https://linkedin.com/in/prafulpatel16

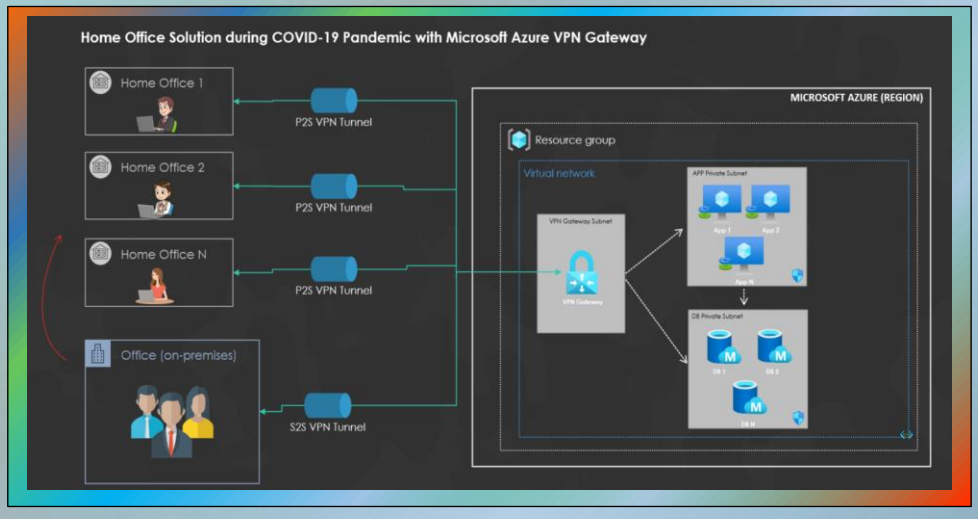
https://github.com/prafulpatel16

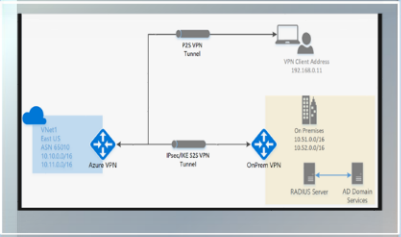
AZURE PROJECT

PROJECT-4: HOME OFFICE SOLUTION DURING COVID-19 PANDEMIC

WITH MICROSOFT AZURE VPN GATEWAY

IMPLETENTED BY: PRAFUL PATEL





Date: MAY 25, 2022

➢ Project Definition:

HOME OFFICE SOLUTION DURING COVID-19 PANDEMIC WITH MICROSOFT AZURE VPN GATEWAY

➢ Project Description:

Web Application Name: Portfolio web application
VPN Solution: Point-to-Site VPN

An IT services Provider Company **PRAfect Systems Inc.** is engaged into providing Cloud/DevOps & software development solutions. Recently, the company had to run into some work challenges after pandemic hit and they have decided to shift the employee to start working from home model. In order to work from home model there was a challenge to access company's internal web portal **"Portfolio web Application"** within the private environment on which the employee were working on that project. The management people decided to move their entire workload to the Microsoft Azure, hence the home-office solution should be within the Azure cloud. The requirement was generated by the management to the Cloud infrastructure team to find out the proposed relevant solution from the Microsoft Azure and come up with the project implementation plan.

After few day's research and analysis an infrastructure team has approached with the proposed solution of this challenge. The solution would be to implement **P2S VPN** so that home-office workers will use their computers to close and encrypted tunnel between their environments with Azure.

This way when the connection VPN is closed, the employee who is connected, for example, to Home Office 1, will be able to access the resources if he is a member of the cloud team.

This project demonstrates an experience of deploying P2S (Point-to-site configuration) and configuring a remote office-home work solution through which workers can access the company's web portal privately.

➢ Solution:

A Point-to-Site (P2S) VPN gateway connection lets you create a secure connection to your virtual network from an individual client computer. A P2S connection is established by starting it from the client computer. This solution is useful for telecommuters who want to connect to Azure VNets from a remote location, such as from home or a conference. P2S VPN is also a useful solution to use instead of S2S VPN when you have only a few clients that need to connect to a VNet.

- Protocols P2S use:

1. Secure Socket Tunneling Protocol (SSTP): TCP 443
2. OpenVPN: TCP 443
3. IKEv2 VPN: TCP 443

- P2S VPN Clients authentication method:
  1. Authenticate using native Azure certificate authentication
  2. Authenticate using native Azure Active Directory authentication

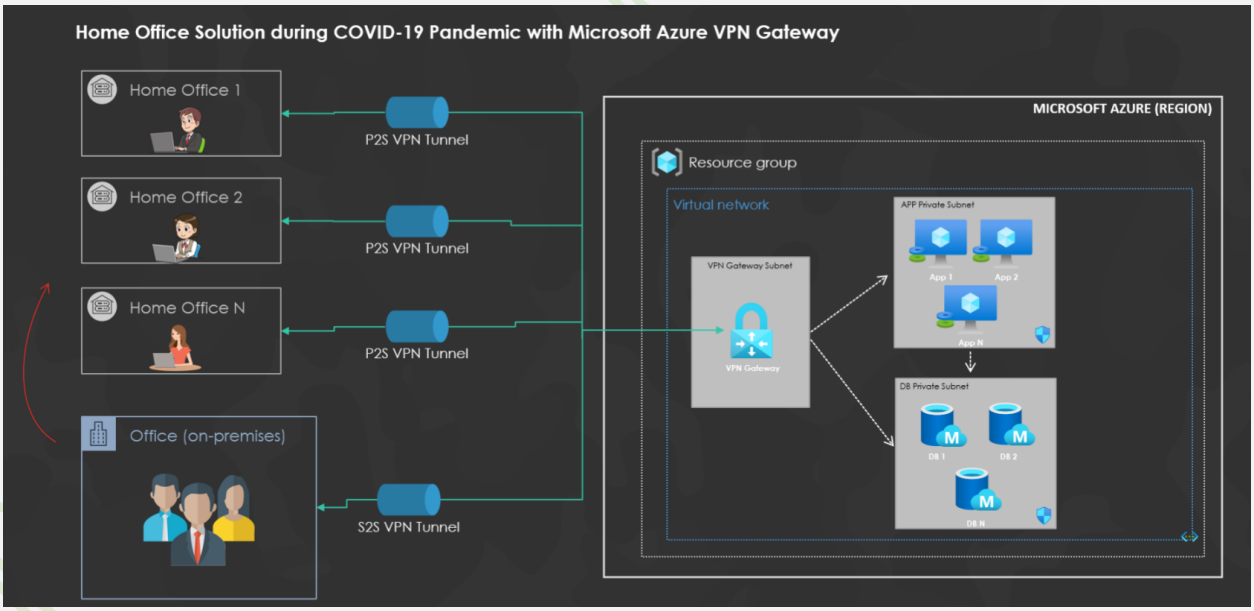
➢ Project Cost Estimation:

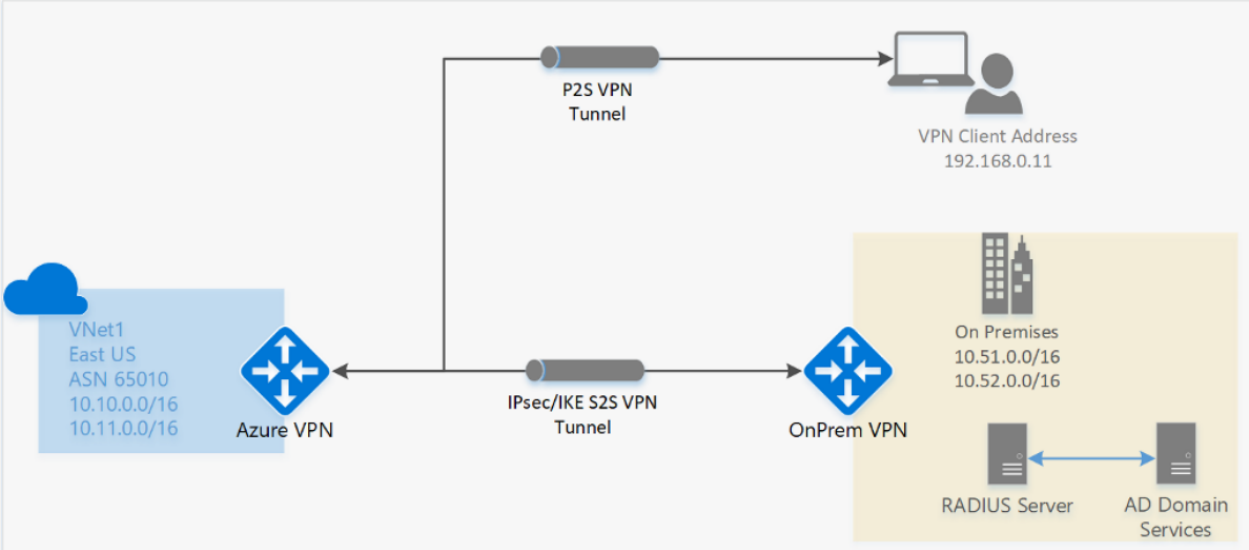
(Note: This cost is Not any actual cost, it's just an estimation based on high level requirement. Price may be vary based on adding and removing services based on requirement.)

➢ Tools & Technologies covered:

- Azure VNet
- Azure VM
- Azure VPN Gateway
- Azure VPN

➢ Solution Architecture:





This project will be completed in 6 implementation phases.

- **Project implementation Phase:**

  - Phase 1: Deploy networking components
  - Phase 2: Deploy Virtual Machine
  - Phase 3: Deploy VPN gateway
  - Phase 4: Deploy Azure VPN
  - Phase 5: Install and configure web application server
  - Phase 6: Test web application accessibility within internal private connection.

- **Implementation:**

  - Phase 1: Deploy networking components
    1. Go to Azure Virtual Networks
    2. Create a Azure vNet
  - Phase 2: Deploy Virtual Machine
    1. Go to Virtual machines
    2. Create Virtual machine
  - Phase 3: Deploy VPN gateway
    1. Go to Virtual network gateway
    2. Select gateway type: VPN
    3. Select VPN Type: Route-based
    4. Configure P2S (Point-2-site configuration)
  - Phase 4: Deploy Azure VPN
    1. Download Azure VPN client
    2. Install certificate on azure vpn
    3. Establish the VPN connection from local laptop
  - Phase 5: Install and configure web application server

1. Create a small bash script to configure apache application server
2. Provide web application source code within the bash script
3. Go to vm and run the bash script to install the web application

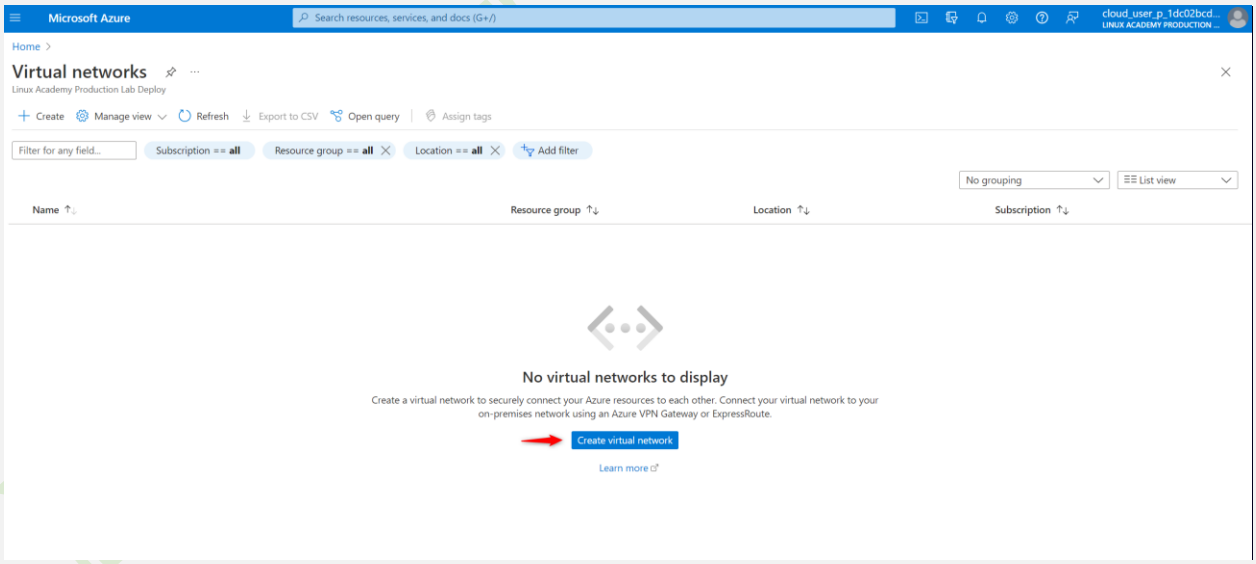
- Phase 6: Test web application accessibility within internal private connection
  1. Access local terminal from on-premise
  2. Copy the private ip of the VM
  3. Ping the private ip, it should be successful
  4. Go to Browser and hit the private ip
  5. Verify that 'Portfolio web application' is accessible from browser

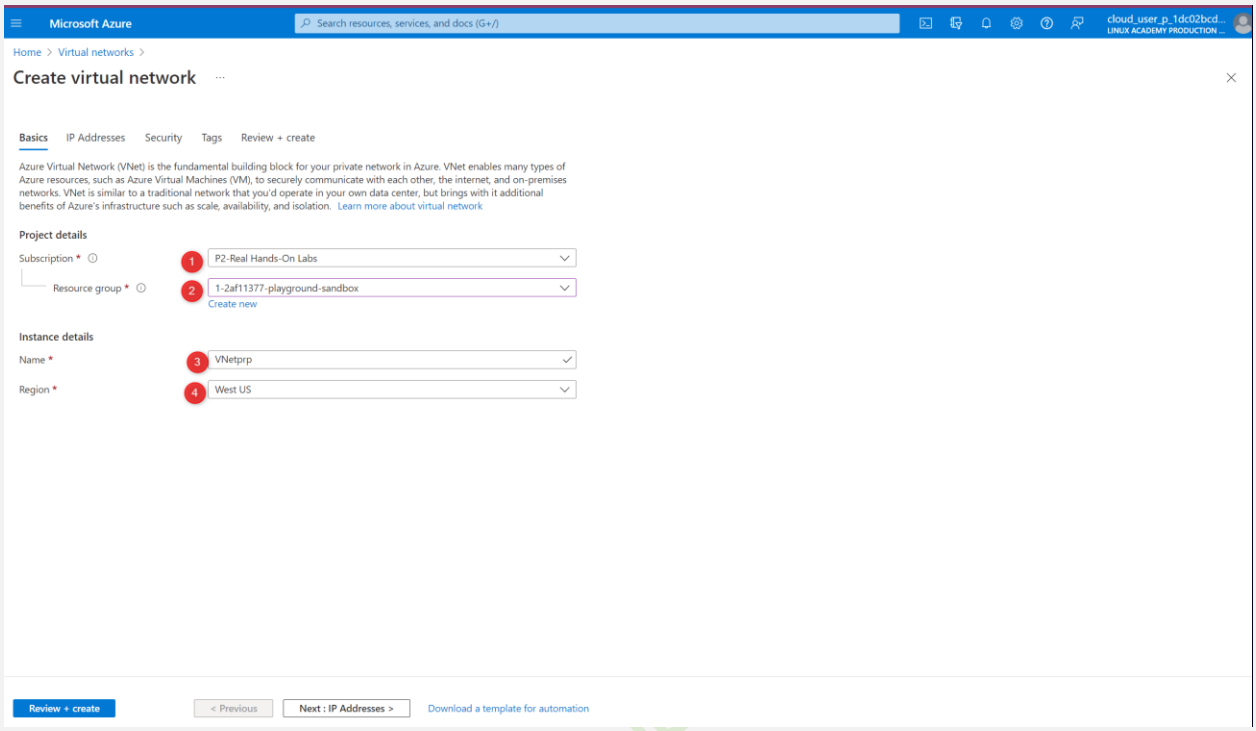
➢ Implementation in an Action:

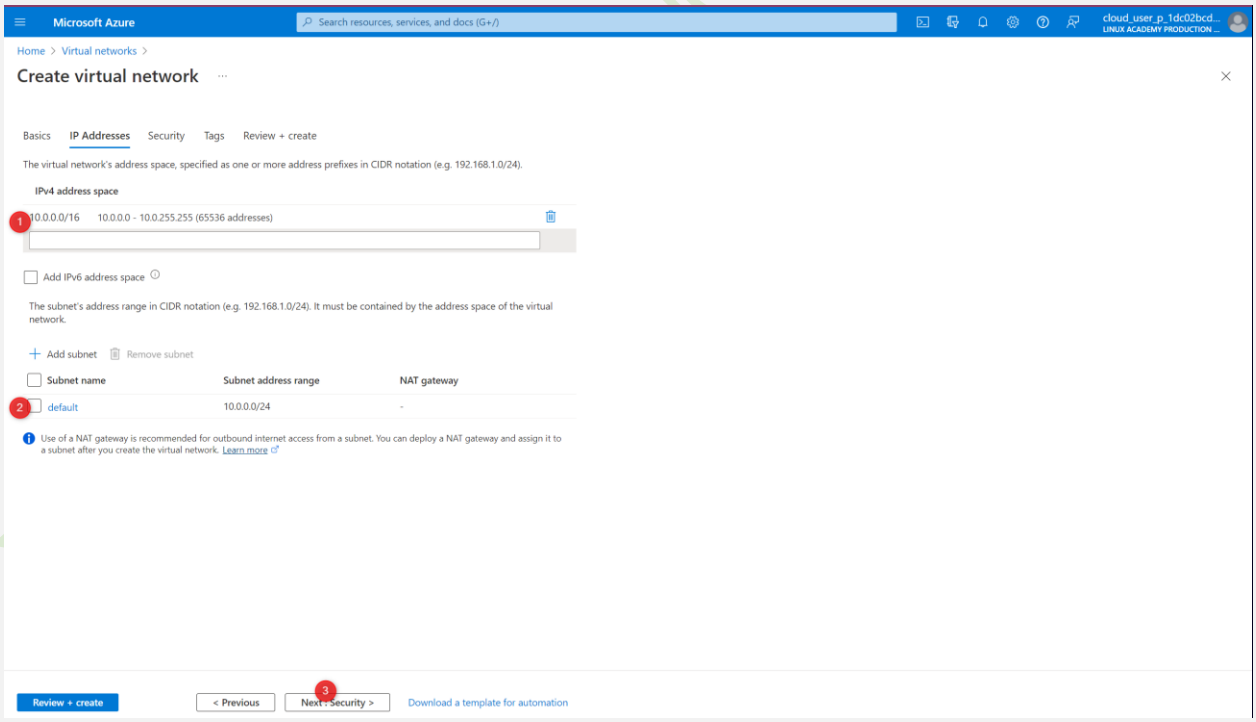
Home Office Solution during COVID-19 Pandemic with Microsoft Azure VPN Gateway

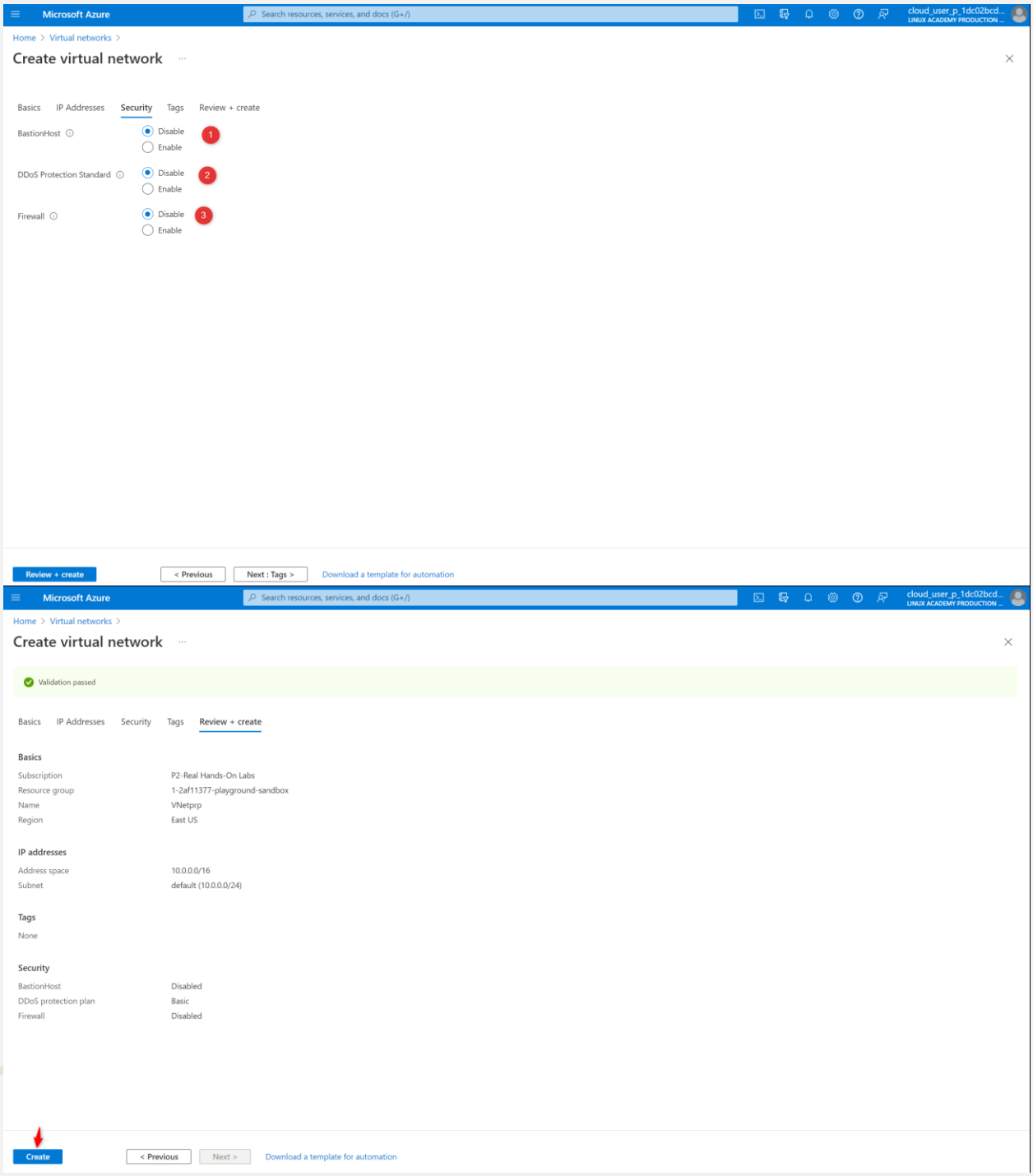
- Phase 1: Deploy networking components

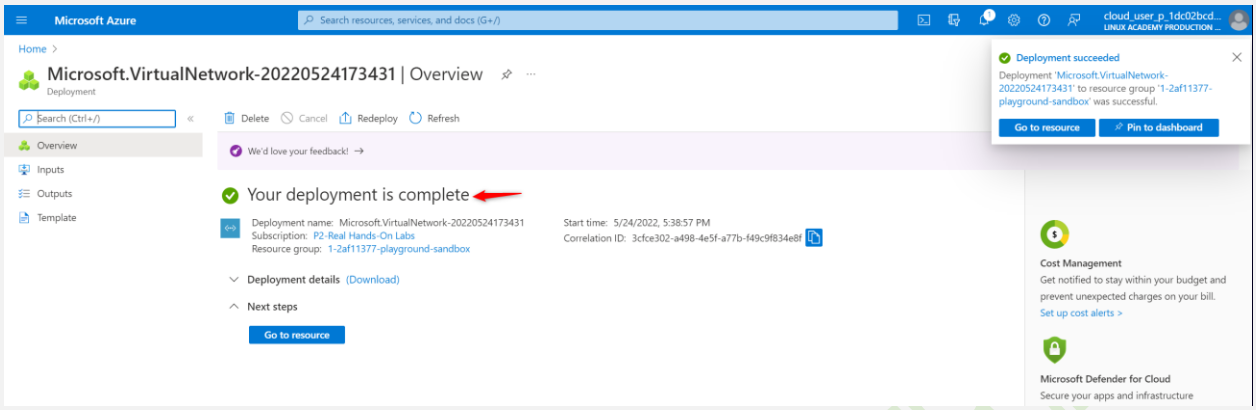
- Creating VNetprp

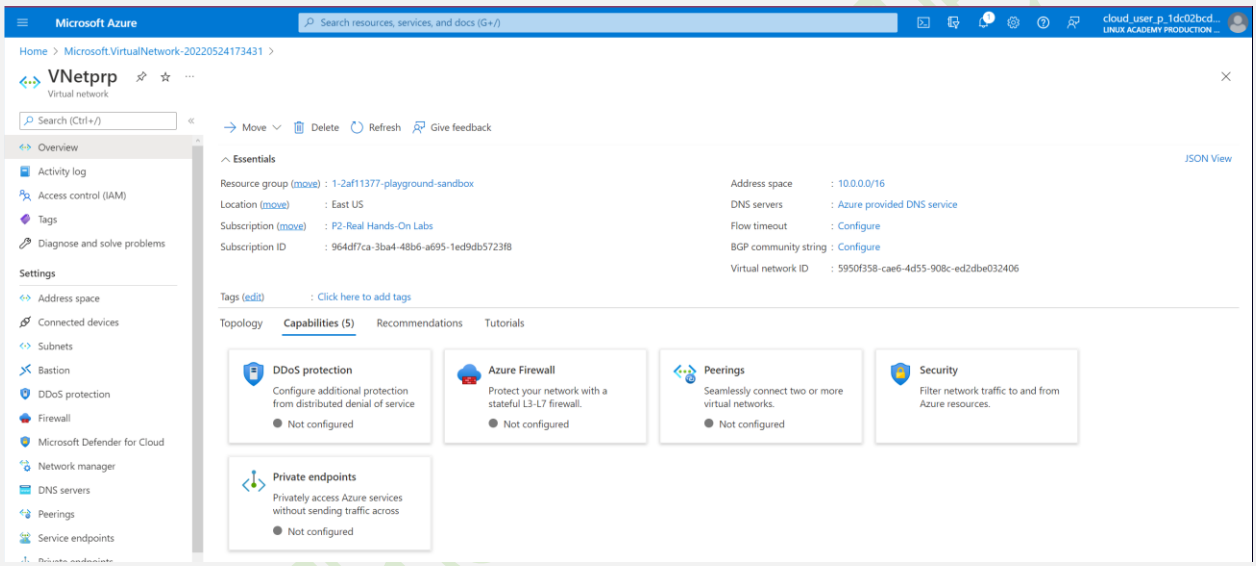



Microsoft Azure
Search resources, services, and docs (G+/)
cloud_user_p_1dc02bcd...
LINUX ACADEMY PRODUCTION ...
Home > Virtual networks >
Create virtual network
Basics
IP Addresses
Security
Tags
Review + create
Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks. VNet is similar to a traditional network that you'd operate in your own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation. Learn more about virtual network
Project details
Subscription *
1
P2-Real Hands-On Labs
Resource group *
2
1-2af11377-playground-sandbox
Create new
Instance details
Name *
3
VNetprp
Region *
4
West US
Review + create
< Previous
Next : IP Addresses >
Download a template for automation


Microsoft Azure
Search resources, services, and docs (G+/)
cloud_user_p_1dc02bcd...
LINUX ACADEMY PRODUCTION ...
Home > Virtual networks >
Create virtual network
Basics
IP Addresses
Security
Tags
Review + create
The virtual network's address space, specified as one or more address prefixes in CIDR notation (e.g. 192.168.1.0/24).
IPv4 address space
1
10.0.0.0/16
10.0.0.0 - 10.0.255.255 (65536 addresses)
Add IPv6 address space
The subnet's address range in CIDR notation (e.g. 192.168.1.0/24). It must be contained by the address space of the virtual network.
Add subnet
Remove subnet
Subnet name
Subnet address range
NAT gateway
2
default
10.0.0.0/24
-
Use of a NAT gateway is recommended for outbound internet access from a subnet. You can deploy a NAT gateway and assign it to a subnet after you create the virtual network. Learn more
Review + create
< Previous
3
Next : Security >
Download a template for automation

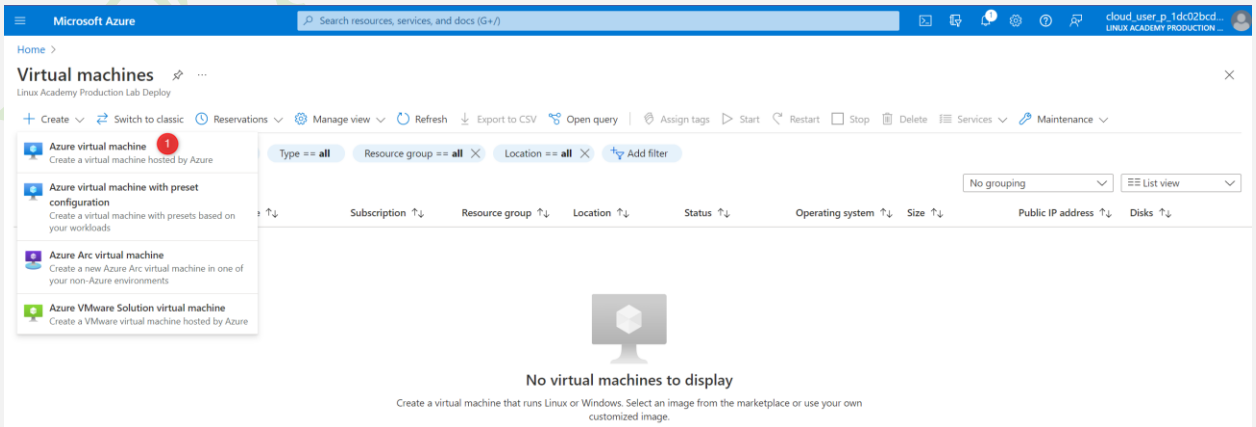

Microsoft Azure
Search resources, services, and docs (G+/)
cloud_user_p_1dc02bcd...
LINUX ACADEMY PRODUCTION ...
Home > Virtual networks >
Create virtual network
Basics
IP Addresses
Security
Tags
Review + create
BastionHost
Disable
Enable
1
DDoS Protection Standard
Disable
Enable
2
Firewall
Disable
Enable
3
Review + create
< Previous
Next : Tags >
Download a template for automation
Microsoft Azure
Search resources, services, and docs (G+/)
cloud_user_p_1dc02bcd...
LINUX ACADEMY PRODUCTION ...
Home > Virtual networks >
Create virtual network
Validation passed
Basics
IP Addresses
Security
Tags
Review + create
Basics
Subscription
P2-Real Hands-On Labs
Resource group
1-2af11377-playground-sandbox
Name
VNetprp
Region
East US
IP addresses
Address space
10.0.0.0/16
Subnet
default (10.0.0.0/24)
Tags
None
Security
BastionHost
Disabled
DDoS protection plan
Basic
Firewall
Disabled
Create
< Previous
Next >
Download a template for automation

