SERVER PROJECT OPEN VPN AND VPN TUNNEL

On your **onpremR** install the following packages:

- yum install epel-release
- yum install openvpn

Confirm installation of openvpn by verifying the following directories are present:

- /etc/openvpn/server
- /etc/openvpn/client
-

Generate the VPN key

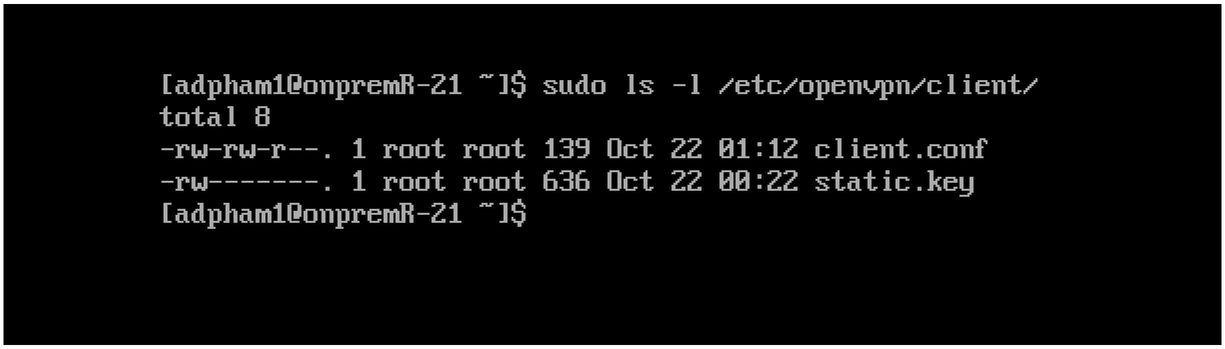
Execute the following command on your **onpremR** to create a static key to be used by **both** the client **(onpremR)** and server **(az-fer)**

- openvpn –keysize 128 –genkey –secret static.key

Confirm the creation of the key by performing a directory listing. You should see it in the current directory.

Copy configuration files and VPN key

Examine the file **client.conf** and understand what it does. Copy **client.conf** (provided with this checkpoint) and **static.key** (the one you just created) to **/etc/openvpn/client**



```
[adpham1@onpremR-21 ~]$ sudo ls -l /etc/openvpn/client/
total 8
-rw-rw-r--. 1 root root 139 Oct 22 01:12 client.conf
-rw-------. 1 root root 636 Oct 22 00:22 static.key
[adpham1@onpremR-21 ~]$
```

Making the VPN persistent through reboots

In order to accomplish this, we need to edit the crontab of the root user and point it to run a script every time the VM starts.

Create the directory **/usr/scripts**

Examine the script **vpnstart-C.sh** and understand what it does. Copy **vpnstart-C.sh** to **/usr/scripts/**

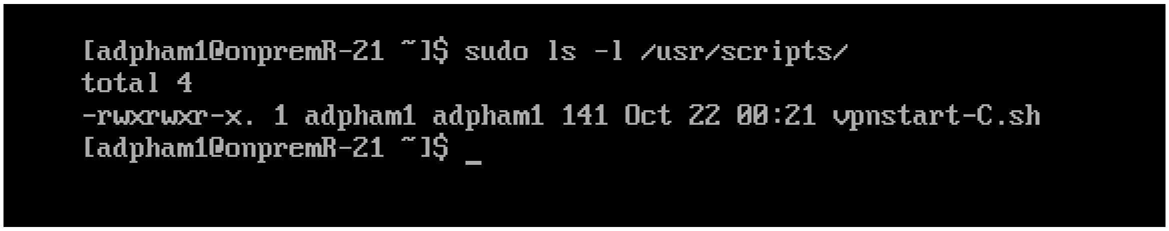
You must now edit the **crontab** of the **root** user to run **vpnstart.sh** at startup.

Sudo crontab -e

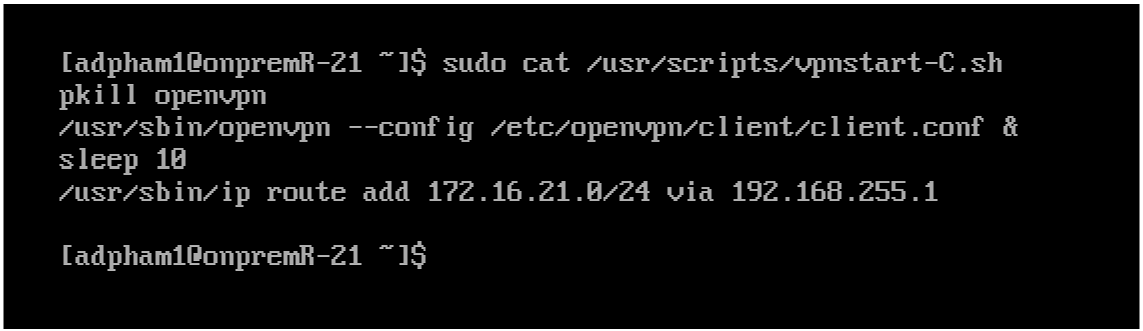
add **@reboot /usr/scripts/vpnstart-C.sh**

Save and exit.

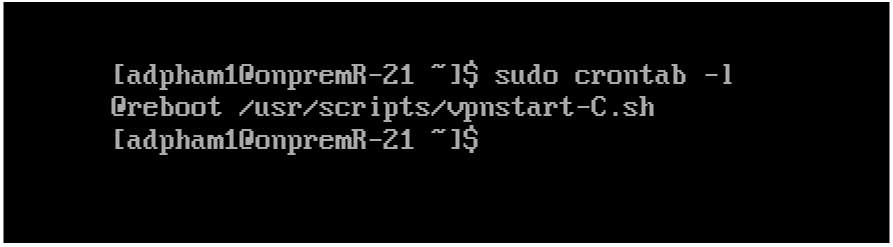
scp vpnstart-C.sh 192.168.26.129:/usr/scripts/
sudo chmod +x /usr/scripts/vpnstart-C.sh
sudo bash /usr/scripts/vpnstart-C.sh



```
[adpham1@onpremR-21 ~]$ sudo ls -l /usr/scripts/
total 4
-rwxrwxr-x. 1 adpham1 adpham1 141 Oct 22 00:21 vpnstart-C.sh
[adpham1@onpremR-21 ~]$ _
```



```
[adpham1@onpremR-21 ~]$ sudo cat /usr/scripts/vpnstart-C.sh
pkill openvpn
/usr/sbin/openvpn --config /etc/openvpn/client/client.conf &
sleep 10
/usr/sbin/ip route add 172.16.21.0/24 via 192.168.255.1

[adpham1@onpremR-21 ~]$
```



```
[adpham1@onpremR-21 ~]$ sudo crontab -l
@reboot /usr/scripts/vpnstart-C.sh
[adpham1@onpremR-21 ~]$
```

You must now repeat this process on the **az-fer** VM however, this will be the server which means the location of the files **server.conf** and **static.key** will be in a different place. Also, note that here is a file **vpnstart-S.sh** Figure out what to do with this.

```
sudo yum install epel-release
sudo yum install openvpn
```

```
sudo mkdir /usr/scripts
```

```
scp server.conf az-fer21347477.canadacentral.cloudapp.azure.com:/etc/openvpn/server/
```

```
scp vpnstart-S.sh az-fer21347477.canadacentral.cloudapp.azure.com:/usr/scripts/
```

```
scp static.key ssh az-fer21347477.canadacentral.cloudapp.azure.com:/etc/openvpn/server/
```

```
sudo chmod +x /usr/scripts/vpnstart-S.sh
sudo bash /usr/scripts/vpnstart-S.sh
```

