

Lab 4: AWS Security and Server Infrastructure

A demo of the basic setup of this lab is at: <https://youtu.be/GaMd8MaqBXA>

A Outline

In previous labs we have set up a range of architectures with VMWare vSphere. This is a private cloud environment and creates infrastructure-as-a-service. Increasingly, we use the public cloud to build our information systems, and which reduces the cost in the investment in data centre costs, while providing the opportunity to quickly scale our server, network and data infrastructure. It is generally as pay-as-you-go model, and where we pay for CPU time, network bandwidth and data costs. The most popular public cloud provider is AWS (Amazon Web Services), and which provides EC2 (for compute), S3 (for data buckets), RDS (for databases) and AWS Network Firewall (for firewalls). Some of these services are outlined in Figure 1.

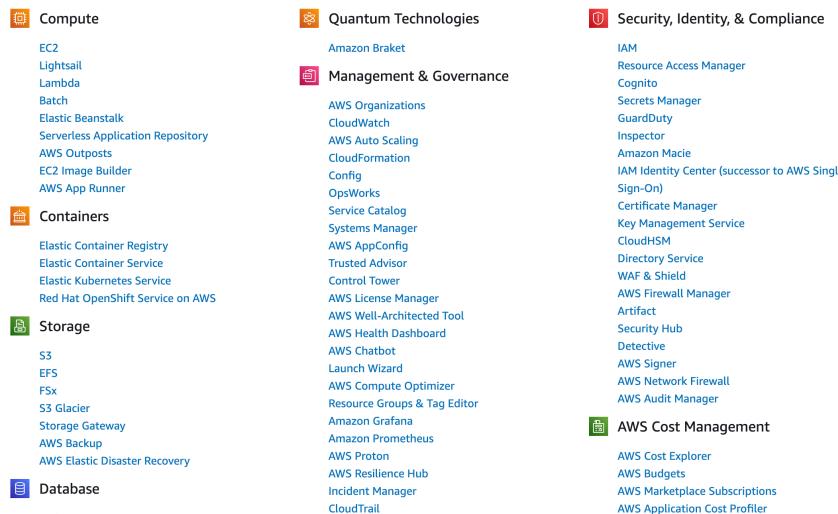


Figure 1: AWS Services

B Enabling your lab

You should have an AWS Academy login, so go to: <https://awsacademy.instructure.com/> and log into the system and select **AWS Academy Learner Lab** (Figure 2).

AWS Academy Learner Lab - Foundation Services [28224]



This is the Edinburgh Napier University AWS Academy Learner Lab for CSN09112, and which has \$100 of credit for you to learn AWS Services. If you exceed your credit, you will lose your environment, so remember to switch your instances off when you are not using them. The lab session is four hours, but you can restart the lab again at any time. All EC2 instances will be shut off after the four hours are up. Do not end the lab, until we have finished with the module. Some resources are:

- Introduction to Cloud Computing: [here](#).
- A demo of setting up EC2 instances is [here](#).

[Click Modules](#) to start the course.

Figure 2: AWS Academy Learner Lab

Next, select “Modules”, and then “Learner Lab - Foundational Services”, and should have the lab environment (Figure 3).

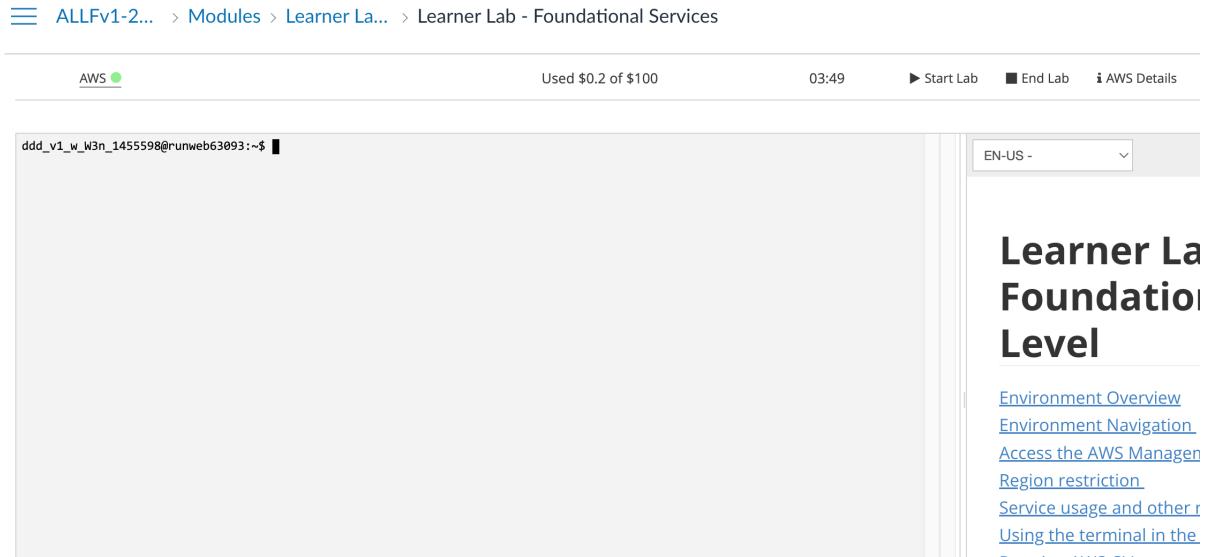


Figure 3: AWS Academy Learner Lab environment

In the console you can interact with your AWS though the console (as you are already logged into AWS). Now, press the “Start Lab” button, and wait for the AWS light to go green. Once, green, you can click on it, and open up your AWS Management console. After this, just select EC2, and you should see your EC2 environment.

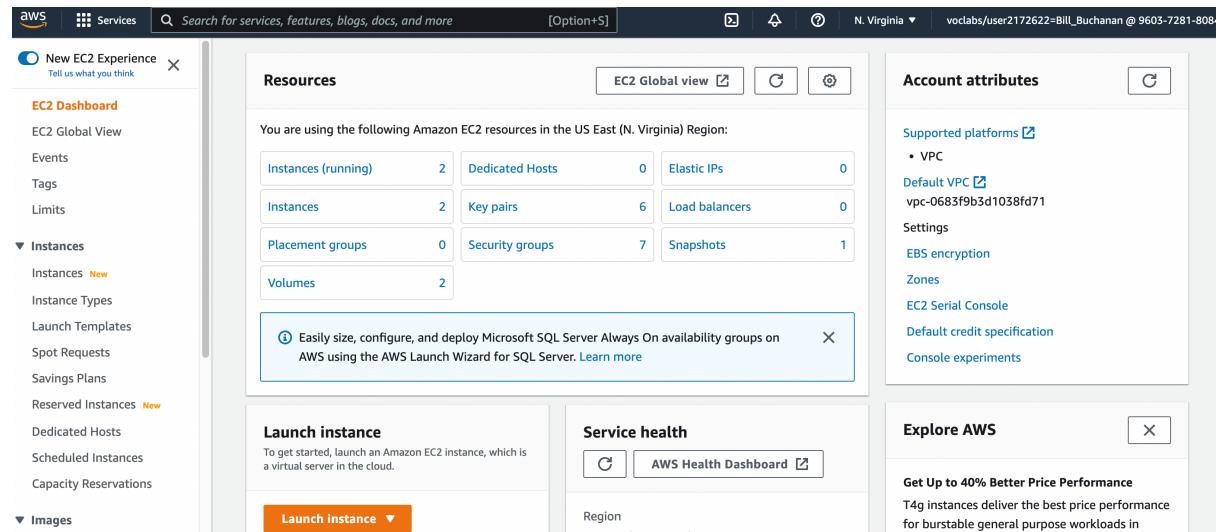


Figure 4: AWS Management Console (EC2)

C Creating and Securing a Linux Server

We will now create a Linux Server, and which should be accessible from the Internet. For this select “Launch Instance”, and then give it a name (such as “My Linux Server”) and select the Amazon Linux instance for the AMI (Amazon Machine Instance) – as shown in Figure 5.