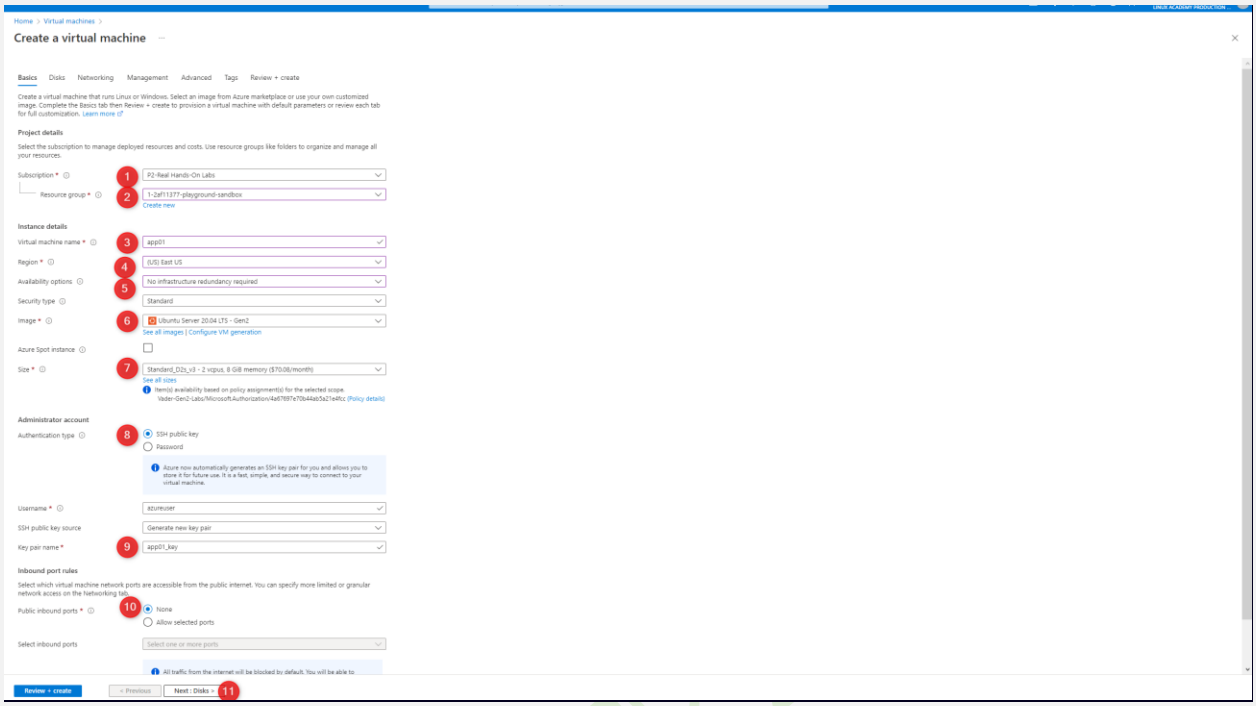


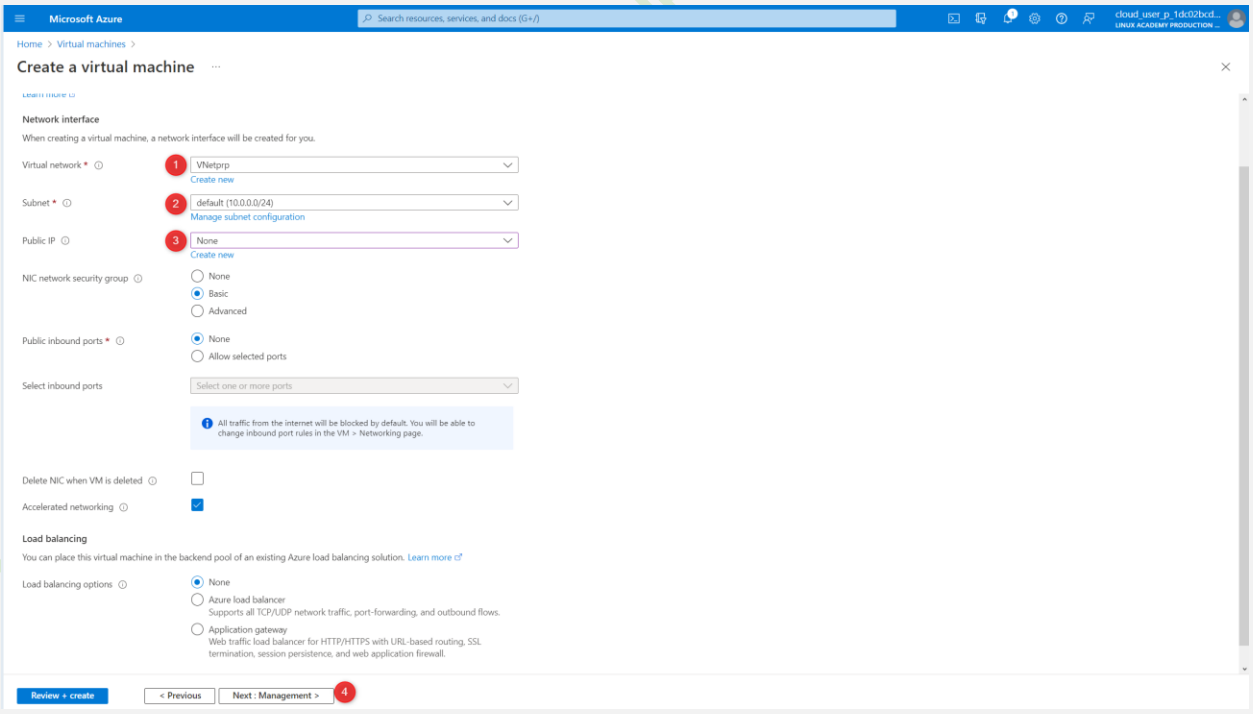


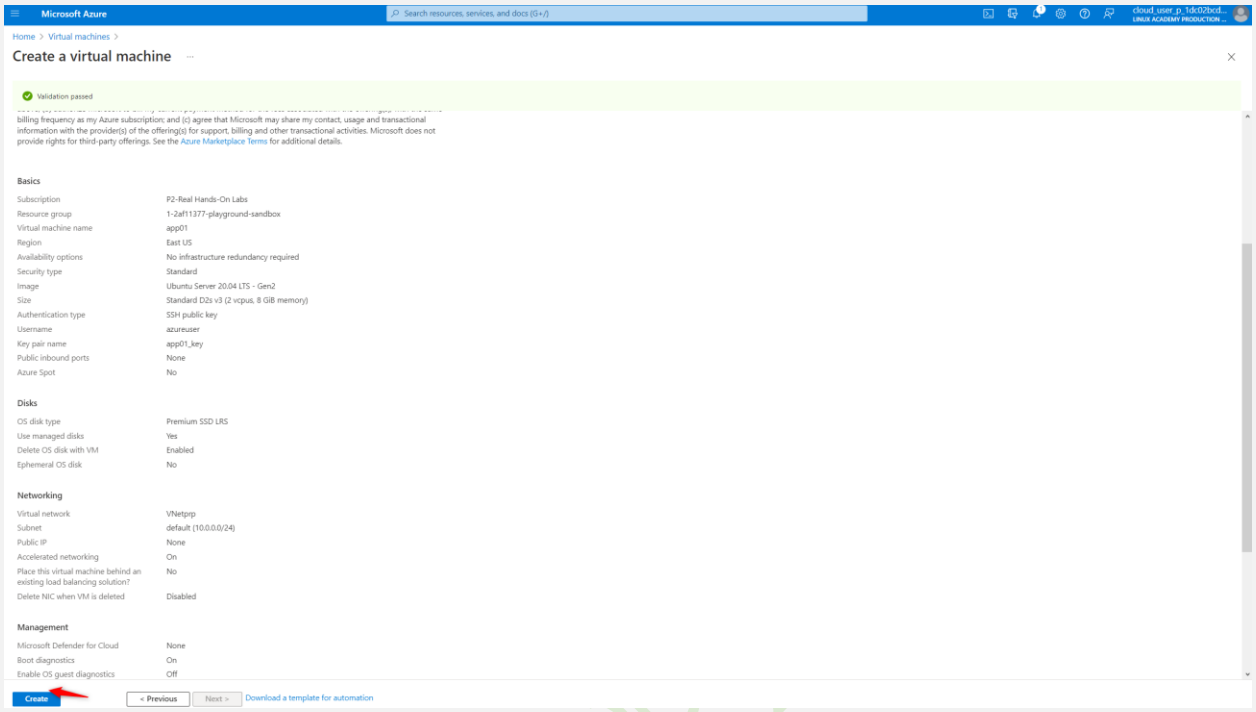
Phase 2: Deploy Virtual Machine

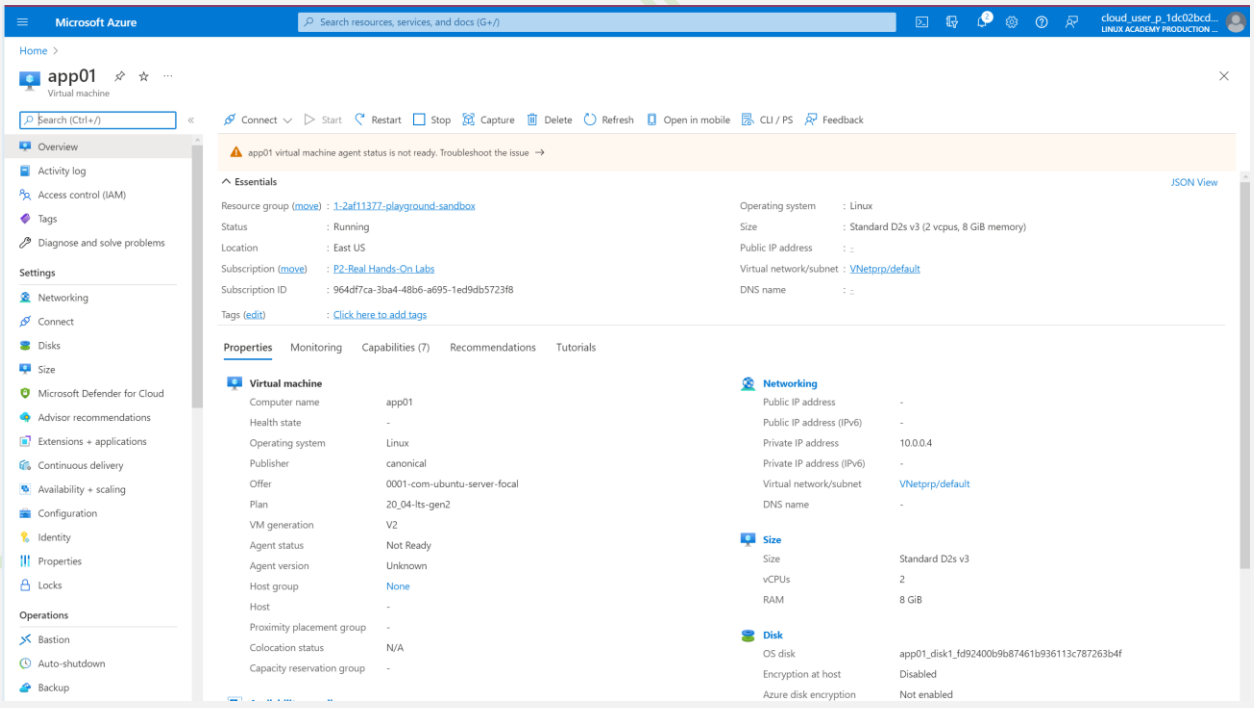
Create VM



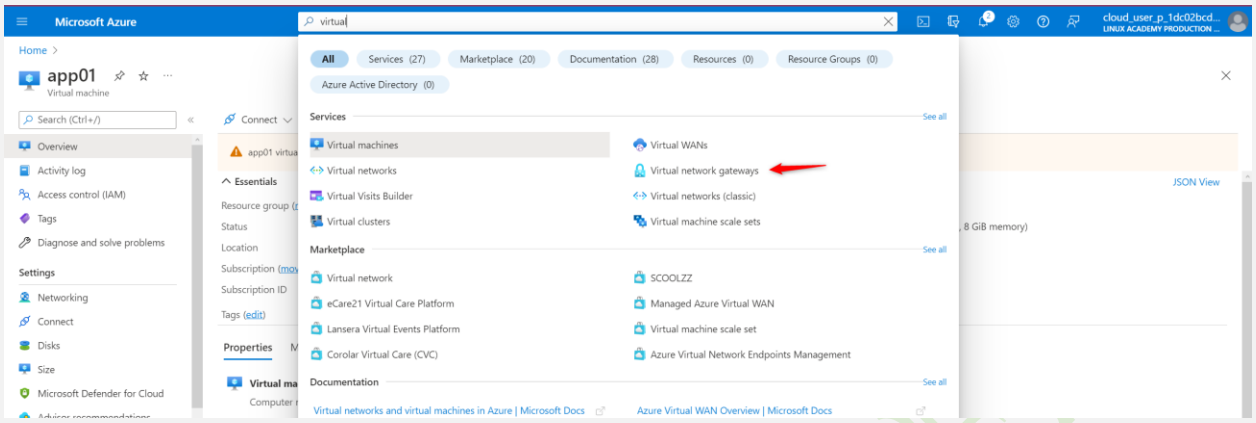

Home > Virtual machines >
Create a virtual machine
Basics Disks Networking Management Advanced Tags Review + create
Project details
Subscription *
Resource group *
Instance details
Virtual machine name *
Region *
Availability options
Security type
Image *
Azure Spot instance
Size *
Administrator account
Authentication type
Username *
SSH public key source
Key pair name *
Inbound port rules
Public inbound ports *
Select inbound ports
Review + create
< Previous
Next : Disks >
1
2
3
4
5
6
7
8
9
10
11


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Virtual machines >
Create a virtual machine
Network interface
When creating a virtual machine, a network interface will be created for you.
Virtual network *
Subnet *
Public IP
NIC network security group
Public inbound ports *
Select inbound ports
Delete NIC when VM is deleted
Accelerated networking
Load balancing
You can place this virtual machine in the backend pool of an existing Azure load balancing solution. Learn more
Load balancing options
Review + create
< Previous
Next : Management >
1
2
3
4