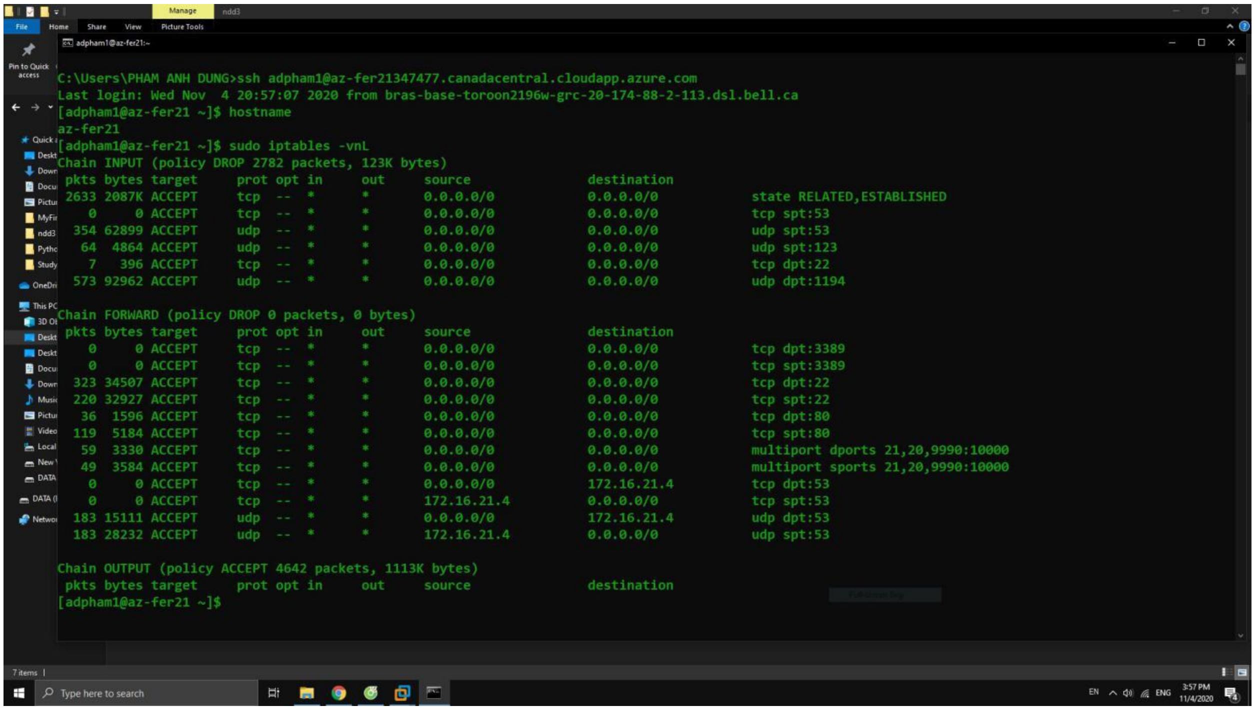
Re-configuring iptables on az-fer

Examine the script **iptables-tun.sh** and understand what it does. Execute the script on az-fer and try to RDP to your **az-ws** VM from your Windows host. Include the results of this test in your documentation with an explanation as to why.

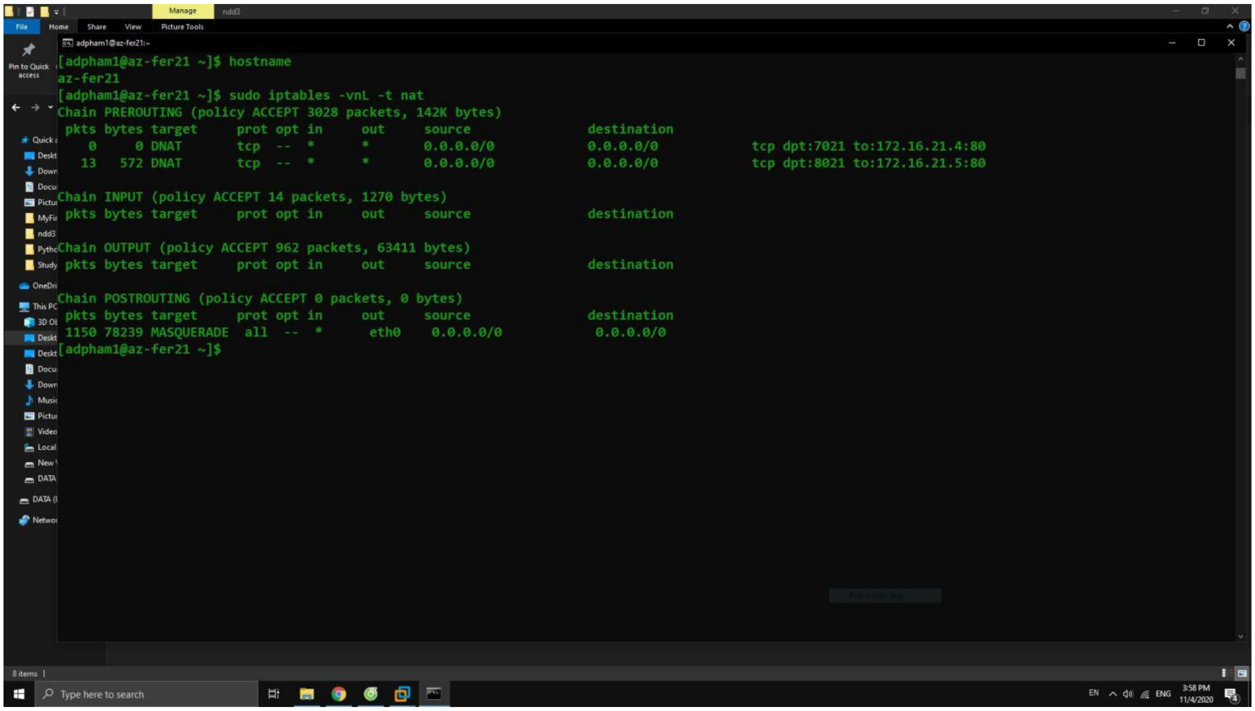
```
scp iptables-tun.sh az-fer21347477.canadacentral.cloudapp.azure.com:
```

```
sudo iptables -I FORWARD 5 -p tcp --dports 80 -j ACCEPT
sudo iptables -I FORWARD 6 -p tcp --sports 80 -j ACCEPT
sudo iptables -I FORWARD 7 -p tcp -m multiport --dports 21,20,9990:10000 -j ACCEPT
sudo iptables -I FORWARD 8 -p tcp -m multiport --sports 21,20,9990:10000 -j ACCEPT
```

```
sudo service iptables save
```



```
C:\Users\PHAM ANH DUNG>ssh adpham1@az-fer21347477.canadacentral.cloudapp.azure.com
Last login: Wed Nov  4 20:57:07 2020 from bras-base-toroon2196w-grc-20-174-88-2-113.dsl.bell.ca
[adpham1@az-fer21 ~]$ hostname
az-fer21
[adpham1@az-fer21 ~]$ sudo iptables -vnL
Chain INPUT (policy DROP 2782 packets, 123K bytes)
 pkts bytes target     prot opt in     out     source               destination
 2633 2087K ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:53
  354 62899 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0            udp spt:53
   64  4864 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0            udp spt:123
    7   396 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22
  573 92962 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0            udp dpt:1194

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:3389
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:3389
  323 34507 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22
  220 32927 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:22
   36  1596 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:80
  119  5184 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:80
   59  3330 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            multiport dports 21,20,9990:10000
   49  3584 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            multiport sports 21,20,9990:10000
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            172.16.21.4          tcp dpt:53
    0     0 ACCEPT     tcp  --  *      *       172.16.21.4          0.0.0.0/0            tcp spt:53
  183 15111 ACCEPT     udp  --  *      *       0.0.0.0/0            172.16.21.4          udp dpt:53
  183 28232 ACCEPT     udp  --  *      *       172.16.21.4          0.0.0.0/0            udp spt:53

Chain OUTPUT (policy ACCEPT 4642 packets, 1113K bytes)
 pkts bytes target     prot opt in     out     source               destination
[adpham1@az-fer21 ~]$
```



```
[adpham1@az-fer21 ~]$ hostname
az-fer21
[adpham1@az-fer21 ~]$ sudo iptables -vnL -t nat
Chain PREROUTING (policy ACCEPT 3028 packets, 142K bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DNAT       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:7021 to:172.16.21.4:80
   13   572 DNAT       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:8021 to:172.16.21.5:80

Chain INPUT (policy ACCEPT 14 packets, 1270 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 962 packets, 63411 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
 1150 78239 MASQUERADE  all  --  *      eth0    0.0.0.0/0            0.0.0.0/0
[adpham1@az-fer21 ~]$
```

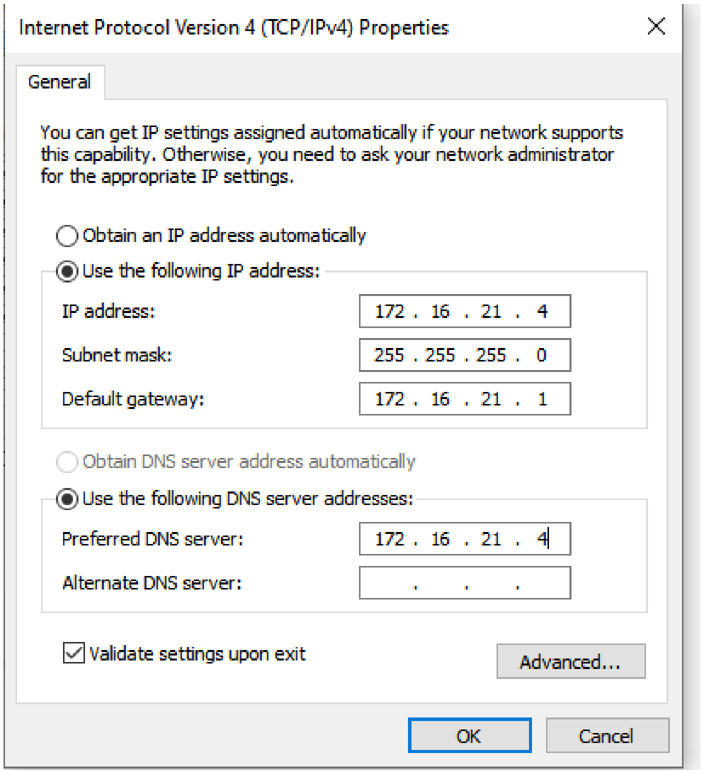
Configure the DNS role on az-ws

Add the DNS role to the server

Create forward lookup zone called ndd430**XX**.com (replace XX with your unique id)

Create A records for **ws-XX**, **ls-XX** and **az-ferXX** (tunnel ip)