Name

Add additional tags

▼ Application and OS Images (Amazon Machine Image) [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images

Quick Start

Amazon Linux macOS Ubuntu Windows Red Hat S >

Amazon Machine Image (AMI)

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type

Free tier eligible

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

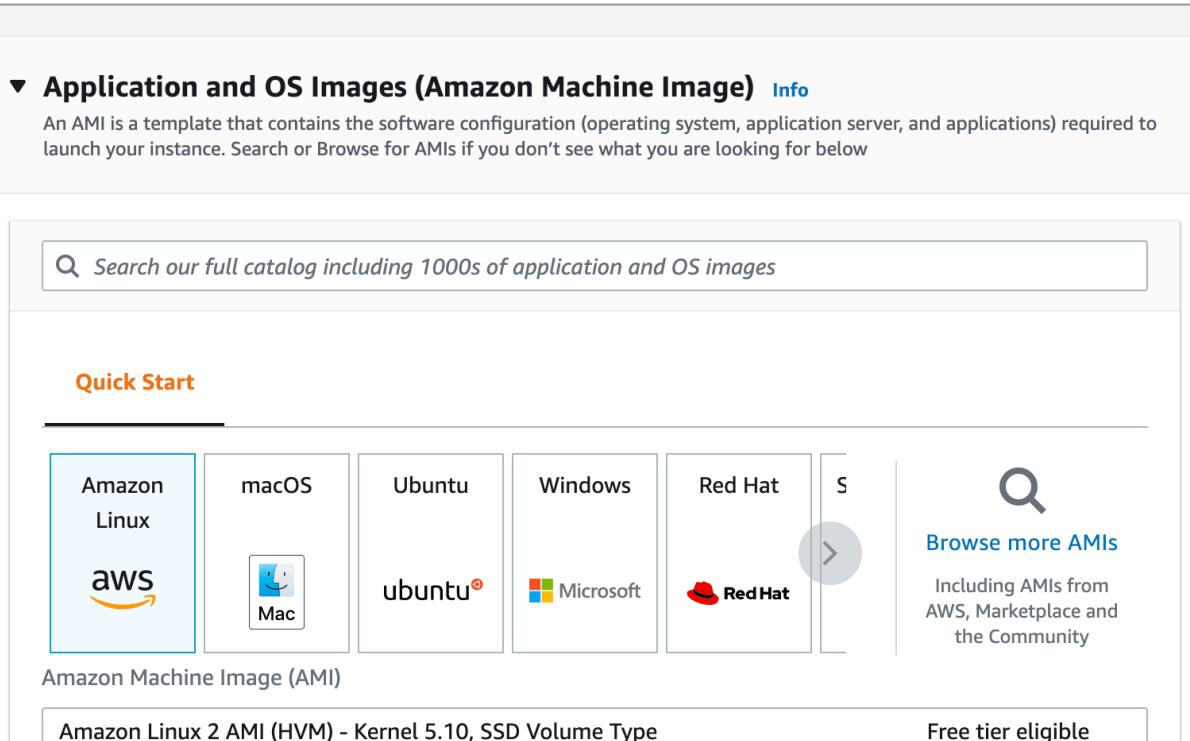


Figure 5: Creating Amazon Linux instance

Now select **t2.micro** for the instance type.

How many vCPUs will the instance have?

How much memory will it have?

How much will it cost per day to run?

If you selected, t2.medium, how much would it cost per day?

If you selected, t2.large, how much would it cost per day?

Now create a new key pair and save it to your local drive. This file contains your private key, and which you will need to connect to your instance. Accept all the other defaults.

Observe the **firewall group** that will be applied.

Which firewall ports are open on the instance?

What do you think is the main issue with this firewall setting?

How would you change it, once you have created the instance?

Observe the disk storage setting for the instance.

What type of disk will be used? [HDD/SSD]

What do you think is the advantage of using SSD?

For disk storage, what is the default size of the disk that you will create?

What is the maximum storage size for a free tier storage of the AMI instance we are creating?

C.1 Creating the instance

Go ahead and create the instance. Then go back to the AWS Management Console, and find your instance. Wait for it to set its state to running.

Now we will connect to it. For this we need to create an SSH connection and use the private key we have generated. The public key will be stored on the instance and will authenticate our access. We do not need a username or password to access the instance, as this is often insecure. Our PEM file will give us access (or you can use Putty for the connection).

Now, we will examine the details of our instance (Figure 6). On the instance summary, determine the following:

The public IP address:

The private IP address:

The instance type:

The public IPv4 DNS:

From your local host, can you ping the public IP address? [Yes/No]

Why can't you successfully ping your instance?

Which region of the world is your instance running in?

C.2 Enabling ICMP on firewall

Now, we will enable ICMP on the instance. First click on the Security tab of the instance summary, and then on the security group.

What is the firewall rule that is applied to the instance?

[SSH/Telnet/FTP/HTTP/HTTPPs] for [0.0.0.0/0 or 0.0.0.0/8 or 0.0.0.0/16 or 0.0.0.0/32]

What does 0.0.0.0/0 represent?

Now go ahead and add an ICMP rule for all hosts (Figure 7).

Can you now successfully ping your instance? [Yes/No]

Now, lock your ICMP rule down to just your IP address (you need to use a /32 address for this). Can you still successfully ping the instance? [Yes/No]

Ask your neighbour or one of the lab tutors to ping your instance. Can they successfully ping it? [Yes/No]

What is the advantage of applying the firewall in AWS, rather than in the instance?

