" and you'll see the product key. If it says Windows is not activated you'll need to enter your key.



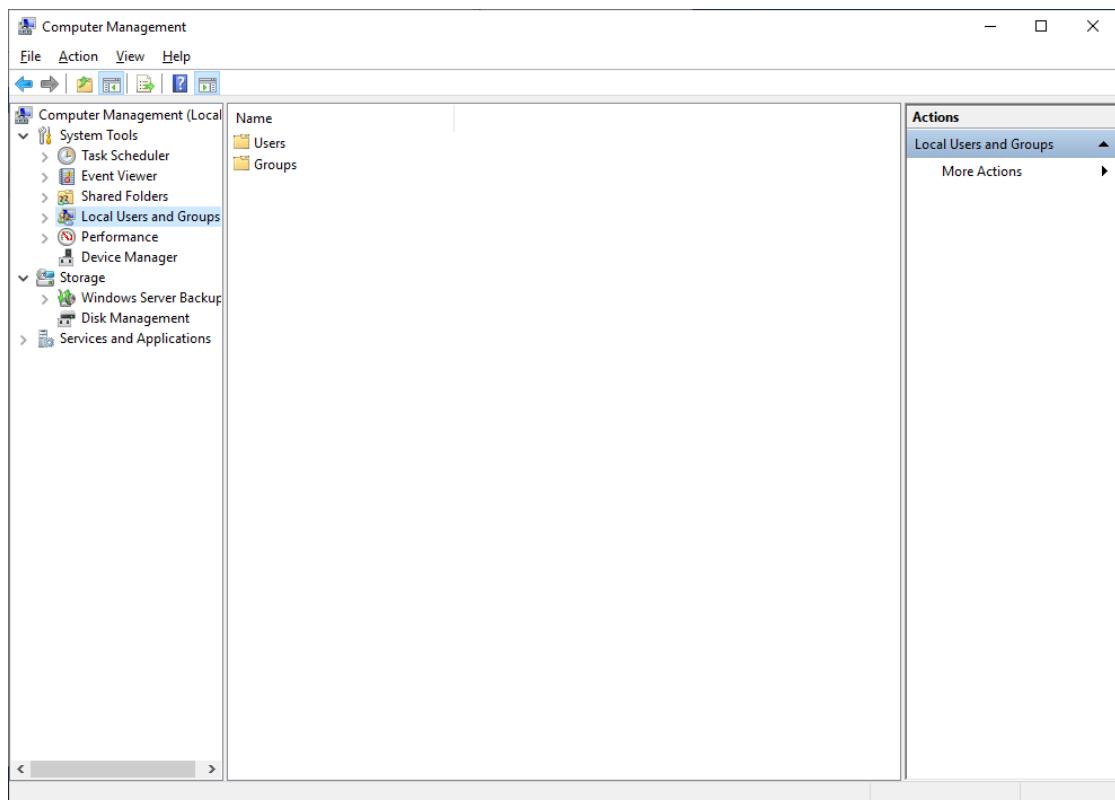
Open **Administrative tools** from your Start menu to set a password for administrator access.



Open **Computer Management**.



Select **Local Users and Groups** from the left pane and then double-click on the **Users** folder.

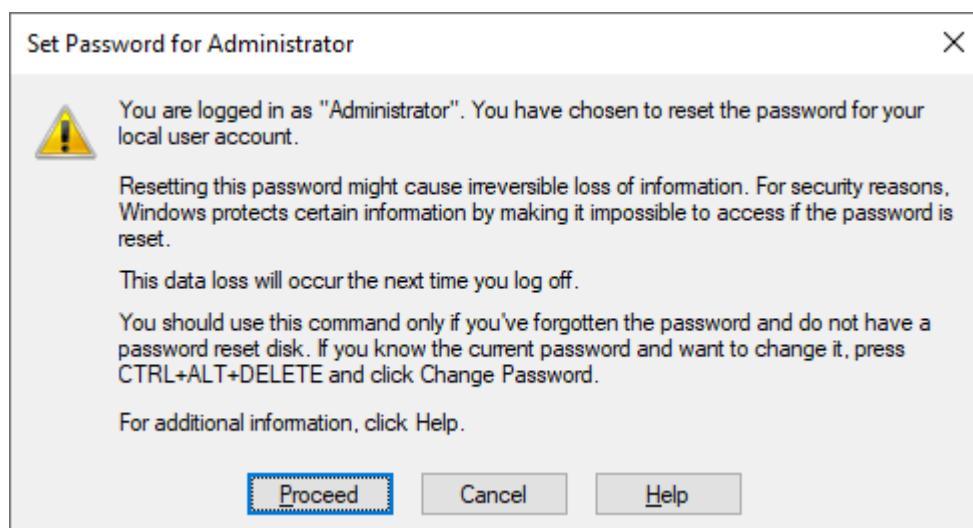


Right-click on **Administrator** and select **Set Password P@ssw0rd!**

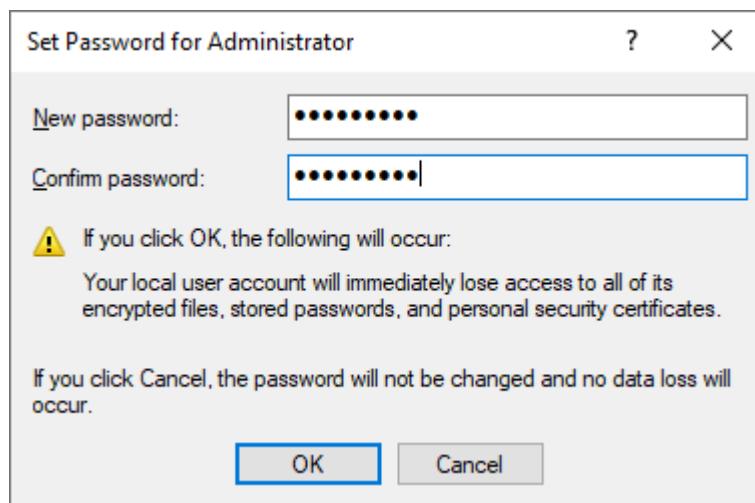
Management

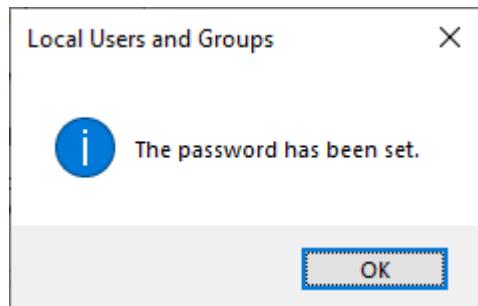
View Help

The screenshot shows the Windows Server Management Console. On the left, there's a navigation pane with various management tools like Tools, Scheduler, and Users. The 'Users' option is selected. In the main pane, a table lists user accounts: Administrator, Default, Guest, and WDAG. The 'Administrator' row is selected, and a context menu is open over it. The menu options are: Set Password..., All Tasks, Delete, Rename, Properties, and Help. The 'Properties' option is highlighted.

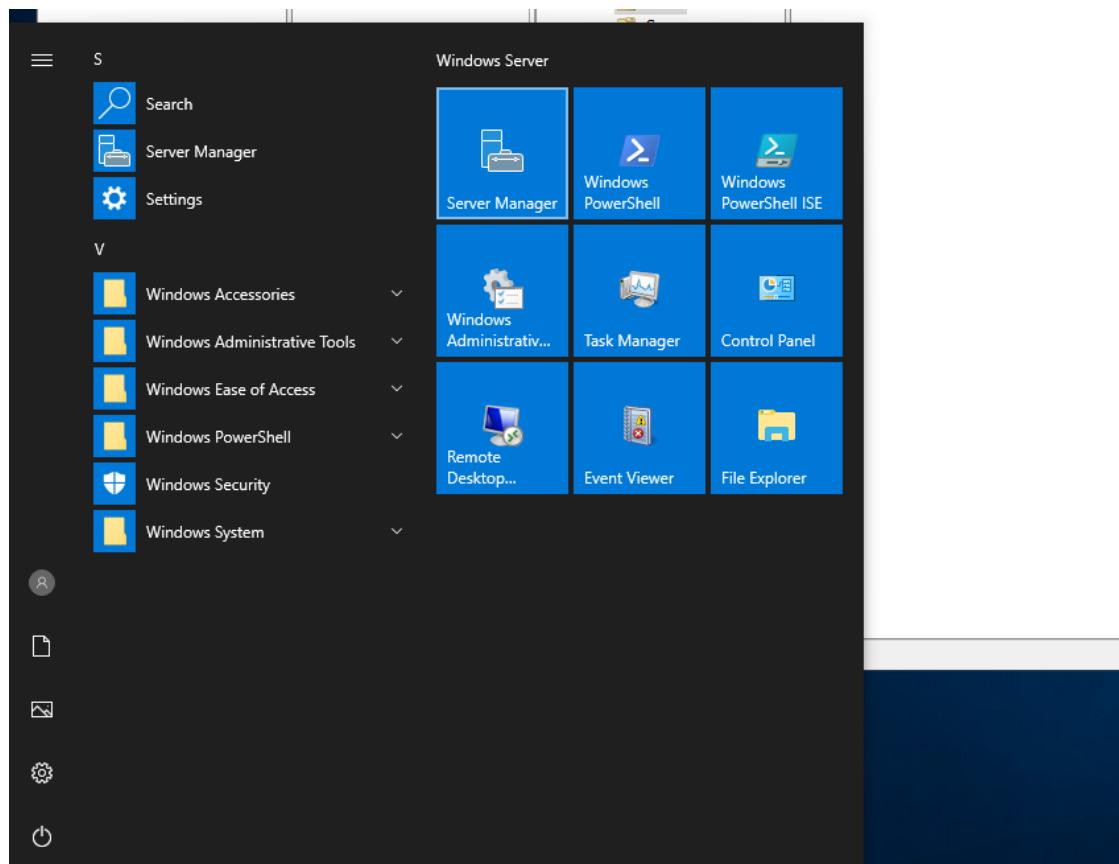
Click Proceed.

Enter and confirm your password. It must contain 8 characters at least, a combination of letters, symbols and numbers.

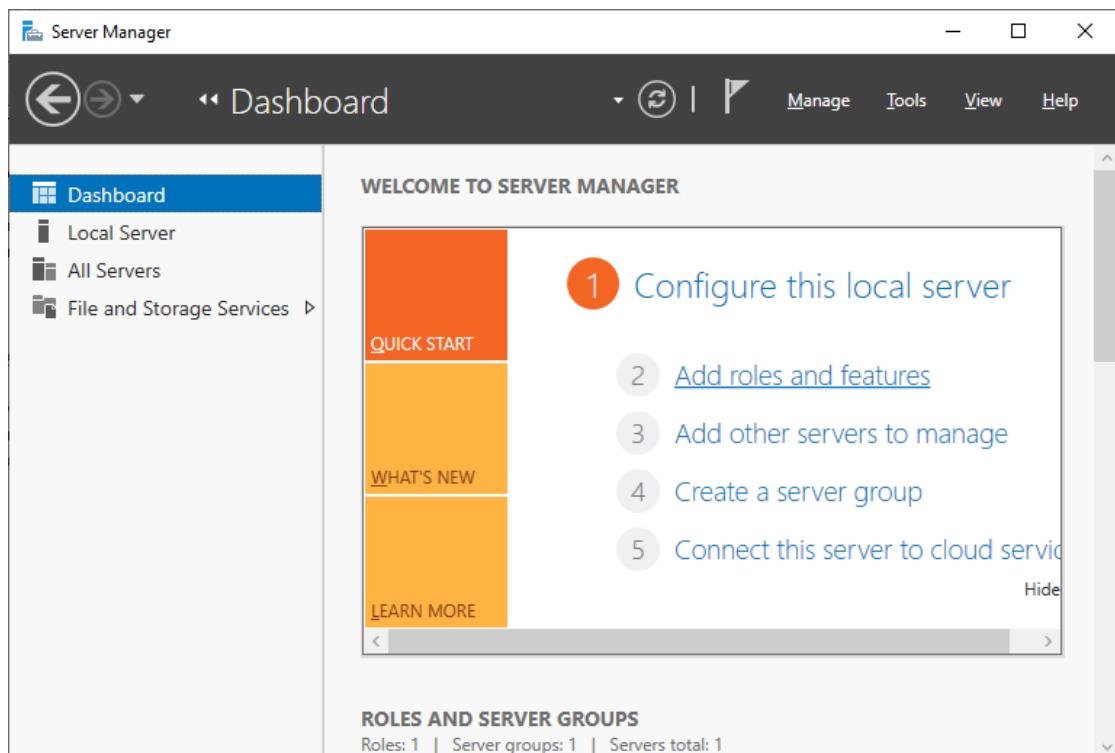




Open **Server Manager** from your taskbar or Start menu.

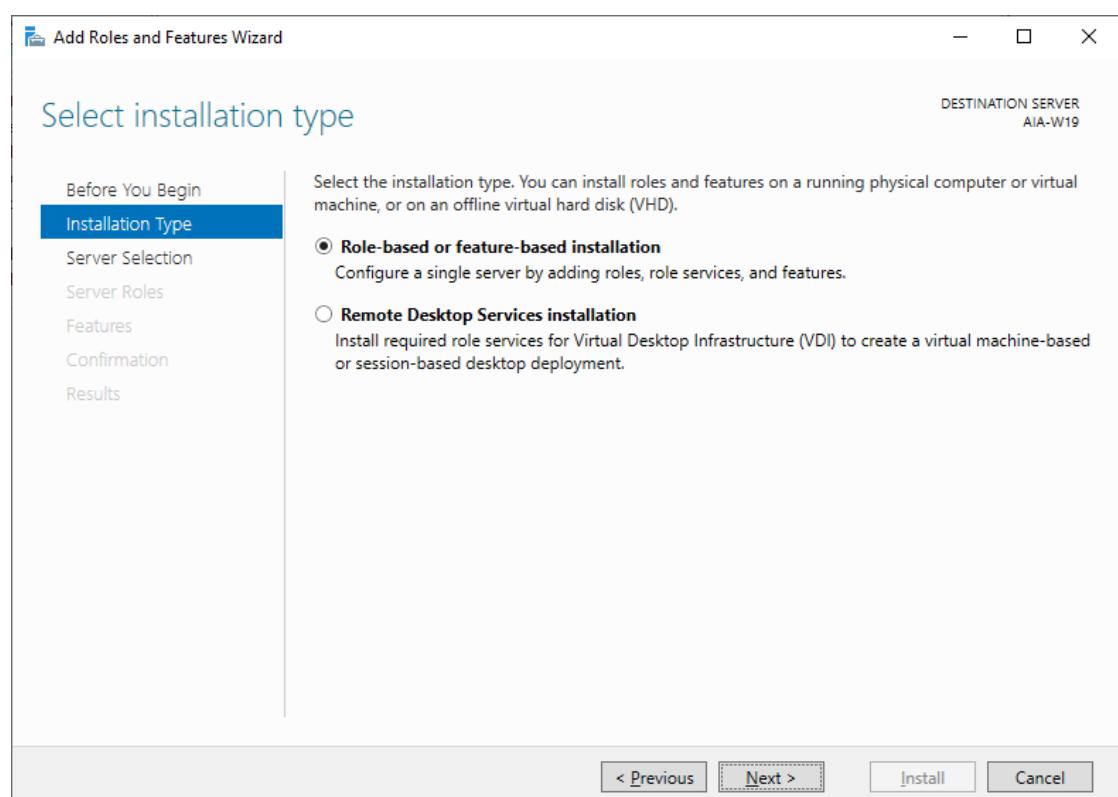


Click **Add roles and features**.

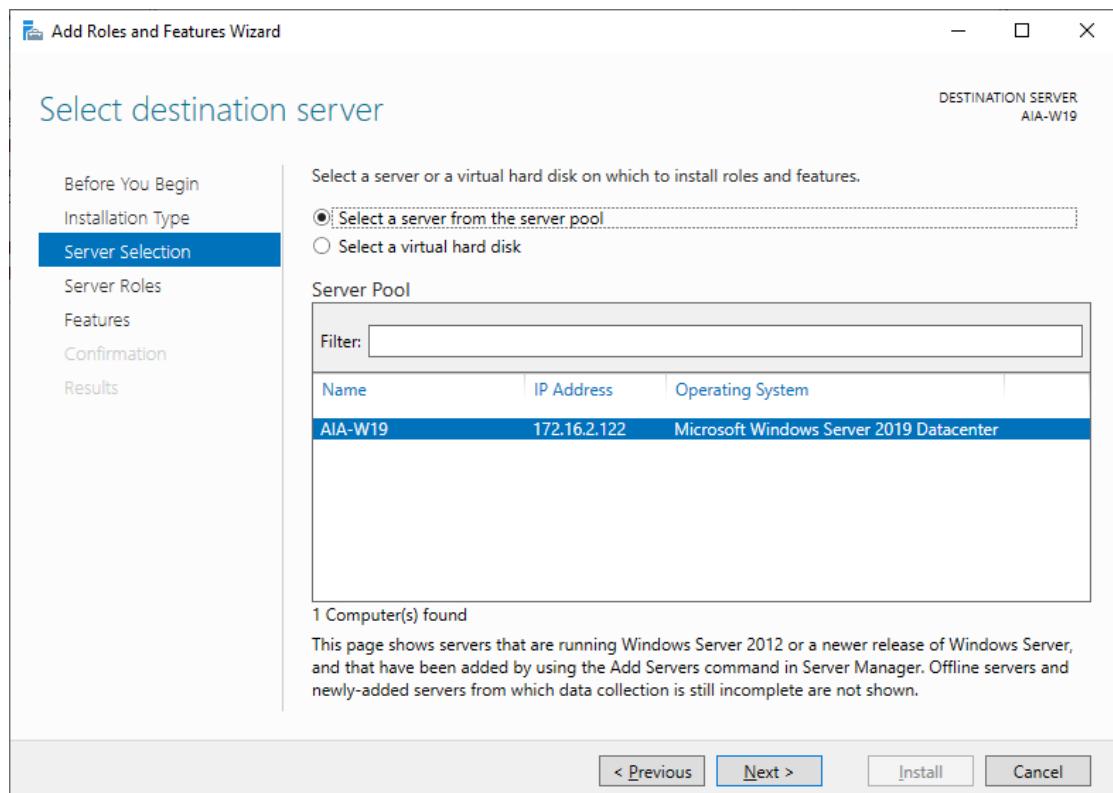


Click **Next**.

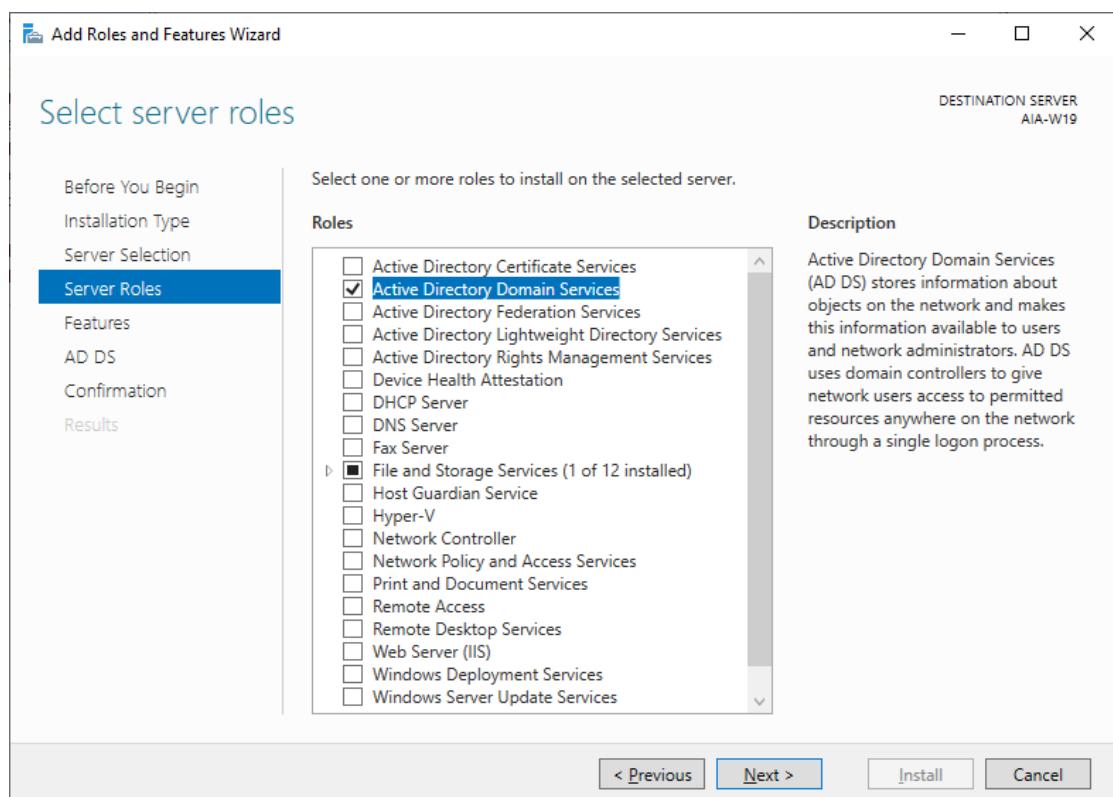
Leave it as it is by default (**Role-based or featured-based installation**) and click **Next**.

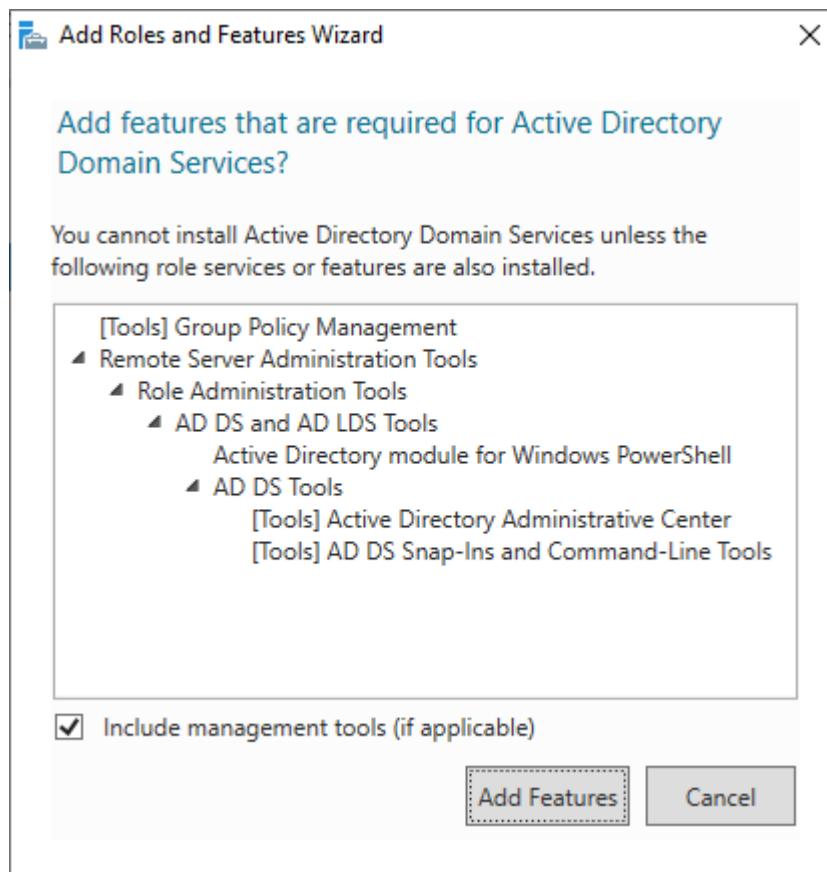


On the **Server Selection** page, you'll find the **Select a server from the server pool** and the default server there. Select it and click **Next**.

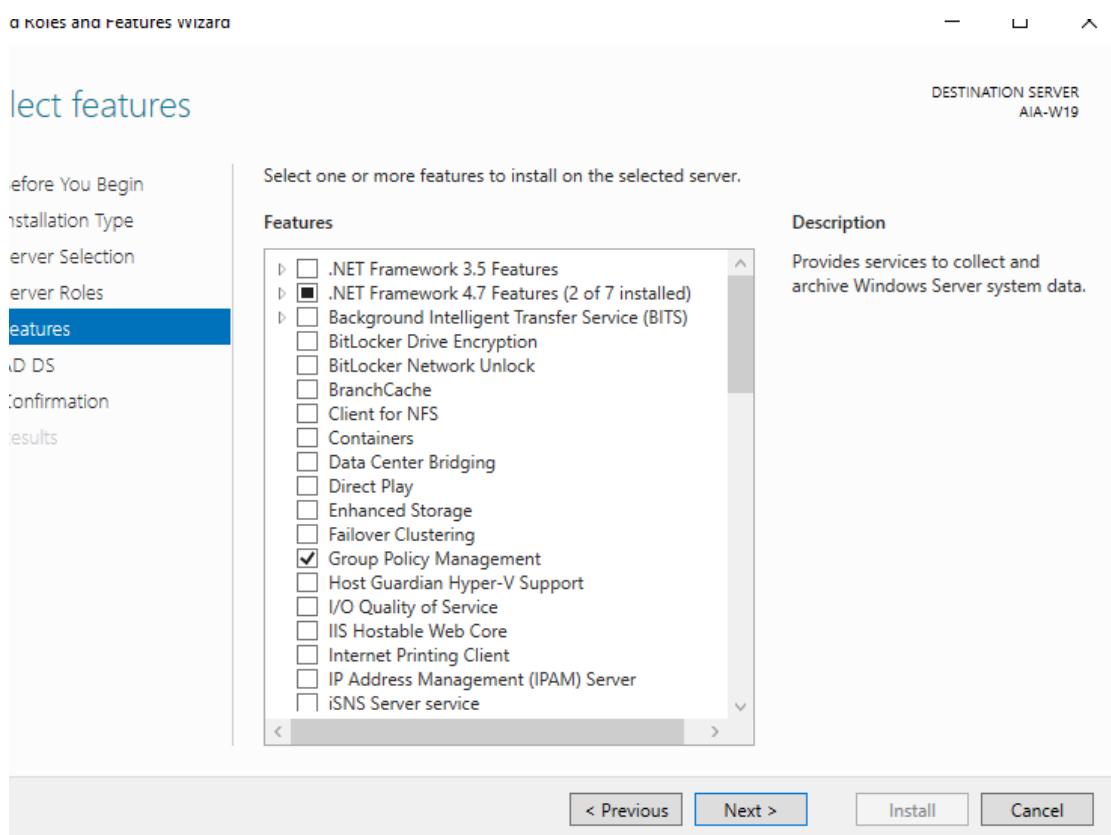


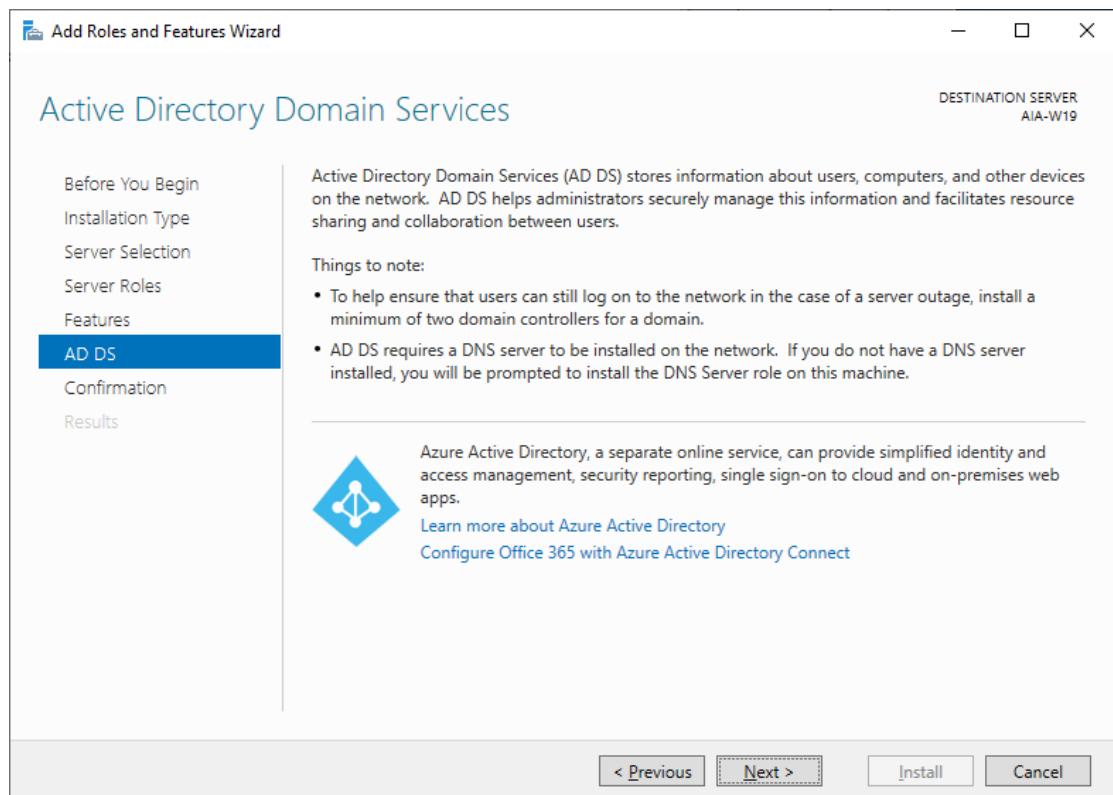
Check Active Directory Domain Services and add feature



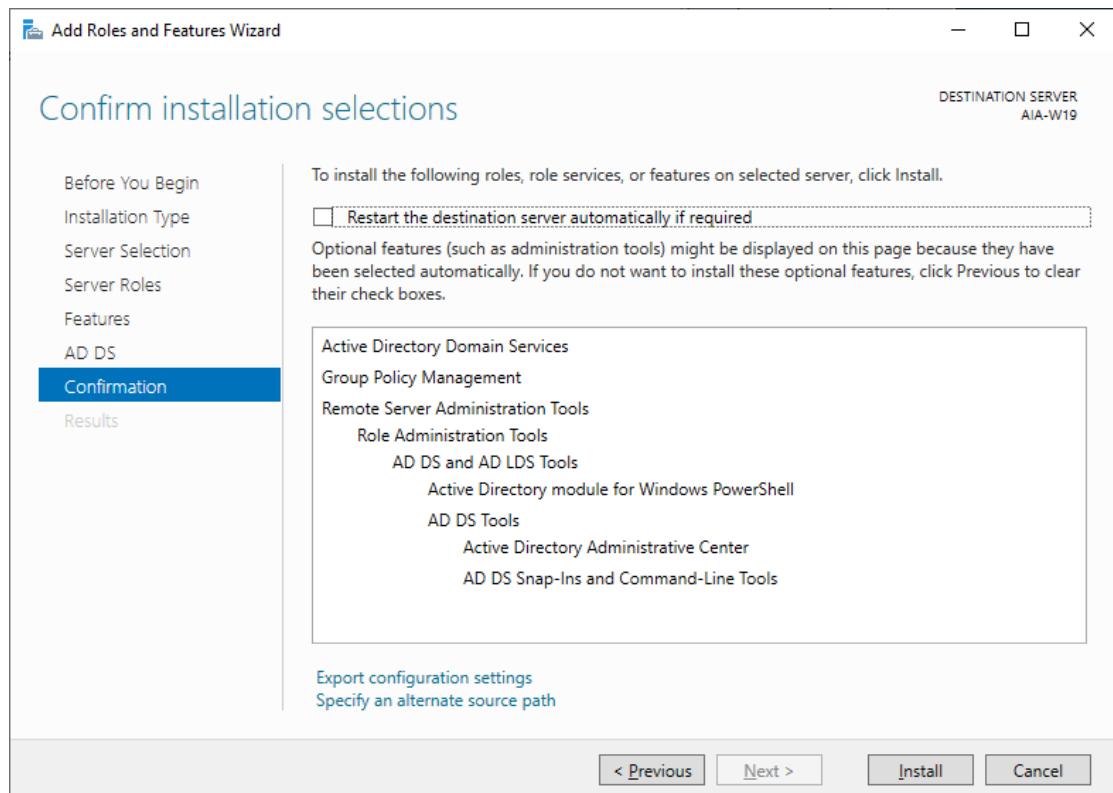


Now once checked, click **Next** and make sure **Group Policy Management** is checked and click **Next**.

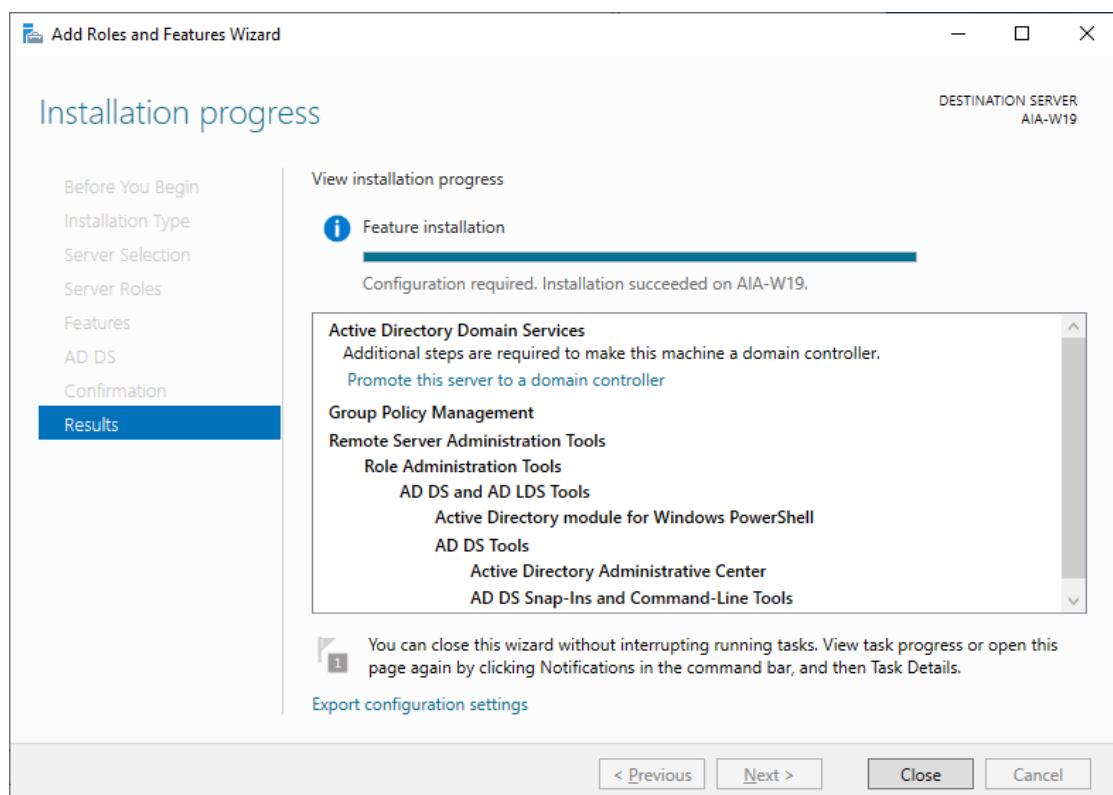
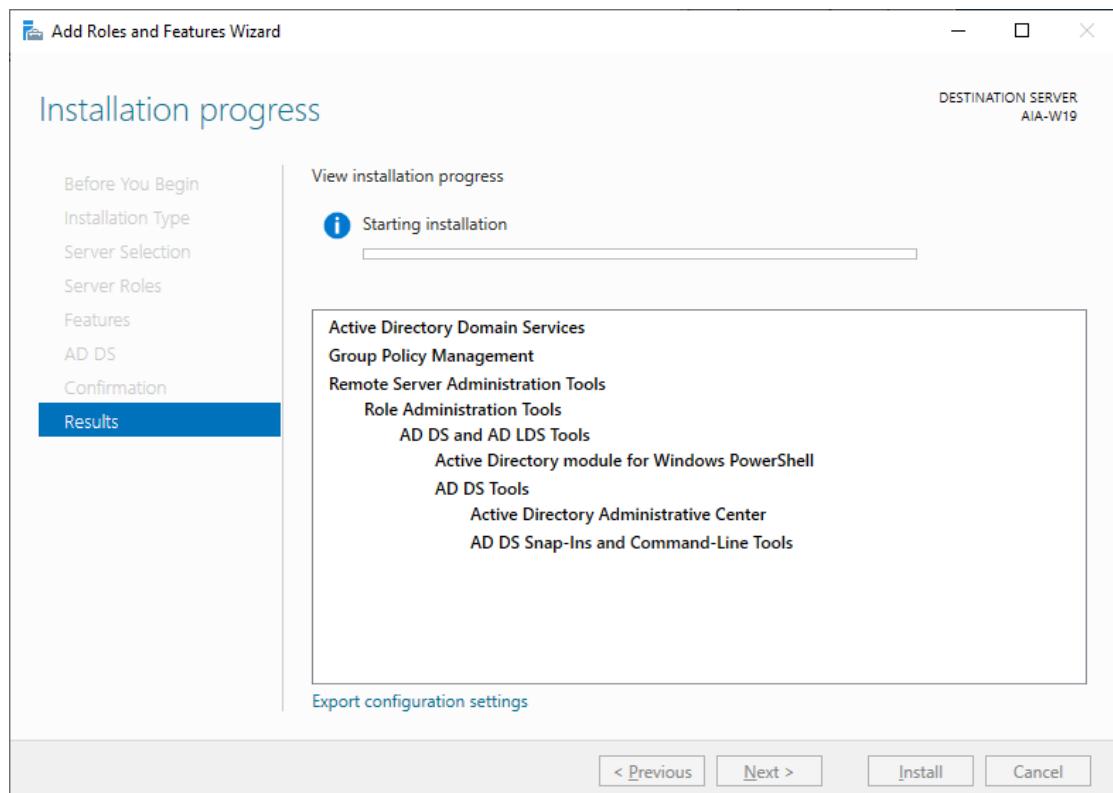




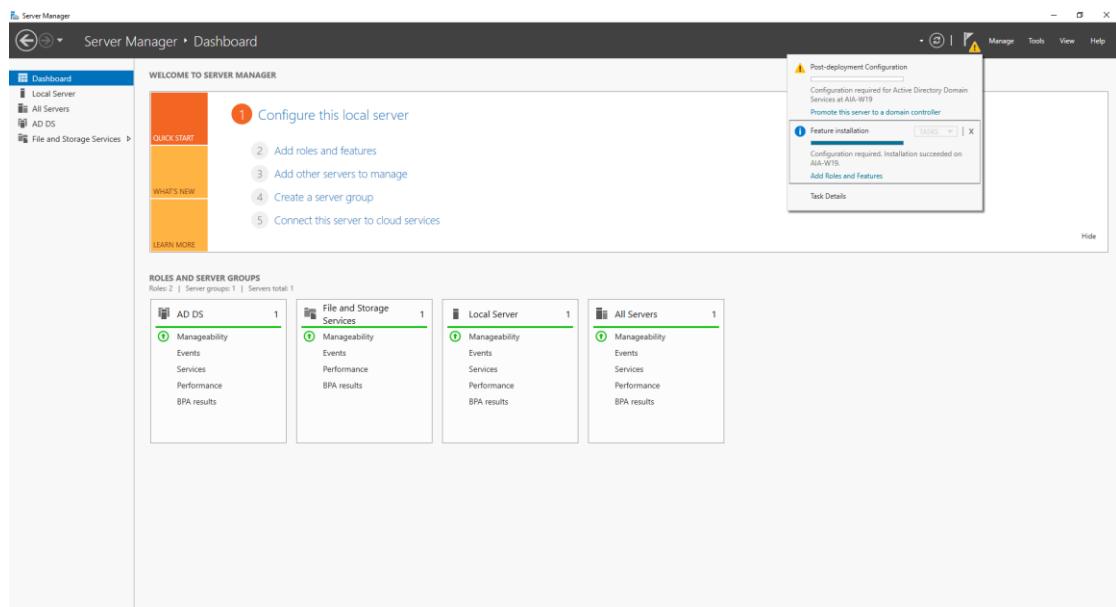
Confirm all your selections and click **Install**.



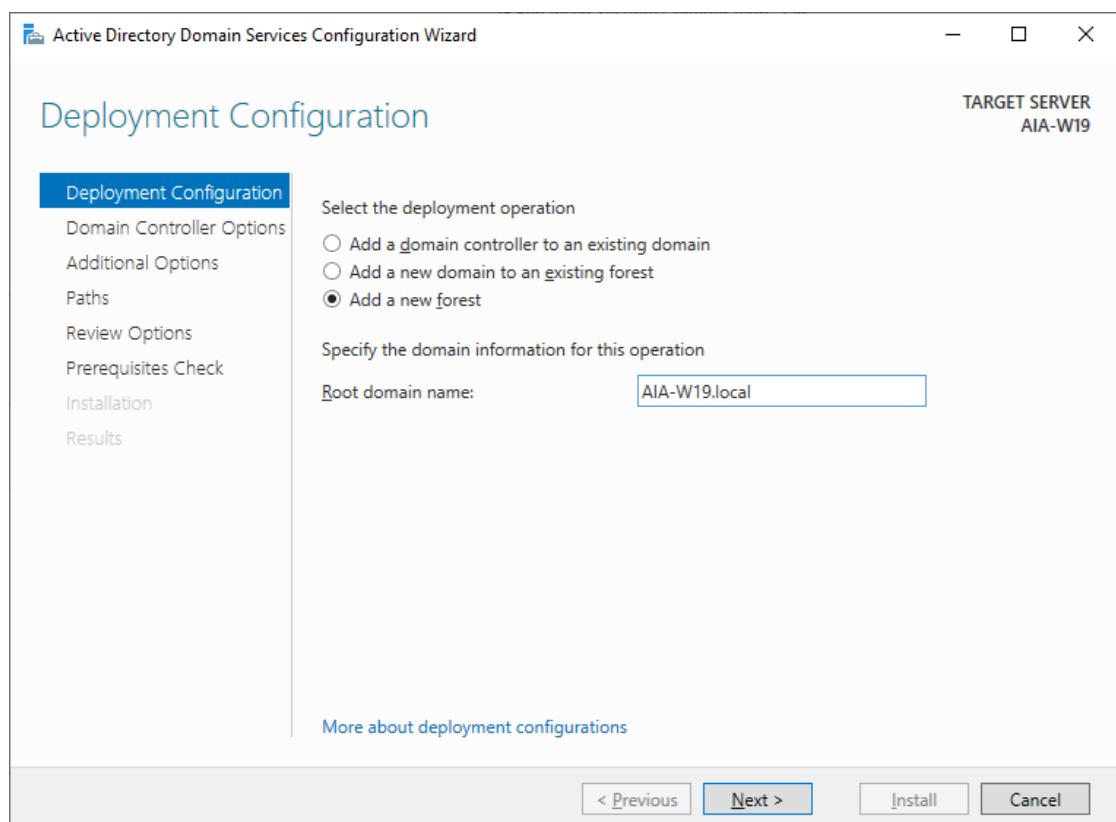
Wait until the installation finishes then click **Close**.



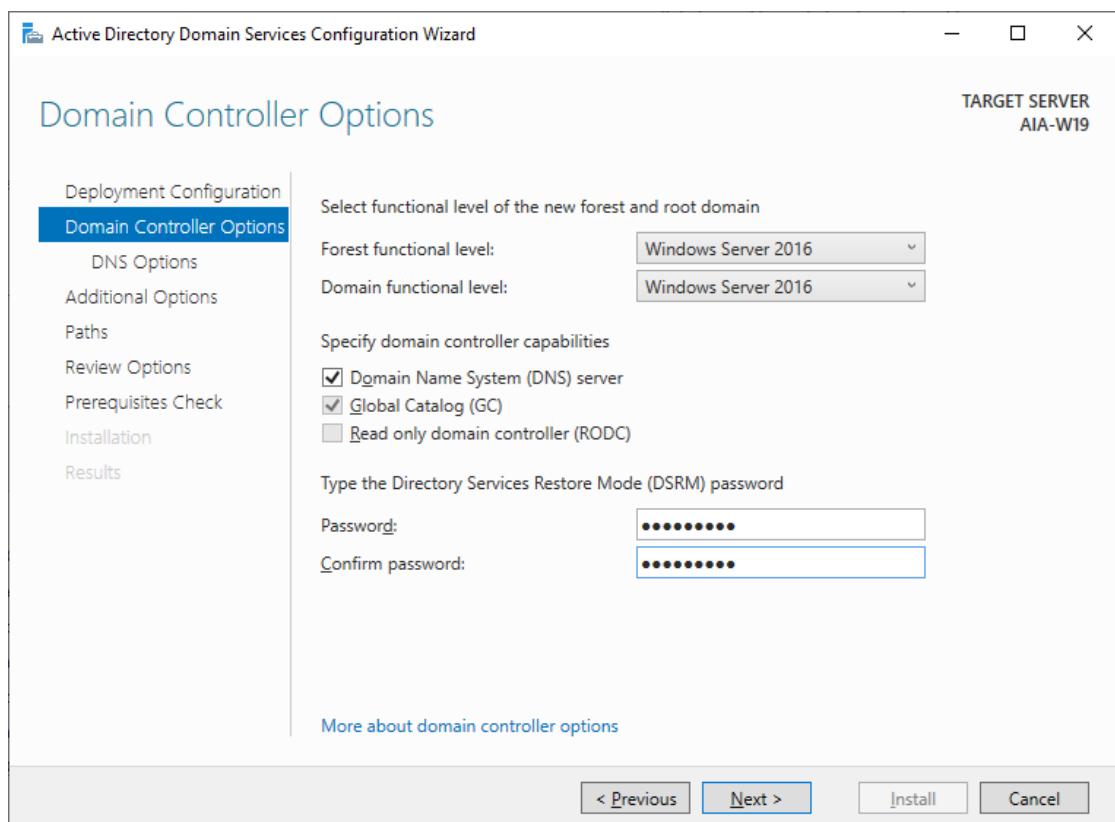
Once done, you'll see a notification on the flag icon. Click on it and select **Promote this server to a domain controller.**



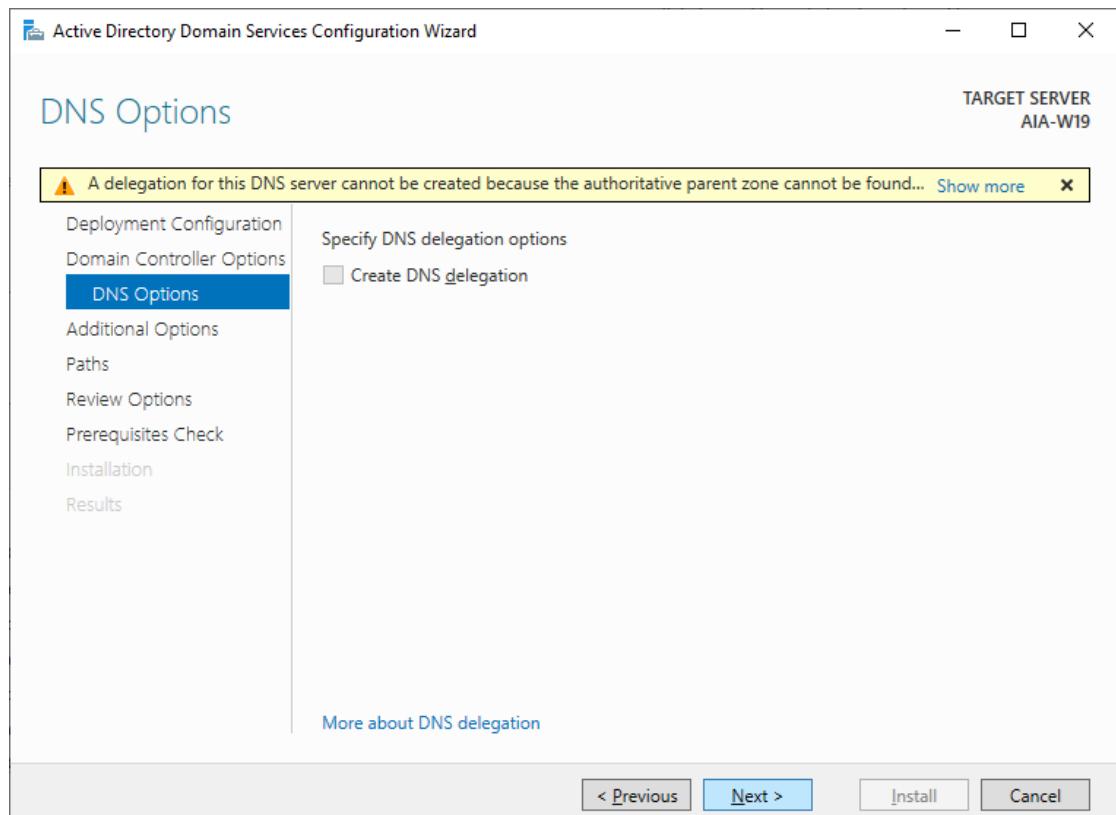
Select **Add a new forest** and enter the domain name ending with **.local** and then click **Next**. (AIA-W19.local)



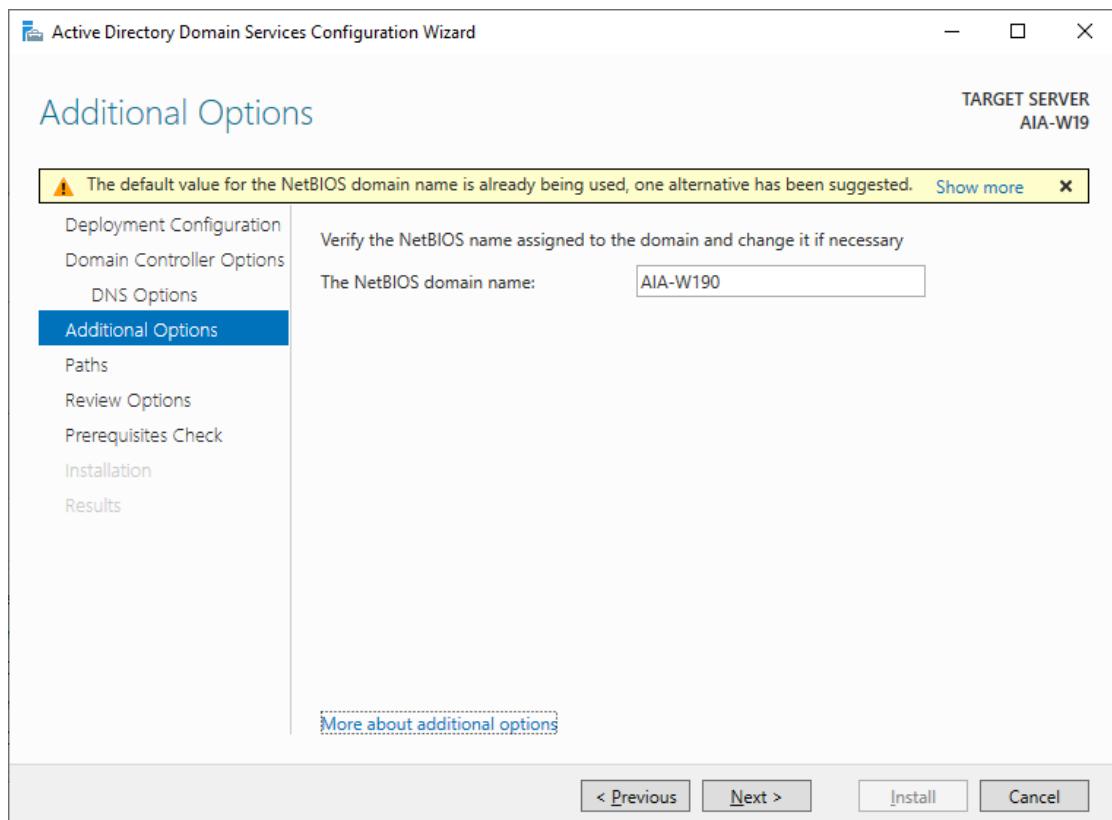
Create a DSRM password and confirm it then click **Next**



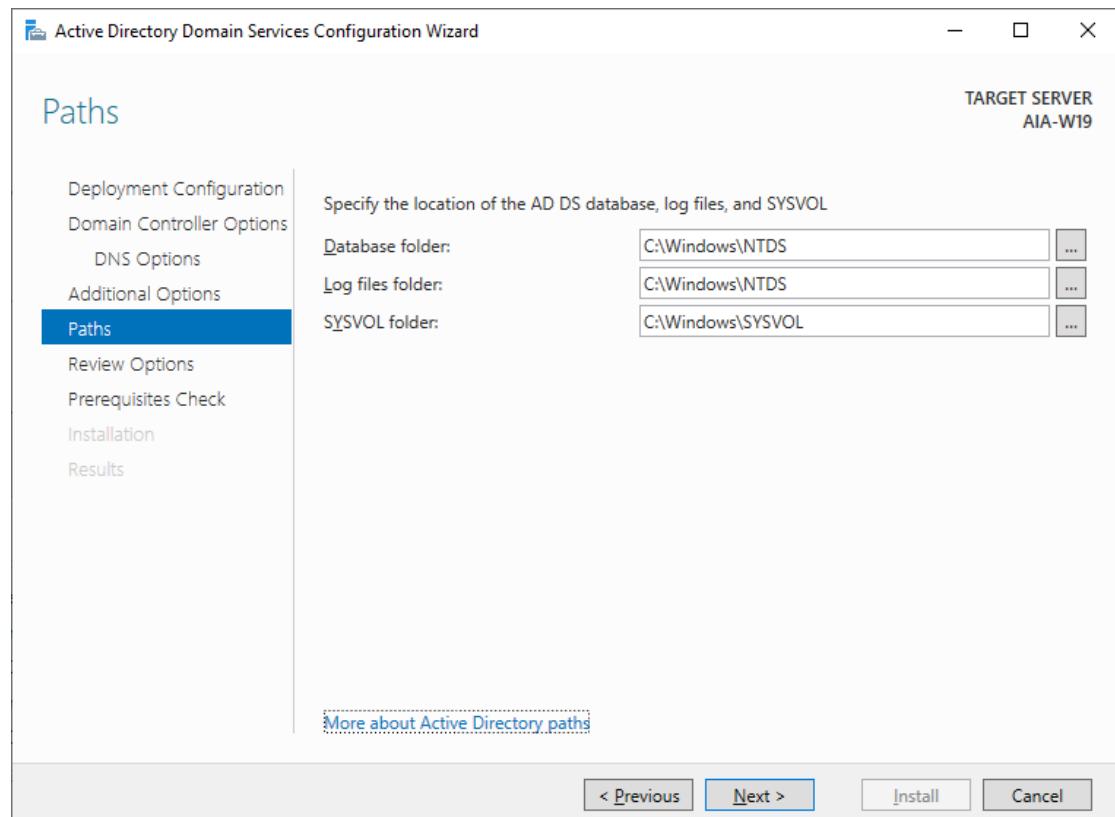
Ignore the DNS warning and click **Next**.