Configure an option for the DNS server to use 8.8.8.8 if a request is made that can not be resolved by your DNS (ex. google.ca)



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

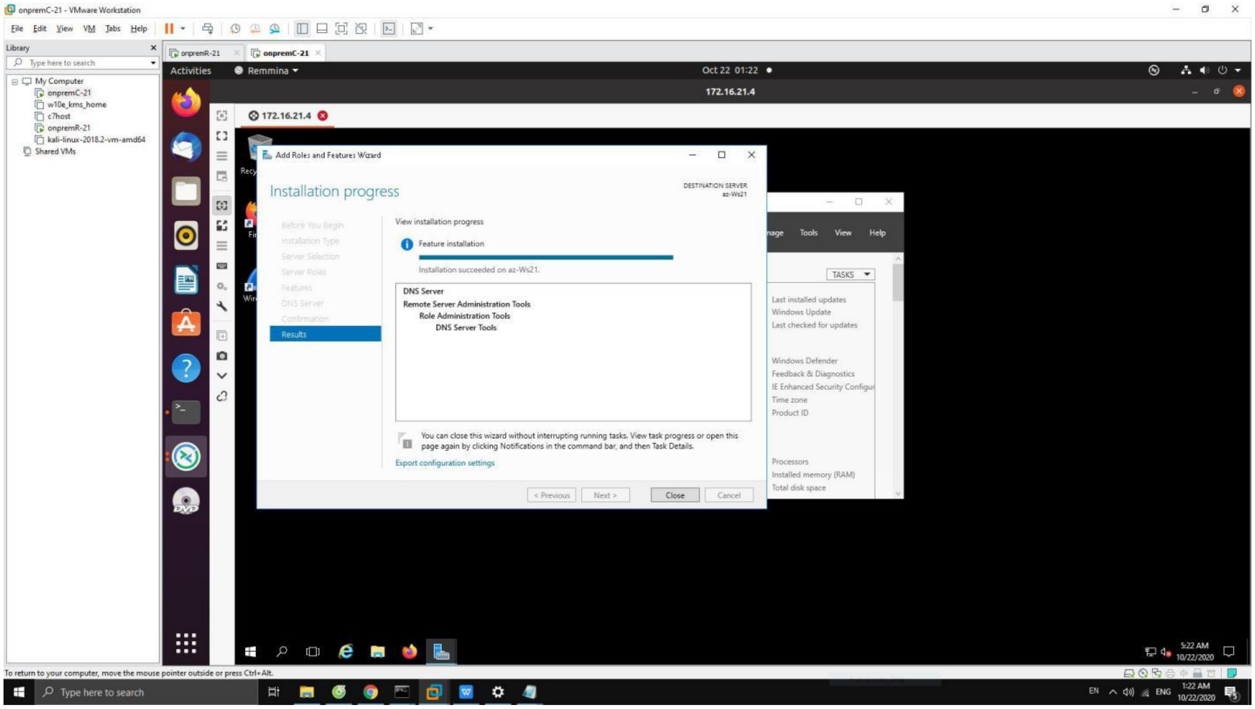
IP address:	172 . 16 . 21 . 4
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	172 . 16 . 21 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server:	172 . 16 . 21 . 4
Alternate DNS server:	. . .

☑ Validate settings upon exit



Installation progress

DESTINATION SERVER
az-Ws21

View installation progress

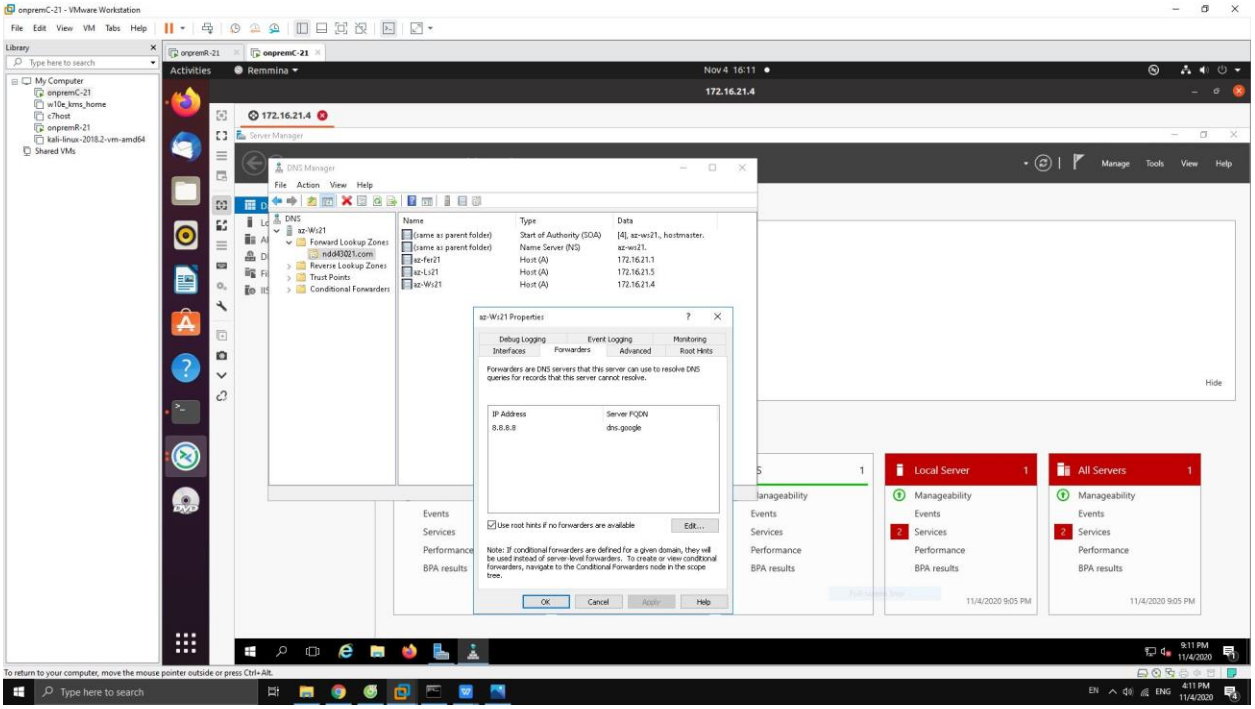
Feature installation

Installation succeeded on az-Ws21.

- DNS Server
- Remote Server Administration Tools
  - Role Administration Tools
    - DNS Server Tools

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

Export configuration settings



DNS
- az-Ws21
  - Forward Lookup Zones
    - ndd43021.com
  - Reverse Lookup Zones
  - Trust Points
  - Conditional Forwarders

Name	Type	Data
(same as parent folder)	Start of Authority (SOA)	[4], az-ws21., hostmaster.
(same as parent folder)	Name Server (NS)	az-ws21.
az-fer21	Host (A)	172.16.21.1
az-Ls21	Host (A)	172.16.21.5
az-Ws21	Host (A)	172.16.21.4

az-Ws21 Properties

Debug Logging | Event Logging | Monitoring | Interfaces | Forwarders | Advanced | Root Hints

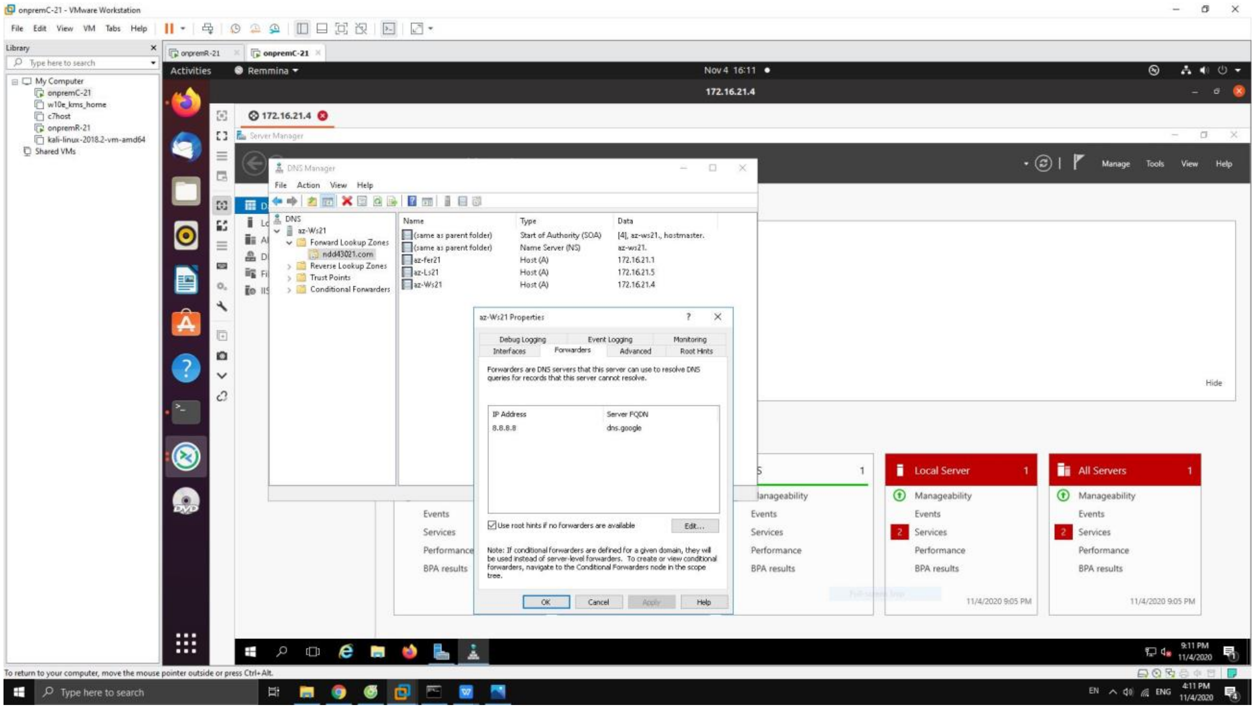
Forwarders are DNS servers that this server can use to resolve DNS queries for records that this server cannot resolve.