EC2 > Instances > i-07b0512e24e263766

Instance summary for i-07b0512e24e263766 (MyLinuxServer) [Info](#)

Updated less than a minute ago

Instance ID	Public IPv4 address	Private IPv4 addresses
i-07b0512e24e263766 (MyLinuxServer)	52.90.3.121 open address	172.31.16.186
IPv6 address	Instance state	Public IPv4 DNS
-	Pending	ec2-52-90-3-121.compute-1.amazonaws.com open address
Hostname type	Private IP DNS name (IPv4 only)	Elastic IP addresses
IP name: ip-172-31-16-186.ec2.internal	ip-172-31-16-186.ec2.internal	-
Answer private resource DNS name	Instance type	AWS Compute Optimizer finding
IPv4 (A)	t2.micro	Opt-in to AWS Compute Optimizer for recommendations.
Auto-assigned IP address	VPC ID	Learn more
52.90.3.121 [Public IP]	vpc-0683f9b3d1038fd71	
IAM Role	Subnet ID	Auto Scaling Group name
-	subnet-00bdb3e7927760f46	-

[Details](#) [Security](#) [Networking](#) [Storage](#) [Status checks](#) [Monitoring](#) [Tags](#)

► Instance details [Info](#)

Figure 6: Details of instance

Inbound rules | Outbound rules | Tags

ⓘ You can now check network connectivity with Reachability Analyzer [Run Reachability Analyzer](#) X

Inbound rules (2)

Name	Security group rule...	IP version	Type	Protocol	Port
-	sgr-0ed01ab1ba175fe5b	IPv4	SSH	TCP	22
-	sgr-04b533407d759a...	IPv4	All ICMP - IPv4	ICMP	All

Figure 7: Enable ICMP

C.3 Accessing your instance

Now we will connect to our instance. For this you need SSH (such as provided by OpenSSH). This may be installed on the host you are using (such as in vSoC 2), or from Apps Anywhere. Once you have SSH, press **Connect** on the summary page, and you should then have tabs for **Connect to instance** (Figure 8). Next select the SSH client tab, and you will see the details of connecting to your instance with SSH.

The screenshot shows the 'Connect to instance' page for an EC2 instance with ID i-07b0512e24e263766 (MyLinuxServer). The page has tabs for 'EC2 Instance Connect', 'Session Manager', 'SSH client' (which is highlighted in orange), and 'EC2 serial console'. Below the tabs, there is an 'Instance ID' section with a copy icon and the text 'i-07b0512e24e263766 (MyLinuxServer)'. A numbered list provides instructions for connecting via SSH:

1. Open an SSH client.
2. Locate your private key file. The key used to launch this instance is mynewkeypair.pem
3. Run this command, if necessary, to ensure your key is not publicly viewable.
 chmod 400 mynewkeypair.pem
4. Connect to your instance using its Public DNS:
 ec2-52-90-3-121.compute-1.amazonaws.com

Below the list is an 'Example:' section with a command line entry:

ssh -i "mynewkeypair.pem" ec2-user@ec2-52-90-3-121.compute-1.amazonaws.com

Figure 8: Connect to instance

Now find your PEM file on your local machine (from the command line), and protect it with:

chmod 400 myfile.pem

What protection does this put on your private key?

Next, use the SSH connection with the name of your PEM file and with the DNS (or IP address) for your instance. For example, in the case in Figure 8, we have:

ssh -i "mynewkeypair.pem" ec2-user@ec2-52-90-3-121.compute-1.amazonaws.com

What is the name of the user that logs in?

An example of connecting is:

```
% ssh -i "mynewkeypair.pem" ec2-user@ec2-52-90-3-121.compute-1.amazonaws.com
The authenticity of host 'ec2-52-90-3-121.compute-1.amazonaws.com (52.90.3.121)'
can't be established.
ED25519 key fingerprint is SHA256:/c5UOK6gprKL19XCptNQ1brb9MpYR5wEeqhD/6t+/wk.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:48: ec2-3-90-189-201.compute-1.amazonaws.com
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-52-90-3-121.compute-1.amazonaws.com' (ED25519) to
the list of known hosts.
Last login: Fri Sep 30 17:07:00 2022 from ec2-18-206-107-27.compute-1.amazonaws.com
```

```
 _\|_(_\|- /) Amazon Linux 2 AMI
```

```
https://aws.amazon.com/amazon-linux-2/  
[ec2-user@ip-172-31-16-186 ~]$
```

Have you managed to connect? [Yes/No]

By using “ip addr show” or “ifconfig” in your instance, what is the private IP address of it?

Can you ping 8.8.8.8 from your instance? [Yes/No]

Is there a folder named .ssh? [Yes/No]

What do you think is the purpose of the file contained in .ssh?

Now create a folder in the top level named “mytestfolder”, and put a new file in there named “mytext.txt” (and put some text in this file).

Now go to the EC2 Instance Connect (Figure 8), and press on the Connect button. You should now get a console terminal in the browser.

From your console (Figure 9), verify that your file has been created. Has it been created in the instance? [Yes/No]

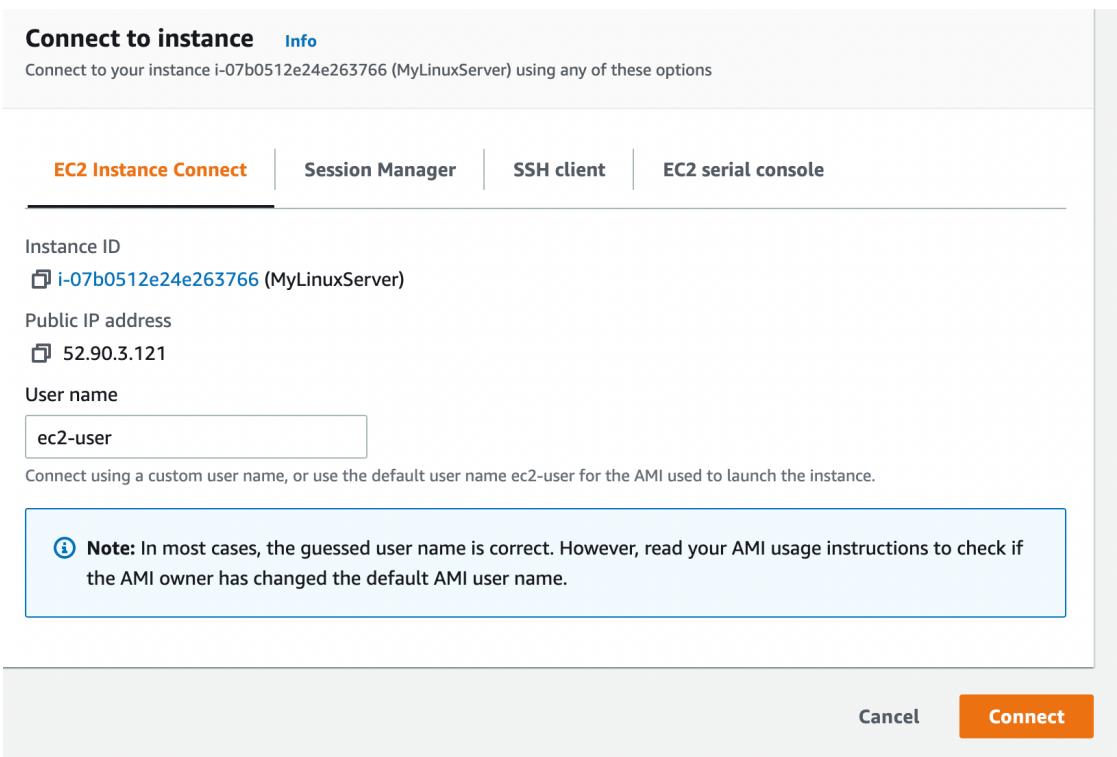


Figure 8: EC2 Instance Connect

```
Last login: Sun Oct 2 11:39:05 2022 from host86-131-160-187.range86-131.btcentralplus.com
[ec2-user@ip-172-31-16-186 ~]$ cd mytestfolder/
[ec2-user@ip-172-31-16-186 mytestfolder]$ ls
mytext.txt
[ec2-user@ip-172-31-16-186 mytestfolder]$ cat mytext.txt
Test
[ec2-user@ip-172-31-16-186 mytestfolder]$
```