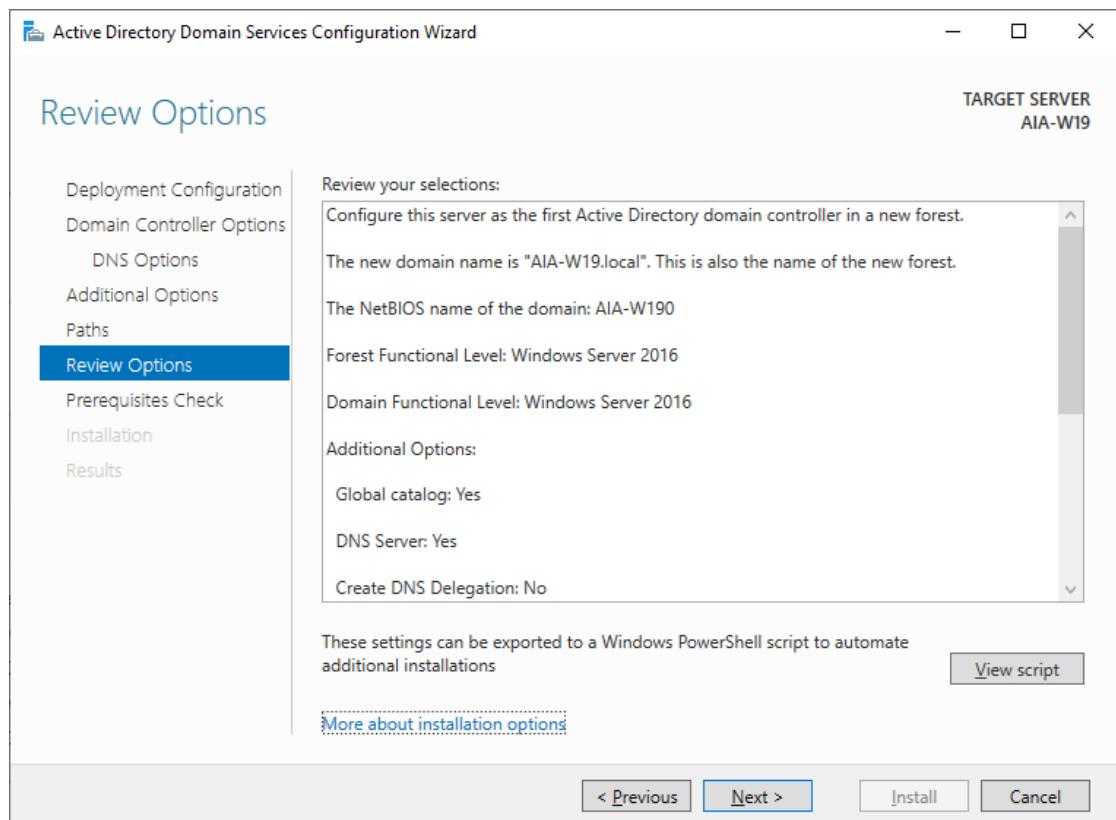
Confirm the NetBIOS domain name (created by default) and click **Next**.



Confirm your paths and click **Next**.

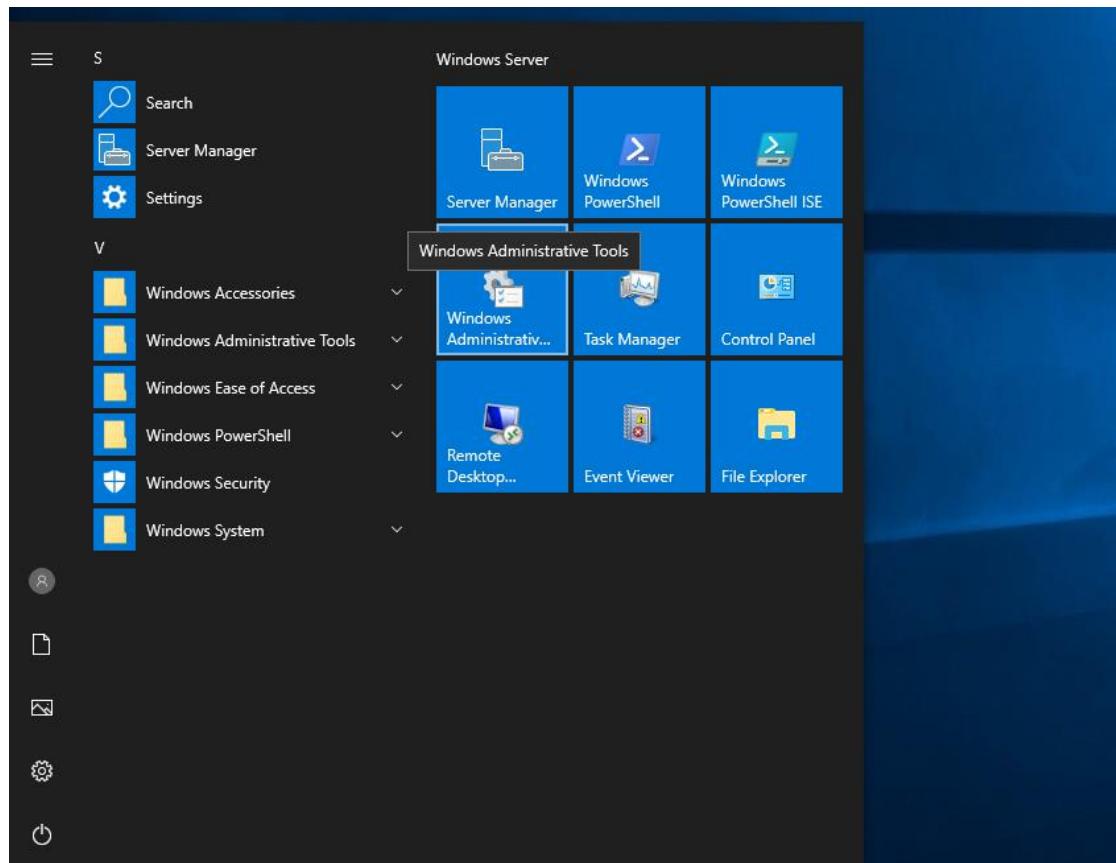


Review your selections and click **Next** and click install (Once finished, the computer will reboot automatically).

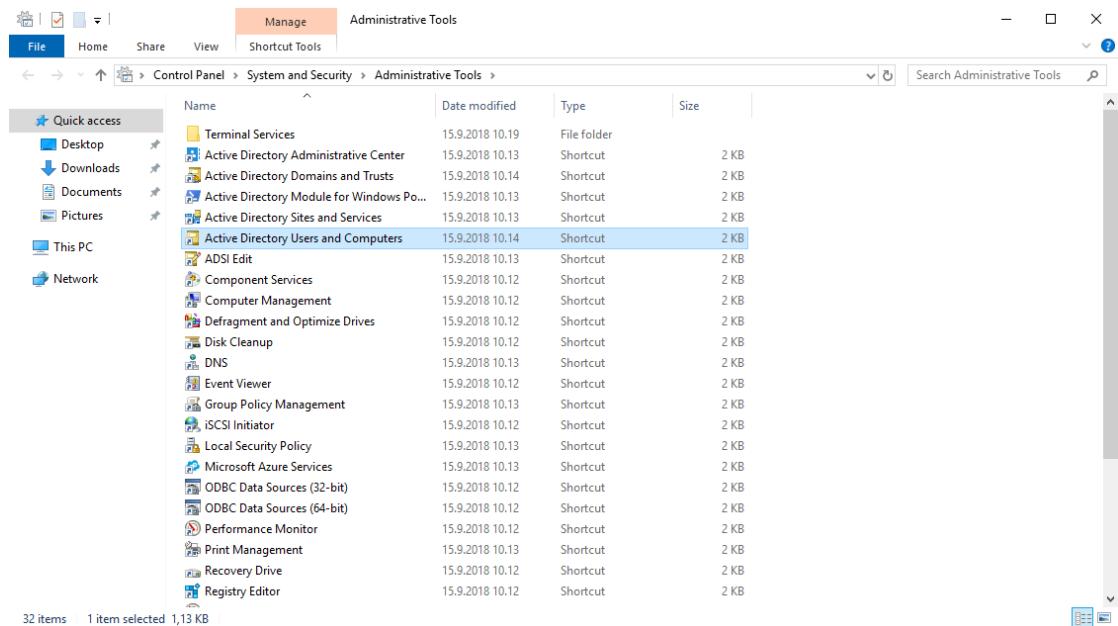


Now the domain is ready, it needs to create a user to enable a computer on the network to join it.

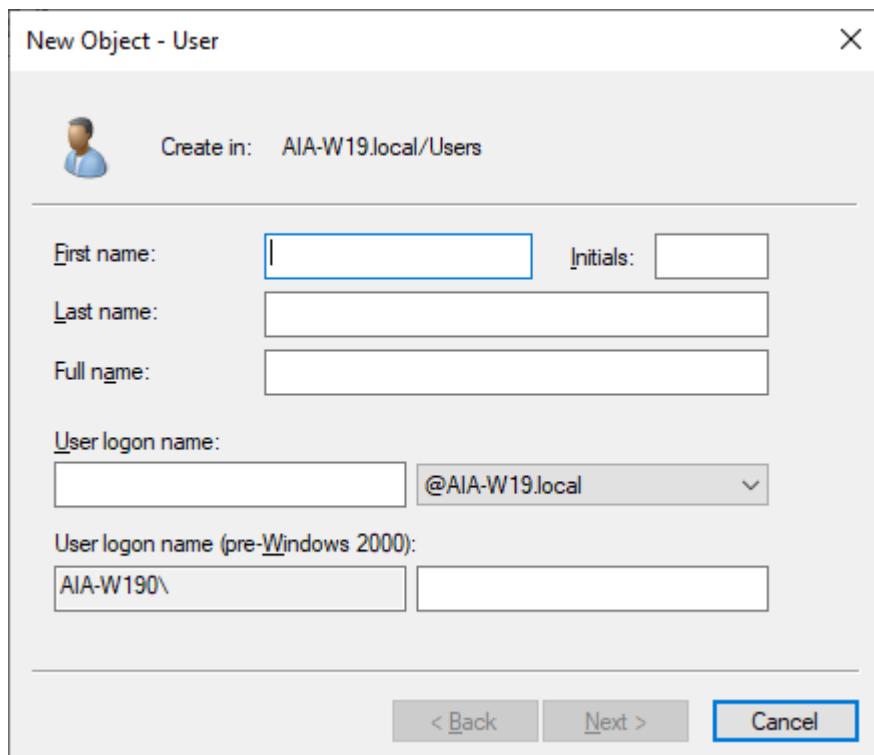
Open **Administrative Tools** from your start menu.



Open **Active Directory Users and Computers**.



Go to the **Users** folder under your domain name from the left pane, right-click and choose **New > User**.



New Object - User

Create in: AIA-W19.local/Users

First name: Aia Initials:

Last name:

Full name: Aia

User logon name:
Aia @AIA-W19.local

User logon name (pre-Windows 2000):
AIA-W190\ Aia

< Back Next > Cancel

Enter a password and retype it

New Object - User

Create in: AIA-W19.local/Users

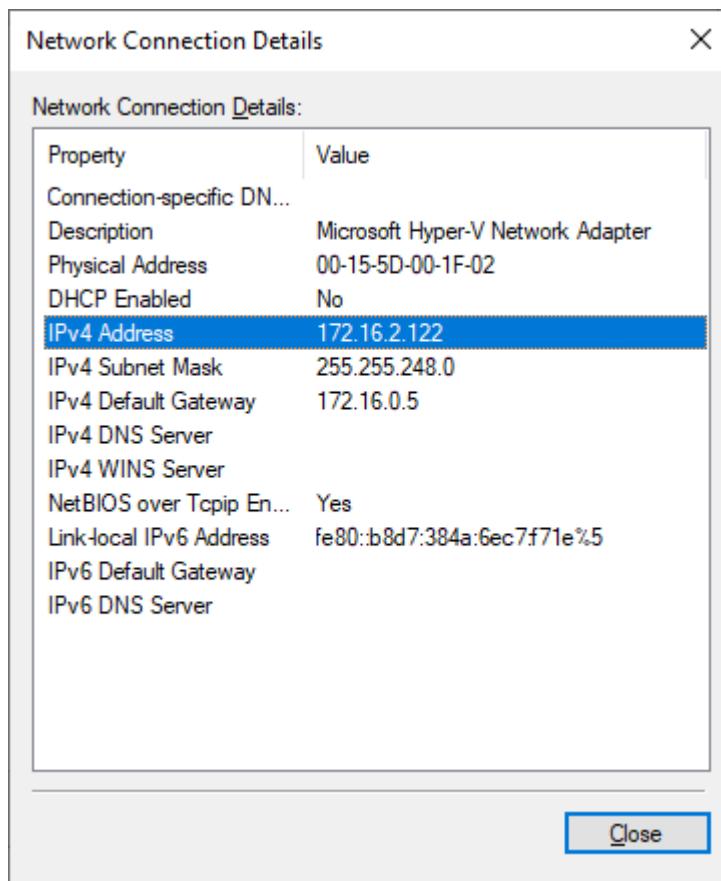
Password: ······

Confirm password: ······

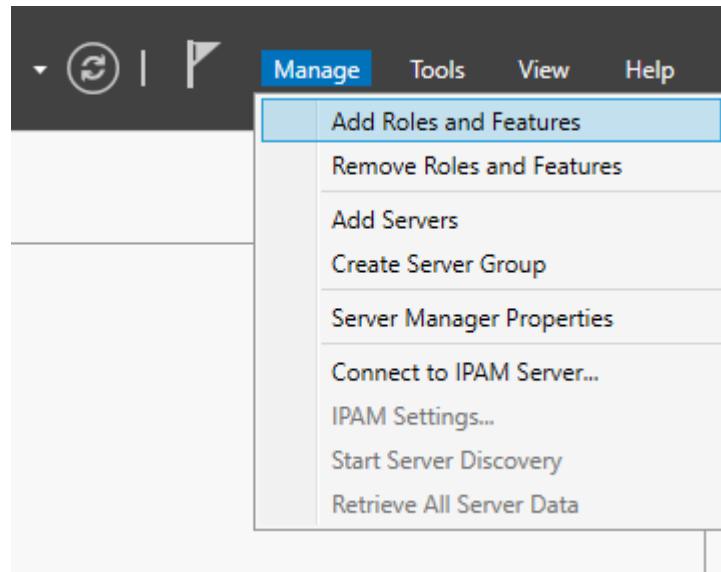
User must change password at next logon
 User cannot change password
 Password never expires
 Account is disabled

< Back Next > Cancel

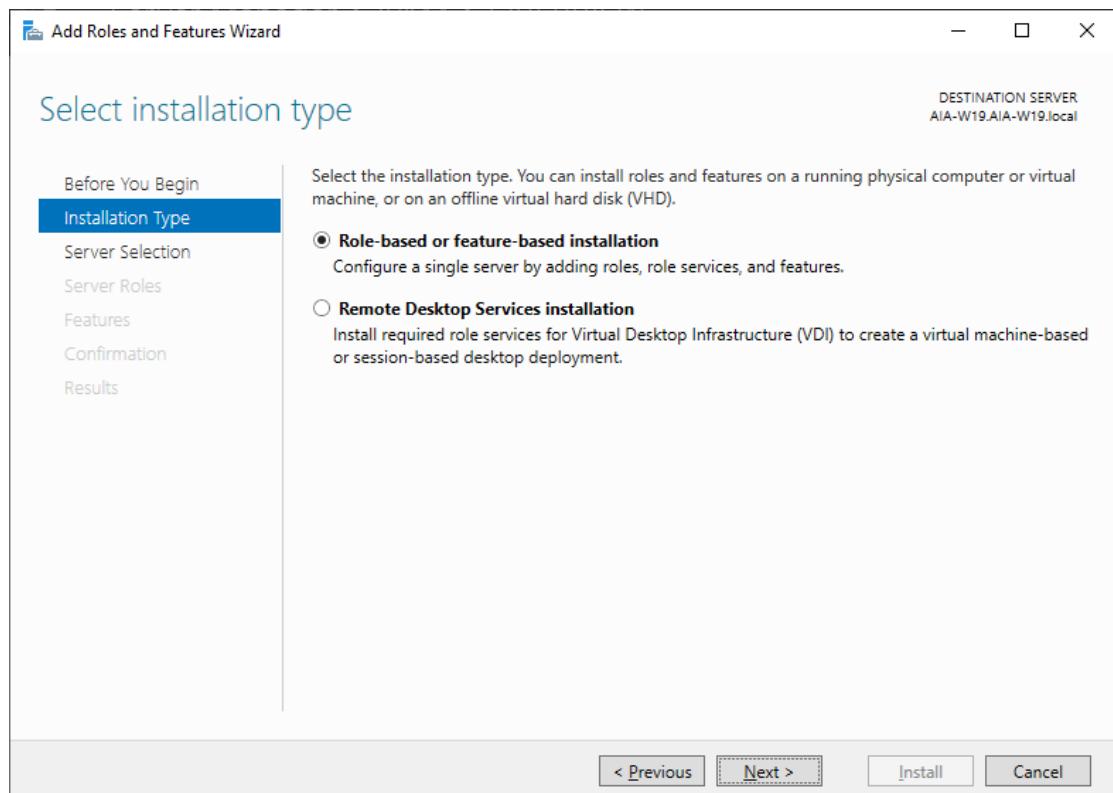
Right-click on your network icon at the clock area and then click **Open Network and Sharing Center**.



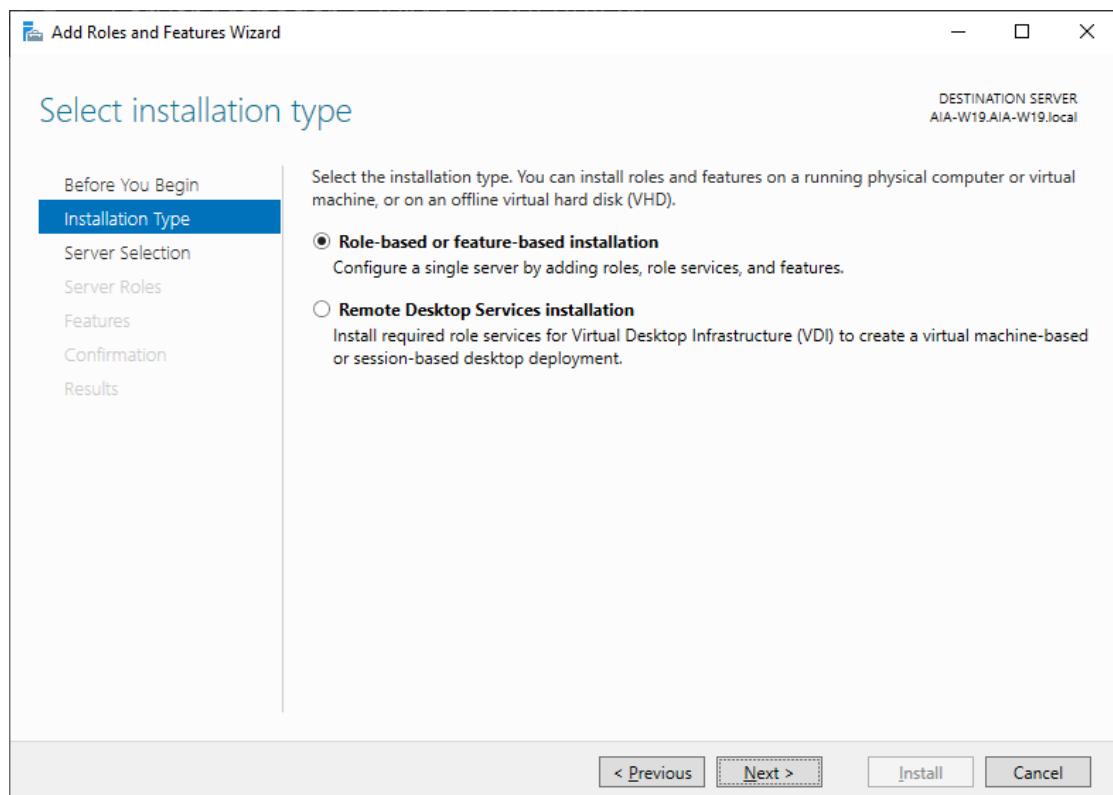
Open the server manager, select Add Role and Features



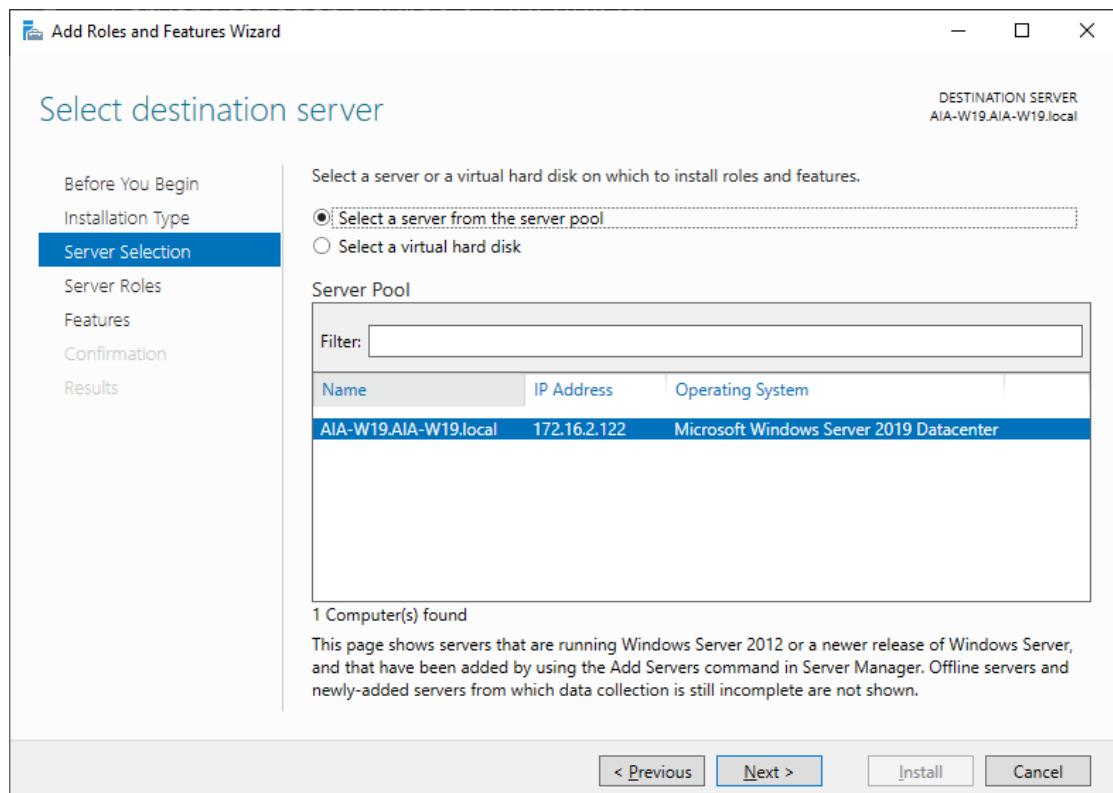
On the Before You Begin screen select next



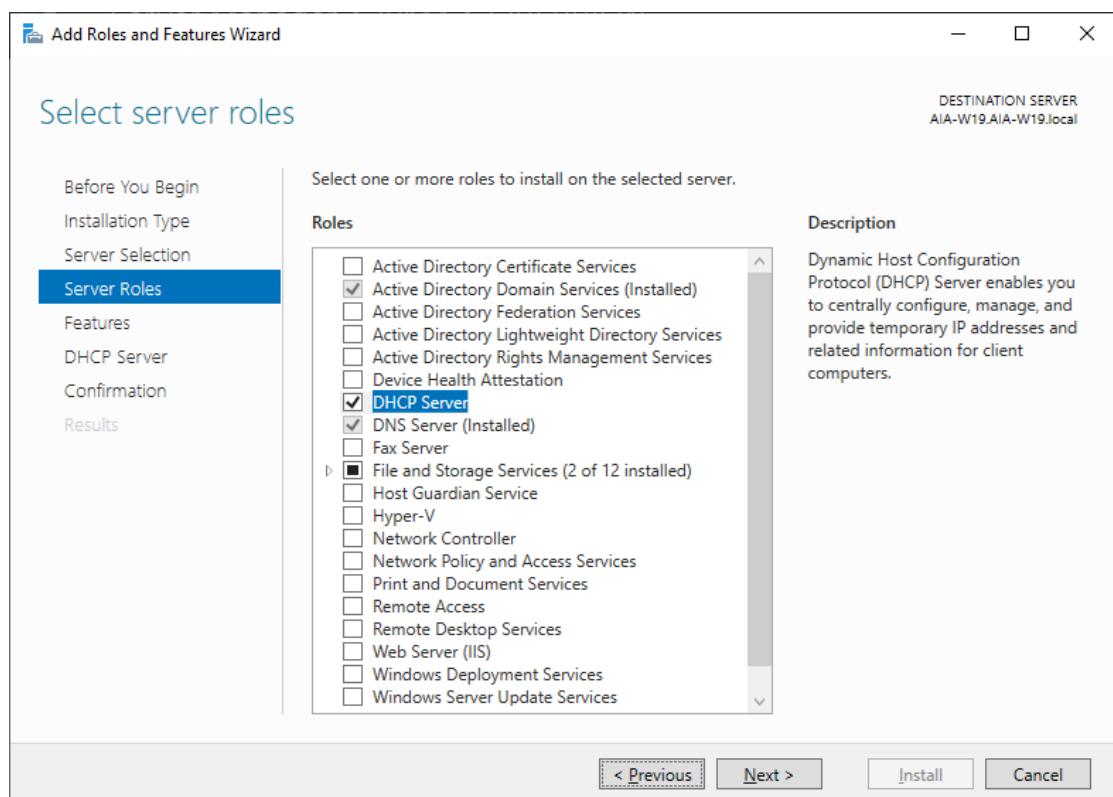
Select Role-based or feature-based installation and click the next button.



Select the server that we want to install the role on and click the next button

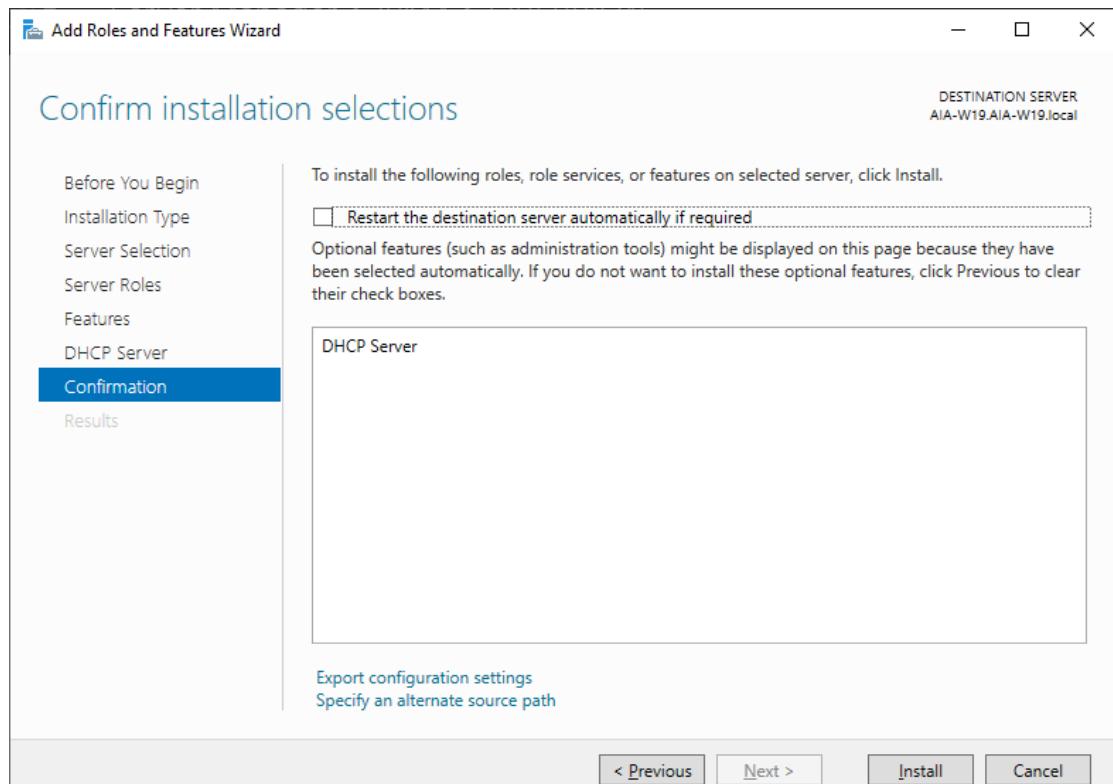


On the next screen tick Active Directory Domain Services and DHCP Server.

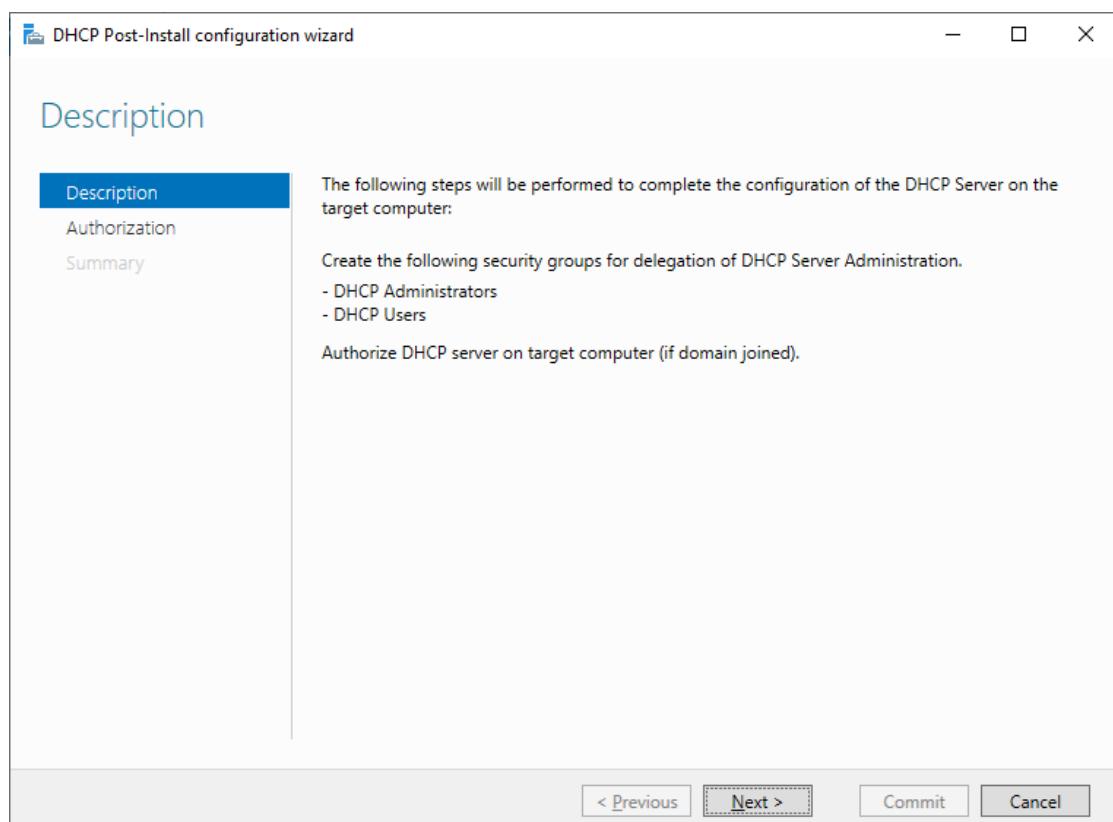


The Active Directory had installed already. On the next screens leave the default settings and select next and then install. Once the installation of DHCP and Active Directory roles is complete you will get a notification in the Server

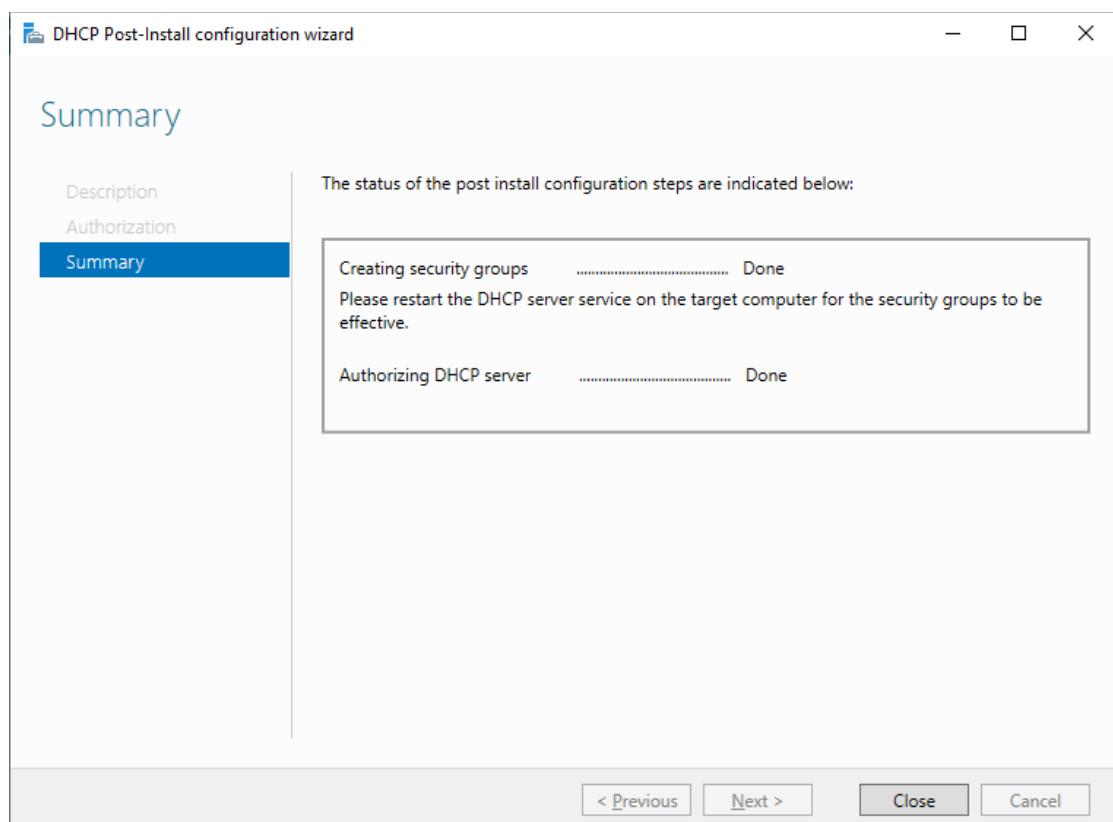
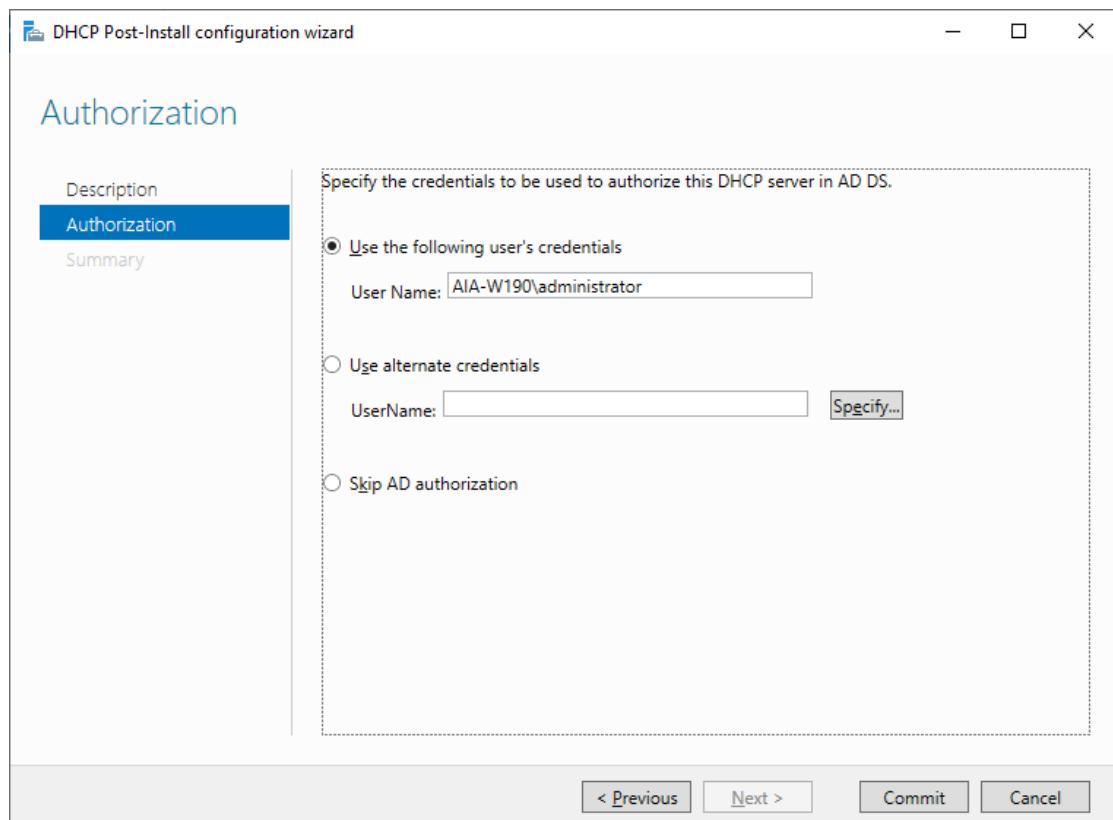
Manager console to “Promote this server to a domain controller” and to “Complete DHCP configuration”. You can to run the “Promote this server to a domain controller” first, click on that.



The screenshot shows the "Add Roles and Features Wizard" window titled "Confirm installation selections". The "DESTINATION SERVER" is listed as "AIA-W19.AIA-W19.local". The "Confirmation" tab is selected. On the left, a list includes "Before You Begin", "Installation Type", "Server Selection", "Server Roles", "Features", "DHCP Server", "Confirmation" (selected), and "Results". A note says: "To install the following roles, role services, or features on selected server, click Install." Below it is a checkbox: "Restart the destination server automatically if required". A note states: "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." A box labeled "DHCP Server" contains the selected feature. At the bottom, buttons include "< Previous", "Next >", "Install", and "Cancel".



The screenshot shows the "DHCP Post-Install configuration wizard" window titled "Description". The "Description" tab is selected. On the left, a list includes "Description" (selected), "Authorization", and "Summary". The main area lists steps: "The following steps will be performed to complete the configuration of the DHCP Server on the target computer:", "Create the following security groups for delegation of DHCP Server Administration.", and "Authorize DHCP server on target computer (if domain joined)". At the bottom, buttons include "< Previous", "Next >" (dashed border), "Commit", and "Cancel".



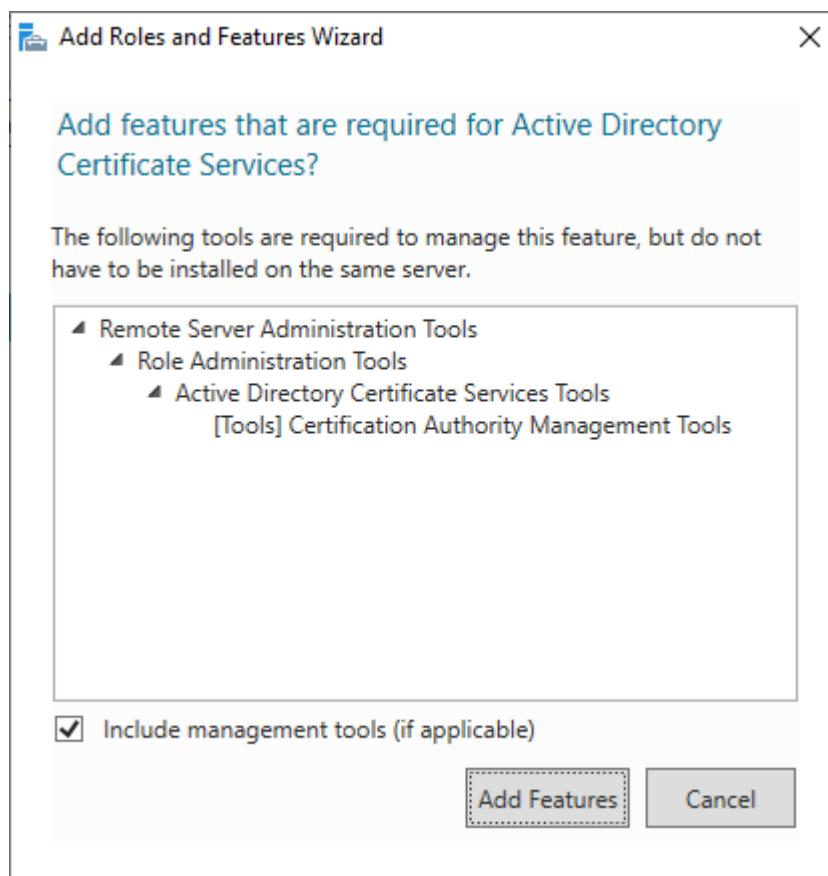
➤ **Smart Card authentication:**

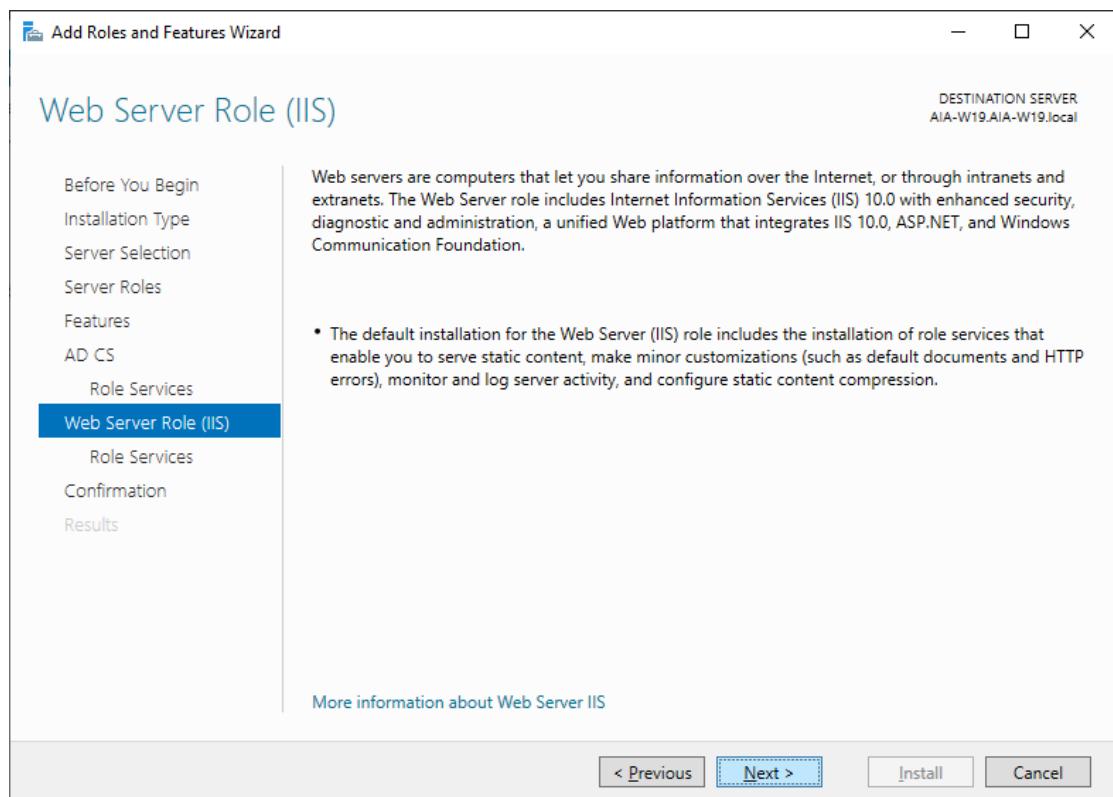
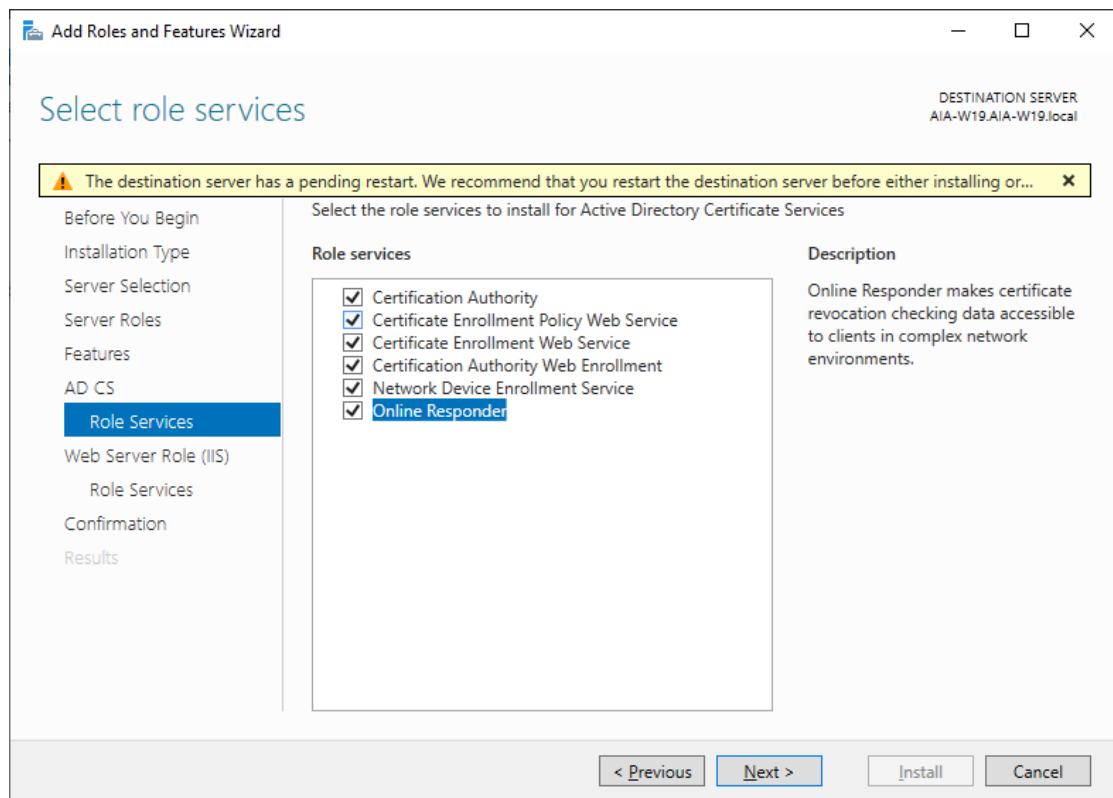
Smart cards are a key component of the public key infrastructure (PKI) that Microsoft is integrating into the Windows platform because smart cards enhance software-only solutions, such as client authentication, logon, and secure email. Smart cards are a point of convergence for public key certificates and associated keys because they:

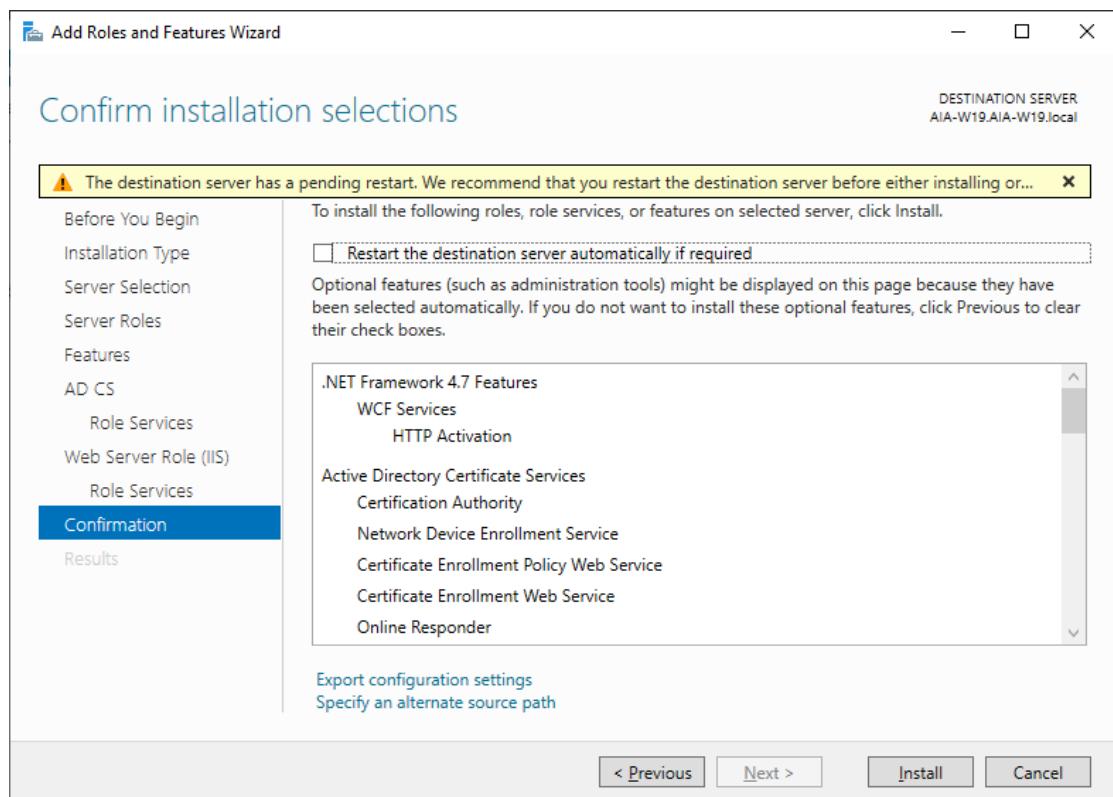
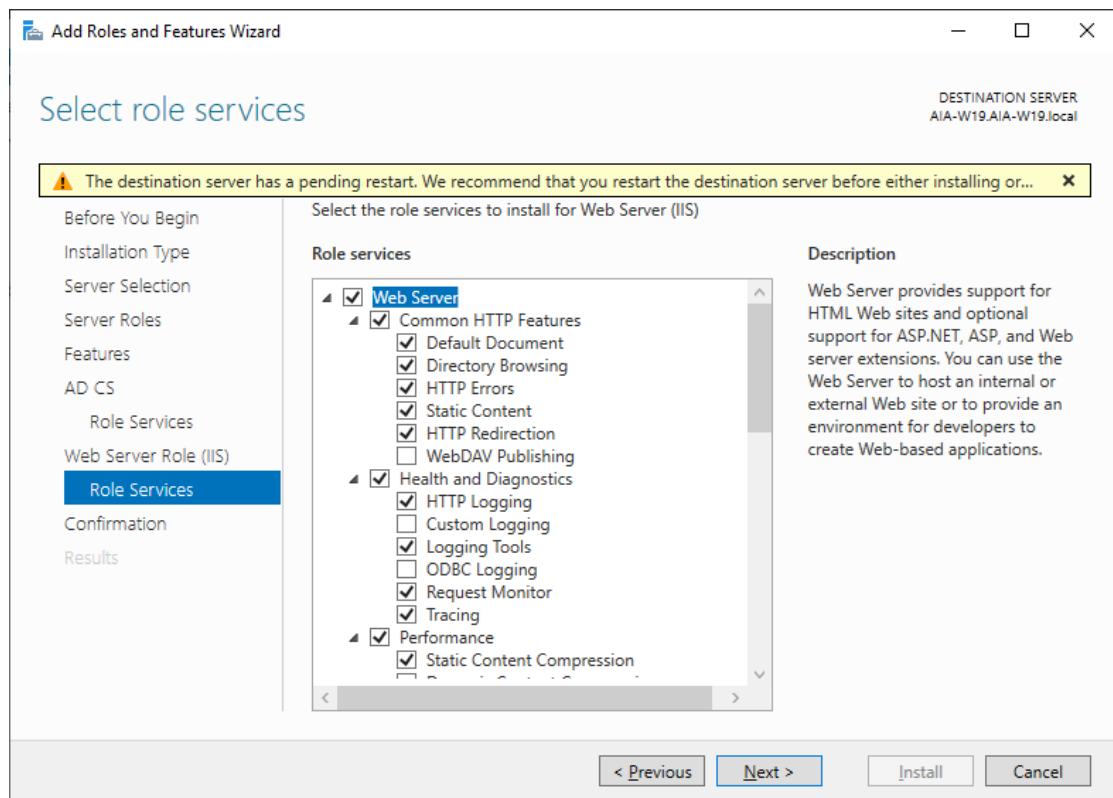
- Provide tamper-resistant storage for protecting private keys and other forms of personal information.
- Isolate security-critical computations, involving authentication, digital signatures, and key exchange from other parts of the system that don't have a need to know.
- Enable portability of credentials and other private information between computers at work, at home, or on the road.

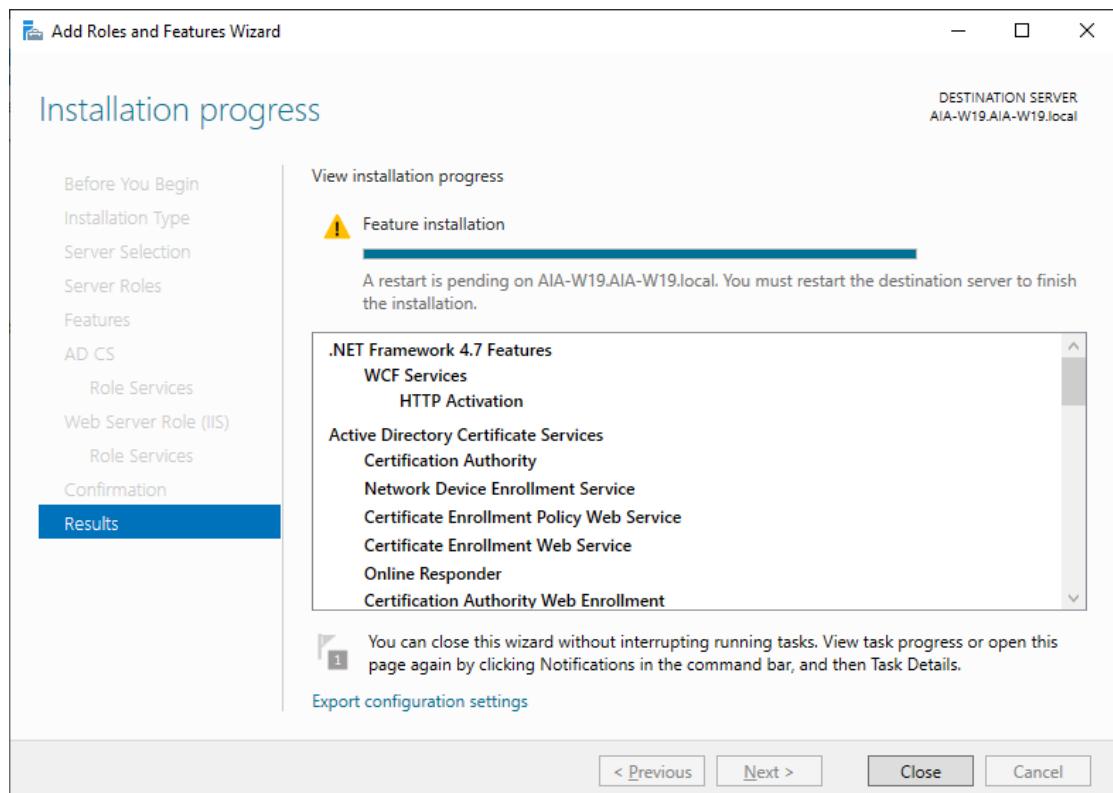
Configure Certificate Authority Templates:

First of all we need to add Certificate Authority role and feature.