IP Address	Server FQDN
8.8.8.8	dns.google

☑ Use root hints if no forwarders are available Edit...

Note: If conditional forwarders are defined for a given domain, they will be used instead of server-level forwarders. To create or view conditional forwarders, navigate to the Conditional Forwarders node in the scope tree.

OK Cancel Apply Help



Name	Type	Data
(same as parent folder)	Start of Authority (SOA)	[4], az-ws21., hostmaster.
(same as parent folder)	Name Server (NS)	az-ws21.
az-fer21	Host (A)	172.16.21.1
az-Ls21	Host (A)	172.16.21.5
az-Ws21	Host (A)	172.16.21.4

az-Ws21 Properties

Debug Logging | Event Logging | Monitoring | Interfaces | Forwarders | Advanced | Root Hints

Forwarders are DNS servers that this server can use to resolve DNS queries for records that this server cannot resolve.

IP Address	Server FQDN
8.8.8.8	dns.google

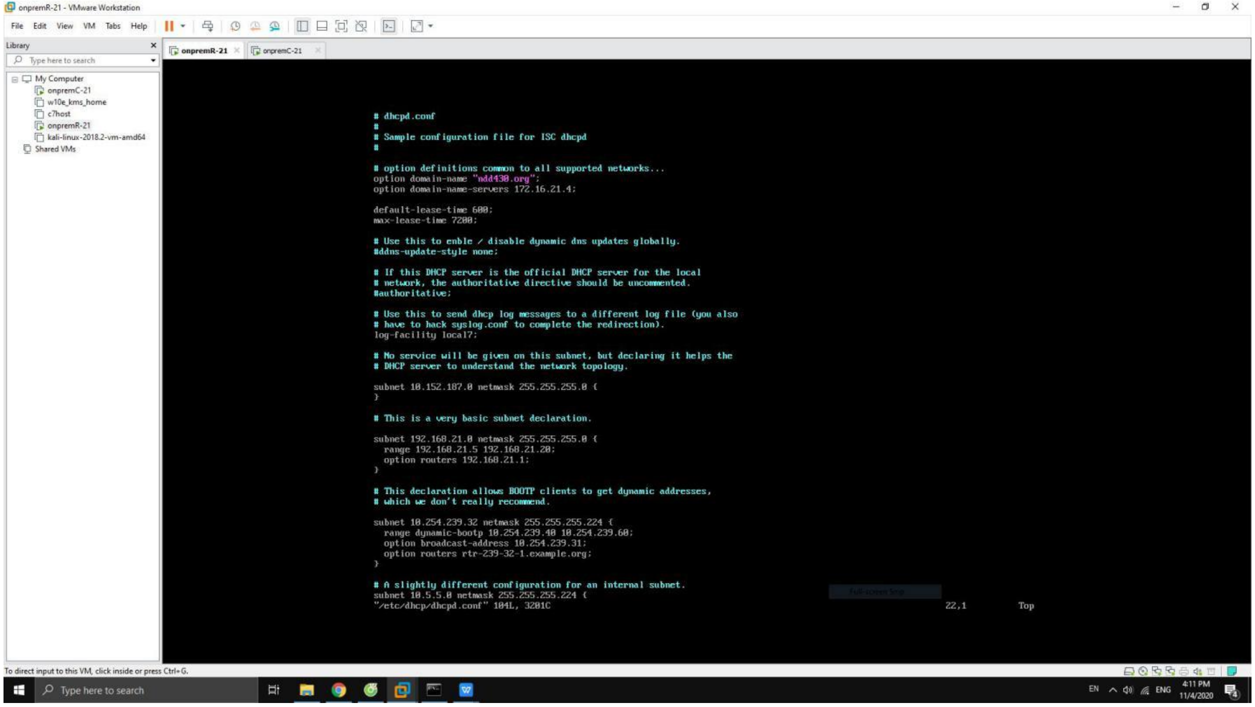
☑ Use root hints if no forwarders are available

Note: If conditional forwarders are defined for a given domain, they will be used instead of server-level forwarders. To create or view conditional forwarders, navigate to the Conditional Forwarders node in the scope tree.

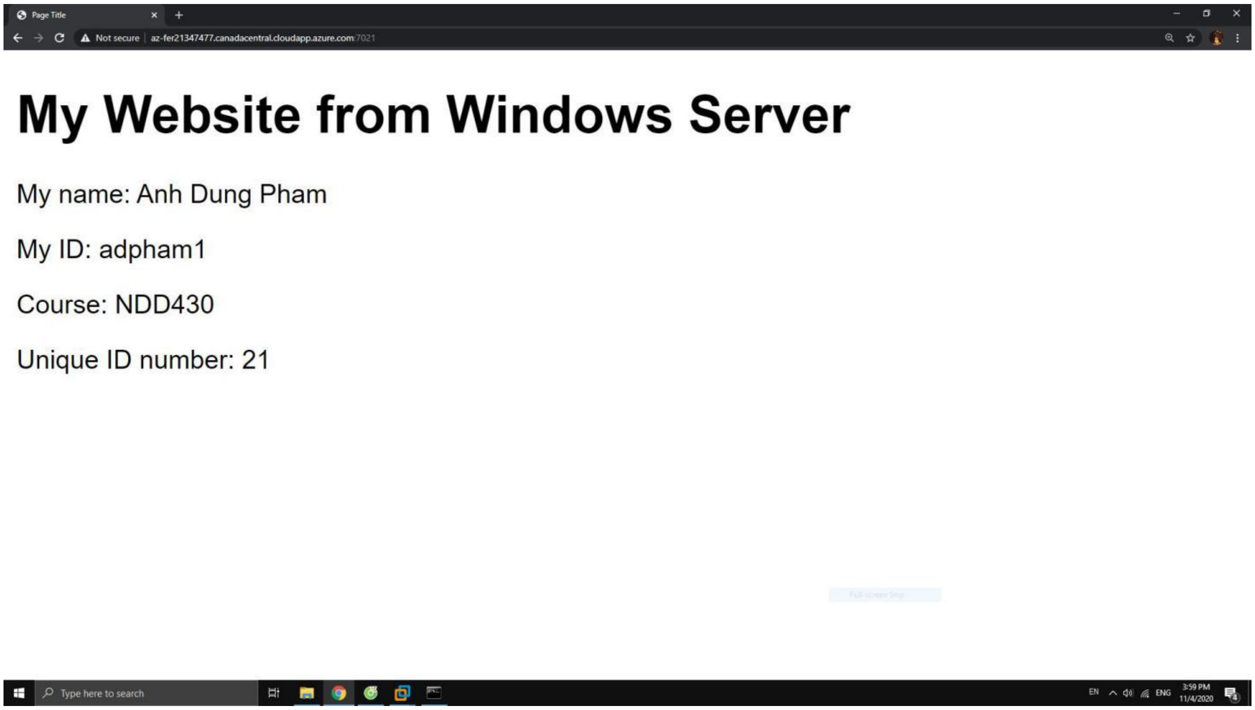
Modify the DHCP service on your **onpremR** VM to assign your client the ip of your **az-ws** for dns

Configure forwarder for DNS server to use 8.8.8.8 if a request is outside your local DNS

sudo vim /etc/dhcp/dhcpd.conf
And fix option domain-name-servers 172.16.21.4



```
# dhcpd.conf
#
# Sample configuration file for ISC dhcpd
#

# option definitions common to all supported networks...
option domain-name "ndd430.org";
option domain-name-servers 172.16.21.4;

default-lease-time 600;
max-lease-time 7200;

# Use this to enble / disable dynamic dns updates globally.
#ddns-update-style none;

# If this DHCP server is the official DHCP server for the local
# network, the authoritative directive should be uncommented.
#authoritative;

# Use this to send dhcp log messages to a different log file (you also
# have to hack syslog.conf to complete the redirection).
log-facility local7;

# No service will be given on this subnet, but declaring it helps the
# DHCP server to understand the network topology.

subnet 10.152.187.0 netmask 255.255.255.0 {
}

# This is a very basic subnet declaration.

subnet 192.168.21.0 netmask 255.255.255.0 {
  range 192.168.21.5 192.168.21.20;
  option routers 192.168.21.1;
}

# This declaration allows BOOTP clients to get dynamic addresses,
# which we don't really recommend.

subnet 10.254.239.32 netmask 255.255.255.224 {
  range dynamic-bootp 10.254.239.40 10.254.239.60;
  option broadcast-address 10.254.239.31;
  option routers rtr-239-32-1.example.org;
}

# A slightly different configuration for an internal subnet.
subnet 10.5.5.0 netmask 255.255.255.224 {
"/etc/dhcp/dhcpd.conf" 104L, 3201C                                    22,1          Top
```


