VIETNAM NATIONAL UNIVERSITY HOCHIMINH CITY

UNIVERSITY OF INFORMATION TECHNOLOGY

ADVANCED PROGRAM IN INFORMATION SYSTEMS

ASSIGNMENT 2 REPORT
CLOUD COMPUTING

Class: **MSIS402.P11.CTTT**

Lecturer: **MSc. Trần Thị Dung**

Group 12:	**Nguyễn Thị Dung**	**20521211**
	Lê Thị Ngọc Châu	**21521855**
	Ngô Minh Trí	**21522705**

Ho Chi Minh City, September 2024

TABLE OF CONTENTS

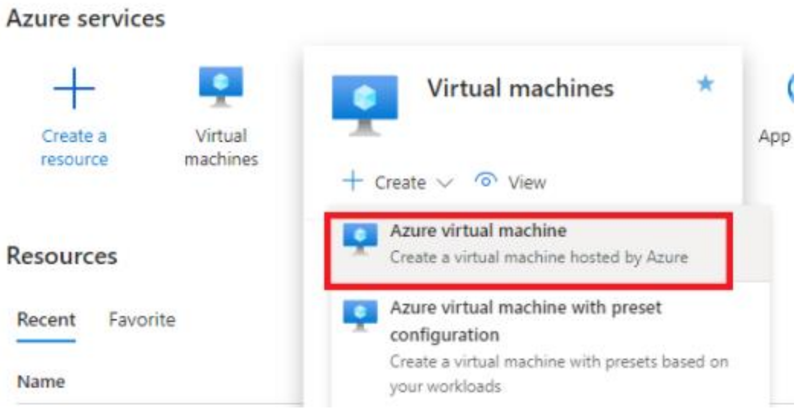
I. ASSIGNMENT 1

Requirements:
1. Create a virtual machine
2. Access VM
3. Install XAMPP

Implementation steps:

Step 1: Access the Azure Portal

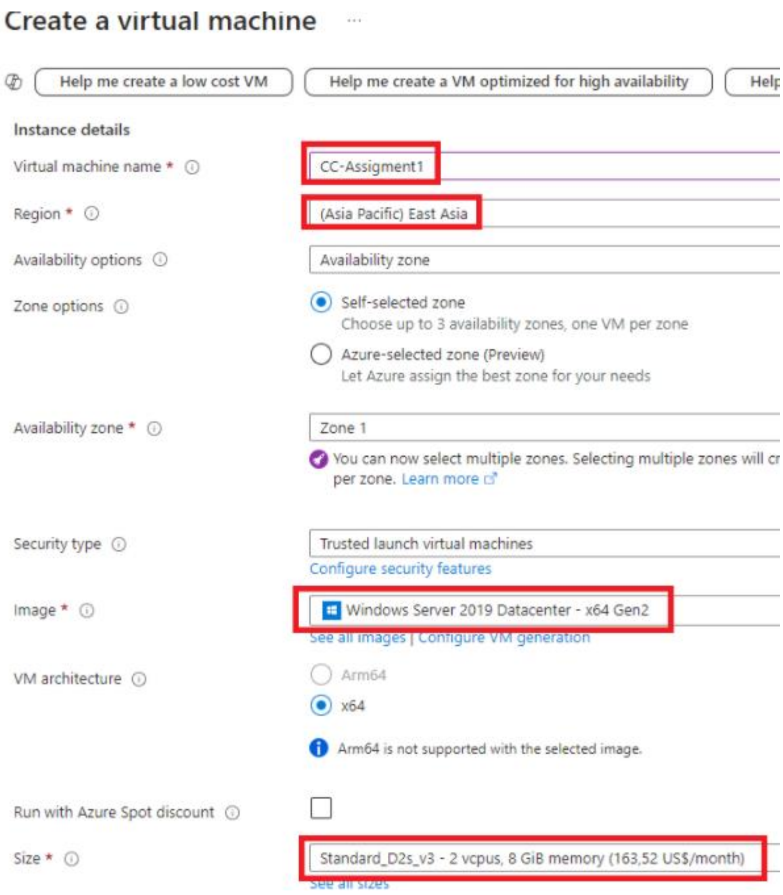
First, go to the official Azure portal by navigating to https://portal.azure.com/. Once we're logged in, locate and select "Virtual Machines" from the dashboard. After that, click on the "CREATE" button to begin setting up a new virtual machine.


Azure services
Create a resource
Virtual machines
Resources
Recent
Favorite
Name
Virtual machines
Create
View
Azure virtual machine
Create a virtual machine hosted by Azure
Azure virtual machine with preset configuration
Create a virtual machine with presets based on your workloads
App

Step 2: Configuring the Virtual Machine

To begin, we need to configure our virtual machine according to the project requirements. This process involves specifying several key details about the virtual machine.

- Virtual machine name: We assign a recognizable name to our VM, such as `CC-Assignment1.
- Region: We choose `(Asia Pacific) East Asia`. Choosing the correct region can affect performance and cost.
- Availability options: We select `Zone 1`, which allows us to distribute resources for higher availability in that specific zone.
- Security type: Ensure that Trusted launch virtual machines is selected to enable security features for the VM.
- Image: We choose the image `Windows Server 2019 Datacenter - x64 Gen2`. This ensures that the VM runs the desired version of Windows Server
- VM Size: We choose Standard_D2s_v3, which provides 2 vCPUs and 8 GiB of memory, balancing cost and performance effectively.



Create a virtual machine ···

Help me create a low cost VM
Help me create a VM optimized for high availability
Help

Instance details

Virtual machine name * ⓘ CC-Assigment1

Region * ⓘ (Asia Pacific) East Asia

Availability options ⓘ Availability zone

Zone options ⓘ
● Self-selected zone
Choose up to 3 availability zones, one VM per zone
○ Azure-selected zone (Preview)
Let Azure assign the best zone for your needs

Availability zone * ⓘ Zone 1
You can now select multiple zones. Selecting multiple zones will cr
per zone. Learn more

Security type ⓘ Trusted launch virtual machines
Configure security features

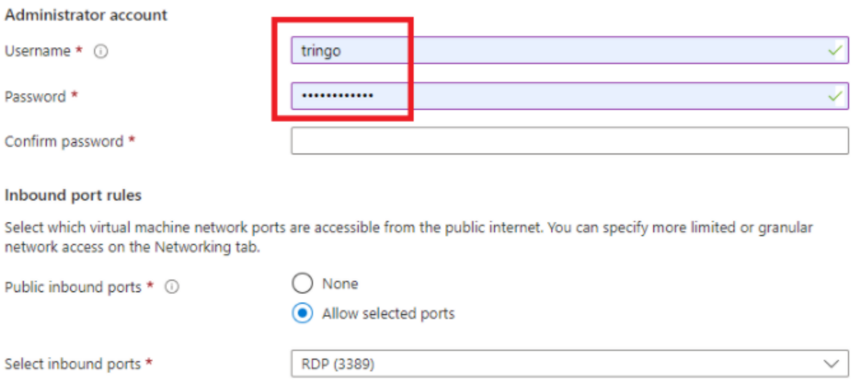
Image * ⓘ Windows Server 2019 Datacenter - x64 Gen2
See all images | Configure VM generation

VM architecture ⓘ
○ Arm64
● x64
Arm64 is not supported with the selected image.