Figure 9: EC2 Instance Connect terminal

Now examine the running services on the instance with:

```
$ netstat -i | grep tcp
$ netstat -i | grep udp
```

Which of the main services are running:

C.4 Installing a Web server

Now we will install a Web server on the instance with:

```
sudo yum update -y
sudo yum install -y httpd.x86_64
sudo systemctl start httpd.service
sudo systemctl enable httpd.service
```

Next open up a browser on your computer and access your instance for Web access.

Can you connect to it? [Yes/No]

Why can't you connect to it?

Now enable a firewall rule on Port 80 and Port 443 and allow access for Web traffic (see Figure 10).

Inbound rules Info								
Security group rule ID	Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info			
sgr-0ed01ab1ba175fe5b	SSH	TCP	22	Custom ▼ <input type="text" value="0.0.0.0/0"/> X	All access to Web server	Delete		
sgr-04b533407d759a286	All ICMP - IPv4	ICMP	All	Anywh... ▼ <input type="text" value="0.0.0.0/0"/> X	Ping	Delete		
-	HTTPS	TCP	443	Anywh... ▼ <input type="text" value="0.0.0.0/0"/> X	All access to Web server	Delete		
-	HTTP	TCP	80	Anywh... ▼ <input type="text" value="0.0.0.0/0"/> X	All access to Web server	Delete		

Figure 10: Enable HTTP and HTTPS rules

Can you now connect to your Web site? [Yes/No] (see Figure 11)

The screenshot shows a web browser window with the address bar displaying 'Not Secure | 52.90.3.121'. The main content area has a red header bar with the text 'Test Page'. Below the header, there is a message: 'This page is used to test the proper operation of the Apache HTTP server after it has been installed. If you can read this page, it means that the Apache HTTP server installed at this site is working properly.' There are two sections of text: 'If you are a member of the general public:' and 'If you are the website administrator:'. Both sections include links to configuration files. At the bottom right, there is a 'Powered by APACHE 2.4' logo.

Figure 11: Sample access to Web site

Now go into the /var/www folder, and create a file named “index.html”, and add:

```
<h1>Main web site</h1>
<p>Hello to you</p>
```

And then save the file.

Has it changed the welcome? [Yes/No]

C.6 Auditing

The main logging output is in the /var/log folder. Go into this folder and observe some of the files in there. Identify the contents of the following files:

What are the likely contents of the “secure” file?

What are the likely contents of the “boot.log” file?

List the log/httpd/access_log file. What are its contents? Can you identify your browser access? (see Figure 12). Which browser type accessed your Web server?

Now try with another browser type (such as Firefox or Chrome) and re-examine the log/httpd/access_log file. Did it detect the new browser type?

Now access a file that does not exist in your site (such as http://AWSIP/test.htm). Now re-examine the log/httpd/access_log file. What is the status code returned for the access?

```
e/105.0.0.0 Safari/537.36"
187 - - [02/Oct/2022:11:56:24 +0000] "GET /icons/apache_pb2.gif HTTP/1.1" 200 13 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36"
187 - - [02/Oct/2022:11:56:24 +0000] "GET /favicon.ico HTTP/1.1" 404 13 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36"
187 - - [02/Oct/2022:11:58:16 +0000] "-" 408 13 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36"
187 - - [02/Oct/2022:12:12:22 +0000] "GET / HTTP/1.1" 200 13 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36"
187 - - [02/Oct/2022:12:19:53 +0000] "GET / HTTP/1.1" 200 13 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36"
187 - - [02/Oct/2022:12:19:53 +0000] "GET /favicon.ico HTTP/1.1" 404 13 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36"
187 - - [02/Oct/2022:12:19:54 +0000] "GET / HTTP/1.1" 304 13 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36"
187 - - [02/Oct/2022:12:19:56 +0000] "GET / HTTP/1.1" 304 13 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36"
```

Figure 12: Sample list of log/httpd/access_log

C.7 Adding a new user

The ec2_user can be used to connect back into the server using access authenticated with the private key. We will now create a new user named “napier”, and which can connect to the instance with SSH. For this we use adduser and passwd on the Linux instance:

```
[ec2-user@ip-172-31-16-186 ~]$ sudo adduser napier
[ec2-user@ip-172-31-16-186 ~]$ sudo passwd napier
Changing password for user napier.
New password: <yourpass>
Retype new password: <yourpass>
passwd: all authentication tokens updated successfully.
```

Now we will add the new user to the login. For this, we use:

```
[ec2-user@ip-172-31-16-186 .ssh]$ sudo nano /etc/ssh/sshd_config
Add line of (see Figure 13):
AllowUsers ec2-user napier
Change the following to "yes" (see Figure 14):
PasswordAuthentication yes
```

Now restart the SSH service with:

```
[ec2-user@ip-172-31-16-186 .ssh]$ sudo systemctl restart sshd
```

Can you now connect to your instance with the new user and password:

```
ssh napier@54.209.145.85
```

Can you connect with the new user? [Yes/No]

```
#      $OpenBSD: sshd_config,v 1.100 2016/08/15 12:32:04 naddy Exp $
AllowUsers ec2-user napier
# This is the sshd server system-wide configuration file. See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/usr/bin

# The strategy used for options in the default sshd_config shipped with
```

Figure 13: Accessing instances

```
# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication yes
#PermitEmptyPasswords no
PasswordAuthentication yes

# Change to no to disable s/key passwords
#ChallengeResponseAuthentication yes
ChallengeResponseAuthentication no
```

Figure 14: Accessing instances

C.8 Accessing from AWS prompt

We can also access our instance from the AWS terminal prompt. For this return to your AWS Academy console, and enter the command (Figure 13):

```
$ aws ec2 describe-instances
```

From the results, can you identify the following.

