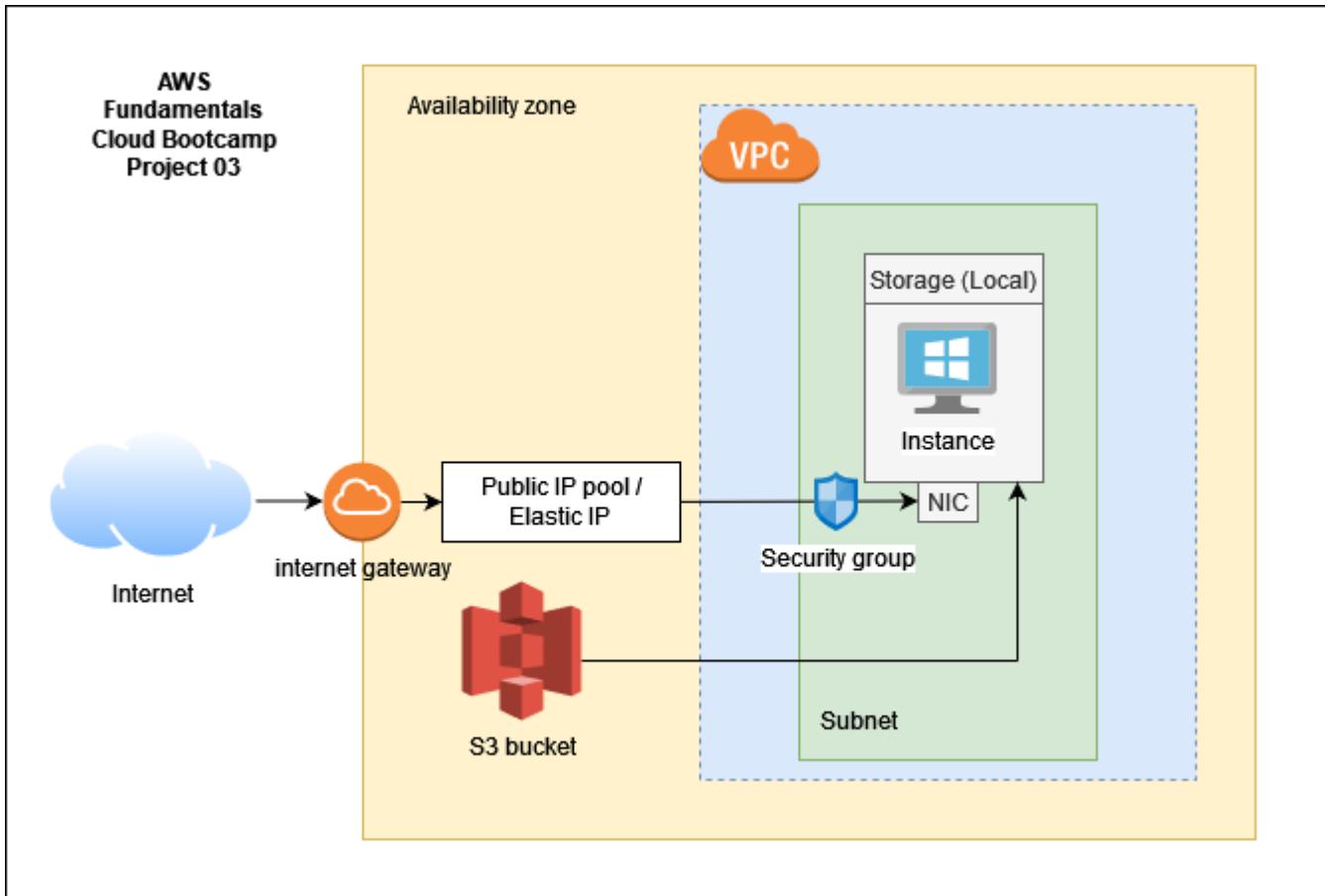


AWS Course Cloud Bootcamp Project 03

- High-level diagram



- AWS Console

Screenshot of the AWS Management Console homepage:

- Header:** AWS Management Console, Services, Thanaponwut, N. Virginia, Support.
- Search Bar:** Search for services, features, marketplace products, and docs.
- AWS services:**
 - Recently visited services: EC2, Billing, VPC, AWS Cost Explorer, S3, IAM.
 - All services: A list of various AWS services including Lambda, SNS, S3, CloudWatch, etc.
- Build a solution:** Get started with simple wizards and automated workflows.
 - Launch a virtual machine: With EC2, 2-3 minutes, icon of a server.
 - Build a web app: With Elastic Beanstalk, 6 minutes, icon of a cloud with a person.
 - Build using virtual servers: With Lightsail, 1-2 minutes, icon of a server with a plus sign.
- Stay connected to your AWS resources on-the-go:** AWS Console Mobile App now supports four additional regions. Download the AWS Console Mobile App to your iOS or Android mobile device. Learn more.
- Explore AWS:**
 - Amazon Location Service: Easily and securely add maps, search for points of interest, geocoding, routes, tracking, and geofencing to your application. Get started.
 - Amazon S3 Multi-Region Access Points: Accelerate performance by up to 60% when accessing replicated data sets. Learn more.
- Footer:** Feedback, English (US), © 2008 - 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved., Privacy Policy, Terms of Use, Cookie preferences.