Page Title
Not secure | az-fer21347477.canadacentral.cloudapp.azure.com:7021

My Website from Windows Server

My name: Anh Dung Pham

My ID: adpham1

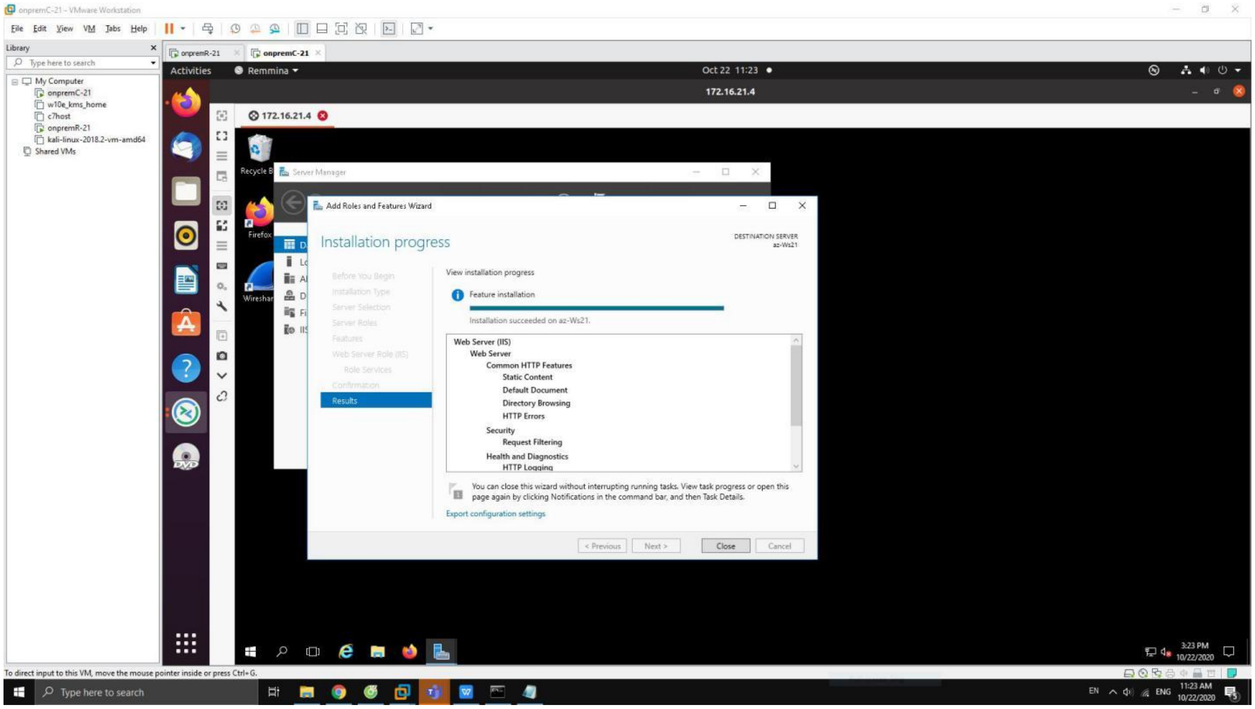
Course: NDD430

Unique ID number: 21

Type here to search
3:59 PM
11/4/2020

Install and configure additional services

Install and configure IIS on the **az-ws** VM. Have the server display a webpage with your name and unique ID number **(XX)** when accessed. **This service should be accessible from any host, anywhere.**



Installation progress

DESTINATION SERVER
az-Ws21

View installation progress

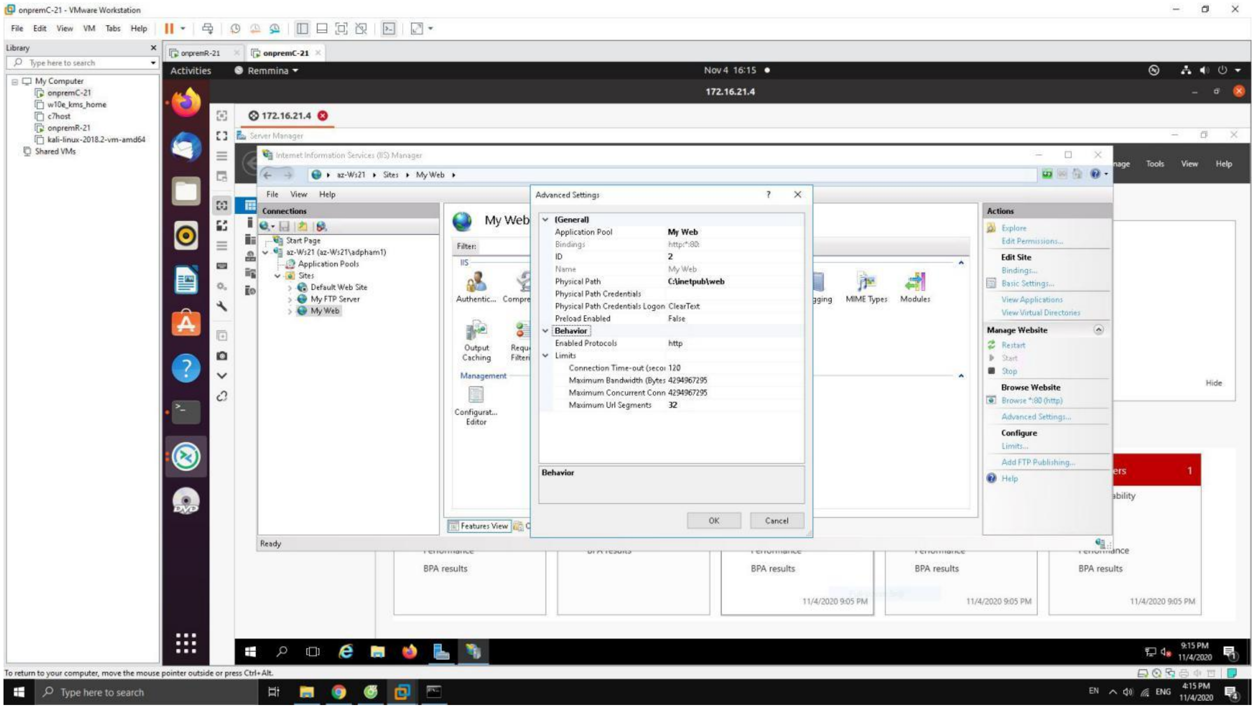
Feature installation

Installation succeeded on az-Ws21.

```
Web Server (IIS)
    Web Server
        Common HTTP Features
            Static Content
            Default Document
            Directory Browsing
            HTTP Errors
        Security
            Request Filtering
        Health and Diagnostics
            HTTP Logging
```

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

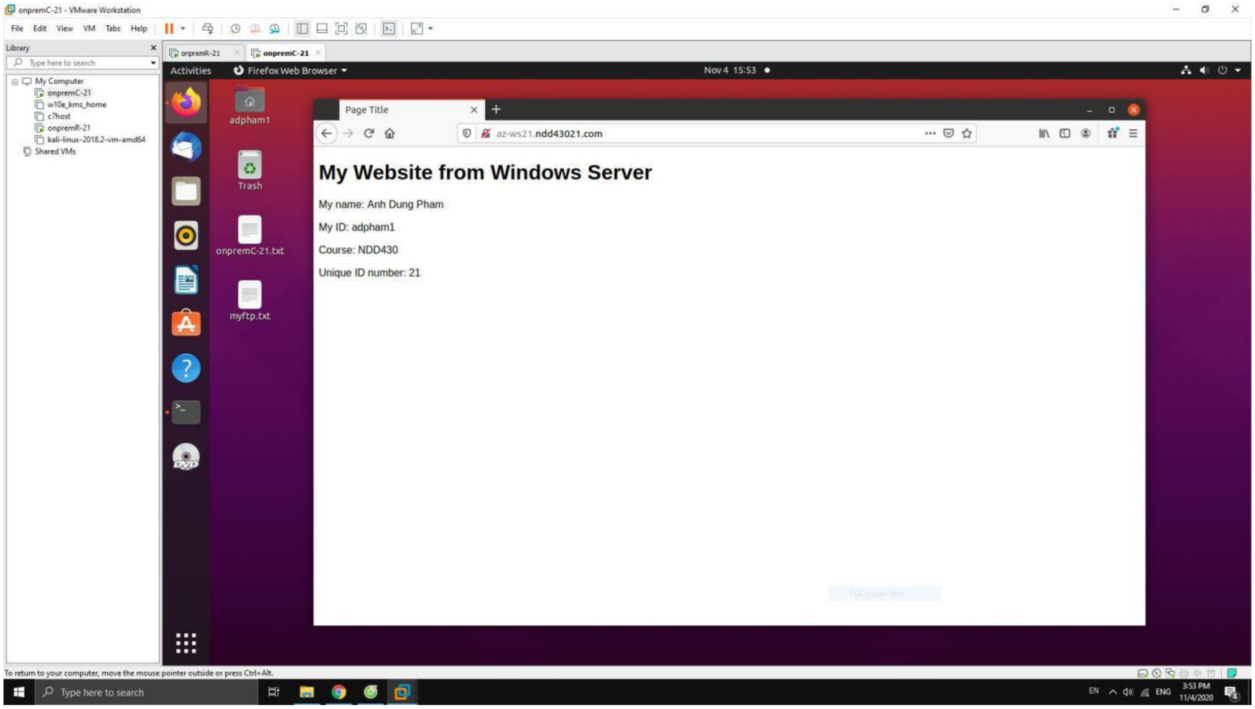
Export configuration settings



Advanced Settings

(General)

```
Application Pool                      My Web
Bindings                              http:*:80:
ID                                    2
Name                                  My Web
Physical Path                         C:\inetpub\web
Physical Path Credentials
Physical Path Credentials Logon       ClearText
Preload Enabled                       False
Behavior
Enabled Protocols                     http
Limits
   Connection Time-out (secoı         120
   Maximum Bandwidth (Bytes           4294967295
   Maximum Concurrent Conn            4294967295
   Maximum Url Segments               32
```