Instance type:

Public IP address:

Private IP address:

State:

```

ddd_v1_w_W3n_1455598@runweb63093:~$ aws ec2 describe-instances
{
    "Reservations": [
        {
            "Groups": [],
            "Instances": [
                {
                    "AmiLaunchIndex": 0,
                    "ImageId": "ami-026b57f3c383c2ec",
                    "InstanceId": "i-07b0512e24e263766",
                    "InstanceType": "t2.micro",
                    "KeyName": "mynewkeypair",
                    "LaunchTime": "2022-10-02T11:14:16+00:00",
                    "Monitoring": {
                        "State": "disabled"
                    },
                    "Placement": {
                        "AvailabilityZone": "us-east-1b",
                        "GroupName": "",
                        "Tenancy": "default"
                    },
                    "PrivateDnsName": "ip-172-31-16-186.ec2.internal",
                    "PrivateIpAddress": "172.31.16.186",
                    "ProductCodes": [],
                    "PublicDnsName": "ec2-52-90-3-121.compute-1.amazonaws.com",
                    "PublicIpAddress": "52.90.3.121",
                    "State": {
                        "Code": 16,
                        "Name": "running"
                    },
                    "StateTransitionReason": "",
                    "SubnetId": "subnet-00bdb2e7927760f46",
                    "VpcId": "vpc-0683f9b3d1038fd71",
                    "Architecture": "x86_64"
                }
            ]
        }
    ]
}

```

Figure 15: Accessing instances

Now try we will stop our instance using an AWS EC2 command. Run the following with your instance ID (see Figure 16):

```
aws ec2 stop-instances --instance-ids [My-instance-ID]
```

From the AWS Management Console, has your instance stopped? [Yes/No]

```

ddd_v1_w_W3n_1455598@runweb62964:~$ aws ec2 stop-instances --instance-ids i-07b0512e24e263766
{
    "StoppingInstances": [
        {
            "CurrentState": {
                "Code": 64,
                "Name": "stopping"
            },
            "InstanceId": "i-07b0512e24e263766",
            "PreviousState": {
                "Code": 16,
                "Name": "running"
            }
        }
    ]
}
ddd_v1_w_W3n_1455598@runweb62964:~$ █

```

Figure 16: Stopping an instance

Now we will restart the instance, with:

```
aws ec2 start-instances --instance-ids [My-instance-ID]
```

Has the instance re-started? [Yes/No]

Now we will change the instance type from t3.micro to t3.small. To do this, run the following commands:

```
aws ec2 stop-instances --instance-ids [My-instance-ID]
aws ec2 wait instance-stopped --instance-ids [My-instance-ID]
aws ec2 modify-instance-attribute --instance-id [My-instance-ID] --instance-type "{\"Value\": \"t3.small\"}"
aws ec2 start-instances --instance-ids [My-instance-ID]
```

Did it change the instance type? [Yes/No]

Can you still get access to your instance?

By observing the script, and investigate what t3.micro and t3.small are, can you determine what has changed about your instance?

Now, revert the instance back to t3.micro, and suspend the instance.

D Creating and Securing a Windows 2022 Server

In this part of the lab we will create a Windows 2022 server instance with t3.micro (note, that this is very low for vCPUs and memory, so the performance may be a little lacking). First create a new instance, and give it a name, such as “MyWindowsServer” (Figure 17).

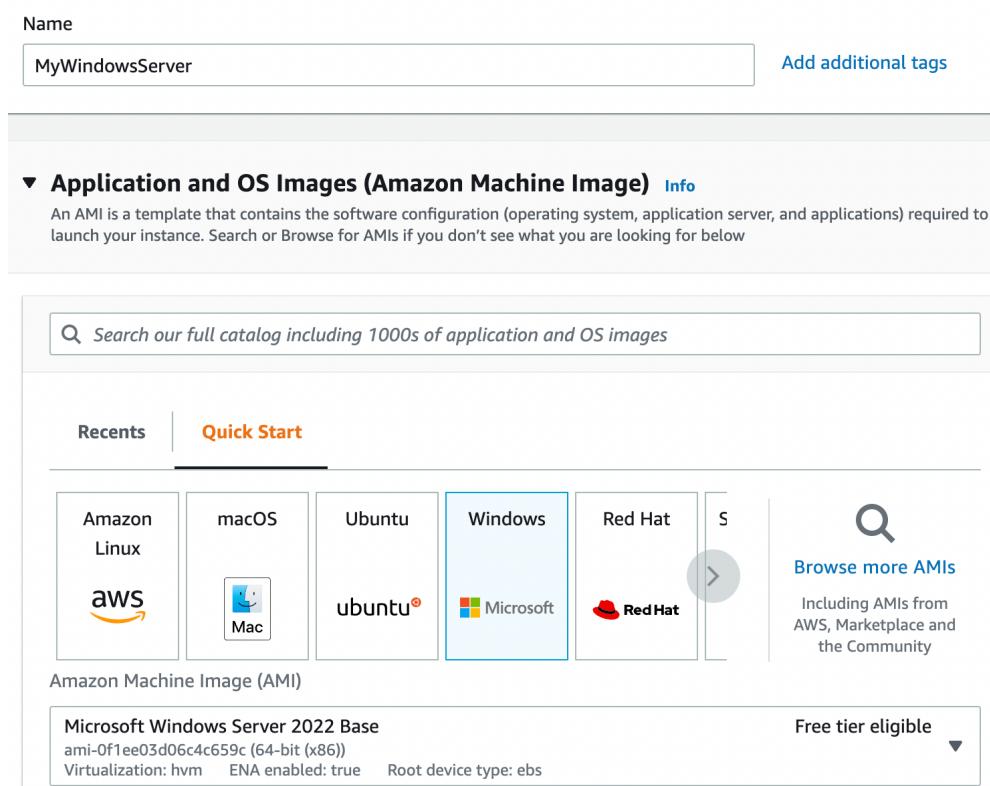


Figure 17: Creating Windows 2022 instance

Now select **t2.micro** for the instance type.

How many vCPUs will the instance have?

How much memory will it have?

How much will it cost per day to run?

If you selected, t2.medium, how much would it cost per day?

If you selected, t2.large, how much would it cost per day?

Now create a new key pair and save it to your local drive. This file contains your private key, and which you will need to connect to your instance. Accept all the other defaults.

Observe the firewall group that will be applied.

Which firewall ports are open on the instance?

What is the main issue with this firewall setting?

How would you change it, once you have created the instance?

Observe the disk storage setting for the instance.

What type of disk will be used? [HDD/SSD]

What is the advantage of using SSD?

For disk storage, what is the size of the disk that you will create?

What is the maximum storage size for a free tier storage of the AMI instance we are creating?

D.1 Creating the instance

Go ahead and create the instance. Go back to the Management Console and find your instance. Wait for it to set its state to running. Now we will connect to it. For this we need to create an RDP connection, and use the private key we have generated to generate the initial password.

Now, we will examine the details of our instance (Figure 18). On the instance summary, determine the following:

The public IP address:

The private IP address:

The instance type:

The public IPv4 DNS:

From your local host, can you ping the public IP address? [Yes/No]

Why can't you successfully ping your instance?

Which region of the world is your instance running in?

C.2 Enabling ICMP on firewall

Now we will enable ICMP on the instance. First click on the Security tab of the instance summary, and then on the security group.

What is the firewall rule that is applied to the instance?