- IAM Dashboard

The screenshot shows the AWS IAM Management Console dashboard. At the top, a blue banner introduces the new IAM dashboard experience, stating: "Introducing the new IAM dashboard experience. We've redesigned the IAM dashboard experience to make it easier to use. Let us know what you think." Below the banner, the dashboard is divided into several sections:

- Identity and Access Management (IAM)**: A sidebar with links to Dashboard, Access management (User groups, Users, Roles, Policies, Identity providers, Account settings), and Access reports (Access analyzer, Archive rules, Analyzers, Settings, Credential report, Organization activity, Service control policies (SCPs)).
- IAM dashboard**: A main area with "Security recommendations" (Root user has MFA, Root user has no active access keys) and "IAM resources" (User groups: 4, Users: 4, Roles: 3, Policies: 0, Identity providers: 0).
- AWS Account**: Displays Account ID (566339489303), Account Alias (566339489303 Create), and Sign-In URL (https://566339489303.sigin.aws.amazon.com/console).
- Quick Links**: My security credentials (Manage access keys, MFA), Policy simulator (Evaluate policies).
- What's new**: Lists recent updates from the IAM Access Analyzer.

At the bottom, there are links for Feedback, English (US), and various AWS services.

- User groups

- Admin – Provides full access to AWS services and resources.
- EC2_Admin – Provides full access to Amazon EC2 via the AWS Management Console.
- Readonly - Provides read-only access to AWS services and resources.
- S3_Admin - Provides full access to all buckets via the AWS Management Console.

The screenshot shows the AWS IAM Management Console User groups page. The sidebar on the left includes links for Dashboard, Access management (User groups, Users, Roles, Policies, Identity providers, Account settings), and Access reports (Access analyzer, Archive rules, Analyzers, Settings, Credential report, Organization activity, Service control policies (SCPs)).

The main content area displays the "User groups (4) info" section, which states: "A user group is a collection of IAM users. Use groups to specify permissions for a collection of users." It includes a search bar ("Filter User groups by property or group name and press enter") and a table with columns: Group name, Users, Permissions, and Creation time. The table lists four user groups:

Group name	Users	Permissions	Creation time
Admin	1	Defined	11 minutes ago
EC2_Admin	1	Defined	10 minutes ago
Readonly	1	Defined	8 minutes ago
S3_Admin	1	Defined	9 minutes ago

At the bottom, there are links for Feedback, English (US), and various AWS services.

- Users

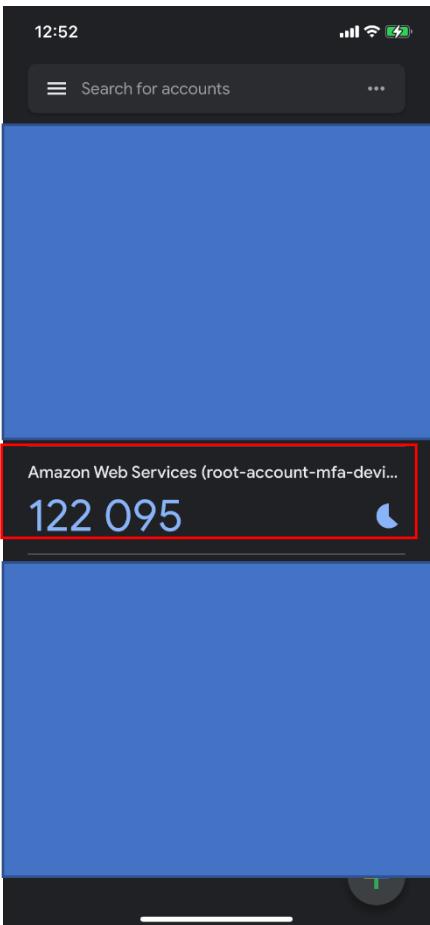
The screenshot shows the IAM Management Console with the 'Users' list page. The left sidebar includes options like Dashboard, Access management (Users selected), Roles, Policies, Identity providers, Account settings, Access reports, Access analyzer, Archive rules, Analyzers, Settings, Credential report, Organization activity, and Service control policies (SCPs). The main area displays a table of users with columns: User name, Groups, Last activity, MFA, Password age, and Active key age. The users listed are EC2admin, S3Admin, Thanapon, and Viewuser.

- Test log in to Viewuser (View only user) and try to create new user

The screenshot shows the 'Add user' wizard at Step 4: Review. The user 'test' has been created with 'AWS Management Console access - with a password'. A warning message states: 'This user has no permissions. You haven't given this user any permissions. This means that the user has no access to any AWS service or resource. Consider returning to the previous step and adding some type of permissions.' The 'Create user' button is visible at the bottom right.

- Configure MFA for enhanced security

The screenshot shows a browser window with two tabs: "aws portal - Google Search" and "Amazon Web Services Sign-In". The "Amazon Web Services Sign-In" tab is active, displaying the AWS multi-factor authentication (MFA) sign-in page. The page includes fields for "Email address" (set to "thanaponwut@hotmail.com"), "MFA code" (an input field), and a "Submit" button. Below these are links for "Troubleshoot MFA" and "Cancel". To the right of the sign-in form is an advertisement for "Amazon MemoryDB for Redis", which features the AWS logo and a dark background with white text and graphics illustrating a database system.



