



SECURITY+ V4 LAB SERIES

Lab 11: Configuring a RADIUS Server

Document Version: **2023-02-27**

Material in this Lab Aligns to the Following	
CompTIA Security+ (SY0-601) Exam Objectives	3.8: Given a scenario, implement authentication and authorization solutions
All-In-One CompTIA Security+ Sixth Edition ISBN-13: 978-1260464009 Chapters	24: Implement Authentication and Authorization

Copyright © 2023 Network Development Group, Inc.
www.netdevgroup.com

NETLAB+ is a registered trademark of Network Development Group, Inc.
KALI LINUX™ is a trademark of Offensive Security.
Microsoft®, Windows®, and Windows Server® are trademarks of the Microsoft group of companies.
VMware is a registered trademark of VMware, Inc.
SECURITY ONION is a trademark of Security Onion Solutions LLC.
Android is a trademark of Google LLC.
pfSense® is a registered mark owned by Electric Sheep Fencing LLC ("ESF").
All trademarks are property of their respective owners.

Contents

Introduction	3
Objective	3
Lab Topology	4
Lab Settings	5
1 Configure RADIUS on Windows	6
1.1 Add the Network Policy Role	6
1.2 Configure the Network Policy Server	11
2 FreeRADIUS on Ubuntu.....	20

Introduction

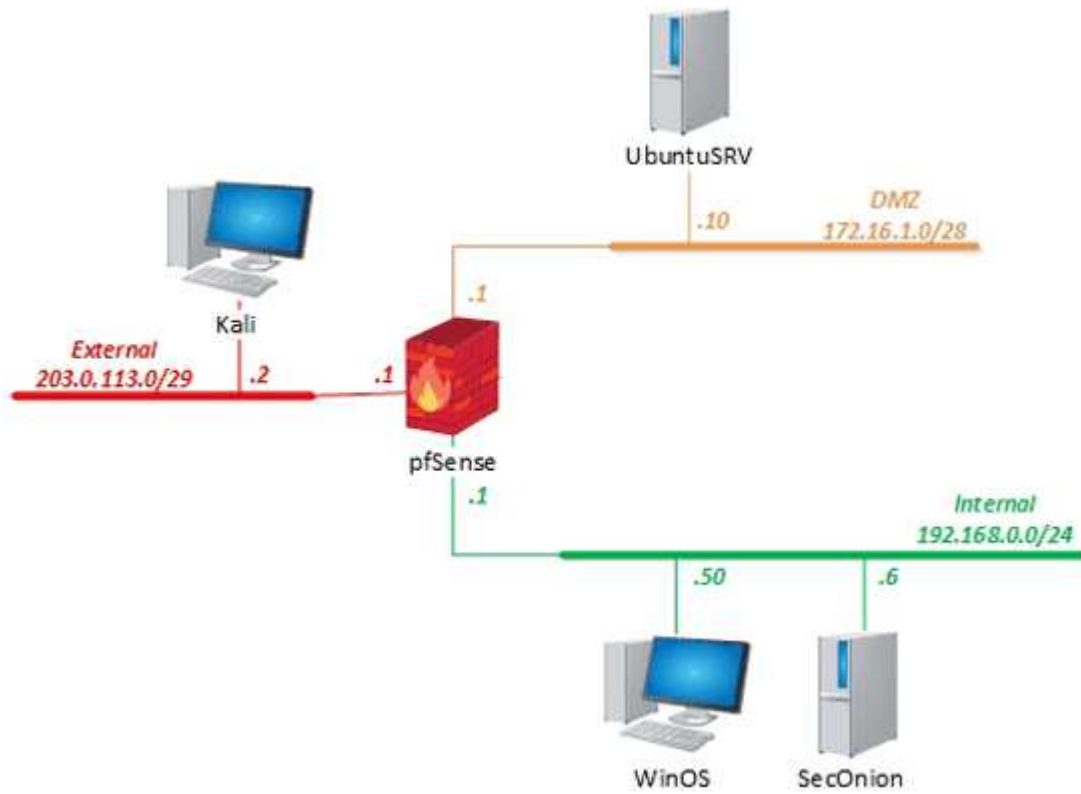
In this lab, you will install, configure, and deploy a RADIUS server within the Windows and Linux operating systems.

Objective

In this lab, you will perform the following tasks:

- Set up and configure RADIUS on Windows
- Set up and configure RADIUS on Linux

Lab Topology



Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

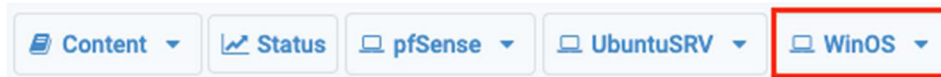
Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Kali	203.0.113.2	kali	kali
pfSense	192.168.0.1	sysadmin	NDGlabpass123!
SecOnion	192.168.0.6	sysadmin	NDGlabpass123!
UbuntuSRV	172.16.1.10	sysadmin	NDGlabpass123!
WinOS	192.168.0.50	Administrator	NDGlabpass123!

1 Configure RADIUS on Windows

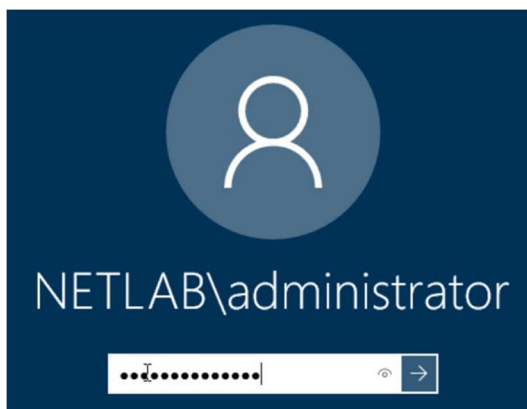
1.1 Add the Network Policy Role

In this task, you will add the role of *Network Policy Server* to the *WinOS* server. You will then add the *Network Policy and Access Services Tools*.

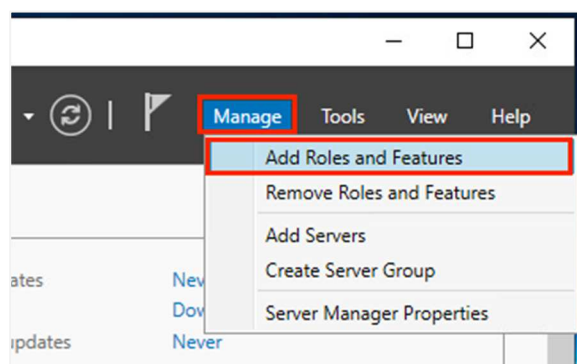
1. Launch the **WinOS** virtual machine to access the graphical login screen.



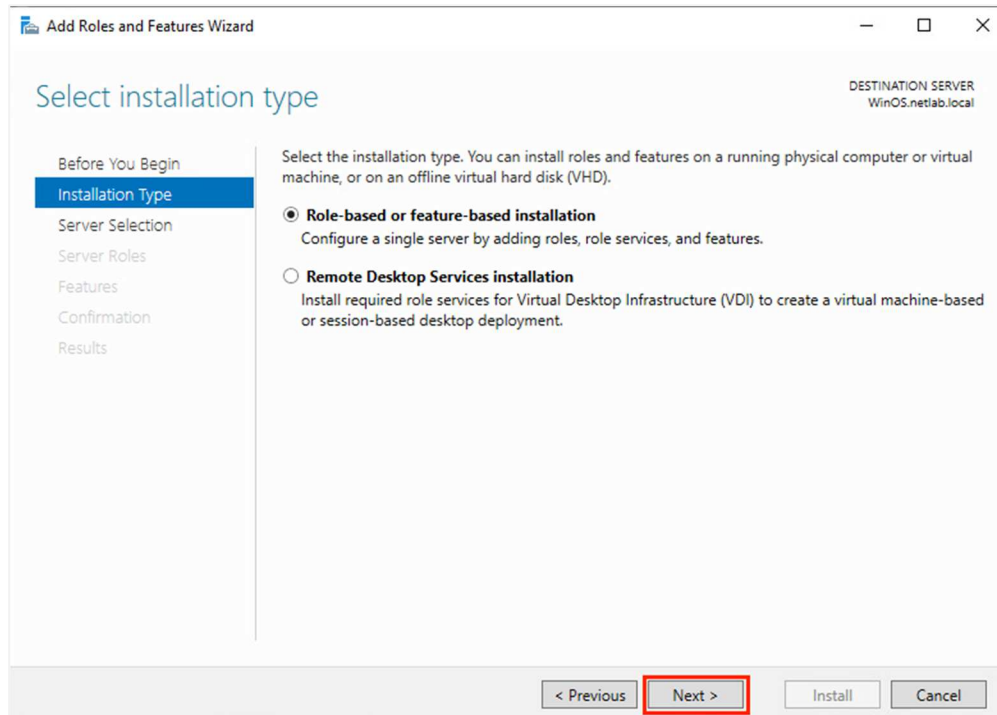
2. While on the splash screen, focus on the *NETLAB+* tabs. Click the dropdown menu for the **WinOS** tab and click on **Send CTRL+ALT+DEL**.
3. Log in as **Administrator** using the password **NDGlabpass123!**.