[SSH/RDP/Telnet/FTP/HTTP/HTTPs] for [0.0.0.0/0 or 0.0.0.0/8 or 0.0.0.0/16 or 0.0.0.0/32]

What does 0.0.0.0/0 represent?

Now go ahead and add an ICMP rule for all hosts (Figure 19).

Can you now successfully ping your instance? [Yes/No]

We will not be able to ping the instance yet, as the firewall on Windows is disabling it.

Instance summary for i-07d723258364f7172 (MyWindowsServer)			Info		Connect	Instance state ▾	Actions ▾
Updated less than a minute ago							
Instance ID i-07d723258364f7172 (MyWindowsServer)	Public IPv4 address 54.83.154.0 open address	Private IPv4 addresses 172.31.85.24					
IPv6 address -	Instance state Running	Public IPv4 DNS ec2-54-83-154-0.compute-1.amazonaws.com open address					
Hostname type IP name: ip-172-31-85-24.ec2.internal	Private IP DNS name (IPv4 only) ip-172-31-85-24.ec2.internal	Elastic IP addresses -					
Answer private resource DNS name IPv4 (A)	Instance type t2.micro	AWS Compute Optimizer finding Opt-in to AWS Compute Optimizer for recommendations. Learn more					
Auto-assigned IP address 54.83.154.0 [Public IP]	VPC ID vpc-0683f9b3d1038fd71	Auto Scaling Group name -					
IAM Role -	Subnet ID subnet-07a3be17bcc59528b						
Details Security Networking Storage Status checks Monitoring Tags							

Figure 18: Details of instance

Inbound rules Info						
Security group rule ID	Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info	
sgr-0101b70fb7c795a97	RDP	TCP	3389	Custom ▾	Q <input type="text"/> 0.0.0.0/0 X	Delete
-	Custom ICMP - IPv4	All	All	Anywh... ▾	Q <input type="text"/> Ping All <input type="text"/> 0.0.0.0/0 X	Delete

Figure 19: Enable ICMP

D.3 Accessing your instance

Now we will connect to our instance. For this you need RDP. Next Connect to instance (Figure 20). Click on “Get password” and present your PEM file, and it should reveal the password (Figure 21).

The screenshot shows the AWS EC2 instance connection interface. At the top, there are three tabs: "Session Manager", "RDP client" (which is highlighted in orange), and "EC2 serial console". Below the tabs, the "Instance ID" is listed as "i-07d723258364f7172 (MyWindowsServer)". Under "Connection Type", there are two options: "Connect using RDP client" (selected) and "Connect using Fleet Manager". The "RDP client" section includes a note: "Download a file to use with your RDP client and retrieve your password." The "Fleet Manager" section includes a note: "To connect to the instance using Fleet Manager Remote Desktop, the SSM Agent must be installed and running on the instance. For more information, see [Working with SSM Agent](#)".

You can connect to your Windows instance using a remote desktop client of your choice, and by downloading and running the RDP shortcut file below:

[Download remote desktop file](#)

When prompted, connect to your instance using the following details:

Public DNS

[ec2-54-83-154-0.compute-1.amazonaws.com](#)

User name

[Administrator](#)

Password [Get password](#)

Figure 20: Connect to instance

Connection Type

● Connect using RDP client

Download a file to use with your RDP client and retrieve your password.

● Connect using Fleet Manager

To connect to the instance using Fleet Manager Remote Desktop, the SSM Agent must be installed and running on the instance. For more information, see [Working with SSM Agent](#)

You can connect to your Windows instance using a remote desktop client of your choice, and by downloading and running the RDP shortcut file below:

 [Download remote desktop file](#)

When prompted, connect to your instance using the following details:

Public DNS

 ec2-54-83-154-0.compute-1.amazonaws.com

User name

 Administrator

Password

 7s8l-G?Jzzh;Lb8%KyGdmn6JwqReoRF-

Figure 21: Reveal password

Have you managed to connect? [Yes/No] (Figure 22)

By using “ipconfig” in your instance, what is the private IP address of it?

Can you ping 8.8.8.8 from your instance? [Yes/No]

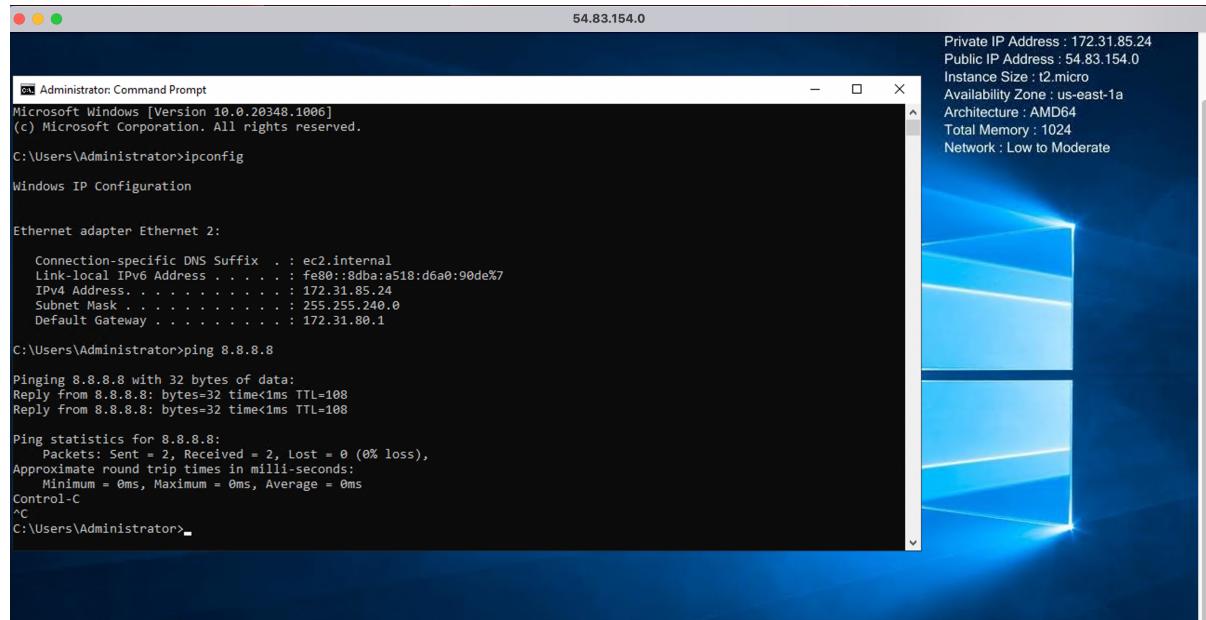


Figure 22: Windows 2022

D.4 Enable ICMP on instance

We have enabled the AWS firewall for ICMP. Now we will open-up ICMP in the instance. For this open-up with Advanced Windows firewall, and enable the rule for “File and Printer Sharing (ICMP-in) – as shown in Figure 23.