- VPC Dashboard

The screenshot shows the AWS VPC Management Console Dashboard. On the left, a sidebar lists various VPC-related services: VPC Dashboard, EC2 Global View, Filter by VPC, VIRTUAL PRIVATE CLOUD (Your VPCs, Subnets, Route Tables, Internet Gateways, Egress Only Internet Gateways, Carrier Gateways, DHCP Options Sets, Elastic IPs, Managed Prefix Lists, Endpoints, Endpoint Services, NAT Gateways, Peering Connections). In the center, the "Resources by Region" section displays a grid of resources across the N. Virginia region. The resources include: VPCs (1), NAT Gateways (0), Subnets (6), VPC Peering Connections (0), Route Tables (1), Network ACLs (1), Internet Gateways (1), Security Groups (2), Egress-only Internet Gateways (0), Customer Gateways (0), DHCP options sets (1), Virtual Private Gateways (0), and Elastic IPs (0). The "Service Health" section indicates that Amazon EC2 - US East (N. Virginia) is operating normally. The "Settings" section includes links to Zones, Console Experiments, and Additional Information (VPC Documentation, All VPC Resources, Forums, Report an Issue). The "Transit Gateway Network Manager" section provides information about managing global network access.

- Your VPCs

The screenshot shows the AWS VPC Management Console under the "Your VPCs" section. The sidebar remains the same as the previous dashboard. The main area displays a table titled "Your VPCs (1/1) Info" showing one VPC entry: "Name" (vpc-089e8422cc8823a98), "VPC ID" (vpc-089e8422cc8823a98), "State" (Available), "IPv4 CIDR" (172.31.0.0/16), and "IPv6 CIDR (Network border group)" (None). Below the table, a detailed view for "vpc-089e8422cc8823a98" is shown. The "Details" tab is selected, displaying the following information: VPC ID (vpc-089e8422cc8823a98), State (Available), DNS hostnames (Enabled), and DNS resolution (Enabled).

- VPC details

The screenshot shows the AWS VPC Management Console with the URL <https://console.aws.amazon.com/vpc/home?region=us-east-1#VpcDetails:VpcId=vpc-089e8422cc8823a98>. The main content area displays the details of a VPC named **vpc-089e8422cc8823a98**. The **Details** tab is selected, showing the following configuration:

VPC ID	State	DNS hostnames	DNS resolution
vpc-089e8422cc8823a98	Available	Enabled	Enabled
Tenancy	DHCP options set	Main route table	Main network ACL
Default	dopt-0d428151868dc0476	rtb-068df21b4950fca19	acl-049eb3e521418e444
Default VPC	IPv4 CIDR	IPv6 pool	IPv6 CIDR (Network border group)
Yes	172.31.0.0/16	-	-
Route 53 Resolver DNS Firewall rule groups	Owner ID		
-	566339489303		

Below the details, there are tabs for **CIDRs**, **Flow logs**, and **Tags**. The **IPv4 CIDRs** section shows one entry: **172.31.0.0/16**.

- VPC subnets

The screenshot shows the AWS Subnets page with the URL <https://console.aws.amazon.com/vpc/home?region=us-east-1#subnets:>. The main content area displays a list of subnets under the heading **Subnets (1/6)**. The table shows the following data:

Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR
subnet-04cbe02bbdee54c2	subnet-04cbe02bbdee54c2	Available	vpc-089e8422cc8823a98	172.31.80.0/20	-
subnet-0610f177f55511374	subnet-0610f177f55511374	Available	vpc-089e8422cc8823a98	172.31.16.0/20	-
subnet-0b3655e897f7b9b4d	subnet-0b3655e897f7b9b4d	Available	vpc-089e8422cc8823a98	172.31.32.0/20	-
subnet-0ff31b1fd890167d1	subnet-0ff31b1fd890167d1	Available	vpc-089e8422cc8823a98	172.31.48.0/20	-
subnet-05519493b68142ef5	subnet-05519493b68142ef5	Available	vpc-089e8422cc8823a98	172.31.0.0/20	-
subnet-0ff03bd9a4681495b	subnet-0ff03bd9a4681495b	Available	vpc-089e8422cc8823a98	172.31.64.0/20	-

Below the table, a detailed view of the subnet **subnet-04cbe02bbdee54c2** is shown. The **Details** tab is selected, displaying the following information:

Subnet ID	Subnet ARN	State	IPv4 CIDR
subnet-04cbe02bbdee54c2	arnaws:ec2:us-east-1:566339489303:subnet/subnet-04cbe02bbdee54c2	Available	172.31.80.0/20

- Routing table

- o IP in 172.31.0.0/16 is local IP.
- o All other IP are routed to internet gateway.

Route Table Details:

Route table ID	rtb-068df21b4950fca19	Main	Yes	Explicit subnet associations	-	Edge associations	-
VPC	vpc-089e8422cc8823a98	Owner ID	566339489303				

Routes (2):

Destination	Target	Status	Propagated
172.31.0.0/16	local	Active	No
0.0.0.0/0	igw-0de1e6a734b3ca57f	Active	No

- Internet gateways: virtual router that connect VPC to the internet.