Run with Azure Spot discount ⓘ □

Size * ⓘ Standard_D2s_v3 - 2 vcpus, 8 GiB memory (163,52 US$/month)
See all sizes

- Administrator username and password: The username is `tringo` and the password is strong to maintain the security of the virtual machine.
- Inbound port rules: We choose Allow selected ports and enable RDP (3389), allowing remote desktop protocol (RDP) access to manage the VM from other devices.



Administrator account

Username * ⓘ tringo

Password * ••••••••••••

Confirm password *

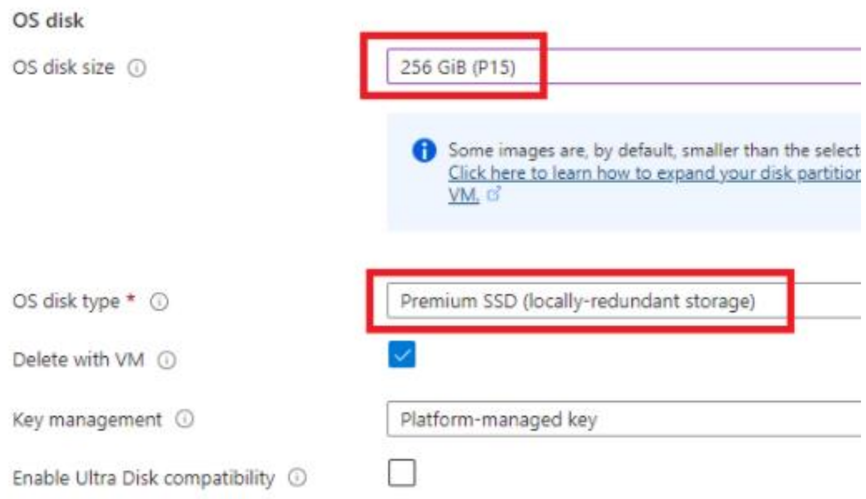
Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports * ⓘ
○ None
● Allow selected ports

Select inbound ports * RDP (3389)

- Disk size: We set the size to 256 GiB (P15), providing enough storage for our operating system and necessary software.
- Disk type: We select Premium SSD (locally-redundant storage) to ensure high performance and reliability.



OS disk

OS disk size: 256 GiB (P15)

Some images are, by default, smaller than the select
Click here to learn how to expand your disk partitior
VM.

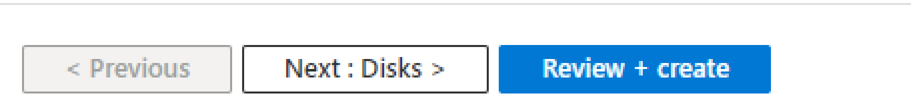
OS disk type *: Premium SSD (locally-redundant storage)

Delete with VM: ☑

Key management: Platform-managed key

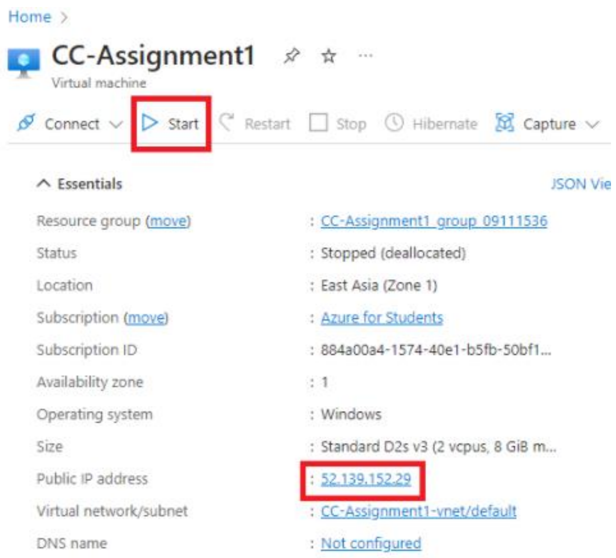
Enable Ultra Disk compatibility: □

After configuring the machine, review all the settings to ensure they meet the necessary requirements. If everything looks good, click "Review + Create" to finalize and create the virtual machine.



Step 3: Starting the Virtual Machine

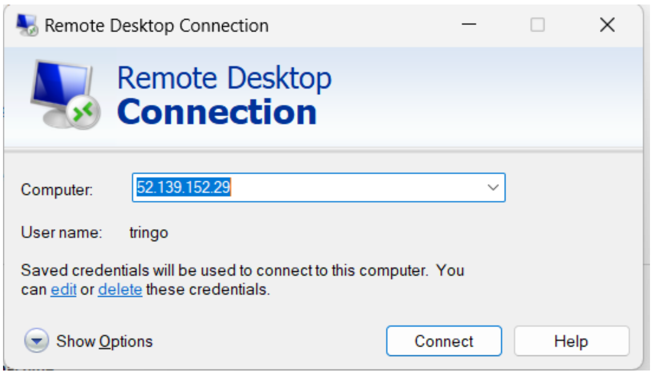
Once the virtual machine is successfully created, click on the "Start" button to power it on. After the machine starts, we will be provided with a public IP address. Make sure to copy this IP address as we will need it for remote access.



Resource group (move)	: CC-Assignment1_group_09111536
Status	: Stopped (deallocated)
Location	: East Asia (Zone 1)
Subscription (move)	: Azure for Students
Subscription ID	: 884a00a4-1574-40e1-b5fb-50bf1...
Availability zone	: 1
Operating system	: Windows
Size	: Standard D2s v3 (2 vcpus, 8 GiB m...
Public IP address	: 52.139.152.29
Virtual network/subnet	: CC-Assignment1-vnet/default
DNS name	: Not configured

Step 4: Connecting to the Virtual Machine

To connect to the virtual machine, open "Remote Desktop Connection" on wer local machine. In the Remote Desktop window, paste the public IP address we copied earlier and click "Connect."



Remote Desktop Connection

Remote Desktop Connection

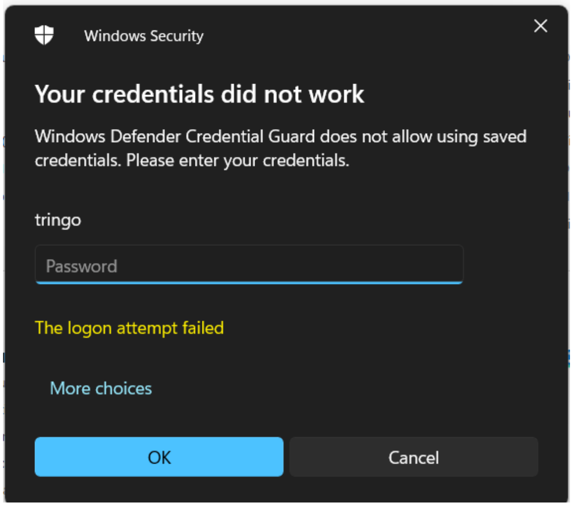
Computer: 52.139.152.29

User name: tringo

Saved credentials will be used to connect to this computer. You can edit or delete these credentials.

Step 6: Authentication

We will be prompted to enter the password that was set during the virtual machine configuration. Enter the password and proceed to log in.