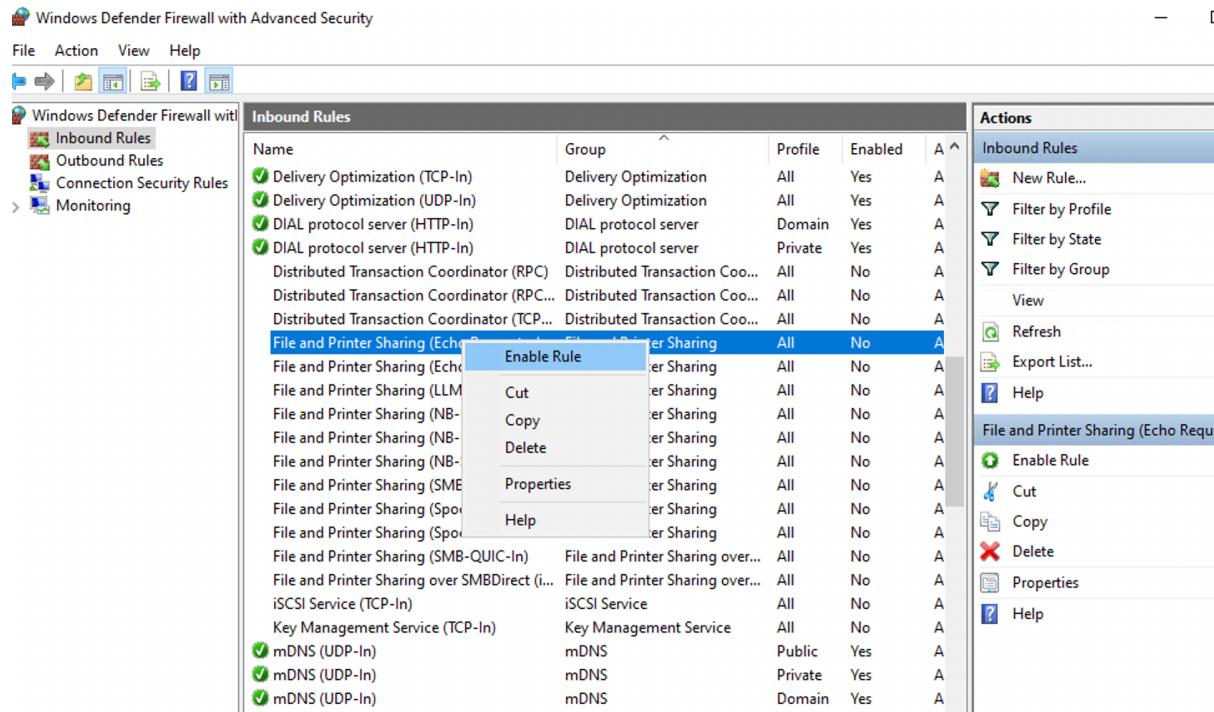


Figure 23: Enable ICMP

Can you successfully ping the instance from your instance? [Yes/No]

D.5 Show running services

Now examine the running services on the instance with:

```
$ netstat -i | grep tcp  
$ netstat -i | grep udp
```

Which of the main services are running?

D.5 Enable Web server

Now select Server Manage, and “Add a Role” for Web Server (IIS) (Figure 24).

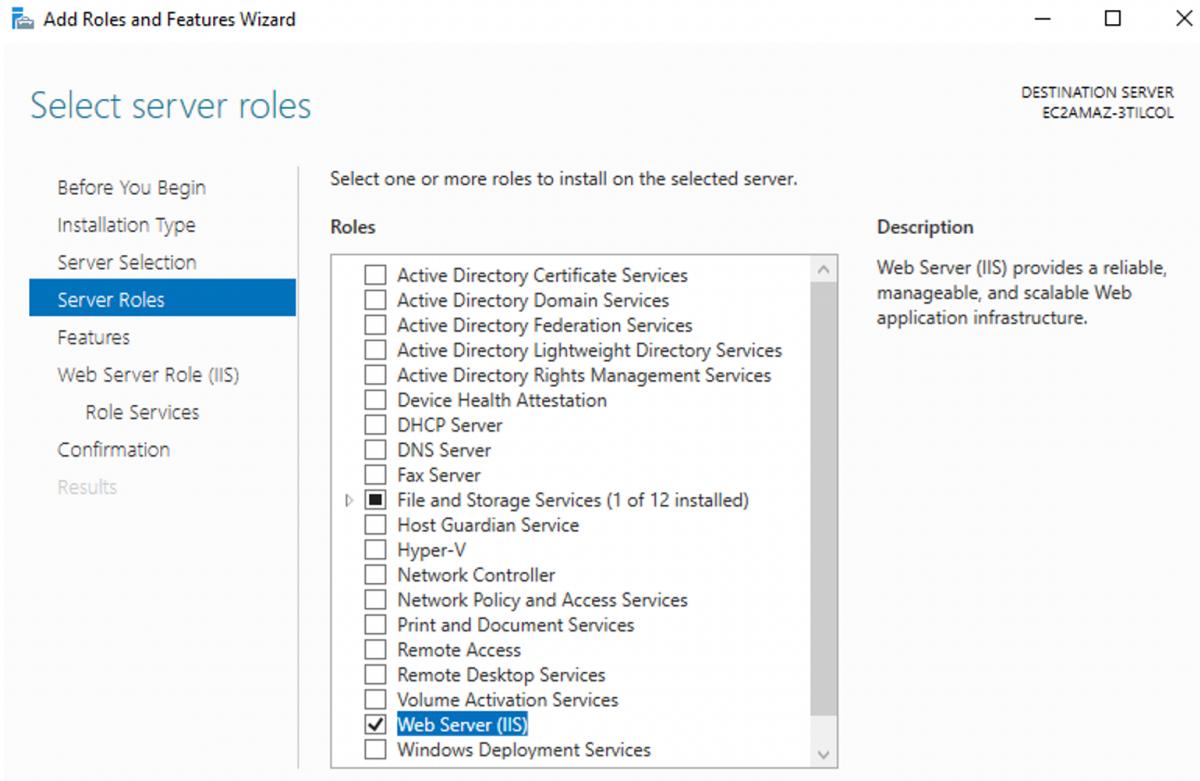


Figure 24: Enable ICMP

Now open a browser on the instance, and access <http://localhost>

Can you connect to the IIS Web server? [Yes/No]

Now open up your AWS firewall for Port 80 (Figure 24).