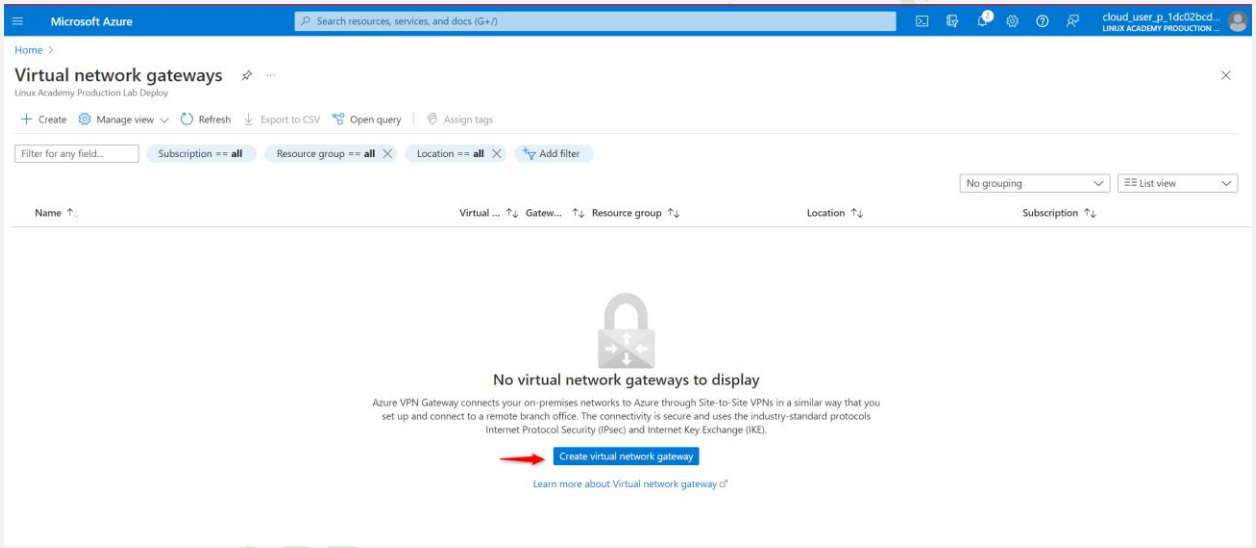


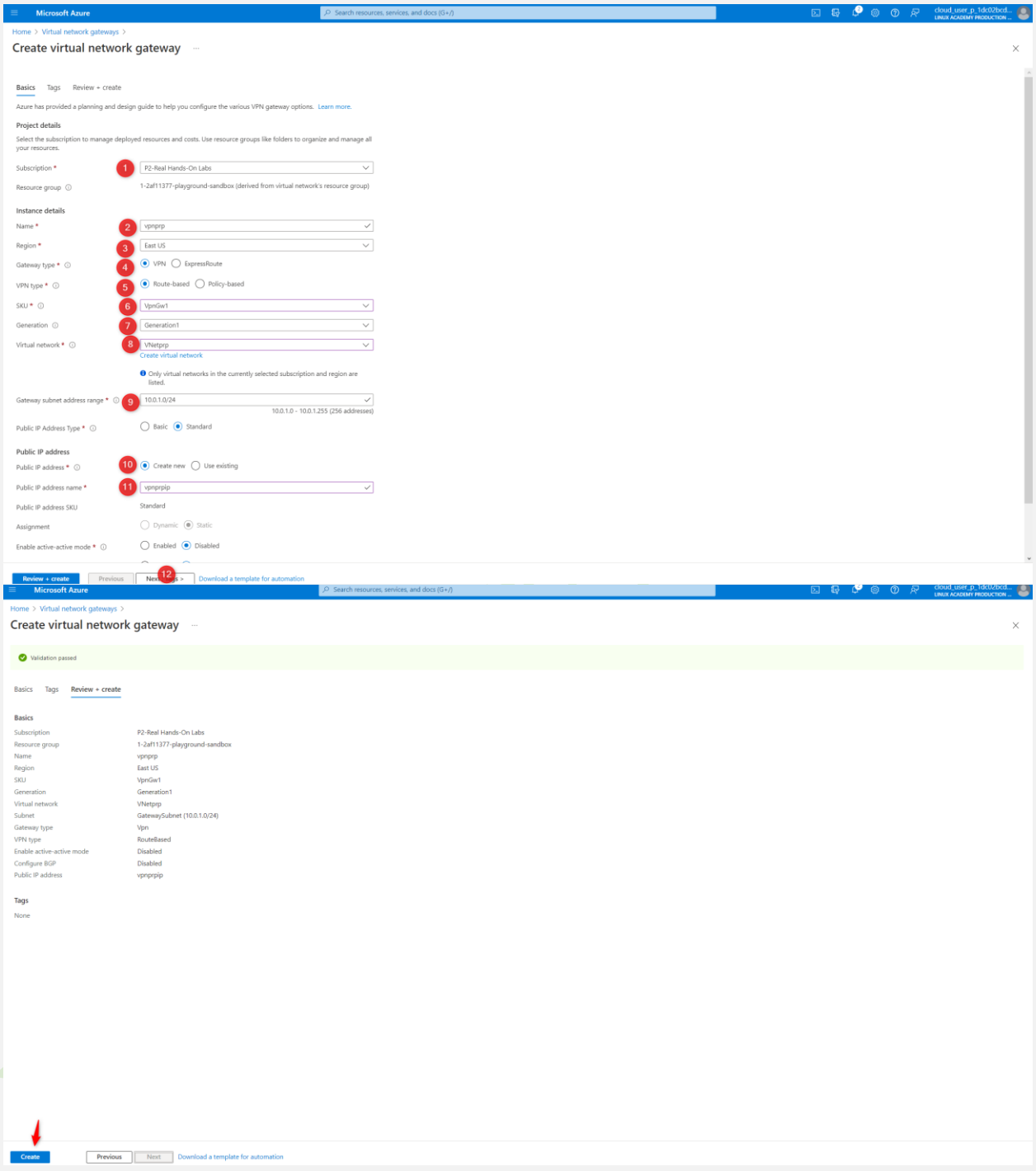


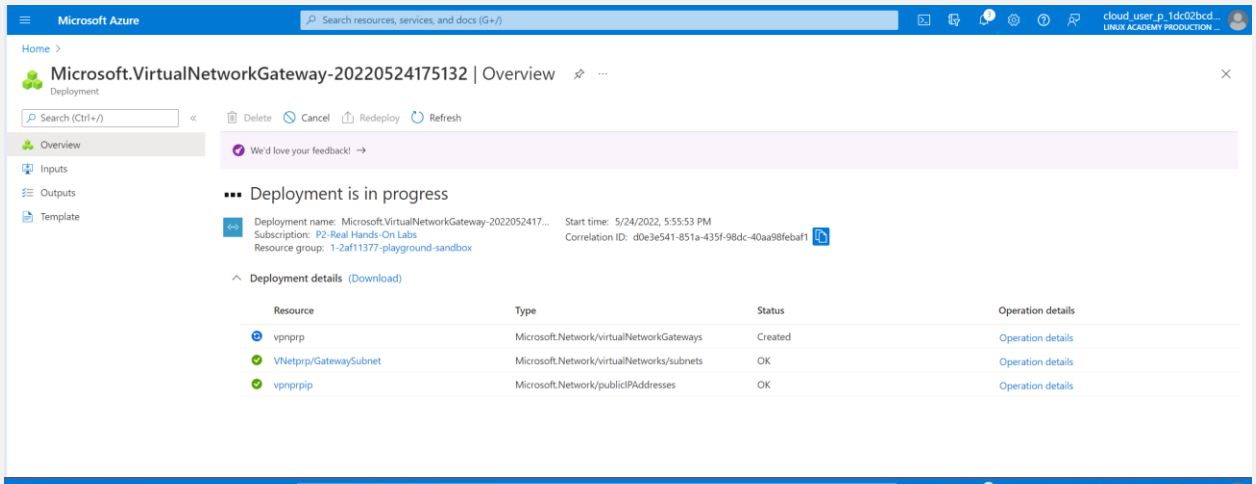
Create Virtual Private Gateway

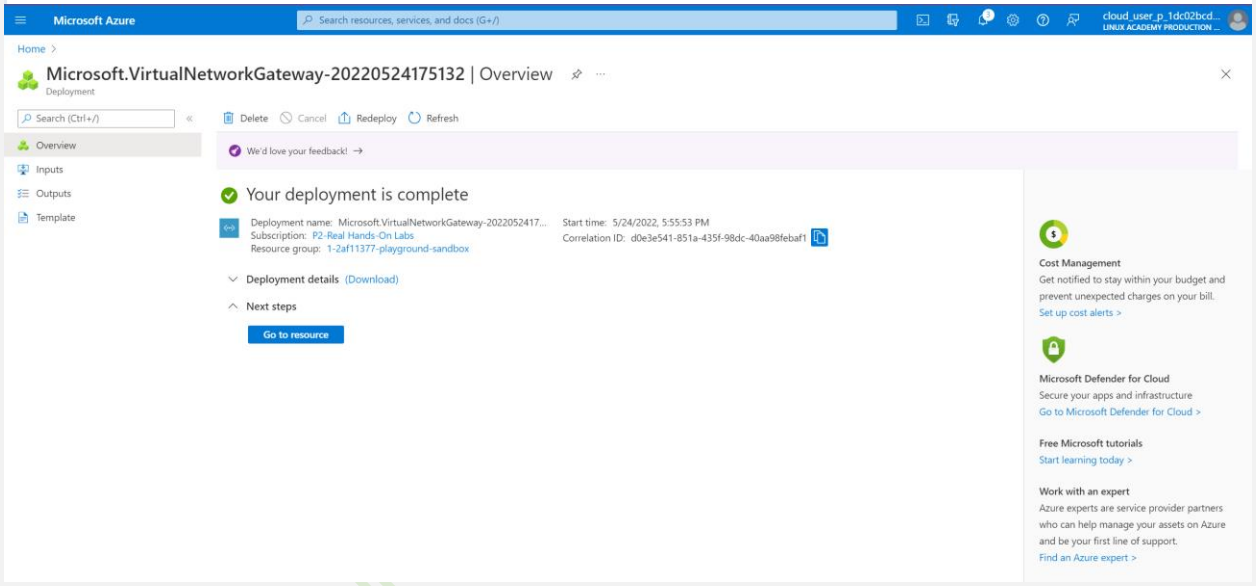


- Phase 3: Deploy VPN gateway



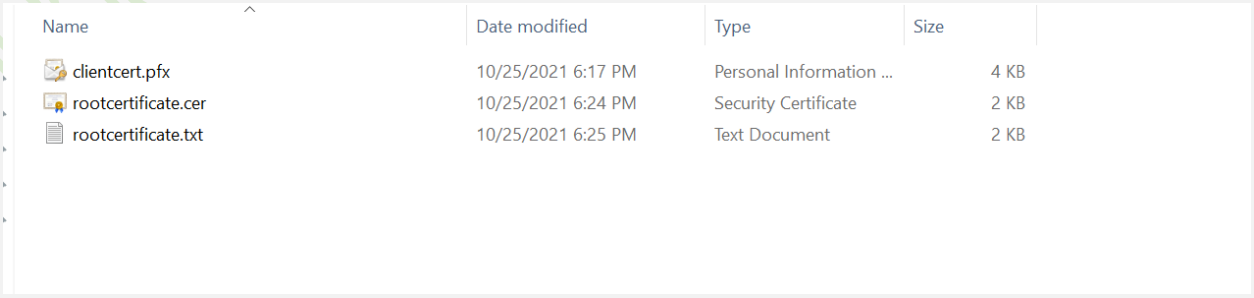

Microsoft Azure
Search resources, services, and docs (G+/)
Home > Virtual network gateways >
Create virtual network gateway
Basics
Tags
Review + create
Azure has provided a planning and design guide to help you configure the various VPN gateway options. Learn more.
Project details
Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.
Subscription *
1
P2-Real Hands-On Labs
Resource group
1-2af11377-playground-sandbox (derived from virtual network's resource group)
Instance details
Name *
2
vpnprp
Region *
3
East US
Gateway type *
4
VPN
ExpressRoute
VPN type *
5
Route-based
Policy-based
SKU *
6
VpnGw1
Generation
7
Generation1
Virtual network *
8
VNetprp
Create virtual network
Only virtual networks in the currently selected subscription and region are listed.
Gateway subnet address range *
9
10.0.1.0/24
10.0.1.0 - 10.0.1.255 (256 addresses)
Public IP Address Type *
Basic
Standard
Public IP address
Public IP address *
10
Create new
Use existing
Public IP address name *
11
vpnprpip
Public IP address SKU
Standard
Assignment
Dynamic
Static
Enable active-active mode *
Enabled
Disabled
Review + create
Previous
Next
12
Download a template for automation
Validation passed
Basics
Tags
Review + create
Subscription
P2-Real Hands-On Labs
Resource group
1-2af11377-playground-sandbox
Name
vpnprp
Region
East US
SKU
VpnGw1
Generation
Generation1
Virtual network
VNetprp
Subnet
GatewaySubnet (10.0.1.0/24)
Gateway type
Vpn
VPN type
RouteBased
Enable active-active mode
Disabled
Configure BGP
Disabled
Public IP address
vpnprpip
Tags
None
Create
Previous
Next
Download a template for automation



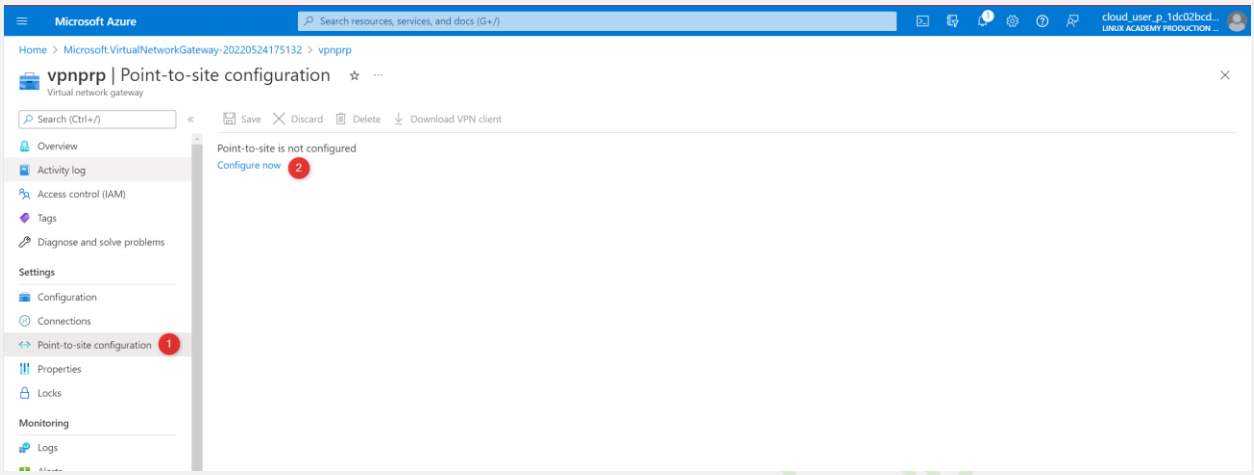


Phase 4: Deploy Azure VPN

- Downloading the certificates (see the attachment from the solution video page)



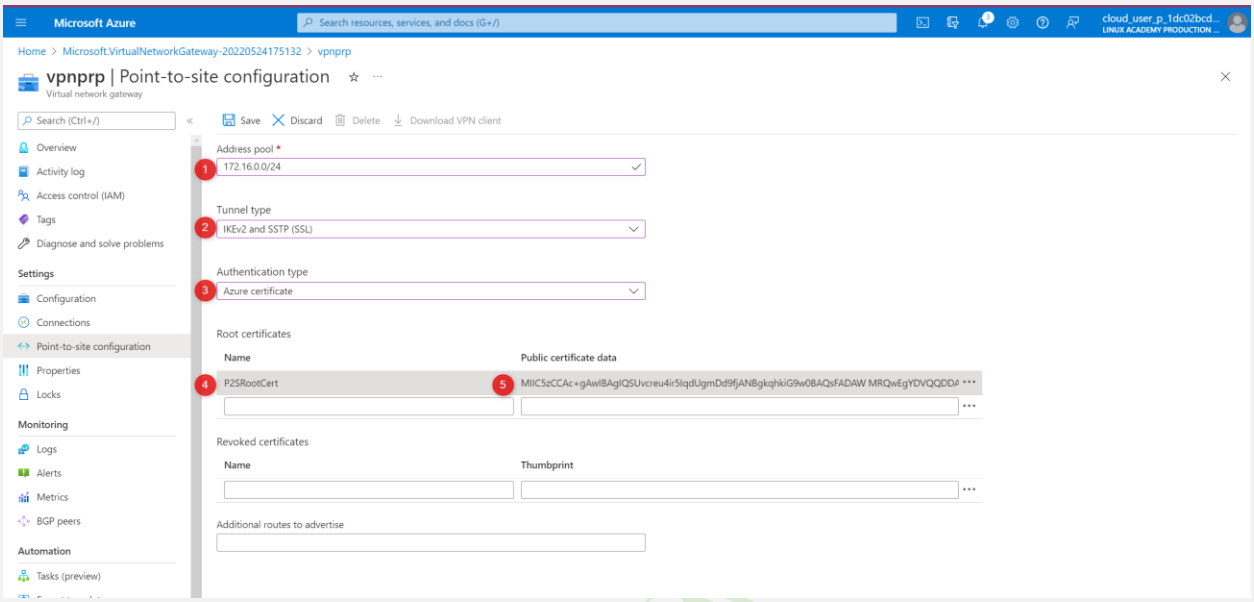
Configuring P2S VPN



Copy certificate

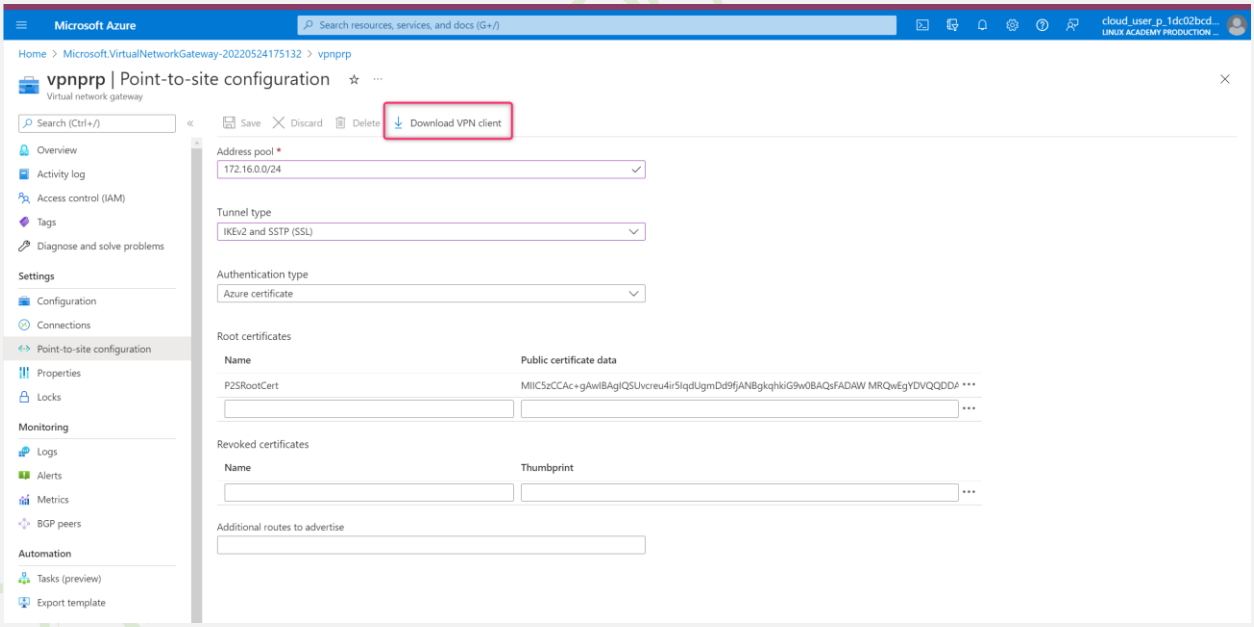
```
-----BEGIN CERTIFICATE-----
MIIC5zCCAc+gAwIBAgIQSUvcreu4ir5IqdUgmDd9fjANBgkqhkiG9w0BAQsFADAW
MRQwEgYDVQQDDAtQMlNSb290Q2VydDAeFw0yMTEwMjUyMzQ5MzdaFw0yMjEwMjYw
MDA5MzdaMBYxFDASBgNVBAMMC1AyU1Jvb3RDZXJ0MIIBIjANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEAy11RX/m3VU778d7nr2BygarpoT6B1DN3/72UXSv5kE8z
gt2XgORVoqiZ2CQ7okyI4UtMinU5cH3O8qMikryJ/oNq2k7pim1iuOGBNAEmyxPg
5u27JmiXtuYD0mDVdpXw8iJvZ4DuK890XViiUX2i5VcCS6ZkN3WK0ORLDlBDSvIr
6FM4GBphQQaG1fz9eyB4ED1xBJrOkJoQKTTZBp0Se1gKLB2Dv2lYY5w8rgsKz8Il
7I2WWmbSRv++pZp54ybJMRHiqF26O6qICOZT9KLQjpZwWSC0qEW4CaCQkl+yG6Bg
ZdEX+QbroqaYoiCN02R7WltZkuw2ltMM2mphDM9F2QIDAQABozEwLzAOBgNVHQ8B
Af8EBAMCAgQwHQYDVR0OBBYEFLYOcYlaalpwl0wMay/qkIYsiiuMMA0GCSqGSIb3
DQEBCwUAA4IBAQC2PUYcma6kVASk9NoLUPD6lYWgHtdPe0d1Whxh9TUztK3bsQLH
y82aQNSwXpOiIWW2l1jQsmnaL2PAUoplJm6g1W5CdEZTDiWU+uoSMQywtMikTG7o
NI6h/guv3fx3vI8BBHtPgUlgsVwlRUJ0OV74Hxmaw4TprUkE4zUkPoEpG+ynZo4a
OR9SwD2zUlbR8PkJtwlFKkn6Zx1+rfb2Q1d/zvZk5qLChanUnA1iJB0oVfc/aDxQ
t7xccyRH1YAXWxNOirTF6RIWPt4BD+WZwcJ0nNXwF1sAAuqxLXEd0Gg+YoUUHngQ
V+NXLdu6hMCZOyKKHLEXk0DRgogjAgsmakkz
-----END CERTIFICATE-----
```