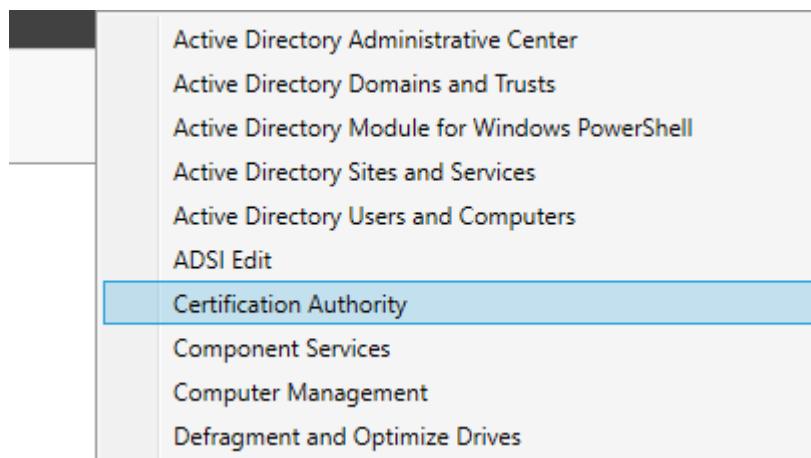




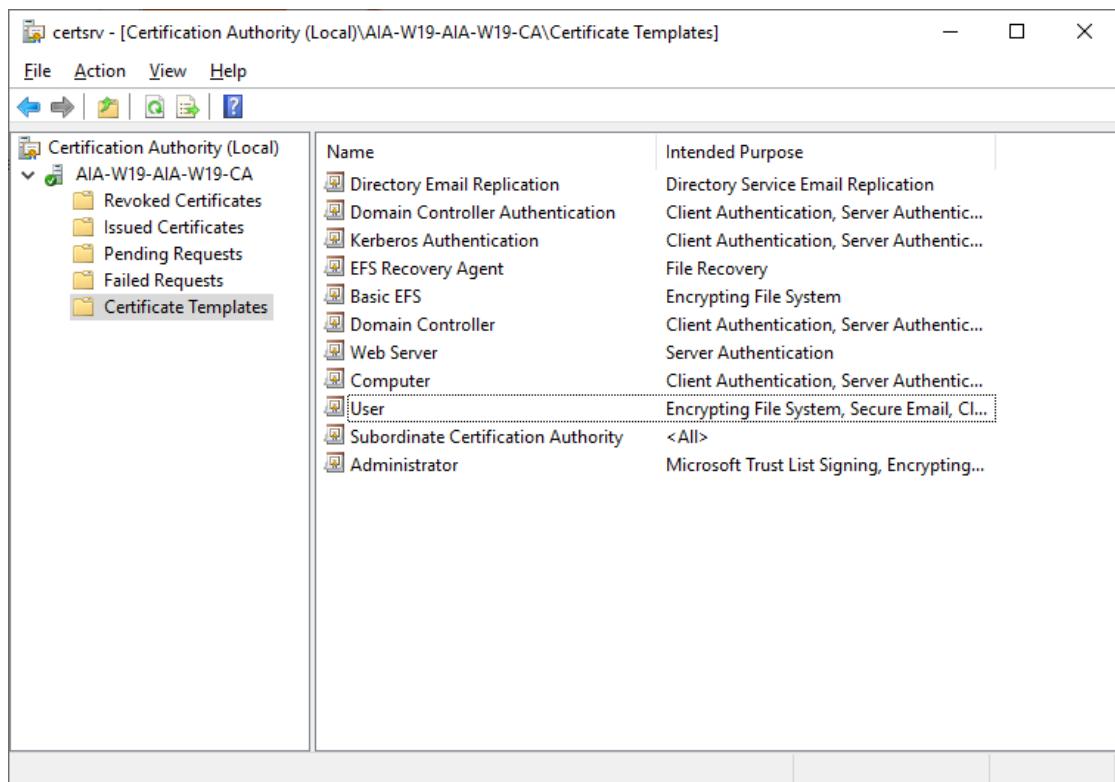




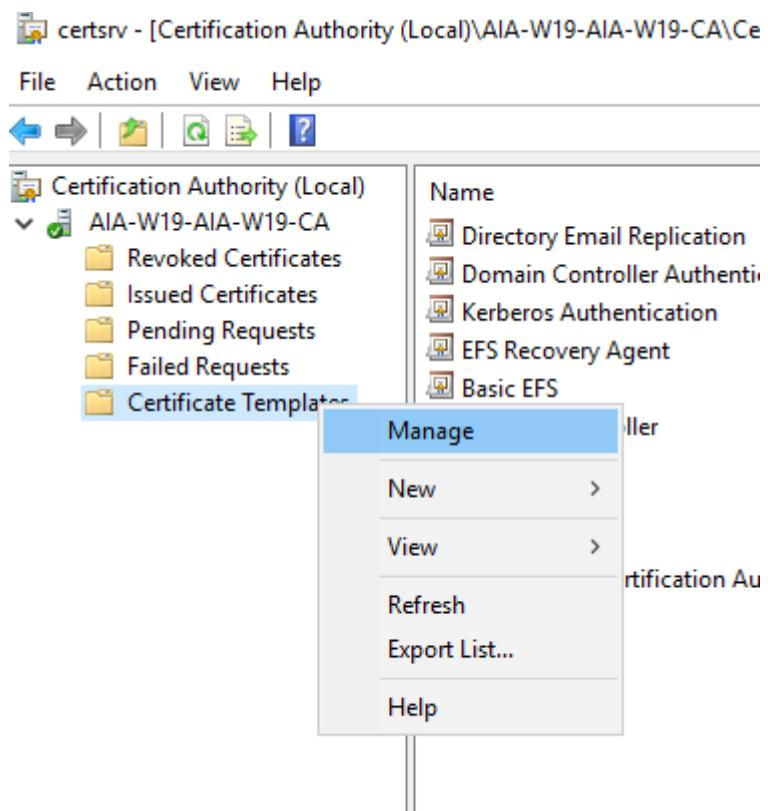
In the Server Manager, choose Tools, then Certification Authority.



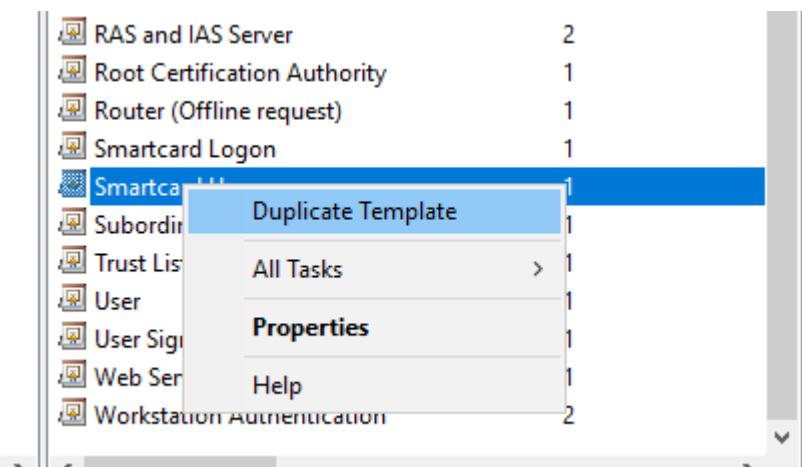
Expand the server name to reveal Certificate Folders.



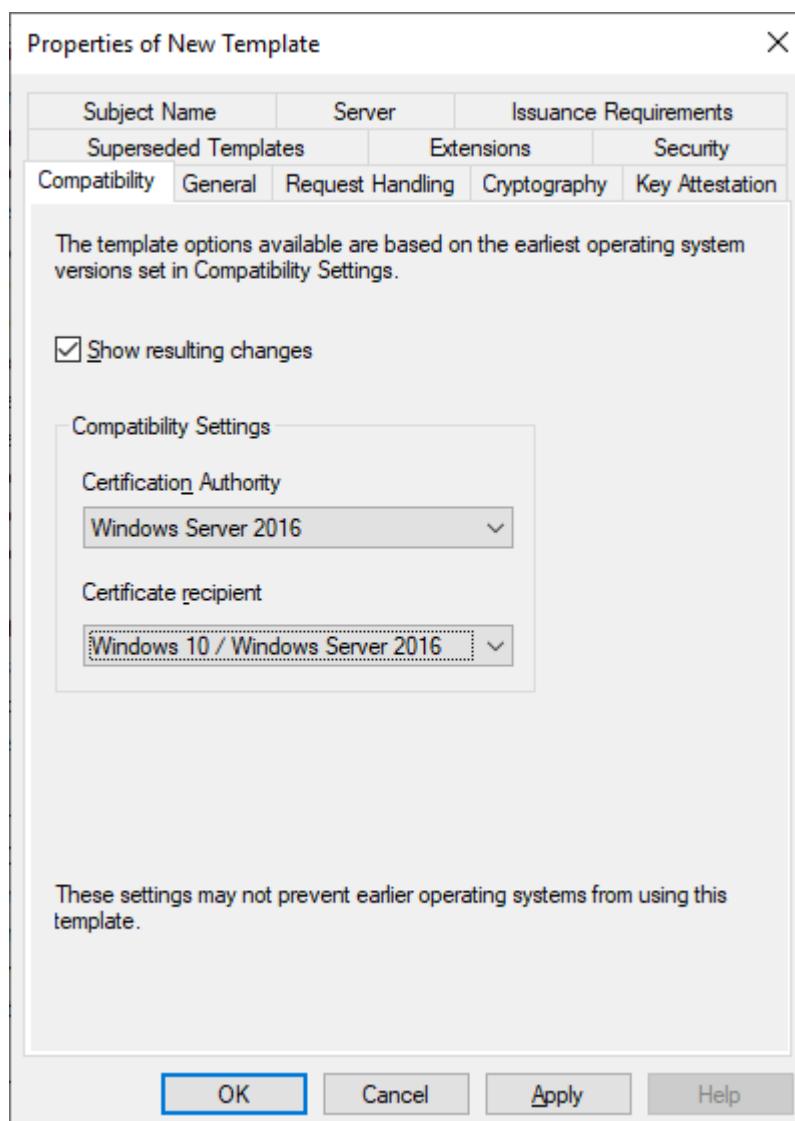
Right click the Certificate Templates folder and choose Manage.



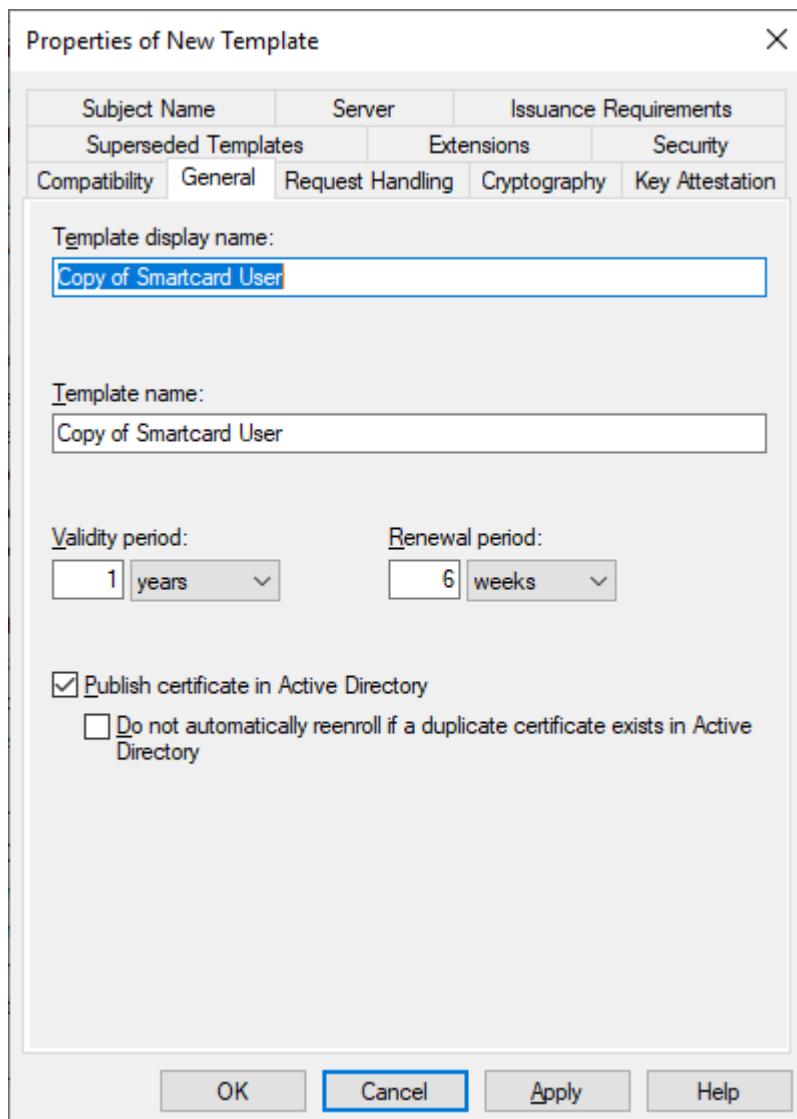
A new window opens with a list of templates in the middle pane. Right click the Smart Card User template and select Duplicate Template. The Smart Card User template is a general use template that enables computer logon, as well as signing and encryption. If only smart card logon is needed, we can instead select the "Smart Card Logon" template.



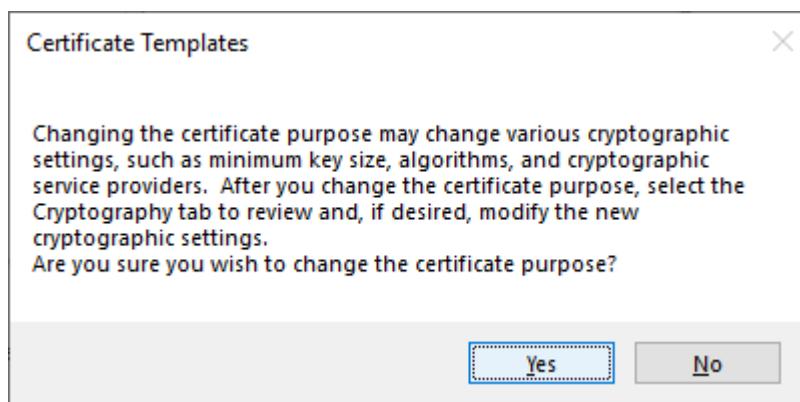
Next, adjust the properties of the new template. Under the Compatibility tab, Windows Server 2016 settings .



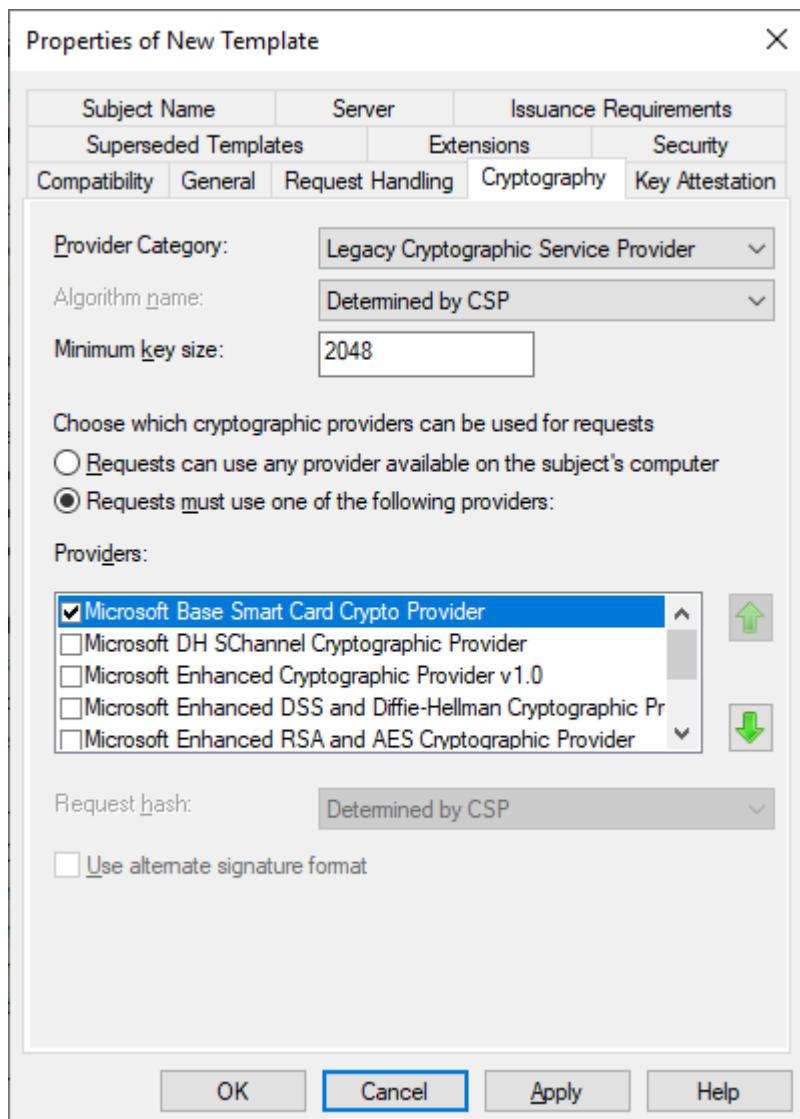
Under the General tab, rename the template.



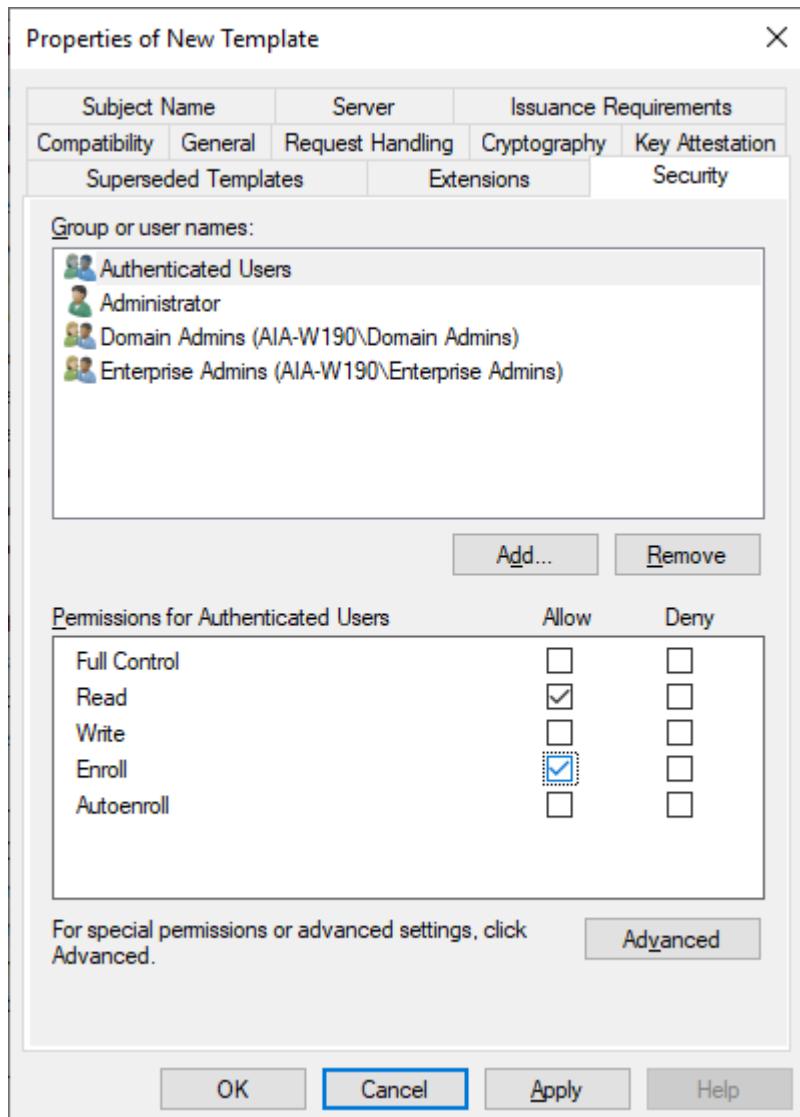
Under the Request Handling tab, select Purpose: "Signature and smartcard logon".



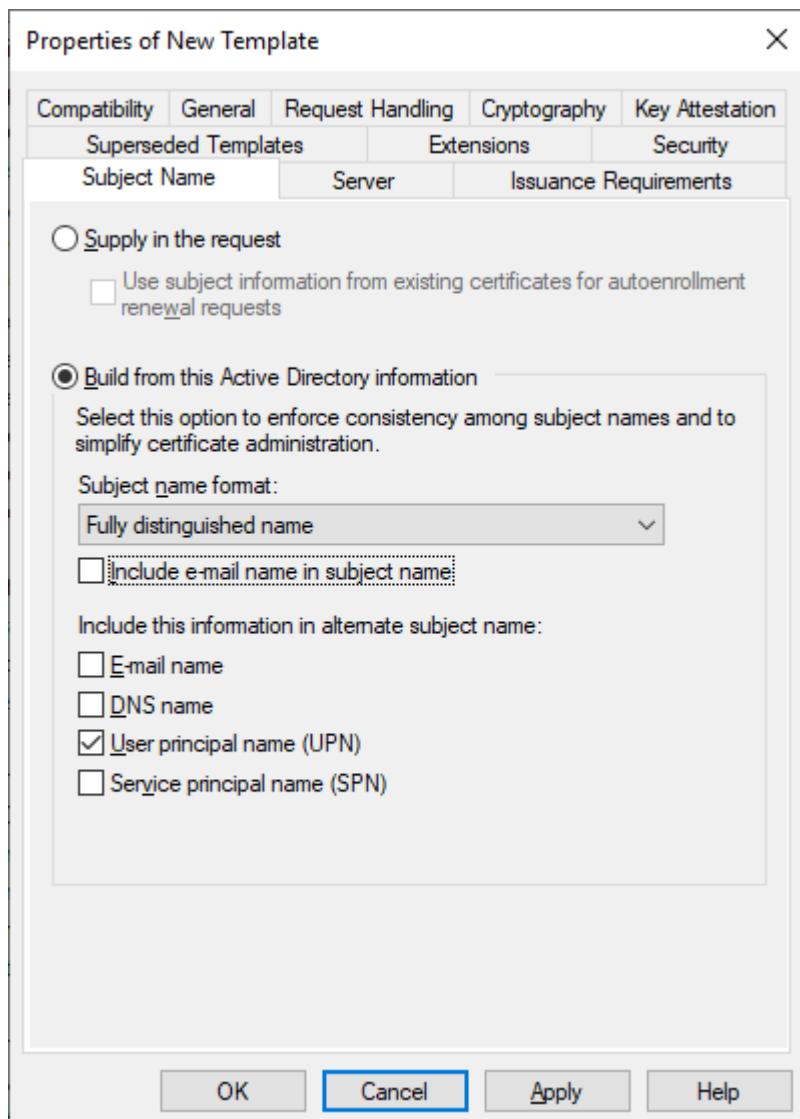
Under the Cryptography tab, change the minimum key size to 2048, select "Requests must use one of the following providers", and check Microsoft Base Smart Card Crypto Provider. This will ensure that the smart card is used for storing the certificate and keys.



Under the Security tab, be sure the Enroll ability is set for the group or users who will be setting up the smart cards for logon (use the Add button to add groups or individual users).

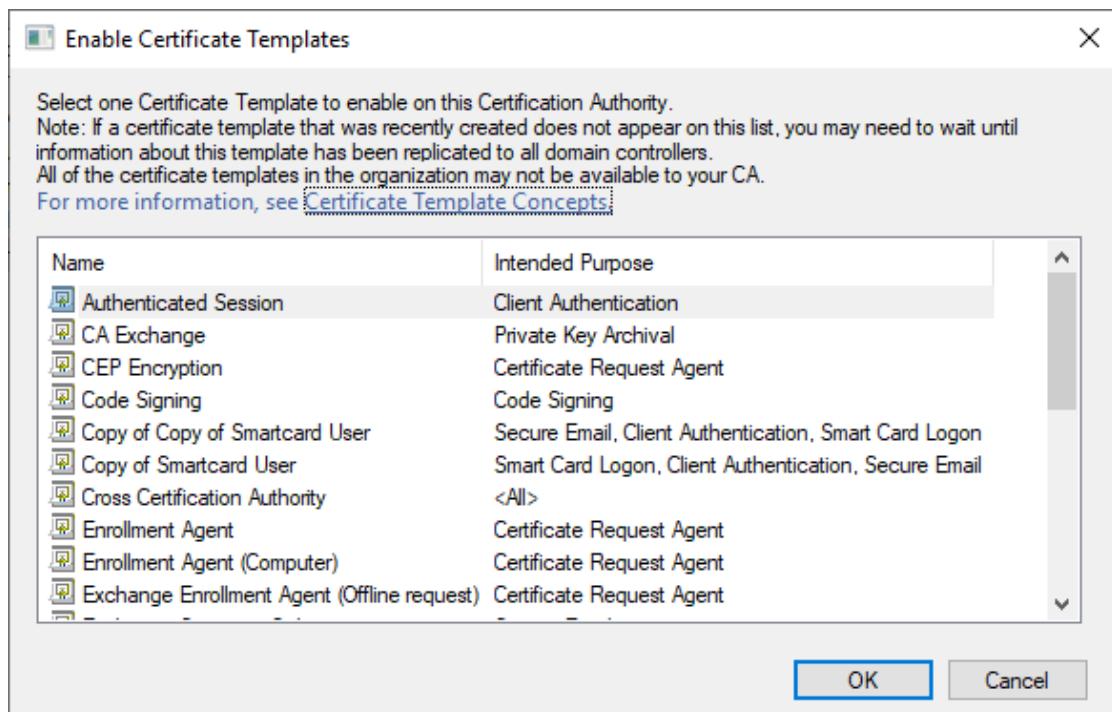


If the users do not have email addresses in their User Properties, **and if you will not be using these certificates to sign emails**, under the Subject Name tab, deselect "Include e-mail name in subject name" and "E-mail name"



Click OK to save the template. Close that window.

The Certificates Template folder contains all the templates assigned to the CA. Some templates are assigned to the CA by default, the new template needs to be issued to be added to the Certification Authority templates. Right click the Certificate Templates folder, choose New, then Certificate Template to Issue.

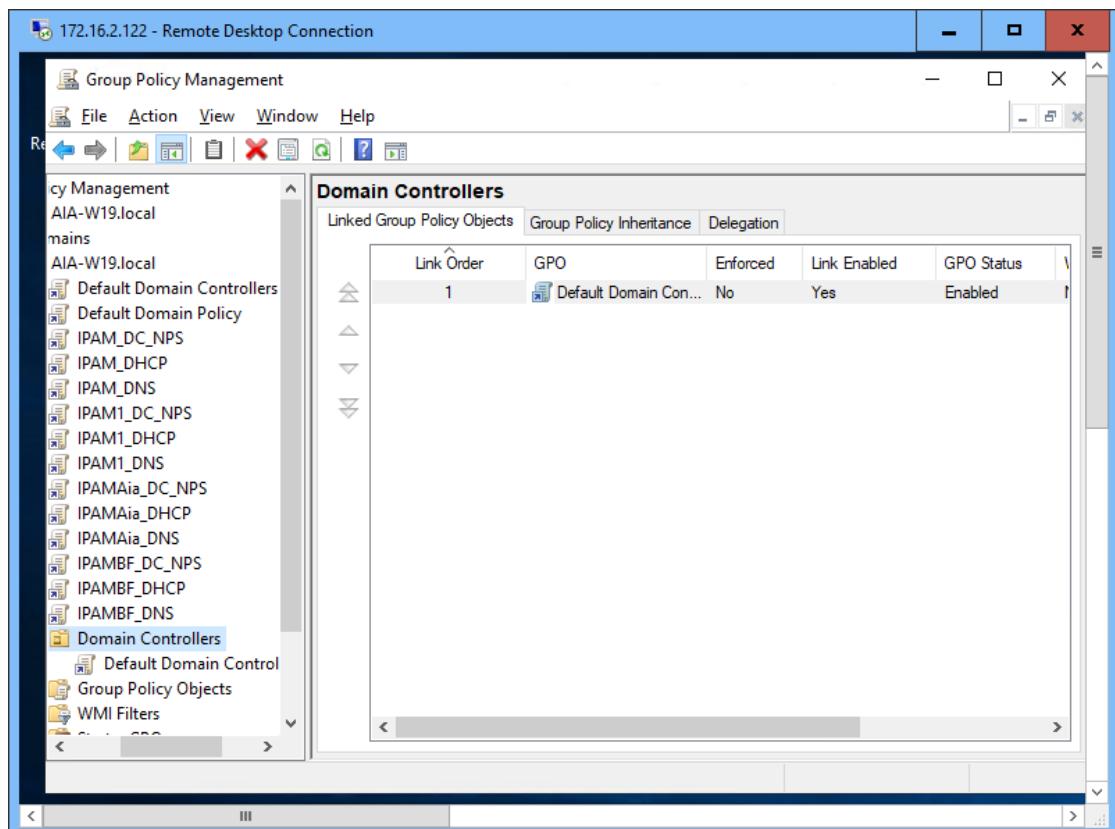


➤ Dynamic access control: File shares, Reimagined:

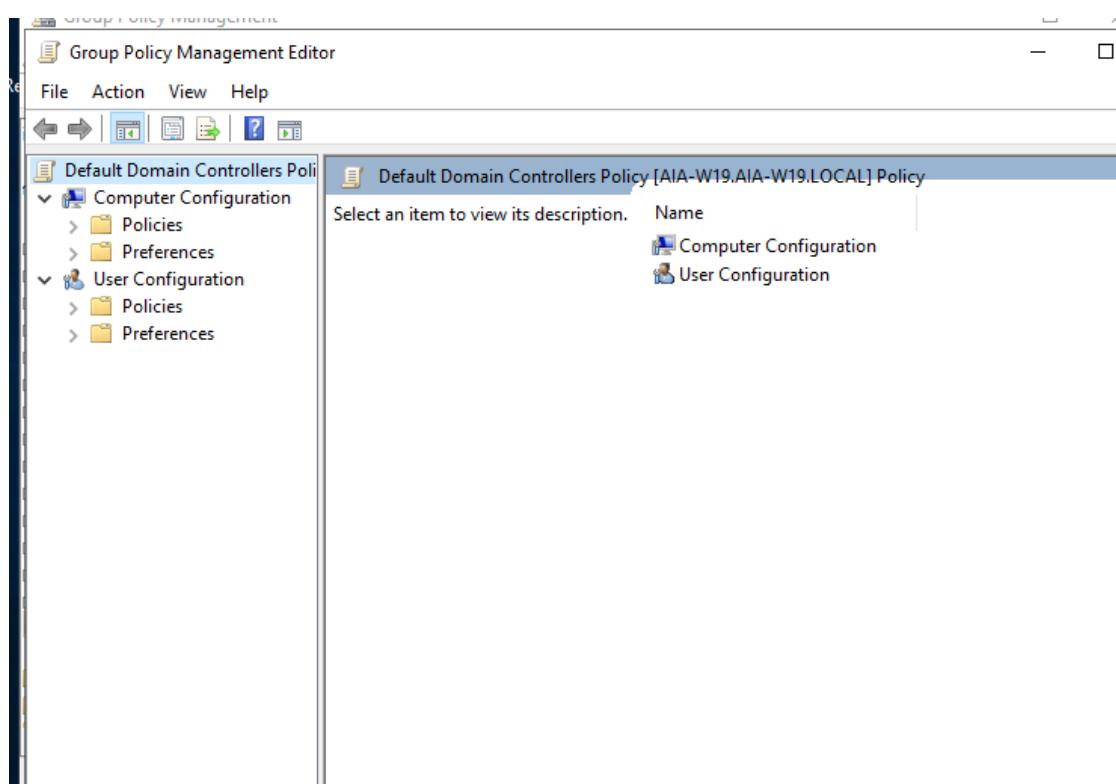
Dynamic Access Control integrates claims into Windows authentication so that users and devices can be described not only by the security groups they belong to, but also by claims such as users in different sections.

Claims are Active Directory attributes defined to be used with Central Access Policies. The claims can be set for both users and devices. Microsoft added a new container to the Active Directory Administrative Center to implement this new feature.

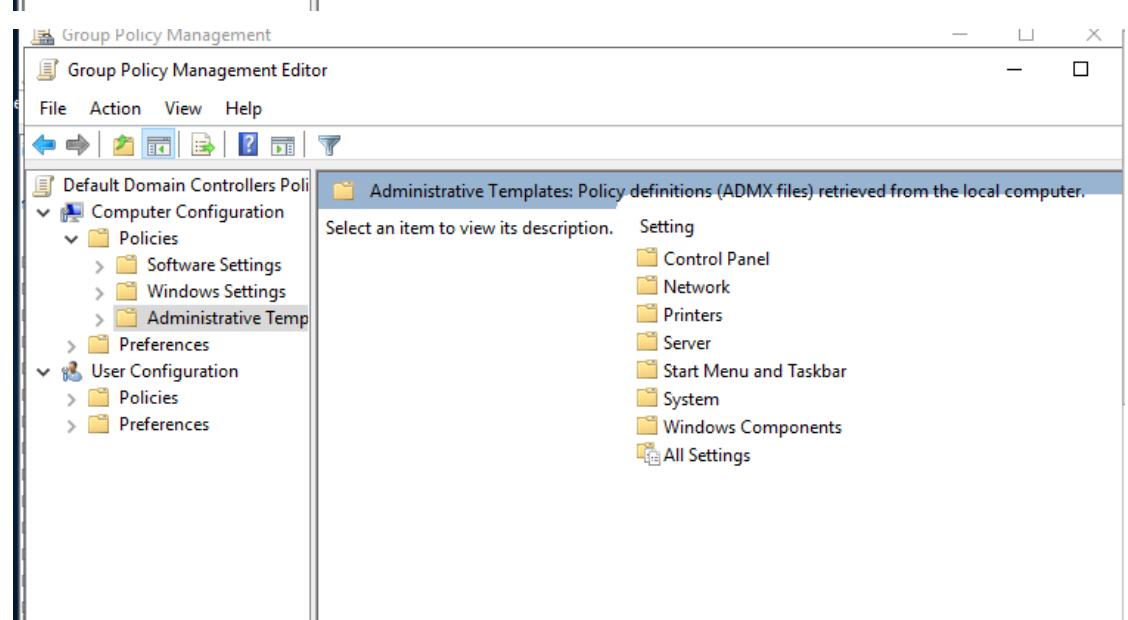
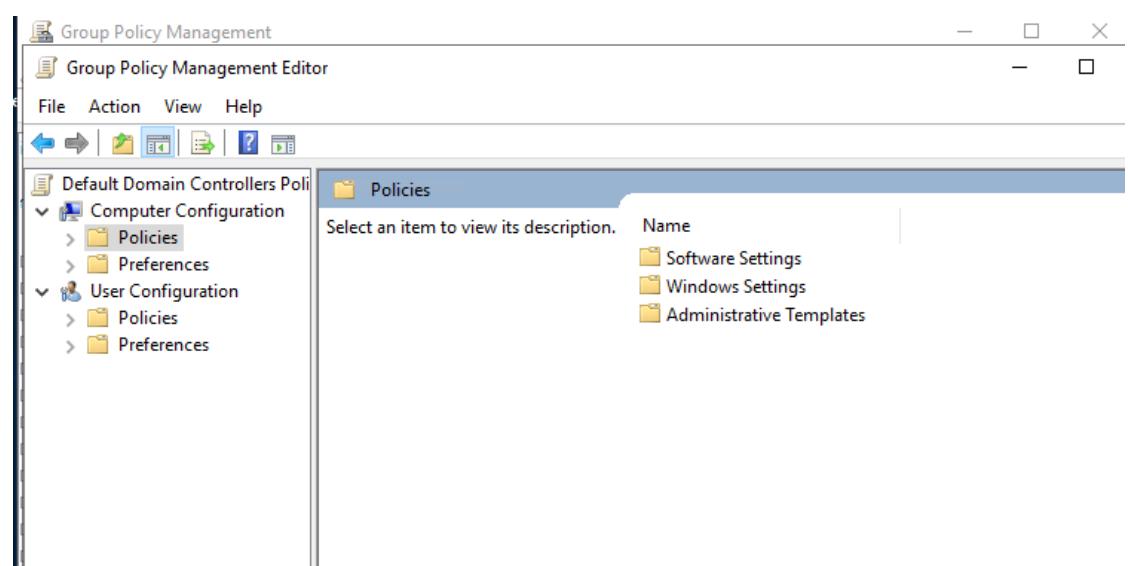
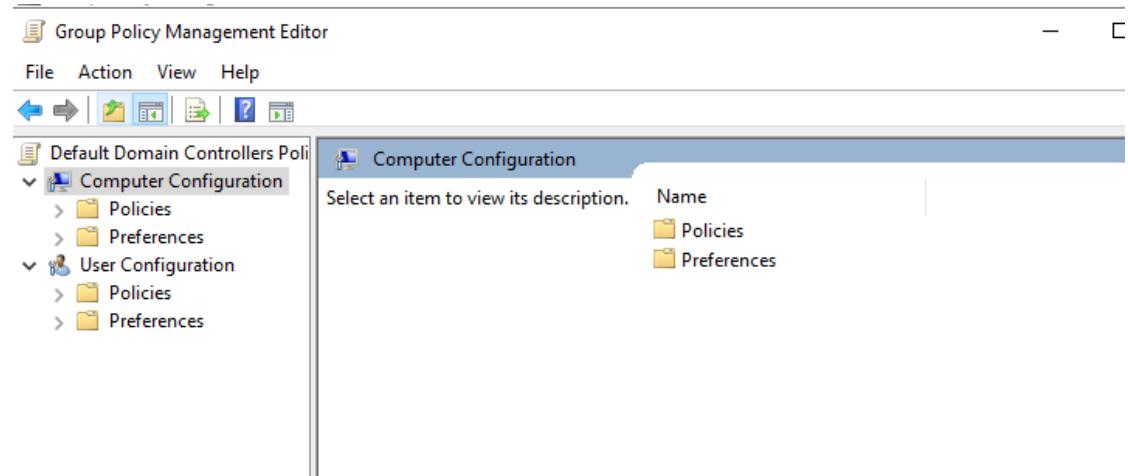
Open the Group Policy Management Console, click **ITCamp.Local**, and then double-click **Domain Controllers**.

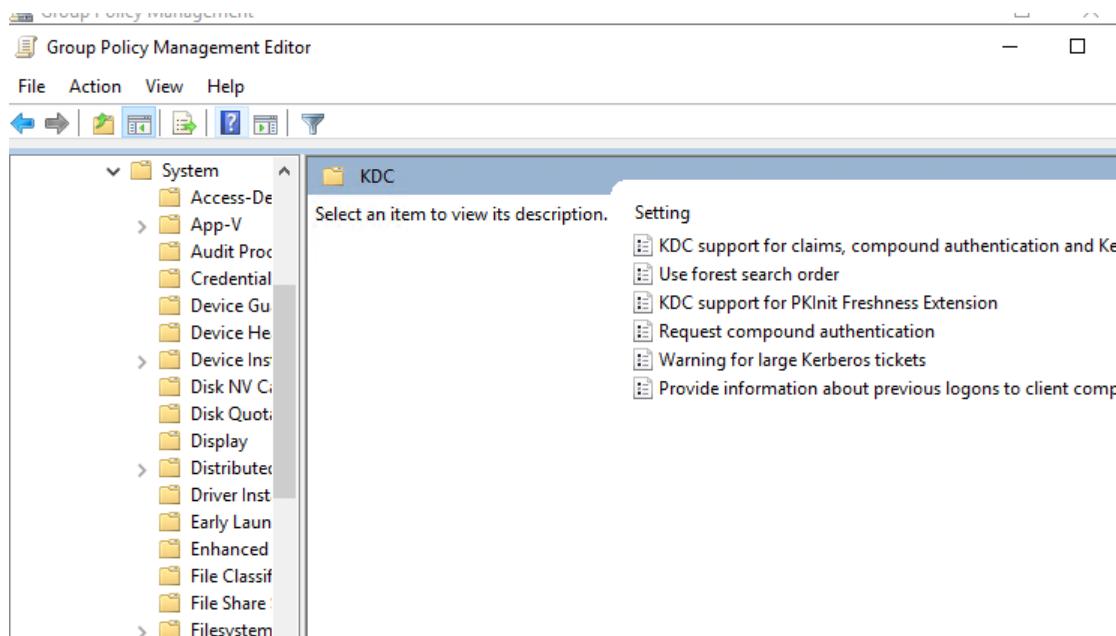
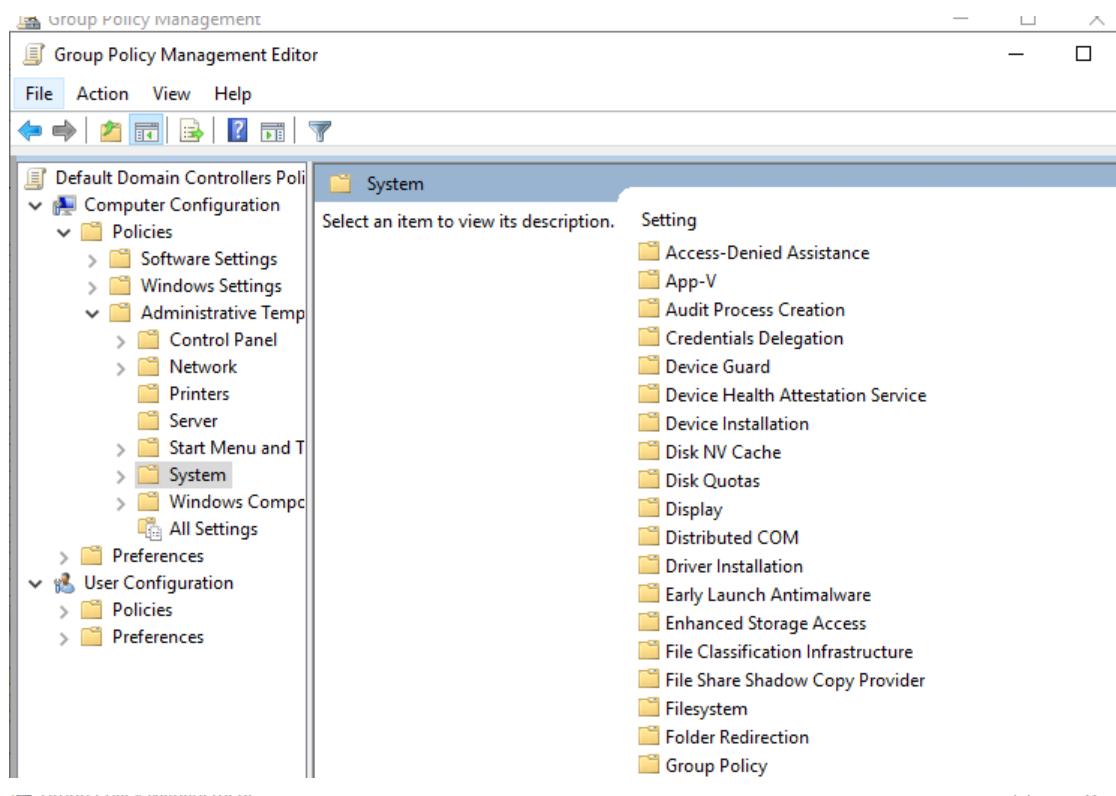


Right-click **Default Domain Controllers Policy**, and select **Edit**.

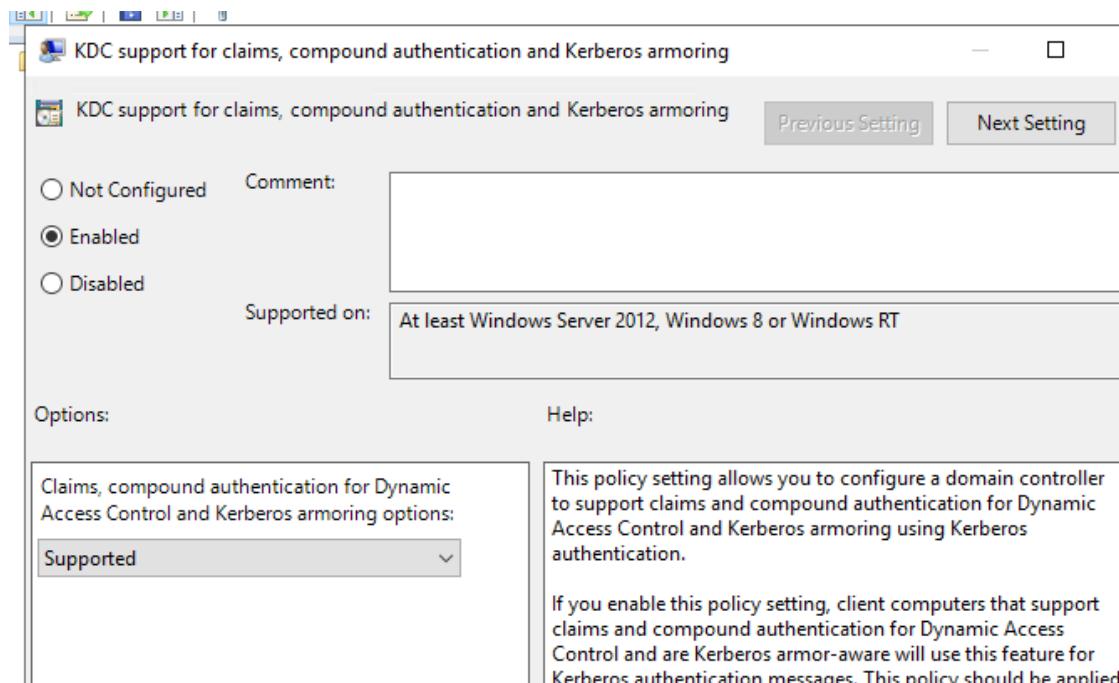


In the Group Policy Management Editor window, double-click **Computer Configuration**, double-click **Policies**, double-click **Administrative Templates**, double-click **System**, and then double-click **KDC**.





Double-click **KDC support for claims, compound authentication, and Kerberos armoring** and select the option next to **Enabled**. You need to enable this setting to use Central Access Policies.



Open an elevated command prompt, and run the following command:

```
gpupdate /force
```

```
PS C:\Users\Administrator> gpupdate /force
Updating policy...
Computer Policy update has completed successfully.
```

Now we will configure the Claim Type for Users. We will add existing Active Directory attributes to the list of attributes that we can use when evaluating dynamic access control.

Open the **Active Directory Administrative Center** to start configuring the Dynamic Access Policy (DAP).

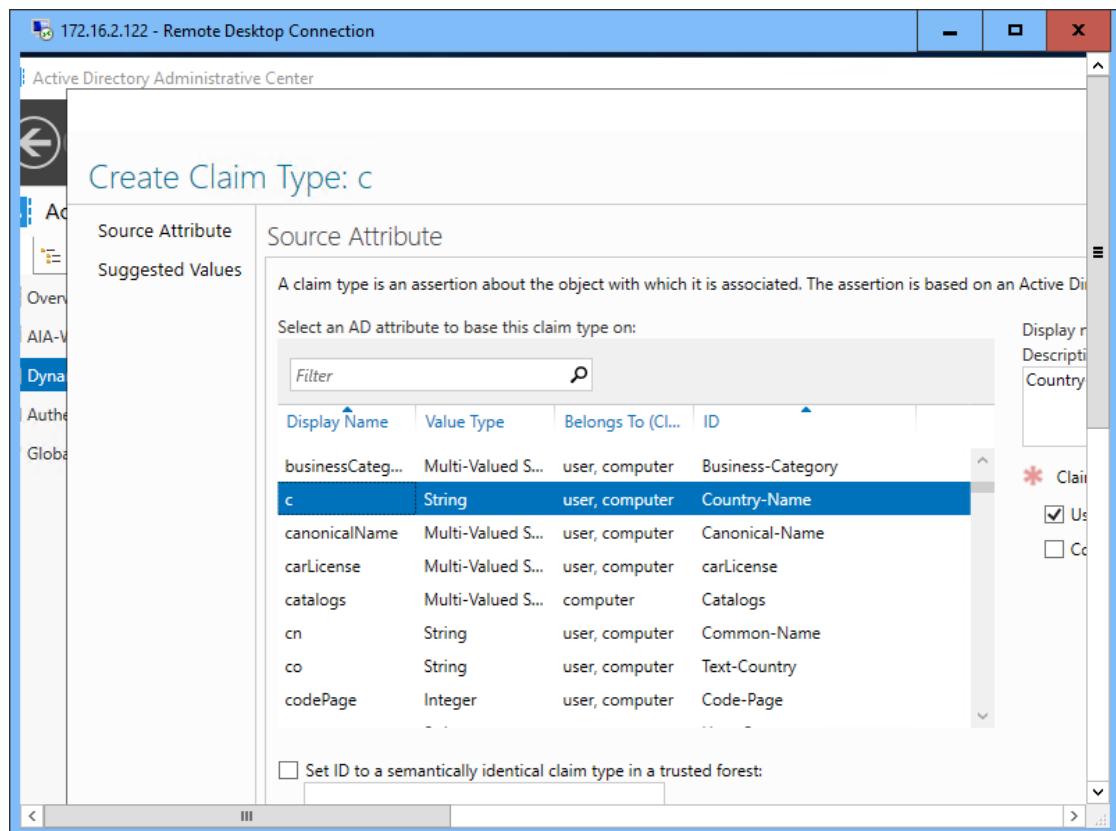
Active Directory Administrative Center

Name	Type	Description
Central Access Policies	msAuthz-C...	
Central Access Rules	msAuthz-C...	
Claim Types	msDS-Clai...	
Resource Properties	msDS-Reso...	
Resource Property Lists	Container	

In the Claim Type Section, click "New" and "Claim Type" in the task pane

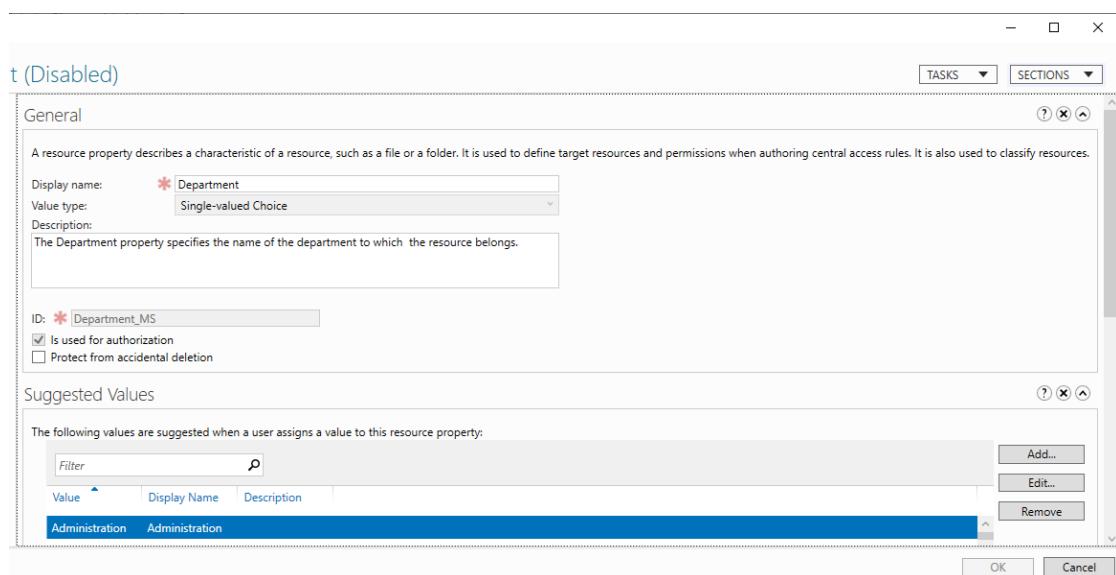
The screenshot shows the 'Dynamic Access Control' section with the 'Claim' item selected. A context menu is open, showing 'New' and 'Claim Type' as options.

Select the attribute we want to use.

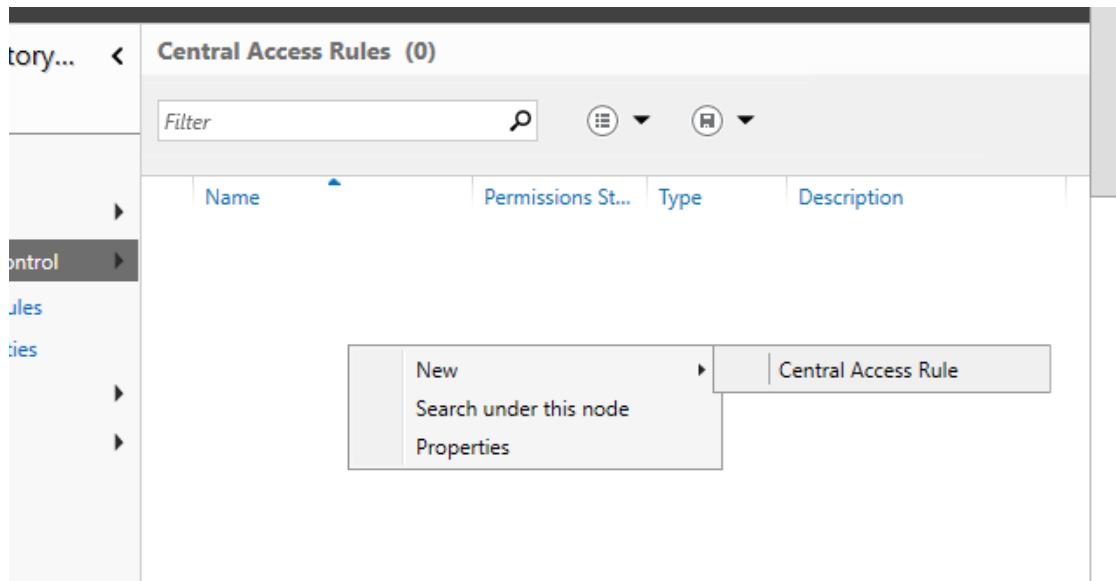


In this step, we will configure the properties which will be downloaded by file servers and used to classify files or directories or shares. The DAC rules will compare user attribute values with resource properties. We can enable existing properties or create new ones.

Click on resource property and here you can select the existing resource properties or also you can create the new ones, I have selected Department.



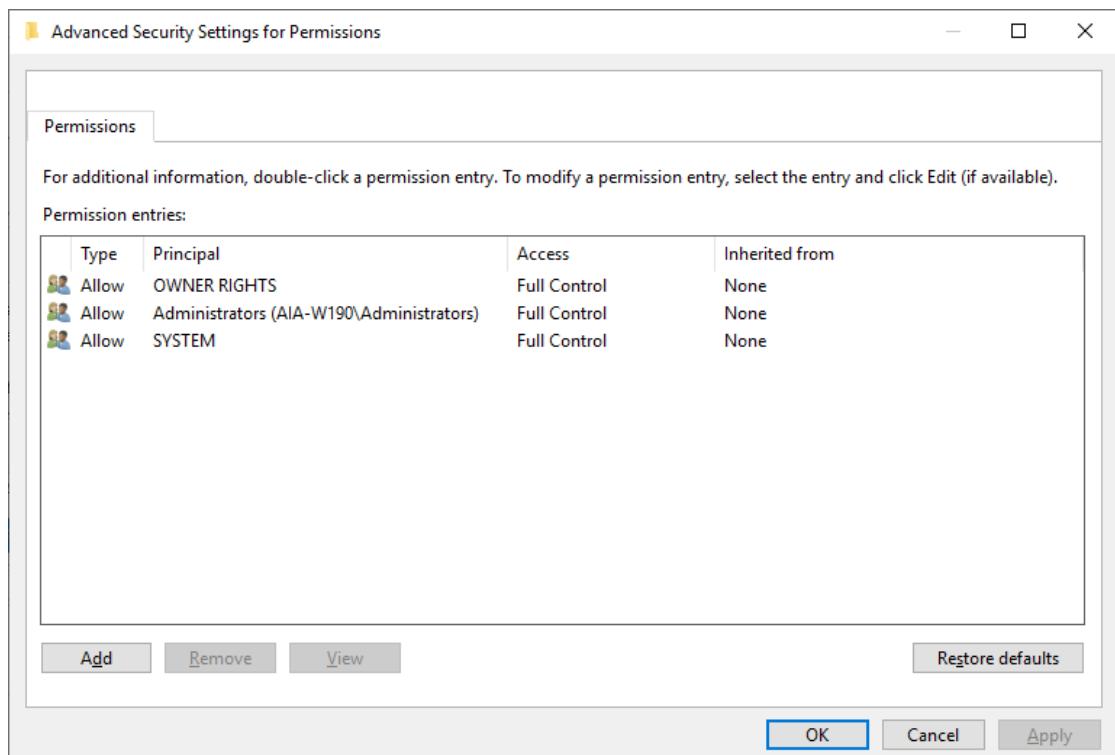
In the Central Access Rule section, click "New" and "Central Access Rule"



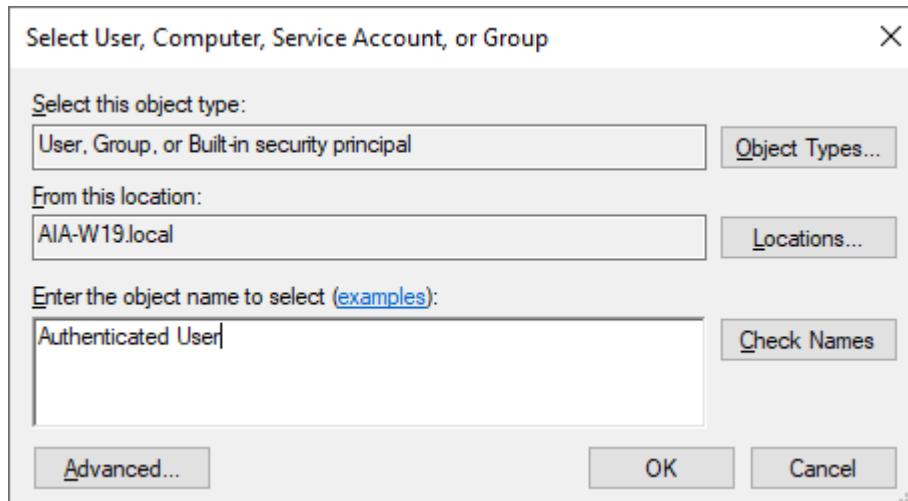
Give it a name in the Create Central Access Rule form.