Windows Security

Your credentials did not work

Windows Defender Credential Guard does not allow using saved credentials. Please enter your credentials.

tringo

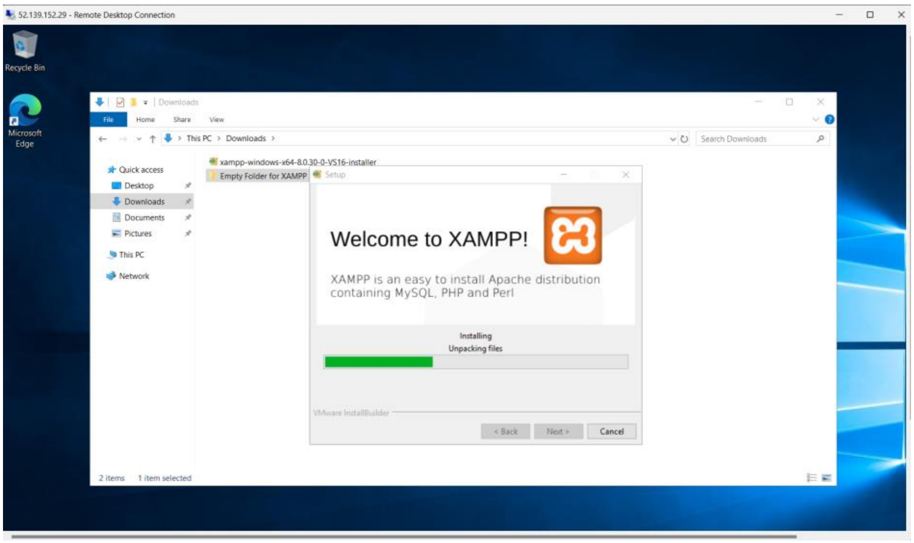
Password

The logon attempt failed

Step 7: Accessing the Virtual Machine Once successfully connected to the virtual machine, we can now use it as a remote desktop environment. Open the Edge browser, which is pre-installed on the virtual machine, and navigate to the official XAMPP website to download the XAMPP software.

Step 8: Installing XAMPP

After downloading the XAMPP installer, run the installation file. Follow the on-screen instructions to complete the installation process. Ensure that we select the necessary components, such as Apache and MySQL, during the installation.

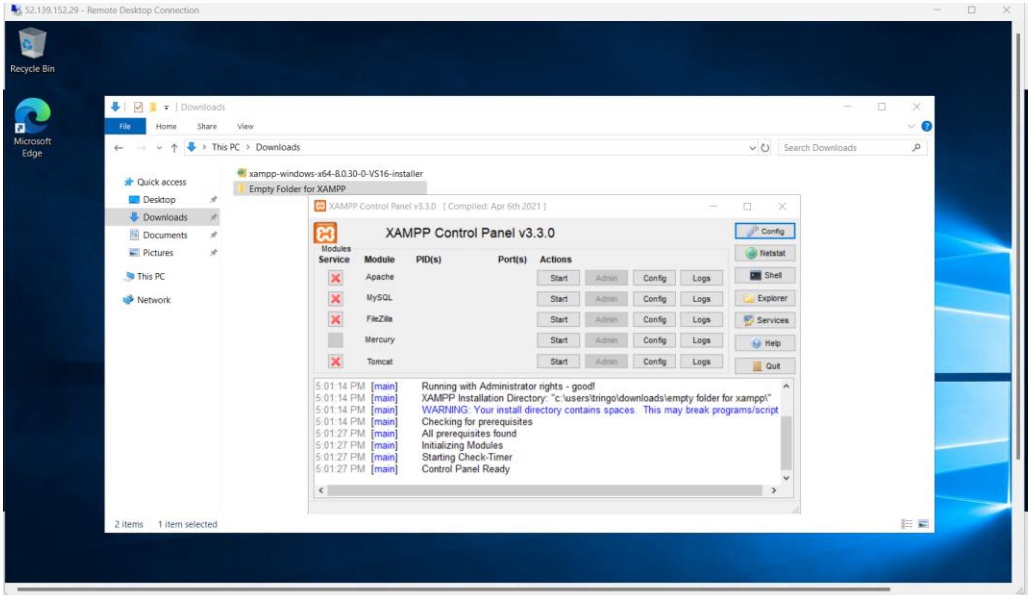


Welcome to XAMPP!

XAMPP is an easy to install Apache distribution containing MySQL, PHP and Perl

Installing
Unpacking files

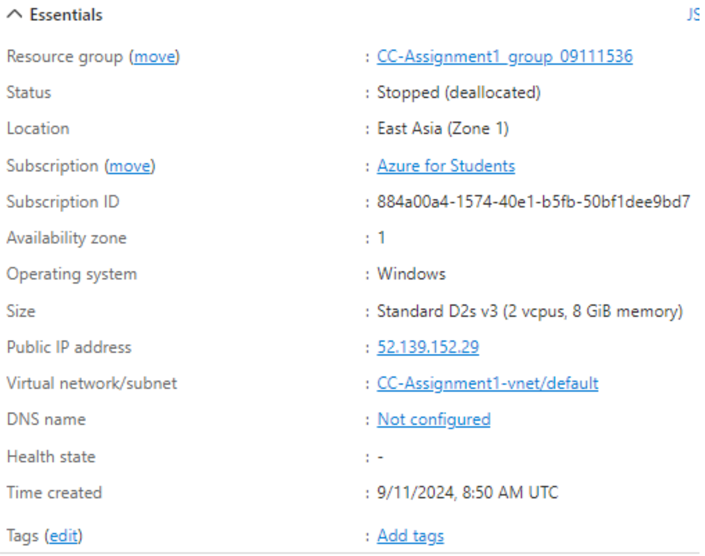
Once the installation process is complete, we should see a confirmation message. We have now successfully installed XAMPP on wer virtual machine, and it is ready for use.



```
5:01:14 PM  [main]   Running with Administrator rights - good!
5:01:14 PM  [main]   XAMPP Installation Directory: "c:\users\tringo\downloads\empty folder for xampp\"
5:01:14 PM  [main]   WARNING: Your install directory contains spaces.  This may break programs/script
5:01:14 PM  [main]   Checking for prerequisites
5:01:27 PM  [main]   All prerequisites found
5:01:27 PM  [main]   Initializing Modules
5:01:27 PM  [main]   Starting Check-Timer
5:01:27 PM  [main]   Control Panel Ready
```

II. VIRTUAL MACHINE CONFIGURATION EXPLAINATION

1. Essentials



^ Essentials

Resource group (move)	: CC-Assignment1_group_09111536
Status	: Stopped (deallocated)
Location	: East Asia (Zone 1)
Subscription (move)	: Azure for Students
Subscription ID	: 884a00a4-1574-40e1-b5fb-50bf1dee9bd7
Availability zone	: 1
Operating system	: Windows
Size	: Standard D2s v3 (2 vcpus, 8 GiB memory)
Public IP address	: 52.139.152.29
Virtual network/subnet	: CC-Assignment1-vnet/default
DNS name	: Not configured
Health state	: -
Time created	: 9/11/2024, 8:50 AM UTC
Tags (edit)	: Add tags

- Resource group: The resource group that contains the virtual machine, in this case, “CC-Assignment1_group_09111536”. The resource group helps manage related resources more easily.

- Status: The current status of the virtual machine is "Stopped (deallocated)", meaning the virtual machine is turned off, and hardware resources (CPU, RAM) have been released, which helps save costs.