Internet Gateways (1/1):

Name	Internet gateway ID	State	VPC ID	Owner
-	igw-0de1e6a734b3ca57f	Attached	vpc-089e8422cc8823a98	566339489303

Details:

Internet gateway ID	igw-0de1e6a734b3ca57f	State	Attached	VPC ID	vpc-089e8422cc8823a98	Owner	566339489303
---------------------	-----------------------	-------	----------	--------	-----------------------	-------	--------------

- Network ACLs: Inbound and Outbound rules for all subnets in a VPC (default value is allow all).

Details

Network ACL ID	Associated with	Default	VPC ID
acl-049eb3e521418e444	6 Subnets	Yes	vpc-089e8422cc8823a98

Inbound rules (2)

Rule number	Type	Protocol	Port range	Source	Allow/Deny
1	tcp	tcp	22	0.0.0.0/0	Allow
2	tcp	tcp	22	0.0.0.0/0	Allow

- Security groups: Inbound and Outbound rules for instances in VPC.

Security Groups (1/2)

Name	Security group ID	Security group name	VPC ID	Description	Owner
sg-05cf1c6c4457b493	my-security-group-01	vpc-089e8422cc8823a98	my-security-group-01 ...	566339489303	
sg-0f74849c6c5bb857c	default	vpc-089e8422cc8823a98	default VPC security gr...	566339489303	

sg-05cf1c6c4457b493 - my-security-group-01

Inbound rules (4)

Rule number	Type	Protocol	Port range	Source	Allow/Deny
1	tcp	tcp	22	0.0.0.0/0	Allow
2	tcp	tcp	22	0.0.0.0/0	Allow
3	tcp	tcp	22	0.0.0.0/0	Allow
4	tcp	tcp	22	0.0.0.0/0	Allow

- Configure inbound rules for new instance.
 - o HTTP and HTTPS for web services access.
 - o ICMP for PING command.
 - o RDP for remote desktop access from my IP only.

Security group name: my-security-group-01
 Security group ID: sg-05cf1c6c4457b493
 Description: my-security-group-01 created 2021-09-21T13:48:50.074-05:00
 Owner: 566339489303
 Inbound rules count: 4 Permission entries
 Outbound rules count: 1 Permission entry

Inbound rules (4)

Name	Security group rule...	IP version	Type	Protocol	Port range
sgr-0fe27a73e6bf69209	IPv4	HTTP	TCP	80	
sgr-0b640ad1f436ce0f7	IPv4	All ICMP - IPv4	ICMP	All	
sgr-01e427f6e1f53054d	IPv4	HTTPS	TCP	443	
sgr-0ff300cab1b7a4e99	IPv4	RDP	TCP	3389	

- Create and run a new instance.

Instances (1/1) Info

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 D
i-0179a47ae086177ae	Running	t2.micro	2/2 checks passed	No alarms	us-east-1b	ec2-18-212-6-	

Instance: i-0179a47ae086177ae

Details	Security	Networking	Storage	Status checks	Monitoring	Tags
Instance summary						
Instance ID: i-0179a47ae086177ae	Public IPv4 address: 18.212.6.39 open address	Private IPv4 addresses: 172.31.89.120				
IPv6 address: -	Instance state: Running	Public IPv4 DNS: ec2-18-212-6-39.compute-1.amazonaws.com open address				

- Instance details

The screenshot shows the AWS EC2 Instance Details page for an instance with ID i-0179a47ae086177ae. The left sidebar includes links for New EC2 Experience, EC2 Dashboard, EC2 Global View, Events, Tags, Limits, Instances (with sub-links for Instances, Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Scheduled Instances, Capacity Reservations), Images (AMIs), and Elastic Block Store (Volumes). The main content area has tabs for Details, Security, Networking, Storage, Status checks, Monitoring, and Tags. The Details tab is selected, showing the following instance details:

Setting	Value	Notes
Platform	AMI ID windows	Monitoring disabled
Platform details	AMI name Windows_Server-2016-English-Full-Base-2021.09.15	Termination protection Disabled
Launch time	AMI location Tue Sep 21 2021 14:01:14 GMT-0500 (Central Daylight Time) (about 1 hour)	Lifecycle normal
Stop-hibernate behavior	AMI Launch index disabled	Key pair name aws-ec2-demo
State transition reason	Credit specification standard	Kernel ID -
State transition message	Usage operation RunInstances:0002	RAM disk ID -
Owner	ClassicLink	Enclaves Support -
Boot mode	-	-

At the bottom, there are links for Feedback, English (US), Privacy Policy, Terms of Use, and Cookie preferences.

- Instance security tab

The screenshot shows the AWS EC2 Instance Security tab for the same instance. The left sidebar is identical to the previous screenshot. The main content area has tabs for Details, Security (selected), Networking, Storage, Status checks, Monitoring, and Tags. The Security tab shows the following security details:

Setting	Value	Notes
IAM Role	Owner ID EC2accessSS	Launch time Tue Sep 21 2021 14:01:14 GMT-0500 (Central Daylight Time)
Security groups	sg-05cf1c6c4457b493 (my-security-group-01)	-

Below this, the Inbound rules section shows a table of port ranges, protocols, sources, and security groups:

Port range	Protocol	Source	Security groups
80	TCP	0.0.0.0/0	my-security-group-01
3389	TCP	47.24.58.176/32	my-security-group-01
443	TCP	0.0.0.0/0	my-security-group-01
-1	ICMP	0.0.0.0/0	my-security-group-01

Below the inbound rules, the Outbound rules section shows a table with a single row:

Port range	Protocol	Source	Security groups
-	-	-	-

At the bottom, there are links for Feedback, English (US), Privacy Policy, Terms of Use, and Cookie preferences.