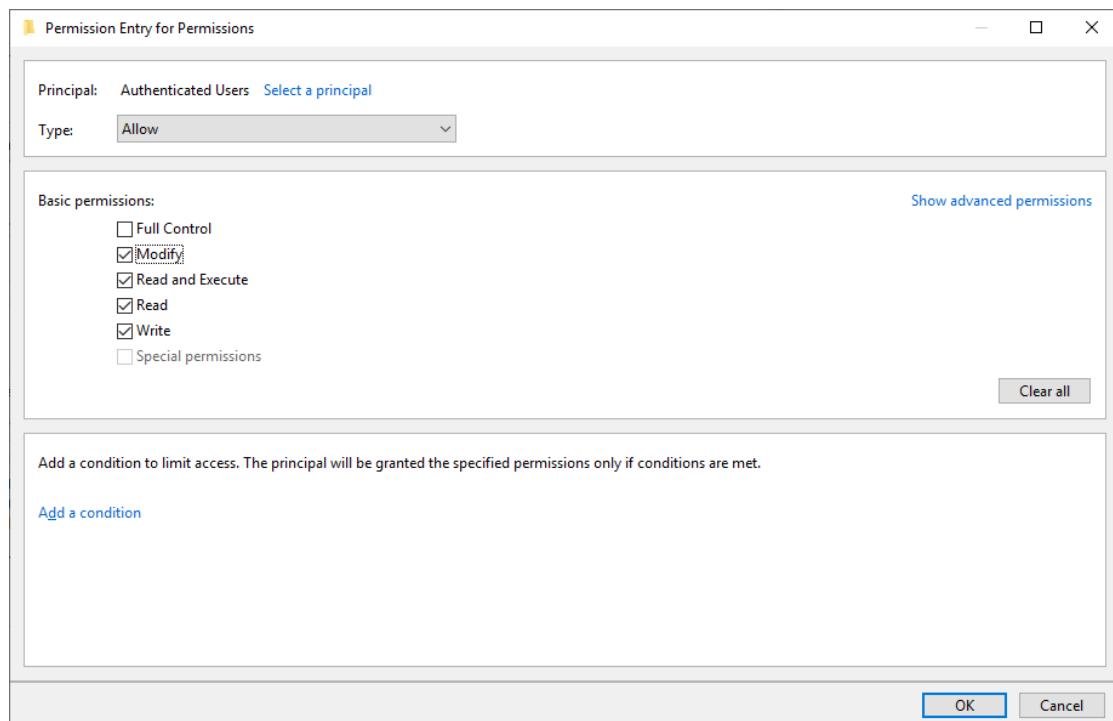
Type	Principal	Access
Allow	OWNER RIGHTS	Full Control
Allow	BUILTIN\Administrators	Full Control
Allow	NT AUTHORITY\SYSTEM	Full Control

In the Permission section, click "Use Following Permissions" and click "Edit"



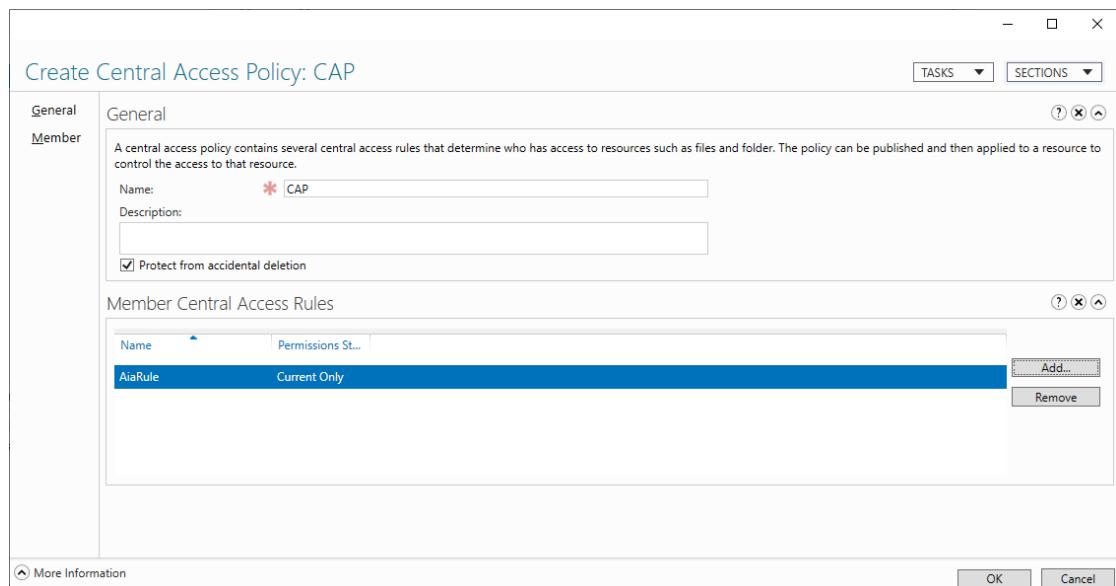
Click "Add" and in the following "permission Entry for Permissions" select The "Authenticated User" as the principal and set the following conditions.



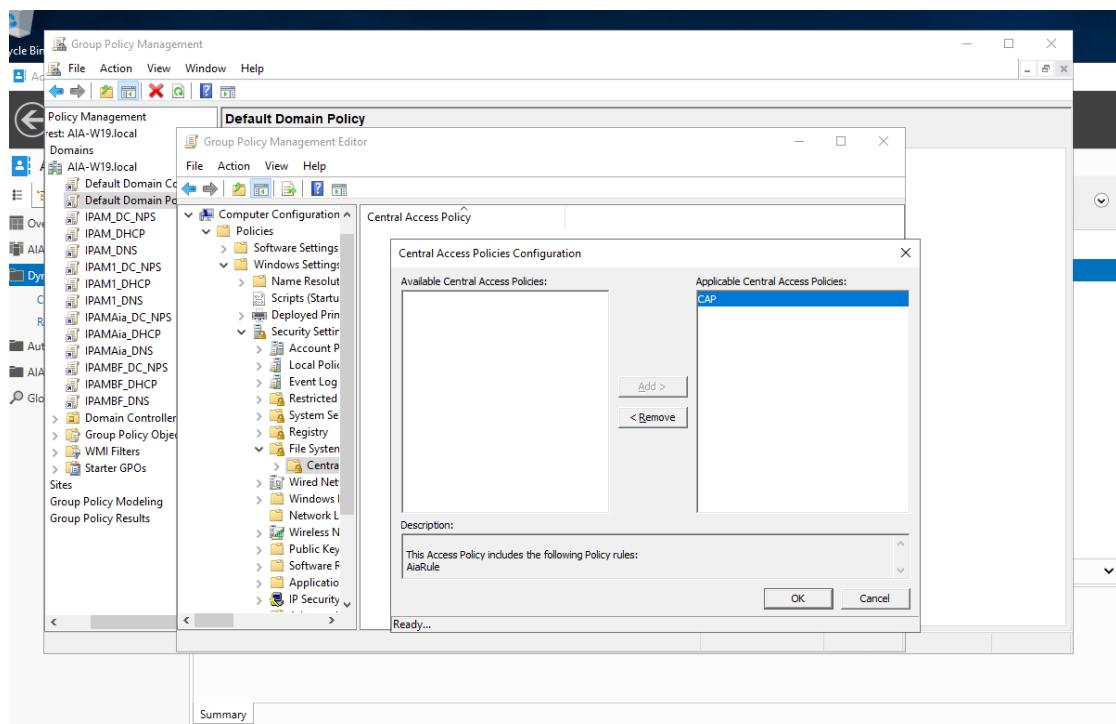


Click "OK" you are back to the DAC configuration screen.

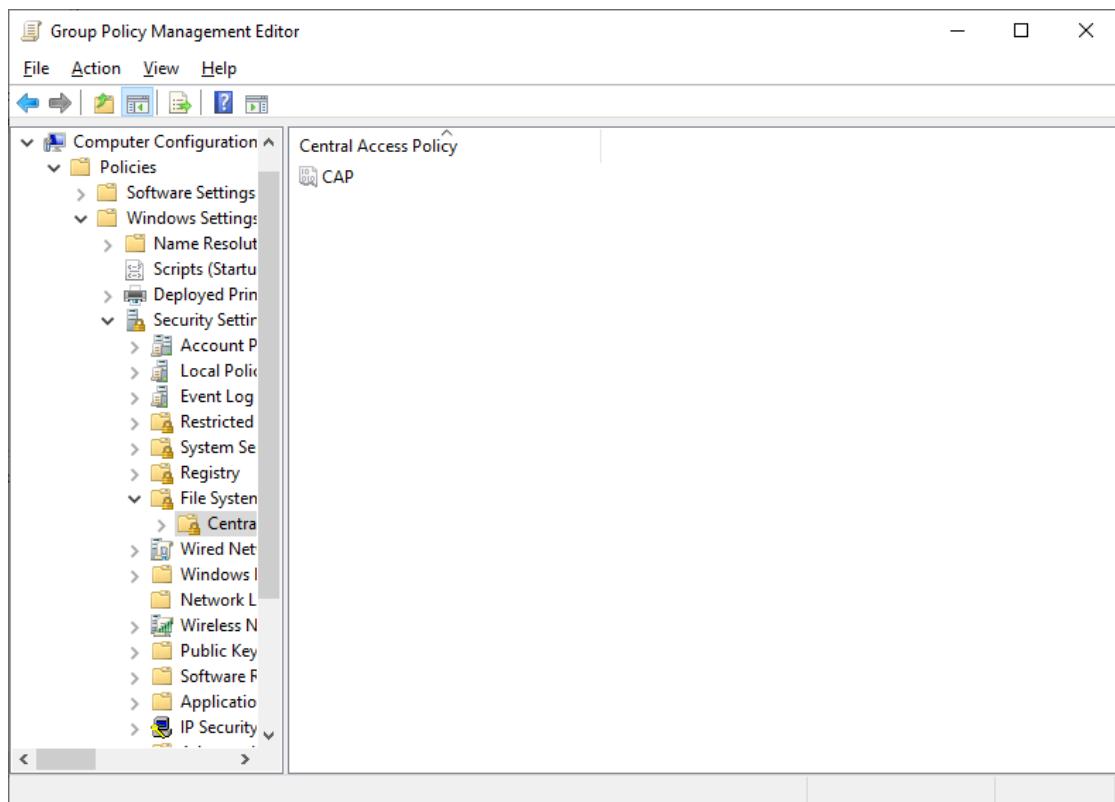
In the Central Access Policy, click "New" and "Central Access Policy" and give the new policy a name in the "Create Central Access Policy" form. We named our CAP. We also need to Add the Central Access Rule you created earlier to the policy.



Once that is created we need to tell AD about the policy. In the "Group Policy Management Console" we edited the "Default domain policy" but you can apply a different policy as you see fit. And in the Computer Management→Policies→Windows Settings→Security settings→File System→Central Access Policy, right-click the right pane and select manage Central Access Policy.

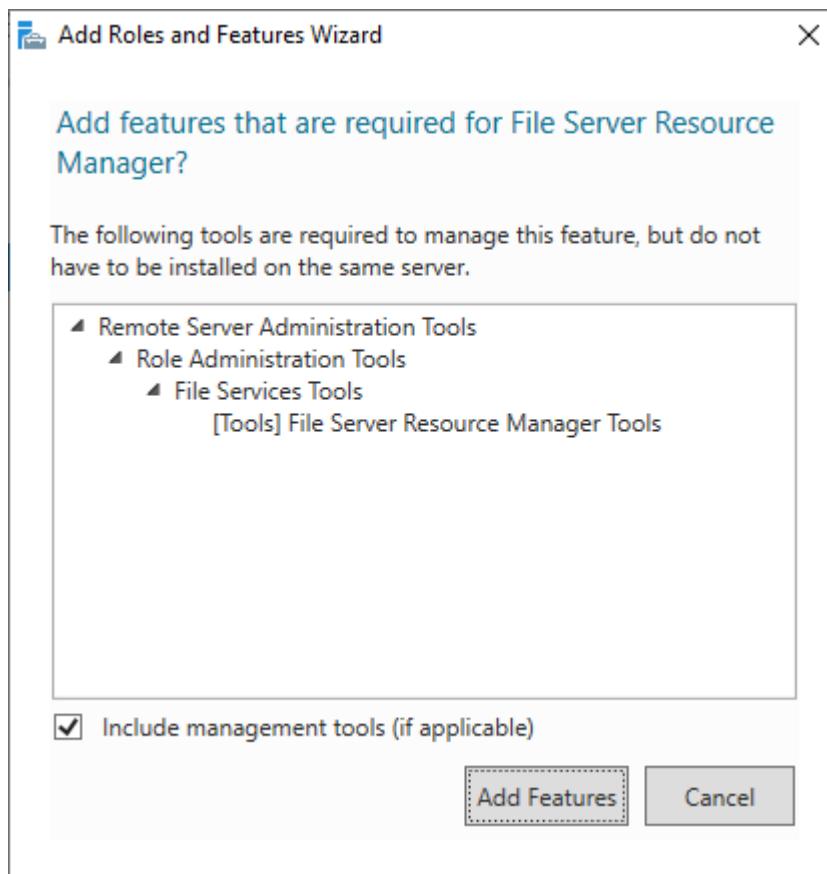


Add the Policy you created to the Applicable Central Access Policies.



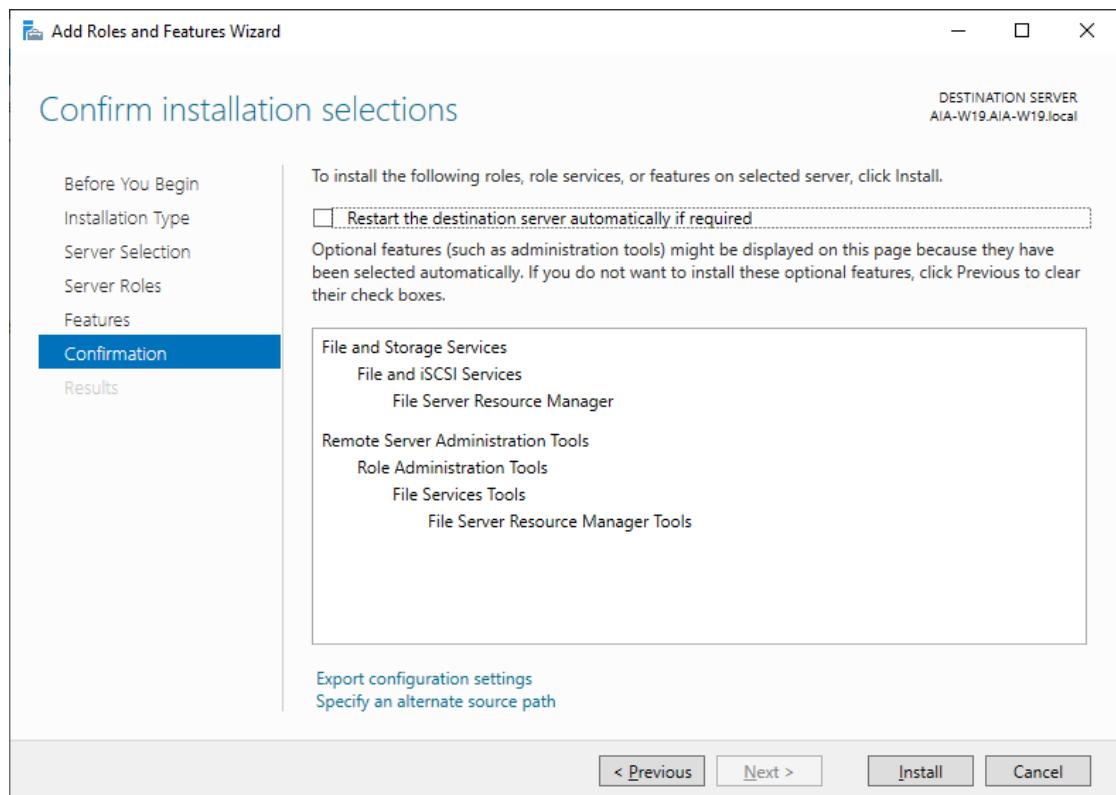
To configure the shares the File Server Resource Manager must be installed on the server that will be used as the files server. In our case the file server we are using is **AIA-W19.local**.

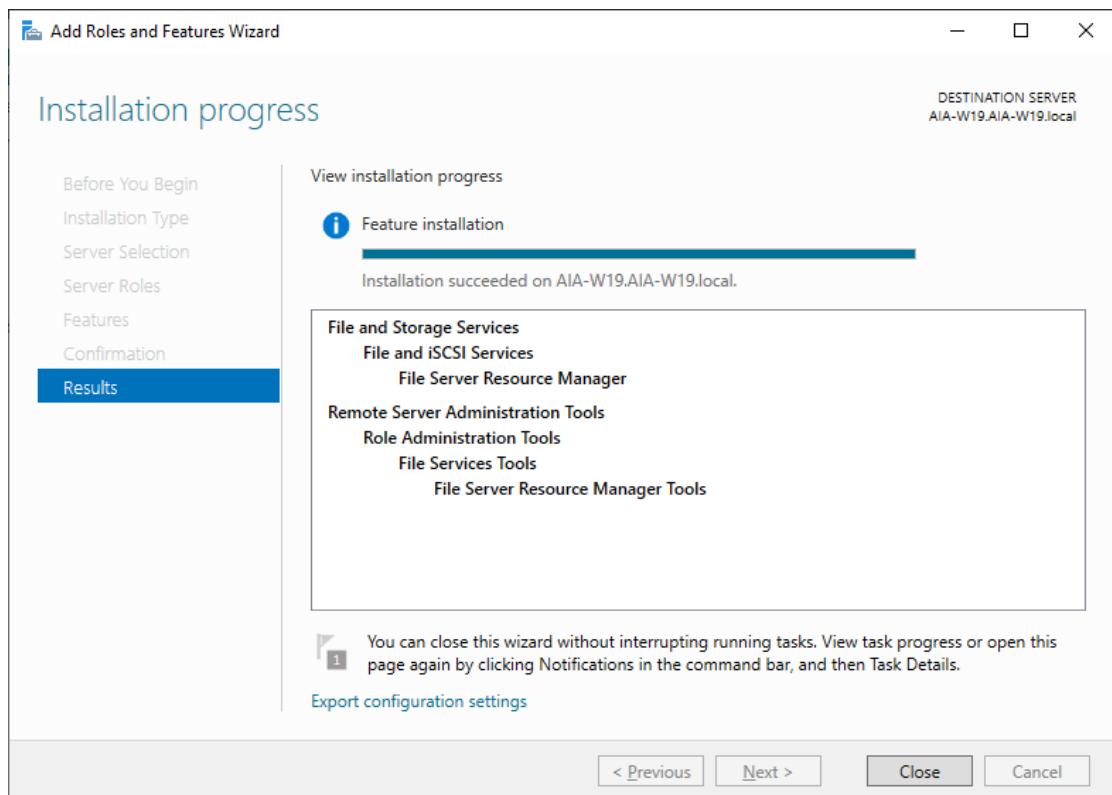
Logon **AIA-W19.local** as **AIA-W19\administrator**, in Server Manager, click **Add Roles and Features**. On the **Before you begin** page, click **Next**. On the **Select Server Roles** page, expand **File and Storage Services**, select the check-box next to **File and iSCSI Services**, expand, and select **File Server Resource Manager**.



On the **Confirm installation selections** page, click **Install**.

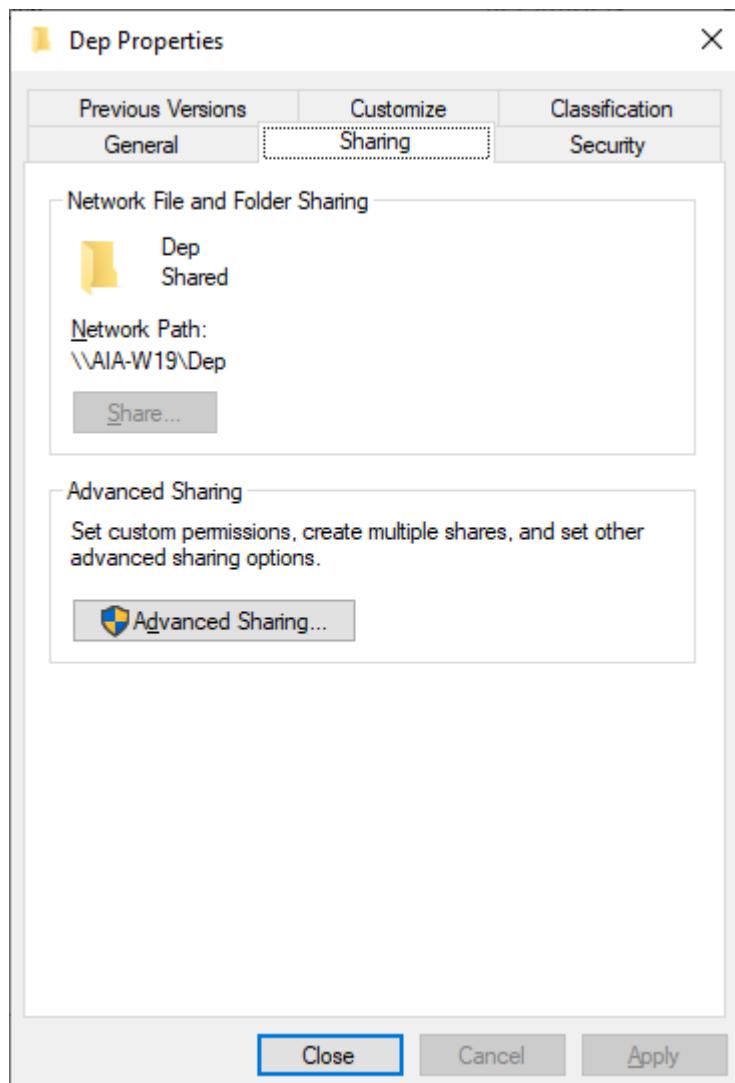
On the **Installation progress** page, click **Close**



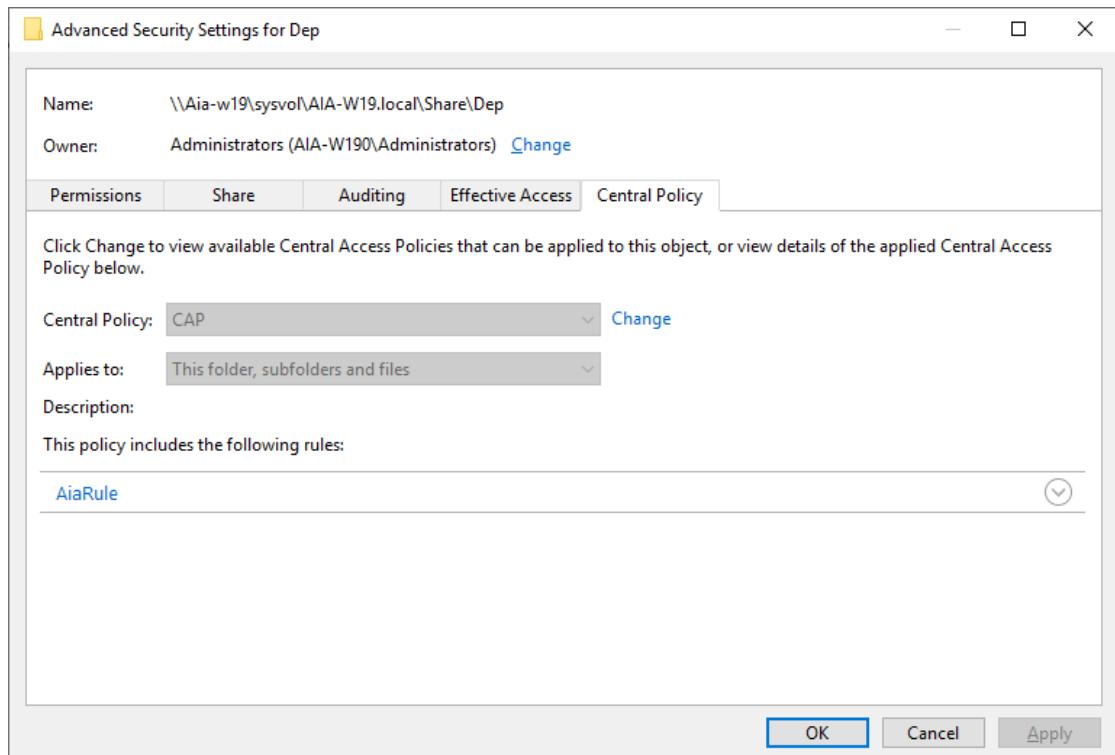


Now we will create a share files select all defaults to complete this part.

Once the shares have been created, we need to go the location where the directory has been created and modify the properties of each folders.



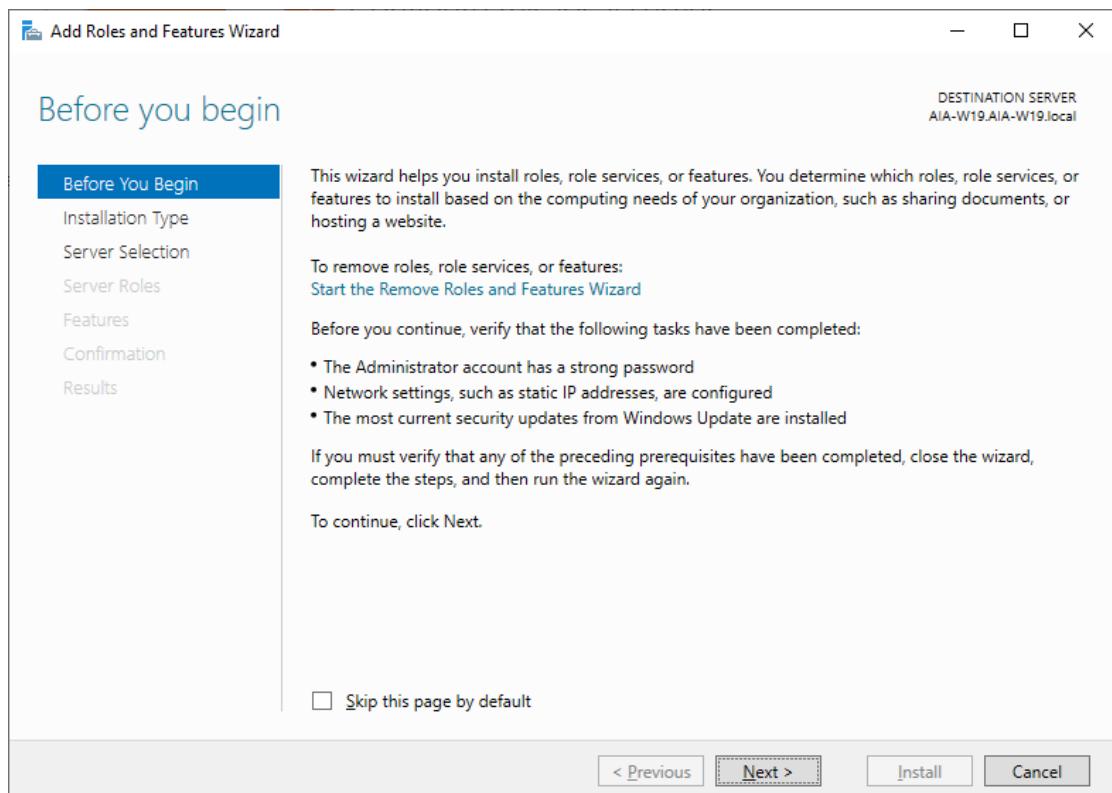
And in the advanced Security Settings, in the Central Policy Tab, change the "No central Access Policy" to "CAP" the policy we defined. You can test to see if everything worked well by using the effective Access tab.



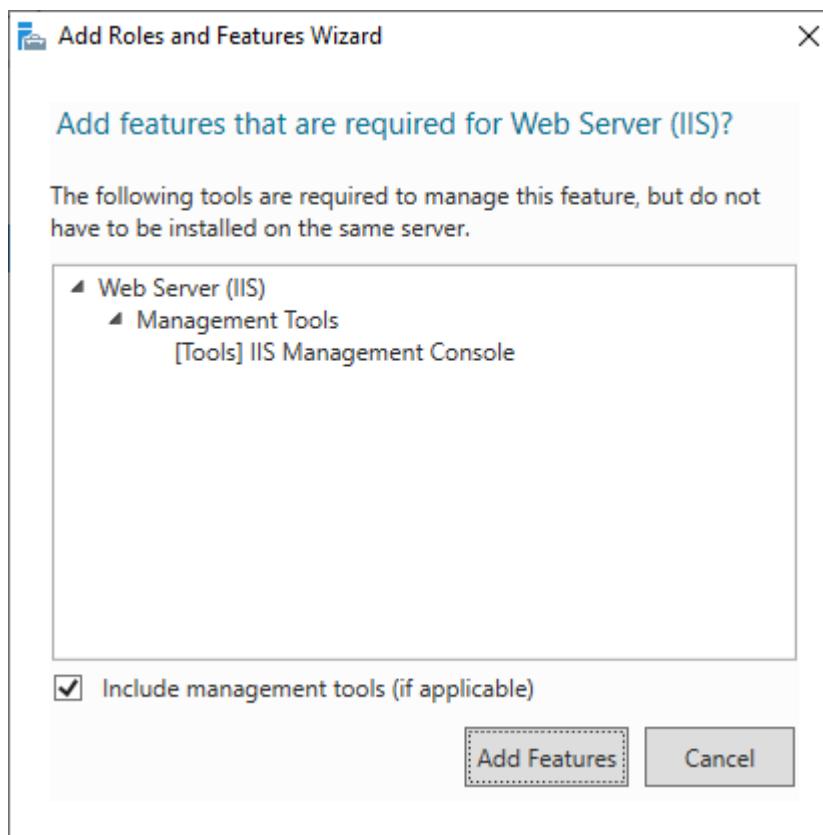
➤ Web Server Management with IIS:

Internet Information Services is a flexible, general purpose web server from Microsoft that runs on Windows systems to serve requested HTML pages or files. An IIS web server accepts requests from remote client computers and returns the appropriate response. It allows web servers to share and deliver information across local area networks and wide area networks.

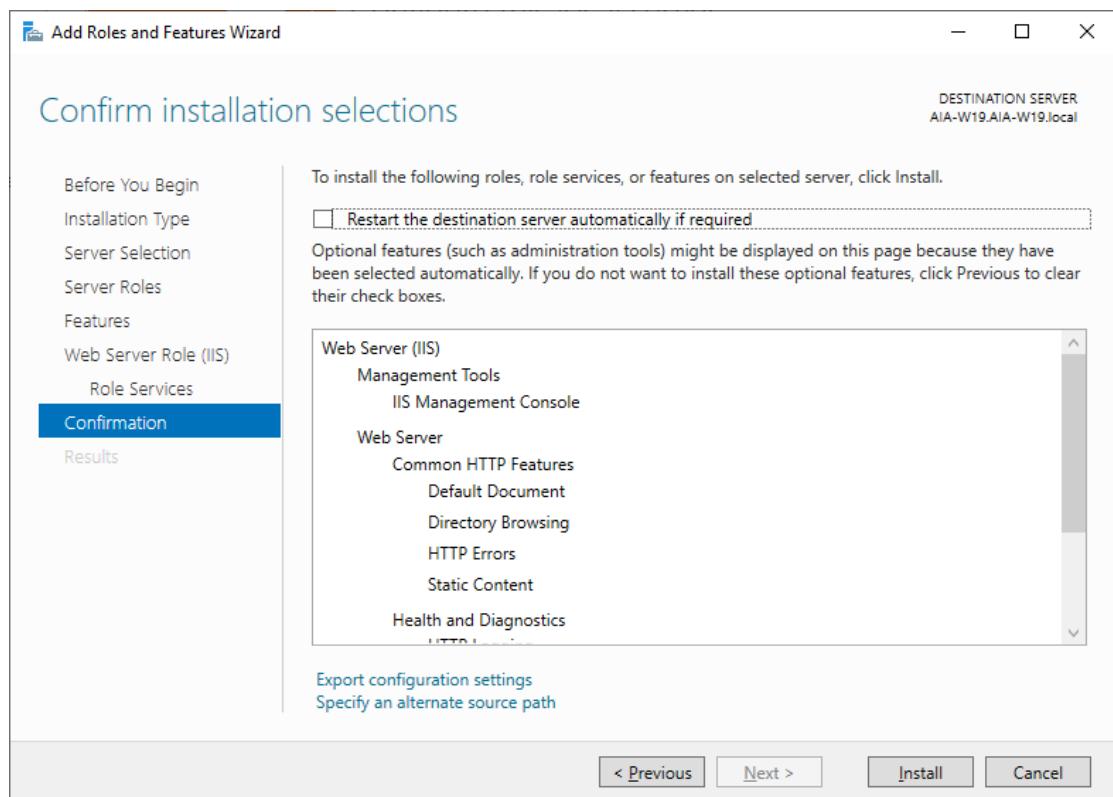
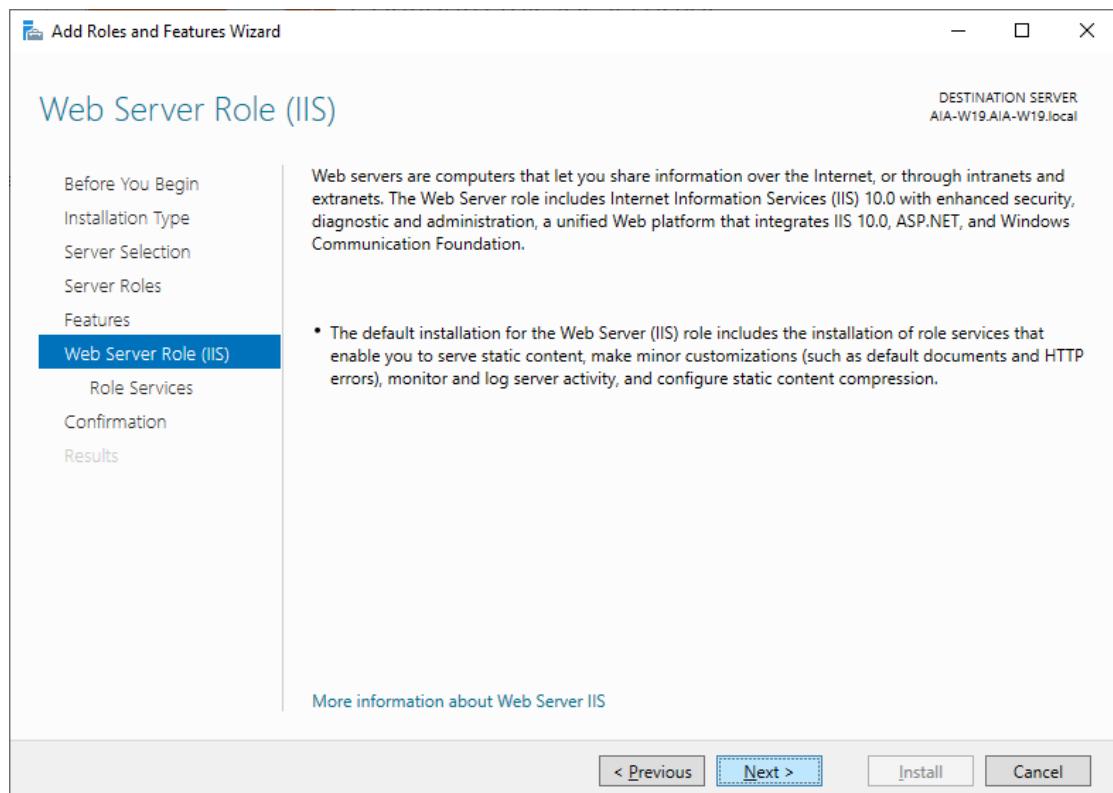
Open the *Server Manager* and click Add Roles and Features:



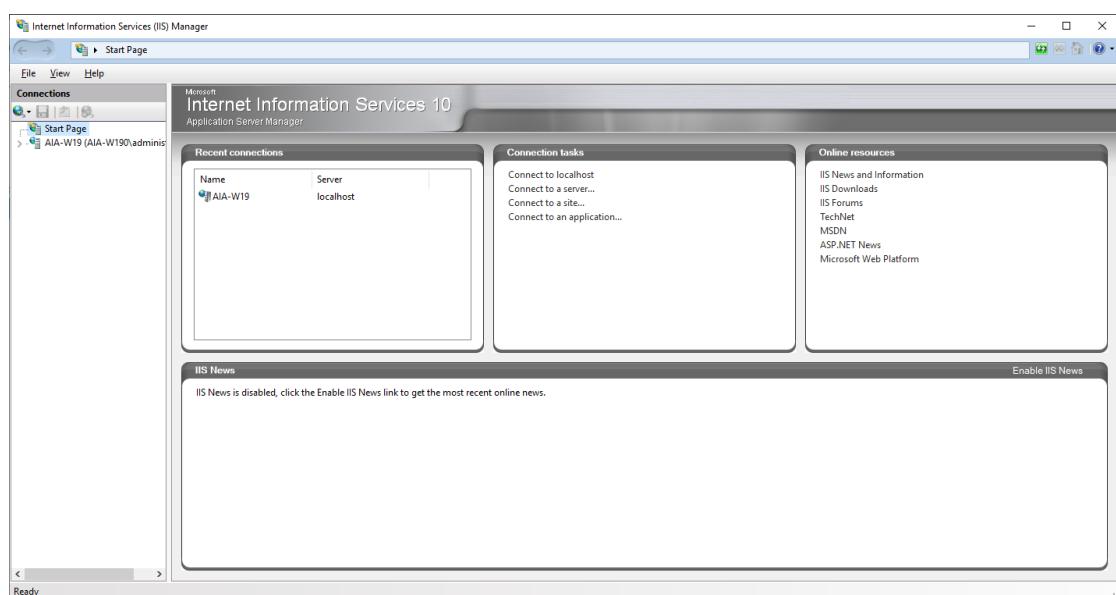
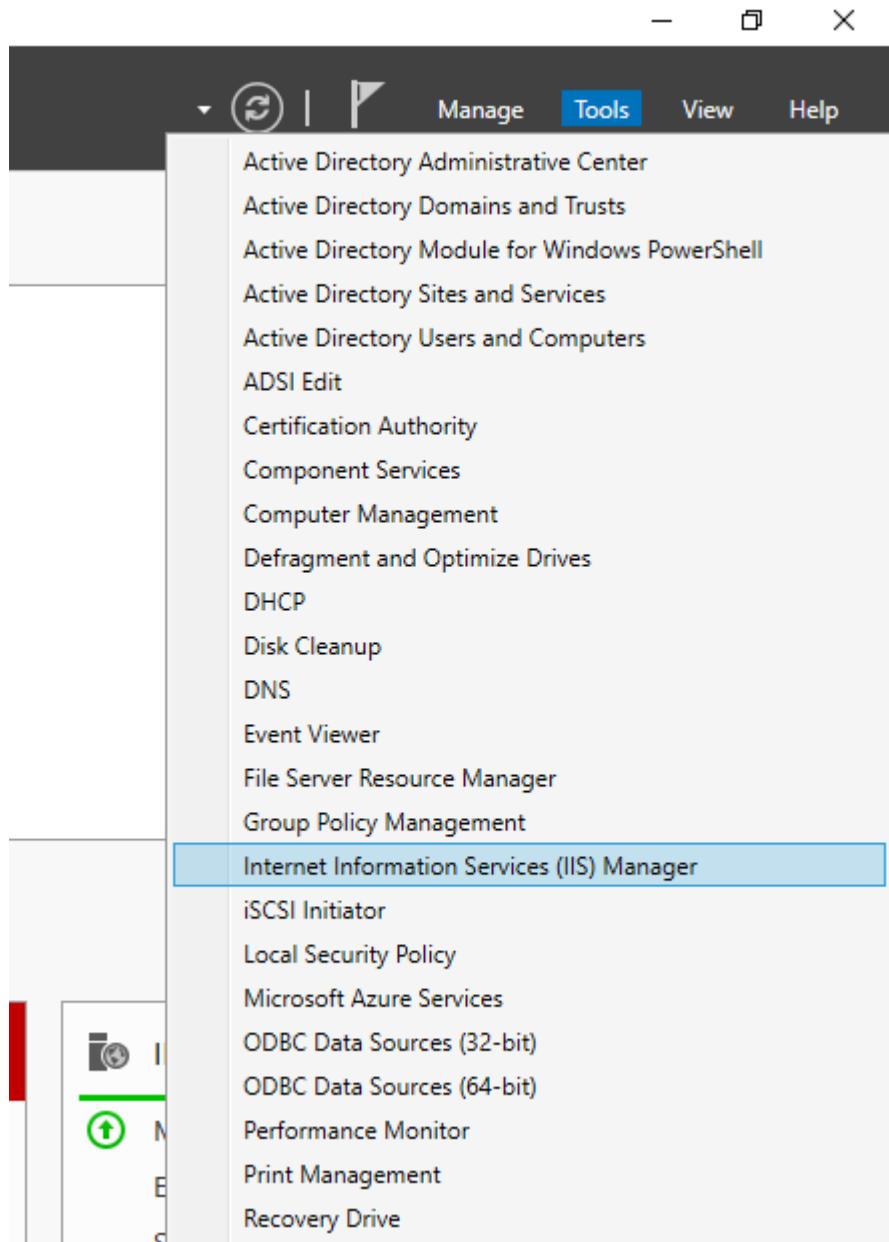
Select Web Server (IIS):



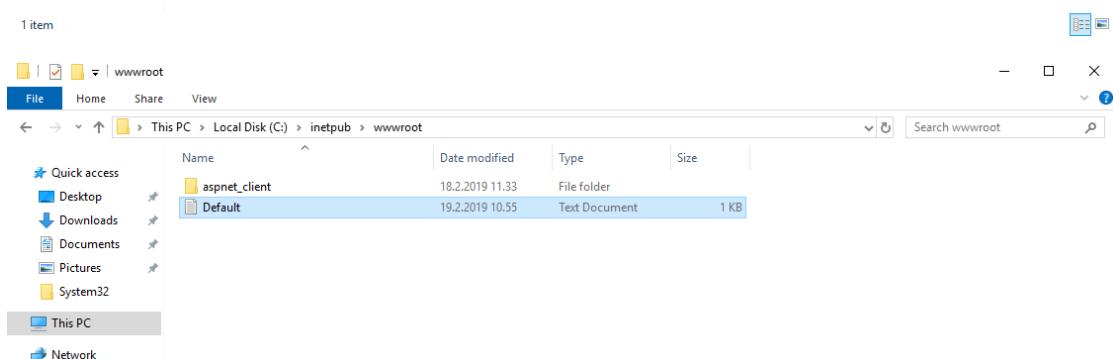
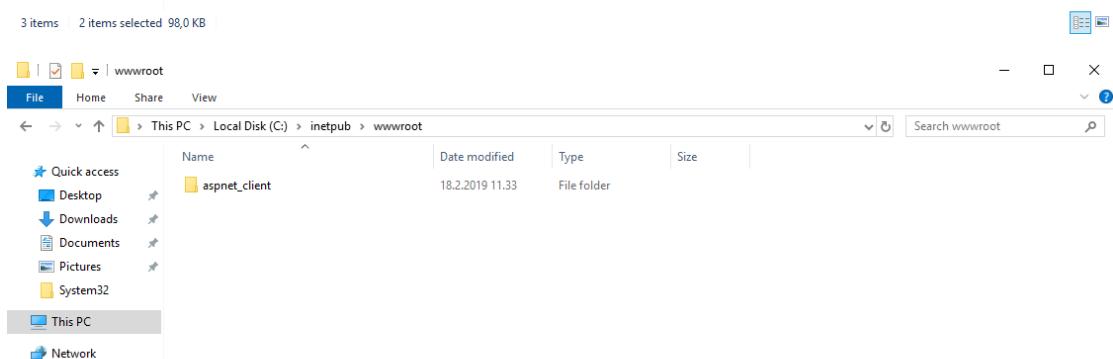
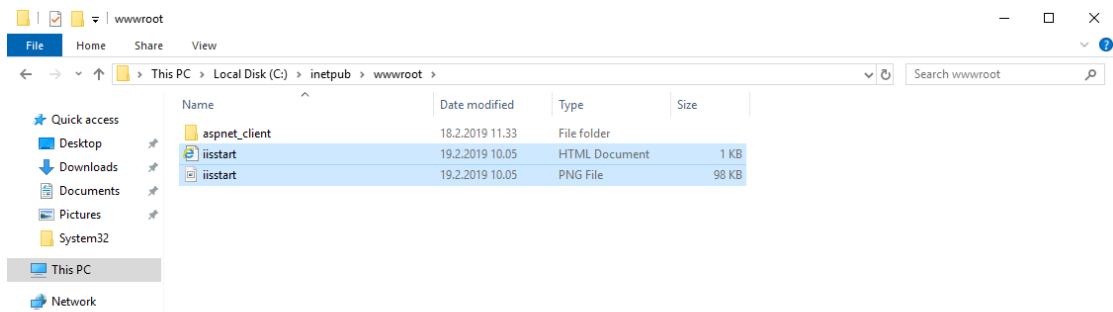
On the Role Services selection list, select all of the role services, and click Next to continue.



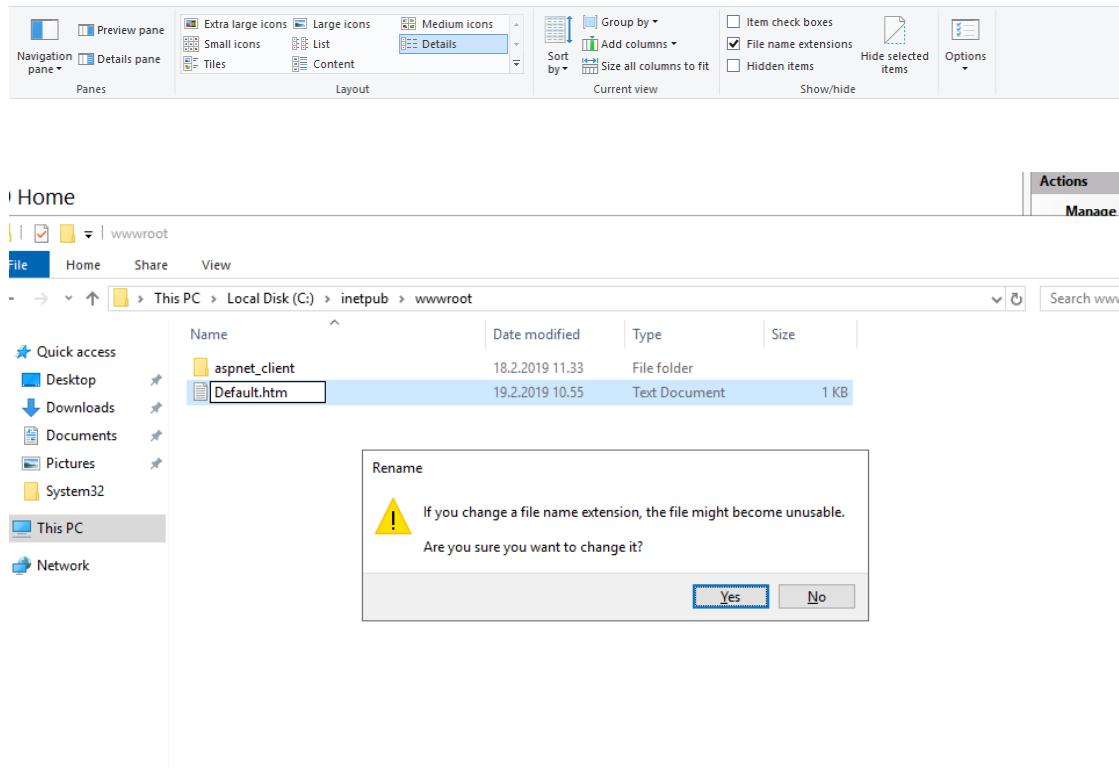
By clicking on Tools in the dashboard and selecting Internet Services Manager to check the default website that available in the server.



We will delete all the files in the file path and create a new text file.



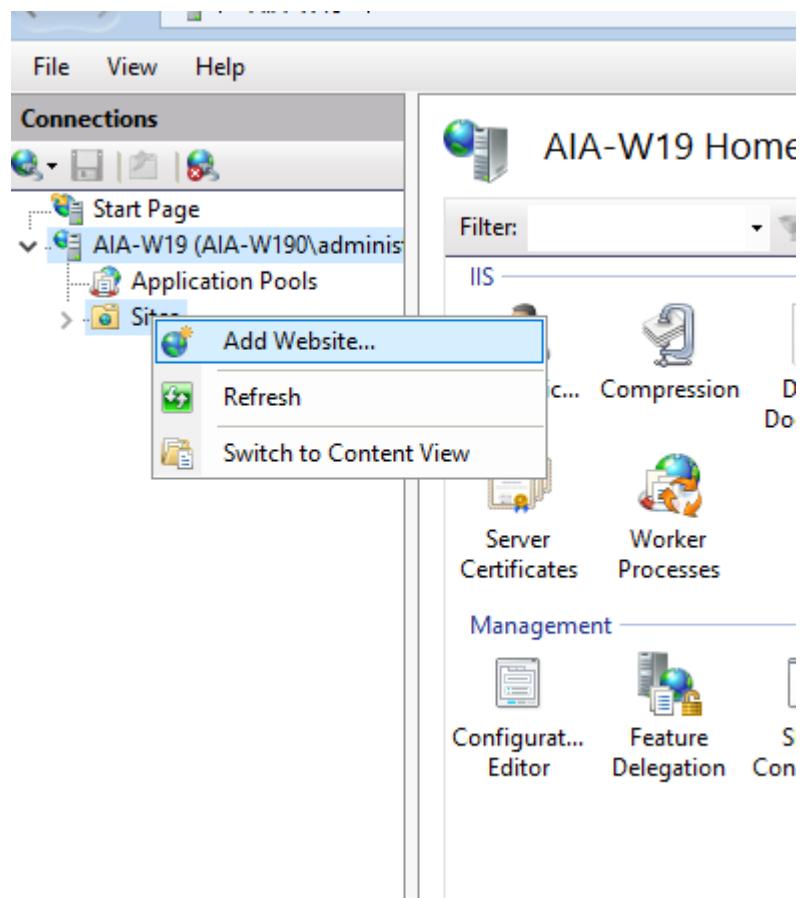
We need also to change the extension file by clicking on view and choose the extensions to change the file to HTML.

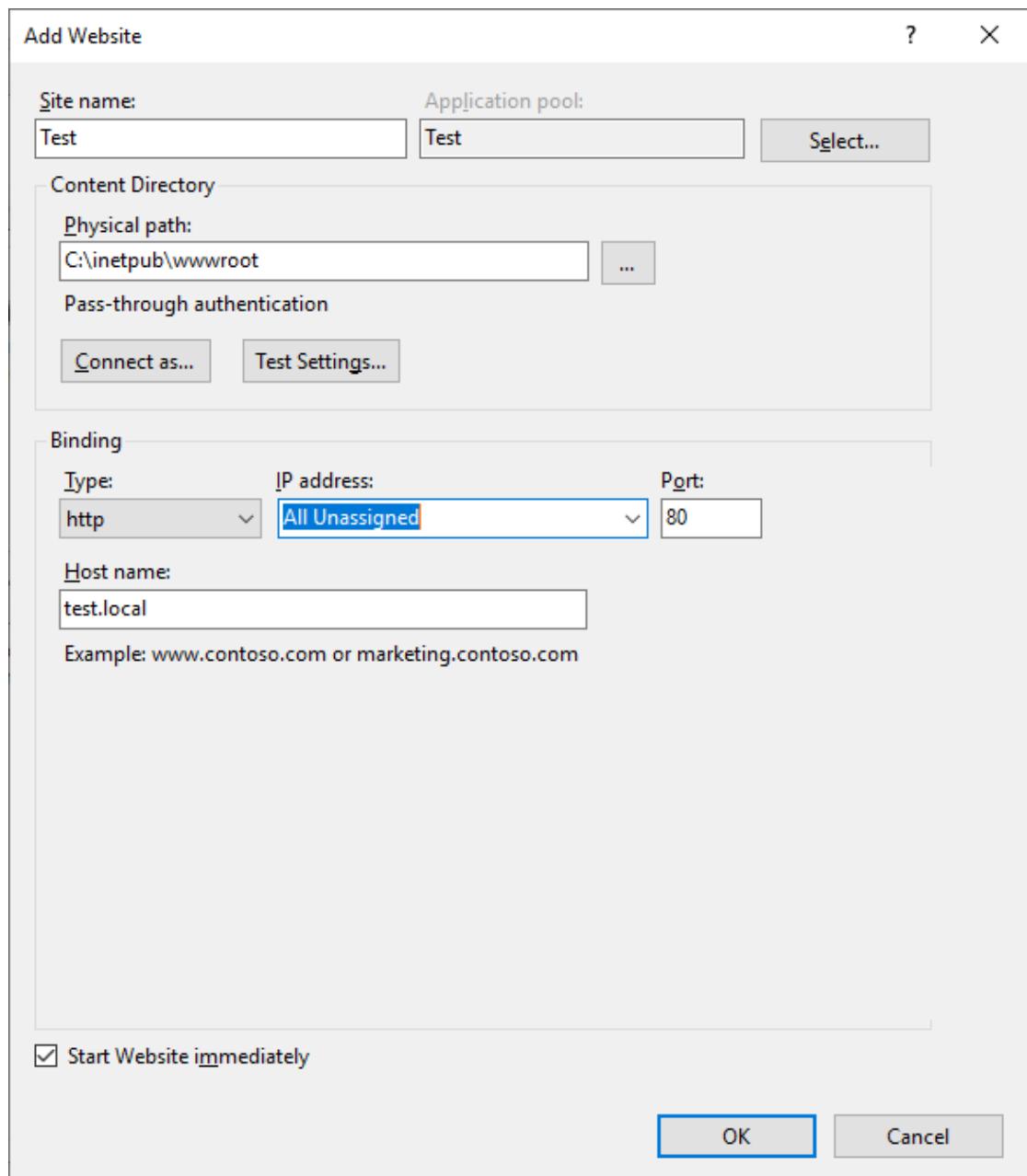


To test if it's working, by browsing using the IP address for the server.