- Location: The geographical location of the virtual machine, in “East Asia (Zone 1)”.

- Subscription: The virtual machine is running under the “Azure for Students” subscription, with a specific “Subscription ID” to manage the account.

- Size: The virtual machine configuration type is “Standard D2s v3”, with 2 vCPUs (virtual CPUs) and 8 GiB (gigabytes) of RAM.

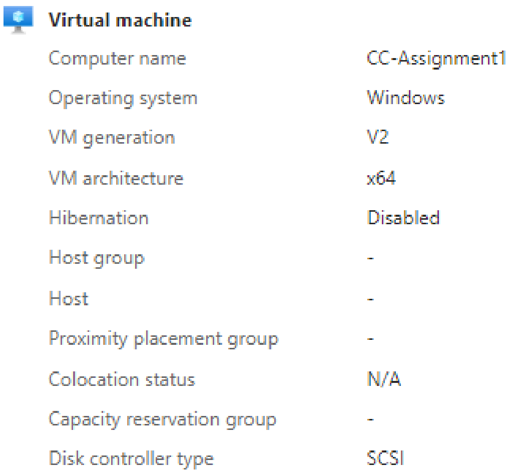
- Public IP address: The public IP address of the virtual machine is “52.139.152.29”, allowing access from external networks.

- Virtual network/subnet: The virtual machine belongs to the virtual network “CC-Assignment1-vnet/default”, which helps manage network connections between resources within the same environment.

- DNS name: The virtual machine does not have a DNS (Domain Name System) name configured yet. DNS would help easily identify and access the virtual machine through a domain name.

- Time created: The time when the virtual machine was created, in this case, “9/11/2024, 8:50 AM UTC”.

2. Virtual machine



Virtual machine

Computer name	CC-Assignment1
Operating system	Windows
VM generation	V2
VM architecture	x64
Hibernation	Disabled
Host group	-
Host	-
Proximity placement group	-
Colocation status	N/A
Capacity reservation group	-
Disk controller type	SCSI

- Computer name: The name of the virtual machine is “CC-Assignment1”.

- Operating system: The operating system installed on the virtual machine is Windows.

- VM generation: The virtual machine is of generation V2, indicating the generation of the virtual hardware being used.

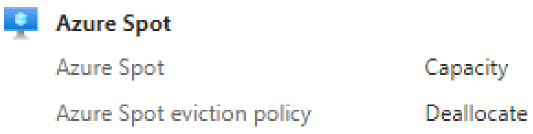
- VM architecture: The architecture of the virtual machine is “x64”, suitable for 64-bit operating systems and software.

- Hibernation: The hibernation feature is disabled.

- Host group/Host/Proximity placement group/Colocation status/Capacity reservation group: These fields are not configured, meaning there is no dedicated host, host group, or specific resource allocation strategy.

- Disk controller type: The disk controller type is SCSI (Small Computer System Interface), a standard for hard drive communication.

3. Azure Spot:



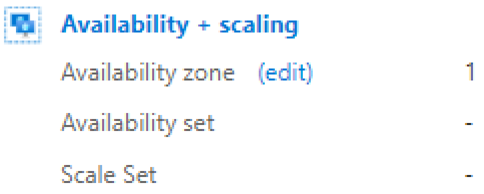
Azure Spot

Azure Spot	Capacity
Azure Spot eviction policy	Deallocate

- Azure Spot: The virtual machine has the Azure Spot feature enabled, which allows using virtual machines at a lower cost but with the possibility of being stopped when Azure needs resources.

- Azure Spot eviction policy: The policy when the machine is stopped is “Deallocate”, meaning resources will be freed.

4. Availability + scaling:



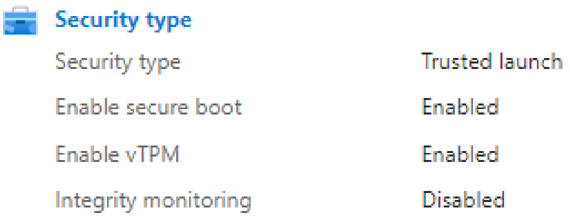
Availability + scaling

Availability zone (edit)	1
Availability set	-
Scale Set	-

- Availability zone: The virtual machine is deployed in “Zone 1”, one of the availability zones within the Azure data center.

- Availability set/Scale Set: The virtual machine is not configured for high availability or scaling sets.

5. Security type:



Security type

Security type	Trusted launch
Enable secure boot	Enabled
Enable vTPM	Enabled
Integrity monitoring	Disabled

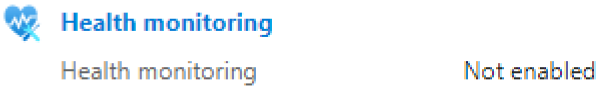
- Trusted launch: This virtual machine supports trusted launch.

- Enable secure boot: The secure boot feature is enabled, protecting the virtual machine from malware during startup.

- Enable vTPM: The virtual TPM (Trusted Platform Module) feature is also enabled, providing encryption and hardware security.

- Integrity monitoring: The integrity monitoring feature is disabled.

6. Health monitoring:

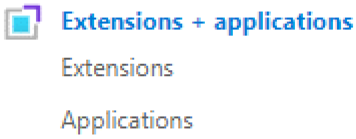


Health monitoring

Health monitoring	Not enabled

- Health monitoring: Health monitoring is not enabled on this virtual machine.

7. Extensions + applications:



Extensions + applications

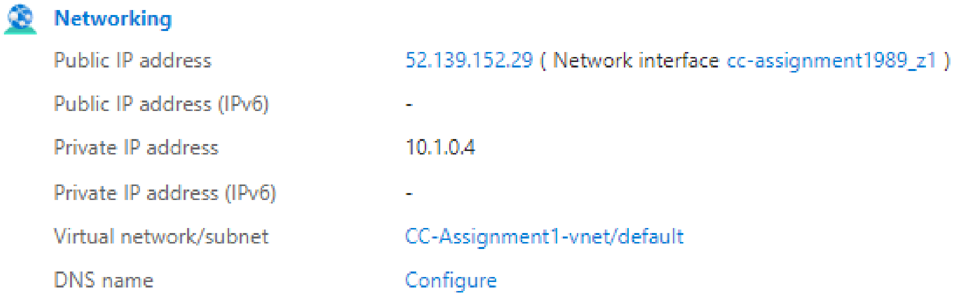
Extensions

Applications

- Extensions: No extensions are installed on the virtual machine.

- Applications: No applications are installed yet.

8. Networking



Networking

Public IP address	52.139.152.29 (Network interface cc-assignment1989_z1)
Public IP address (IPv6)	-
Private IP address	10.1.0.4
Private IP address (IPv6)	-
Virtual network/subnet	CC-Assignment1-vnet/default
DNS name	Configure

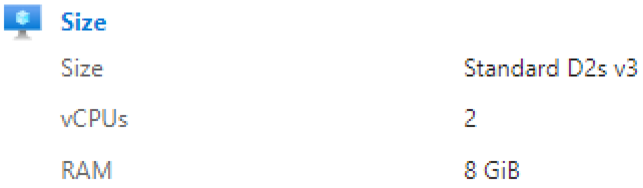
- Public IP address: The public IP address of the virtual machine is “52.139.152.29”.

- Private IP address: The virtual machine also has a private IP address of “10.1.0.4” for internal communication within its private network.