- Instance networking tab

The screenshot shows the AWS EC2 Instance Details page for an instance with ID i-0179a47ae086177ae. The Networking tab is selected. A message at the top says, "You can now check network connectivity with Reachability Analyzer." Below it, the Networking details section shows:

Public IPv4 address	Private IPv4 addresses	VPC ID
18.212.6.39 [open address]	172.31.89.120	vpc-089e8422cc8823a98
Public IPv4 DNS	Private IPv4 DNS	Subnet ID
ec2-18-212-6-39.compute-1.amazonaws.com [open address]	ip-172-31-89-120.ec2.internal	subnet-04cbe02bbdee54c2
IPv6 addresses	Secondary private IPv4 addresses	Availability zone
-	-	us-east-1b
Carrier IP addresses (ephemeral)	Outpost ID	-
-	-	

Below this, the Network Interfaces section shows one interface:

Network interfaces (1)

Filter network interfaces	
Network interface	Description
eni-04cbe02bbdee54c2	Attached to instance i-0179a47ae086177ae

- Instance storage tab (VM local disk)

The screenshot shows the AWS EC2 Instance Details page for the same instance. The Storage tab is selected. The Root device details section shows:

Root device name	Root device type	EBS optimization
/dev/sda1	EBS	disabled

The Block devices section shows a table of volumes attached to the instance:

Volume ID	Device name	Volume size (GiB)	Attachment status	Attachment time	Encrypted	KMS key ID
vol-013a66f73860a6f94	/dev/sda1	30	Attached	Tue Sep 21 2021 14:01:22 ...	No	-

A red box highlights the first row of this table.

Below the table, the Recent root volume replacement tasks section shows:

Task ID	Task state	Start time	Completion time	Tags
No recent replace root volume tasks				

- Instance status checks tab

The screenshot shows the AWS EC2 Instance Details page for instance i-0179a47ae086177ae. The Status Checks tab is selected. Key details shown include:

- System status checks:** System reachability check passed.
- Instance status checks:** Instance reachability check passed.
- Report instance status:** A button to report the instance status.

The left sidebar shows the Instances section with options like Instances, Instance Types, Launch Templates, and Spot Requests.