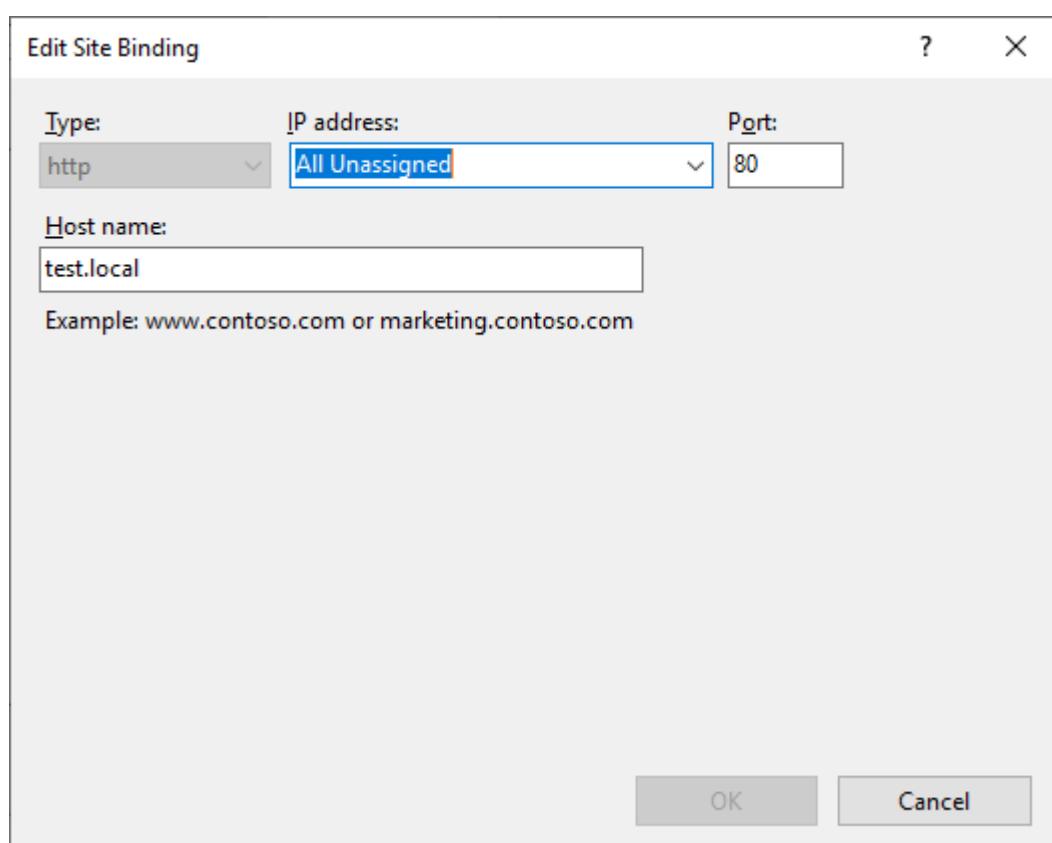
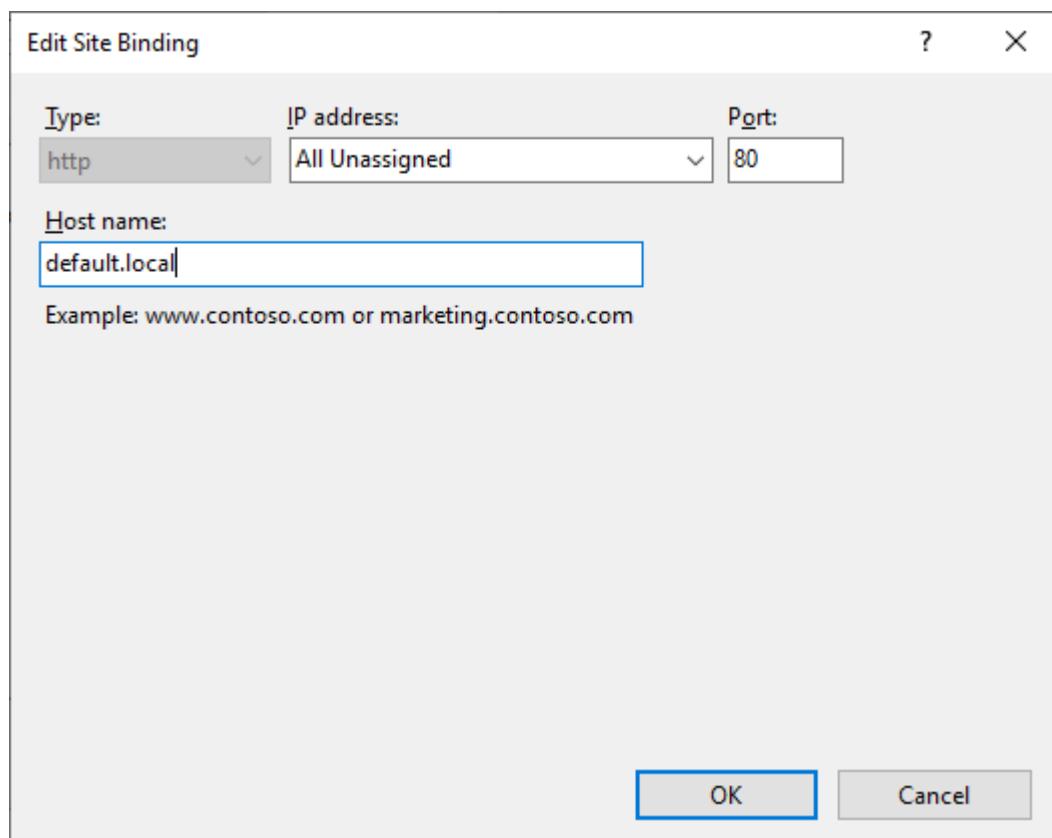


Also we can create a new website by right click on Sites and click create a new website





Now cause both of the websites will use the same IP address, so we can implement headers for each website to access the website with a shared IP and different name.

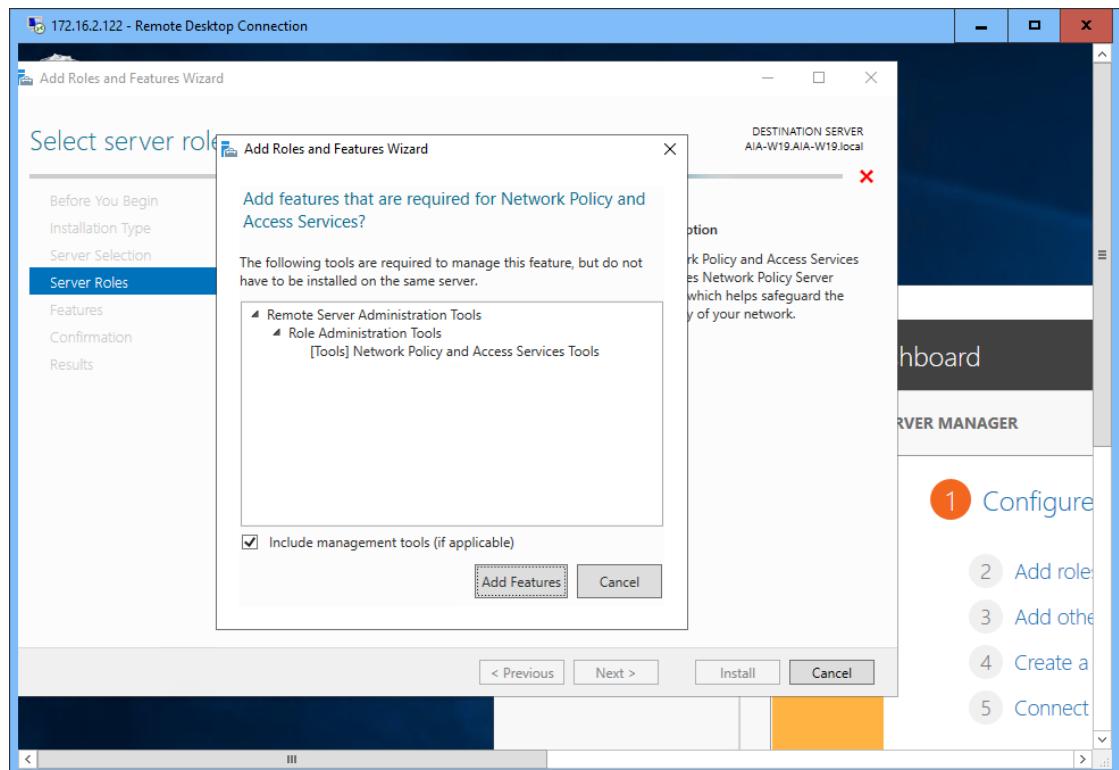


➤ **VPNs:**

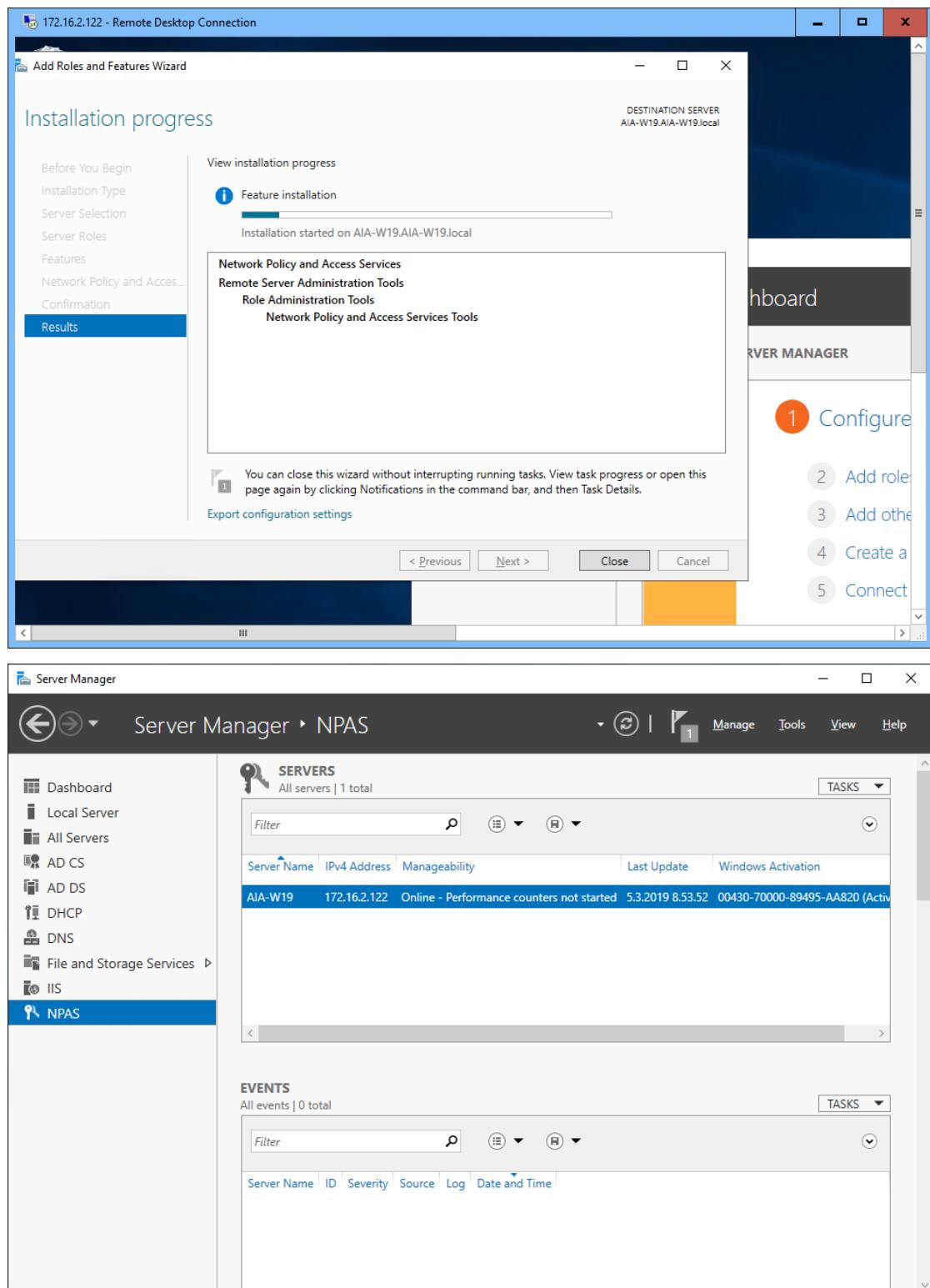
VPN used to provide access to a private network over a public network, the public network is often the Internet, but it could be leased lines that are shared by different companies. The VPN server has at least two network interface cards, one has public IP address and can be reached by user who access to the Internet. The other NIC has a private address connected to the internal network.

Installing the Network Policy and Access Services Role:

From the Server Manager > Local Server > Manage menu, choose the Add Roles and Features option. When we reach the Select Server Roles dialog box, scroll down until we find the Network Policy and Access Services option in the Roles list, and check the box beside it.

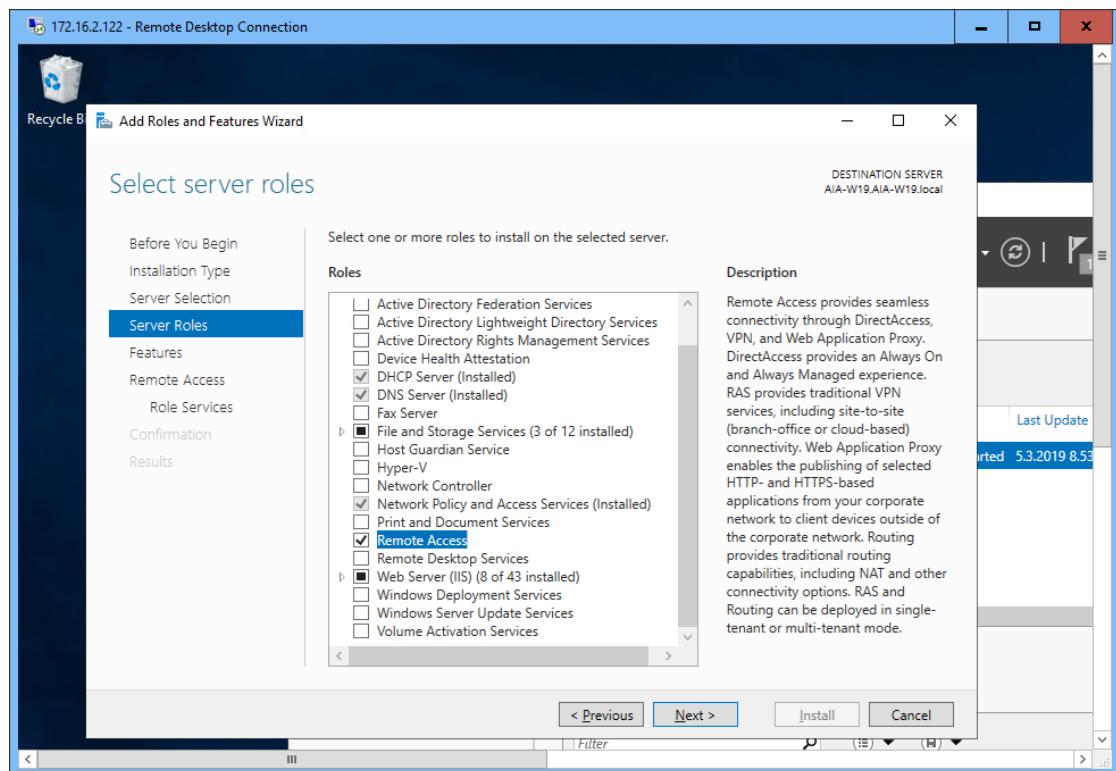


Add some required features here, such as the Remote Server Administration Tools (RSAT), so just click the Add Features button in the window that pops up.

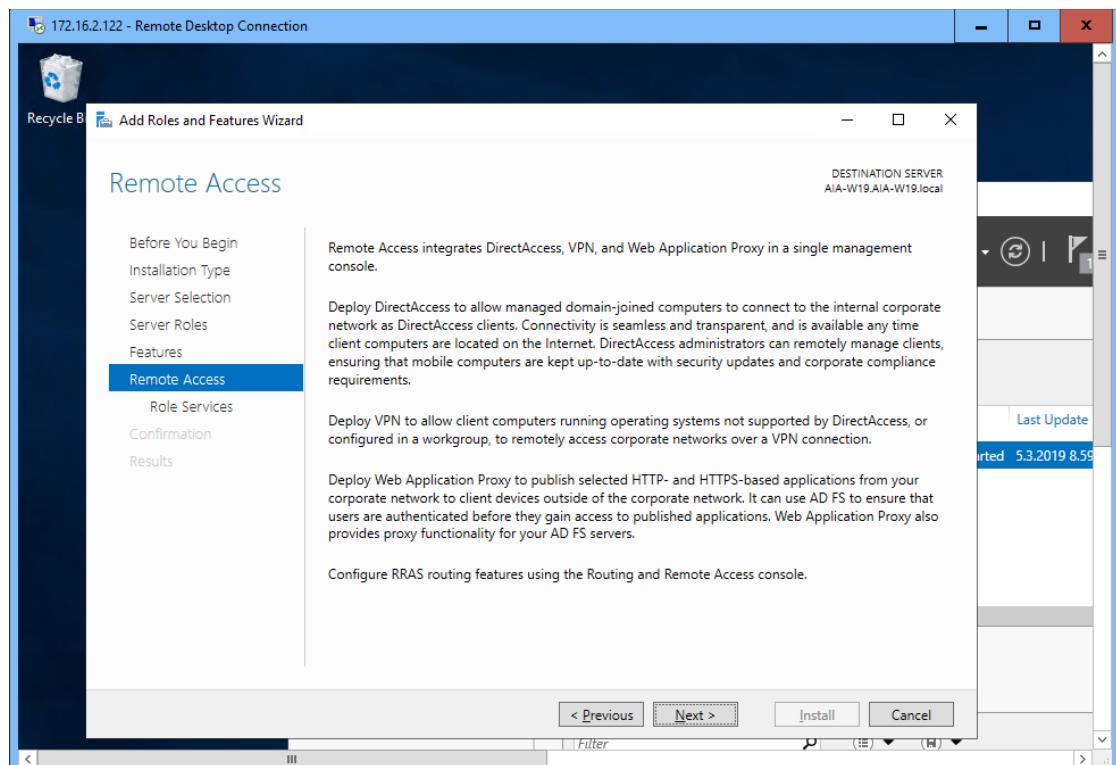


Installing the Remote Access Role:

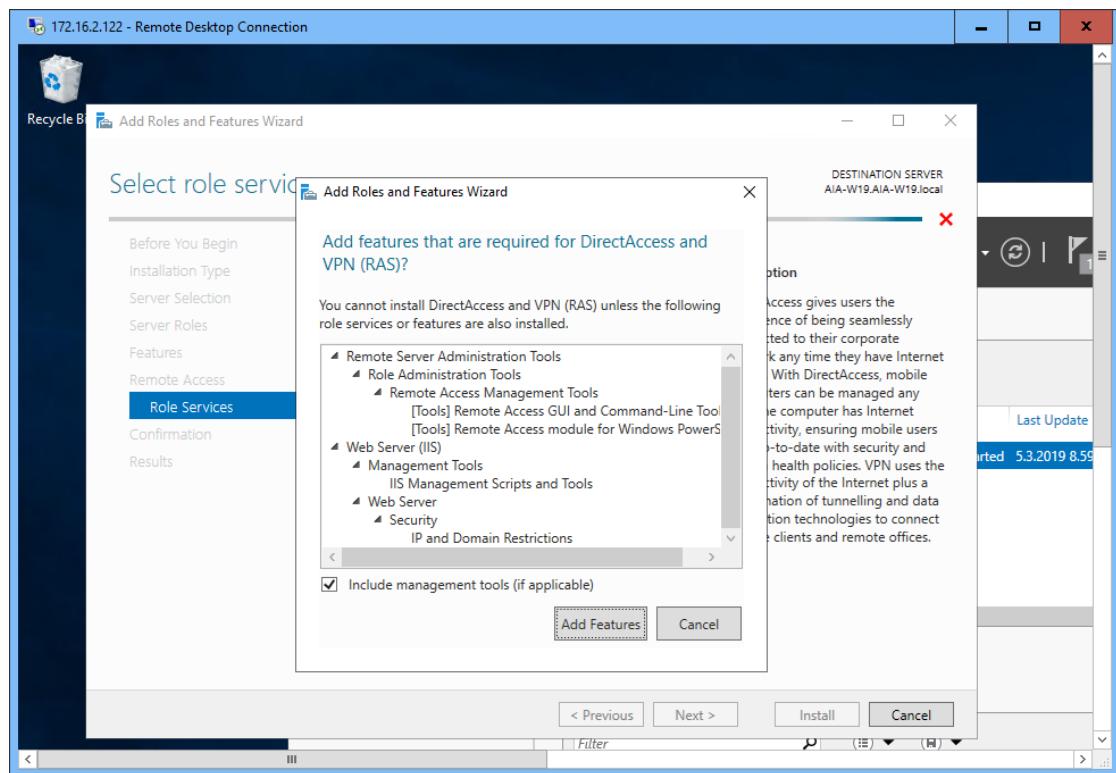
Server Manager > Local Server > Manage menu, choose the Add Roles and Features option. Scroll down to find Remote access option.



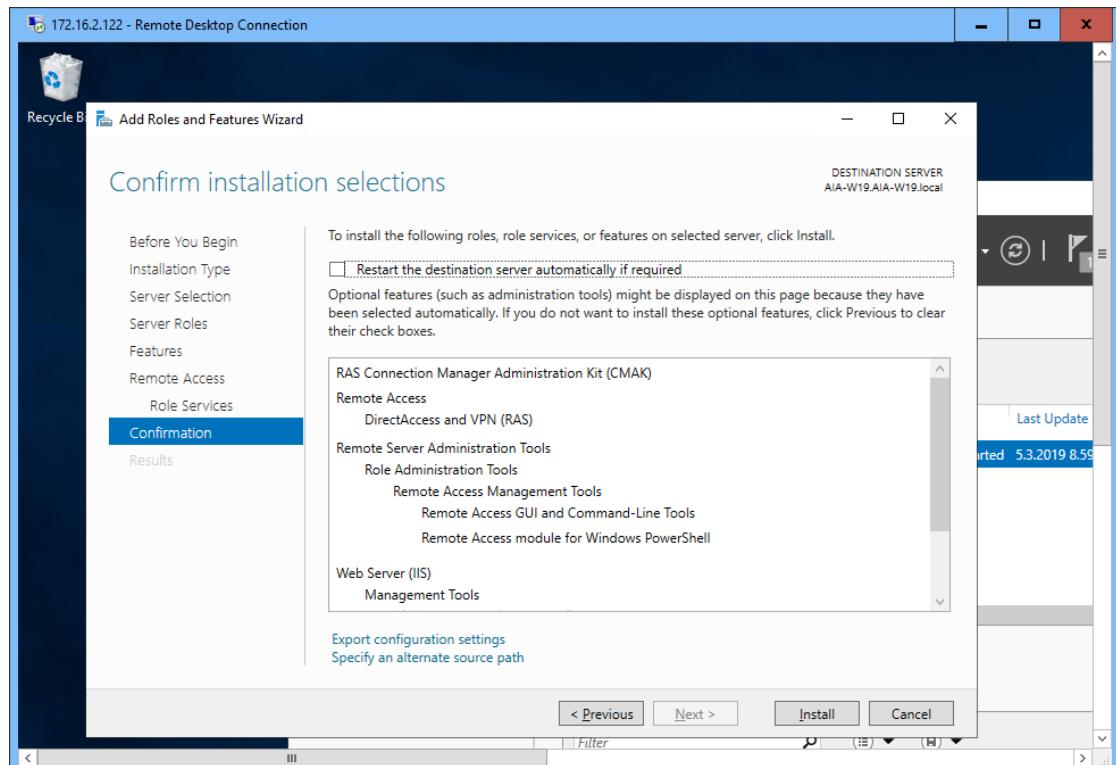
Add some required features here, such as the RAS Connection Manager Administration Kit (CMAK) and Web Server (IIS), so just click the Add Features button in the window that pops up.



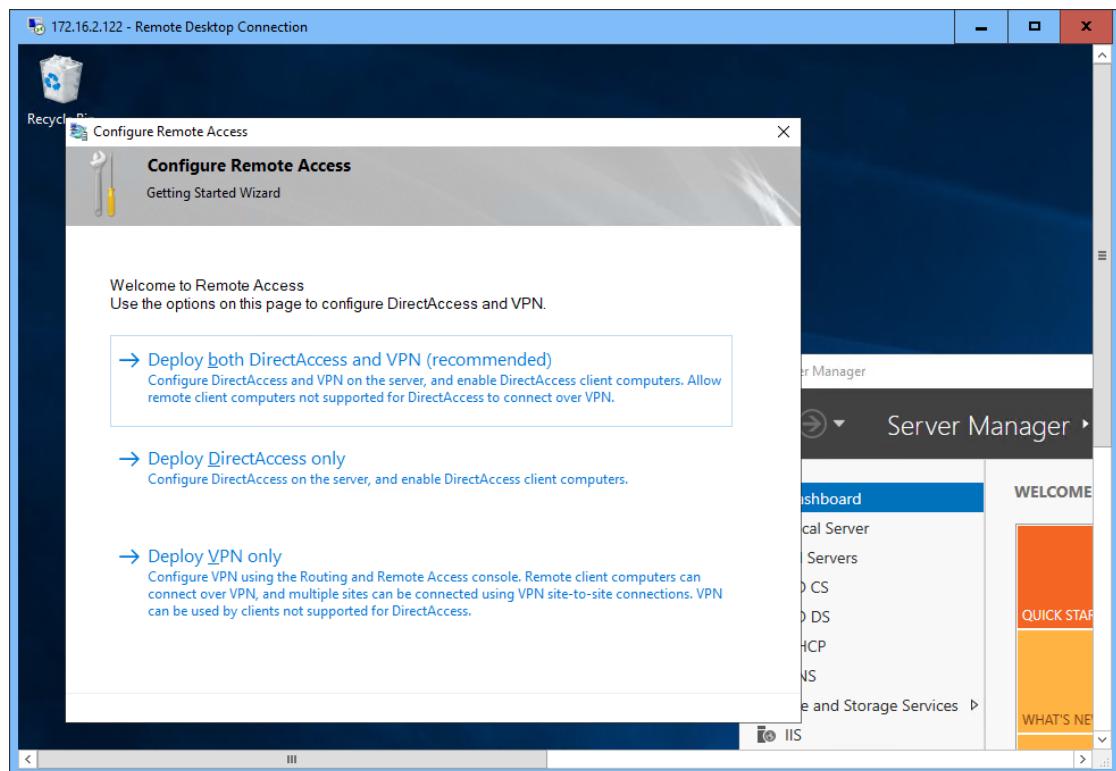
Check the box beside DirectAccess and VPN (RAS); then click Next three times, leaving the Web Server Role (IIS) selections at their defaults.



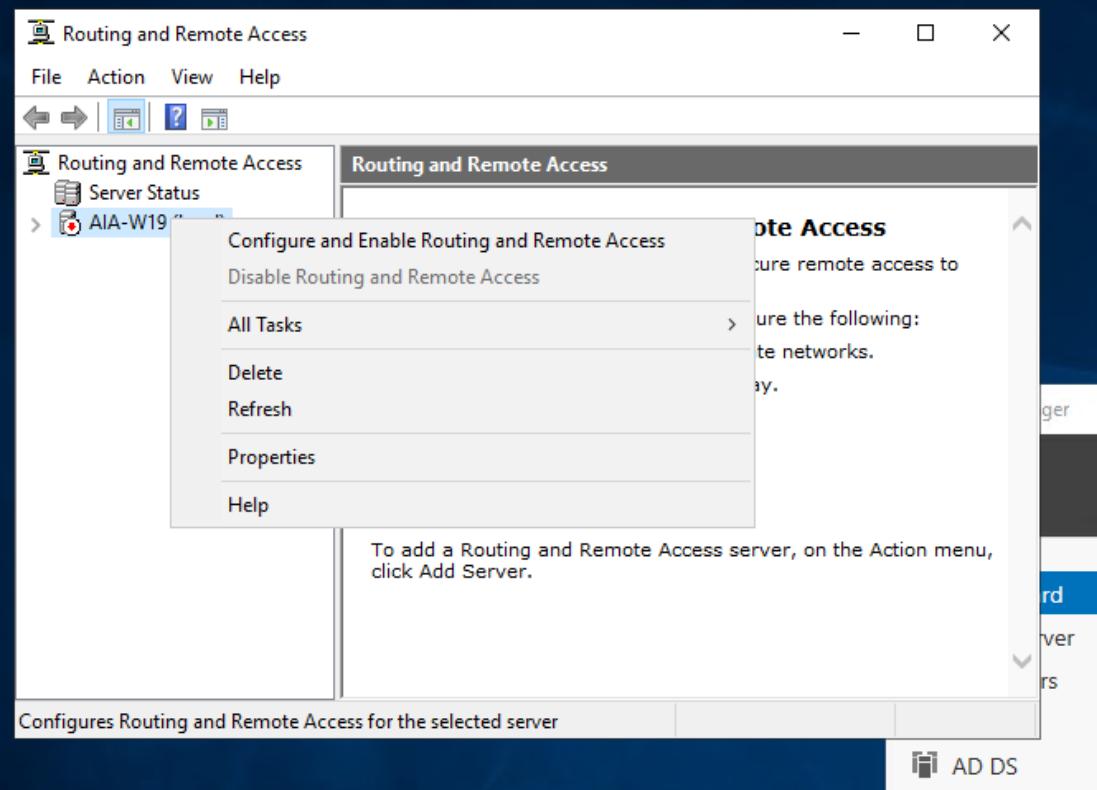
In the Confirm Installation Selections dialog box, ensure that your settings have been chosen correctly, and then click **Install** to begin.



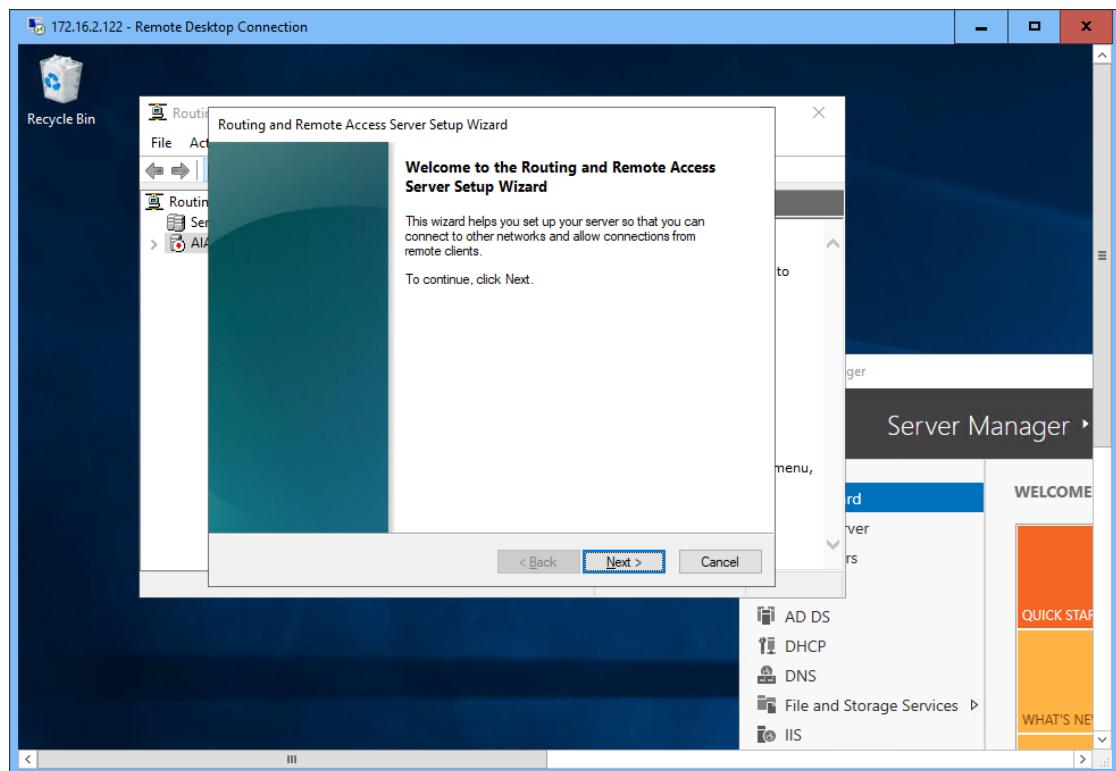
Configuring routing and remote access:
Select the Deploy VPN Only option.



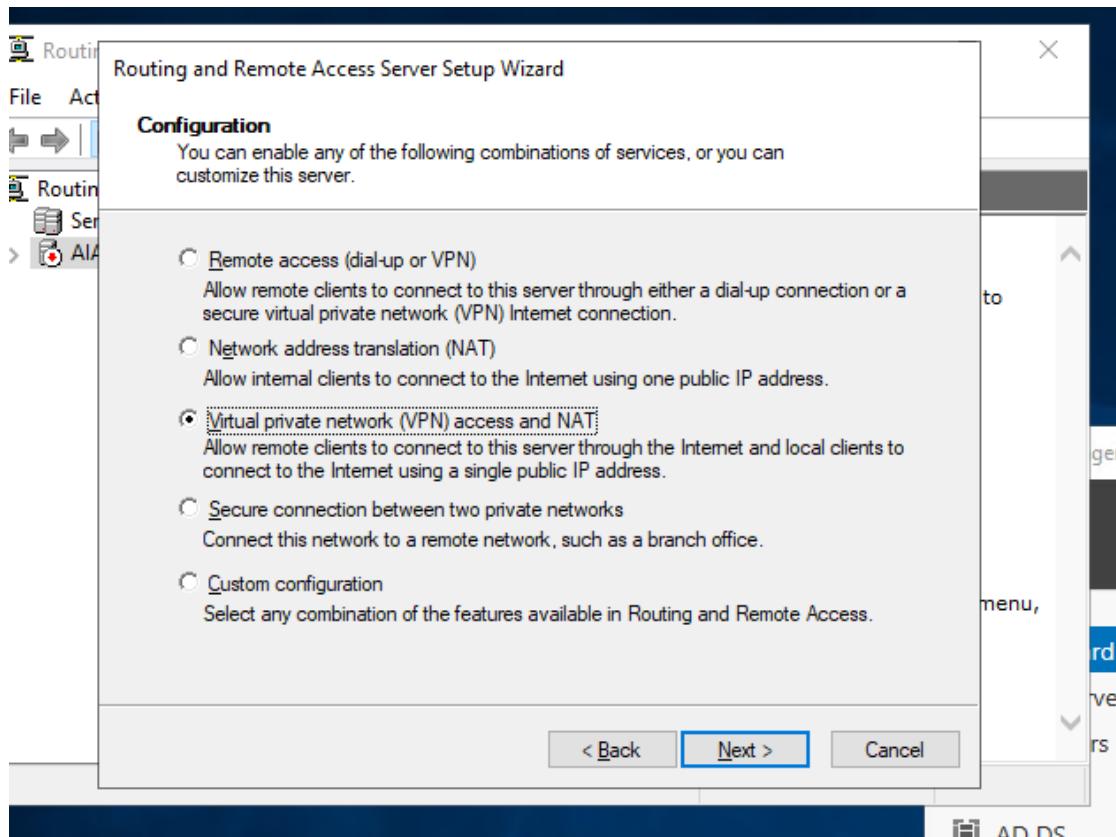
In the Routing and Remote Access snap-in, right-click your server name and then choose the Configure and Enable Routing and Remote Access option from the context menu.



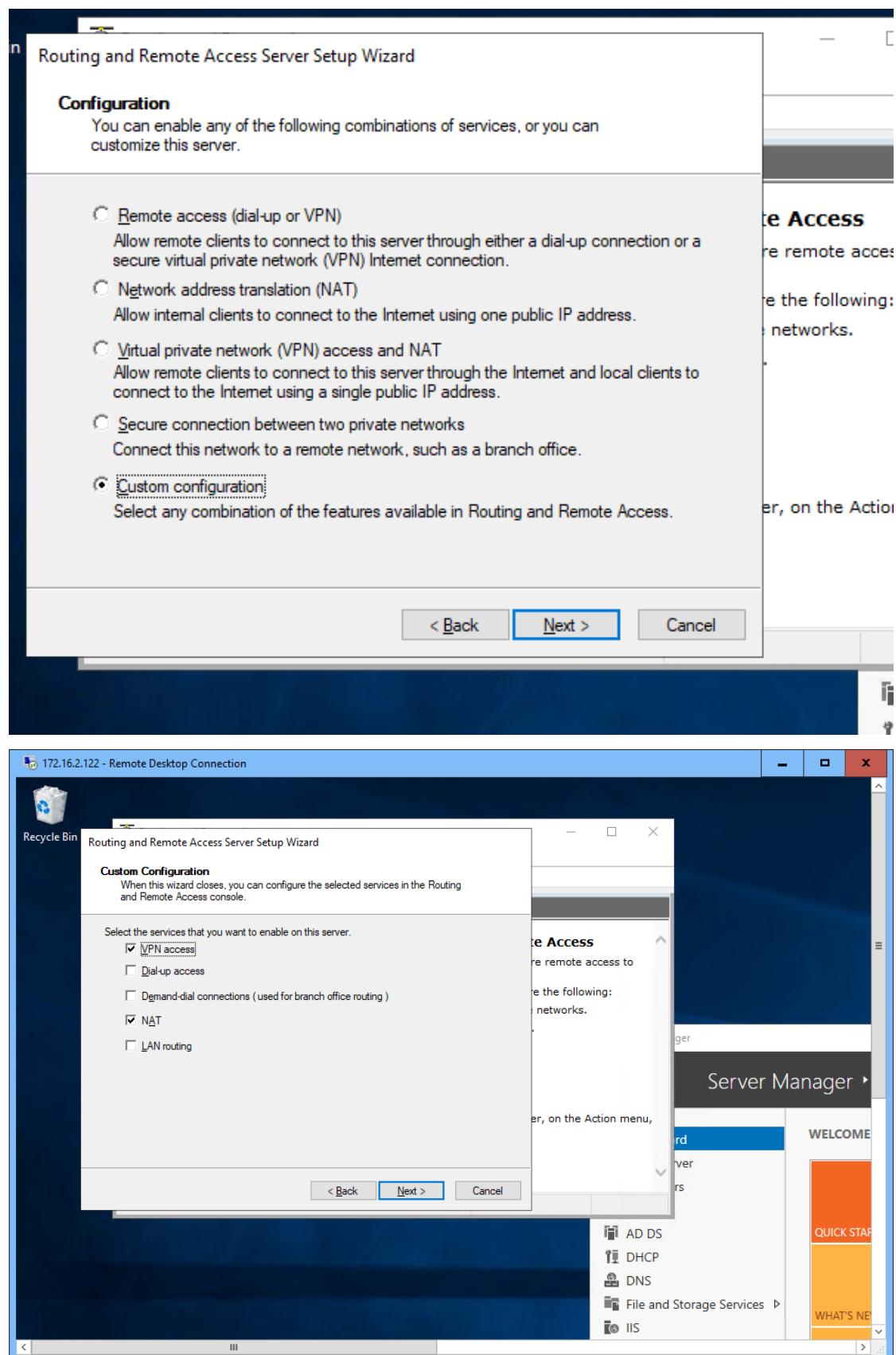
This opens the Routing and Remote Access Server Setup Wizard; click Next to continue.

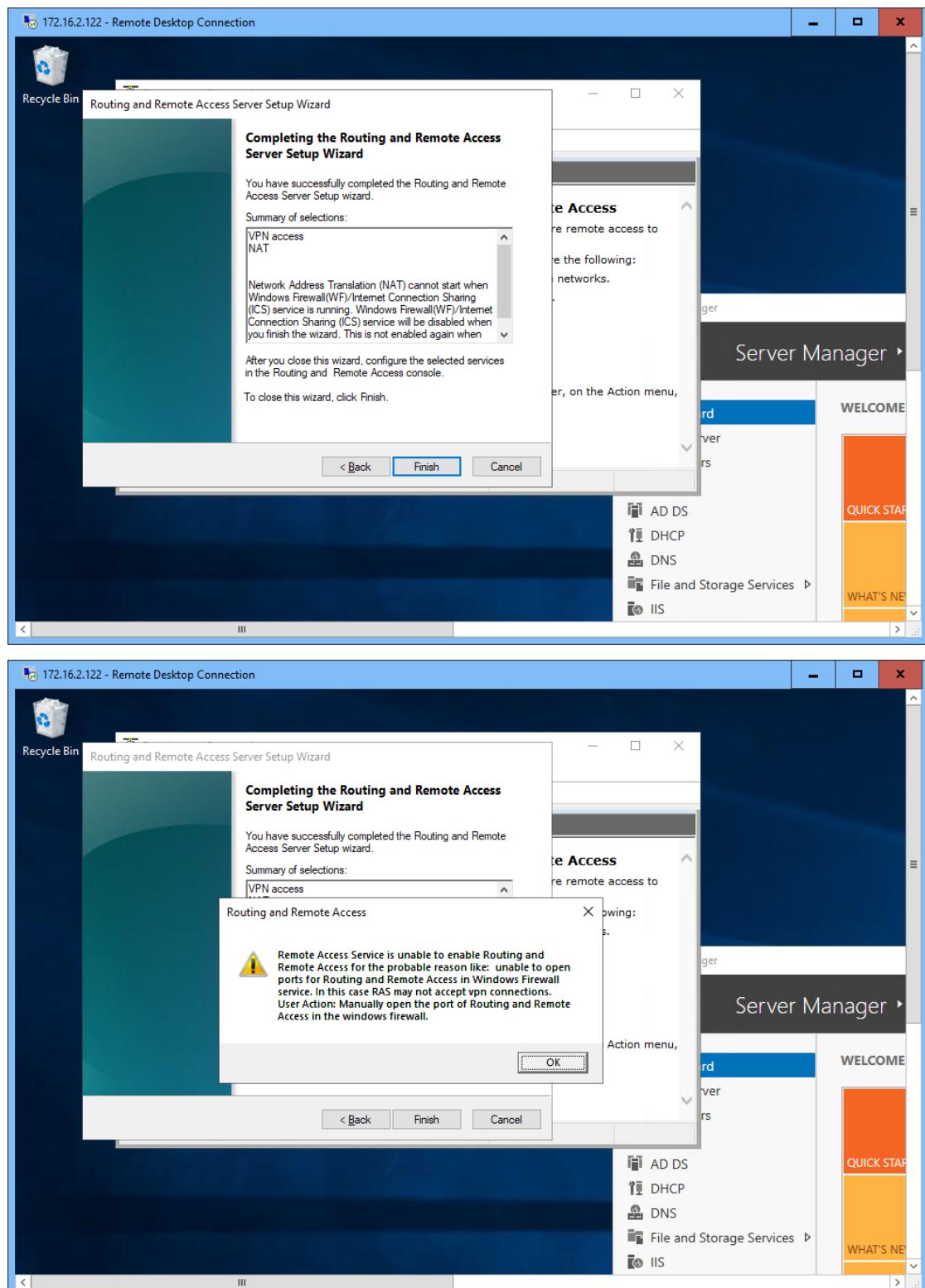


From the options presented in the Configuration dialog box, select “Virtual private network (VPN) access and NAT”; then click Next.



Because the server doesn't have two NIC, we will choose the Custom configuration option to configure the VPN access and NAT.



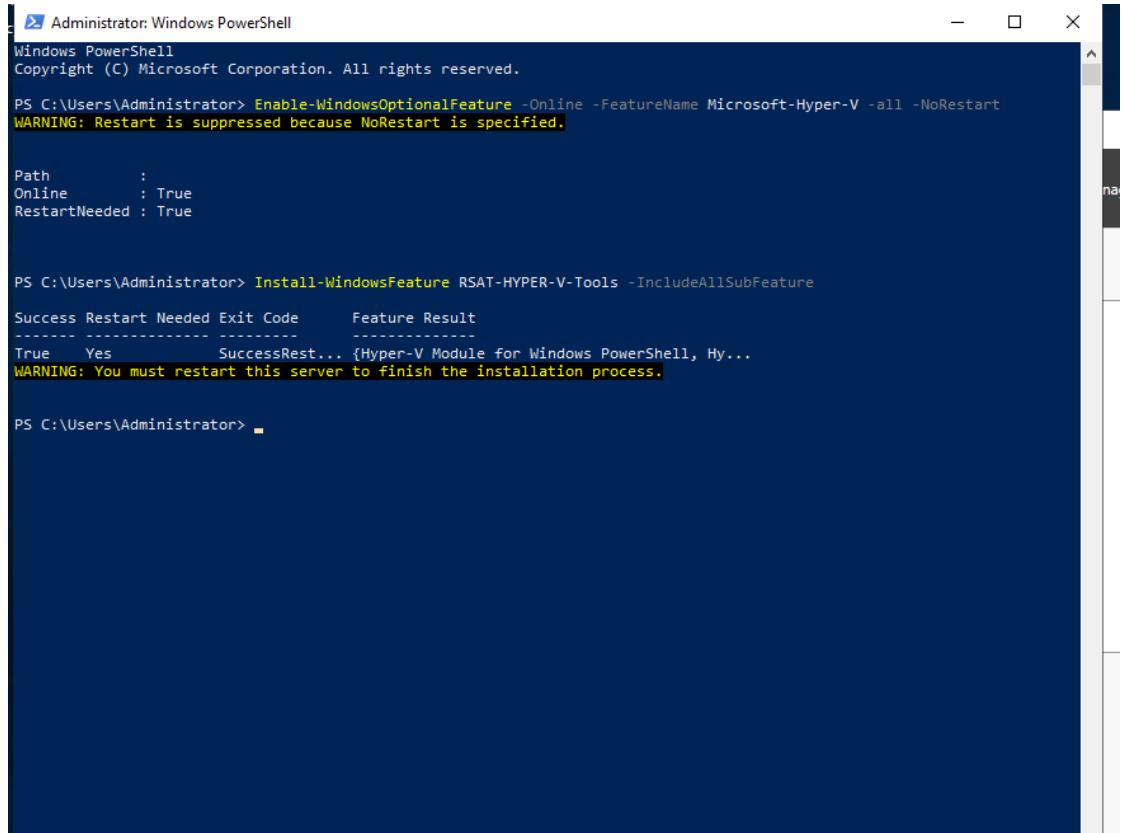


VPN configuration was a challenging section to configure it didn't went well, first of all there are no two network interfaces cards installed, the public IP was necessary to be configured to access the server remotely.

➤ Server Virtualization with Hyper-V:

The term virtualization is used for a lot of different things nowadays. It is used in association with applications, storage, network, servers, screen presentation, and so on. In this chapter, virtualization means the ability to run a full operating system on a software platform in such a way that the OS thinks it is running on a “real” computer.

Installing Hyperv –V feature:



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> Enable-WindowsOptionalFeature -Online -FeatureName Microsoft-Hyper-V -all -NoRestart
WARNING: Restart is suppressed because NoRestart is specified.

Path          :
Online        : True
RestartNeeded : True

PS C:\Users\Administrator> Install-WindowsFeature RSAT-HYPER-V-Tools -IncludeAllSubFeature
Success Restart Needed Exit Code      Feature Result
----- ----- ----- -----
True      Yes           SuccessRest... {Hyper-V Module for Windows PowerShell, Hy...
WARNING: You must restart this server to finish the installation process.

PS C:\Users\Administrator>
```

By configuring the VM and set up the network adapters same as we did in Lab 1 of Advanced Server Enterprises course.

```

172.16.2.122 - Remote Desktop Connection
Administrator: Windows PowerShell

Cmdlet      Start-VMFailover          2.0.0.0   Hyper-V
Cmdlet      Start-VMInitialReplication 2.0.0.0   Hyper-V
Cmdlet      Start-VMTrace           2.0.0.0   Hyper-V
Cmdlet      Stop-VM                2.0.0.0   Hyper-V
Cmdlet      Stop-VMFailover         2.0.0.0   Hyper-V
Cmdlet      Stop-VMInitialReplication 2.0.0.0   Hyper-V
Cmdlet      Stop-VMReplication       2.0.0.0   Hyper-V
Cmdlet      Stop-VMTrace           2.0.0.0   Hyper-V
Cmdlet      Suspend-VM             2.0.0.0   Hyper-V
Cmdlet      Suspend-VMReplication    2.0.0.0   Hyper-V
Cmdlet      Test-VHD               2.0.0.0   Hyper-V
Cmdlet      Test-VMNetworkAdapter   2.0.0.0   Hyper-V
Cmdlet      Test-VMReplicationConnection 2.0.0.0   Hyper-V
Cmdlet      Update-VMVersion        2.0.0.0   Hyper-V
Cmdlet      Wait-VM                2.0.0.0   Hyper-V

PS C:\Users\Administrator>
PS C:\Users\Administrator>
PS C:\Users\Administrator>
PS C:\Users\Administrator>
PS C:\Users\Administrator> Get-VM

Name      State CPUUsage(%) MemoryAssigned(M) Uptime      Status      Version
----      ----  -----  -----  -----  -----
Aia-VMnew Off     0          0 00:00:00 Operating normally 9.0

PS C:\Users\Administrator> Get-VMSwitch

Name      SwitchType NetAdapterInterfaceDescription
----      -----
Aia-VM2    External   Microsoft Hyper-V Network Adapter
Aia_Internal Internal
Aia-Private Private