- Virtual network/subnet: The virtual machine is part of the virtual network "CC-Assignment1-vnet/default".

- DNS name: No DNS name has been configured for the virtual machine.

9. Size

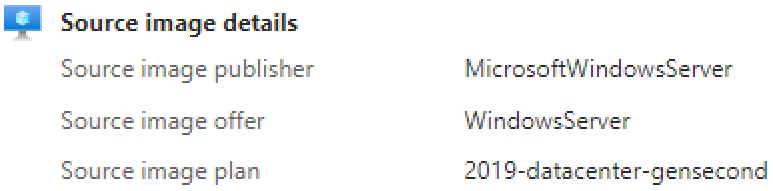


Size

Size	Standard D2s v3
vCPUs	2
RAM	8 GiB

- Size: The virtual machine configuration is "Standard D2s v3", with 2 vCPUs and 8 GiB RAM.

10. Source image details



Source image details

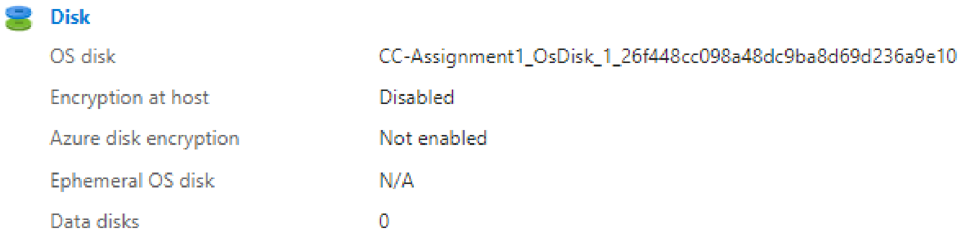
Source image publisher	MicrosoftWindowsServer
Source image offer	WindowsServer
Source image plan	2019-datacenter-gensecond

- Source image publisher: The virtual machine is using the operating system published by "MicrosoftWindowsServer".

- Source image offer: The virtual machine is running Windows Server from the "WindowsServer" offer.

- Source image plan: This offer is from the "2019-datacenter-gensecond" release, a data center edition of Windows Server.

11. Disk



Disk

OS disk	CC-Assignment1_OsDisk_1_26f448cc098a48dc9ba8d69d236a9e10
Encryption at host	Disabled
Azure disk encryption	Not enabled
Ephemeral OS disk	N/A
Data disks	0

- OS disk: The operating system disk is labeled “CC-Assignment1_OsDisk_1”.

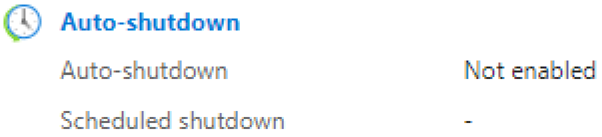
- Encryption at host: Encryption at the host level is disabled.

- Azure disk encryption: The virtual machine is not using Azure disk encryption.

- Ephemeral OS disk: No ephemeral operating system disk is being used.

- Data disks: No data disks are attached to the virtual machine.

12. Auto-shutdown



Auto-shutdown

Auto-shutdown	Not enabled
Scheduled shutdown	-

- Auto-shutdown: The auto-shutdown feature is not enabled.

- Scheduled shutdown: No scheduled shutdown is configured.

III. ASSIGNMENT 2

Requirements:

1. Deploy a static website

2. Deploy the website with a database connection

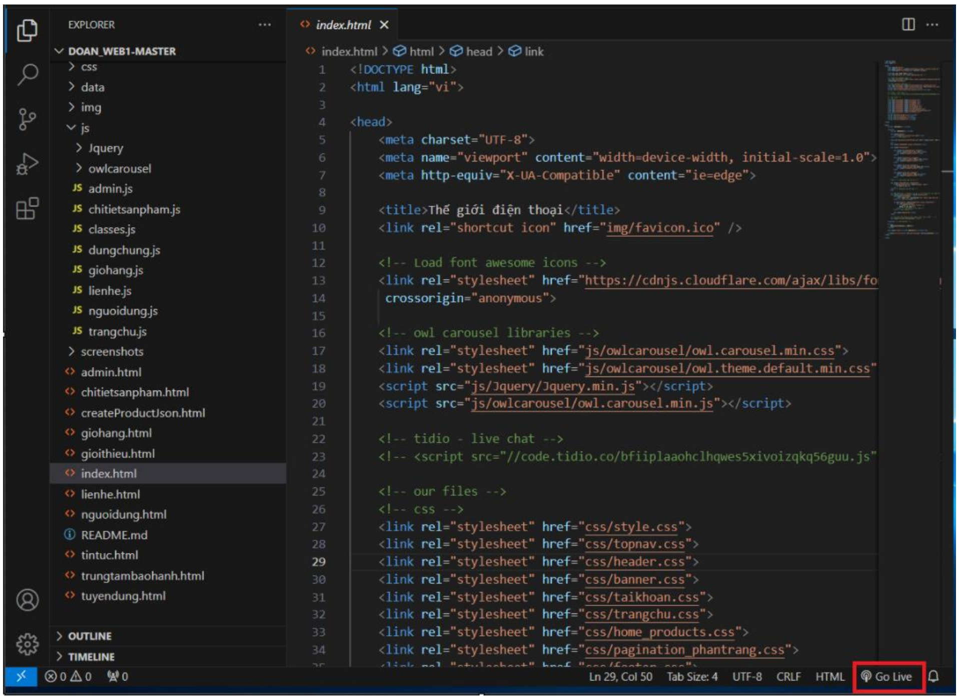
Implementation steps:

Step 1: Opening the Source Code and Deploying Locally

In this step, we begin by accessing the source code of our project through the integrated development environment (IDE), Visual Studio Code (VSCode). Once the necessary project files are loaded, the file explorer on the left panel clearly displays the structure of the website, including HTML, CSS, and JavaScript files.

We select the `index.html` file, which is the main entry point of our static website. The code is written in standard HTML with links to various stylesheets and scripts that enhance the website's functionality and design. To preview the website locally, we utilize the “Live Server” extension in VSCode, a useful tool that allows us to instantly serve the website on a local web server.

By clicking the "Go Live" button located at the bottom-right corner of the IDE, our website is launched in the browser. This feature ensures that any changes made to the code are instantly reflected in real time without needing to refresh the page manually. At this point, our static website is successfully deployed in a local environment, and we can begin testing its layout and interactive features.

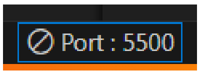


```html
<!DOCTYPE html>
<html lang="vi">

<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <meta http-equiv="X-UA-Compatible" content="ie=edge">

    <title>Thế giới điện thoại</title>
    <link rel="shortcut icon" href="img/favicon.ico" />

    <!-- Load font awesome icons -->
    <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/fo
     crossorigin="anonymous">

    <!-- owl carousel libraries -->
    <link rel="stylesheet" href="js/owlcarousel/owl.carousel.min.css">
    <link rel="stylesheet" href="js/owlcarousel/owl.theme.default.min.css"
    <script src="js/Jquery/Jquery.min.js"></script>
    <script src="js/owlcarousel/owl.carousel.min.js"></script>

    <!-- tidio - live chat -->
    <!-- <script src="//code.tidio.co/bfiiplaaohclhqwes5xivoizqkq56guu.js"

    <!-- our files -->
    <!-- css -->
    <link rel="stylesheet" href="css/style.css">
    <link rel="stylesheet" href="css/topnav.css">
    <link rel="stylesheet" href="css/header.css">
    <link rel="stylesheet" href="css/banner.css">
    <link rel="stylesheet" href="css/taikhoan.css">
    <link rel="stylesheet" href="css/trangchu.css">
    <link rel="stylesheet" href="css/home_products.css">
    <link rel="stylesheet" href="css/pagination_phantrang.css">
```

After successfully launching our local server using the **Go Live** feature in Visual Studio Code, it's important to note the port number that our local server is using. In this case, as shown in the image, the local server is running on **Port 5500**.