Inbound rules Info						
Security group rule ID	Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info	
sgr-088cf5bfd7b0741f4	All ICMP - IPv4	ICMP	All	Custom ▾	<input type="text"/> Q 0.0.0.0/0 X	Ping All Delete
sgr-0101b70fb7c795a97	RDP	TCP	3389	Custom ▾	<input type="text"/> Q 0.0.0.0/0 X	Delete
-	HTTP	TCP	80	Anywh... ▾	<input type="text"/> Q 0.0.0.0/0 X	Web Delete

Figure 23: Enable HTTP

Now open a browser on the instance, and access [http://\[IP of AWS\]](http://[IP of AWS])

Can you connect to the IIS Web server? [Yes/No] (Figure 23)

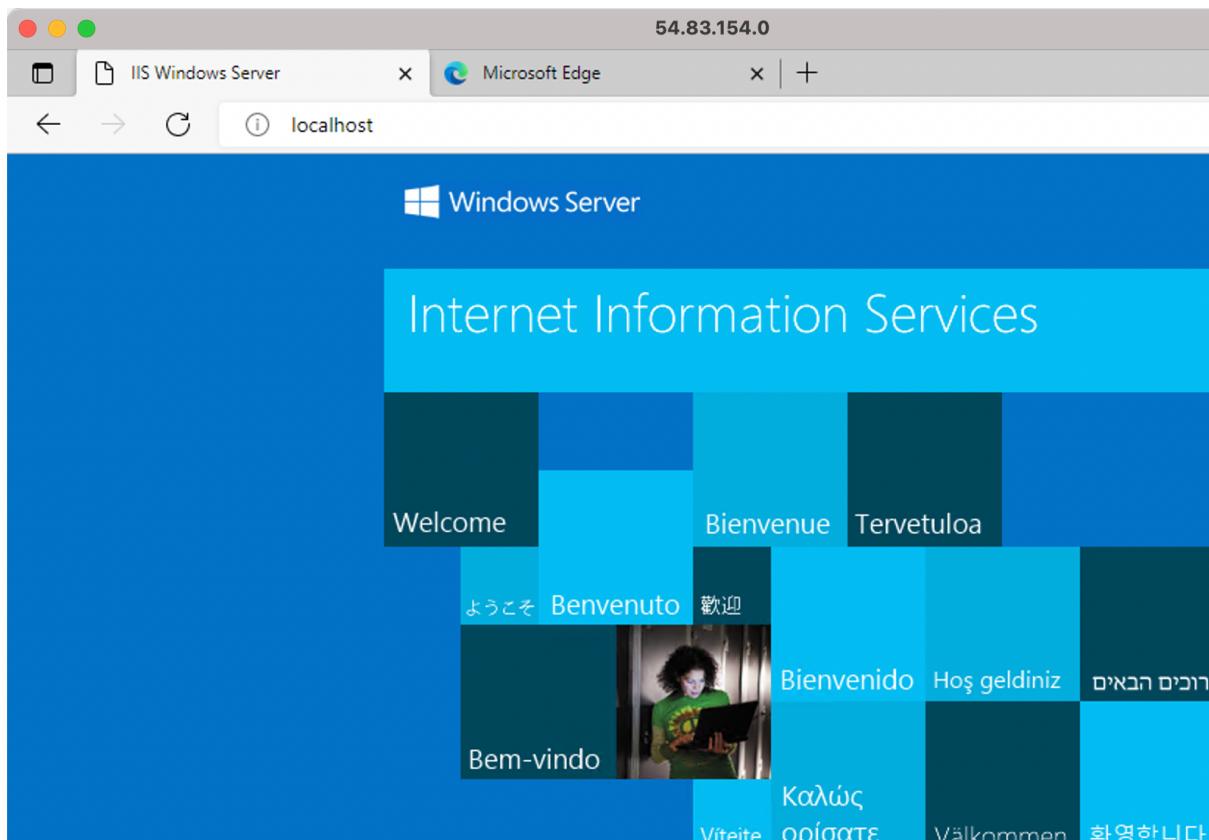


Figure 24: Local host

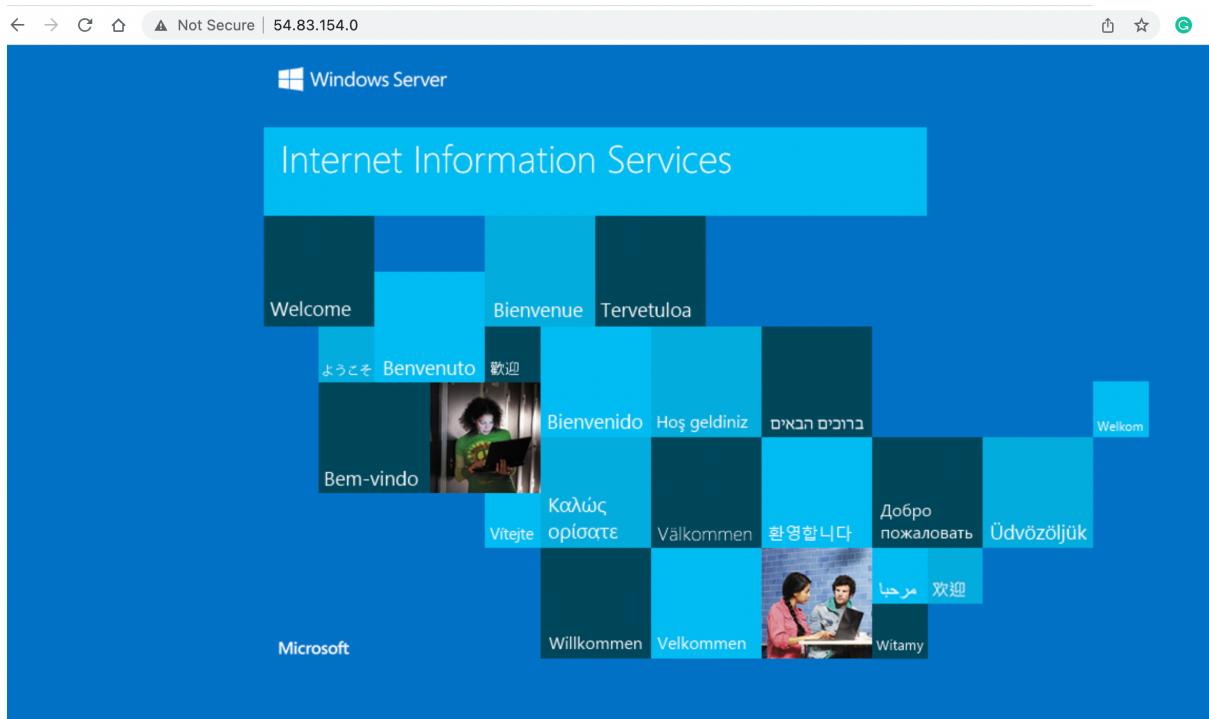


Figure 25: Remote access

Now go into the /inetpub/www folder, and create a file named “iisstart.html”, and add:

```
<h1>Main web site</h1>
```

```
<p>Hello to you</p>
```

And then save the file.

Has it changed the welcome? [Yes/No]

D.6 Auditing

The main logging output is in the “C:\inetpub\logs\LogFiles\W3SVC1” folder. Identify the contents of the following files:

Go into the “C:\inetpub\logs\LogFiles\W3SVC1” folder, and list the file in there. What are its contents? Can you identify your browser access? (see Figure 12). Which browser type accessed your Web server?

Now try with another browser type, and re-examine the log/httpd/access_log file. Did it detect the new browser type?

Now access a file that does not exist in your site (such as http://AWSIP/test.htm). Now re-examine the file. What is the status code returned for the access?

D.6 Changing Administrator password

We can change the Administrator password, with something like:

```
net user administrator mynewpassword$$7k1
```