PS C:\Users\Administrator> -

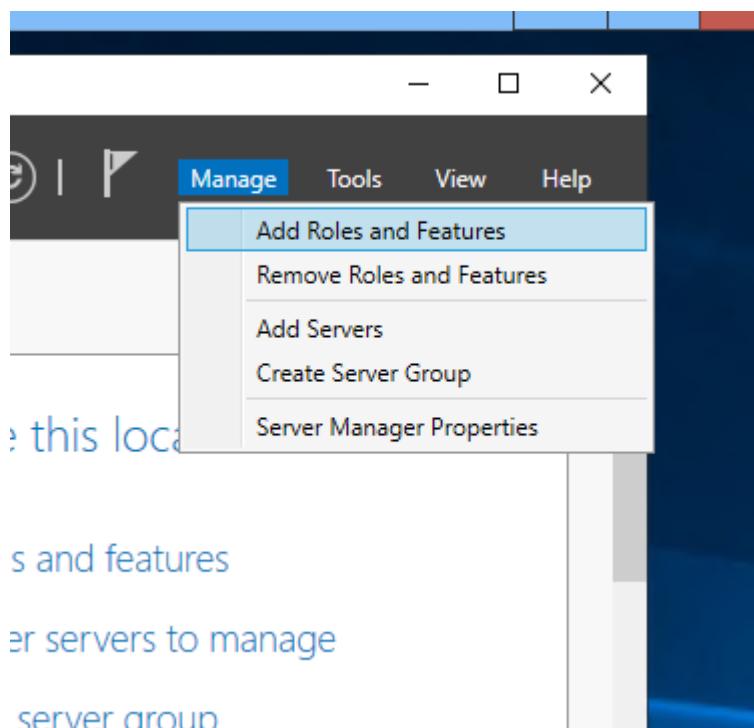
```

➤ Patch Management:

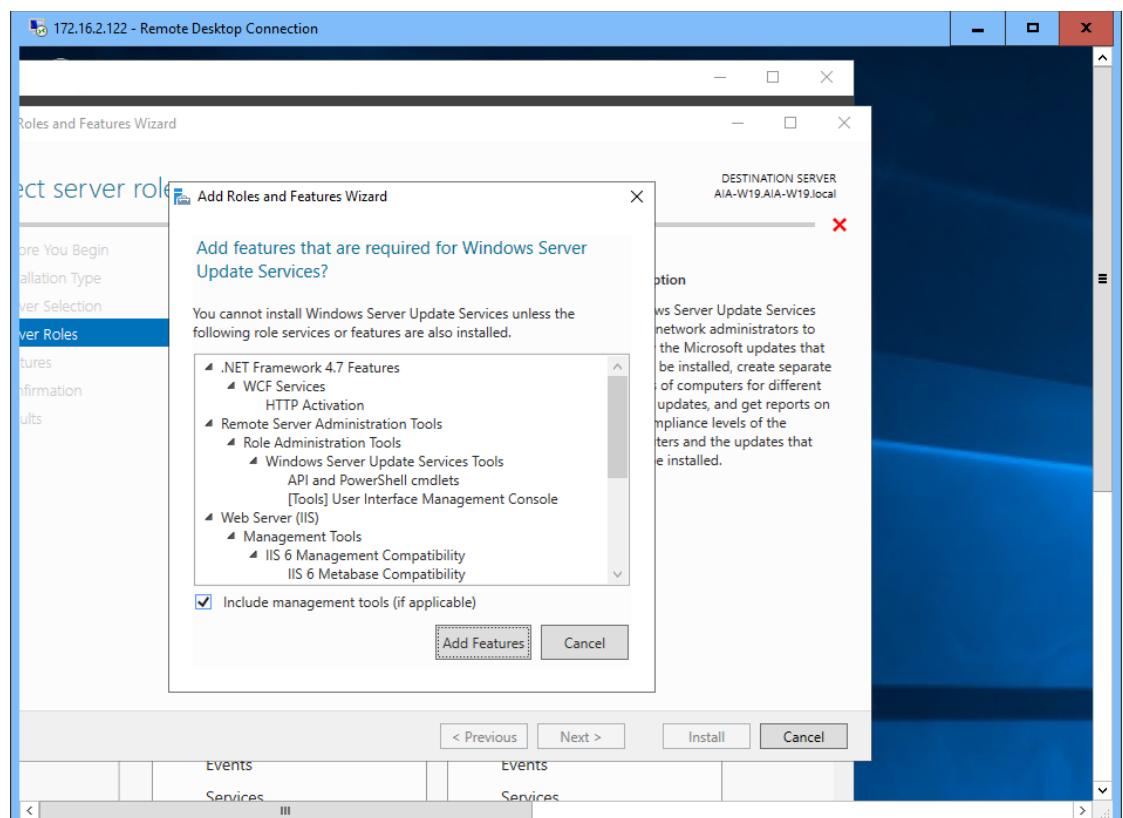
Patch management has been the process of minimizing the organization's threat and vulnerability surface by managing and deploying software updates, but over time it has moved to support feature updates and overall product updates. Updates can be deployed and managed by a number of different products and tools. Windows Server Updates Services (WSUS) is a Windows role that allows administrators to use the Server Management tool to configure and manage updates, the same rich reporting and status updates are included with some new features and changes to the past functionality.

Installing and configuring of Patch management:

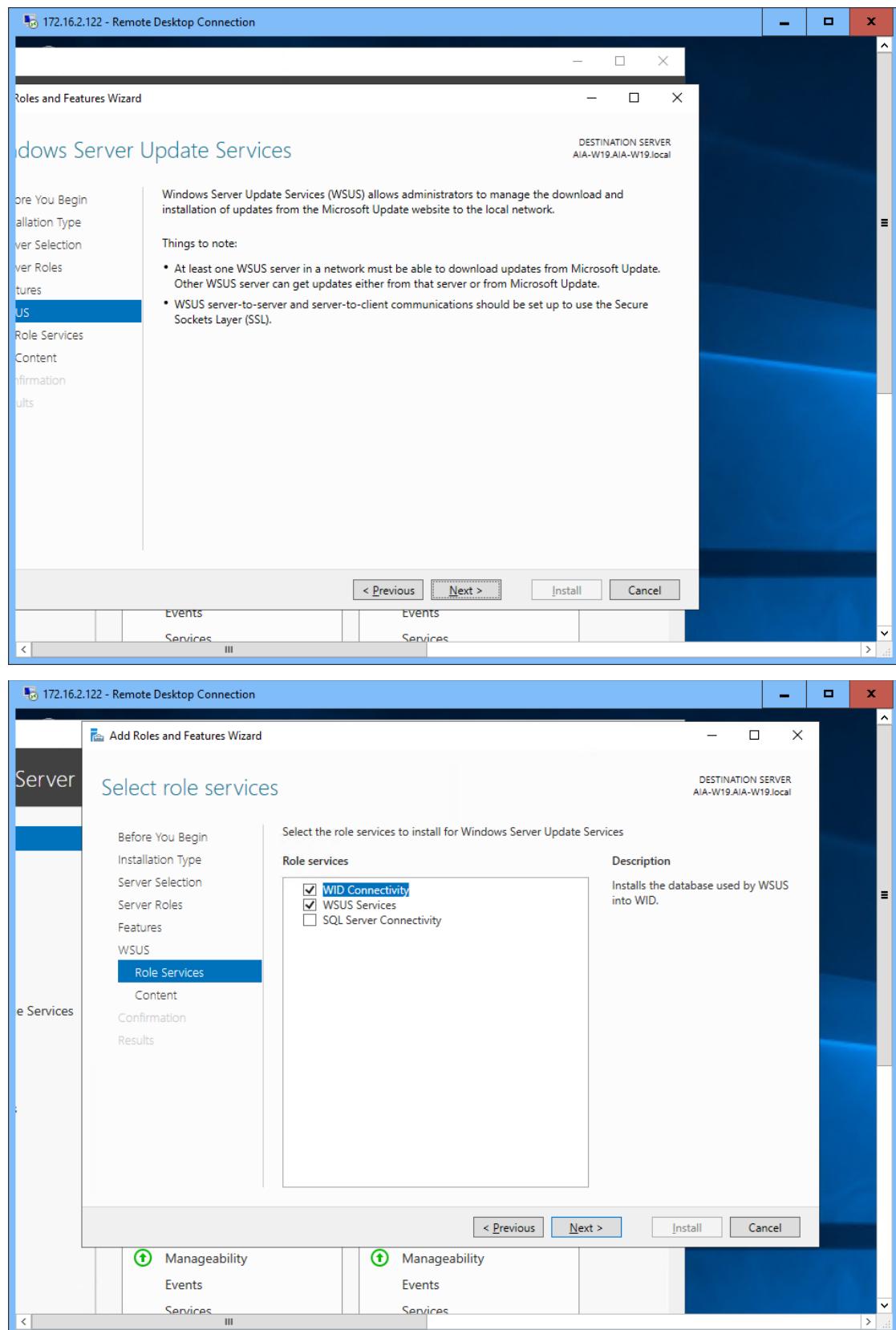
In **Server Manager**, click **Manage**, and then click **add Roles and Features**.



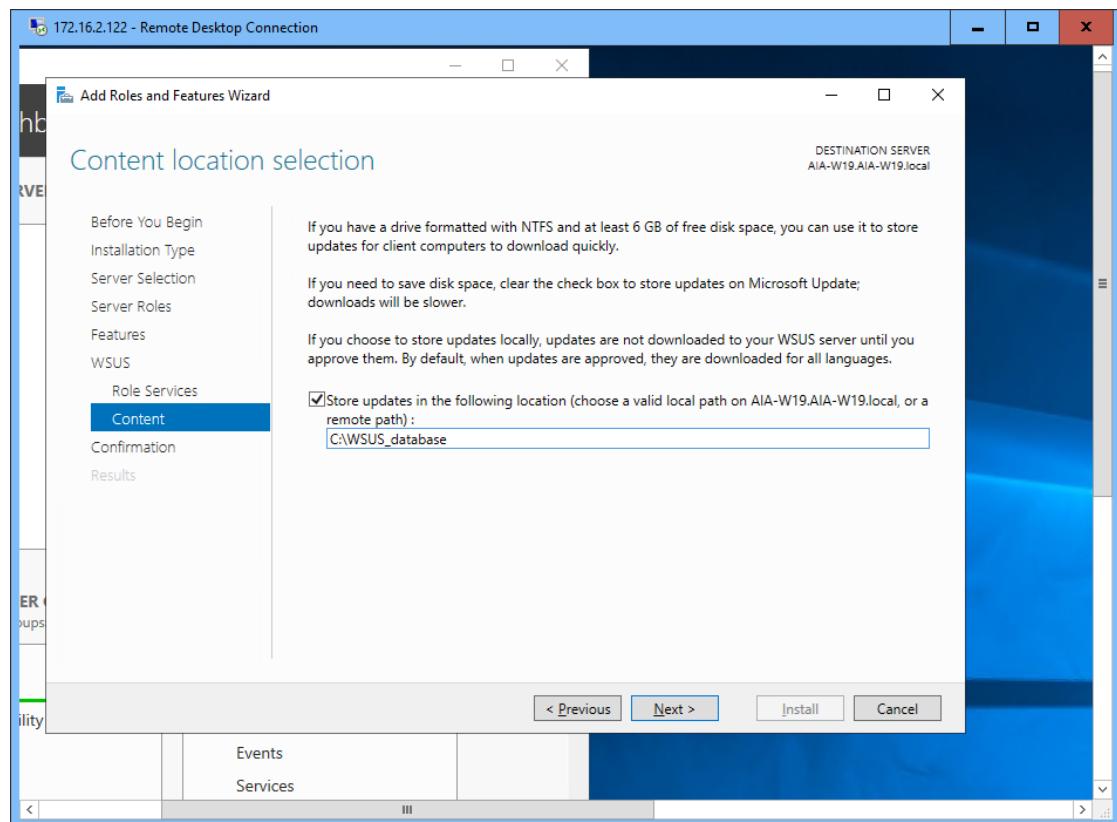
On the **Before you begin** page, click **Next**. On the **select server roles** page, select **Windows Server Update Services**. Add features that are required for **Windows Server Update Services** opens. Click **Add Features**, and then click **Next**.



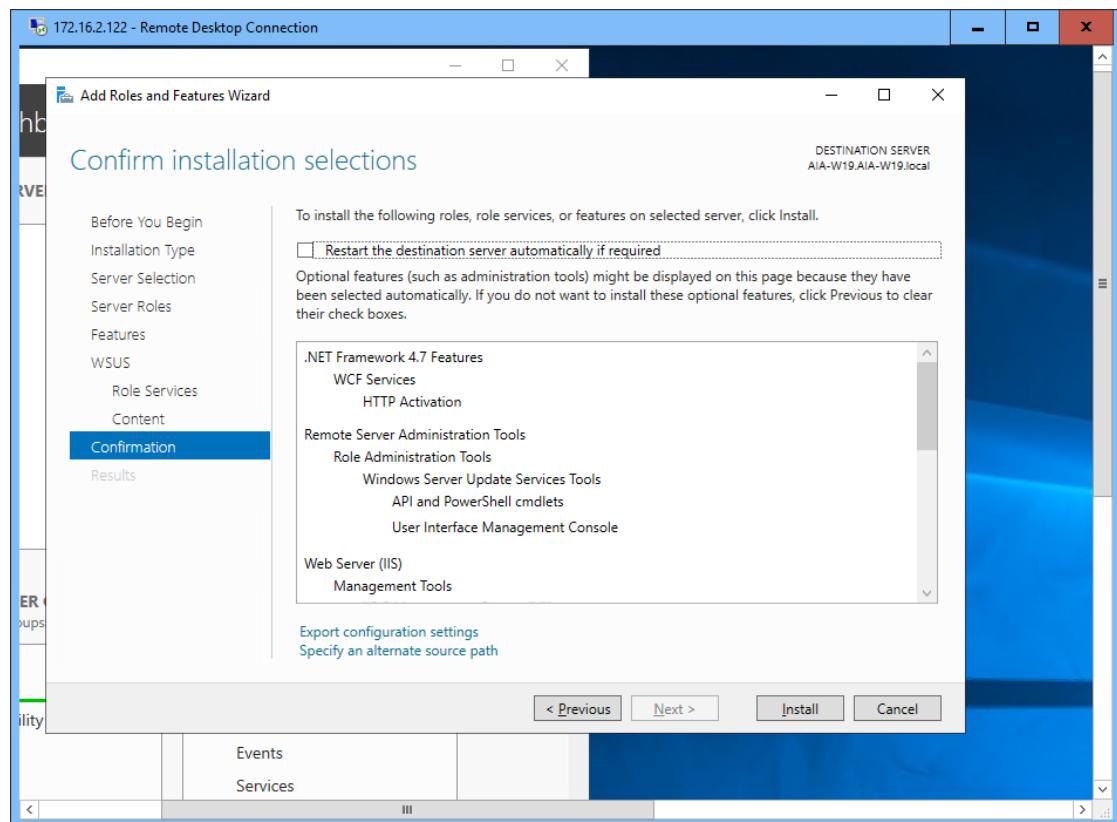
On the **select features** page, retain the default selections, and then click **Next**.



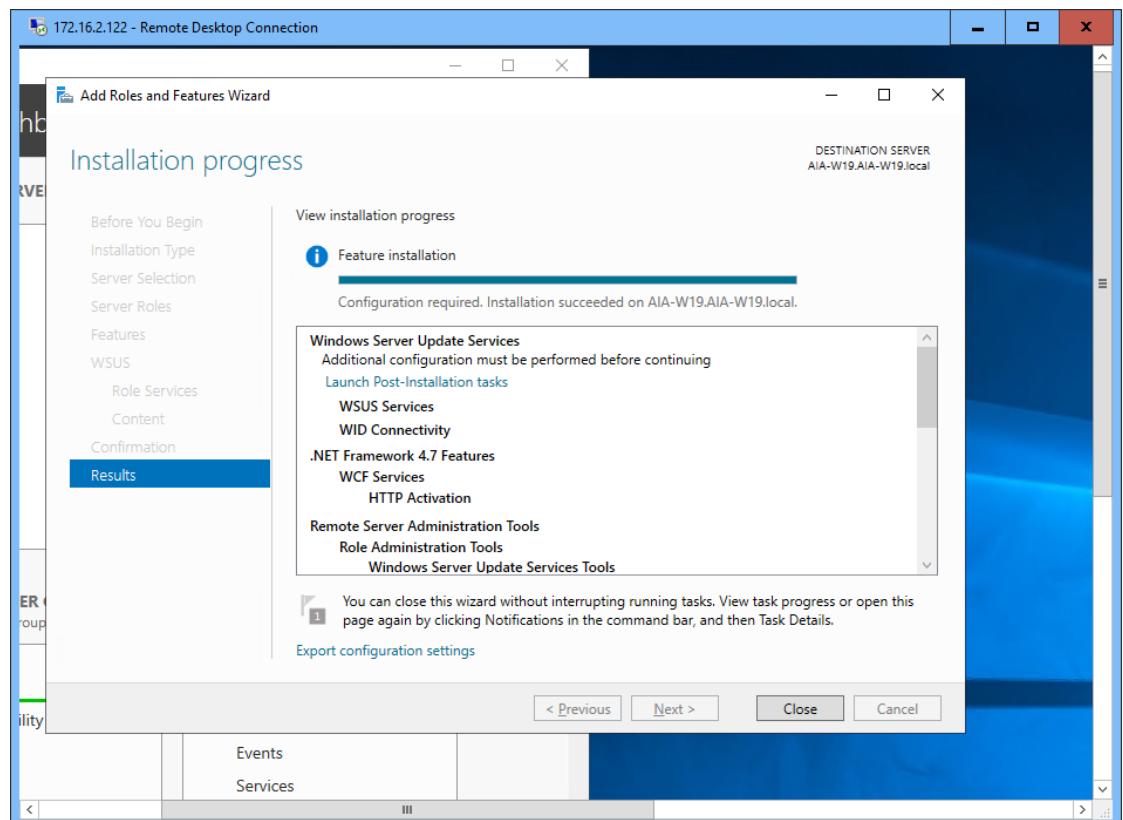
On the **Select Role Services** page, leave the default selections, and then click **Next**. On the **Content location selection** page, type a valid location to store the updates. for this purpose, and type **C:\WSUS_database** as the valid location.



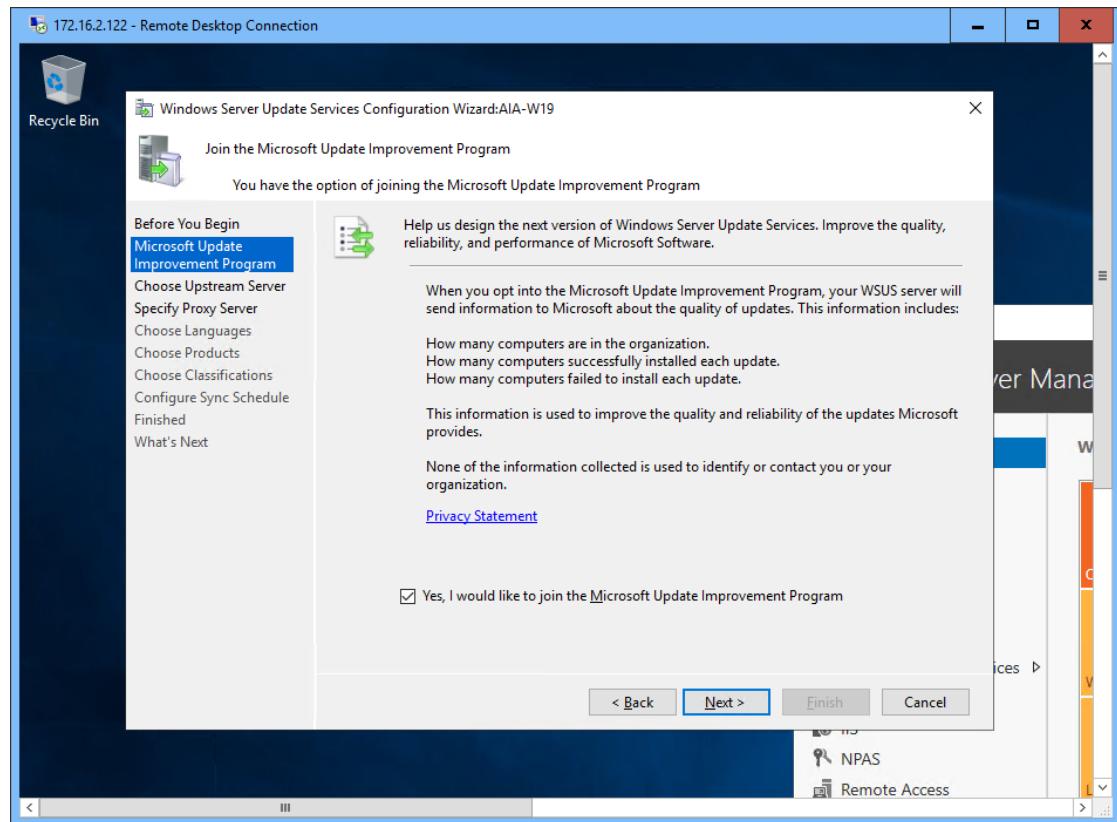
click **Next**. The **Web Server Role (IIS)** page opens. Review the information, and then click **Next**. In **select the role services to install for Web Server (IIS)**, retain the defaults, and then click **Nex**



Once WSUS installation is complete, in the summary window on the **Installation progress** page, click **Launch Post-Installation tasks**. The text changes, requesting: **Please wait while your server is configured**. When the task has finished, the text changes to: **Configuration successfully completed**. Click **Close**.



The Windows Server Update Services Wizard opens. On the **Before you Begin** page, review the information, and then click **Next**.

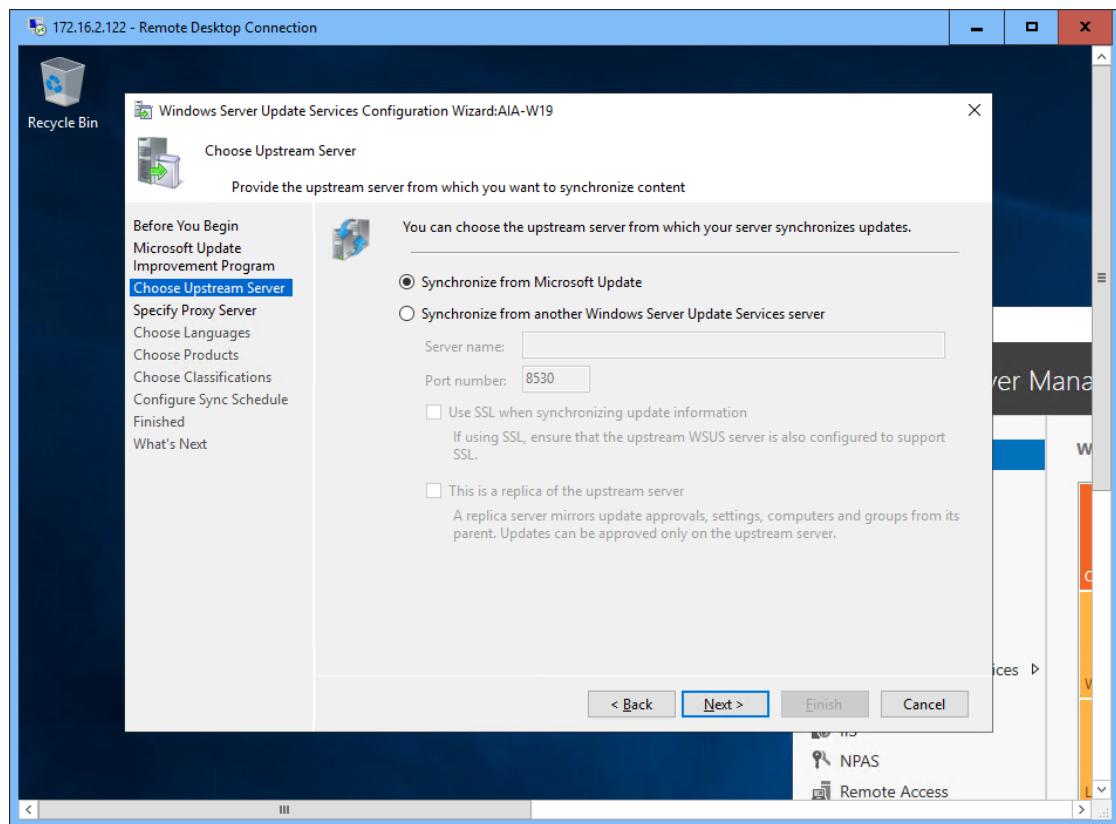


Read the instructions on the **Join the Microsoft Update Improvement Program** page and evaluate if you want to participate. If you want to participate in the program, retain the default selection, or clear the check box, and then click **Next**.

On the Choose Upstream Server page, there are two options:

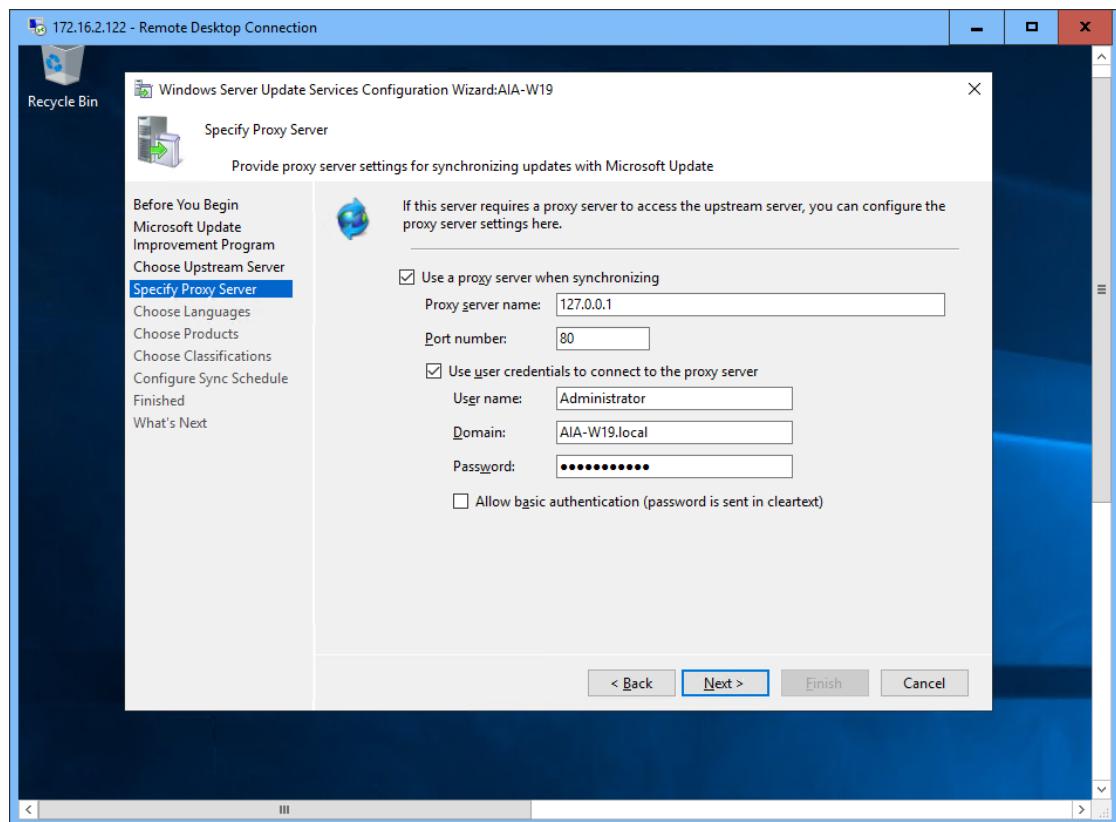
Synchronize the updates with Microsoft Update, Synchronize from another Windows Server Update Services server.

- if you choose to synchronize from another WSUS server, specify the server name and the port on which this server will communicate with the upstream server.
- To use SSL, select the **Use SSL when synchronizing update information** check box. The servers will use port 443 for synchronization. (Make sure that this server and the upstream server support SSL).
- if this is a replica server, select the **This is a replica of the upstream server** check box.

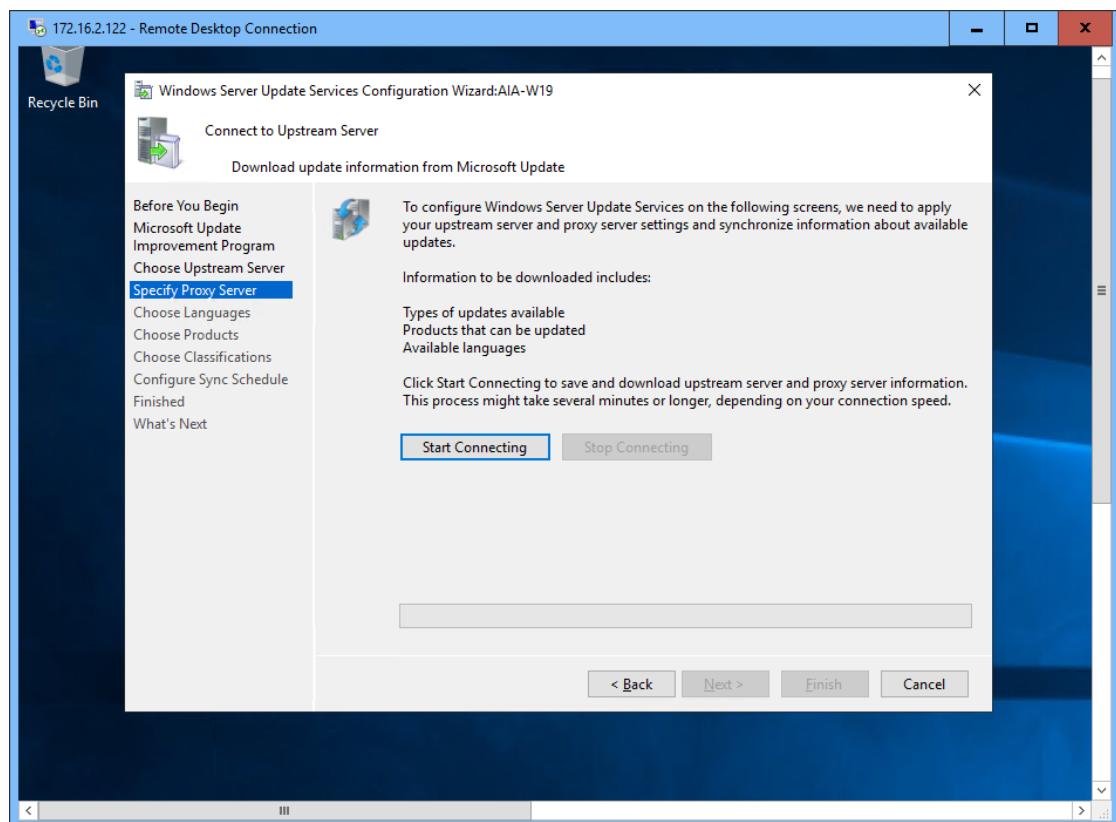


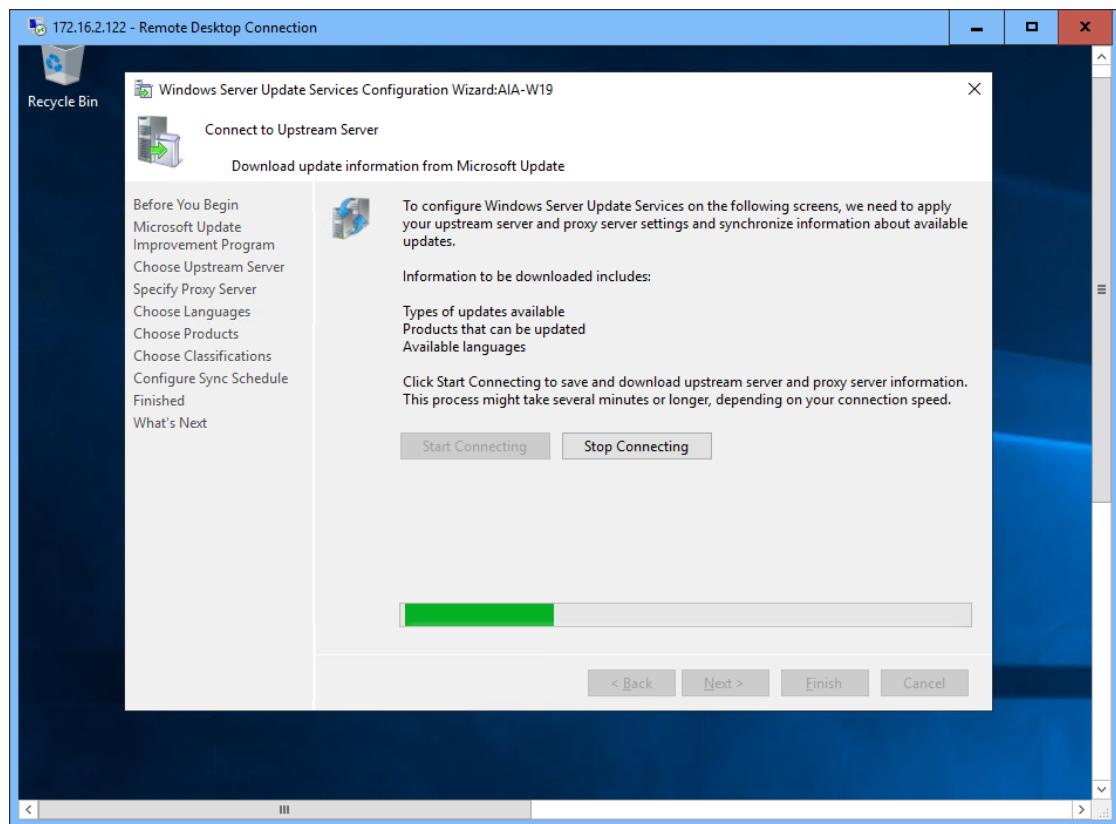
After selecting the proper options for your deployment, click **Next** to proceed.

On the **Specify Proxy Server** page, select the **Use a proxy server when synchronizing** check box, and then type the proxy server name and port number (port 80 by default) in the corresponding boxes.

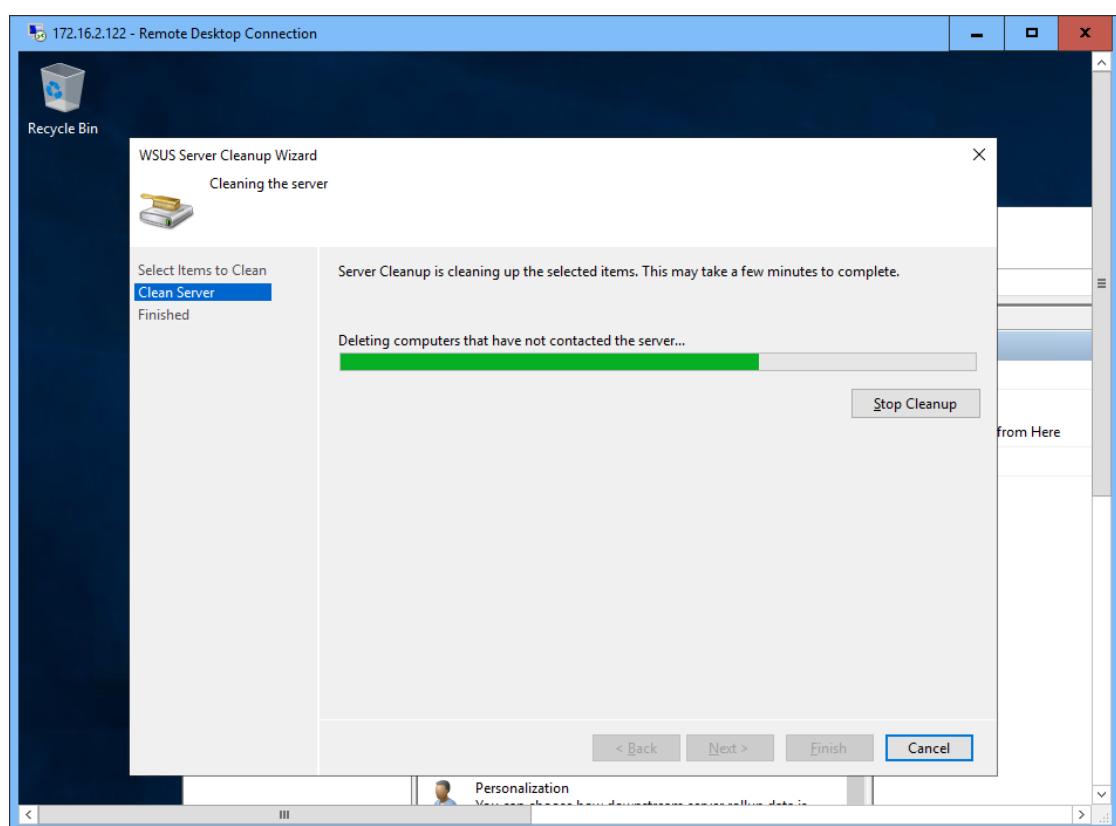
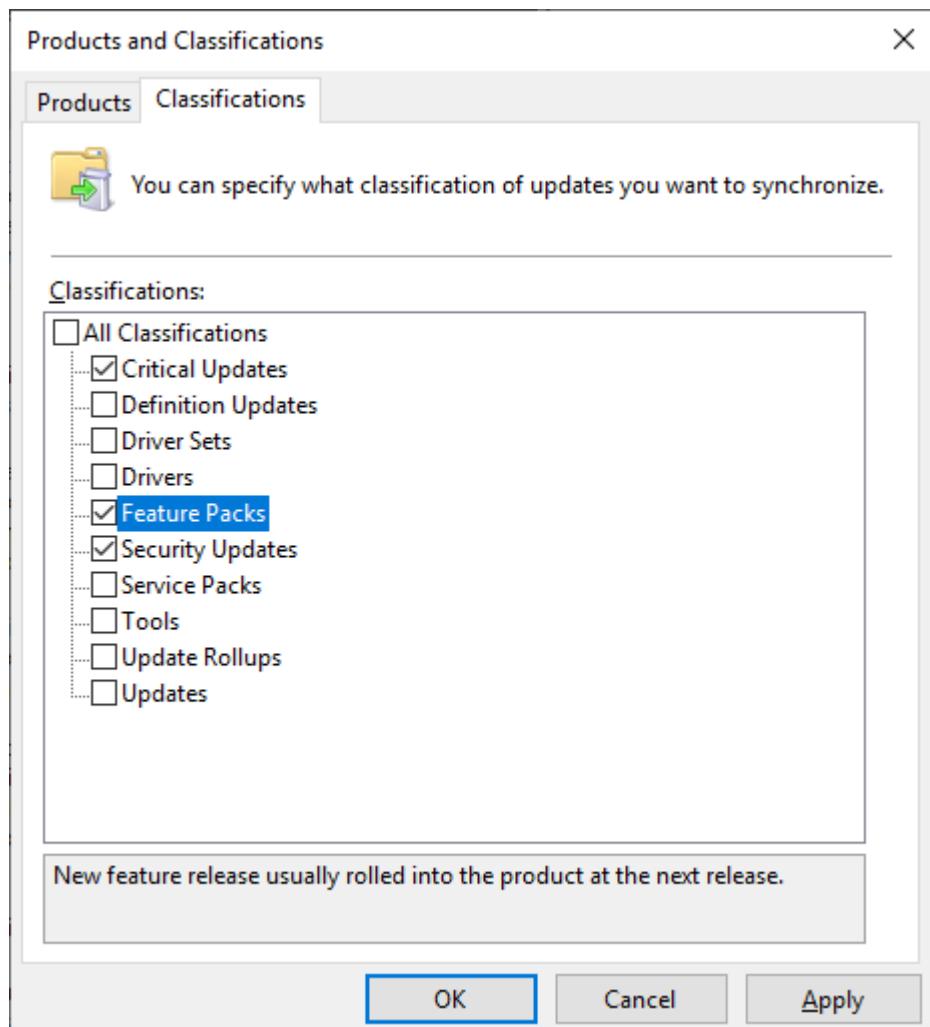


Click Next. On the Connect to Upstream Server page, click start Connecting.





On the **Choose Classifications** page, select the update classifications that you want to obtain. Choose all the classifications or a subset of them, and then click **Next**.



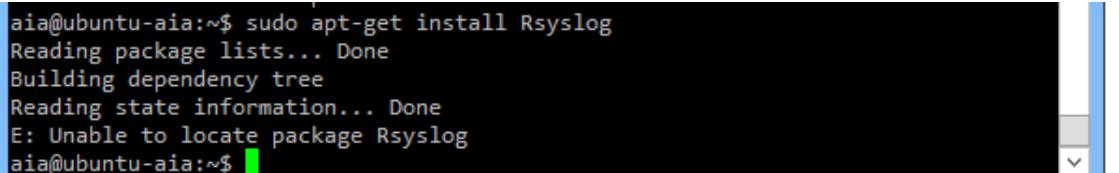
3.2 Linux Server configuration

➤ Enabling system logging with rsyslog

Rsyslogd daemon is the system logging daemon, it accepts log messages from a variety of other programs and writes them to the appropriate log files. It's better than having every program write directly to its own log file because it enables the administrator to centrally manage how log files are handled. With remote logging, if the system on the network is broken into, the cracker can't delete or modify the log files because those files are stored on a separate computer, it's important to remember that those log messages are not encrypted by default.

The Rsyslog daemon is installed automatically in most Linux distributions, but if not, we must execute the following commands:

```
sudo apt-get install Rsyslog
```



```
aia@ubuntu-aia:~$ sudo apt-get install Rsyslog
Reading package lists... Done
Building dependency tree
Reading state information... Done
E: Unable to locate package Rsyslog
aia@ubuntu-aia:~$
```

To configure a rsyslog program to be run in server mode, we must edit the configuration file in the /etc/rsyslog.conf directory.

```
sudo nano /etc/rsyslog.conf
```

```
sudo nano /etc/rsyslog.d
```

```
GNU nano 2.9.3          New Buffer          Modified
#####
#Log anything (except mail) of level info or higher
#Don't log private authentication message!
*.info;mail.none;authpriv.none;cron.none      /var/log/messages
#The authpriv file has restricted access.
authpriv.*                                     /var/log/secure
#Log all the mail messages in one place
mail.*                                         -/var/log/maillog
#Log cron stuff
cron.*                                         /var/log/cron

File Name to Write: rsyslog.d
^G Get Help          M-D DOS Format       M-A Append        M-B Backup File
^C Cancel           M-M Mac Format       M-P Prepend       ^T To Files
```

The first entry shows that info level messages from all services (*) are matched by that rule, with the exception of messages from mail, authpriv and cron services . They are all matched messages are directed to the /var/log/message file.

The mail, authpriv and cron services each have their own log files .

```
GNU nano 2.9.3          /var/log/messages      Modified
Feb 12 8:10 network:Bringing up loopback interface: succeeded
Feb 12 8:15 network:Brining up interface eth0: succeeded
Feb 12 8:30 vsftpd(pam_unix)[10565]: authentication failure;
    logname= uid=0 euid=0 tty= ruser = rhost=10.0.0.3 user=chris
Feb 12 9:10 su(pam_unix)[11439]: session opened for user root by chris(uid=500)

Save modified buffer? (Answering "No" will DISCARD changes.)
Y Yes
N No
```

The message in the /var/log/messages file are divided into five main parts:

- The date and time that the message was logged
- The name of the computer that message came from
- The program or service name to which message pertains
- The process number
- The actual text message

Sending up and using a loghost with rsyslogd:

On the client side:

Instead of a file, start by replacing the log file name with the @ character followed by the name of the loghost.

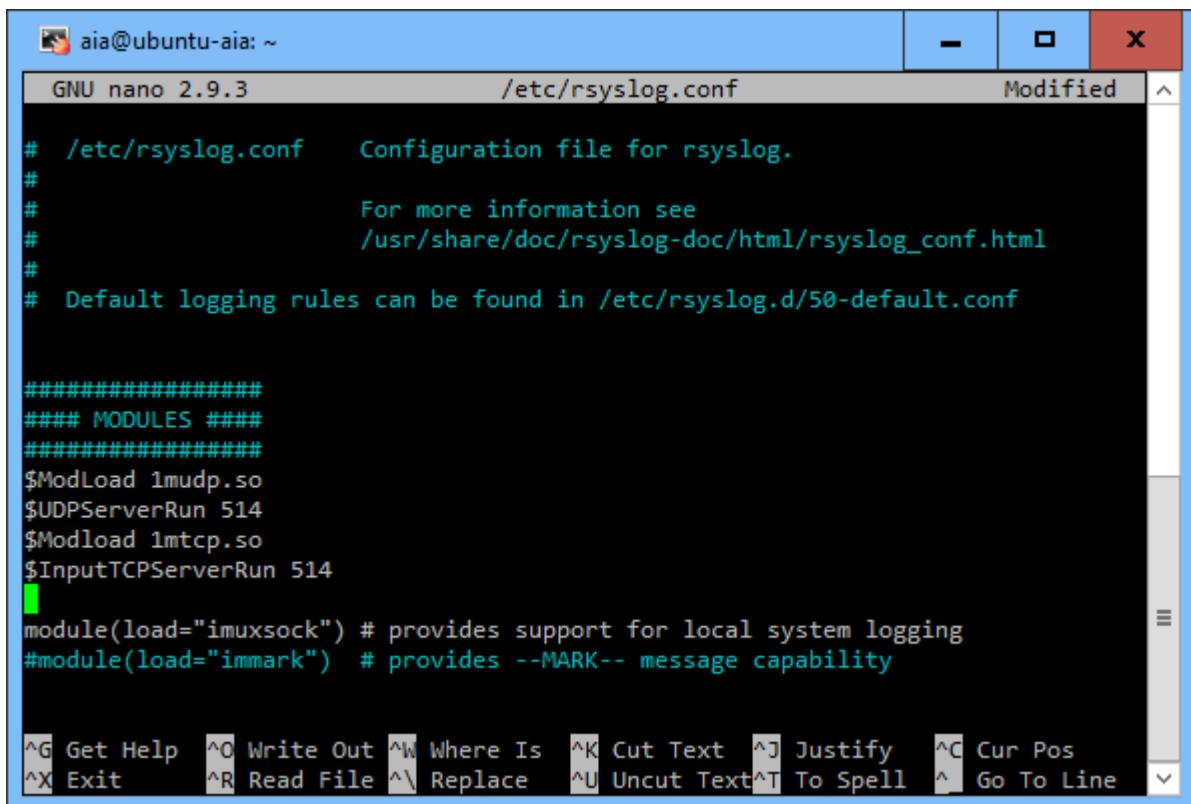
`sudo nano /etc/rsyslog.conf`

```
# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;news.none;authpriv.none;
cron.none /var/log/messages
*.info;mail.none;news.none;authpriv.none;
cron.none @loghost
# The authpriv file has restricted access.
authpriv.@

/var/log/secure authpriv.* @loghost
# Log all the mail messages in one place.
mail.* -/var/log/maillog
mail.* @loghost
```

On the loghost side:

- Edit the `/etc/rsyslog.conf` file on the loghost system and uncomment the lines that enable the `rsyslogd` daemon to listen for remote log messages. Uncomment the first two lines to enable incoming UDP log messages on port 514 (default); uncomment the two lines after that to allow messages that use TCP protocol (also port 514): `$ModLoad imudp.so $UDPServerRun 514 $ModLoad imtcp.so $InputTCPServerRun 514`

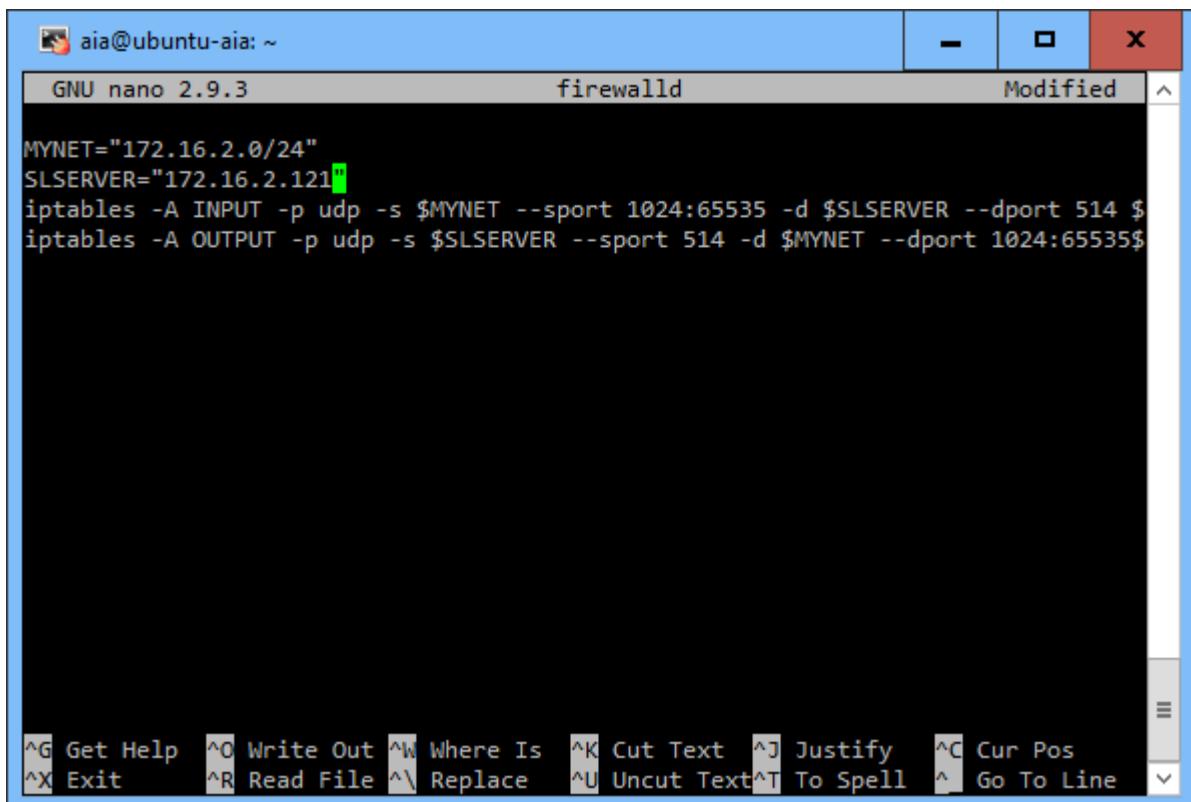


```
# /etc/rsyslog.conf      Configuration file for rsyslog.
#
# For more information see
# /usr/share/doc/rsyslog-doc/html/rsyslog_conf.html
#
# Default logging rules can be found in /etc/rsyslog.d/50-default.conf

#####
#### MODULES #####
#####
$ModLoad 1mudp.so
$UDPServerRun 514
$Modload 1mtcp.so
$InputTCPServerRun 514

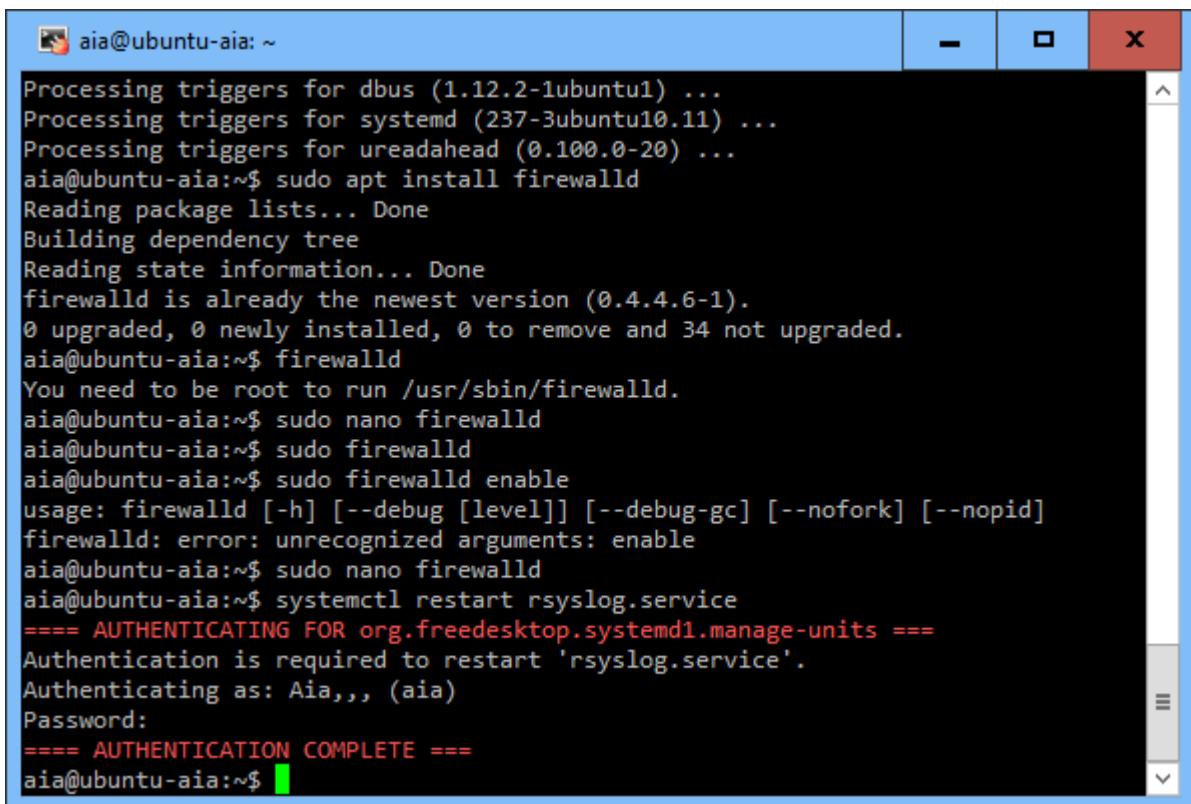
module(load="imuxsock") # provides support for local system logging
#module(load="immark")  # provides --MARK-- message capability
```

- Open your firewall (iptables or firewalld) to allow new messages to be directed to your loghost.



```
MYNET="172.16.2.0/24"
SLSERVER="172.16.2.121"
iptables -A INPUT -p udp -s $MYNET --sport 1024:65535 -d $SLSERVER --dport 514 $ 
iptables -A OUTPUT -p udp -s $SLSERVER --sport 514 -d $MYNET --dport 1024:65535$
```

- Restart the rsyslog service (service rsyslog restart or systemctl restart rsyslog.service).

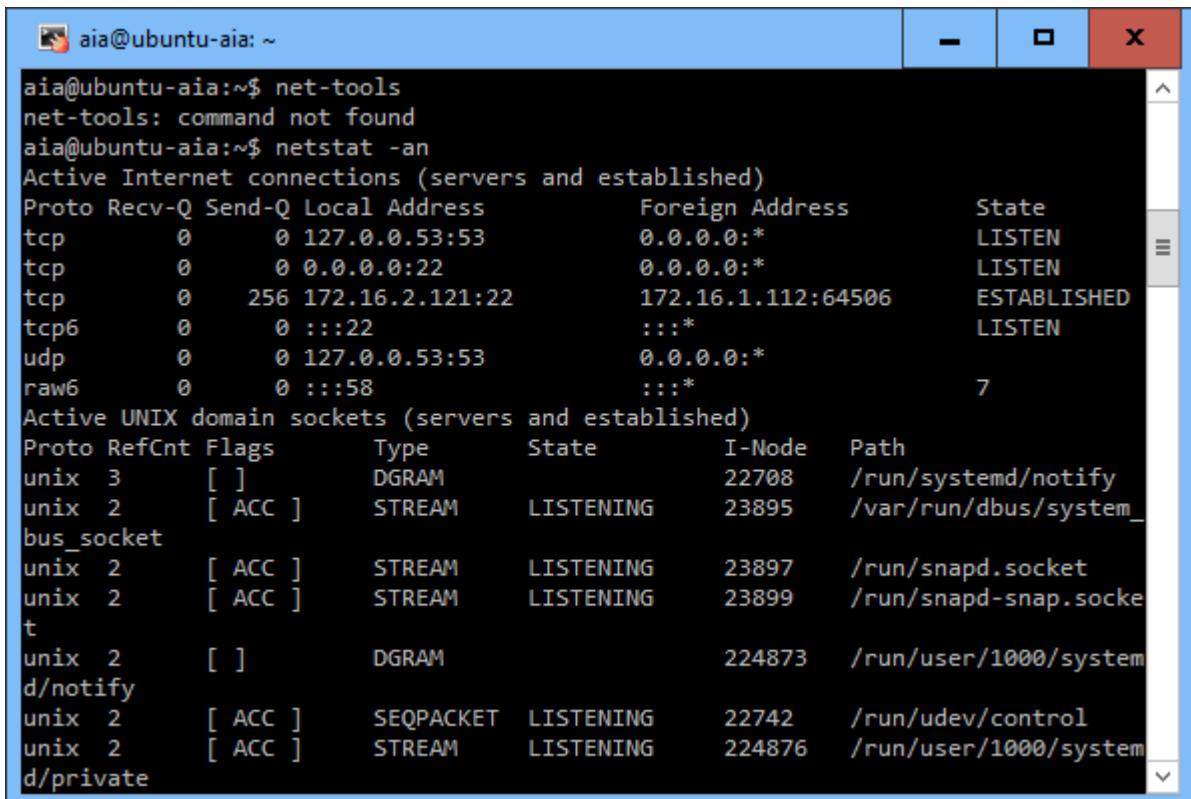


```

aia@ubuntu-aia: ~
Processing triggers for dbus (1.12.2-1ubuntu1) ...
Processing triggers for systemd (237-3ubuntu10.11) ...
Processing triggers for ureadahead (0.100.0-20) ...
aia@ubuntu-aia:~$ sudo apt install firewalld
Reading package lists... Done
Building dependency tree
Reading state information... Done
firewalld is already the newest version (0.4.4.6-1).
0 upgraded, 0 newly installed, 0 to remove and 34 not upgraded.
aia@ubuntu-aia:~$ firewalld
You need to be root to run /usr/sbin/firewalld.
aia@ubuntu-aia:~$ sudo nano firewalld
aia@ubuntu-aia:~$ sudo firewalld
aia@ubuntu-aia:~$ sudo firewalld enable
usage: firewalld [-h] [--debug [level]] [--debug-gc] [--nofork] [--nopid]
firewalld: error: unrecognized arguments: enable
aia@ubuntu-aia:~$ sudo nano firewalld
aia@ubuntu-aia:~$ systemctl restart rsyslog.service
===== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ===
Authentication is required to restart 'rsyslog.service'.
Authenticating as: Aia,,, (aia)
Password:
===== AUTHENTICATION COMPLETE ===
aia@ubuntu-aia:~$ 
```

- If the service is running, you should be able to see that the service is listening on the ports you enabled (UDP and/or TCP ports 514). Run the netstat command as follows to see that the rsyslogd daemon is listening on IPv4 and IPv6 ports 514 for both UDP and TCP services:

```
$ netstat -an
```



```

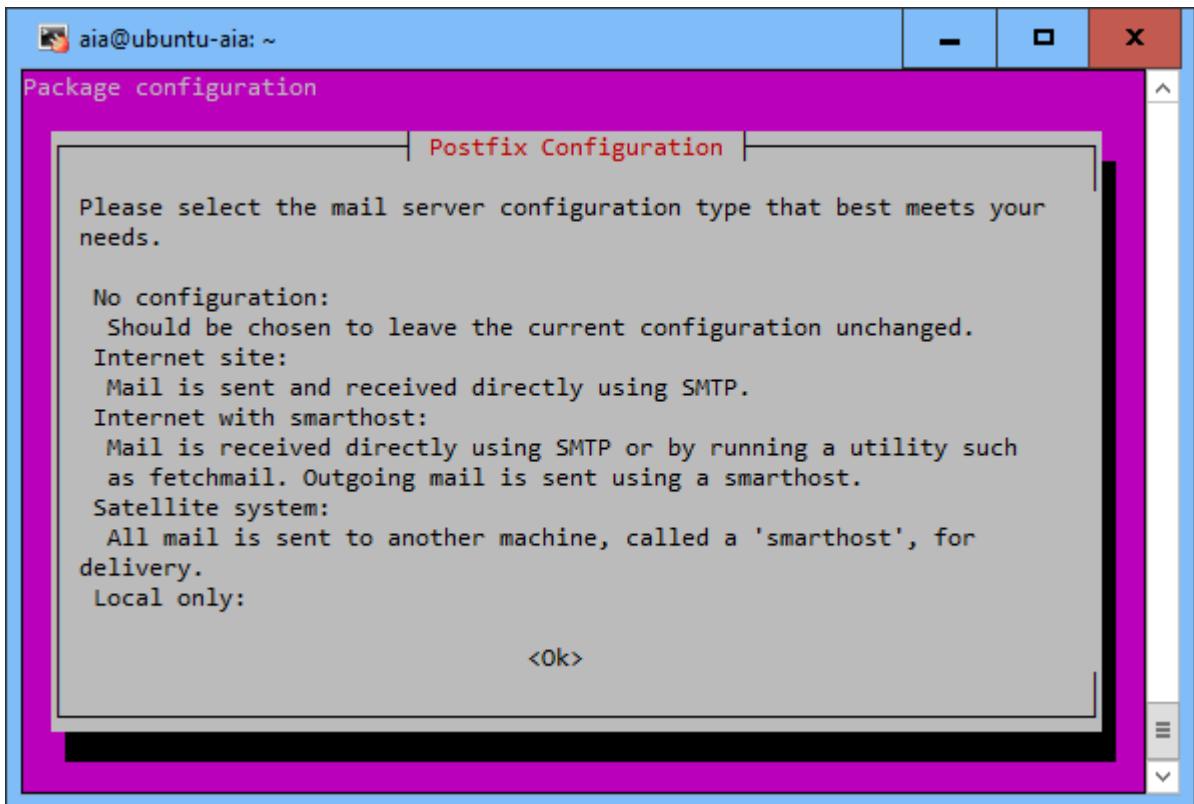
aia@ubuntu-aia: ~
aia@ubuntu-aia:~$ net-tools
net-tools: command not found
aia@ubuntu-aia:~$ netstat -an
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address          Foreign Address        State
tcp      0      0 127.0.0.53:53           0.0.0.0:*
tcp      0      0 0.0.0.0:22             0.0.0.0:*
tcp      0    256 172.16.2.121:22         172.16.1.112:64506 ESTABLISHED
tcp6     0      0 :::22                  :::*
udp      0      0 127.0.0.53:53           0.0.0.0:*
raw6     0      0 :::58                  :::*
                                            7
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type      State         I-Node  Path
unix    3      [ ]        DGRAM          22708   /run/systemd/notify
unix    2      [ ACC ]     STREAM        LISTENING   23895   /var/run/dbus/system_
bus_socket
unix    2      [ ACC ]     STREAM        LISTENING   23897   /run/snapd.socket
unix    2      [ ACC ]     STREAM        LISTENING   23899   /run/snapd-snap.socke
t
unix    2      [ ]        DGRAM          224873   /run/user/1000/system
d/notify
unix    2      [ ACC ]     SEQPACKET    LISTENING   22742   /run/udev/control
unix    2      [ ACC ]     STREAM        LISTENING   224876   /run/user/1000/system
d/private 
```

Watching logs with logwatch:

The logwatch service runs in most Linux systems that do system logging with rsyslog . Because logs on busy systems can become very large over time, it doesn't take long for there to be too many messages for a system administrator to watch every message in every log. To install the logwatch facility:

```
sudo apt-get install logwatch
```

The logwatch service runs from a cron job (01logwatch) placed in /etc/cron.daily . The /etc/logwatch/conf/logwatch.conf file holds local settings. The default options used to gather log messages are set in the /usr/share/logwatch/default.conf/logwatch.conf file.



for other settings to change (such as detail level or the time range for each report).