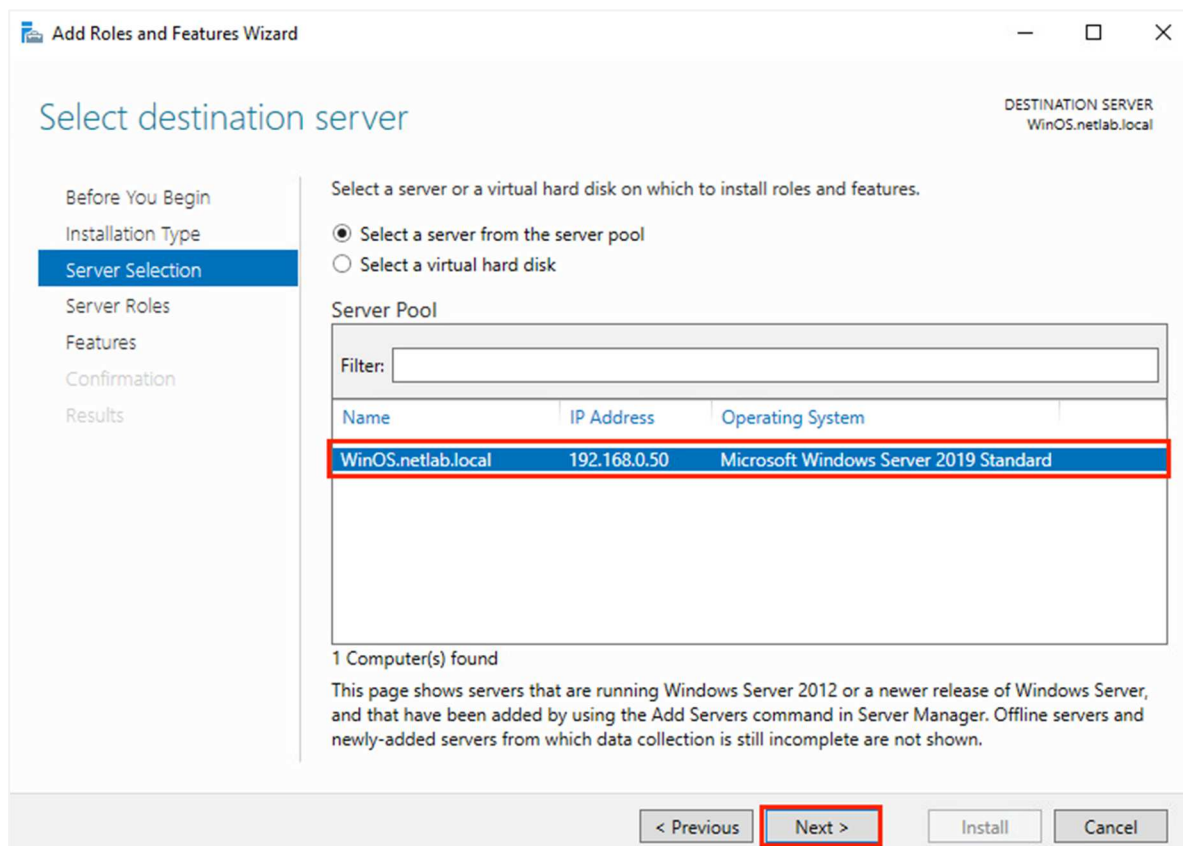
4. Once logged in, click the **Server Manager** icon to launch it. In the *Server Manager* window, click on **Manage** in the top-right corner and select **Add Roles and Features**.



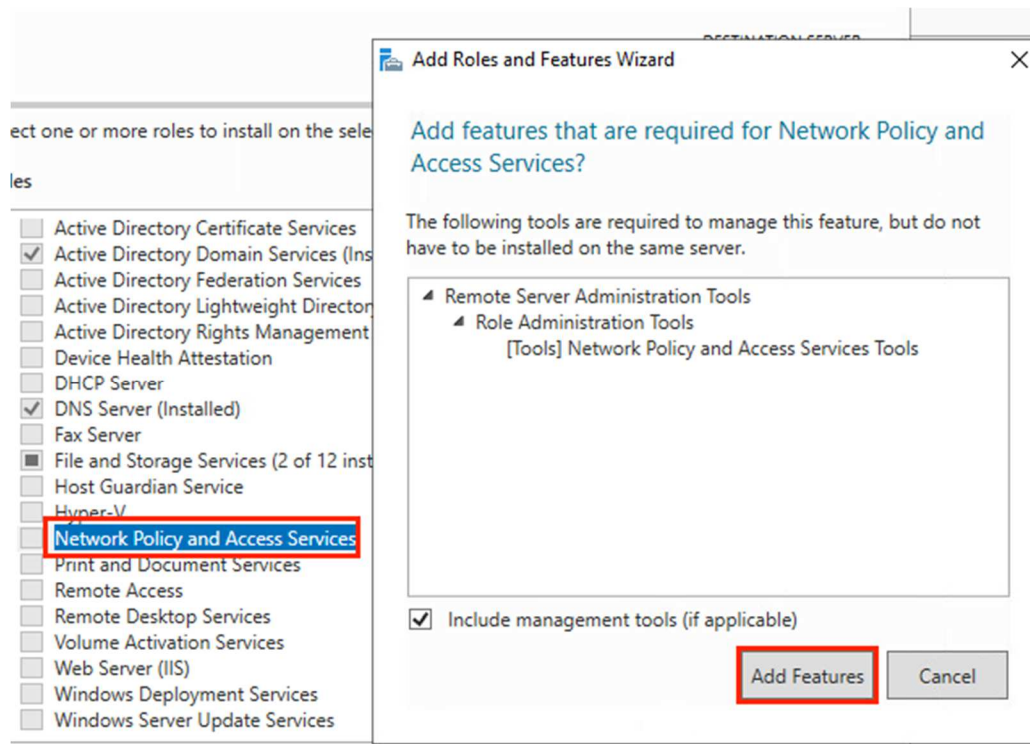
5. Notice the *Add Roles and Features Wizard* appears. On the *Installation Type* step, keep the default setting of **Role-based or feature-based Installation** and click **Next**.



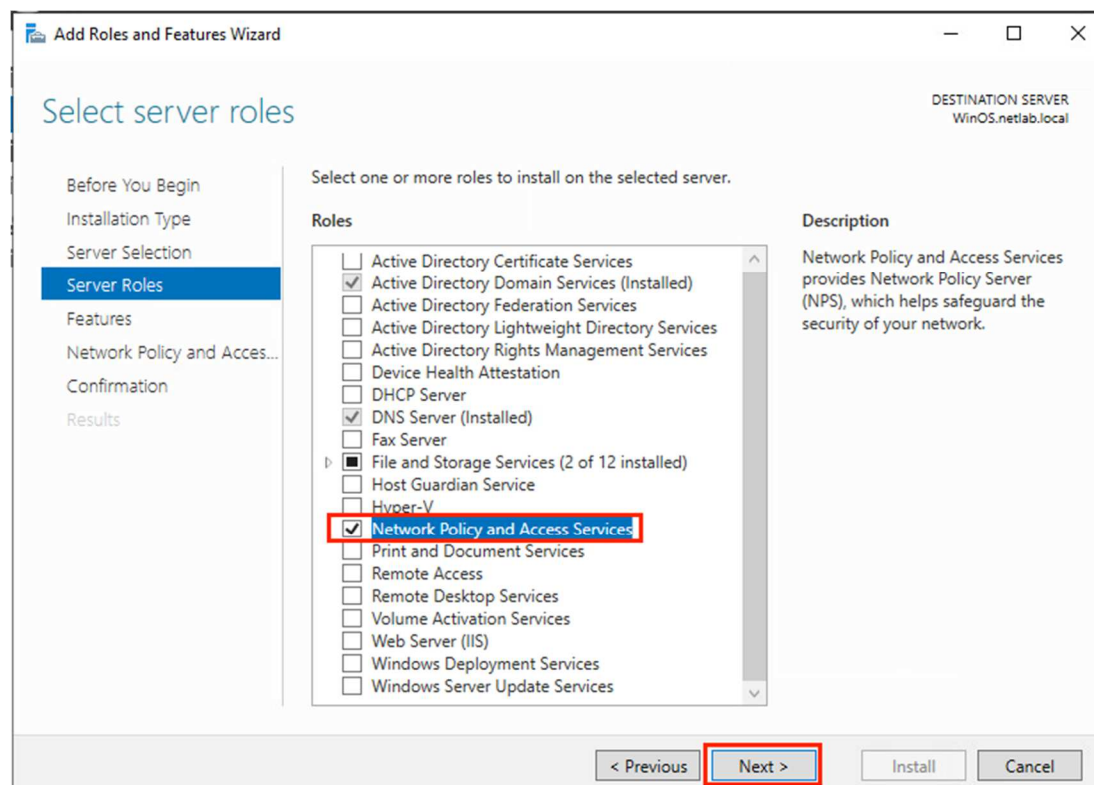
6. On the *Server Selection* step, select the **WinOS.netlab.local** server from the pool and click **Next**.



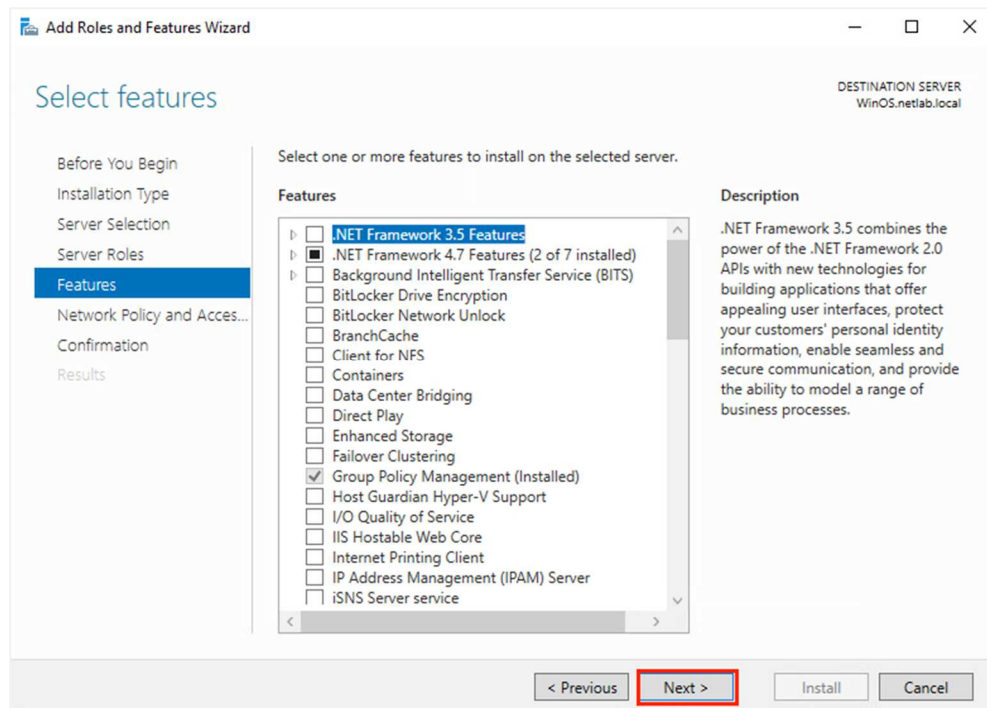
7. On the *Server Roles* step, check the checkbox for **Network Policy and Access Services** and notice a pop-up window appears. Click the **Add Features** button.