This port number is crucial for accessing our website locally through a web browser. For example, to view the website, we would enter http://localhost:5500 in the browser's address bar.

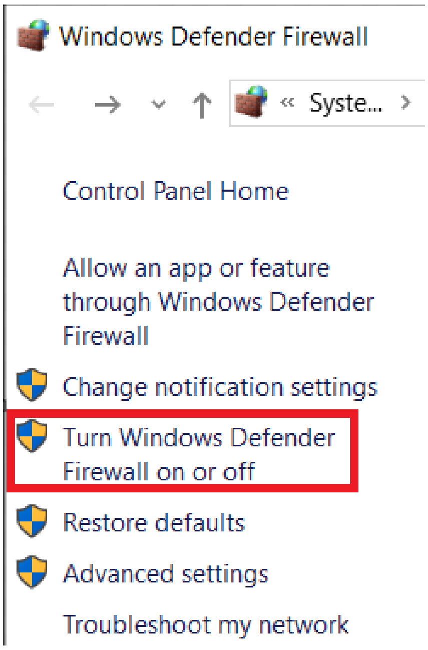
By remembering this port number, we can consistently access and interact with the website while making further adjustments or testing different functionalities.



Step 2: Turning Off the Firewall on the Virtual Machine

To ensure our virtual machine can serve the website without any interruptions, we need to adjust the firewall settings. Specifically, we will turn off the firewall to allow unrestricted access for testing purposes.

We begin by accessing the Windows Defender Firewall settings on the virtual machine. From the Control Panel, we select the option Turn Windows Defender Firewall on or off, as highlighted in the image. This option allows us to temporarily disable the firewall for both public and private networks.



Windows Defender Firewall

« Syste... ›

Control Panel Home

Allow an app or feature through Windows Defender Firewall

Change notification settings

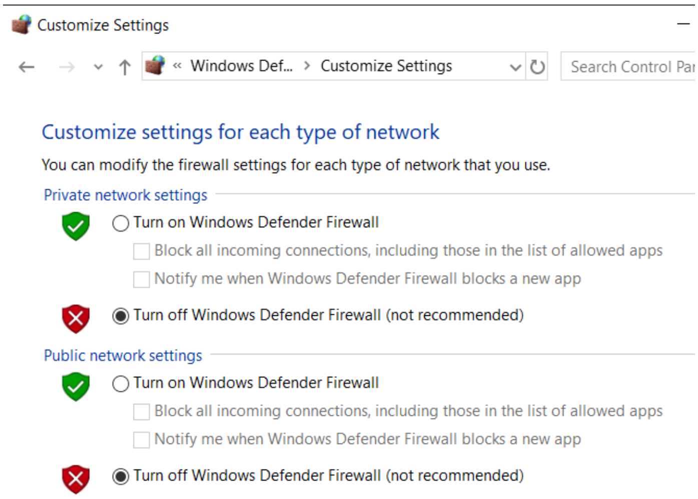
Turn Windows Defender Firewall on or off

Restore defaults

Advanced settings

Troubleshoot my network

By turning off the firewall, we remove any potential blocks that might prevent our local server from functioning properly or from being accessed externally. However, it is essential to remember that this step should only be performed in a secure testing environment to prevent unauthorized access.



Customize Settings

« Windows Def... › Customize Settings

Search Control Pai

Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.

Private network settings

○ Turn on Windows Defender Firewall

□ Block all incoming connections, including those in the list of allowed apps

□ Notify me when Windows Defender Firewall blocks a new app

● Turn off Windows Defender Firewall (not recommended)

Public network settings

○ Turn on Windows Defender Firewall

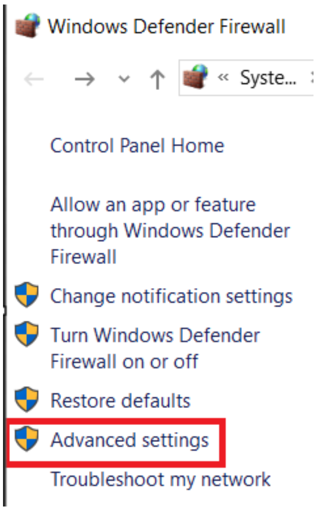
□ Block all incoming connections, including those in the list of allowed apps

□ Notify me when Windows Defender Firewall blocks a new app

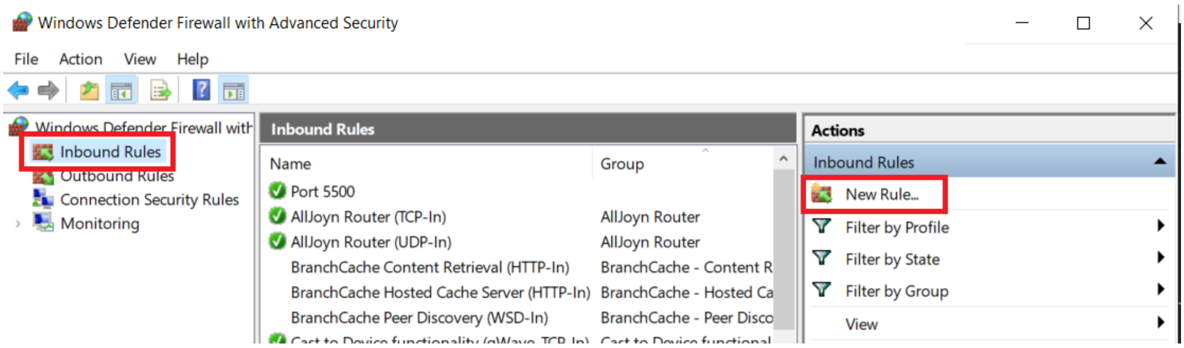
● Turn off Windows Defender Firewall (not recommended)

Step 3: Configuring the Inbound Rule in Windows Firewall

In this step, we need to configure the firewall to allow traffic through the specific port used by our local server (Port 5500). To do this, we will create a new inbound rule to allow connections on this port.