```

# mail
Heirloom Mail version 12.5 7/5/10. Type ? for help.
"/var/spool/mail/root": 2 messages 2 new
>N 1 logwatch@abc.ex Sun Feb 15 04:02 45/664 "Logwatch for abc"
    2 logwatch@abc.ex Mon Feb 16 04:02 45/664 "Logwatch for abc"
& 1
& x

```

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
 ^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^ Go To Line

➤ Administering Networking:

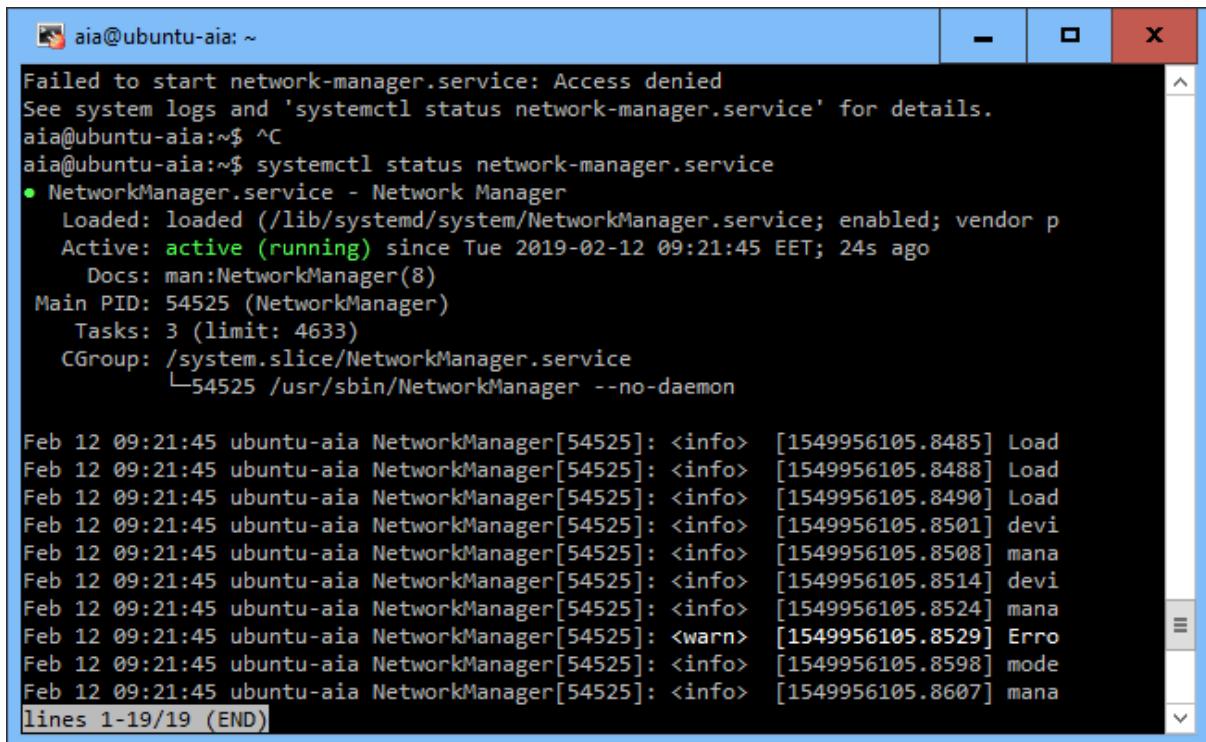
use the nmtui or system-config-network commands to configure basic networking with a menu-based interface from a shell.

It require installing network manager to access the network configuration by the command:

`sudo apt install network-manager`

`service network-manager start`

As root it appears that the network-manager start running



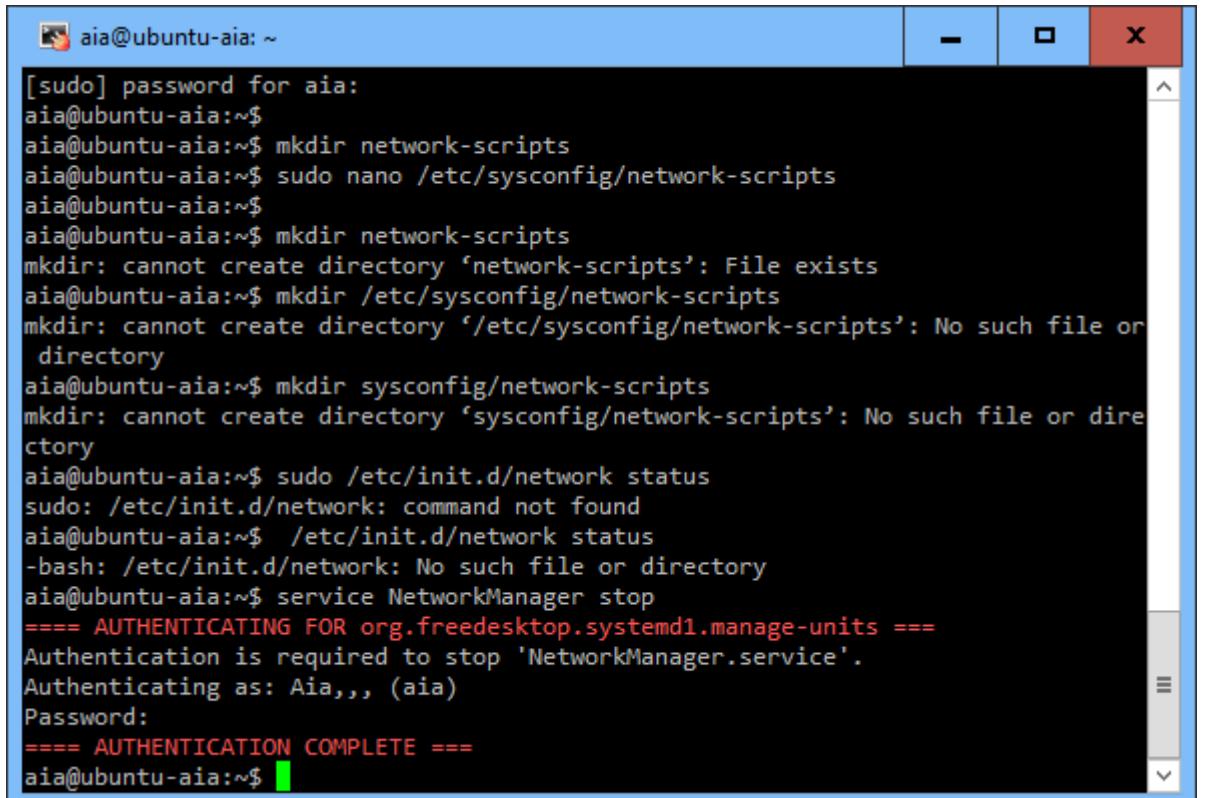
```
aia@ubuntu-aia: ~
Failed to start network-manager.service: Access denied
See system logs and 'systemctl status network-manager.service' for details.
aia@ubuntu-aia:~$ ^C
aia@ubuntu-aia:~$ systemctl status network-manager.service
● NetworkManager.service - Network Manager
  Loaded: loaded (/lib/systemd/system/NetworkManager.service; enabled; vendor p
  Active: active (running) since Tue 2019-02-12 09:21:45 EET; 24s ago
    Docs: man:NetworkManager(8)
   Main PID: 54525 (NetworkManager)
     Tasks: 3 (limit: 4633)
    CGroup: /system.slice/NetworkManager.service
           └─54525 /usr/sbin/NetworkManager --no-daemon

Feb 12 09:21:45 ubuntu-aia NetworkManager[54525]: <info>  [1549956105.8485] Load
Feb 12 09:21:45 ubuntu-aia NetworkManager[54525]: <info>  [1549956105.8488] Load
Feb 12 09:21:45 ubuntu-aia NetworkManager[54525]: <info>  [1549956105.8490] Load
Feb 12 09:21:45 ubuntu-aia NetworkManager[54525]: <info>  [1549956105.8501] devi
Feb 12 09:21:45 ubuntu-aia NetworkManager[54525]: <info>  [1549956105.8508] mana
Feb 12 09:21:45 ubuntu-aia NetworkManager[54525]: <info>  [1549956105.8514] devi
Feb 12 09:21:45 ubuntu-aia NetworkManager[54525]: <info>  [1549956105.8524] mana
Feb 12 09:21:45 ubuntu-aia NetworkManager[54525]: <warn>  [1549956105.8529] Erro
Feb 12 09:21:45 ubuntu-aia NetworkManager[54525]: <info>  [1549956105.8598] mode
Feb 12 09:21:45 ubuntu-aia NetworkManager[54525]: <info>  [1549956105.8607] mana
lines 1-19/19 (END)
```

To turn NetworkManager off (immediately and permanently) on a RHEL 6 or older Fedora system:

#service NetworkManager stop

Ensure that the Network Manager service is stopped using the `service` command.



```
[sudo] password for aia:
aia@ubuntu-aia: ~
[sudo] password for aia:
aia@ubuntu-aia:~$ mkdir network-scripts
aia@ubuntu-aia:~$ sudo nano /etc/sysconfig/network-scripts
aia@ubuntu-aia:~$ 
aia@ubuntu-aia:~$ mkdir network-scripts
mkdir: cannot create directory 'network-scripts': File exists
aia@ubuntu-aia:~$ mkdir /etc/sysconfig/network-scripts
mkdir: cannot create directory '/etc/sysconfig/network-scripts': No such file or
directory
aia@ubuntu-aia:~$ mkdir sysconfig/network-scripts
mkdir: cannot create directory 'sysconfig/network-scripts': No such file or dire
ctory
aia@ubuntu-aia:~$ sudo /etc/init.d/network status
sudo: /etc/init.d/network: command not found
aia@ubuntu-aia:~$ /etc/init.d/network status
-bash: /etc/init.d/network: No such file or directory
aia@ubuntu-aia:~$ service NetworkManager stop
===== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ===
Authentication is required to stop 'NetworkManager.service'.
Authenticating as: Aia,,, (aia)
Password:
===== AUTHENTICATION COMPLETE ===
aia@ubuntu-aia:~$
```

#service network restart

```
sudo service network-manager restart
```

- Ensure that the network manager service is disable using the `chkconfig` command.

```
#chkconfig NetworkManager off
```

first it needs to install `chkconfig` tool by using the following command:

```
sudo apt-get install chkconfig
```

```
#chkconfig network on
```

For RHEL 7 and newer Fedora systems that use the `systemctl` command to start, stop, enable, and disable services.

```
#systemctl stop NetworkManager.service
```

```
aia@ubuntu-aia:~$ chkconfig
chkconfig: command not found
aia@ubuntu-aia:~$ nano chkconfig
aia@ubuntu-aia:~$ sudo chkconfig
sudo: chkconfig: command not found
aia@ubuntu-aia:~$ su-

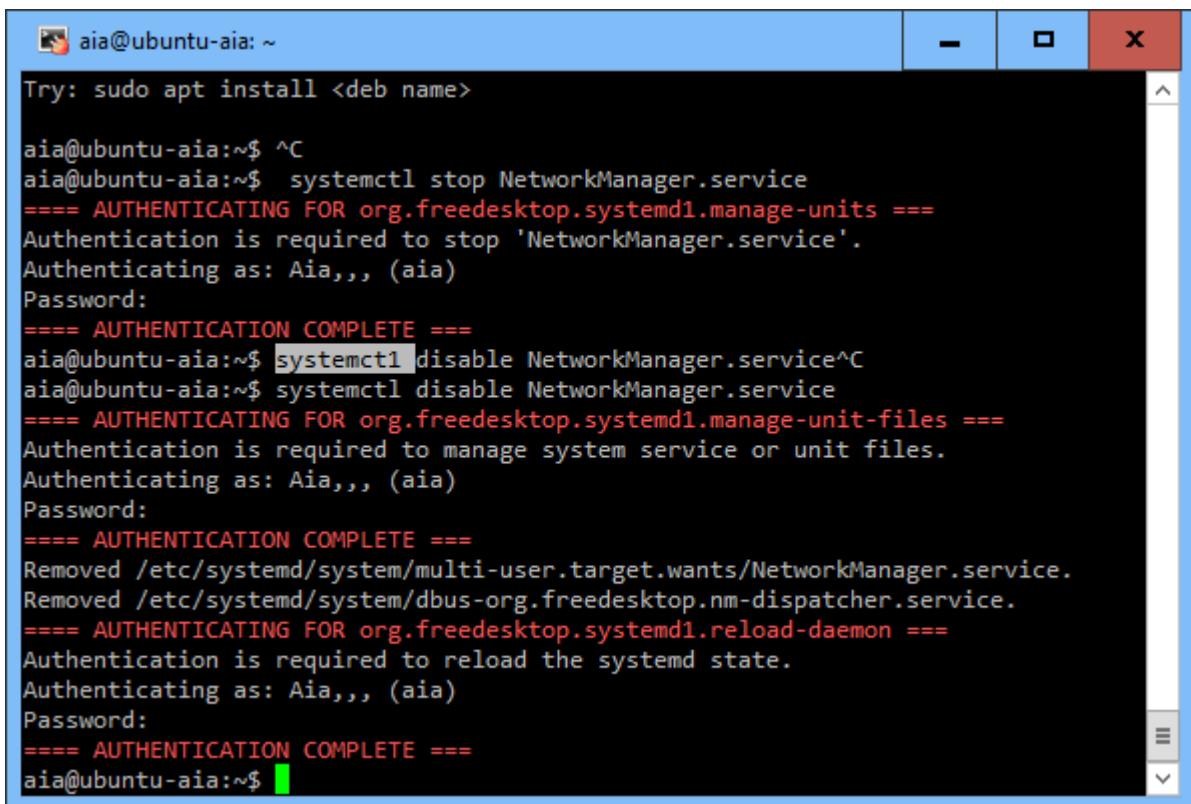
Command 'su-' not found, did you mean:

  command 'sur' from deb subtle
  command 'sum' from deb coreutils
  command 'su1' from deb htools
  command 'su' from deb login
  command 'sup' from deb sup

Try: sudo apt install <deb name>

aia@ubuntu-aia:~$ systemctl stop NetworkManager.service
===== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ===
Authentication is required to stop 'NetworkManager.service'.
Authenticating as: Aia,,, (aia)
Password:
===== AUTHENTICATION COMPLETE ===
aia@ubuntu-aia:~$
```

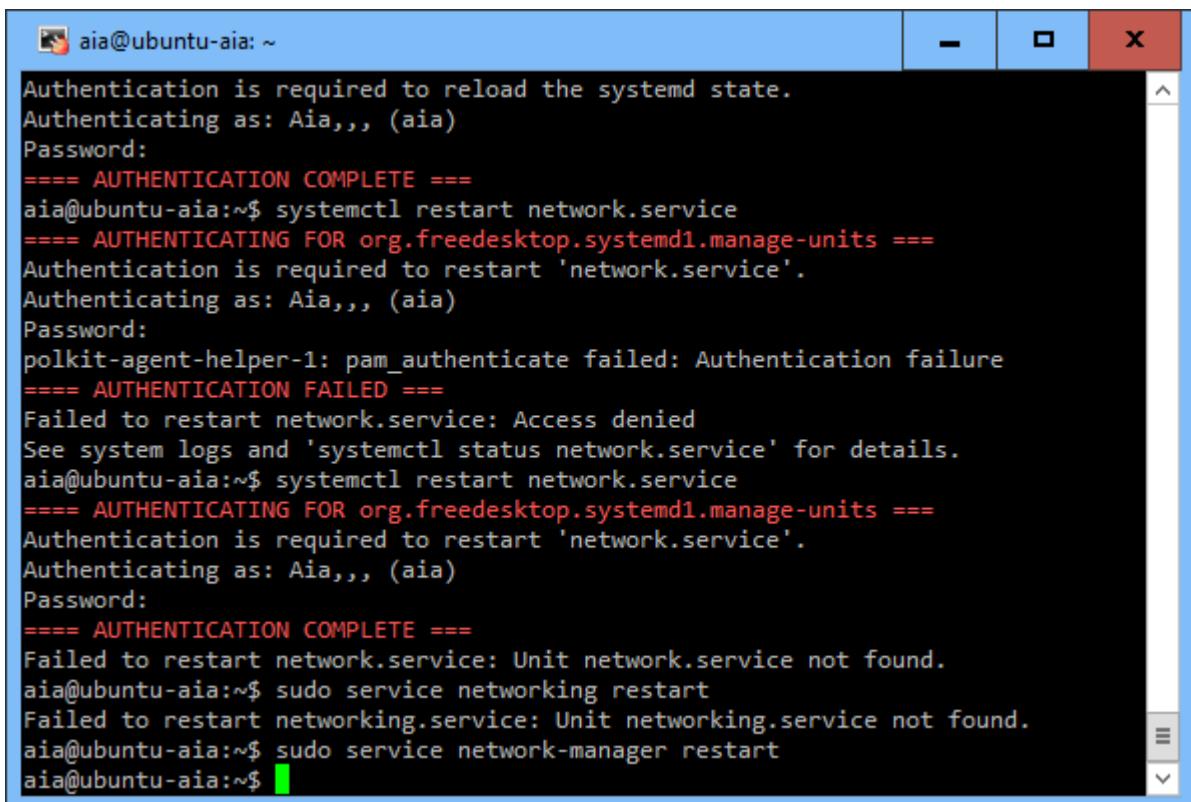
```
#systemctl disable NetworkManager.service
```



```
aia@ubuntu-aia:~$ sudo apt install <deb name>
aia@ubuntu-aia:~$ ^C
aia@ubuntu-aia:~$ systemctl stop NetworkManager.service
===== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ===
Authentication is required to stop 'NetworkManager.service'.
Authenticating as: Aia,,, (aia)
Password:
===== AUTHENTICATION COMPLETE ===
aia@ubuntu-aia:~$ systemctl disable NetworkManager.service^C
aia@ubuntu-aia:~$ systemctl disable NetworkManager.service
===== AUTHENTICATING FOR org.freedesktop.systemd1.manage-unit-files ===
Authentication is required to manage system service or unit files.
Authenticating as: Aia,,, (aia)
Password:
===== AUTHENTICATION COMPLETE ===
Removed /etc/systemd/system/multi-user.target.wants/NetworkManager.service.
Removed /etc/systemd/system/dbus-org.freedesktop.nm-dispatcher.service.
===== AUTHENTICATING FOR org.freedesktop.systemd1.reload-daemon ===
Authentication is required to reload the systemd state.
Authenticating as: Aia,,, (aia)
Password:
===== AUTHENTICATION COMPLETE ===
aia@ubuntu-aia:~$
```

#systemctl restart network.service it didn't work, there is other command it managed to configure.

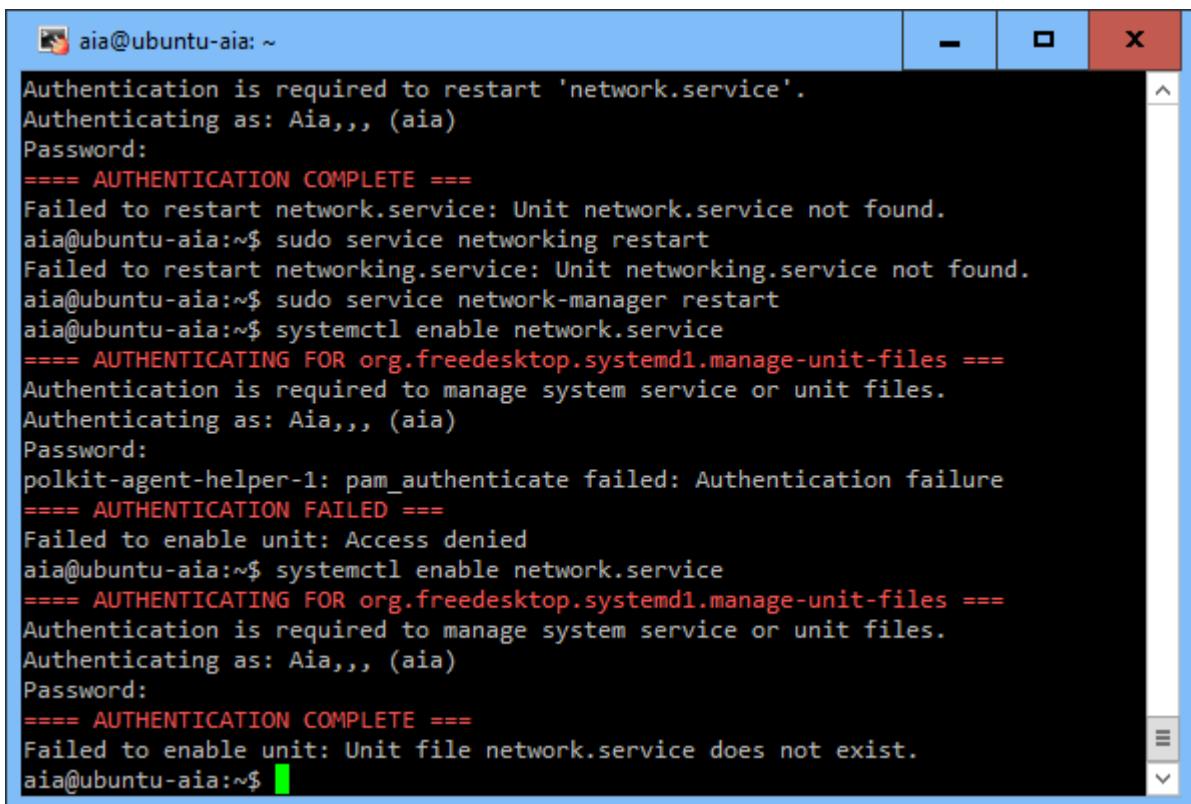
#sudo service network-manager restart



```
aia@ubuntu-aia:~$ 
Authentication is required to reload the systemd state.
Authenticating as: Aia,,, (aia)
Password:
===== AUTHENTICATION COMPLETE ===
aia@ubuntu-aia:~$ systemctl restart network.service
===== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ===
Authentication is required to restart 'network.service'.
Authenticating as: Aia,,, (aia)
Password:
polkit-agent-helper-1: pam_authenticate failed: Authentication failure
===== AUTHENTICATION FAILED ===
Failed to restart network.service: Access denied
See system logs and 'systemctl status network.service' for details.
aia@ubuntu-aia:~$ systemctl restart network.service
===== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ===
Authentication is required to restart 'network.service'.
Authenticating as: Aia,,, (aia)
Password:
===== AUTHENTICATION COMPLETE ===
Failed to restart network.service: Unit network.service not found.
aia@ubuntu-aia:~$ sudo service networking restart
Failed to restart networking.service: Unit networking.service not found.
aia@ubuntu-aia:~$ sudo service network-manager restart
aia@ubuntu-aia:~$
```

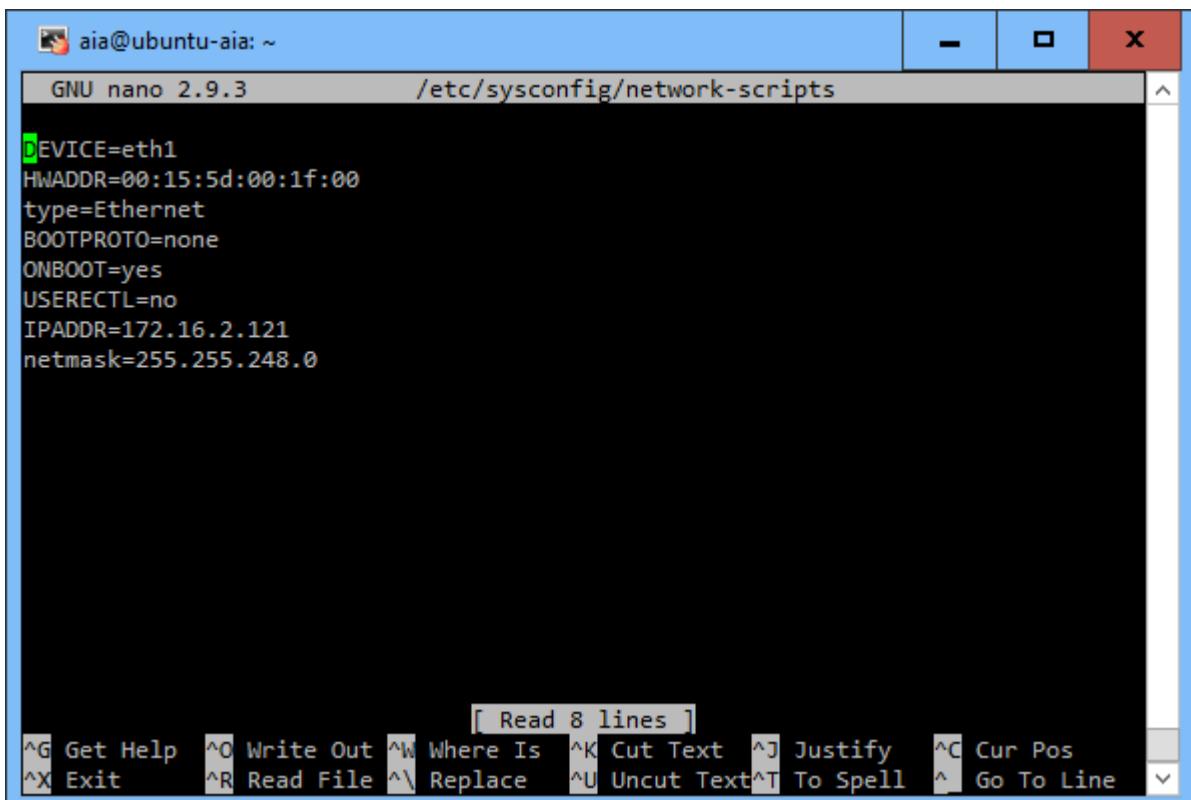
To enable the network service using the command:

#systemctl enable network.service



```
aia@ubuntu-aia: ~
Authentication is required to restart 'network.service'.
Authenticating as: Aia,,, (aia)
Password:
==== AUTHENTICATION COMPLETE ===
Failed to restart network.service: Unit network.service not found.
aia@ubuntu-aia:~$ sudo service networking restart
Failed to restart networking.service: Unit networking.service not found.
aia@ubuntu-aia:~$ sudo service network-manager restart
aia@ubuntu-aia:~$ systemctl enable network.service
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-unit-files ===
Authentication is required to manage system service or unit files.
Authenticating as: Aia,,, (aia)
Password:
polkit-agent-helper-1: pam_authenticate failed: Authentication failure
==== AUTHENTICATION FAILED ===
Failed to enable unit: Access denied
aia@ubuntu-aia:~$ systemctl enable network.service
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-unit-files ===
Authentication is required to manage system service or unit files.
Authenticating as: Aia,,, (aia)
Password:
==== AUTHENTICATION COMPLETE ===
Failed to enable unit: Unit file network.service does not exist.
aia@ubuntu-aia:~$
```

It is safe to use the sections to help directly edit network configuration files. `ifcfg-eth1` file might look like for a wired Ethernet interface that uses static IP addresses:

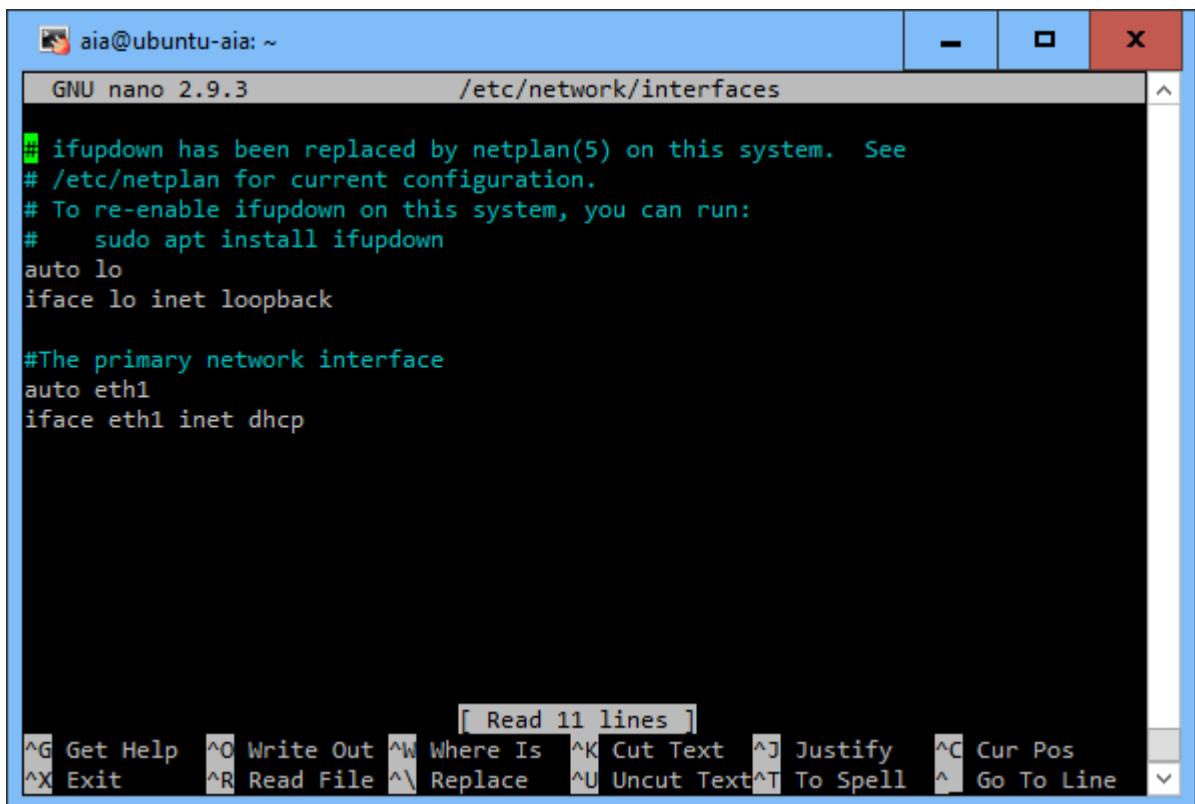


```
GNU nano 2.9.3          /etc/sysconfig/network-scripts
DEVICE=eth1
HWADDR=00:15:5d:00:1f:00
type=Ethernet
BOOTPROTO=none
ONBOOT=yes
USERCTL=no
IPADDR=172.16.2.121
netmask=255.255.248.0
```

The bottom of the screen shows the nano editor's command bar:

- [Read 8 lines]
- ^G Get Help** **^O Write Out** **^W Where Is** **^K Cut Text** **^J Justify** **^C Cur Pos**
- ^X Exit** **^R Read File** **^\\ Replace** **^U Uncut Text** **^T To Spell** **^** **Go To Line**

To configure your Ubuntu distribution to be a DHCP client, you need to modify the `/etc/network/interfaces` file. You will need to add the following line to the file:



```
aia@ubuntu-aia: ~
GNU nano 2.9.3          /etc/network/interfaces

ifupdown has been replaced by netplan(5) on this system. See
# /etc/netplan for current configuration.
# To re-enable ifupdown on this system, you can run:
#   sudo apt install ifupdown
auto lo
iface lo inet loopback

#The primary network interface
auto eth1
iface eth1 inet dhcp
```

The system should now request network parameters from the DHCP server when booting.

To run the DHCP process manually, you can use the *dhclient* command.

```
sudo dhclient -r eth1
```

Configuring DNS settings:

To enable name resolution, you need to configure your Linux system to use DNS servers. To do this in Ubuntu, open the **/etc/network/interfaces** configuration file in a text editor

```

aia@ubuntu-aia: ~
GNU nano 2.9.3          /etc/network/interfaces      Modified ^

# ifupdown has been replaced by netplan(5) on this system. See
# /etc/netplan for current configuration.
# To re-enable ifupdown on this system, you can run:
#   sudo apt install ifupdown
auto lo
iface lo inet loopback

#The primary network interface
auto eth1
iface eth1 inet dhcp

auto eth0
iface eth0 inet static
address 172.16.2.121
netmask 255.255.248.0
gateway 172.16.2.1

^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify  ^C Cur Pos
^X Exit      ^R Read File  ^\ Replace   ^U Uncut Text^T To Spell  ^ Go To Line

```

This file is used to configure your network settings manually. The first Ethernet interface is usually identified as **eth0**. To configure a DNS server, add the **dns-nameservers IP_ADDRESS**. The line **dns-nameservers 8.8.8.8** sets up a DNS server with the IP address of **8.8.8.8** as our DNS server (it is a public DNS server from Google). To configure multiple DNS servers, just add spaces between them: **dns-nameservers IP_ADDRESS1 IP_ADDRESS2 IP_ADDRESS3**

```

aia@ubuntu-aia: ~
GNU nano 2.9.3          /etc/network/interfaces      [ Read 17 lines ]

# ifupdown has been replaced by netplan(5) on this system. See
# /etc/netplan for current configuration.
# To re-enable ifupdown on this system, you can run:
#   sudo apt install ifupdown
auto lo
iface lo inet loopback

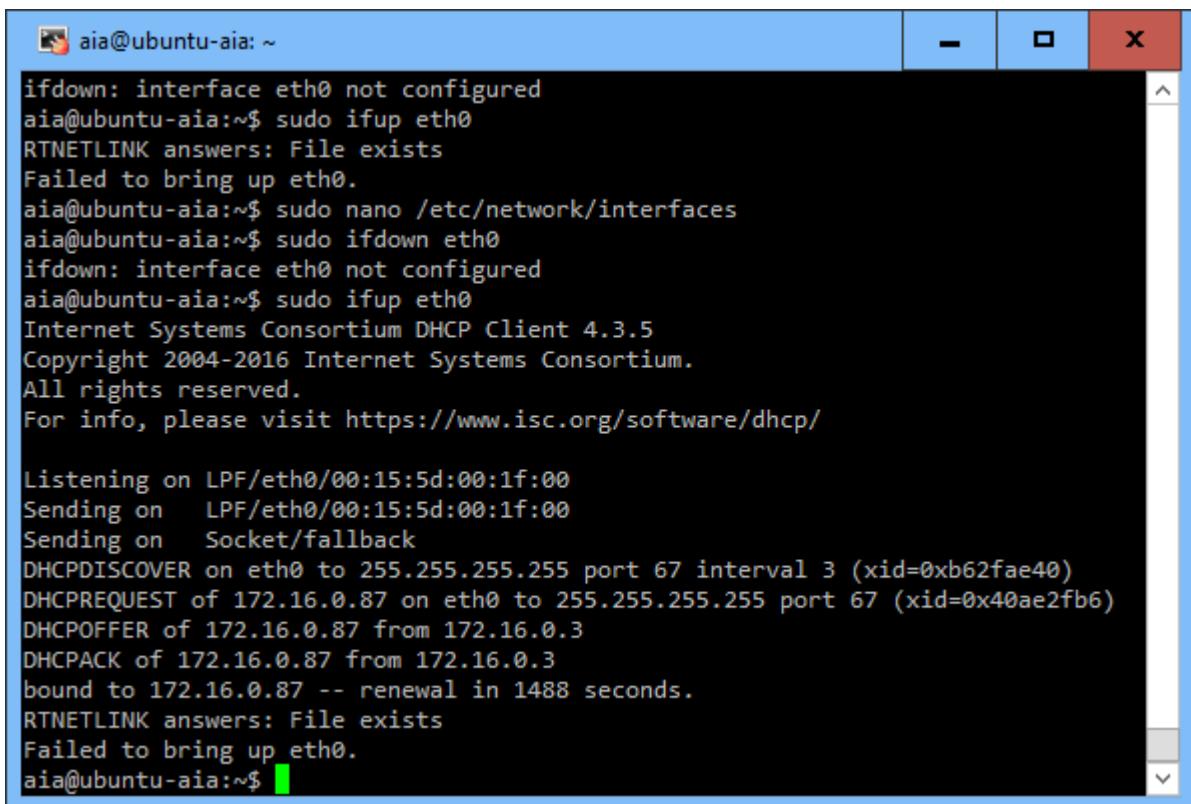
#The primary network interface
auto eth1
iface eth1 inet dhcp

auto eth0
iface eth0 inet static
address 172.16.2.121
netmask 255.255.248.0
gateway 172.16.2.1
dns-nameservers 8.8.8.8

^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify  ^C Cur Pos
^X Exit      ^R Read File  ^\ Replace   ^U Uncut Text^T To Spell  ^ Go To Line

```

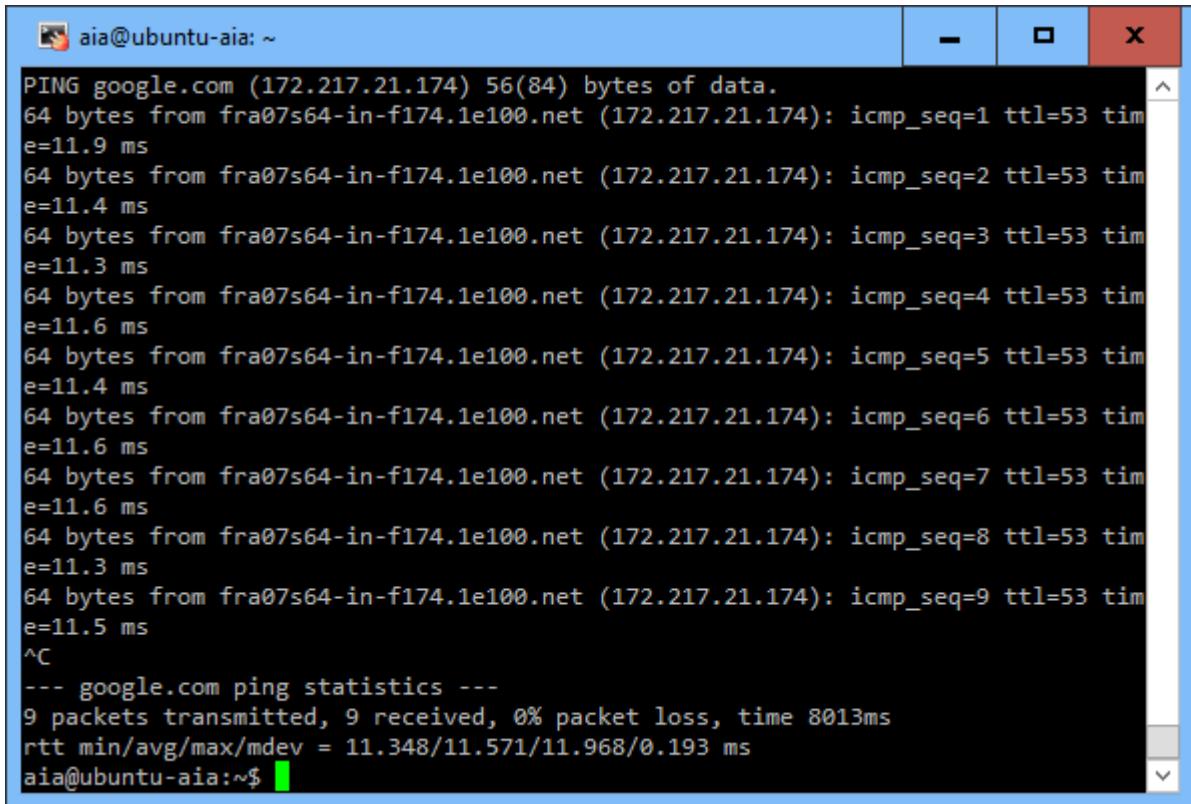
sudo ifup eth0 commands to apply the changes:



```
aia@ubuntu-aia: ~
ifdown: interface eth0 not configured
aia@ubuntu-aia:~$ sudo ifup eth0
RTNETLINK answers: File exists
Failed to bring up eth0.
aia@ubuntu-aia:~$ sudo nano /etc/network/interfaces
aia@ubuntu-aia:~$ sudo ifdown eth0
ifdown: interface eth0 not configured
aia@ubuntu-aia:~$ sudo ifup eth0
Internet Systems Consortium DHCP Client 4.3.5
Copyright 2004-2016 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/eth0/00:15:5d:00:1f:00
Sending on  LPF/eth0/00:15:5d:00:1f:00
Sending on  Socket/fallback
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 3 (xid=0xb62fae40)
DHCPOREQUEST of 172.16.0.87 on eth0 to 255.255.255.255 port 67 (xid=0x40ae2fb6)
DHCPOFFER of 172.16.0.87 from 172.16.0.3
DHCPACK of 172.16.0.87 from 172.16.0.3
bound to 172.16.0.87 -- renewal in 1488 seconds.
RTNETLINK answers: File exists
Failed to bring up eth0.
aia@ubuntu-aia:~$
```

By testing the DNS name resolution ping to google.com



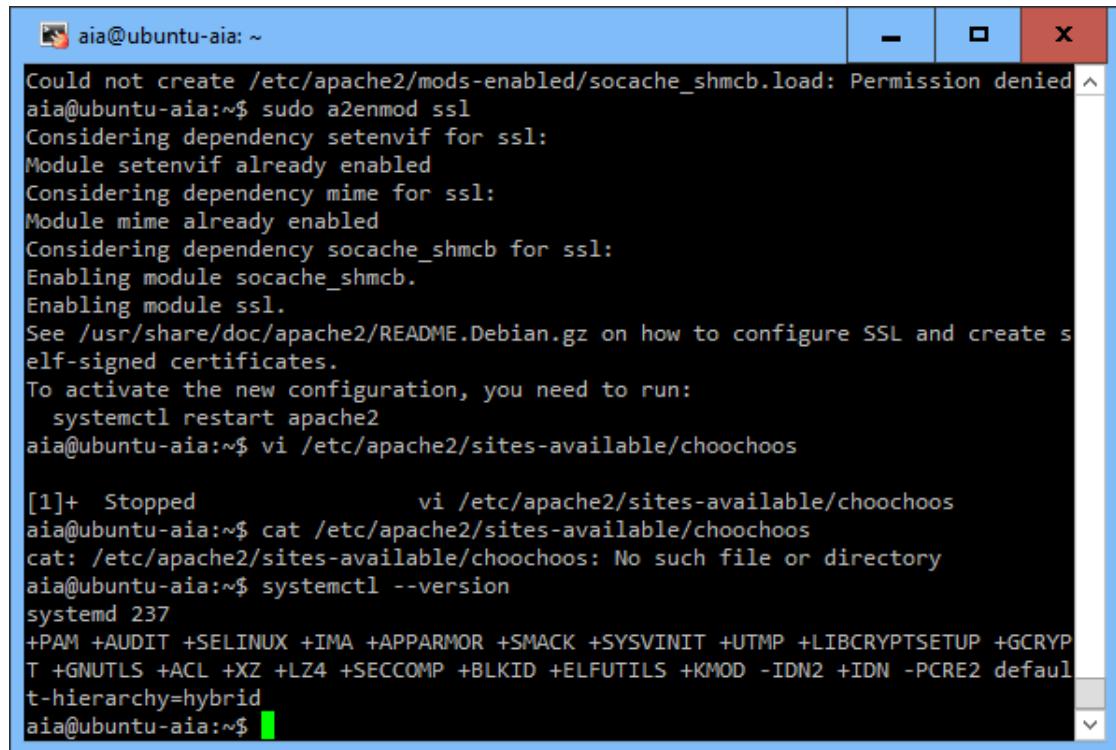
```
aia@ubuntu-aia: ~
PING google.com (172.217.21.174) 56(84) bytes of data.
64 bytes from fra07s64-in-f174.1e100.net (172.217.21.174): icmp_seq=1 ttl=53 time=11.9 ms
64 bytes from fra07s64-in-f174.1e100.net (172.217.21.174): icmp_seq=2 ttl=53 time=11.4 ms
64 bytes from fra07s64-in-f174.1e100.net (172.217.21.174): icmp_seq=3 ttl=53 time=11.3 ms
64 bytes from fra07s64-in-f174.1e100.net (172.217.21.174): icmp_seq=4 ttl=53 time=11.6 ms
64 bytes from fra07s64-in-f174.1e100.net (172.217.21.174): icmp_seq=5 ttl=53 time=11.4 ms
64 bytes from fra07s64-in-f174.1e100.net (172.217.21.174): icmp_seq=6 ttl=53 time=11.6 ms
64 bytes from fra07s64-in-f174.1e100.net (172.217.21.174): icmp_seq=7 ttl=53 time=11.6 ms
64 bytes from fra07s64-in-f174.1e100.net (172.217.21.174): icmp_seq=8 ttl=53 time=11.3 ms
64 bytes from fra07s64-in-f174.1e100.net (172.217.21.174): icmp_seq=9 ttl=53 time=11.5 ms
^C
--- google.com ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8013ms
rtt min/avg/max/mdev = 11.348/11.571/11.968/0.193 ms
aia@ubuntu-aia:~$
```

➤ Starting and Stopping Service:

systemd is the new way of running services on Linux. systemd has a superceded sysvinit. systemd brings faster boot-times to Linux and is now, a standard way to manage Linux services. While stable, systemd is still evolving. systemd as an init system, is used to manage both services and daemons that need status changes after the Linux kernel has been booted. By status change starting, stopping, reloading, and adjusting service state is applied.

Check the version of systemd currently running on our server.

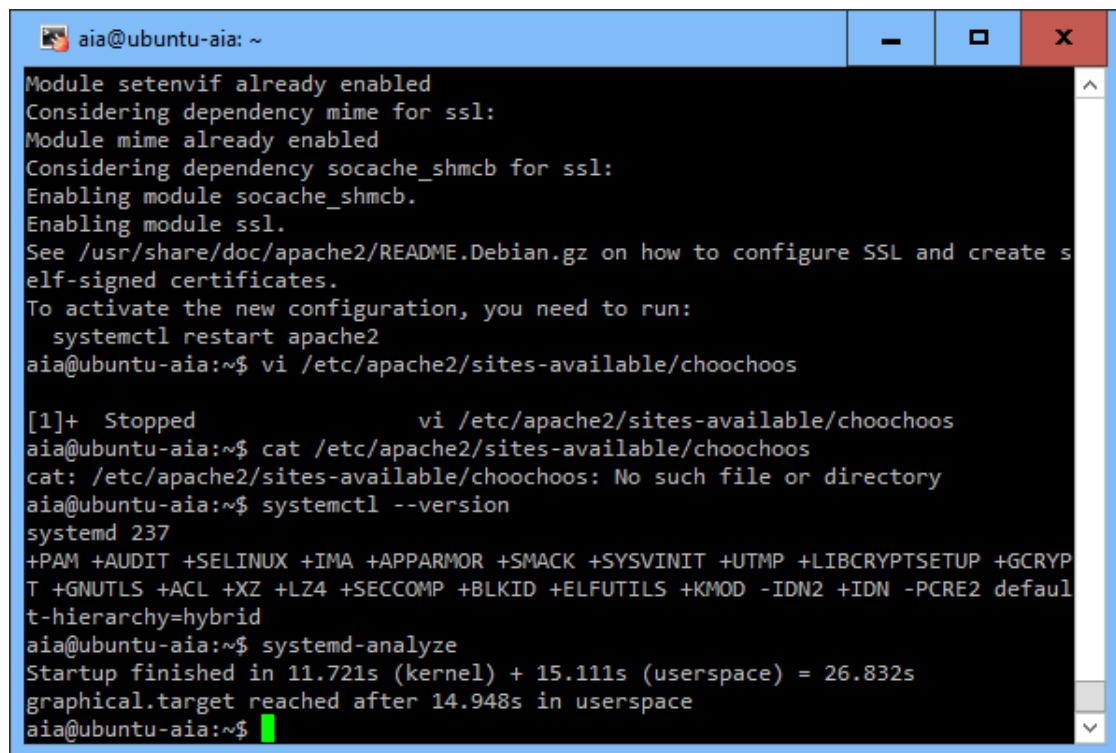
```
$ systemctl --version
```



```
aia@ubuntu-aia: ~
Could not create /etc/apache2/mods-enabled/socache_shmcb.load: Permission denied
aia@ubuntu-aia:~$ sudo a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certificates.
To activate the new configuration, you need to run:
  systemctl restart apache2
aia@ubuntu-aia:~$ vi /etc/apache2/sites-available/choochoos

[1]+  Stopped                  vi /etc/apache2/sites-available/choochoos
aia@ubuntu-aia:~$ cat /etc/apache2/sites-available/choochoos
cat: /etc/apache2/sites-available/choochoos: No such file or directory
aia@ubuntu-aia:~$ systemctl --version
systemd 237
+PAM +AUDIT +SELINUX +IMA +APPARMOR +SMACK +SYSVINIT +UTMP +LIBCRYPTSETUP +GCRYPT
+GNUTLS +ACL +XZ +LZ4 +SECCOMP +BLKID +ELFUTILS +KMOD -IDN2 +IDN -PCRE2 default
t-hierarchy=hybrid
aia@ubuntu-aia:~$
```

Fully updated at the time of this writing systemd version 237 is the current stable version.



The screenshot shows a terminal window titled 'aia@ubuntu-aia: ~'. The terminal displays the following text:

```

Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certificates.
To activate the new configuration, you need to run:
  systemctl restart apache2
aia@ubuntu-aia:~$ vi /etc/apache2/sites-available/choochoos

[1]+  Stopped                  vi /etc/apache2/sites-available/choochoos
aia@ubuntu-aia:~$ cat /etc/apache2/sites-available/choochoos
cat: /etc/apache2/sites-available/choochoos: No such file or directory
aia@ubuntu-aia:~$ systemctl --version
systemd 237
+PAM +AUDIT +SELINUX +IMA +APPARMOR +SMACK +SYSVINIT +UTMP +LIBCRYPTSETUP +GCRYPT
+GNUTLS +ACL +XZ +LZ4 +SECCOMP +BLKID +ELFUTILS +KMOD -IDN2 +IDN -PCRE2 default-hierarchy=hybrid
aia@ubuntu-aia:~$ systemd-analyze
Startup finished in 11.721s (kernel) + 15.111s (userspace) = 26.832s
graphical.target reached after 14.948s in userspace
aia@ubuntu-aia:~$ 
```

```
$ systemd-analyze
```

We can also analyze the last server boot time with *systemd-analyze*

When the system boot times are slower, we can use the *systemd-analyze blame* command.