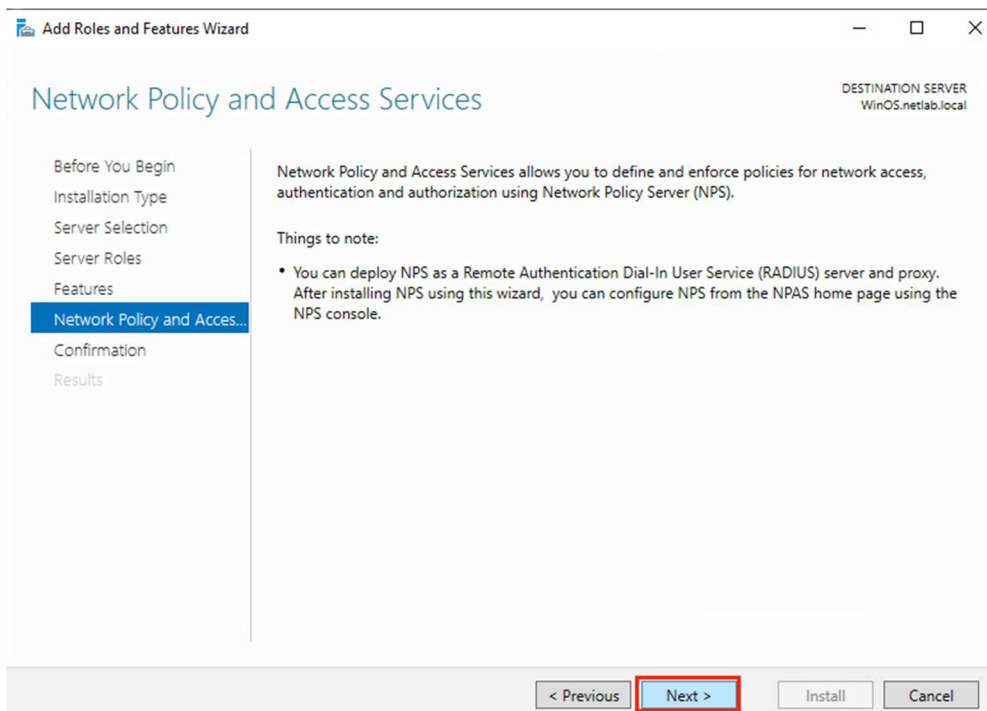
8. Back on the main wizard window, ensure that **Network Policy and Access Services** is checked, and click **Next**.



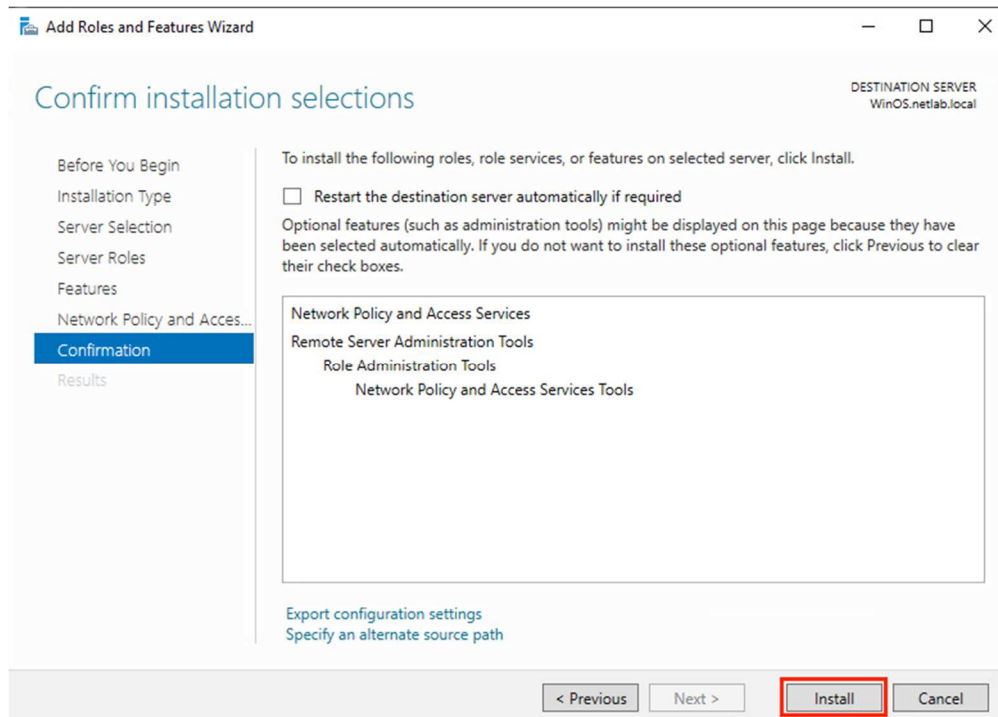
9. On the *Features* step, leave the defaults and click **Next**.



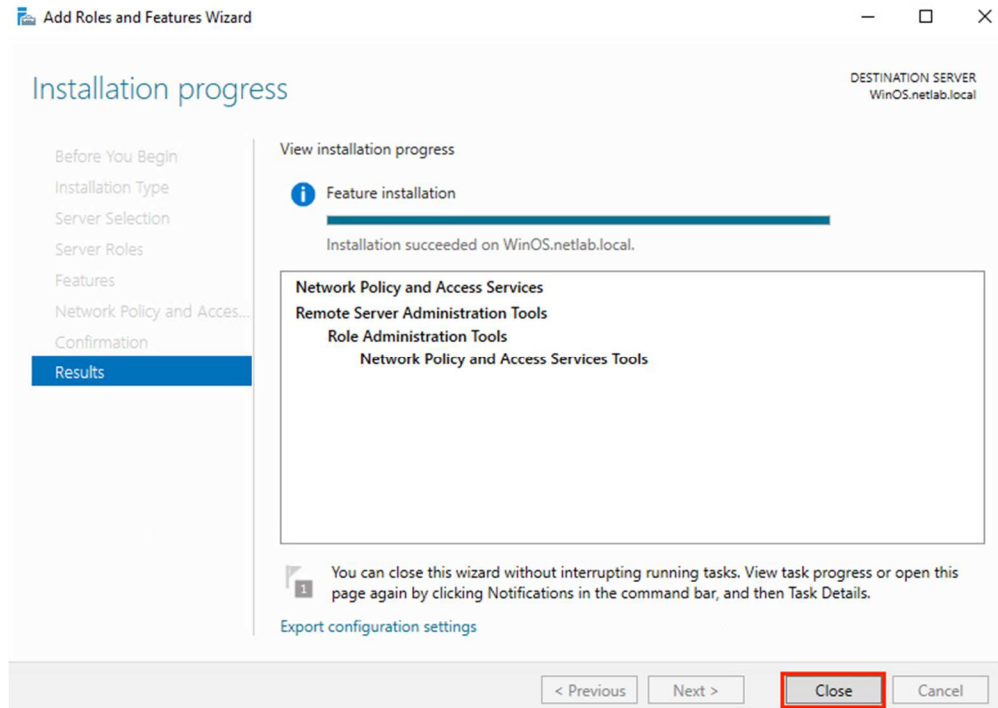
10. On the *Network Policy and Access Services* step, review the information and click **Next**.



11. On the *Confirmation* step, click **Install** to finish the installation of the *Network Policy Server*.

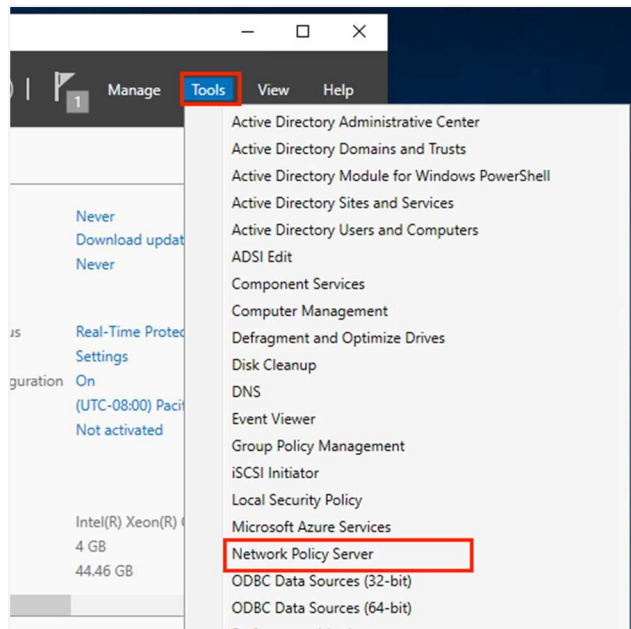


12. The installation will take about 3 minutes. After the install is complete, click **Close**.

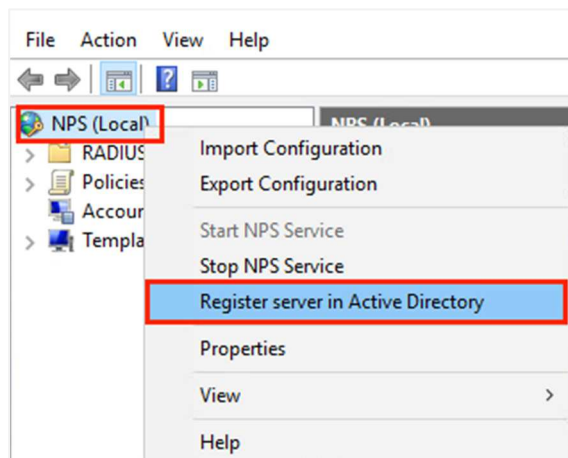


1.2 Configure the Network Policy Server

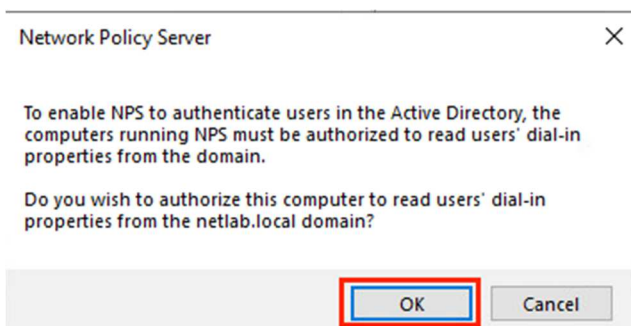
1. Back on the *Server Manager* window, navigate to **Tools > Network Policy Server**.