az-ws21.ndd43021.com

My Website from Windows Server

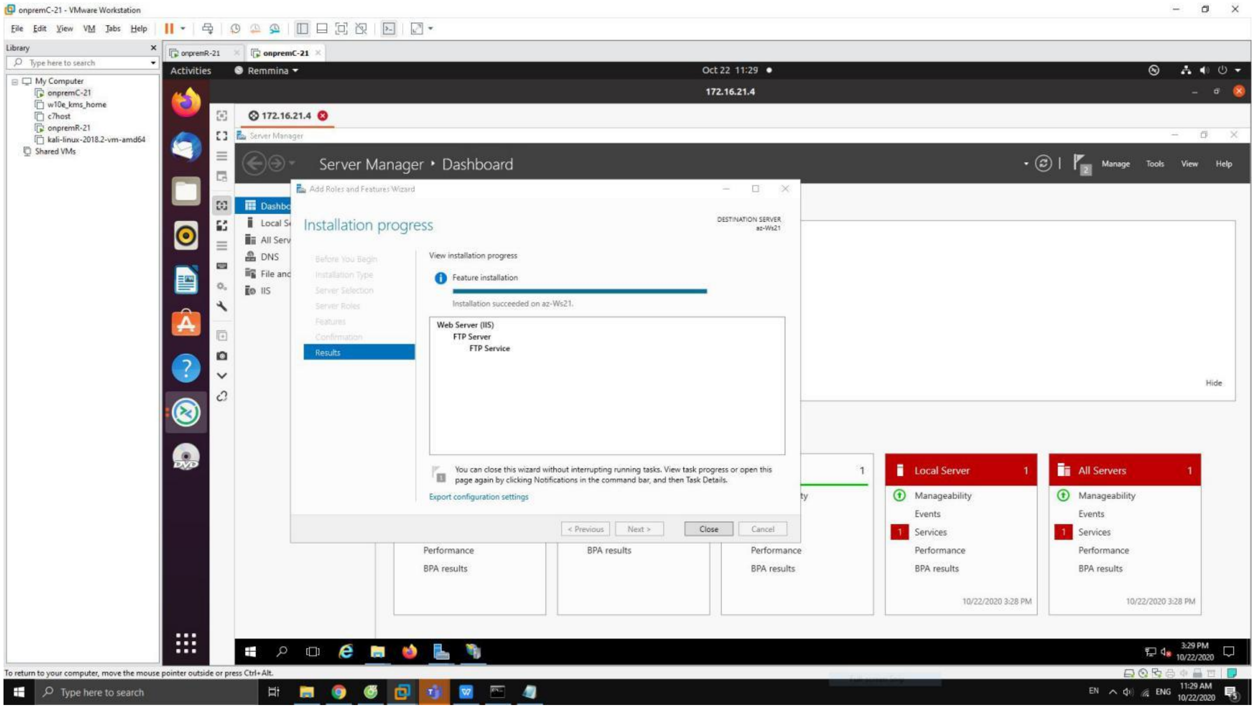
My name: Anh Dung Pham

My ID: adpham1

Course: NDD430

Unique ID number: 21

Install and configure the windows FTP service. Create a user that can log into the service and transfer files. **Only your onpremC should have access to this service – no access from outside the VPN**



Add Roles and Features Wizard

Installation progress

DESTINATION SERVER
az-Ws21

View installation progress

Feature installation

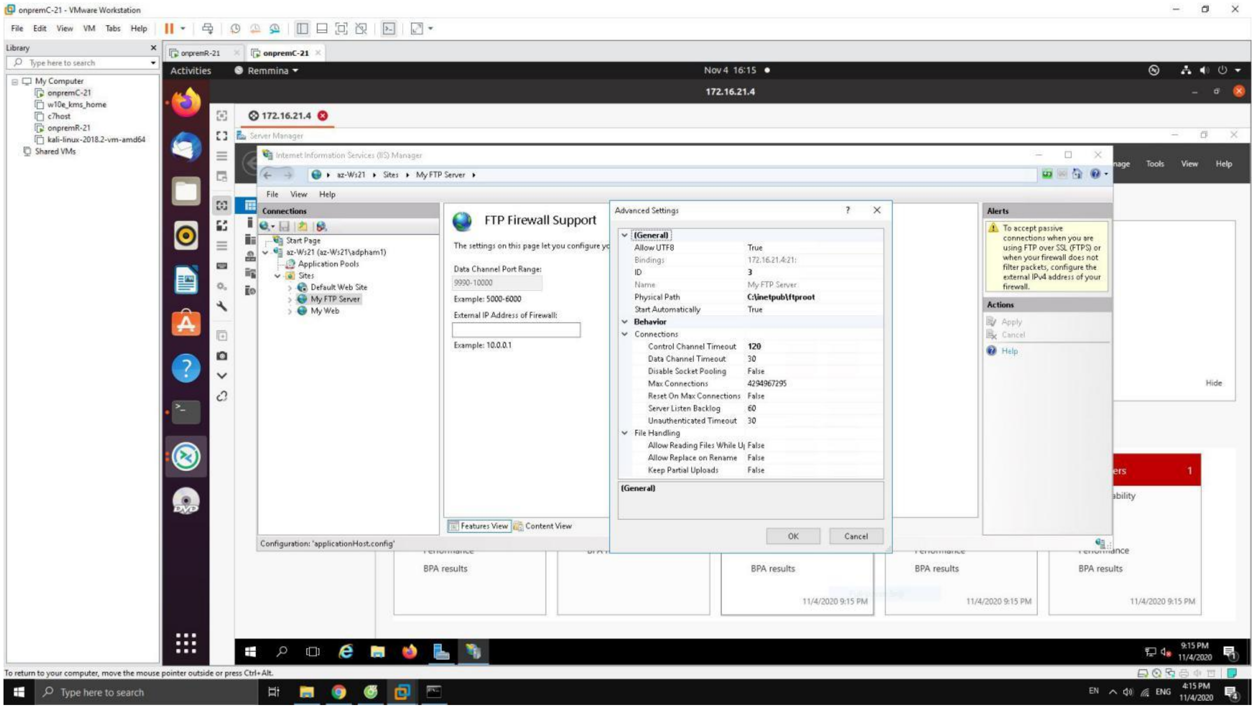
Installation succeeded on az-Ws21.

Web Server (IIS)
FTP Server
FTP Service

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

Export configuration settings

To return to your computer, move the mouse pointer outside or press Ctrl+Alt.



Internet Information Services (IIS) Manager

FTP Firewall Support

The settings on this page let you configure yo

Data Channel Port Range:
9990-10000
Example: 5000-6000

External IP Address of Firewall:

Example: 10.0.0.1

Advanced Settings

(General)	
Allow UTF8	True
Bindings	172.16.21.4:21:
ID	3
Name	My FTP Server
Physical Path	C:\inetpub\ftproot
Start Automatically	True
Behavior	
Connections	
Control Channel Timeout	120
Data Channel Timeout	30
Disable Socket Pooling	False
Max Connections	4294967295
Reset On Max Connections	False
Server Listen Backlog	60
Unauthenticated Timeout	30
File Handling	
Allow Reading Files While U[	False
Allow Replace on Rename	False
Keep Partial Uploads	False