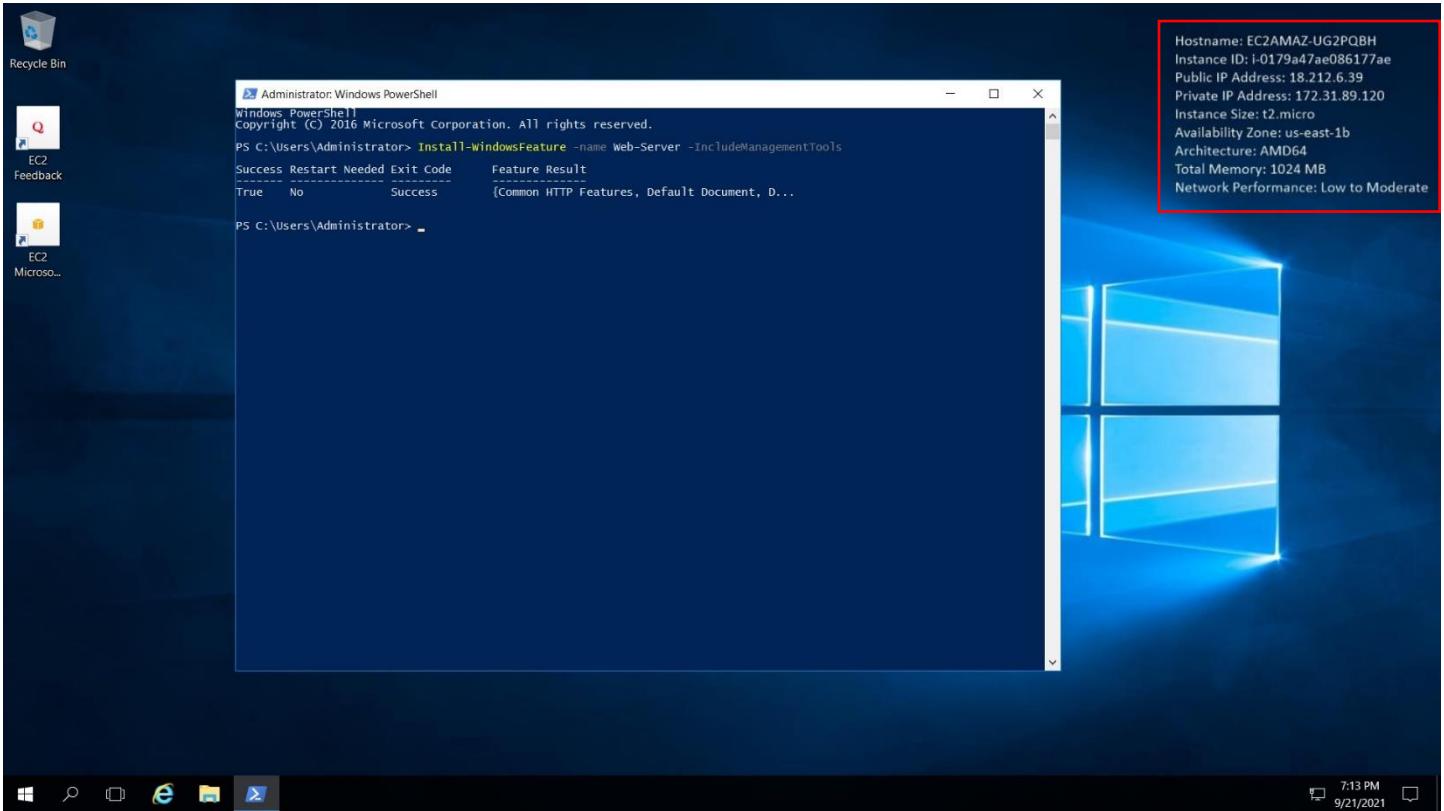
- Create S3 bucket

The screenshot shows the AWS S3 Management Console. A new bucket named "my-aws-bucket-bootcamp" has been created in the US East (N. Virginia) region. The bucket details are as follows:

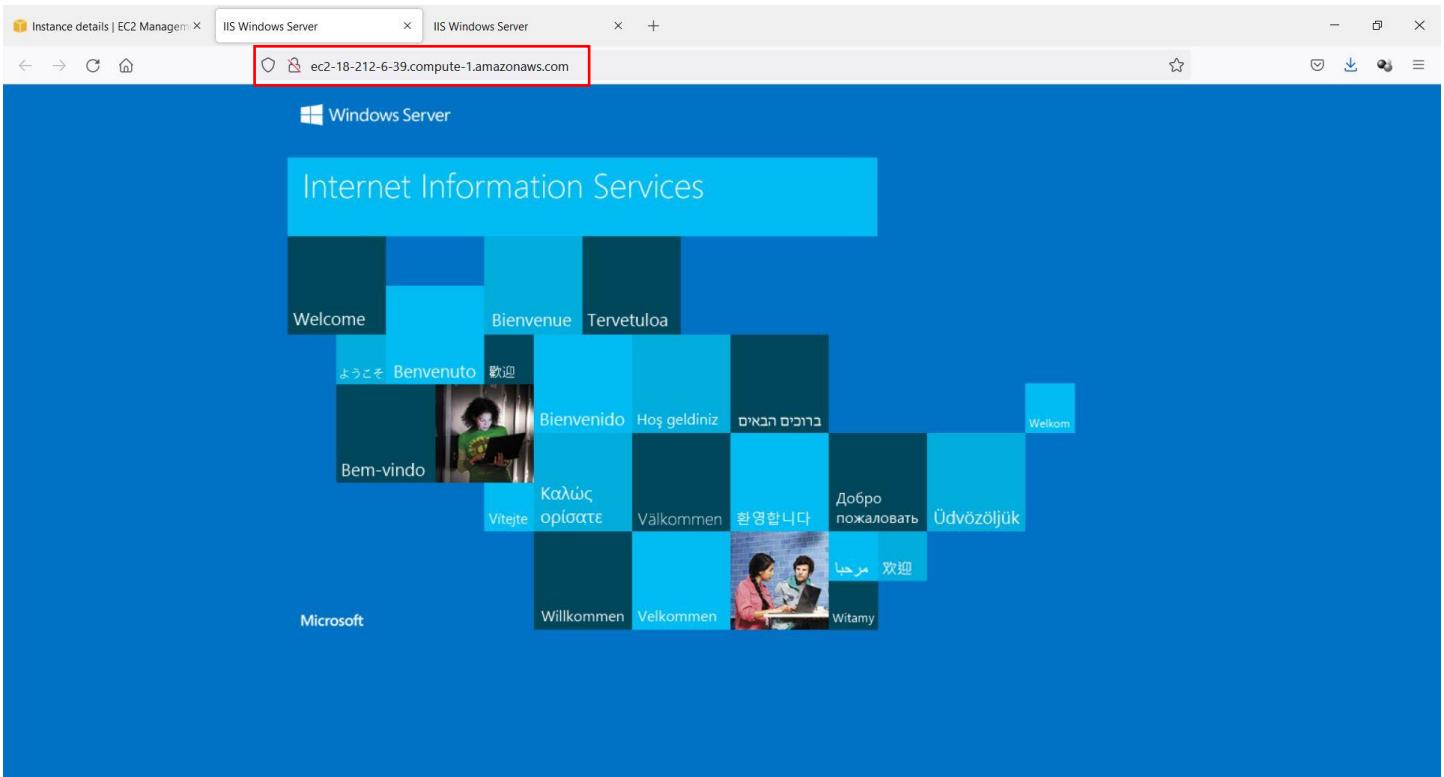
Name	AWS Region	Access	Creation date
my-aws-bucket-bootcamp	US East (N. Virginia) us-east-1	Bucket and objects not public	September 21, 2021, 14:24:03 (UTC-05:00)

The left sidebar shows the Buckets section with options like Access Points, Object Lambda Access Points, Multi-Region Access Points, and Batch Operations.