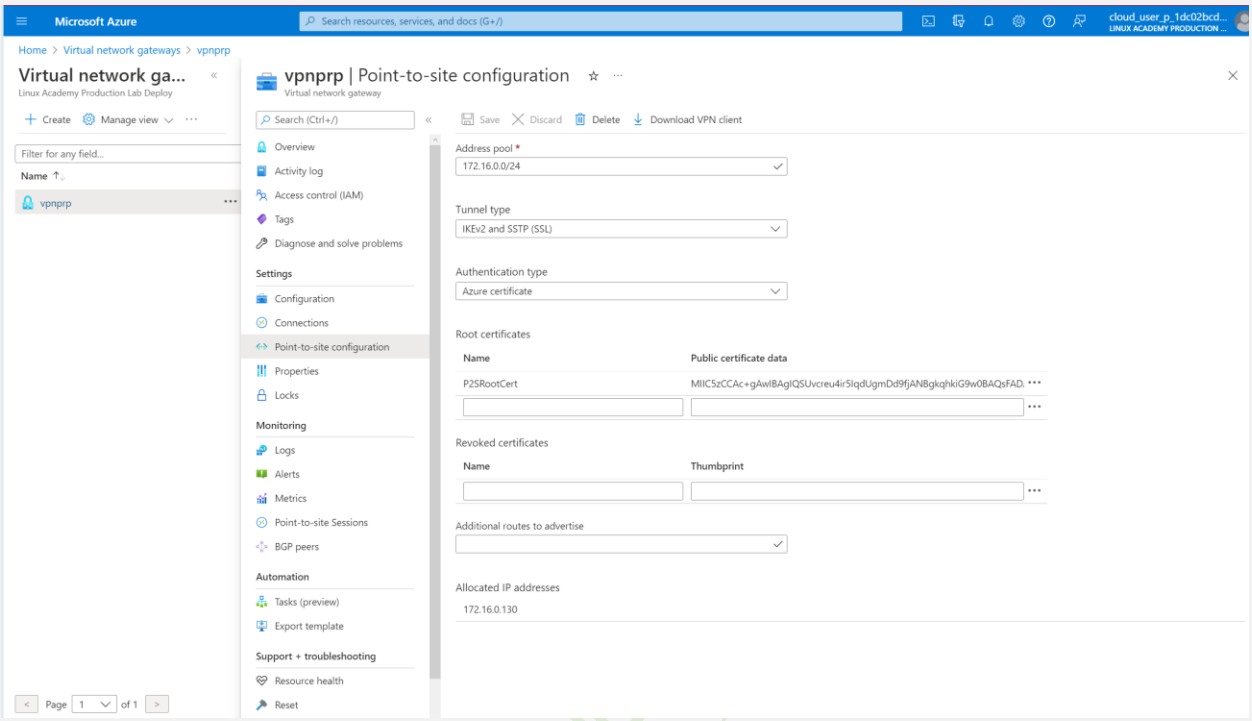
- Adding a pool of IPs (range): 172.16.0.0/24



Wait till the SAVE is complete and “Download VPN Client” option gets enabled

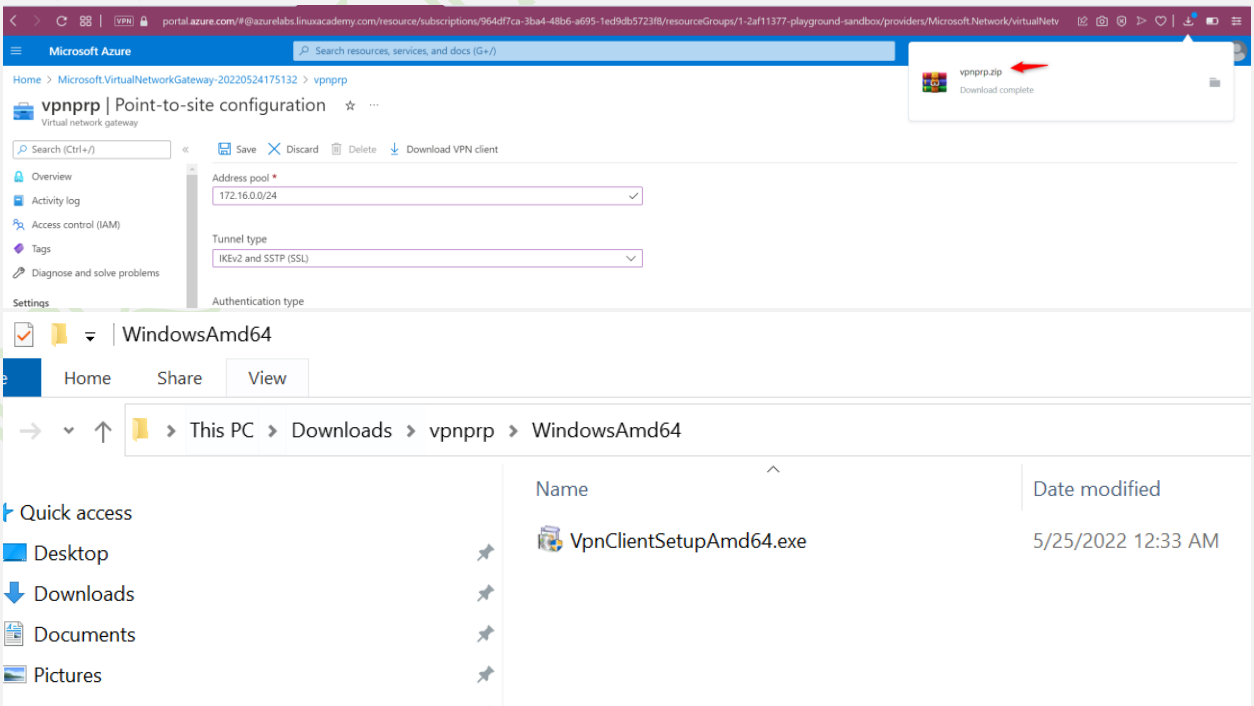
- Generating and installing VPN Azure

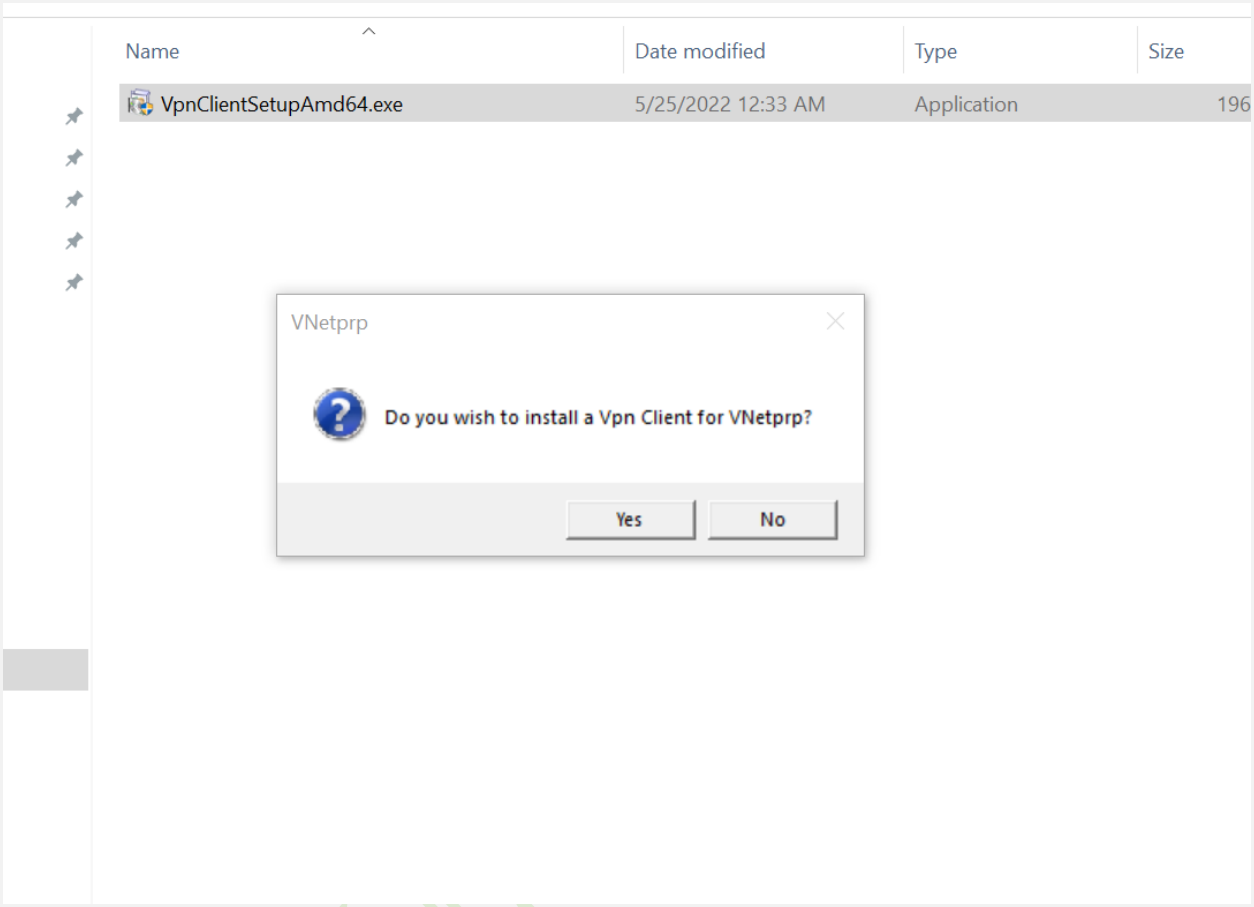


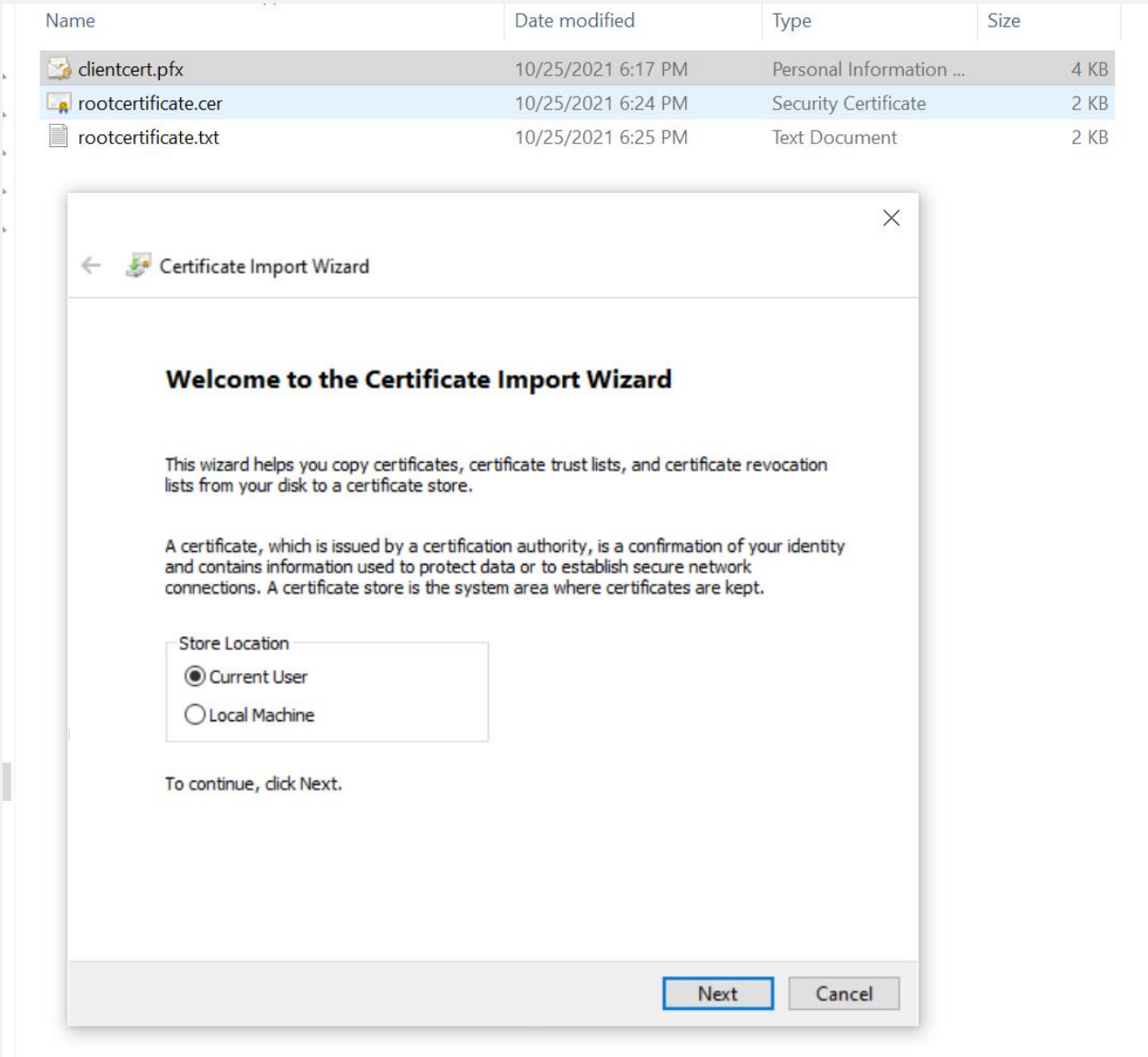


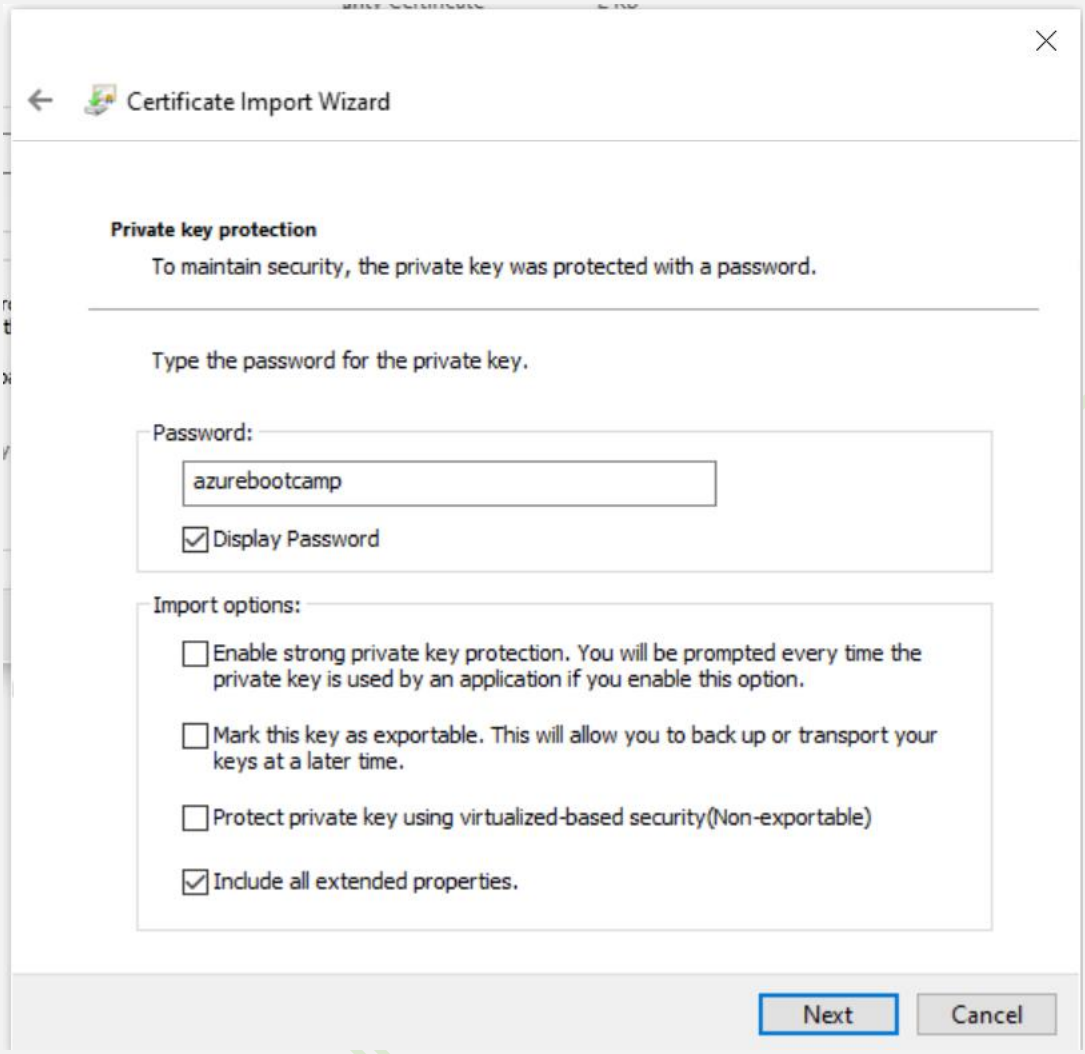
Remote connection via VPN:

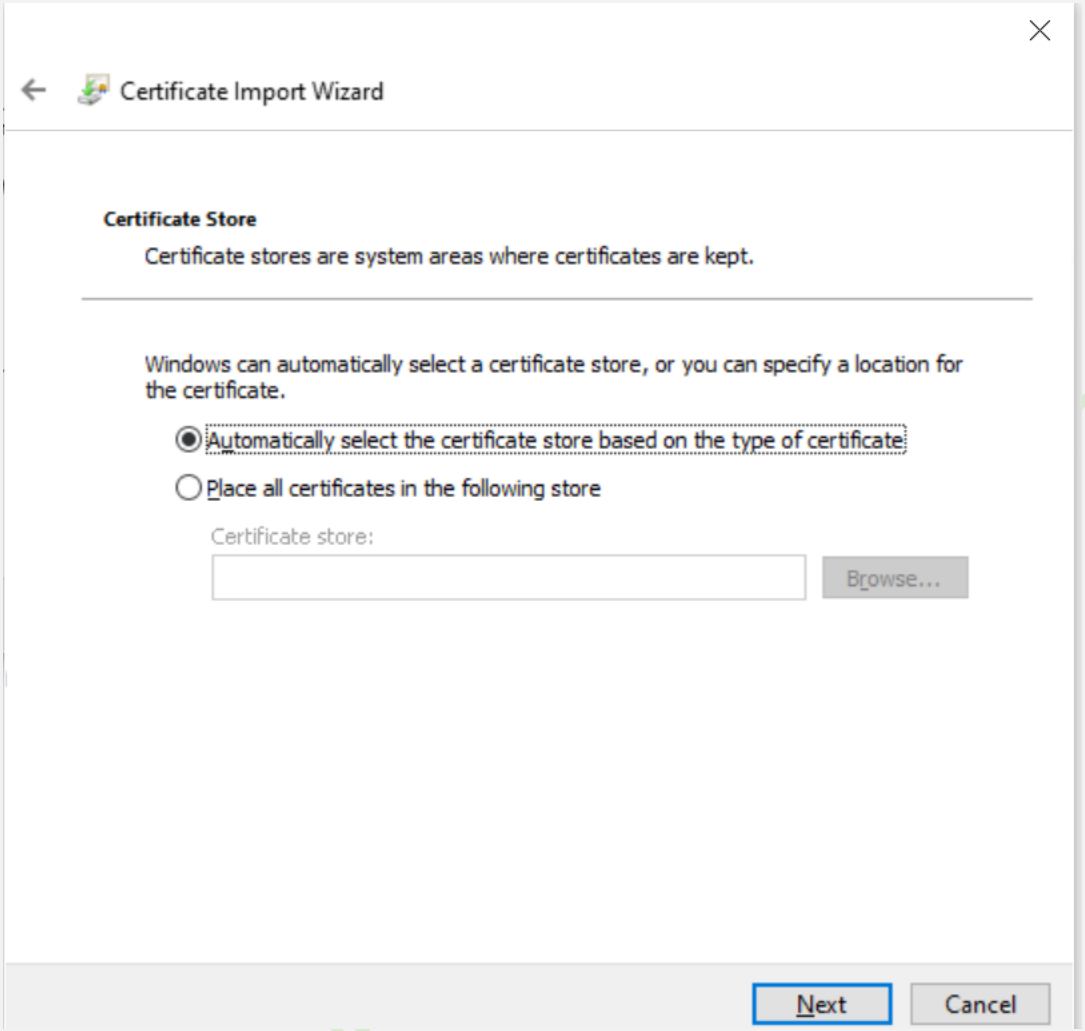
- Installing the certificate
Password: azurebootcamp
Unzip the vpn and install

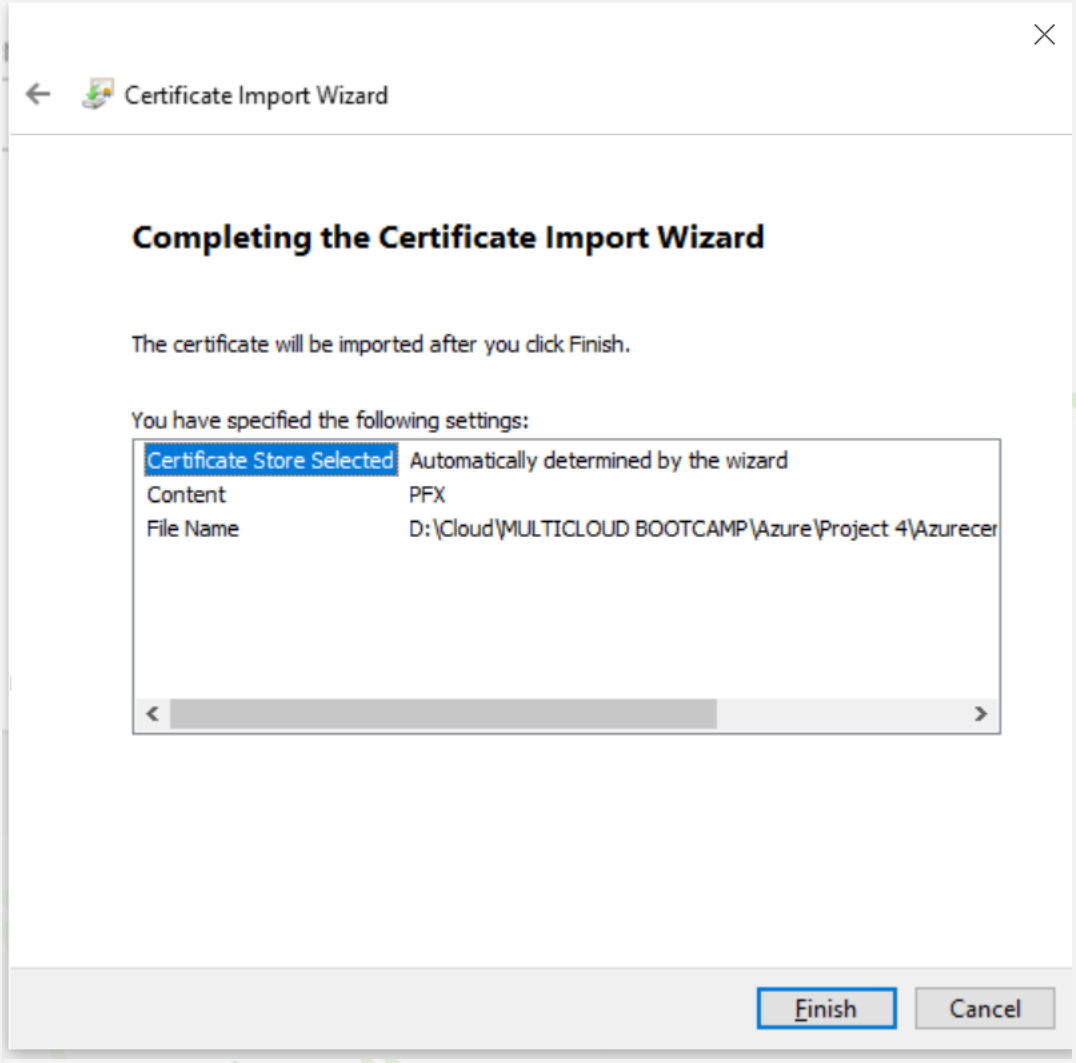


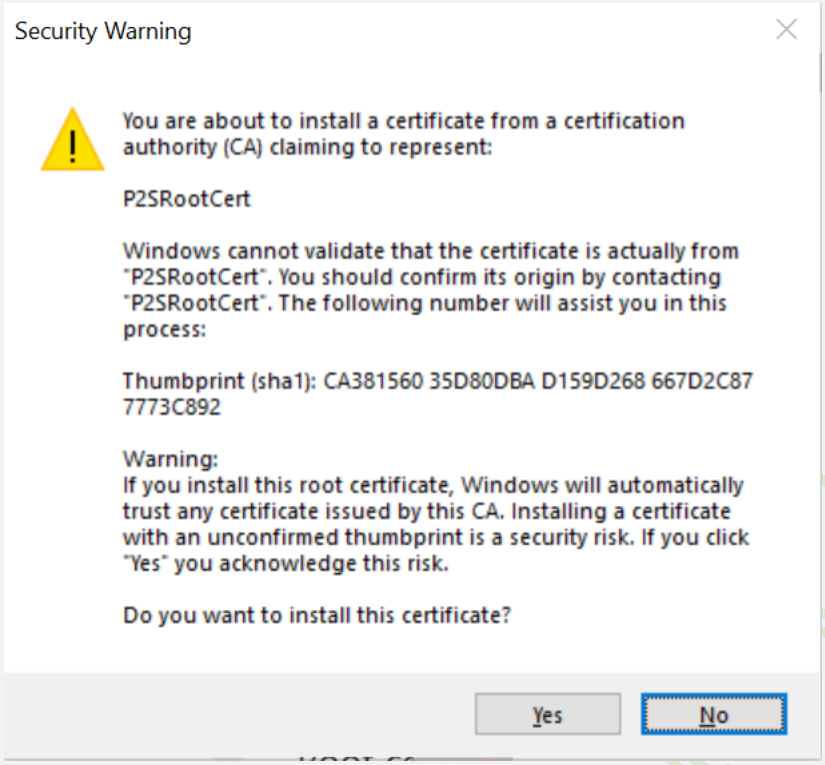

Name
Date modified
Type
Size
VpnClientSetupAmd64.exe
5/25/2022 12:33 AM
Application
196
VNetprp
Do you wish to install a Vpn Client for VNetprp?
Yes
No

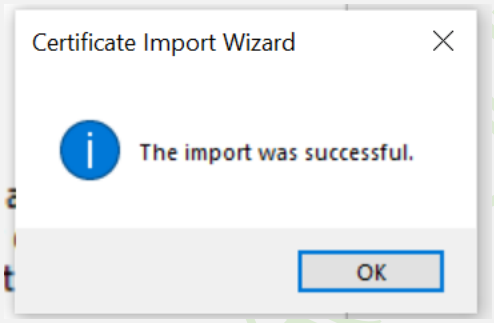

Name
Date modified
Type
Size
clientcert.pfx
10/25/2021 6:17 PM
Personal Information ...
4 KB
rootcertificate.cer
10/25/2021 6:24 PM
Security Certificate
2 KB
rootcertificate.txt
10/25/2021 6:25 PM
Text Document
2 KB
Certificate Import Wizard
Welcome to the Certificate Import Wizard
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
Store Location
Current User
Local Machine
To continue, click Next.
Next
Cancel


Certificate Import Wizard
Private key protection
To maintain security, the private key was protected with a password.
Type the password for the private key.
Password:
azurebootcamp
Display Password
Import options:
Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.
Mark this key as exportable. This will allow you to back up or transport your keys at a later time.
Protect private key using virtualized-based security(Non-exportable)
Include all extended properties.
Next
Cancel

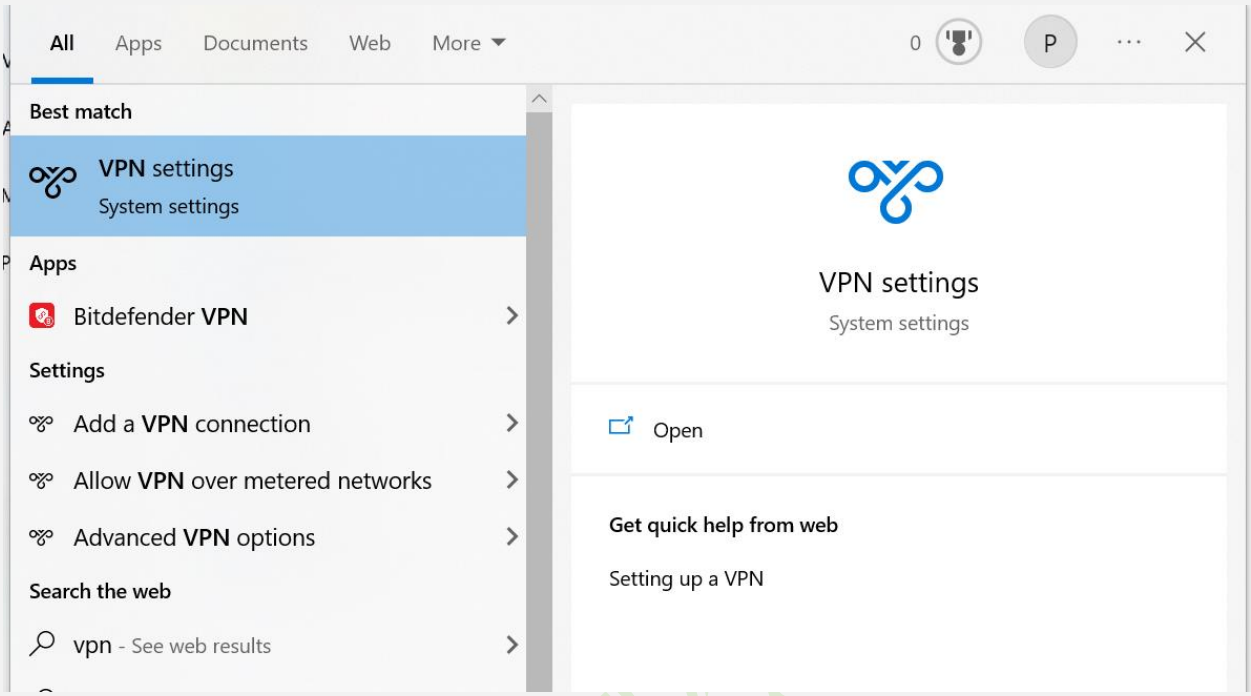

Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for the certificate.
Automatically select the certificate store based on the type of certificate
Place all certificates in the following store
Certificate store:
Browse...
Next
Cancel


Certificate Import Wizard
Completing the Certificate Import Wizard
The certificate will be imported after you click Finish.
You have specified the following settings:
Certificate Store Selected
Automatically determined by the wizard
Content
PFX
File Name
D:\Cloud\MULTICLOUD BOOTCAMP\Azure\Project 4\Azurecer
Finish
Cancel