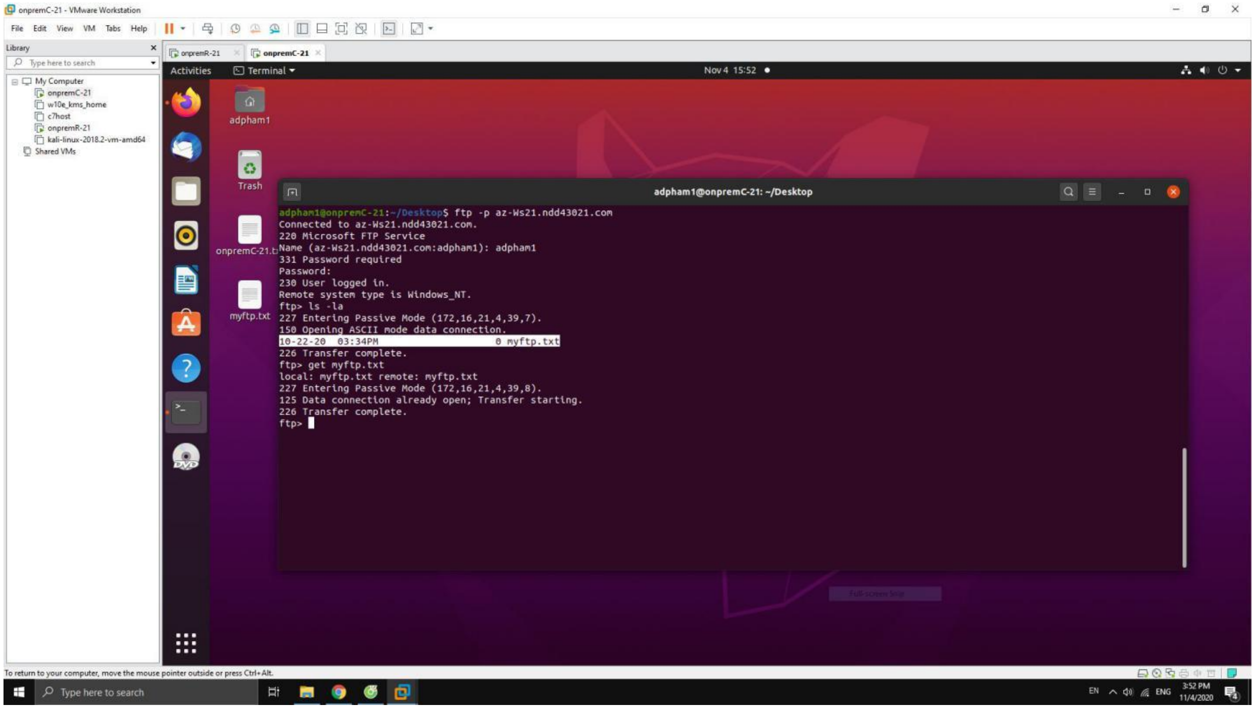
(General)

Alerts

To accept passive connections when you are using FTP over SSL (FTPS) or when your firewall does not filter packets, configure the external IPv4 address of your firewall.

Configuration: 'applicationHost.config'

To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

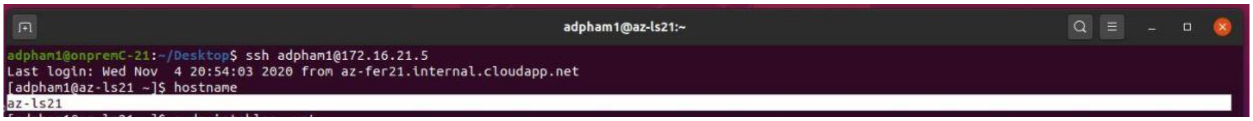


```
adpham1@onpremC-21:~/Desktop$ ftp -p az-Ws21.ndd43021.com
Connected to az-Ws21.ndd43021.com.
220 Microsoft FTP Service
Name (az-Ws21.ndd43021.com:adpham1): adpham1
331 Password required
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> ls -la
227 Entering Passive Mode (172,16,21,4,39,7).
150 Opening ASCII mode data connection.
10-22-20  03:34PM                  0 myftp.txt
226 Transfer complete.
ftp> get myftp.txt
local: myftp.txt remote: myftp.txt
227 Entering Passive Mode (172,16,21,4,39,8).
125 Data connection already open; Transfer starting.
226 Transfer complete.
ftp>
```

Or execute the link below in Firefox browser

ftp://az-ws21.ndd43021.com/

Verify SSH is configured and working on your ls-**XX** linux server. **Only your onpremC should have access to this service – no access from outside the VPN**



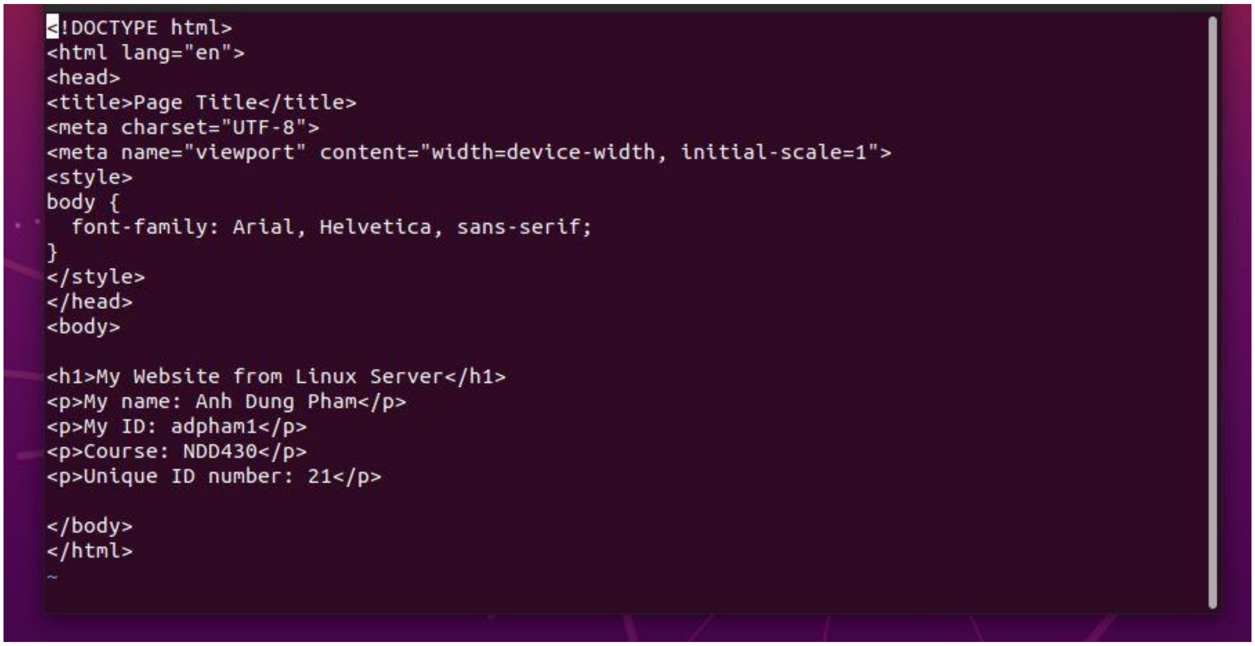
```
adpham1@onpremC-21:~/Desktop$ ssh adpham1@172.16.21.5
Last login: Wed Nov  4 20:54:03 2020 from az-fer21.internal.cloudapp.net
[adpham1@az-ls21 ~]$ hostname
az-ls21
```

Install and configure Apache on the az-ls VM. Have the server display a webpage with your name and unique ID number **(XX)** when accessed. **This service should be accessible from any host, anywhere.**

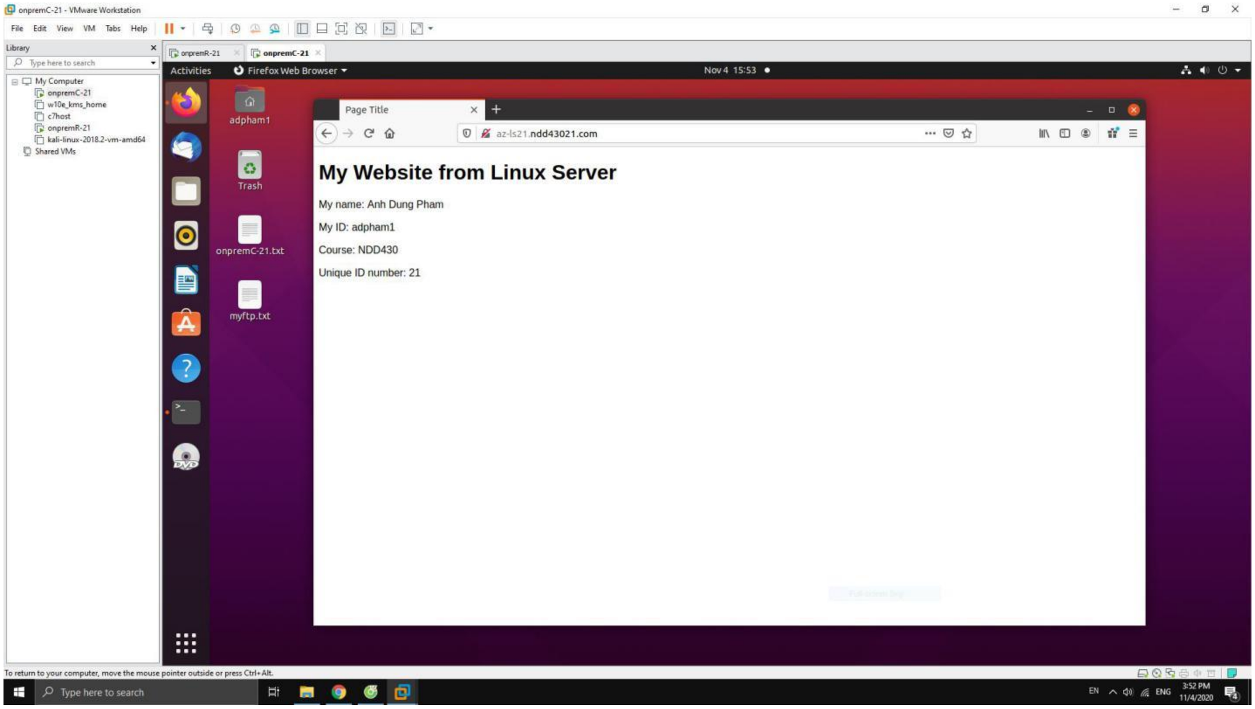
```
sudo yum install httpd
sudo systemctl enable httpd
sudo systemctl start httpd
sudo touch /var/www/html/index.html
sudo vi /var/www/html/index.html
```