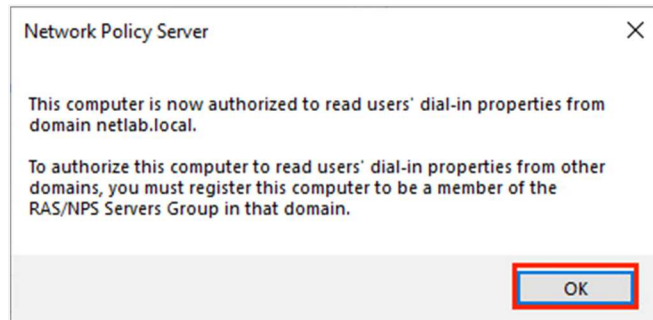
2. In the *Network Policy Server* window, in the left pane, right-click on **NPS (Local)** and select **Register Server in Active Directory**.



3. When prompted to authorize, click **OK** to continue.



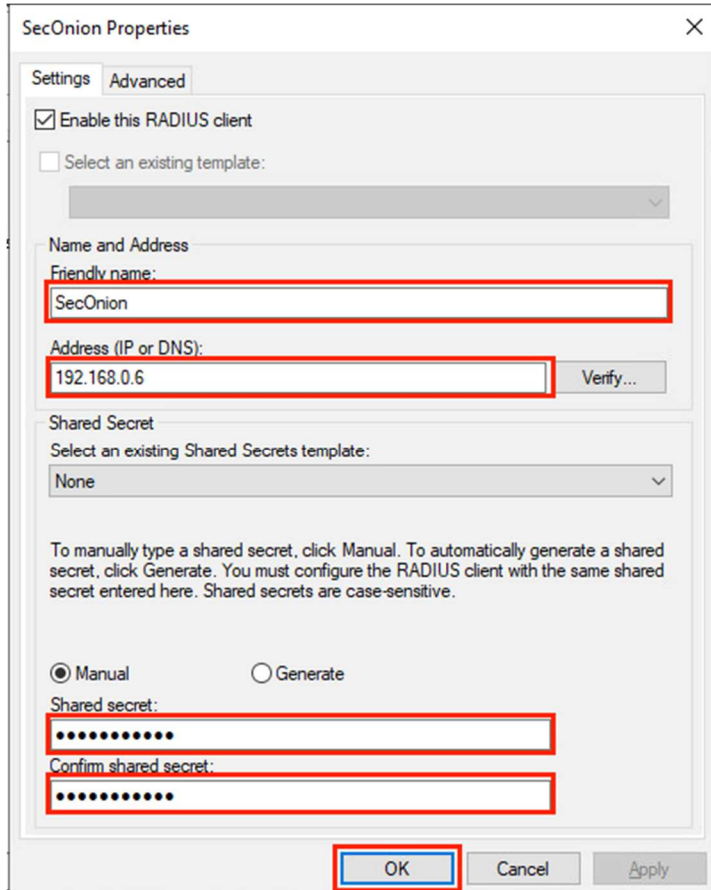
- Click **OK** again to confirm that the system is now authorized.



- Expand the **RADIUS Clients and Servers** inventory object, right-click on **RADIUS Clients** and click **New**.



6. In the *New RADIUS Client* window, fill in the following information:
 - a. *Friendly name*: SecOnion
 - b. *Address*: 192.168.0.6
 - c. *Shared secret*: password123
 - d. *Confirm shared secret*: password123



SecOnion Properties

Settings Advanced

☒ Enable this RADIUS client

☐ Select an existing template:

Name and Address

Friendly name:
SecOnion

Address (IP or DNS):
192.168.0.6 Verify...

Shared Secret

Select an existing Shared Secrets template:
None

To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

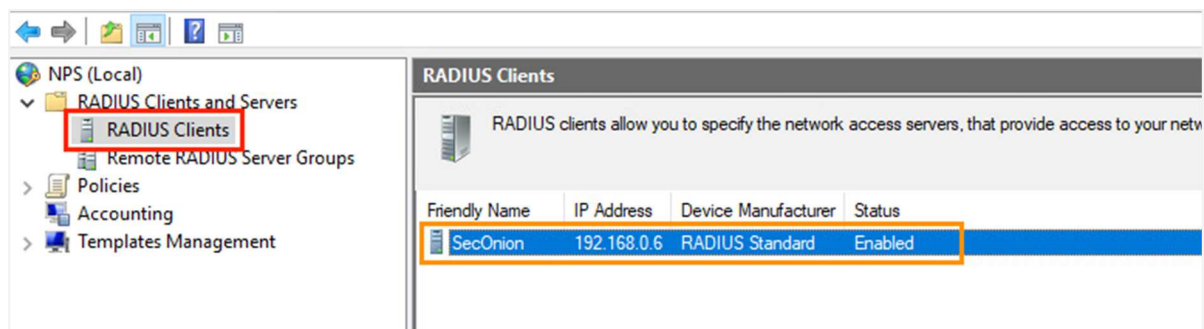
☒ Manual ☐ Generate

Shared secret:
password123

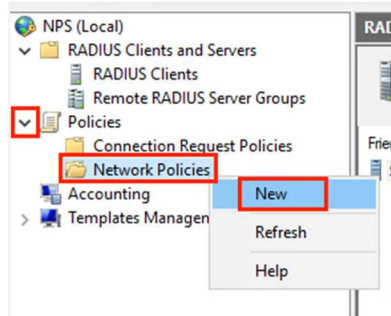
Confirm shared secret:
password123

OK Cancel Apply

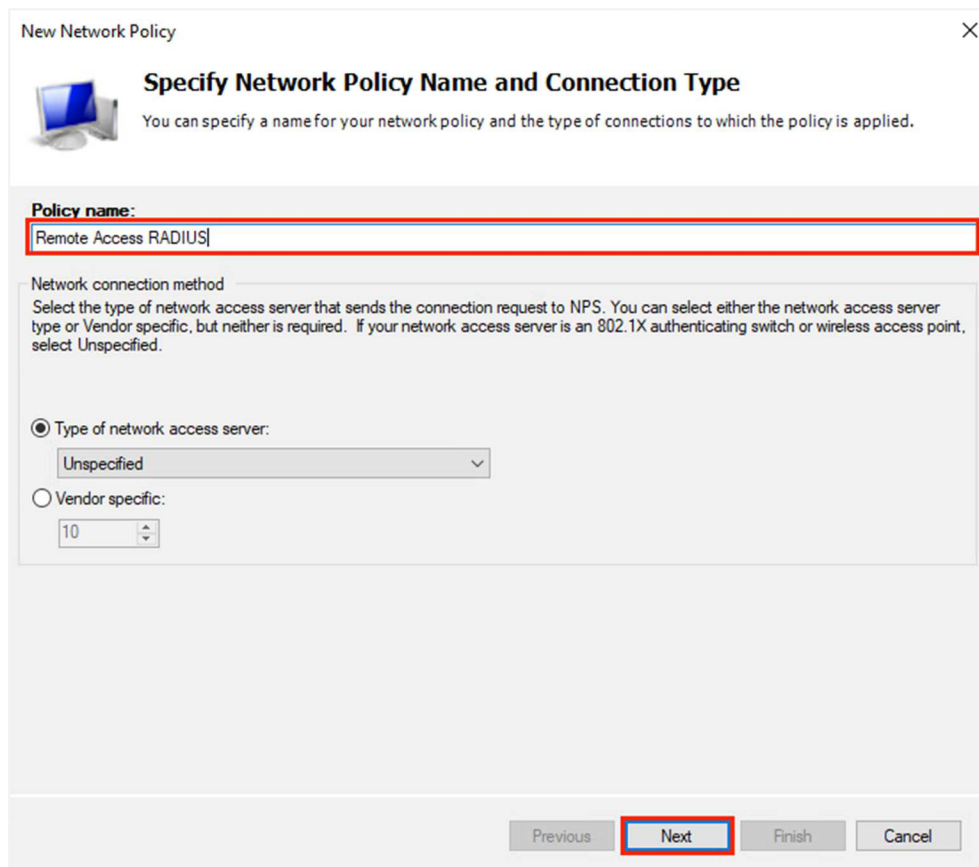
7. Once the configurations are made, click **OK**.
8. Select **RADIUS Clients** from the left pane and verify that the *SecOnion Client* appears in the right pane and that it is enabled.



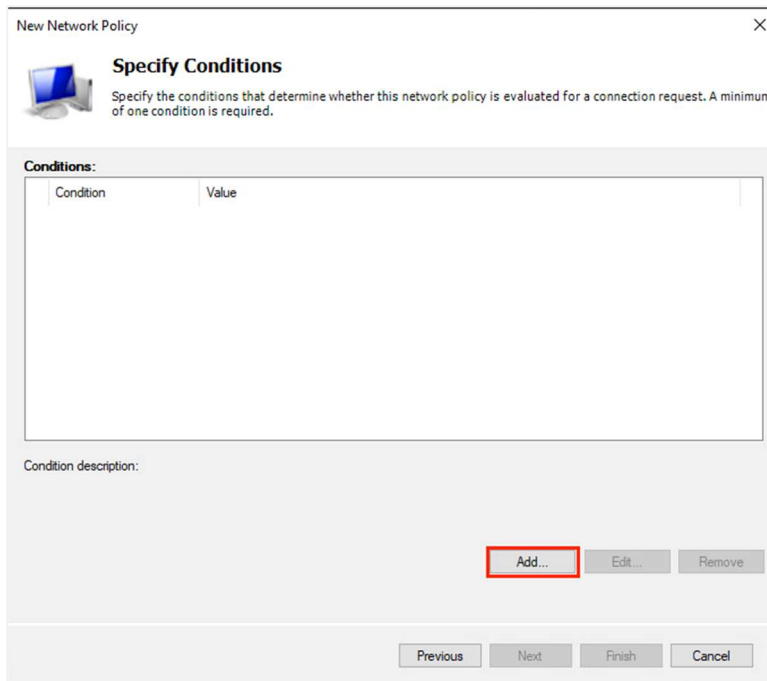
9. Now it is time to create a new network policy. In the left pane, expand **Policies**, right-click on **Network Policies** and select **New**.



10. In the *New Network Policy* window, type **Remote Access RADIUS** in the *Policy name* text field and click **Next**.