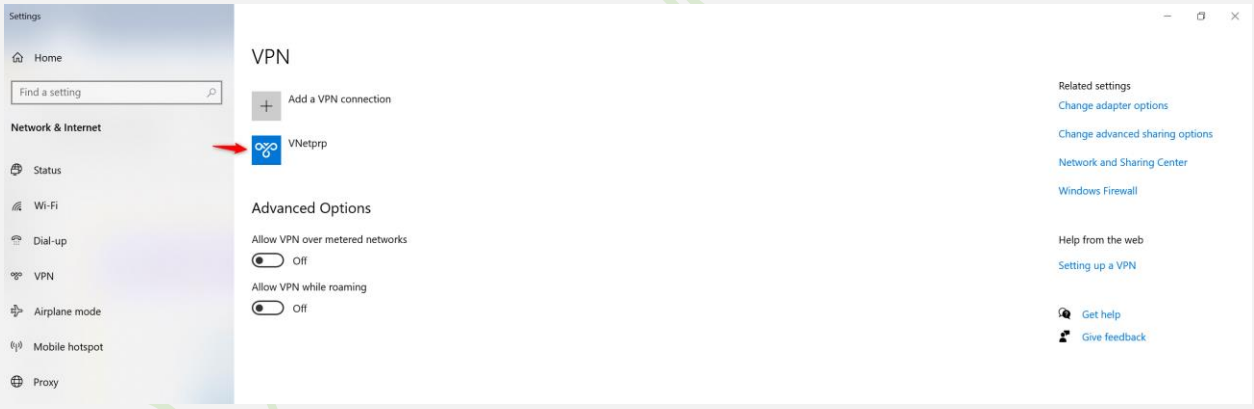




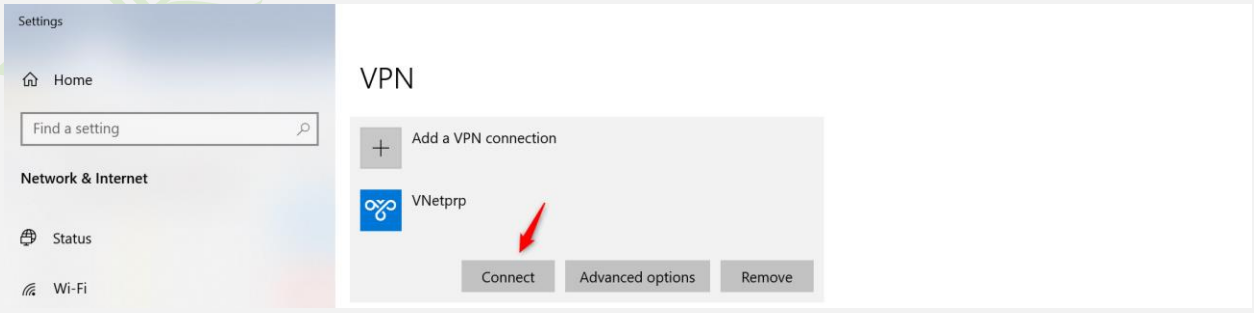
Now Search for installed VPN

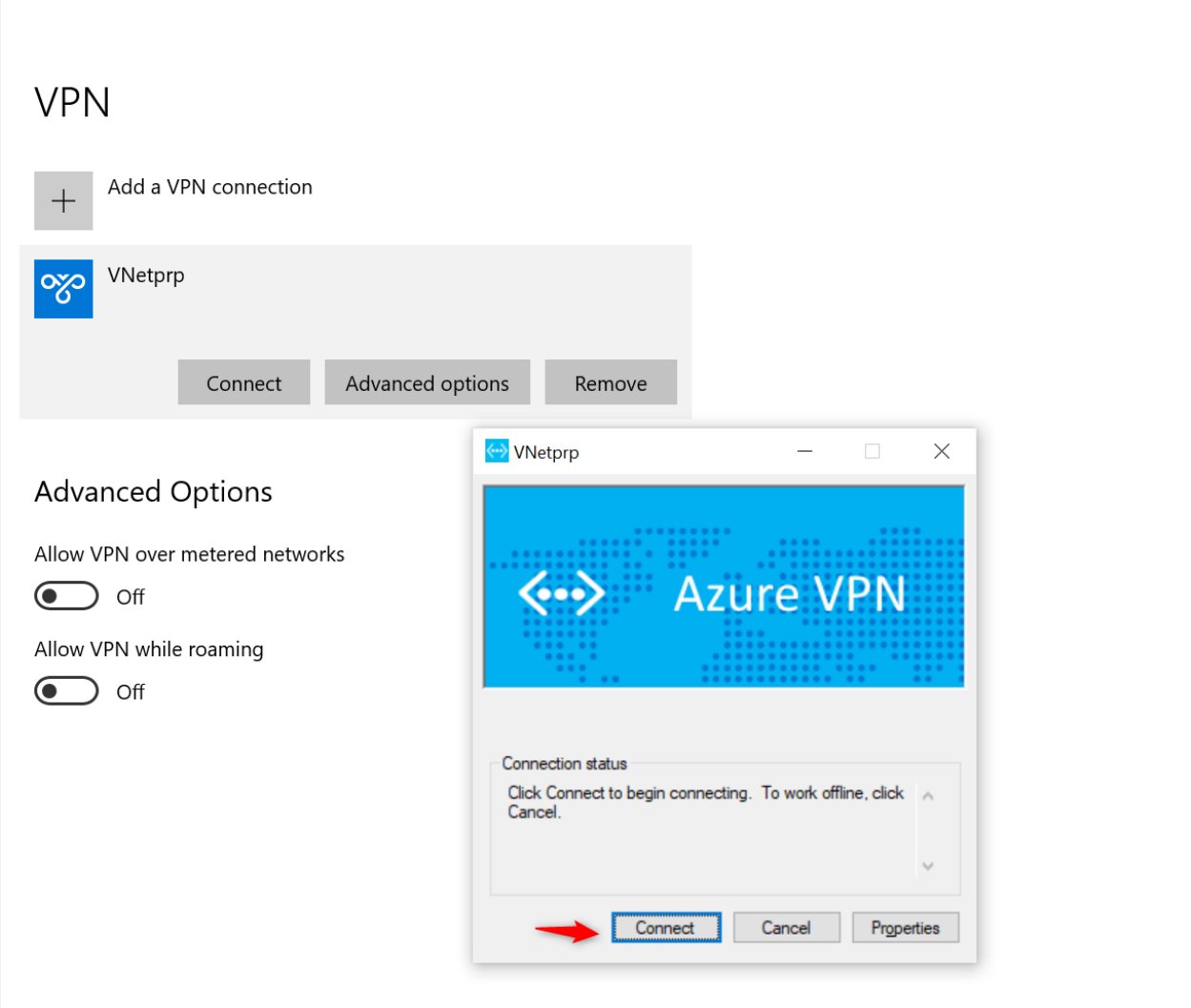


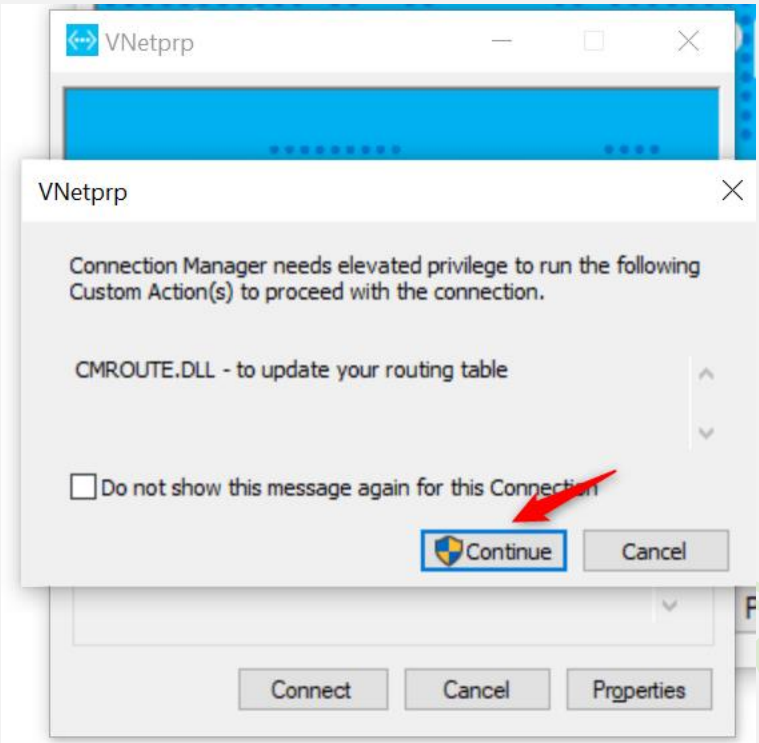
Found installed VPN client



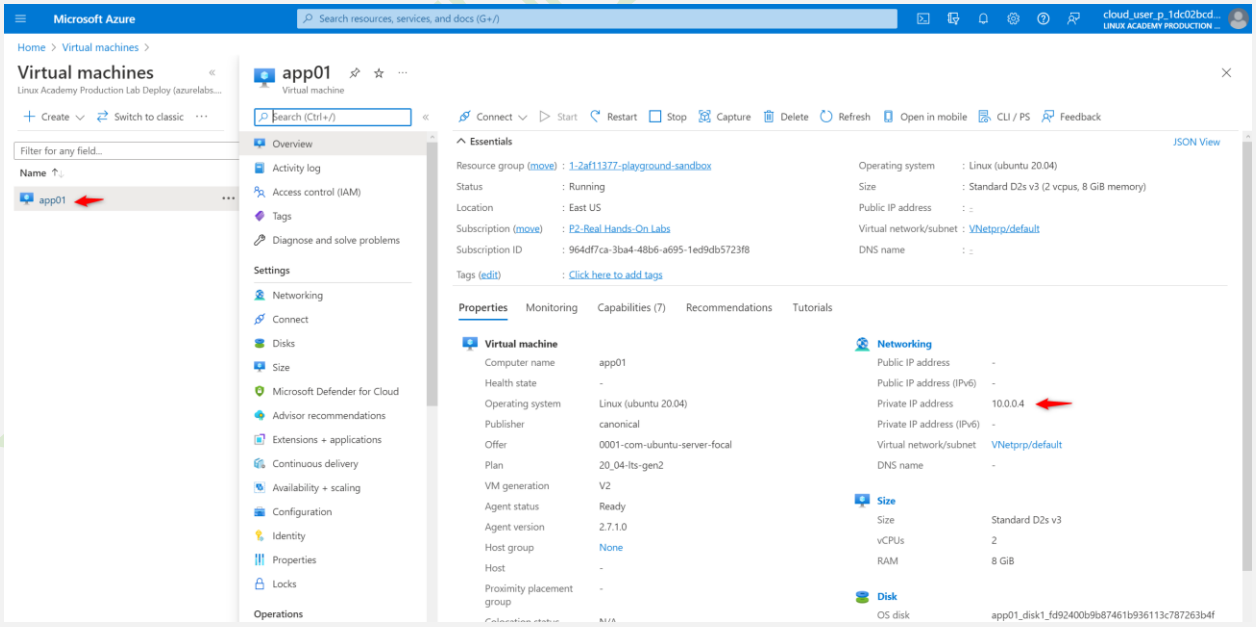
Connect VPN




VPN
Add a VPN connection
VNetprp
Connect
Advanced options
Remove
Advanced Options
Allow VPN over metered networks
Off
Allow VPN while roaming
Off
VNetprp
Azure VPN
Connection status
Click Connect to begin connecting. To work offline, click Cancel.
Connect
Cancel
Properties



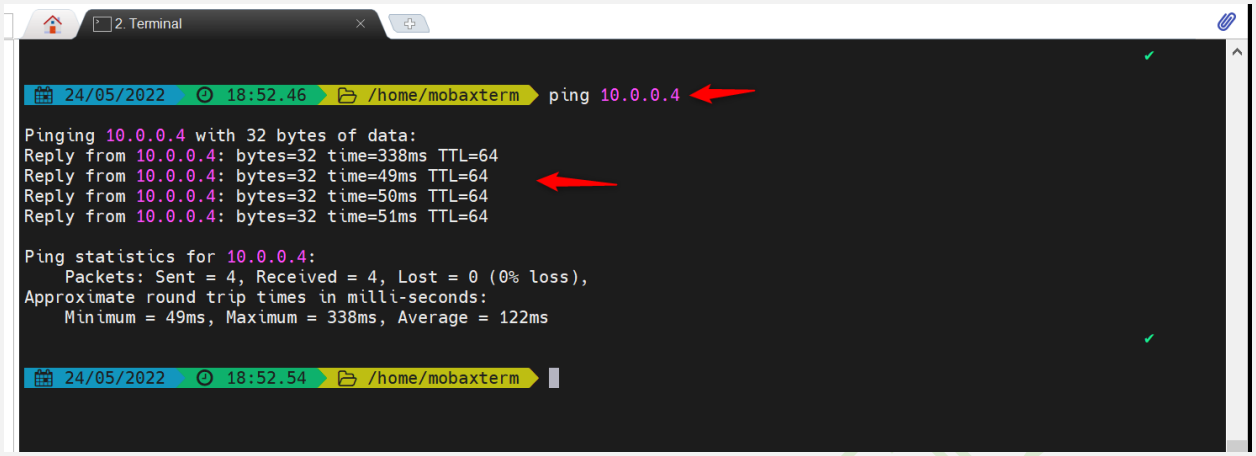
Test the connection from vm



Copy private ip

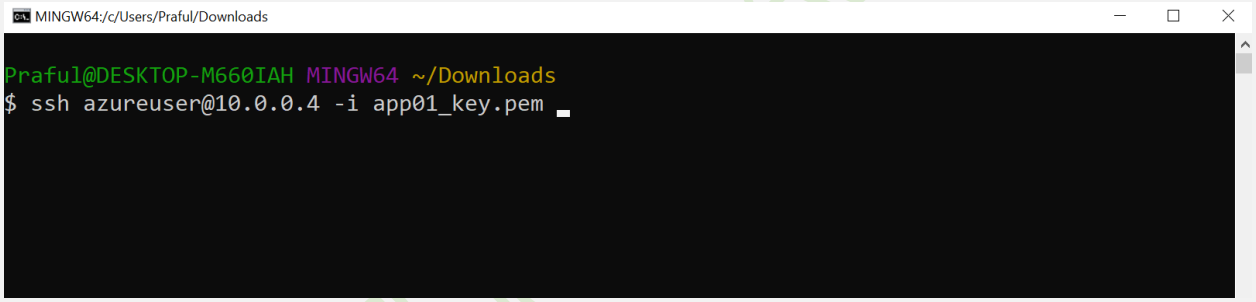
10.0.0.4

Open local terminal from the laptop and ping to private ip of vm



The connection is successful

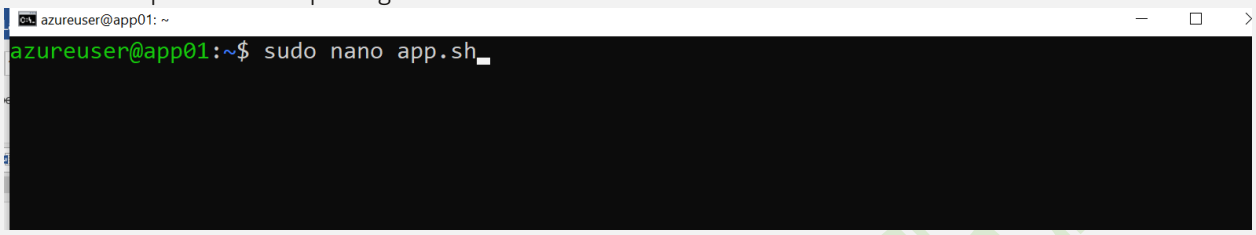
Let's SSH to the VM inside Azure from on premise site using private ip



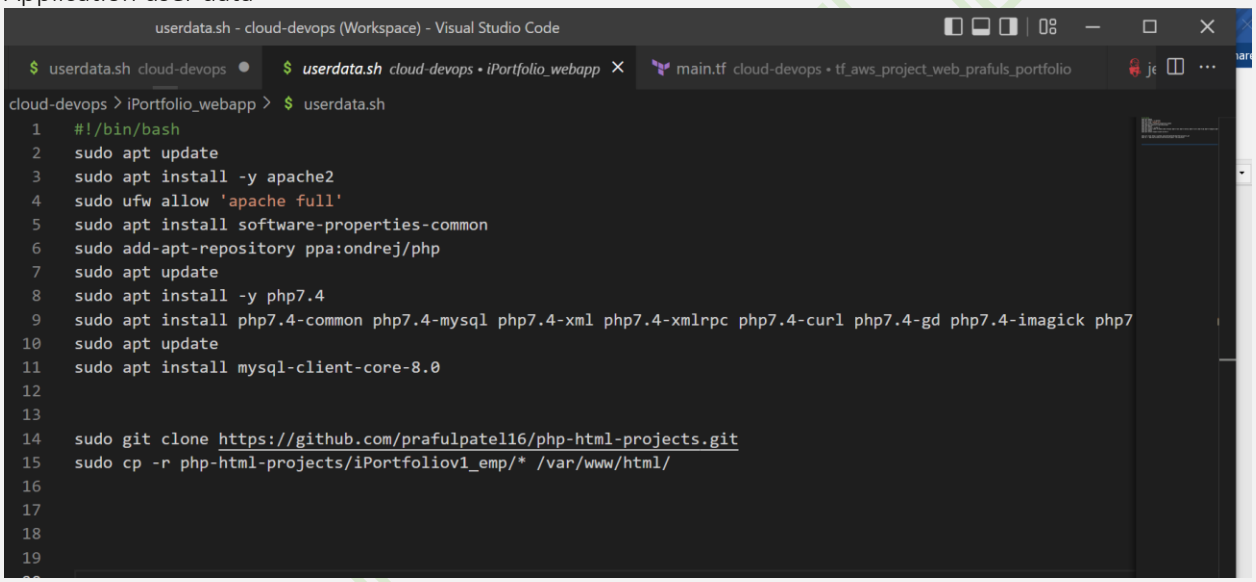

Select azureuser@app01: ~
Praful@DESKTOP-M660IAH MINGW64 ~/Downloads
$ ssh azureuser@10.0.0.4 -i app01_key.pem
The authenticity of host '10.0.0.4 (10.0.0.4)' can't be established.
ED25519 key fingerprint is SHA256:e+jf1jmG3hKduW7VL9YHhlnLZGMWsLYmYyXUHfVEHmE.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.0.4' (ED25519) to the list of known hosts.
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.13.0-1023-azure x86_64)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
System information as of Wed May 25 00:58:02 UTC 2022
System load: 0.0 Processes: 118
Usage of /: 4.9% of 28.90GB Users logged in: 0
Memory usage: 3% IPv4 address for eth0: 10.0.0.4
Swap usage: 0%
* Super-optimized for small spaces - read how we shrank the memory
footprint of MicroK8s to make it the smallest full K8s around.
https://ubuntu.com/blog/microk8s-memory-optimisation
1 update can be applied immediately.
To see these additional updates run: apt list --upgradable
The list of available updates is more than a week old.
To check for new updates run: sudo apt update
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
Select azureuser@app01: ~
The list of available updates is more than a week old.
To check for new updates run: sudo apt update
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
azureuser@app01:~$