Then copy the following html format into index.html

```
<!DOCTYPE html>
<html lang="en">
<head>
<title>Page Title</title>
<meta charset="UTF-8">
<meta name="viewport" content="width=device-width, initial-scale=1">
<style>
body {
  font-family: Arial, Helvetica, sans-serif;
}
</style>
</head>
<body>

<h1>My Website from Linux Server</h1>
<p>My name: Anh Dung Pham</p>
<p>My ID: adpham1</p>
<p>Course: NDD430</p>
<p>Unique ID number: 21</p>

</body>
</html>
```



```
<!DOCTYPE html>
<html lang="en">
<head>
<title>Page Title</title>
<meta charset="UTF-8">
<meta name="viewport" content="width=device-width, initial-scale=1">
<style>
body {
  font-family: Arial, Helvetica, sans-serif;
}
</style>
</head>
<body>

<h1>My Website from Linux Server</h1>
<p>My name: Anh Dung Pham</p>
<p>My ID: adpham1</p>
<p>Course: NDD430</p>
<p>Unique ID number: 21</p>

</body>
</html>
~
```



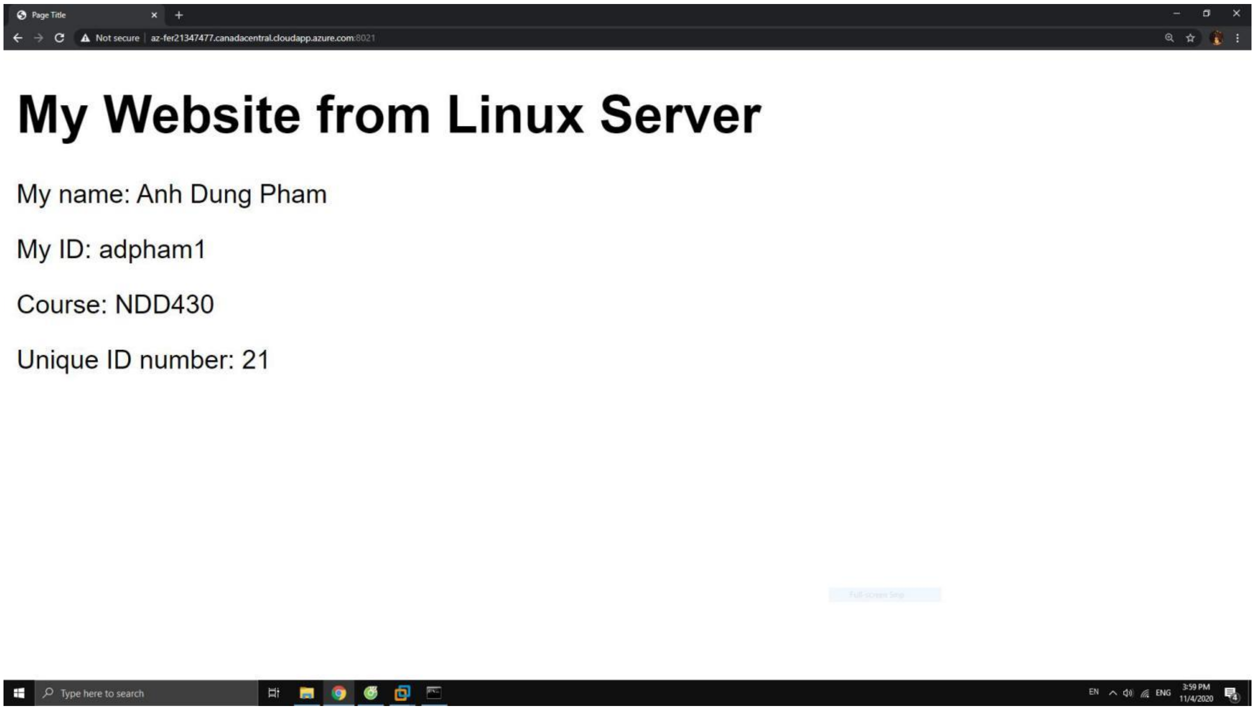
My Website from Linux Server

My name: Anh Dung Pham

My ID: adpham1

Course: NDD430

Unique ID number: 21



My Website from Linux Server

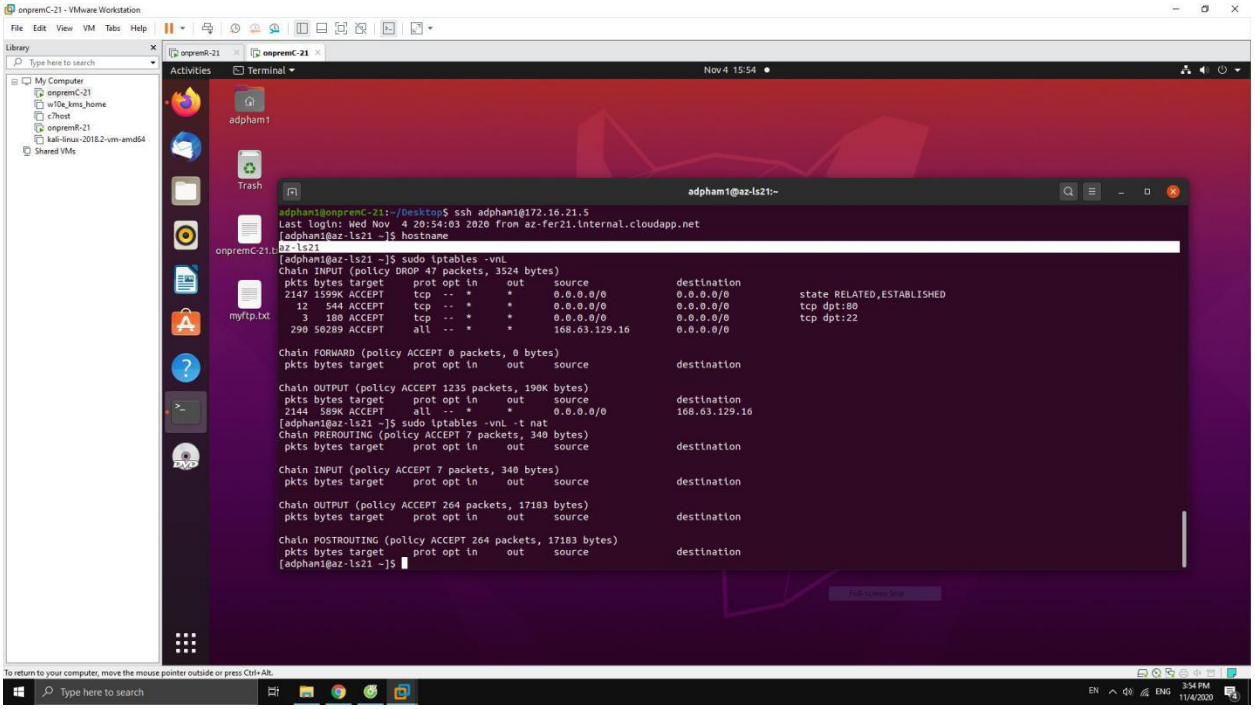
My name: Anh Dung Pham

My ID: adpham1

Course: NDD430

Unique ID number: 21

Configure the iptables firewall on your ls-XX linux server to allow only traffic to your Apache service and SSH service. Also, it should allow all traffic **IN** with a source address of **168.53.129.16** and all traffic **OUT** with a destination address of **168.53.129.16. No other ports should be open in the firewall on this server.**



```
adpham1@onpremC-21:~/Desktop$ ssh adpham1@172.16.21.5
Last login: Wed Nov  4 20:54:03 2020 from az-fer21.internal.cloudapp.net
[adpham1@az-ls21 ~]$ hostname
az-ls21
[adpham1@az-ls21 ~]$ sudo iptables -vnL
Chain INPUT (policy DROP 47 packets, 3524 bytes)
 pkts bytes target     prot opt in     out     source               destination
 2147 1599K ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED
   12   544 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:80
    3   180 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22
  290 50289 ACCEPT     all  --  *      *       168.63.129.16        0.0.0.0/0

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 1235 packets, 190K bytes)
 pkts bytes target     prot opt in     out     source               destination
 2144  589K ACCEPT     all  --  *      *       0.0.0.0/0            168.63.129.16
[adpham1@az-ls21 ~]$ sudo iptables -vnL -t nat
Chain PREROUTING (policy ACCEPT 7 packets, 340 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain INPUT (policy ACCEPT 7 packets, 340 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 264 packets, 17183 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain POSTROUTING (policy ACCEPT 264 packets, 17183 bytes)
 pkts bytes target     prot opt in     out     source               destination
[adpham1@az-ls21 ~]$
```