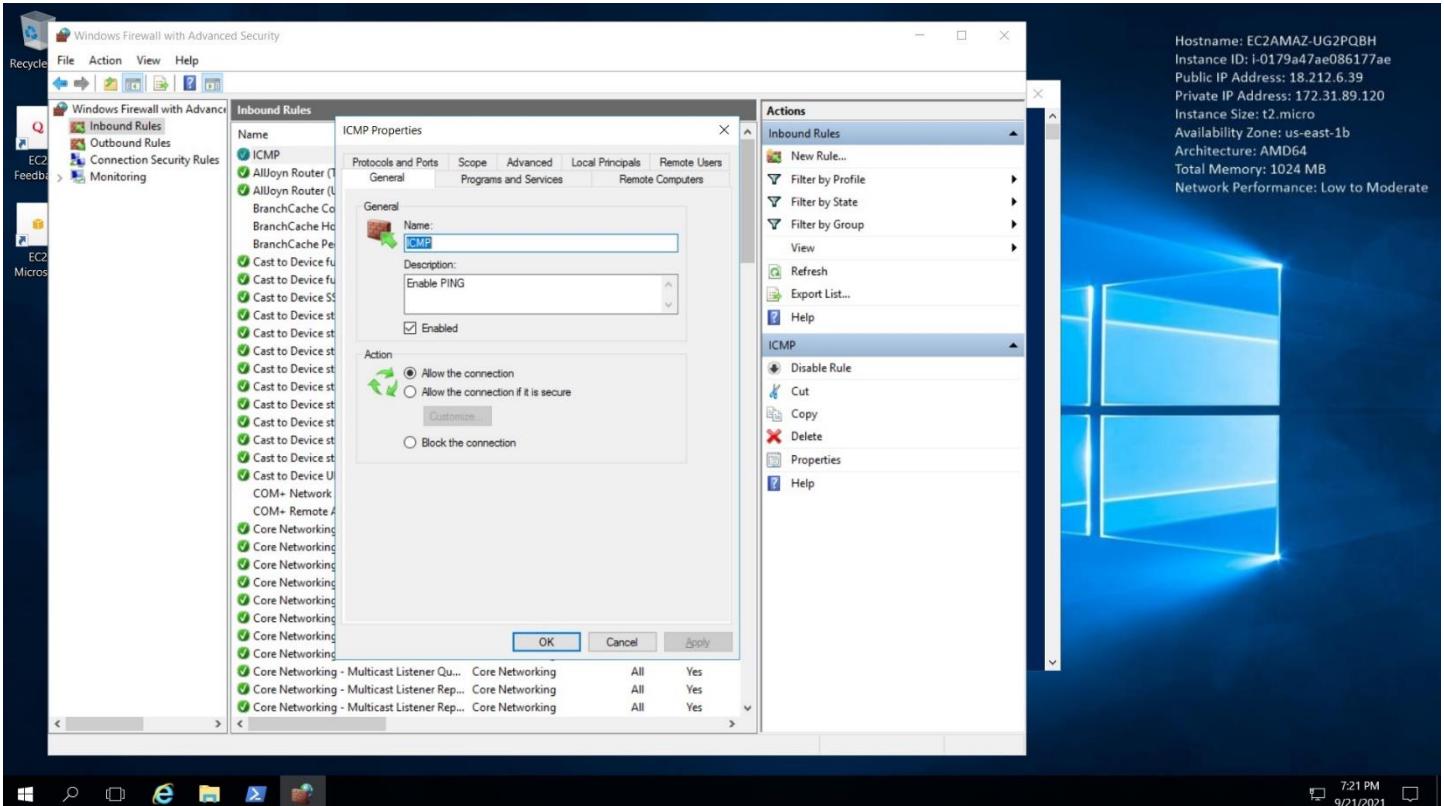
- Log in to instance console via remote desktop and install IIS web service.



- Test access web site over internet.