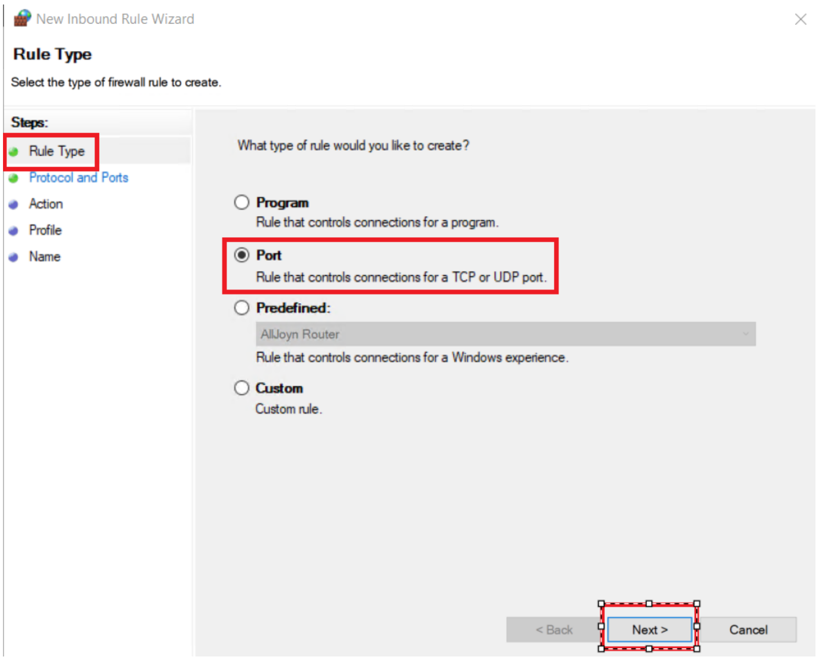

Windows Defender Firewall
« Syste...
Control Panel Home
Allow an app or feature through Windows Defender Firewall
Change notification settings
Turn Windows Defender Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network

We begin by navigating to the Advanced settings section of the Windows Defender Firewall. From the Inbound Rules section, we select New Rule to create a new custom rule.



Name	Group
✓ Port 5500	
✓ AllJoyn Router (TCP-In)	AllJoyn Router
✓ AllJoyn Router (UDP-In)	AllJoyn Router
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content R
BranchCache Hosted Cache Server (HTTP-In)	BranchCache - Hosted Ca
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Disco
✓ Cast to Device functionality (qWave-TCP-In)	Cast to Device functional

Rule Type: We choose the Port option, as we want to control connections based on a specific port. After selecting this option, we click Next



New Inbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

What type of rule would you like to create?

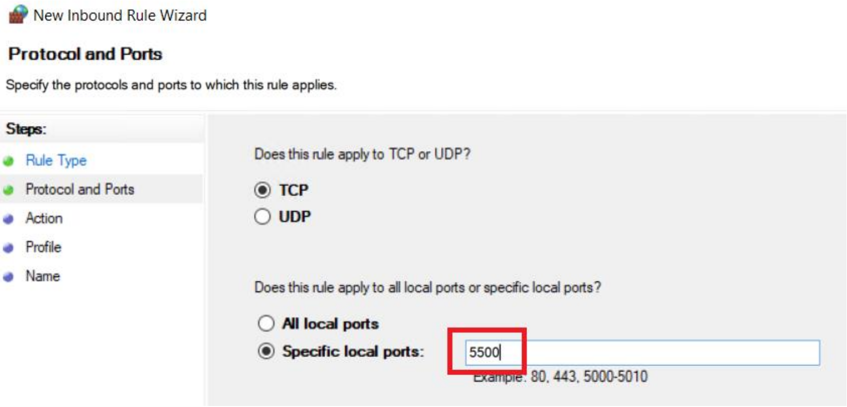
○ **Program**
Rule that controls connections for a program.

● **Port**
Rule that controls connections for a TCP or UDP port.

○ **Predefined:**
AllJoyn Router
Rule that controls connections for a Windows experience.

○ **Custom**
Custom rule.

Protocol and Ports: We select TCP as the protocol and specify 5500 as the local port. This ensures that all incoming traffic on Port 5500 is allowed. Once again, we click Next to proceed.



New Inbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

Does this rule apply to TCP or UDP?

● **TCP**
○ **UDP**

Does this rule apply to all local ports or specific local ports?

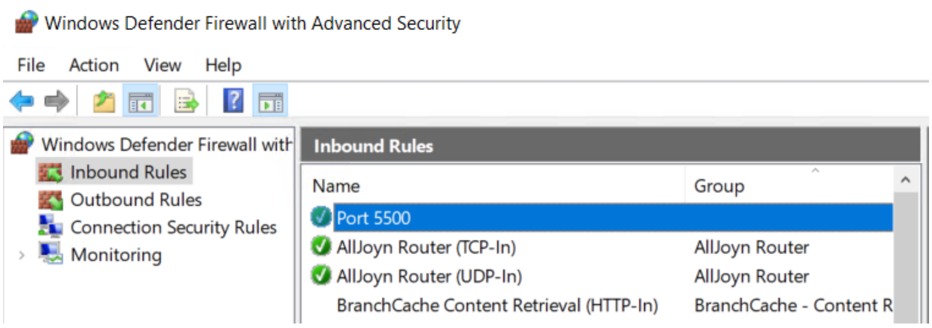
○ **All local ports**
● **Specific local ports:** 5500
Example: 80, 443, 5000-5010

Action: We choose to Allow the connection to permit traffic through the specified port.

Profile: We select all the profile types (Domain, Private, Public) to ensure the rule applies in all network environments. Afterward, we click Next.

Name: We name the rule, for example, Port 5500, to easily identify it in the firewall rules list. Finally, we confirm by clicking Finish.

After completing these steps, the new inbound rule for Port 5500 appears in the list, and our virtual machine is now set to accept traffic through this port.


Windows Defender Firewall with Advanced Security
File
Action
View
Help
Windows Defender Firewall with
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring

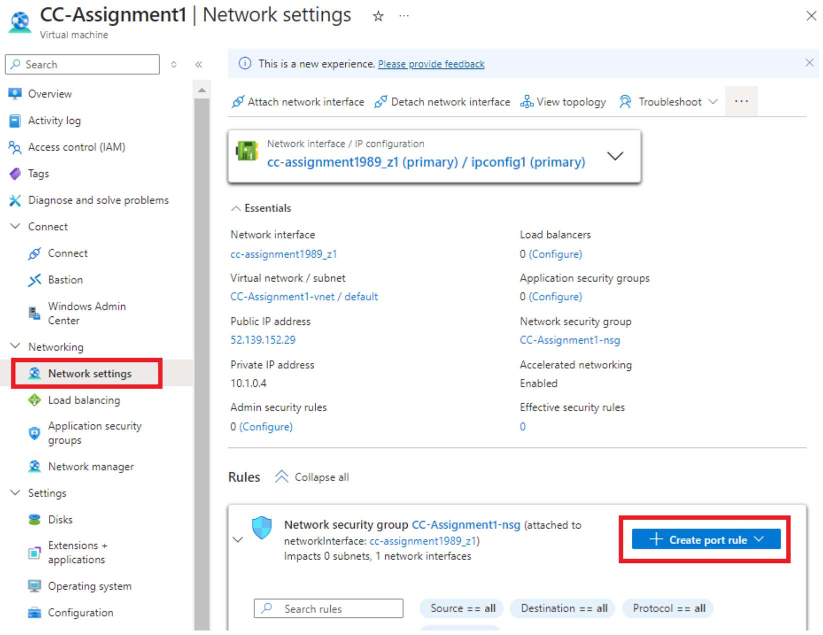
Inbound Rules

Name	Group
Port 5500	
AllJoyn Router (TCP-In)	AllJoyn Router
AllJoyn Router (UDP-In)	AllJoyn Router
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content R

Step 4: Configuring Port 5500 in Azure Virtual Machine

In this step, we configure port 5500 for our virtual machine within the Azure portal to ensure proper network connectivity. This is essential for enabling external traffic to access our virtual machine through this specific port.