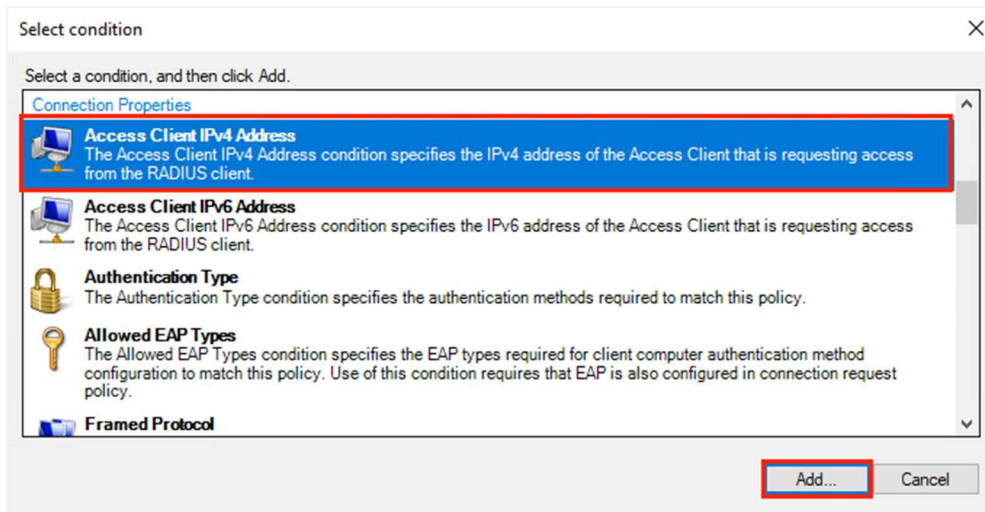
A screenshot of the 'New Network Policy' wizard window. The title bar says 'New Network Policy'. The main heading is 'Specify Network Policy Name and Connection Type'. Below this is a sub-heading: 'You can specify a name for your network policy and the type of connections to which the policy is applied.' The 'Policy name:' text box contains the text 'Remote Access RADIUS'. Below this is the 'Network connection method' section, which includes a description: 'Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.' There are two radio buttons: 'Type of network access server:' (selected) and 'Vendor specific:'. The 'Type of network access server:' dropdown menu is set to 'Unspecified'. The 'Vendor specific:' dropdown menu is set to '10'. At the bottom of the window, there are four buttons: 'Previous', 'Next', 'Finish', and 'Cancel'. The 'Next' button is highlighted with a red border.

11. On the *Specify Conditions* step, click the **Add** button.



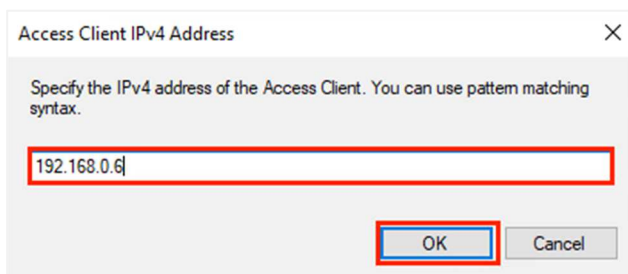
The dialog box titled "New Network Policy" has a tab labeled "Specify Conditions". Below the tab is a description: "Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required." Below this is a table with two columns: "Condition" and "Value". The table is currently empty. At the bottom right of the table area are three buttons: "Add...", "Edit...", and "Remove". The "Add..." button is highlighted with a red rectangle. At the very bottom of the dialog are four buttons: "Previous", "Next", "Finish", and "Cancel".

12. In the *Select condition* window, scroll down and select **Access Client IPv4 Address** and click **Add**.



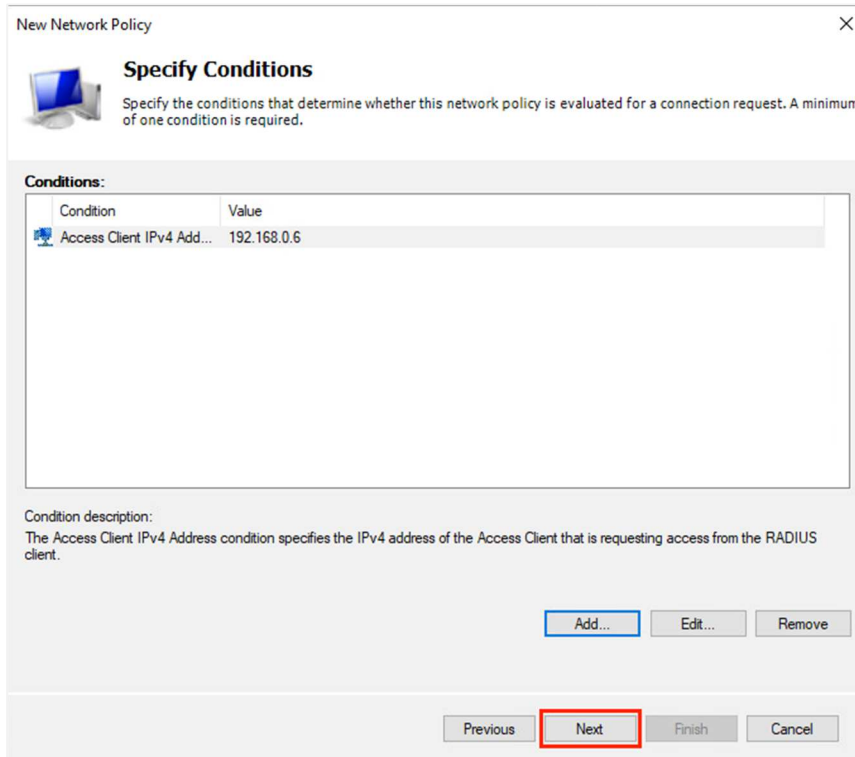
The dialog box titled "Select condition" has a tab labeled "Connection Properties". Below the tab is a list of conditions. The first condition, "Access Client IPv4 Address", is highlighted with a blue background and a red border. The description for this condition is: "The Access Client IPv4 Address condition specifies the IPv4 address of the Access Client that is requesting access from the RADIUS client." Below this are other conditions: "Access Client IPv6 Address", "Authentication Type", "Allowed EAP Types", and "Framed Protocol". At the bottom right of the dialog are two buttons: "Add..." and "Cancel". The "Add..." button is highlighted with a red rectangle.

13. When prompted for an *IPv4* address, type **192.168.0.6** and click **OK**.



The dialog box titled "Access Client IPv4 Address" has a description: "Specify the IPv4 address of the Access Client. You can use pattern matching syntax." Below this is a text input field containing the value "192.168.0.6". The input field is highlighted with a red rectangle. At the bottom right of the dialog are two buttons: "OK" and "Cancel". The "OK" button is highlighted with a red rectangle.

14. Back on the *Specify Conditions* step, ensure that the new condition is listed and click **Next**.

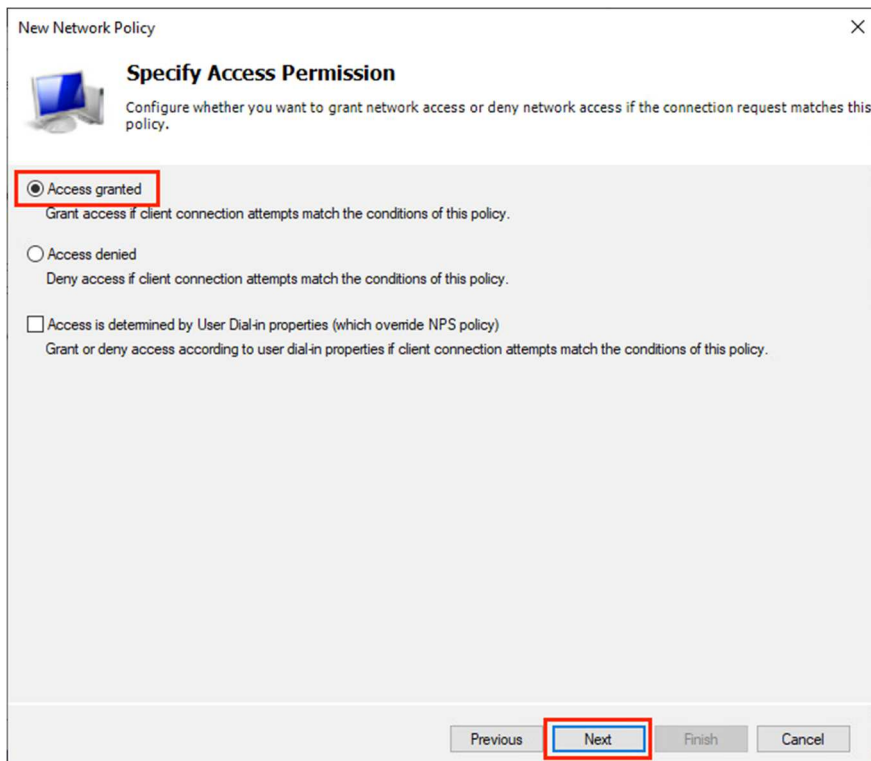


The dialog box is titled "New Network Policy" and "Specify Conditions". It contains a table with the following data:

Condition	Value
Access Client IPv4 Add...	192.168.0.6

Below the table is a "Condition description:" section with the text: "The Access Client IPv4 Address condition specifies the IPv4 address of the Access Client that is requesting access from the RADIUS client." At the bottom right are buttons for "Add...", "Edit...", and "Remove". At the very bottom are navigation buttons: "Previous", "Next" (highlighted with a red box), "Finish", and "Cancel".