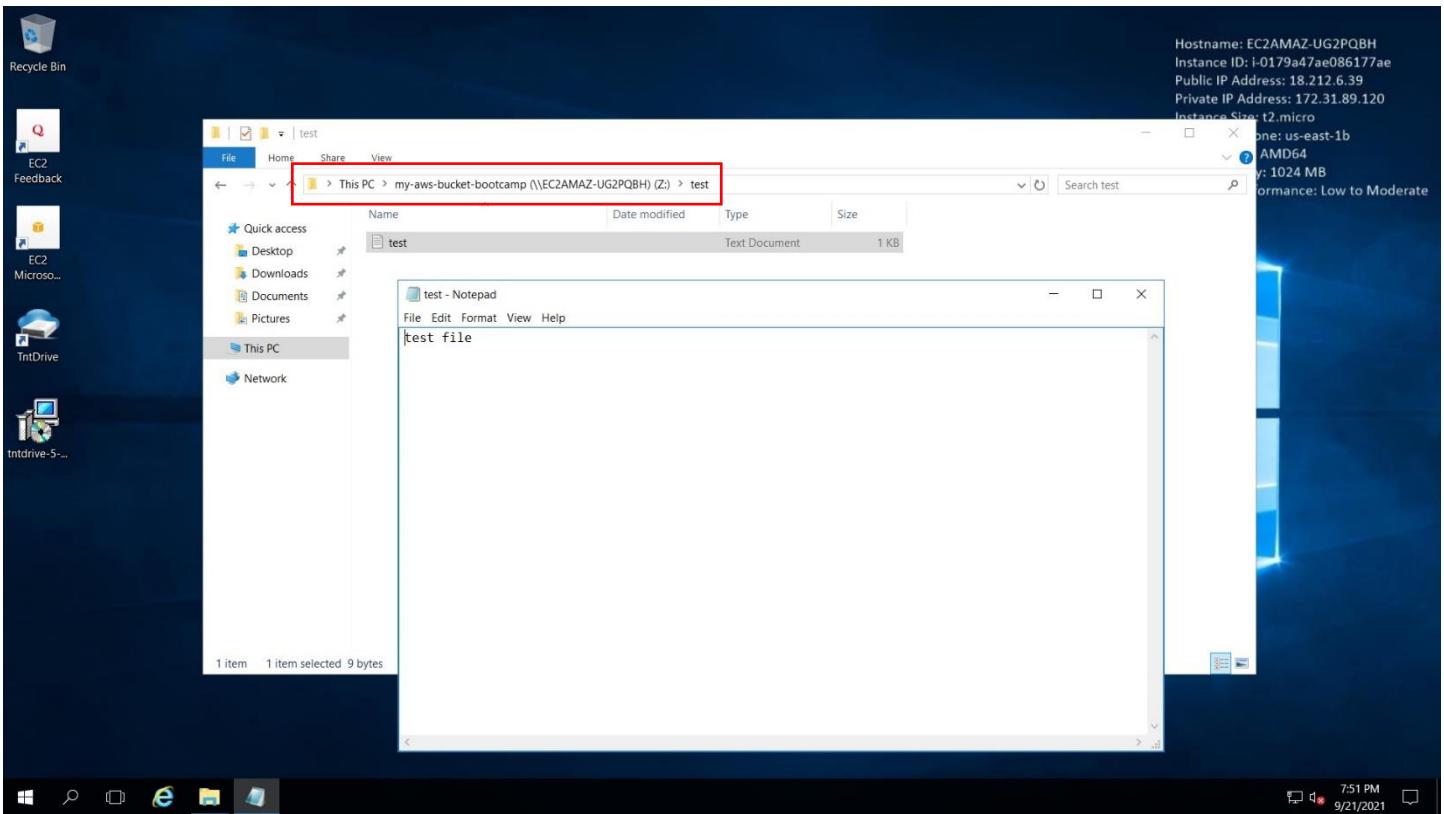
- Configure firewall rule to allow ICMP packets



- Test ping an instance

```
cmd Command Prompt
Ping statistics for 18.212.6.39:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\wuthi>ping 18.212.6.39
Pinging 18.212.6.39 with 32 bytes of data:
Reply from 18.212.6.39: bytes=32 time=45ms TTL=109
Reply from 18.212.6.39: bytes=32 time=41ms TTL=109
Reply from 18.212.6.39: bytes=32 time=57ms TTL=109
Reply from 18.212.6.39: bytes=32 time=43ms TTL=109
Ping statistics for 18.212.6.39:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 41ms, Maximum = 57ms, Average = 46ms
C:\Users\wuthi>ping ec2-18-212-6-39.compute-1.amazonaws.com
Pinging ec2-18-212-6-39.compute-1.amazonaws.com [18.212.6.39] with 32 bytes of data:
Reply from 18.212.6.39: bytes=32 time=48ms TTL=109
Reply from 18.212.6.39: bytes=32 time=46ms TTL=109
Reply from 18.212.6.39: bytes=32 time=42ms TTL=109
Reply from 18.212.6.39: bytes=32 time=42ms TTL=109
Ping statistics for 18.212.6.39:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 42ms, Maximum = 48ms, Average = 44ms
C:\Users\wuthi>
```

- Map S3 bucket to an instance and test create folder and file.



- Check data in S3 console

Amazon S3

Buckets

- Access Points
- Object Lambda Access Points
- Multi-Region Access Points
- Batch Operations
- Access analyzer for S3

Block Public Access settings for this account

Storage Lens

- Dashboards
- AWS Organizations settings

Feature spotlight (3)

AWS Marketplace for S3

Objects (1)

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

Name	Type	Last modified	Size	Storage class
test/	Folder	-	-	-

Feedback English (US) © 2008 - 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use Cookie preferences

- Install AWS cli and test access S3 bucket

The screenshot shows a Windows Command Prompt window titled "Command Prompt". The window contains the following text:

```
C:\Users\wuthi>aws configure
AWS Access Key ID [None]:
AWS Secret Access Key [None]:
Default region name [None]:
Default output format [None]

C:\Users\wuthi>aws s3 ls s3://my-aws-bucket-bootcamp
                           PRE test/

C:\Users\wuthi>aws s3 ls s3://my-aws-bucket-bootcamp
                           PRE test/

C:\Users\wuthi>aws s3 ls s3://my-aws-bucket-bootcamp --recursive
2021-09-21 14:50:42      0 test/
2021-09-21 14:51:19      9 test/test.txt

C:\Users\wuthi>aws s3 ls s3://my-aws-bucket-bootcamp --recursive --human-readable --summarize
2021-09-21 14:50:42      0 Bytes test/
2021-09-21 14:51:19      9 Bytes test/test.txt

Total Objects: 2
  Total Size: 9 Bytes

C:\Users\wuthi>
```

A blue rectangular box highlights the first three lines of the command history. A red rectangular box highlights the last four lines of the command history.