We begin by navigating to the Network settings of the virtual machine in the Azure portal. In this section, we select Create port rule to add a new network security rule.



This is a new experience. Please provide feedback

Network interface / IP configuration: cc-assignment1989_z1 (primary) / ipconfig1 (primary)

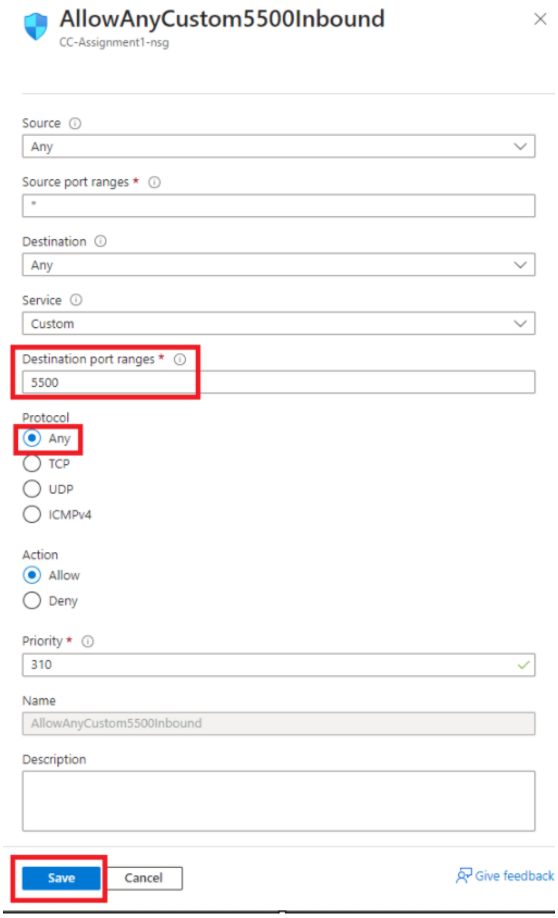
Network interface: cc-assignment1989_z1
Load balancers: 0 (Configure)
Virtual network / subnet: CC-Assignment1-vnet / default
Application security groups: 0 (Configure)
Public IP address: 52.139.152.29
Network security group: CC-Assignment1-nsg
Private IP address: 10.1.0.4
Accelerated networking: Enabled
Admin security rules: 0 (Configure)
Effective security rules: 0

Network security group CC-Assignment1-nsg (attached to networkInterface: cc-assignment1989_z1)
Impacts 0 subnets, 1 network interfaces

In the Destination port ranges, we set the port to 5500. This ensures that all traffic directed to port 5500 is properly routed.

For the Protocol, we choose Any to allow all types of network protocols through this port. This broad setting ensures flexibility in testing and communication.

After confirming the settings, we click Save to apply the rule.



AllowAnyCustom5500Inbound
CC-Assignment1-nsg

Source: Any

Source port ranges *: *

Destination: Any

Service: Custom

Destination port ranges *: 5500

Protocol
● Any
○ TCP
○ UDP
○ ICMPv4

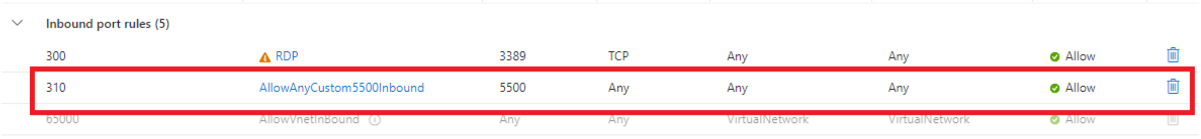
Action
● Allow
○ Deny

Priority *: 310 ✓

Name: AllowAnyCustom5500Inbound

Description:

Once completed, our new inbound rule appears in the list, confirming that port 5500 is now configured and ready to accept external connections.



Inbound port rules (5)

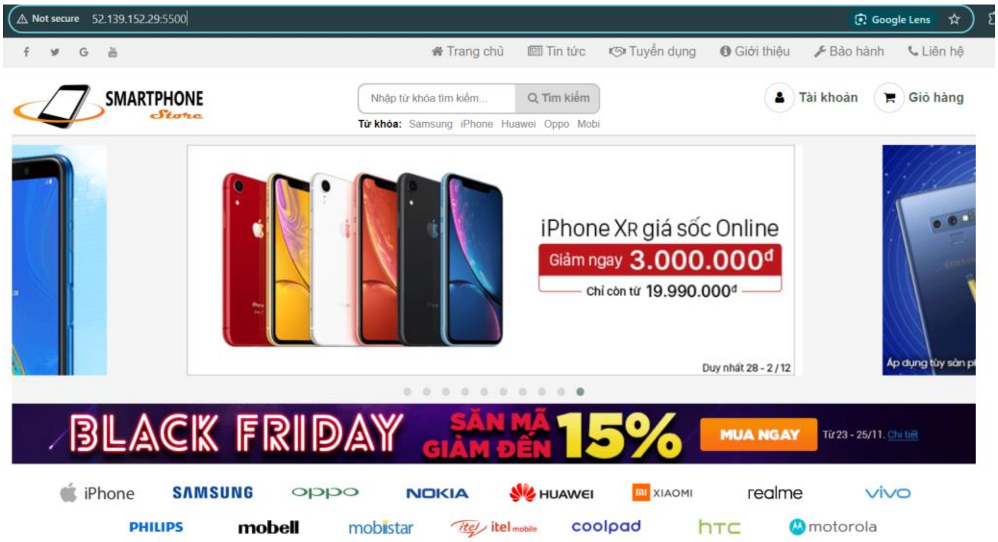
300	⚠ RDP	3389	TCP	Any	Any	✓ Allow	🗑
310	AllowAnyCustom5500Inbound	5500	Any	Any	Any	✓ Allow	🗑
65000	AllowVnetInBound ⓘ	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow	🗑

Step 5: Accessing the Website from External Devices

We copy the Public IP Address along with the port number that we previously configured (in this case, http://52.139.152.29:5500/). This IP address allows us to access the website hosted on the virtual machine.

Next, we paste the URL into the web browser of another device that is connected to the same Wi-Fi network. This ensures that the device can communicate with the virtual machine through the specified port.

Once the URL is entered, we are able to view our website live in the browser. As shown in the image, the website is fully operational and accessible from external devices, confirming that the network and firewall configurations are successful.


Not secure 52.139.152.29:5500
Google Lens
Trang chủ
Tin tức
Tuyển dụng
Giới thiệu
Bảo hành
Liên hệ
SMARTPHONE Store
Nhập từ khóa tìm kiếm...
Tìm kiếm
Từ khóa: Samsung iPhone Huawei Oppo Mobi
Tài khoản
Giỏ hàng
iPhone XR giá sốc Online
Giảm ngay 3.000.000đ
Chỉ còn từ 19.990.000đ
Duy nhất 28 - 2 / 12
Áp dụng tùy sản p
BLACK FRIDAY
SĂN MÃ GIẢM ĐẾN 15%
MUA NGAY
Từ 23 - 25/11. Chi tiết
iPhone
SAMSUNG
oppo
NOKIA
HUAWEI
XIAOMI
realme
vivo
PHILIPS
mobell
mobiistar
itel mobile
coolpad
htc
motorola

--- END ---