15. On the *Specify Access Permission* step, leave **Access granted** selected and click **Next**.

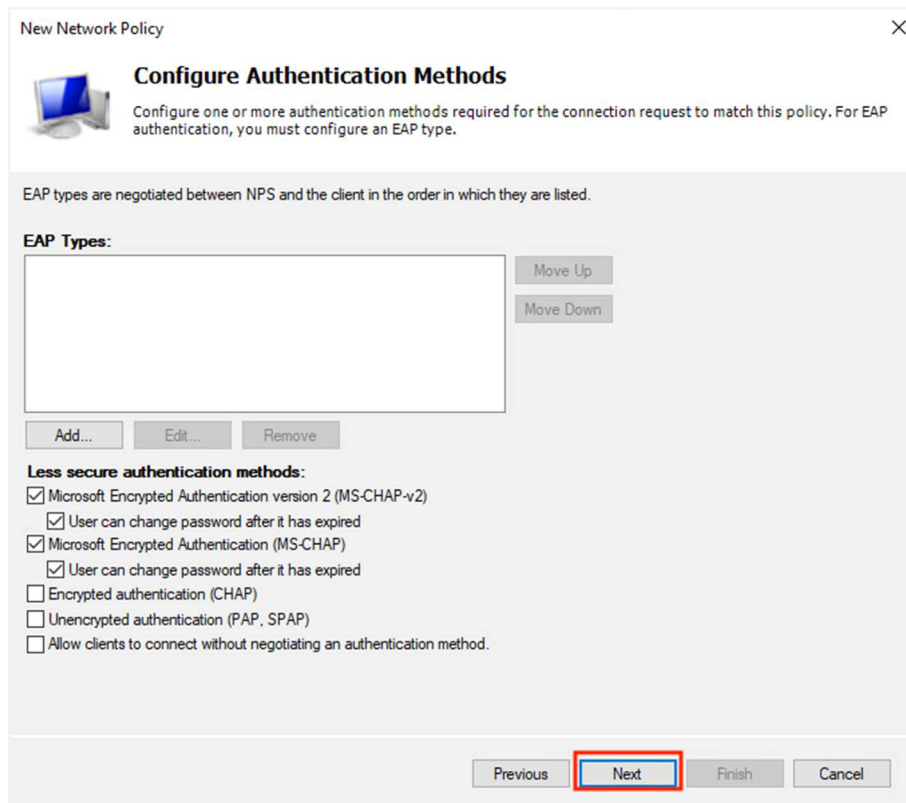


The dialog box is titled "New Network Policy" and "Specify Access Permission". It contains three radio button options:

- ☒ **Access granted** (highlighted with a red box). Grant access if client connection attempts match the conditions of this policy.
- ☐ Access denied. Deny access if client connection attempts match the conditions of this policy.
- ☐ Access is determined by User Dial-in properties (which override NPS policy). Grant or deny access according to user dial-in properties if client connection attempts match the conditions of this policy.

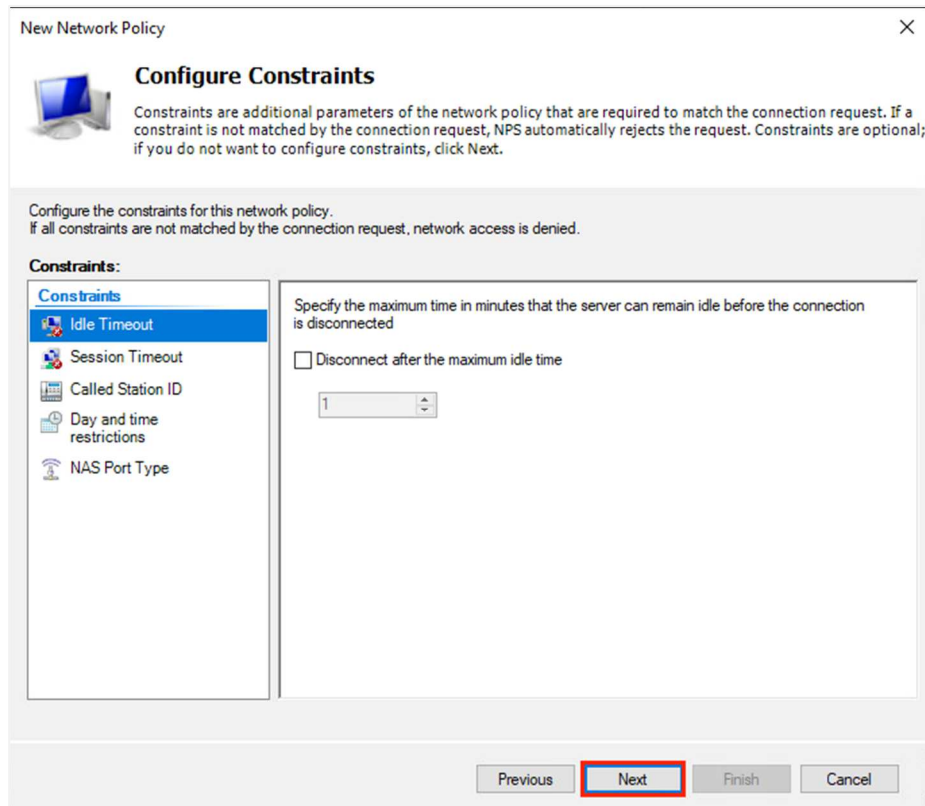
At the bottom are navigation buttons: "Previous", "Next" (highlighted with a red box), "Finish", and "Cancel".

16. On the *Configure Authentication Methods* step, leave the default settings and click **Next**.



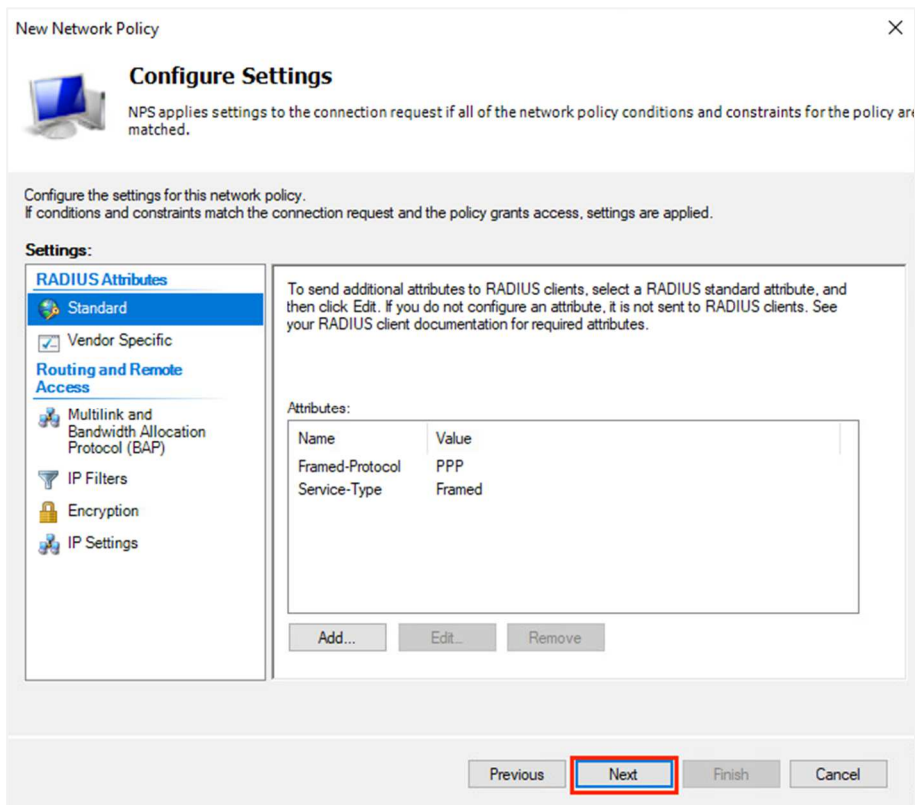
The screenshot shows the 'Configure Authentication Methods' step of the 'New Network Policy' wizard. The title bar says 'New Network Policy' with a close button. Below the title is a computer icon and the heading 'Configure Authentication Methods'. A descriptive text says: 'Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type.' Below this, it states: 'EAP types are negotiated between NPS and the client in the order in which they are listed.' There is a section labeled 'EAP Types:' with an empty list box and 'Move Up' and 'Move Down' buttons. Below the list box are 'Add...', 'Edit...', and 'Remove' buttons. A section titled 'Less secure authentication methods:' contains several checkboxes: 'Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)' (checked), 'User can change password after it has expired' (checked), 'Microsoft Encrypted Authentication (MS-CHAP)' (checked), 'User can change password after it has expired' (checked), 'Encrypted authentication (CHAP)' (unchecked), 'Unencrypted authentication (PAP, SPAP)' (unchecked), and 'Allow clients to connect without negotiating an authentication method.' (unchecked). At the bottom are 'Previous', 'Next' (highlighted with a red box), 'Finish', and 'Cancel' buttons.

17. On the *Configure Constraints* step, leave the default settings and click **Next**.



The screenshot shows the 'Configure Constraints' step of the 'New Network Policy' wizard. The title bar says 'New Network Policy' with a close button. Below the title is a computer icon and the heading 'Configure Constraints'. A descriptive text says: 'Constraints are additional parameters of the network policy that are required to match the connection request. If a constraint is not matched by the connection request, NPS automatically rejects the request. Constraints are optional; if you do not want to configure constraints, click Next.' Below this, it states: 'Configure the constraints for this network policy. If all constraints are not matched by the connection request, network access is denied.' There is a section labeled 'Constraints:' with a list of constraints: 'Idle Timeout' (selected), 'Session Timeout', 'Called Station ID', 'Day and time restrictions', and 'NAS Port Type'. To the right of the list, there is a text box with the label 'Specify the maximum time in minutes that the server can remain idle before the connection is disconnected'. Below this text box is a checkbox labeled 'Disconnect after the maximum idle time' which is unchecked. Below the checkbox is a spin box with the value '1'. At the bottom are 'Previous', 'Next' (highlighted with a red box), 'Finish', and 'Cancel' buttons.

18. On the *Configure Settings* step, leave the defaults and click **Next**.



New Network Policy

Configure Settings

NPS applies settings to the connection request if all of the network policy conditions and constraints for the policy are matched.

Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

RADIUS Attributes

Standard

☒ Vendor Specific

Routing and Remote Access

Multilink and Bandwidth Allocation Protocol (BAP)

IP Filters

Encryption

IP Settings

To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

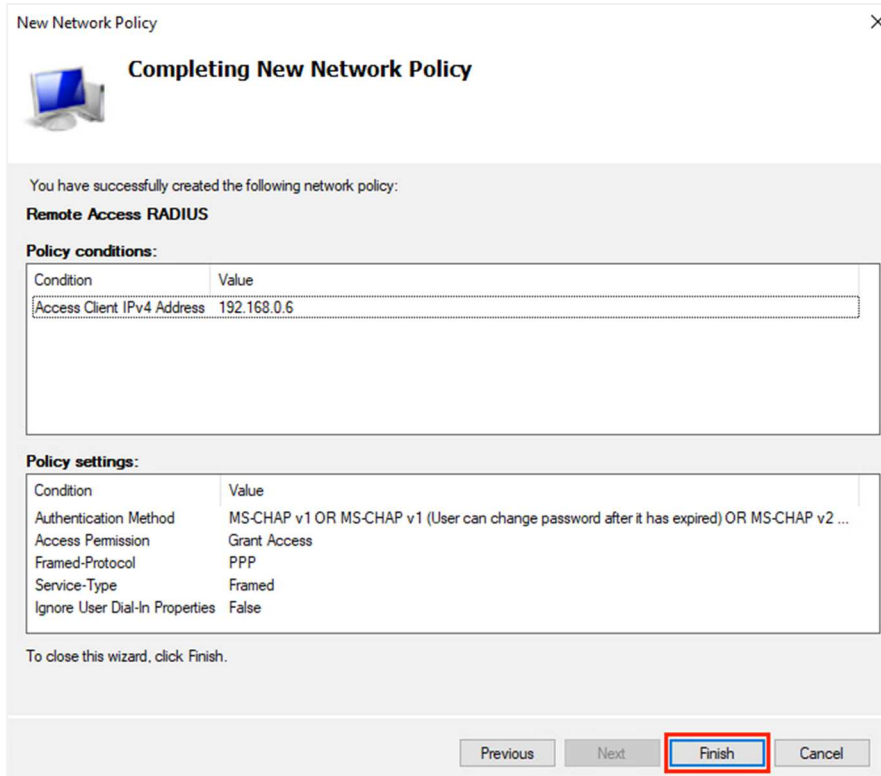
Attributes:

Name	Value
Framed-Protocol	PPP
Service-Type	Framed

Add... Edit... Remove

Previous **Next** Finish Cancel

19. On the *Completing New Network Policy* step, leave the defaults and click **Finish**.



New Network Policy

Completing New Network Policy

You have successfully created the following network policy:

Remote Access RADIUS

Policy conditions:

Condition	Value
Access Client IPv4 Address	192.168.0.6

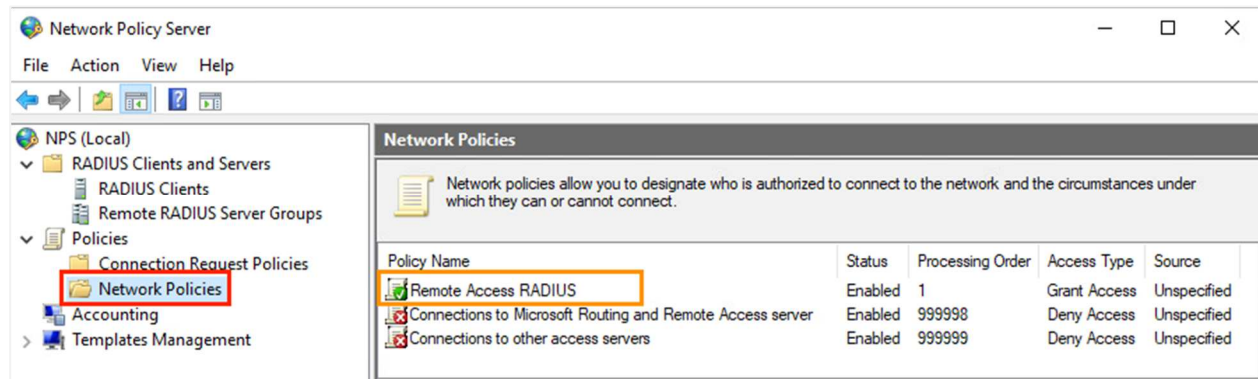
Policy settings:

Condition	Value
Authentication Method	MS-CHAP v1 OR MS-CHAP v1 (User can change password after it has expired) OR MS-CHAP v2 ...
Access Permission	Grant Access
Framed-Protocol	PPP
Service-Type	Framed
Ignore User Dial-In Properties	False

To close this wizard, click Finish.

Previous Next **Finish** Cancel

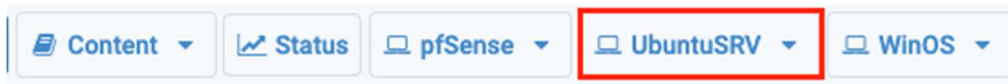
20. Back on the *Network Policy Server* window, in the left pane, click on **Network Policies** and confirm the new policy appears in the right pane.



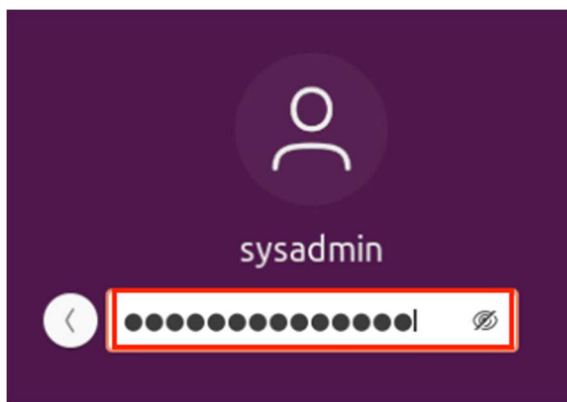
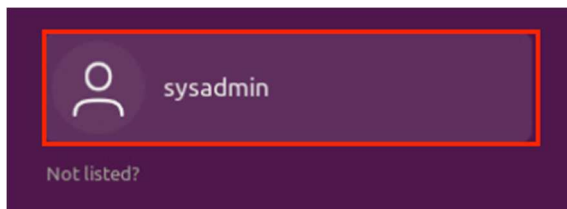
21. This section is now complete. Proceed to the next section to configure RADIUS on the Ubuntu system.

2 FreeRADIUS on Ubuntu

1. Launch the **UbuntuSRV** virtual machine to access the graphical login screen.



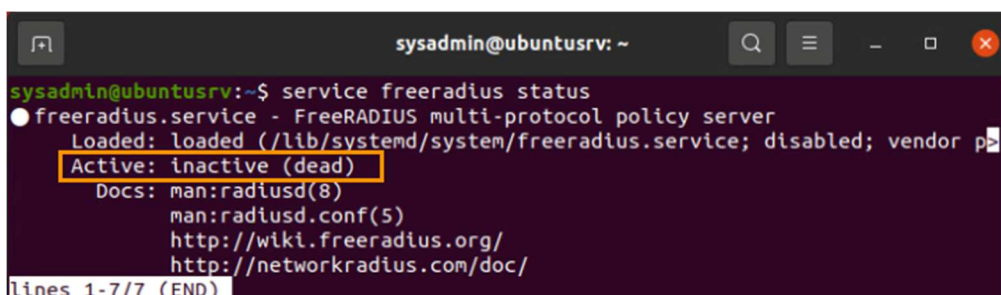
2. Log in as **sysadmin** using the password **NDGLabpass123!**.



3. Click the **Terminal** icon in the dock to start *Terminal*.



4. In the new *Terminal* window, type the command **service freeradius status** to check the status of the service. It should say *inactive*. Press **q** on the keyboard to get out of the status check.



```
sysadmin@ubuntusrv: ~  
sysadmin@ubuntusrv:~$ service freeradius status  
● freeradius.service - FreeRADIUS multi-protocol policy server  
   Loaded: loaded (/lib/systemd/system/freeradius.service; disabled; vendor p  
   Active: inactive (dead)  
     Docs: man:radiusd(8)  
           man:radiusd.conf(5)  
           http://wiki.freeradius.org/  
           http://networkradius.com/doc/  
lines 1-7/7 (END)
```

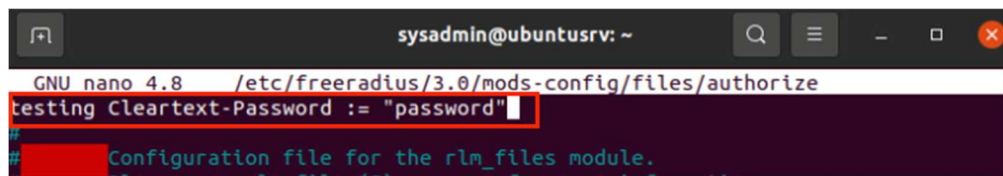
5. We are going to create a test account to locally test the RADIUS server. Type the command below in the *Terminal*. Enter **NDGLabpass123!** when prompted for a password.

```
sudo nano /etc/freeradius/3.0/mods-config/files/authorize
```



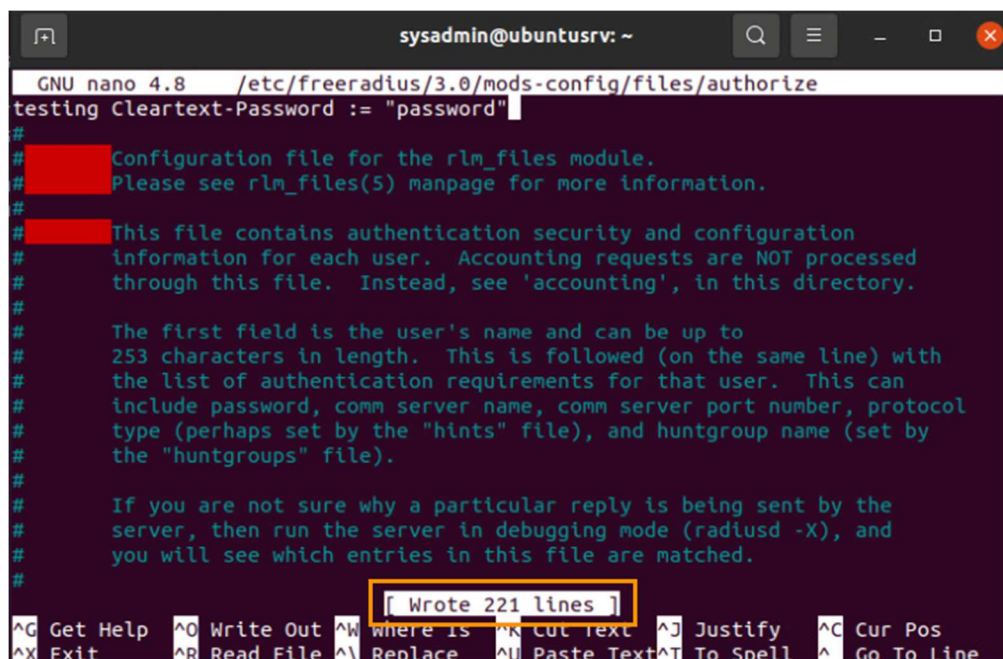
```
http://wiki.freeradius.org/
http://networkradius.com/doc/
sysadmin@ubuntusrv:~$ sudo nano /etc/freeradius/3.0/mods-config/files/authorize
[sudo] password for sysadmin: 
```