```
$ systemd-analyze blame
```

```
aia@ubuntu-aia:~$ systemd-analyze
Startup finished in 11.721s (kernel) + 15.111s (userspace) = 26.832s
graphical.target reached after 14.948s in userspace
aia@ubuntu-aia:~$ systemd-analyze blame
 30.229s apt-daily.service
   7.329s dev-mapper-ubuntu\x2d\x2daia\x2d\x2dvg\x2droot.device
   5.323s apt-daily-upgrade.service
   3.411s apparmor.service
   3.038s lvm2-pvscan@8:1.service
   3.023s networkd-dispatcher.service
   2.788s lxd-containers.service
   2.620s grub-common.service
   2.206s systemd-networkd-wait-online.service
   2.120s accounts-daemon.service
   2.001s lvm2-monitor.service
   1.886s systemd-logind.service
   1.588s snapd.service
   1.334s dev-mqueue.mount
   1.328s apport.service
   1.264s kmod-static-nodes.service
   1.262s systemd-journal-flush.service
   1.249s ufw.service
   1.238s keyboard-setup.service
   1.224s dev-hugepages.mount
```

When working with *systemd*, it is important to understand the concept of *units*.

Units are the resources *systemd* knows how to interpret. Units are categorized into 12 types:

- .service
- .socket
- .device
- .mount
- .automount
- .swap
- .target
- .path
- .timer
- .snapshot
- .slice
- .scope

Manage Service with *systemctl*:

Starting the service

```
$ systemctl -t service
```

```
aia@ubuntu-aia: ~
● UNIT           LOAD  ACTIVE SUB   DESCRIPTION
accounts-daemon.service loaded active running Accounts Service
apache2.service        loaded active running The Apache HTTP Server
apparmor.service       loaded active exited  AppArmor initialization
apport.service         loaded active exited  LSB: automatic crash report
apt-daily.service     ● failed failed Daily apt download activit
atd.service          loaded active running Deferred execution schedul
blk-availability.service loaded active exited Availability of block devi
console-setup.service loaded active exited Set console font and keyma
cron.service          loaded active running Regular background program
dbus.service          loaded active running D-Bus System Message Bus
firewalld.service     loaded active running firewalld - dynamic firewa
getty@tty1.service    loaded active running Getty on tty1
grub-common.service   loaded active exited  LSB: Record successful boo
irqbalance.service   loaded active running irqbalance daemon
keyboard-setup.service loaded active exited Set the console keyboard l
kmod-static-nodes.service loaded active exited Create list of required st
lvm2-lvmetad.service loaded active running LVM2 metadata daemon
lvm2-monitor.service  loaded active exited Monitoring of LVM2 mirrors
lvm2-pvscan@8:1.service loaded active exited  LVM2 PV scan on device 8:1
lxcfs.service         loaded active running FUSE filesystem for LXC
lxd-containers.service loaded active exited LXD - container startup/sh
ModemManager.service  loaded active running Modem Manager
lines 1-23
```

Stopping the service

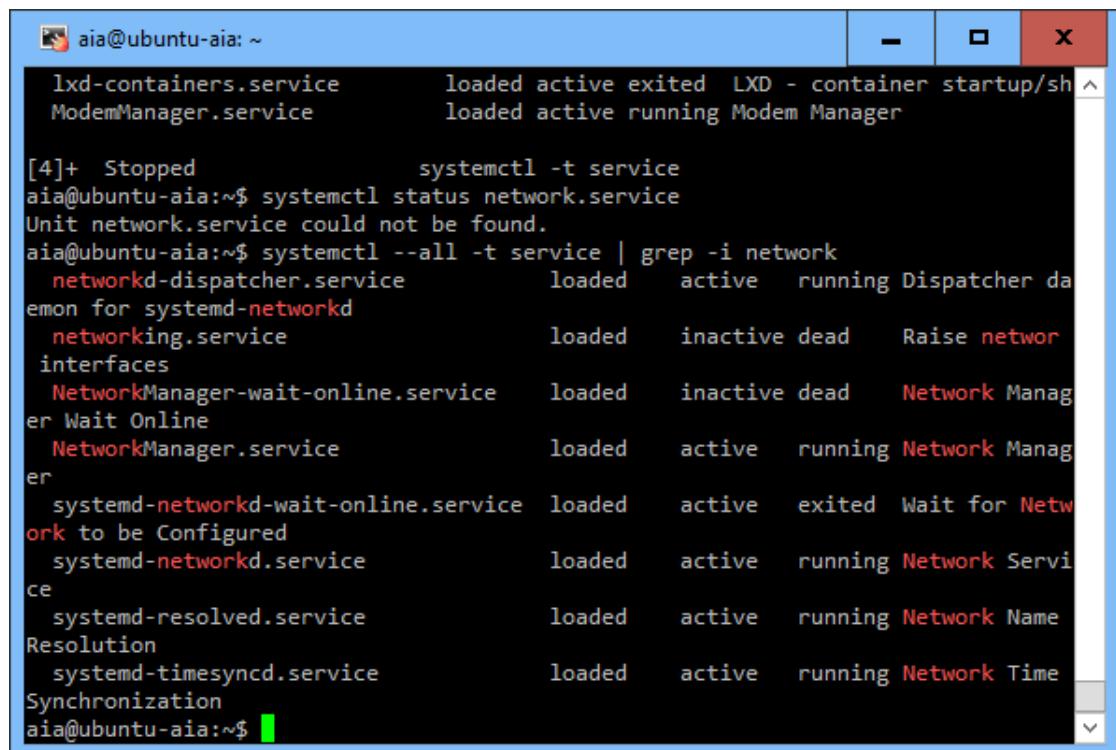
```
$ systemctl stop Bluetooth
```

```
aia@ubuntu-aia: ~
● UNIT           LOAD  ACTIVE SUB   DESCRIPTION
cron.service      loaded active running Regular background program
dbus.service       loaded active running D-Bus System Message Bus
firewalld.service loaded active running firewalld - dynamic firewa
getty@tty1.service loaded active running Getty on tty1
grub-common.service loaded active exited  LSB: Record successful boo
irqbalance.service loaded active running irqbalance daemon
keyboard-setup.service loaded active exited Set the console keyboard l
kmod-static-nodes.service loaded active exited Create list of required st
lvm2-lvmetad.service loaded active running LVM2 metadata daemon
lvm2-monitor.service loaded active exited Monitoring of LVM2 mirrors
lvm2-pvscan@8:1.service loaded active exited  LVM2 PV scan on device 8:1
lxcfs.service      loaded active running FUSE filesystem for LXC
lxd-containers.service loaded active exited LXD - container startup/sh
ModemManager.service loaded active running Modem Manager

[3]+ Stopped                  systemctl -t service
aia@ubuntu-aia:~$ systemctl stop bluetooth
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ===
Authentication is required to stop 'bluetooth.service'.
Authenticating as: Aia,,, (aia)
Password:
==== AUTHENTICATION COMPLETE ===
Failed to stop bluetooth.service: Unit bluetooth.service not loaded.
aia@ubuntu-aia:~$
```

Show us the current status of the *networking* service. If we want to see all the services related to networking

```
$ systemctl --all -t service | grep -i network
```

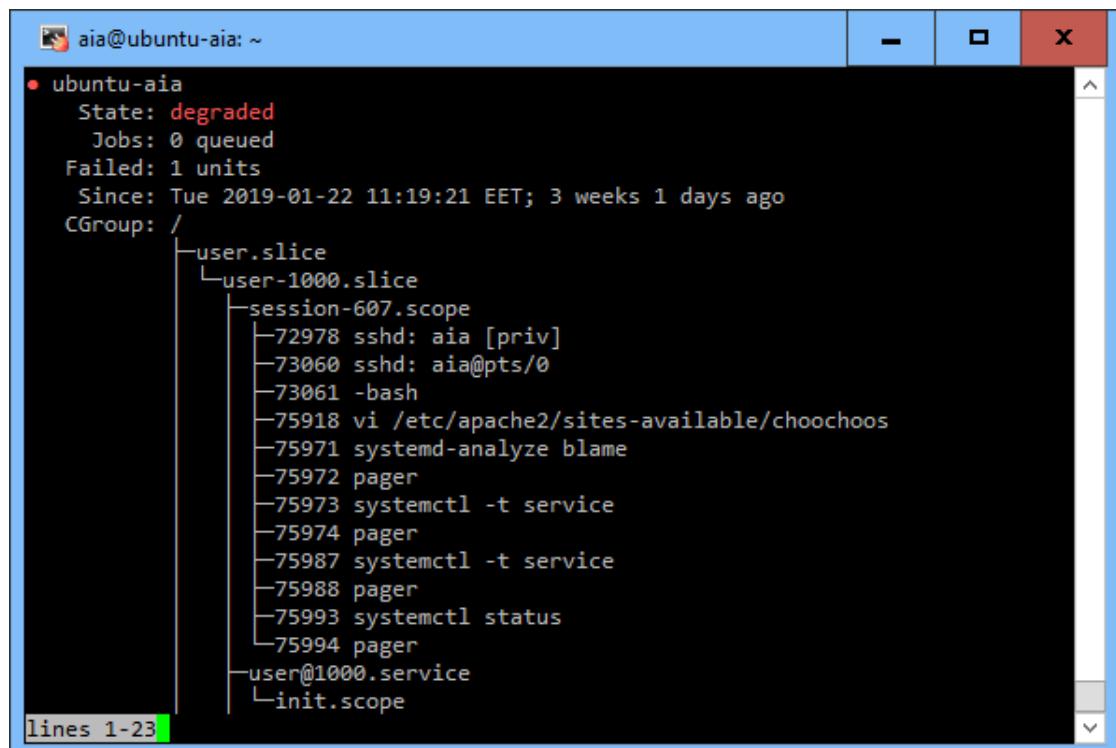


```
aia@ubuntu-aia: ~
lxr-containers.service      loaded active exited  LXD - container startup/sh
ModemManager.service        loaded active running Modem Manager

[4]+ Stopped                  systemctl -t service
aia@ubuntu-aia:~$ systemctl status network.service
Unit network.service could not be found.
aia@ubuntu-aia:~$ systemctl --all -t service | grep -i network
    networkd-dispatcher.service          loaded   active  running Dispatcher da
emon for systemd-networkd
    networking.service                 loaded   inactive dead   Raise networ
interfaces
    NetworkManager-wait-online.service loaded   inactive dead   Network Manag
er Wait Online
    NetworkManager.service            loaded   active  running Network Manag
er
    systemd-networkd-wait-online.service loaded   active  exited  Wait for Netw
ork to be Configured
    systemd-networkd.service          loaded   active  running Network Servi
ce
    systemd-resolved.service         loaded   active  running Network Name
Resolution
    systemd-timesyncd.service       loaded   active  running Network Time
Synchronization
aia@ubuntu-aia:~$
```

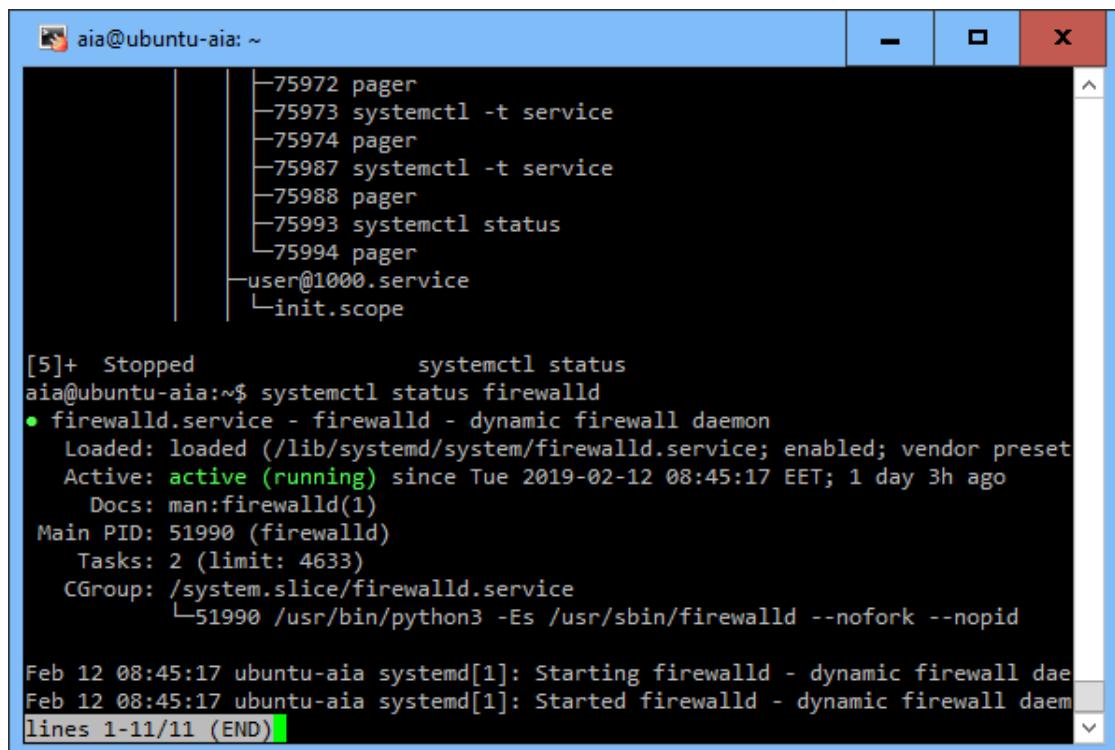
Status is most simple form it can be used for checking the system status:

```
$systemctl status
```



```
aia@ubuntu-aia: ~
● ubuntu-aia
  State: degraded
  Jobs: 0 queued
  Failed: 1 units
  Since: Tue 2019-01-22 11:19:21 EET; 3 weeks 1 days ago
  CGroup: /
    └─user.slice
      └─user-1000.slice
        ├─session-607.scope
        │  ├─72978 sshd: aia [priv]
        │  ├─73060 sshd: aia@pts/0
        │  ├─73061 -bash
        │  ├─75918 vi /etc/apache2/sites-available/choochoos
        │  ├─75971 systemd-analyze blame
        │  ├─75972 pager
        │  ├─75973 systemctl -t service
        │  ├─75974 pager
        │  ├─75987 systemctl -t service
        │  ├─75988 pager
        │  ├─75993 systemctl status
        │  ├─75994 pager
        │  └─user@1000.service
          └─init.scope
lines 1-23
```

```
$ systemctl status firewalld
```



```

aia@ubuntu-aia: ~
[5]+ Stopped                  systemctl status
aia@ubuntu-aia:~$ systemctl status firewalld
● firewalld.service - firewalld - dynamic firewall daemon
  Loaded: loaded (/lib/systemd/system/firewalld.service; enabled; vendor preset: enabled)
  Active: active (running) since Tue 2019-02-12 08:45:17 EET; 1 day 3h ago
    Docs: man:firewalld(1)
   Main PID: 51990 (firewalld)
     Tasks: 2 (limit: 4633)
    CGroup: /system.slice/firewalld.service
            └─51990 /usr/bin/python3 -Es /usr/sbin/firewalld --nofork --nopid

Feb 12 08:45:17 ubuntu-aia systemd[1]: Starting firewalld - dynamic firewall dae
Feb 12 08:45:17 ubuntu-aia systemd[1]: Started firewalld - dynamic firewall daem
lines 1-11/11 (END)

```

➤ Configuring a Web Server:

The server takes the requested file or page from you and maps it to the corresponding file from the server. The server sends the file back to the browser with some information such as its MIME type, the length of the content and some other useful information. Sometimes the requested file is a static page like HTML pages or dynamic pages like PHP, Java, Perl or any other server-side language.

we will use **Apache server** for several reasons:

- It is stable.
- It is flexible.
- It is secure.

HTTP:

When you request a file or a page from a web server, the client at first connects to the server on port 80. After successful connection, the client then sends HTTP commands (also methods) to the server. This command includes a request header which includes information about the client.

Installing Apache Web server:

```
sudo apt-get install http
```

```
sudo apt-get install apache2
```

If we are using a firewall like iptables, you should add a role for port 80.

```
sudo apt-get install iptables-persistent
```

first we need to upgrade iptables persistent

This command shows that apache2 have been installed:

```
$ ls -l /var/www
```

```
aia@ubuntu-aia: ~
Try 'snap info microk8s' for all the latest goodness.

* Canonical Livepatch is available for installation.
  - Reduce system reboots and improve kernel security. Activate at:
    https://ubuntu.com/livepatch

35 packages can be updated.
0 updates are security updates.

*** System restart required ***
Last login: Tue Feb 12 11:28:31 2019 from 172.16.1.112
aia@ubuntu-aia:~$ sudo apt-get install iptables-persistent
[sudo] password for aia:
Reading package lists... Done
Building dependency tree
Reading state information... Done
iptables-persistent is already the newest version (1.0.4+nmu2).
0 upgraded, 0 newly installed, 0 to remove and 35 not upgraded.
aia@ubuntu-aia:~$ ls -l /var/www
total 4
drwxr-xr-x 2 root root 4096 Feb 12 11:05 html
aia@ubuntu-aia:~$
```

```
$ dpkg -l | grep apache | tr -s ''
```

```
aia@ubuntu-aia: ~
0 updates are security updates.

*** System restart required ***
Last login: Tue Feb 12 11:28:31 2019 from 172.16.1.112
aia@ubuntu-aia:~$ sudo apt-get install iptables-persistent
[sudo] password for aia:
Reading package lists... Done
Building dependency tree
Reading state information... Done
iptables-persistent is already the newest version (1.0.4+nmu2).
0 upgraded, 0 newly installed, 0 to remove and 35 not upgraded.
aia@ubuntu-aia:~$ ls -l /var/www
total 4
drwxr-xr-x 2 root root 4096 Feb 12 11:05 html
aia@ubuntu-aia:~$ ^C
aia@ubuntu-aia:~$ dpkg -l | grep apache | tr -s ' '
ii apache2 2.4.29-1ubuntu4.5 amd64 Apache HTTP Server
ii apache2-bin 2.4.29-1ubuntu4.5 amd64 Apache HTTP Server (modules and other binary files)
ii apache2-data 2.4.29-1ubuntu4.5 all Apache HTTP Server (common files)
ii apache2-utils 2.4.29-1ubuntu4.5 amd64 Apache HTTP Server (utility programs for web servers)
aia@ubuntu-aia:~$
```

Running apache:

This command is used to check the status of the service.

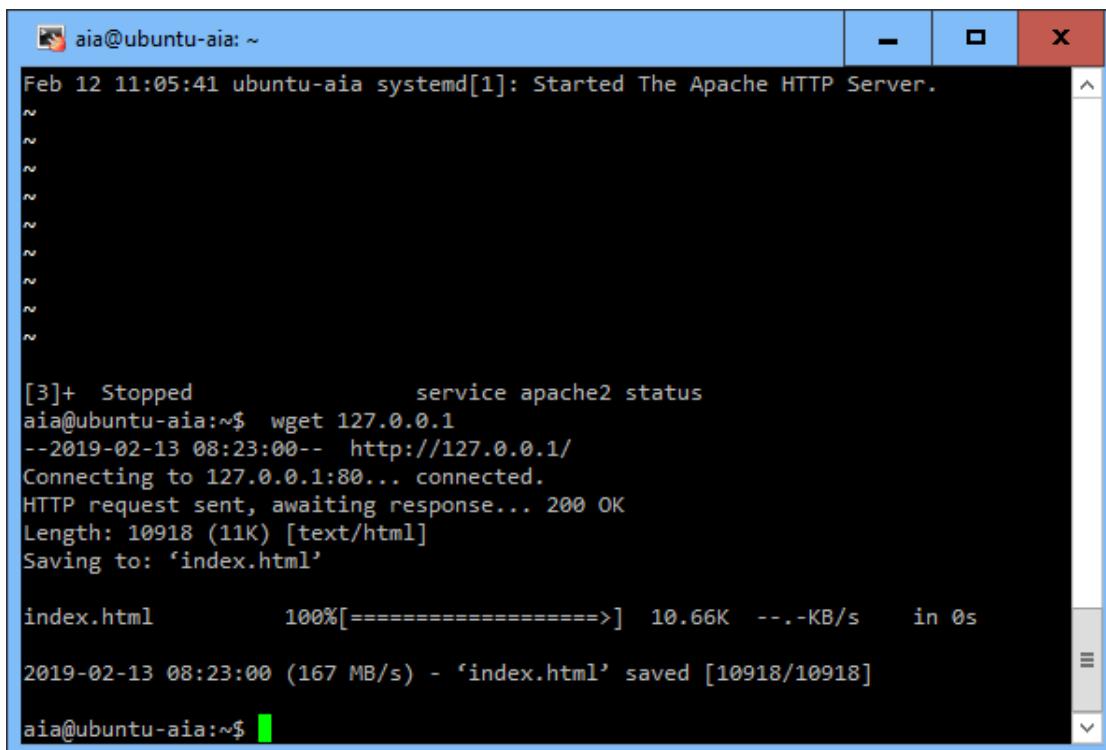
`$ service apache2 status`

```
aia@ubuntu-aia:~$ ^C
aia@ubuntu-aia:~$ dpkg -l | grep apache | tr -s ' '
ii apache2 2.4.29-1ubuntu4.5 amd64 Apache HTTP Server
ii apache2-bin 2.4.29-1ubuntu4.5 amd64 Apache HTTP Server (modules and other binary files)
ii apache2-data 2.4.29-1ubuntu4.5 all Apache HTTP Server (common files)
ii apache2-utils 2.4.29-1ubuntu4.5 amd64 Apache HTTP Server (utility programs for web servers)
aia@ubuntu-aia:~$ service apache2 status
● apache2.service - The Apache HTTP Server
  Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: 
  Drop-In: /lib/systemd/system/apache2.service.d
            └─apache2-systemd.conf
    Active: active (running) since Tue 2019-02-12 11:05:41 EET; 21h ago
      Main PID: 57564 (apache2)
        Tasks: 55 (limit: 4633)
       CGroup: /system.slice/apache2.service
               ├─57564 /usr/sbin/apache2 -k start
               ├─57565 /usr/sbin/apache2 -k start
               ├─57566 /usr/sbin/apache2 -k start
               └─57567 /usr/sbin/apache2 -k start

Feb 12 11:05:41 ubuntu-aia systemd[1]: Starting The Apache HTTP Server...
Feb 12 11:05:41 ubuntu-aia systemd[1]: Started The Apache HTTP Server.
lines 1-14/14 (END)
```

Use wget and file to verify that your web server serves an html document

`$ wget 127.0.0.1`

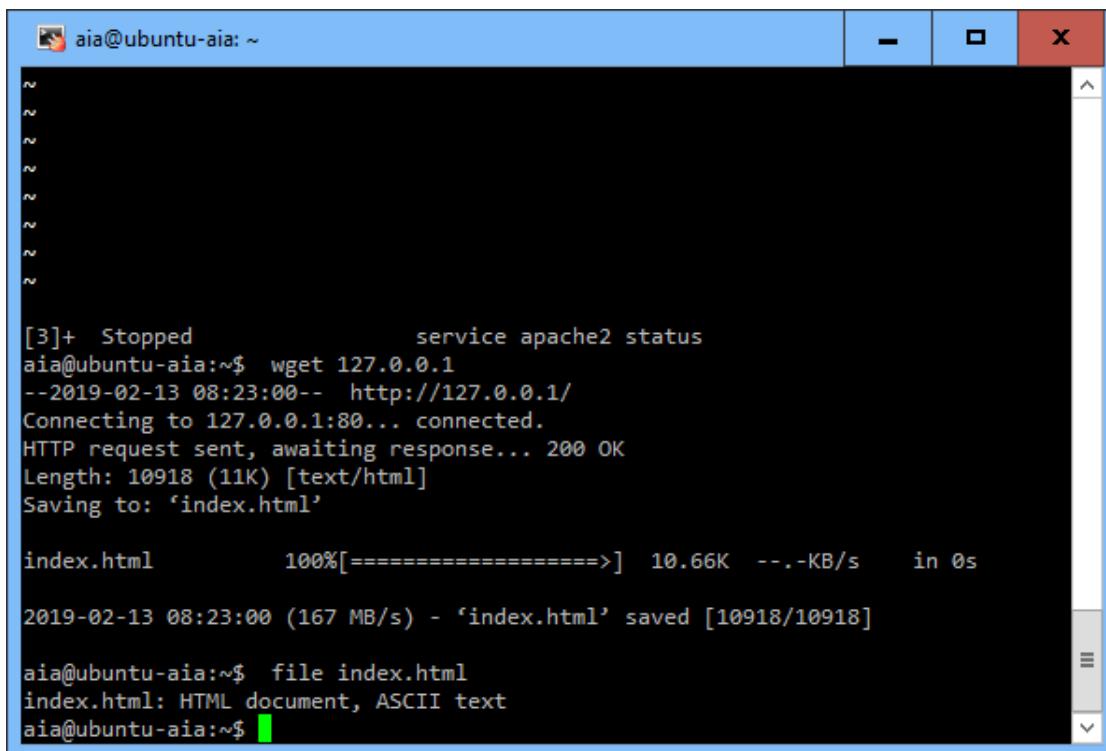


```
aia@ubuntu-aia: ~
Feb 12 11:05:41 ubuntu-aia systemd[1]: Started The Apache HTTP Server.
~
~
~
~
~
~
~
[3]+  Stopped                  service apache2 status
aia@ubuntu-aia:~$ wget 127.0.0.1
--2019-02-13 08:23:00-- http://127.0.0.1/
Connecting to 127.0.0.1:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 10918 (11K) [text/html]
Saving to: 'index.html'

index.html      100%[=====>]  10.66K  --.-KB/s   in 0s

2019-02-13 08:23:00 (167 MB/s) - 'index.html' saved [10918/10918]
aia@ubuntu-aia:~$
```

\$ file index.html



```
aia@ubuntu-aia: ~
~
~
~
~
~
~
[3]+  Stopped                  service apache2 status
aia@ubuntu-aia:~$ wget 127.0.0.1
--2019-02-13 08:23:00-- http://127.0.0.1/
Connecting to 127.0.0.1:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 10918 (11K) [text/html]
Saving to: 'index.html'

index.html      100%[=====>]  10.66K  --.-KB/s   in 0s

2019-02-13 08:23:00 (167 MB/s) - 'index.html' saved [10918/10918]
aia@ubuntu-aia:~$ file index.html
index.html: HTML document, ASCII text
aia@ubuntu-aia:~$
```

To avoid the 'could not reliably determine the fqdn' message when restarting apache.

\$ sudo nano /etc/apache2/apache2.conf

```
aia@ubuntu-aia: ~
GNU nano 2.9.3          /etc/apache2/apache2.conf

# This is the main Apache server configuration file. It contains the
# configuration directives that give the server its instructions.
# See http://httpd.apache.org/docs/2.4/ for detailed information about
# the directives and /usr/share/doc/apache2/README.Debian about Debian specific
# hints.
#
#
# Summary of how the Apache 2 configuration works in Debian:
# The Apache 2 web server configuration in Debian is quite different to
# upstream's suggested way to configure the web server. This is because Debian's
# default Apache2 installation attempts to make adding and removing modules,
# virtual hosts, and extra configuration directives as flexible as possible, in
# order to make automating the changes and administering the server as easy as
# possible.

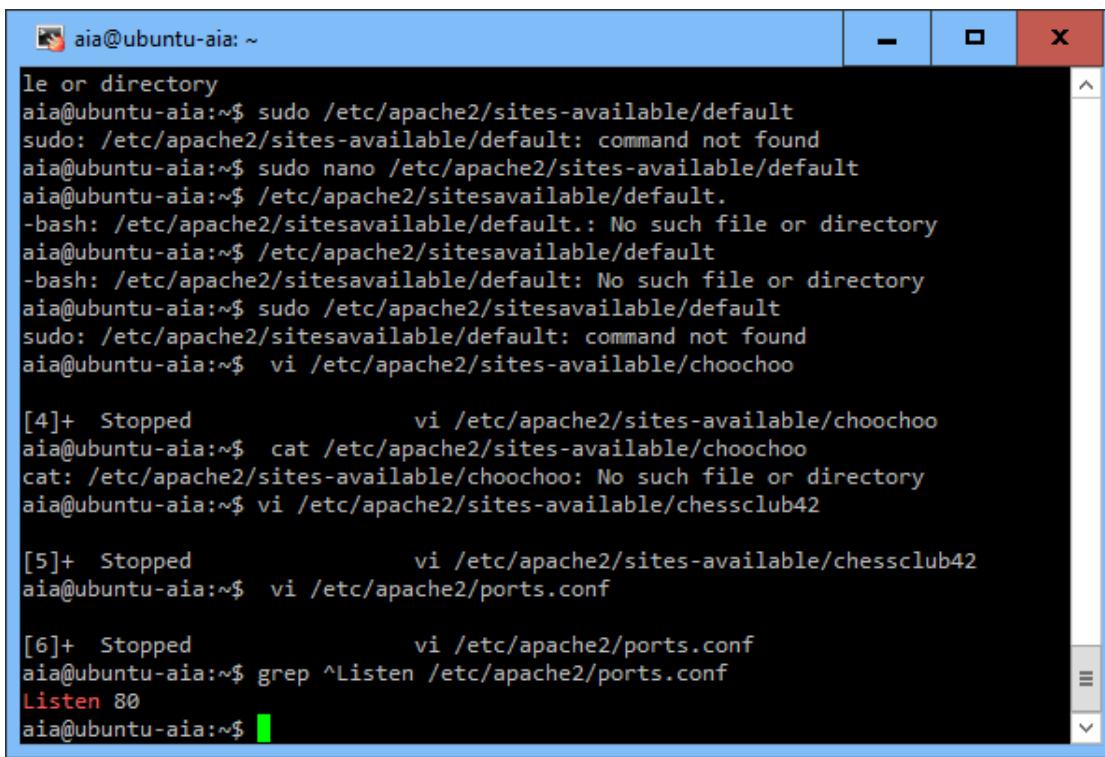
# It is split into several files forming the configuration hierarchy outlined
# below, all located in the /etc/apache2/ directory:
#
#       /etc/apache2/
[ Read 227 lines ]
^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify  ^C Cur Pos
^X Exit      ^R Read File   ^\ Replace    ^U Uncut Text ^T To Spell  ^_ Go To Line
```

To enable the port on apache in the ports.conf file. Open this file with vi and add the lines to listen on the extra ports.

```
$ vi /etc/apache2/ports.conf
```

Verify with grep that the Listen directives are added correctly.

```
$ grep ^Listen /etc/apache2/ports.conf
```



The screenshot shows a terminal window titled 'aia@ubuntu-aia: ~'. The user is navigating through the Apache configuration directory. They attempt to run 'sudo /etc/apache2/sites-available/default' but receive a 'command not found' error. They then try to edit the file with 'nano' and 'vi', but both commands are also not found. They then try to use 'cat' to view the file, which also fails because it does not exist. Finally, they successfully edit the file using 'vi /etc/apache2/sites-available/choochoo' and then use 'cat' to verify its contents.

```

le or directory
aia@ubuntu-aia:~$ sudo /etc/apache2/sites-available/default
sudo: /etc/apache2/sites-available/default: command not found
aia@ubuntu-aia:~$ sudo nano /etc/apache2/sites-available/default
aia@ubuntu-aia:~$ /etc/apache2/sitesavailable/default.
-bash: /etc/apache2/sitesavailable/default.: No such file or directory
aia@ubuntu-aia:~$ /etc/apache2/sitesavailable/default
-bash: /etc/apache2/sitesavailable/default: No such file or directory
aia@ubuntu-aia:~$ sudo /etc/apache2/sitesavailable/default
sudo: /etc/apache2/sitesavailable/default: command not found
aia@ubuntu-aia:~$ vi /etc/apache2/sites-available/choochoo

[4]+  Stopped                  vi /etc/apache2/sites-available/choochoo
aia@ubuntu-aia:~$ cat /etc/apache2/sites-available/choochoo
cat: /etc/apache2/sites-available/choochoo: No such file or directory
aia@ubuntu-aia:~$ vi /etc/apache2/sites-available/chessclub42

[5]+  Stopped                  vi /etc/apache2/sites-available/chessclub42
aia@ubuntu-aia:~$ vi /etc/apache2/ports.conf

[6]+  Stopped                  vi /etc/apache2/ports.conf
aia@ubuntu-aia:~$ grep ^Listen /etc/apache2/ports.conf
Listen 80
aia@ubuntu-aia:~$ 

```

➤ Configuring a FTP Server:

FTP stand for **F**ile **T**ransfer **P**rotocol. As the name suggest this network protocol allows you to transfer files or directories from one host to another over the network whether it is your LAN or Internet. Main features of vsFTPD are: Virtual IP configurations, Virtual users, Standalone or inetd operation, Powerful per-user configurability, Bandwidth throttling, Per-source-IP configurability, Per-source-IP limits, IPv6 and Encryption support through SSL integration.

Installing of FTP server in Ubuntu:

```
$ sudo apt-get install vsftpd
```

We need to update the system package sources list and then install **VSFTPD**

```
$ sudo apt-get update
```

```
[aia@ubuntu-aia: ~]
[720 kB]
Get:9 http://fi.archive.ubuntu.com/ubuntu bionic-updates/multiverse amd64 Packages [6,384 B]
Get:10 http://fi.archive.ubuntu.com/ubuntu bionic-updates/multiverse i386 Packages [6,544 B]
Get:11 http://security.ubuntu.com/ubuntu bionic-security/main i386 Packages [203 kB]
Get:12 http://security.ubuntu.com/ubuntu bionic-security/main amd64 Packages [268 kB]
Get:13 http://security.ubuntu.com/ubuntu bionic-security/main Translation-en [100 kB]
Get:14 http://security.ubuntu.com/ubuntu bionic-security/universe i386 Packages [120 kB]
Get:15 http://security.ubuntu.com/ubuntu bionic-security/universe amd64 Packages [123 kB]
Get:16 http://security.ubuntu.com/ubuntu bionic-security/universe Translation-en [69.1 kB]
Get:17 http://security.ubuntu.com/ubuntu bionic-security/multiverse amd64 Packages [3,324 B]
Get:18 http://security.ubuntu.com/ubuntu bionic-security/multiverse i386 Packages [3,500 B]
Fetched 3,578 kB in 1s (2,892 kB/s)
Reading package lists... Done
aia@ubuntu-aia:~$
```

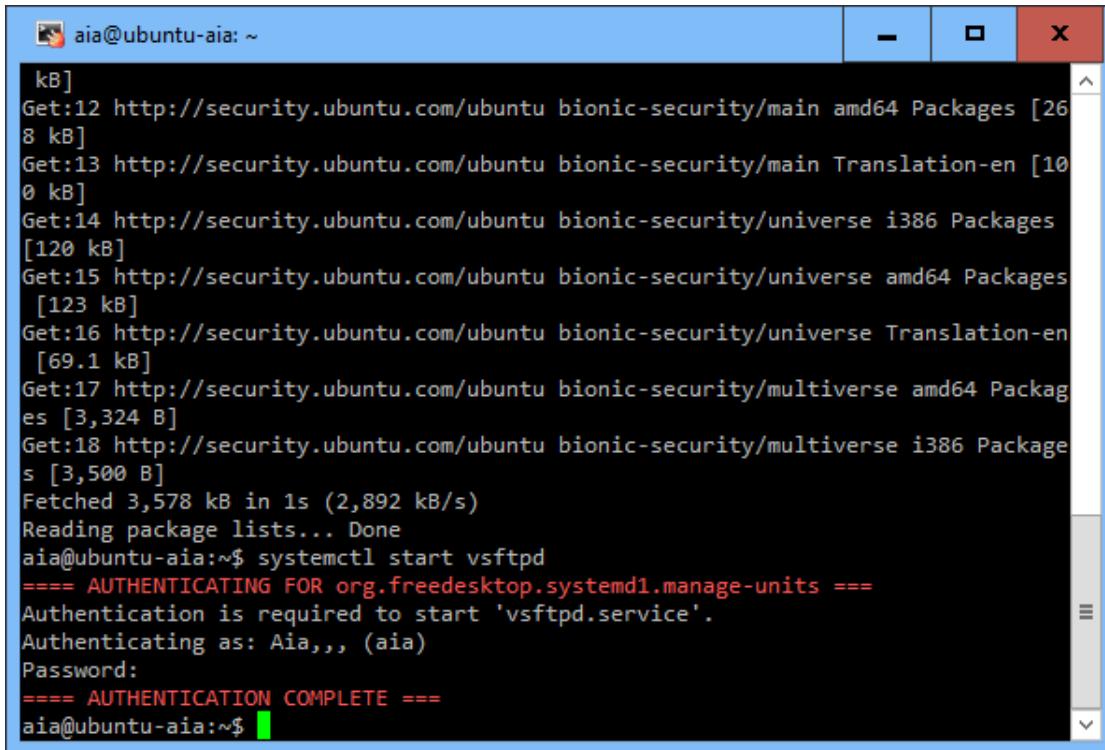
```
[aia@ubuntu-aia: ~]
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  vsftpd
0 upgraded, 1 newly installed, 0 to remove and 35 not upgraded.
Need to get 115 kB of archives.
After this operation, 334 kB of additional disk space will be used.
Get:1 http://fi.archive.ubuntu.com/ubuntu bionic/main amd64 vsftpd amd64 3.0.3-9build1 [115 kB]
Fetched 115 kB in 0s (879 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 141002 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.3-9build1_amd64.deb ...
Unpacking vsftpd (3.0.3-9build1) ...
Processing triggers for ureadahead (0.100.0-20) ...
Setting up vsftpd (3.0.3-9build1) ...
Created symlink /etc/systemd/system/multi-user.target.wants/vsftpd.service → /lib/systemd/system/vsftpd.service.
Processing triggers for systemd (237-3ubuntu10.11) ...
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...
Processing triggers for ureadahead (0.100.0-20) ...
aia@ubuntu-aia:~$
```

The vsftpd service starts the vsftpd daemon, which runs in the background.

```
$ sudo service vsftpd start
```

The above syntax applies to all other commands so simply replace start with a command you wish to execute.

Once the installation completes, the service will be disabled initially, therefore, we need to start it manually for the mean time and also enable it to start automatically from the next system boot:



```
aia@ubuntu-aia: ~
kB]
Get:12 http://security.ubuntu.com/ubuntu bionic-security/main amd64 Packages [26
8 kB]
Get:13 http://security.ubuntu.com/ubuntu bionic-security/main Translation-en [10
0 kB]
Get:14 http://security.ubuntu.com/ubuntu bionic-security/universe i386 Packages
[120 kB]
Get:15 http://security.ubuntu.com/ubuntu bionic-security/universe amd64 Packages
[123 kB]
Get:16 http://security.ubuntu.com/ubuntu bionic-security/universe Translation-en
[69.1 kB]
Get:17 http://security.ubuntu.com/ubuntu bionic-security/multiverse amd64 Packag
es [3,324 B]
Get:18 http://security.ubuntu.com/ubuntu bionic-security/multiverse i386 Package
s [3,500 B]
Fetched 3,578 kB in 1s (2,892 kB/s)
Reading package lists... Done
aia@ubuntu-aia:~$ systemctl start vsftpd
===== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ===
Authentication is required to start 'vsftpd.service'.
Authenticating as: Aia,,, (aia)
Password:
===== AUTHENTICATION COMPLETE ===
aia@ubuntu-aia:~$
```

If the firewall enables on the server, it needs to open ports 21 and 20 where the FTP daemons are listening, in order to allow access to FTP services from remote machines and then add the new firewall rules

```
$ sudo ufw allow 20/tcp
$ sudo ufw allow 21/tcp
$ sudo ufw status
```

```
aia@ubuntu-aia: ~
Synchronizing state of vsftpd.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable vsftpd
==== AUTHENTICATING FOR org.freedesktop.systemd1.reload-daemon ===
Authentication is required to reload the systemd state.
Authenticating as: Aia,,, (aia)
Password:
==== AUTHENTICATION COMPLETE ===
==== AUTHENTICATING FOR org.freedesktop.systemd1.reload-daemon ===
Authentication is required to reload the systemd state.
Authenticating as: Aia,,, (aia)
Password:
==== AUTHENTICATION COMPLETE ===
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-unit-files ===
Authentication is required to manage system service or unit files.
Authenticating as: Aia,,, (aia)
Password:
[1]+ Stopped                  systemctl enable vsftpd
aia@ubuntu-aia:~$ chkconfig --level 35 vsftpd on
chkconfig: command not found
aia@ubuntu-aia:~$ sudo ufw allow 20/tcp
Rules updated
Rules updated (v6)
aia@ubuntu-aia:~$
```

```
==== AUTHENTICATING FOR org.freedesktop.systemd1.reload-daemon ===
Authentication is required to reload the systemd state.
Authenticating as: Aia,,, (aia)
Password:
==== AUTHENTICATION COMPLETE ===
==== AUTHENTICATING FOR org.freedesktop.systemd1.reload-daemon ===
Authentication is required to reload the systemd state.
Authenticating as: Aia,,, (aia)
Password:
==== AUTHENTICATION COMPLETE ===
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-unit-files ===
Authentication is required to manage system service or unit files.
Authenticating as: Aia,,, (aia)
Password:
[1]+ Stopped                  systemctl enable vsftpd
aia@ubuntu-aia:~$ chkconfig --level 35 vsftpd on
chkconfig: command not found
aia@ubuntu-aia:~$ sudo ufw allow 20/tcp
Rules updated
Rules updated (v6)
aia@ubuntu-aia:~$ sudo ufw allow 21/tcp
Rules updated
Rules updated (v6)
aia@ubuntu-aia:~$
```

```

aia@ubuntu-aia: ~
Authenticating as: Aia,,, (aia)
Password:
==== AUTHENTICATION COMPLETE ====
==== AUTHENTICATING FOR org.freedesktop.systemd1.reload-daemon ===
Authentication is required to reload the systemd state.
Authenticating as: Aia,,, (aia)
Password:
==== AUTHENTICATION COMPLETE ====
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-unit-files ===
Authentication is required to manage system service or unit files.
Authenticating as: Aia,,, (aia)
Password:
[1]+ Stopped                  systemctl enable vsftpd
aia@ubuntu-aia:~$ chkconfig --level 35 vsftpd on
chkconfig: command not found
aia@ubuntu-aia:~$ sudo ufw allow 20/tcp
Rules updated
Rules updated (v6)
aia@ubuntu-aia:~$ sudo ufw allow 21/tcp
Rules updated
Rules updated (v6)
aia@ubuntu-aia:~$ sudo ufw status
Status: inactive
aia@ubuntu-aia:~$ 

```

Configuring and securing VsFTP server :

Now we will perform a few configurations to setup and secure our FTP server, first we will create a backup of the original config file **/etc/vsftpd/vsftpd.conf**

```

aia@ubuntu-aia: ~
GNU nano 2.9.3          New Buffer          Modified ^

anonymous_enable=NO      # disable anonymous login
local_enable=YES         # permit local logins
write_enable=YES          # enable FTP commands which change the filesystem
local_umask=022           # value of umask for file creation for local users
dirmessage_enable=YES    # enable showing of messages when users first enter a directory
xferlog_enable=YES        # a log file will be maintained detailing uploaded files
connect_from_port_20=YES # use port 20 (ftp-data) on the server machine
xferlog_std_format=YES   # keep standard log file format
listen=NO                # prevent vsftpd from running in standalone mode
listen_ipv6=YES          # vsftpd will listen on an IPv6 socket instead of IPv4
pam_service_name=vsftpd  # name of the PAM service vsftpd will use
userlist_enable=YES       # enable vsftpd to load a list of usernames
tcp_wrappers=YES          # turn on tcp wrappers

Save modified buffer? (Answering "No" will DISCARD changes.) [Y] Yes [N] No [^C] Cancel 

```

Configure **VSFTPD** to allow/deny FTP access to users based on the user list file **/etc/vsftpd.userlist**.

```
aia@ubuntu-aia: ~
GNU nano 2.9.3          /etc/vsftpd.userlist      Modified
userlist_enable=YES      # vsftpd will load a list of usernames, f$#
userlist_file=/etc/vsftpd.userlist  # stores usernames.
userlist_deny=NO

File Name to Write: /etc/vsftpd.userlist
^G Get Help      M-D DOS Format      M-A Append      M-B Backup File
^C Cancel        M-M Mac Format      M-P Prepend     ^T To Files
```

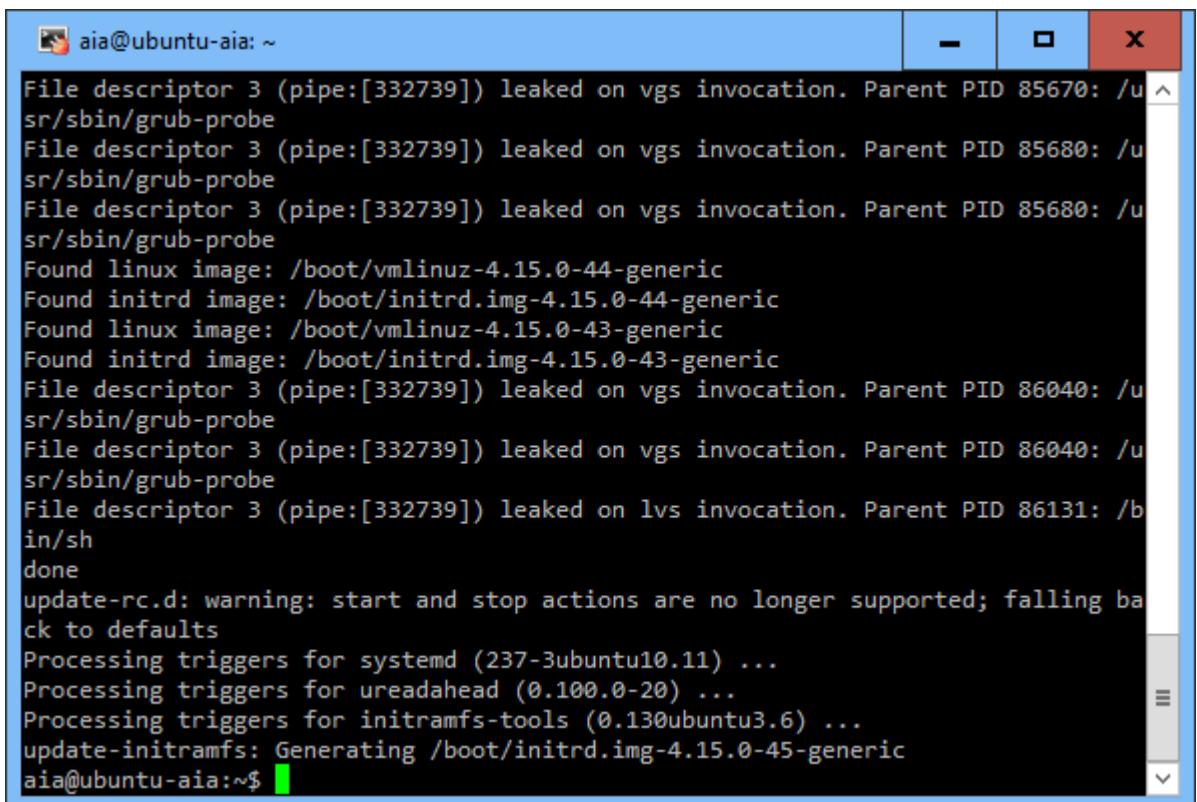
- **Enhancing Linux Security with SELinux:**

Designed by NSA, Security-enhanced Linux (SELinux) is an implementation of a mandatory access control mechanism. This mechanism is in the Linux kernel, checking for allowed operations after standard Linux discretionary access controls are checked.

SELinux is implemented in the Linux kernel using the LSM (Linux Security Modules) framework. The SELinux operates in one of these modes: permissive, disabled or enforcing.

Installing the SELinux package:

```
$ Sudo apt-get install selinux
```



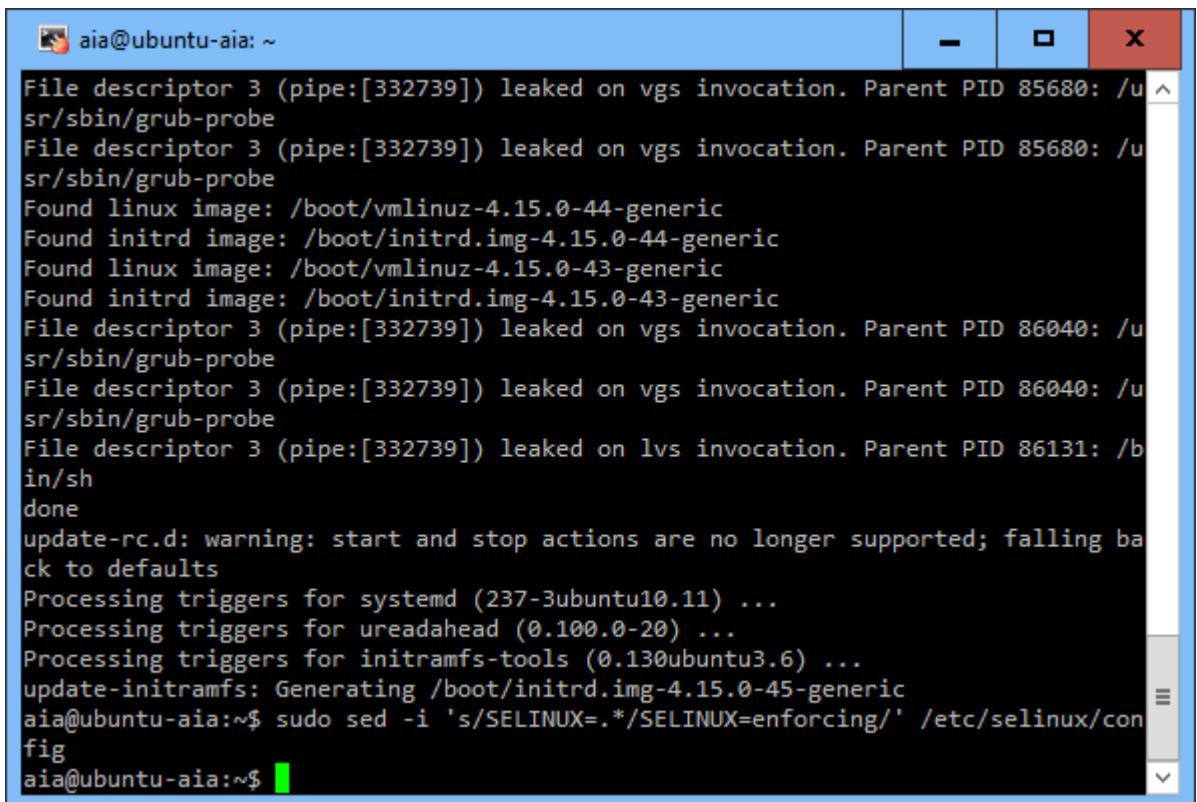
```
aia@ubuntu-aia: ~
File descriptor 3 (pipe:[332739]) leaked on vgs invocation. Parent PID 85670: /u
sr/sbin/grub-probe
File descriptor 3 (pipe:[332739]) leaked on vgs invocation. Parent PID 85680: /u
sr/sbin/grub-probe
File descriptor 3 (pipe:[332739]) leaked on vgs invocation. Parent PID 85680: /u
sr/sbin/grub-probe
Found linux image: /boot/vmlinuz-4.15.0-44-generic
Found initrd image: /boot/initrd.img-4.15.0-44-generic
Found linux image: /boot/vmlinuz-4.15.0-43-generic
Found initrd image: /boot/initrd.img-4.15.0-43-generic
File descriptor 3 (pipe:[332739]) leaked on vgs invocation. Parent PID 86040: /u
sr/sbin/grub-probe
File descriptor 3 (pipe:[332739]) leaked on vgs invocation. Parent PID 86040: /u
sr/sbin/grub-probe
File descriptor 3 (pipe:[332739]) leaked on lvs invocation. Parent PID 86131: /b
in/sh
done
update-rc.d: warning: start and stop actions are no longer supported; falling ba
ck to defaults
Processing triggers for systemd (237-3ubuntu10.11) ...
Processing triggers for ureadahead (0.100.0-20) ...
Processing triggers for initramfs-tools (0.130ubuntu3.6) ...
update-initramfs: Generating /boot/initrd.img-4.15.0-45-generic
aia@ubuntu-aia:~$
```

Change the SELinux mode in /etc/selinux/config:

1. Enforcing:

It turn on and all the security policy rules and enforced.

```
# sudo sed -i 's/SELINUX=.*/SELINUX=enforcing/' /etc/selinux/config
```

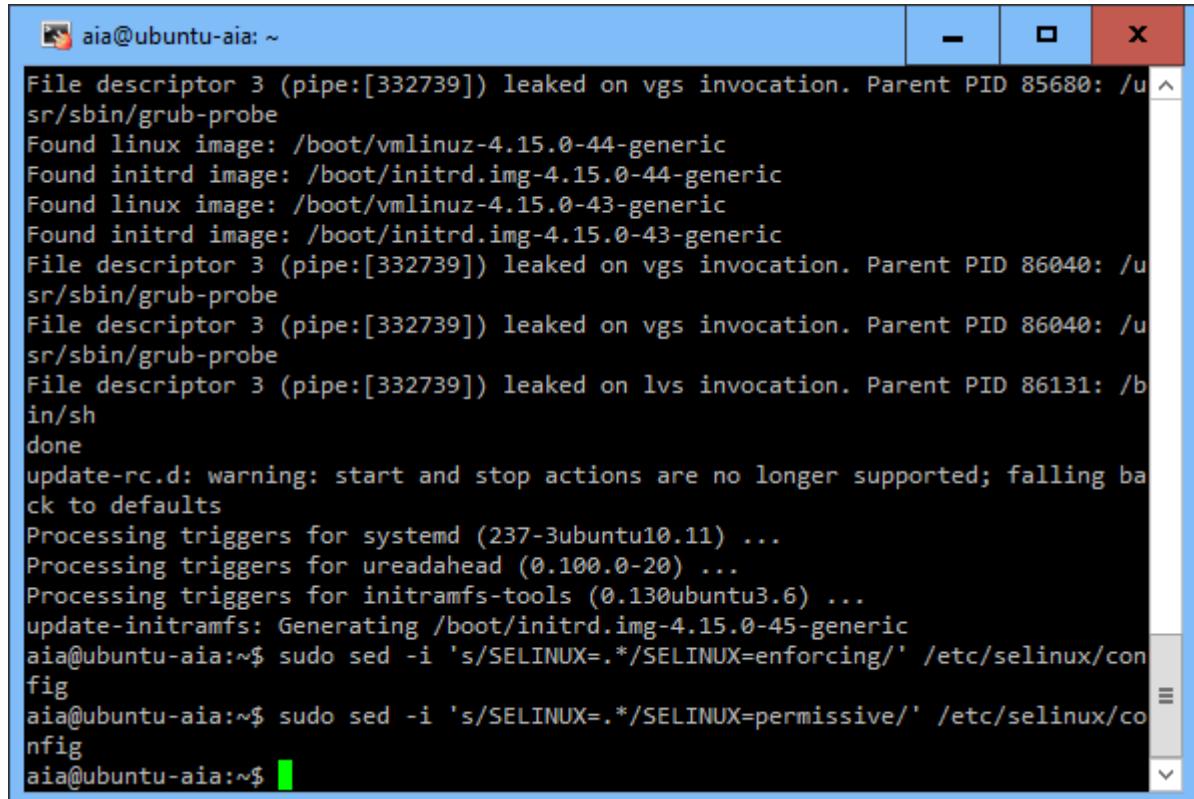


```
aia@ubuntu-aia: ~
File descriptor 3 (pipe:[332739]) leaked on vgs invocation. Parent PID 85680: /u
sr/sbin/grub-probe
File descriptor 3 (pipe:[332739]) leaked on vgs invocation. Parent PID 85680: /u
sr/sbin/grub-probe
Found linux image: /boot/vmlinuz-4.15.0-44-generic
Found initrd image: /boot/initrd.img-4.15.0-44-generic
Found linux image: /boot/vmlinuz-4.15.0-43-generic
Found initrd image: /boot/initrd.img-4.15.0-43-generic
File descriptor 3 (pipe:[332739]) leaked on vgs invocation. Parent PID 86040: /u
sr/sbin/grub-probe
File descriptor 3 (pipe:[332739]) leaked on vgs invocation. Parent PID 86040: /u
sr/sbin/grub-probe
File descriptor 3 (pipe:[332739]) leaked on lvs invocation. Parent PID 86131: /b
in/sh
done
update-rc.d: warning: start and stop actions are no longer supported; falling ba
ck to defaults
Processing triggers for systemd (237-3ubuntu10.11) ...
Processing triggers for ureadahead (0.100.0-20) ...
Processing triggers for initramfs-tools (0.130ubuntu3.6) ...
update-initramfs: Generating /boot/initrd.img-4.15.0-45-generic
aia@ubuntu-aia:~$ sudo sed -i 's/SELINUX=.*/SELINUX=enforcing/' /etc/selinux/con
fig
aia@ubuntu-aia:~$
```

1. Permissive:

It's used for auditing the current SELinux policy rules, testing new applications to see what effect SELinux policy rules will have on them, testing new SELinux policy rules to see what effect the new rules will have on current services and applications , and troubleshooting why a particular service or application is no longer working properly under SELinux.

```
# sudo sed -i 's/SELINUX=.*/SELINUX=permissive/' /etc/selinux/config
```



The screenshot shows a terminal window titled 'aia@ubuntu-aia: ~'. The window contains several lines of text output from SELinux audit logs and command-line operations. The logs mention file descriptor leaks for 'vgs' and 'lvs' invocations, and various triggers being processed. At the bottom, two commands are shown: 'sudo sed -i 's/SELINUX=.*\$/SELINUX=enforcing/' /etc/selinux/config' followed by 'sudo sed -i 's/SELINUX=.*\$/SELINUX=permissive/' /etc/selinux/config'. The terminal window has a standard Linux-style interface with a title bar, window controls (minimize, maximize, close), and scroll bars.

```
File descriptor 3 (pipe:[332739]) leaked on vgs invocation. Parent PID 85680: /u
sr/sbin/grub-probe
Found linux image: /boot/vmlinuz-4.15.0-44-generic
Found initrd image: /boot/initrd.img-4.15.0-44-generic
Found linux image: /boot/vmlinuz-4.15.0-43-generic
Found initrd image: /boot/initrd.img-4.15.0-43-generic
File descriptor 3 (pipe:[332739]) leaked on vgs invocation. Parent PID 86040: /u
sr/sbin/grub-probe
File descriptor 3 (pipe:[332739]) leaked on vgs invocation. Parent PID 86040: /u
sr/sbin/grub-probe
File descriptor 3 (pipe:[332739]) leaked on lvs invocation. Parent PID 86131: /b
in/sh
done
update-rc.d: warning: start and stop actions are no longer supported; falling ba
ck to defaults
Processing triggers for systemd (237-3ubuntu10.11) ...
Processing triggers for ureadahead (0.100.0-20) ...
Processing triggers for initramfs-tools (0.130ubuntu3.6) ...
update-initramfs: Generating /boot/initrd.img-4.15.0-45-generic
aia@ubuntu-aia:~$ sudo sed -i 's/SELINUX=.*$/SELINUX=enforcing/' /etc/selinux/con
fig
aia@ubuntu-aia:~$ sudo sed -i 's/SELINUX=.*$/SELINUX=permissive/' /etc/selinux/co
nfig
aia@ubuntu-aia:~$
```

4. CONCLUSION

The aim of this project is to have a smart remote serve that can be connecting the administrators out of the private network with high security and authentication.

REFERENCES

Acer EPBU, July 2012. Smart Server Manager v1.2, Best Practices Guide at: <http://content.etylize.com/User-Manual/1023217498.pdf>

Smart Technologies. System administrator guide – 171333 at: <https://support.smarttech.com/docs/software/remote-management/en/documents/default.cshtml> [Accessed by January 8, 2019]

IONOS Product, Digital guide, August 2018. Virtual Machines, at: <https://www.ionos.com/digitalguide/server/know-how/virtual-machines/>

VMware, Inc. 2019, Virtual Machine Guide, VMware 1.0 at: https://www.vmware.com/pdf/server_vm_manual.pdf.

John McCabe with the Windows Server team, June, 2016. Introducing Windows Server 2016 at: <https://mva.microsoft.com/ebooks> [Accessed by 15.01.2019]

Erin Chapple, Director of Program Management, Windows Server. March 20, 2018. Introducing Windows Server 2019, at: <https://cloudblogs.microsoft.com/windowsserver/2018/03/20/introducing-windows-server-2019-now-available-in-preview/> [Accessed by 15.01.2019]

Ubuntu Server Guide 18.04, at: <https://help.ubuntu.com/lts/serverguide/index.html.en>

Smart IT configuration at: <https://docs.bmc.com/docs/itsm81/configuring-smart-it-after-installation-478790597.html>

Virtual Machine Guide, VMware Server 1.0 at: https://www.vmware.com/pdf/server_vm_manual.pdf

TeamViewer Software Features:
<https://www.teamviewer.com/en-us/features/vpn-alternative/>

Windows_Server_2019_Feature_Comparison_Guide_EN_US.pdf, at: www.download.microsoft.com

Mark Minasi, K. Greene, Ch. Booth, R. Butler, J. McCabe, R. Panek, M. Rice, S. Roth, 2012. Mastering Windows Server 2012 R2.

Paul Cobbaut, May 24, 2015. Linux Server. Pdf, at: <http://linux-training.be/linuxsrv.pdf> [Accessed by 05.02.2019]

Christopher Negus, 2012. Linux Bible, at: <https://kaakkuri.finna.fi/Record/kaakkuri.180086> [Accessed by 08.02.2019]