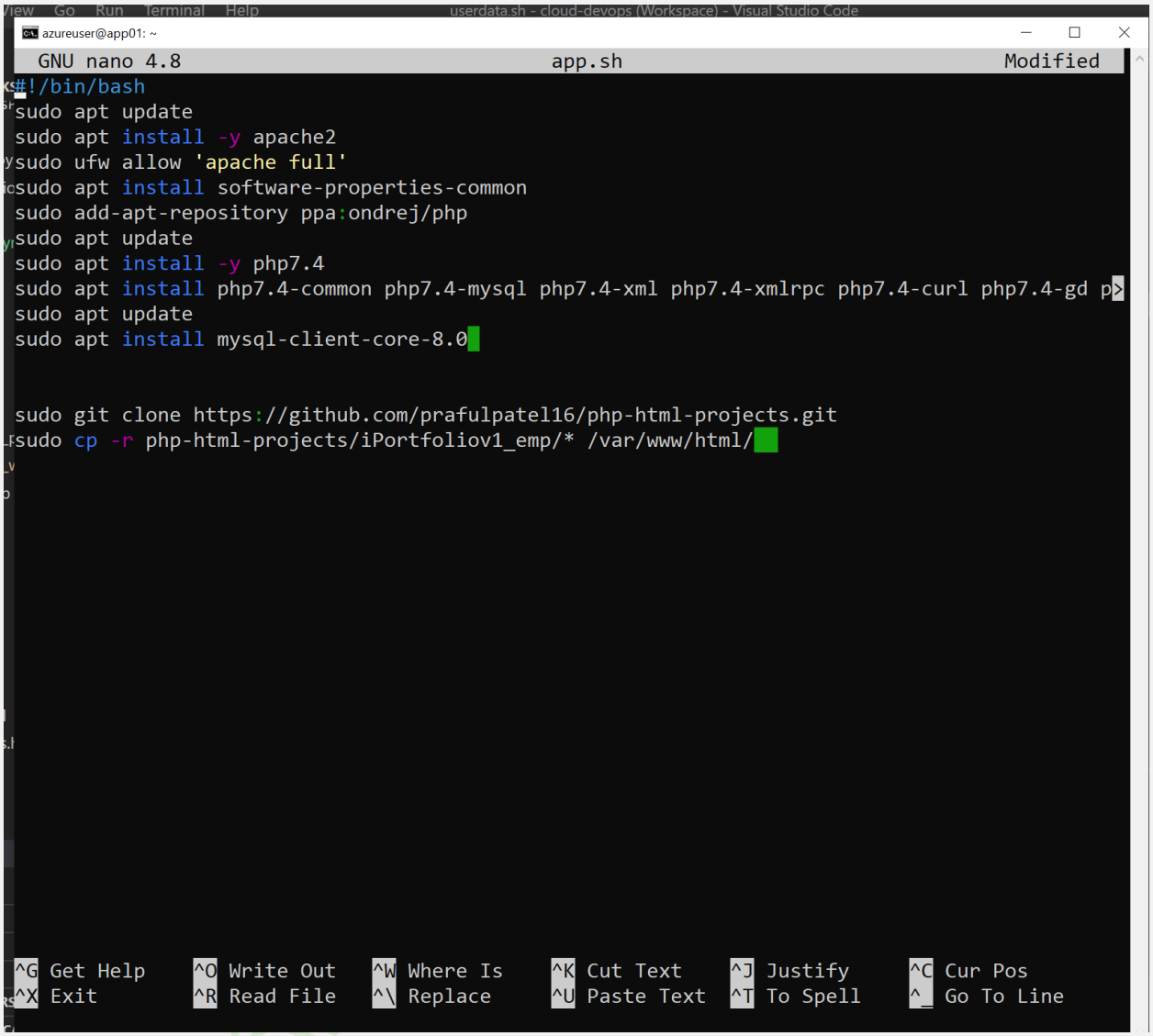
- Phase 5: Install and configure web application server

Install application server and deploy a web application
Create a script to install a packages

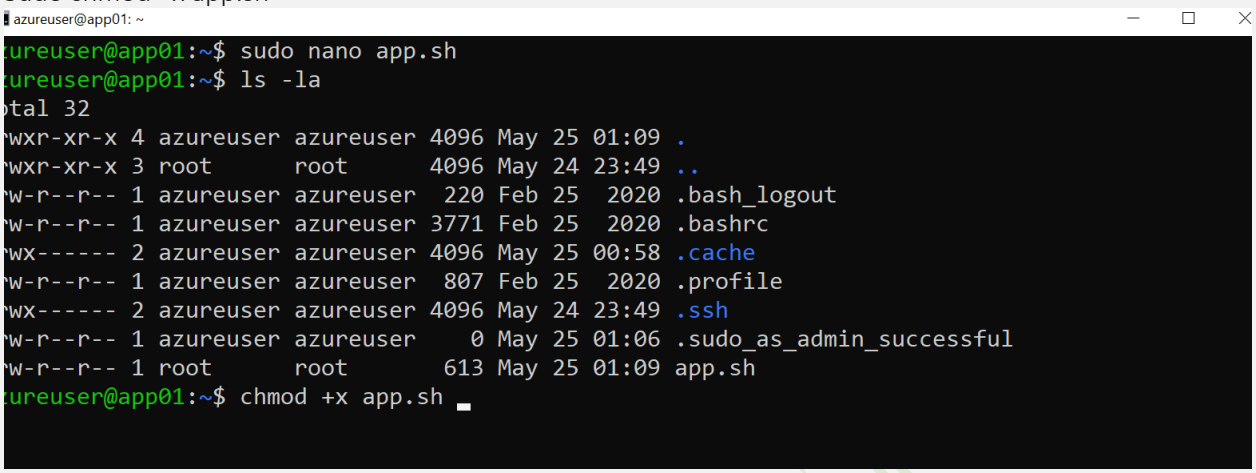


Application user data

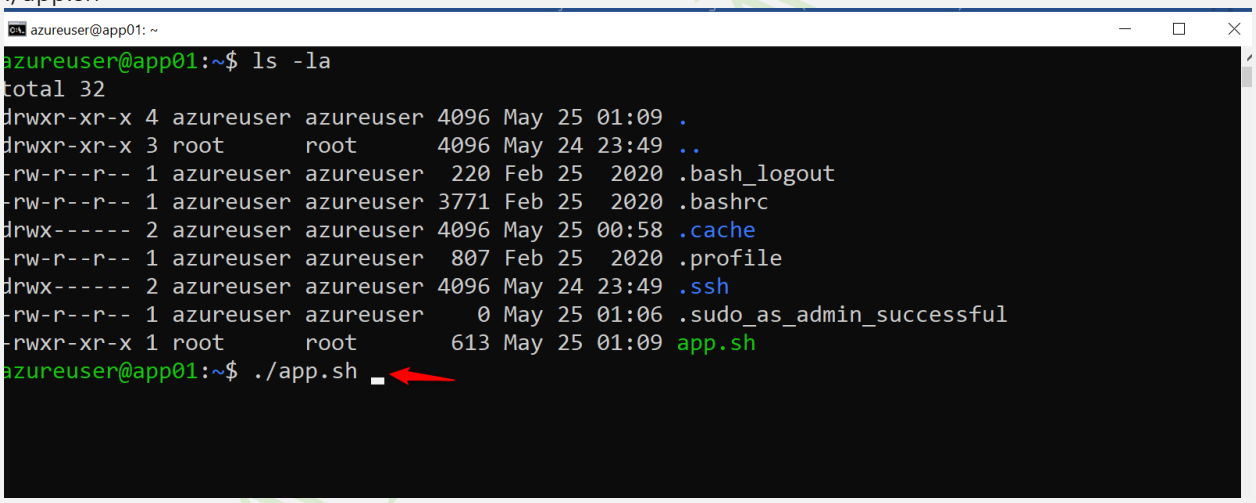



View Go Run Terminal Help
userdata.sh - cloud-devops (Workspace) - Visual Studio Code
azureuser@app01: ~
GNU nano 4.8
app.sh
Modified
#!/bin/bash
sudo apt update
sudo apt install -y apache2
sudo ufw allow 'apache full'
sudo apt install software-properties-common
sudo add-apt-repository ppa:ondrej/php
sudo apt update
sudo apt install -y php7.4
sudo apt install php7.4-common php7.4-mysql php7.4-xml php7.4-xmlrpc php7.4-curl php7.4-gd p
sudo apt update
sudo apt install mysql-client-core-8.0
sudo git clone https://github.com/prafulpatel16/php-html-projects.git
sudo cp -r php-html-projects/iPortfoliov1_emp/* /var/www/html/
^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

Allow +x permission to script
Sudo chmod +x app.sh

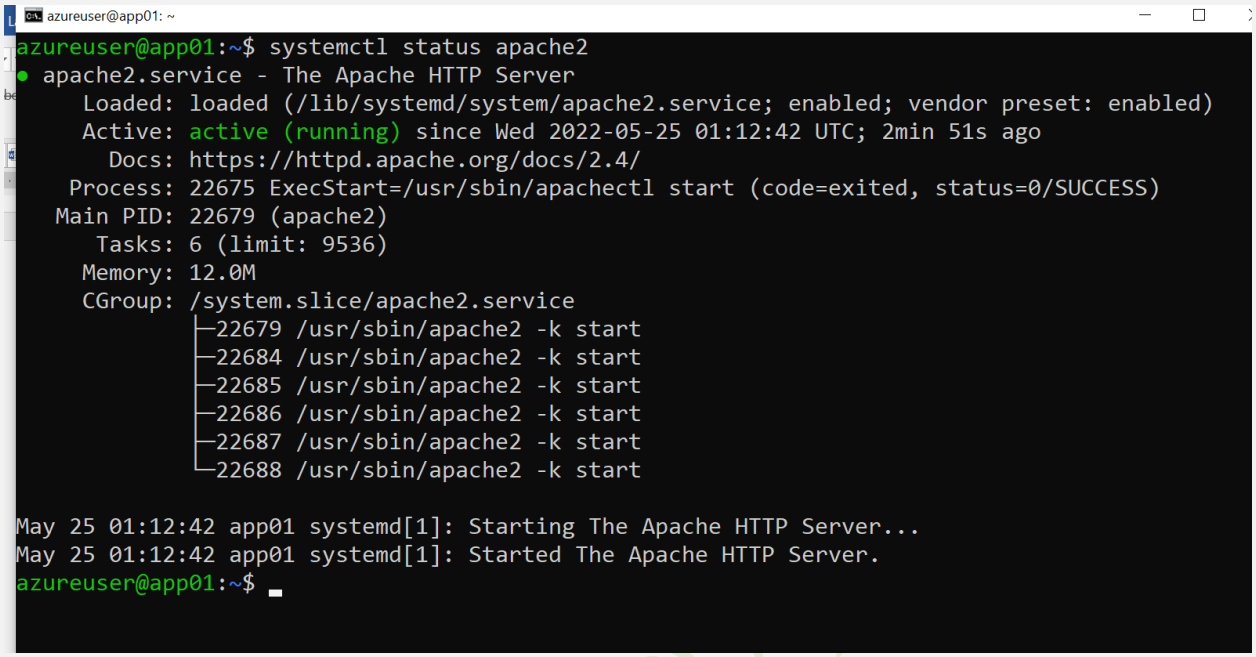


Run the script file
./app.sh



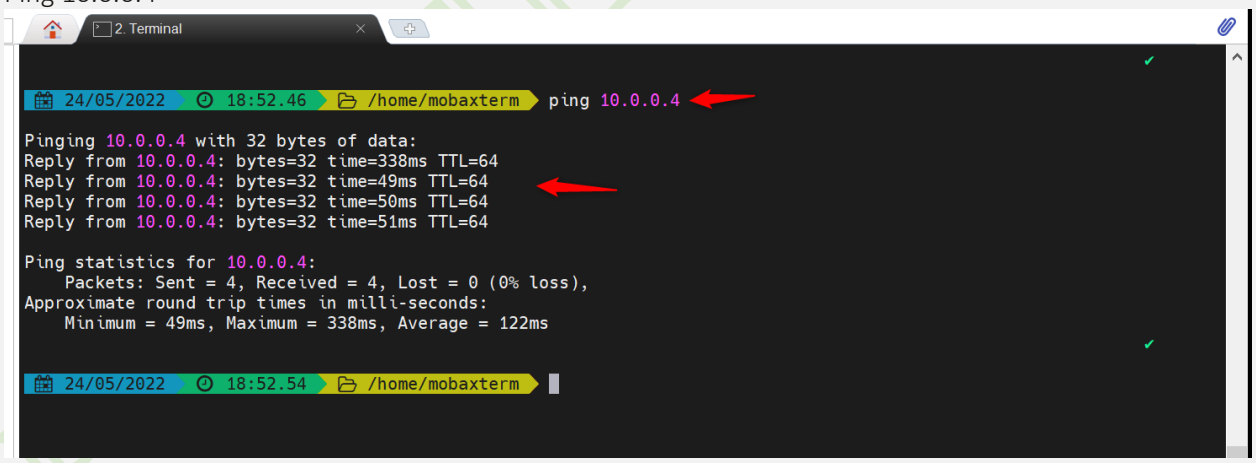
Installation complete and web application source code copied to apache root directory

Let's verify the web application is running

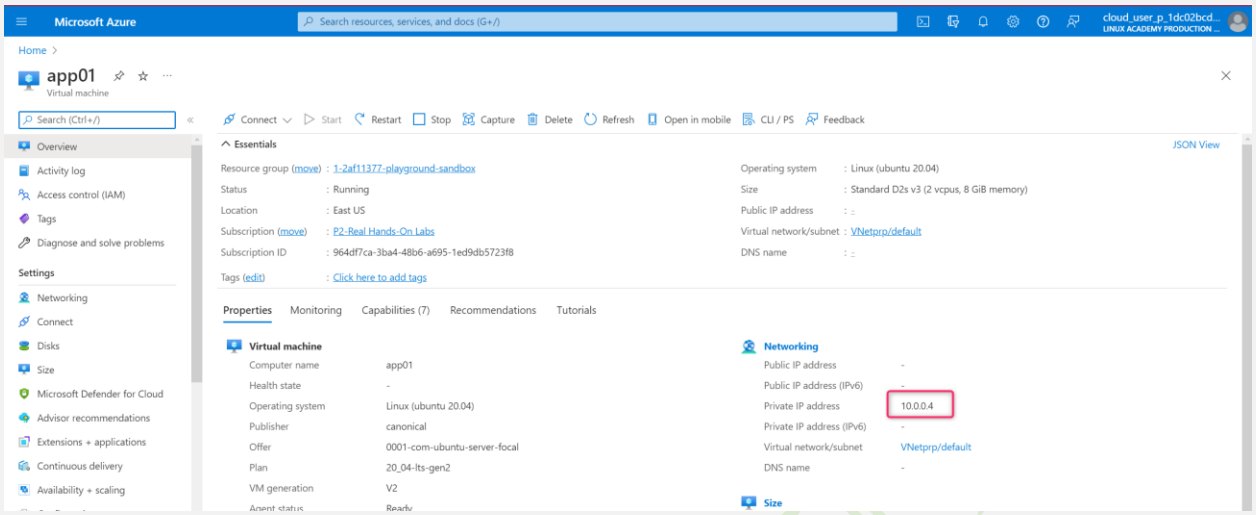


- Phase 6: Test web application accessibility within internal private connection

Verify if the private connectivity is established from on-premise location
Ping 10.0.0.4



Access web application from the browser using VM's private ip: 10.0.0.4



http://10.0.0.4

Web application is successfully accessed from on-premise location using private ip

CHALLENGE

Congratulations!!!!