6. Once in the editor, press **Enter** to insert a newline at the top of the file. Then add the user info by typing: **testing Cleartext-Password := "password"**



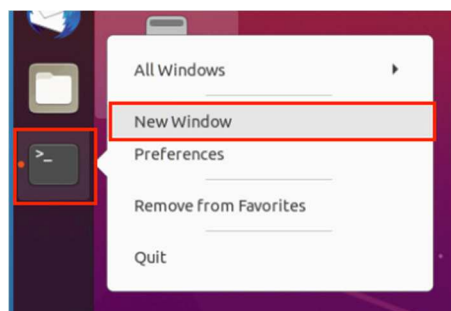
```
sysadmin@ubuntusrv: ~
GNU nano 4.8 /etc/freeradius/3.0/mods-config/files/authorize
testing Cleartext-Password := "password"
#
# Configuration file for the rlm_files module.
# Please see rlm_files(5) manpage for more information.
```

7. Then, press **Ctrl + S** to save the file and **Ctrl + X** to quit the editor.

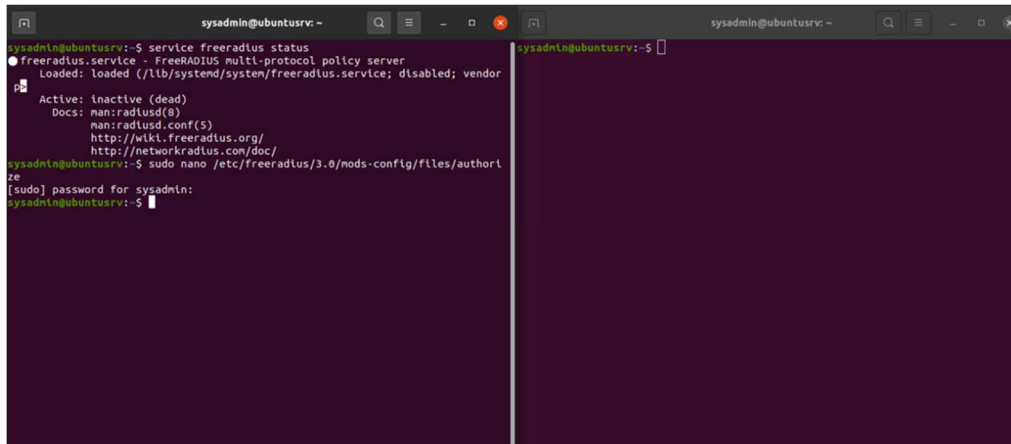


```
sysadmin@ubuntusrv: ~
GNU nano 4.8 /etc/freeradius/3.0/mods-config/files/authorize
testing Cleartext-Password := "password"
#
# Configuration file for the rlm_files module.
# Please see rlm_files(5) manpage for more information.
#
# This file contains authentication security and configuration
# information for each user. Accounting requests are NOT processed
# through this file. Instead, see 'accounting', in this directory.
#
# The first field is the user's name and can be up to
# 253 characters in length. This is followed (on the same line) with
# the list of authentication requirements for that user. This can
# include password, comm server name, comm server port number, protocol
# type (perhaps set by the "hints" file), and huntgroup name (set by
# the "huntgroups" file).
#
# If you are not sure why a particular reply is being sent by the
# server, then run the server in debugging mode (radiusd -X), and
# you will see which entries in this file are matched.
#
[ Wrote 221 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 Paste Text ^T To Spell ^_ Go To Line
```

8. Start a new *Terminal* by right-clicking the **Terminal** icon in the dock and selecting **New Window**.



- Rearrange the two windows to make them side-by-side.



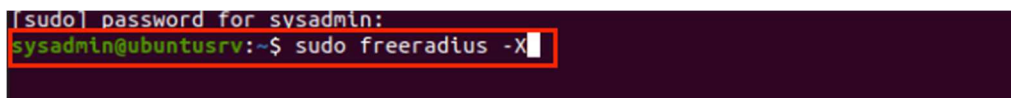
```

sysadmin@ubuntu:~$ service freeradius status
● freeradius.service - FreeRADIUS multi-protocol policy server
   Loaded: loaded (/lib/systemd/system/freeradius.service; disabled; vendor
   Active: inactive (dead)
     Docs: man:radiusd(8)
           man:radiusd.conf(5)
           http://wiki.freeradius.org/
           http://networkradius.com/doc/
sysadmin@ubuntu:~$ sudo nano /etc/freeradius/3.0/mods-config/files/authorize
[sudo] password for sysadmin:
sysadmin@ubuntu:~$

```

- RADIUS is mostly used for *Business Wireless Access Point* authentication. It is an alternative method to Active Directory. In this lab, we are only going to test and learn the functionality of RADIUS rather than configure it.

In the first *Terminal* window, type the command `sudo freeradius -X` and press **Enter** to run it. The `-X` option will run the *freeradius* service in debugging mode. Enter **NDGlabpass123!** when prompted for the password.

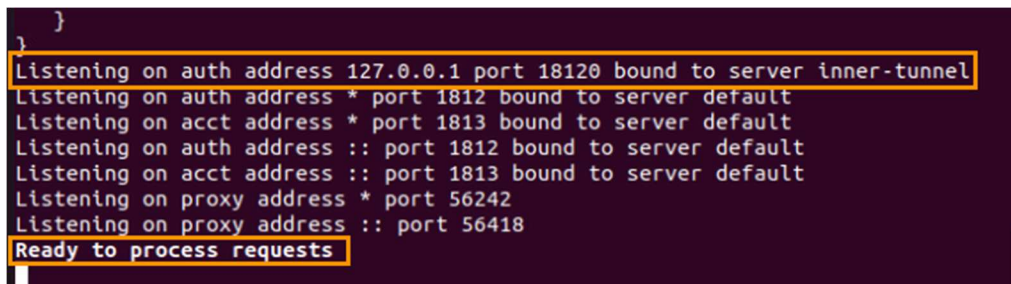


```

[sudo] password for sysadmin:
sysadmin@ubuntu:~$ sudo freeradius -X

```

- When you see the *Ready to process requests* prompt, it means the RADIUS server is up and running. And for local testing, it is bound to port **18120**.

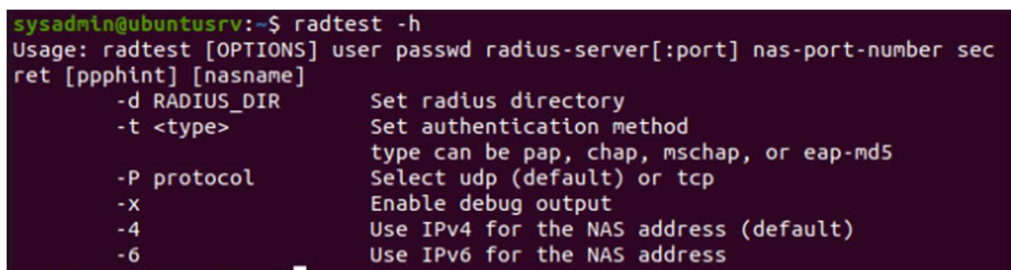


```

}
}
Listening on auth address 127.0.0.1 port 18120 bound to server inner-tunnel
Listening on auth address * port 1812 bound to server default
Listening on acct address * port 1813 bound to server default
Listening on auth address :: port 1812 bound to server default
Listening on acct address :: port 1813 bound to server default
Listening on proxy address * port 56242
Listening on proxy address :: port 56418
Ready to process requests

```

- Now switch to the other *Terminal* window. Enter the command `radtest -h` to bring up the help page.



```

sysadmin@ubuntu:~$ radtest -h
Usage: radtest [OPTIONS] user passwd radius-server[:port] nas-port-number sec
ret [pphint] [nasname]
  -d RADIUS_DIR      Set radius directory
  -t <type>          Set authentication method
                     type can be pap, chap, mschap, or eap-md5
  -P protocol        Select udp (default) or tcp
  -X                 Enable debug output
  -4                 Use IPv4 for the NAS address (default)
  -6                 Use IPv6 for the NAS address

```


13. Based on the help info, the command we will be using is:

```
radtest testing password 127.0.0.1 18120 testing123
```

14. If you see the result showing *Received Access-Accept*, it means the RADIUS server is working.

```
sysadmin@ubuntu:~$ radtest testing password 127.0.0.1 18120 testing123
Sent Access-Request Id 235 from 0.0.0.0:54668 to 127.0.0.1:1812 length 77
  User-Name = "testing"
  User-Password = "password"
  NAS-IP-Address = 172.16.1.10
  NAS-Port = 18120
  Message-Authenticator = 0x00
  Cleartext-Password = "password"
Received Access-Accept Id 235 from 127.0.0.1:1812 to 127.0.0.1:54668 length 2
0
sysadmin@ubuntu:~$
```

15. And you should see the response scrolling in the other window.

```
(0) [pap] = ok
(0) } # Auth-Type PAP = ok
(0) # Executing section post-auth from file /etc/freeradius/3.0/sites-enabled/default
(0) post-auth {
(0)   if (session-state:User-Name && reply:User-Name && request:User-Name &
& (reply:User-Name == request:User-Name)) {
(0)     if (session-state:User-Name && reply:User-Name && request:User-Name &
& (reply:User-Name == request:User-Name)) -> FALSE
(0)     update {
(0)       No attributes updated for RHS &session-state:
(0)     } # update = noop
(0)     [exec] = noop
(0)     policy remove_reply_message_if_eap {
(0)       if (&reply:EAP-Message && &reply:Reply-Message) {
(0)         if (&reply:EAP-Message && &reply:Reply-Message) -> FALSE
(0)       } else {
(0)         [noop] = noop
(0)       } # else = noop
(0)     } # policy remove_reply_message_if_eap = noop
(0)   } # post-auth = noop
(0) Sent Access-Accept Id 235 from 127.0.0.1:1812 to 127.0.0.1:54668 length 0
(0) Finished request
Waking up in 4.9 seconds.
(0) Cleaning up request packet ID 235 with timestamp +532
Ready to process requests
```

16. The lab is now complete; you may end your reservation.